Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακή Εργασία

Αναζήτηση Επιθέσεων & Εξομοίωση Αντιπάλου με χρήση του MITRE ATT&CK Framework

Threat Hunting and Adversary Emulation through MITRE ATT&CK Framework

Μαραγκός - Μπέλμπας Ελπιδοφόρος
MTE2020

Επιβλέπων:

Γκρίτζαλης Στέφανος
Καθηγητής

Πειραιάς - Αθήνα, Ιούνιος 2022

.....

Ελπιδοφόρος Μαραγκός - Μπέλμπας
Τμήμα Ψηφιακών Συστημάτων
Πανεπιστήμιο Πειραιώς

Ευχαριστίες

Μέσω αυτής της εργασίας ολοκληρώνονται οι σπουδές μου στο μεταπτυχιακό πρόγραμμα σπουδών «Ασφάλεια Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιώς συνεπώς θα ήθελα να ευχαριστήσω τον κ. Γκρίτζαλη Στέφανο για την καθοδήγηση που μου παρείχε κατά την εκπόνηση της εργασίας αλλά και καθ' όλη τη διάρκεια της φοίτησής μου. Θα ήθελα επίσης να ευχαριστήσω τους γονείς μου για την συμπαράσταση, τη στήριξη και τη συνολική τους βοήθεια κατά τη διάρκεια των σπουδών μου.

Ιούνιος 2022

Περίληψη

Στην σύγχρονη εποχή οι επιτιθέμενοι προσπαθούν διαρκώς να παραβιάσουν εταιρείες και οργανισμούς με εξελιγμένες μεθόδους που είναι δύσκολες να εντοπιστούν. Από την άλλη πλευρά οι οργανισμοί προσπαθούν να ανταποκριθούν σε αυτές τις απειλές χρησιμοποιώντας reactive μεθόδους άμυνας που εστιάζουν στην αποτροπή και τον περιορισμό των περιστατικών που έχουν ήδη πραγματοποιηθεί, χρησιμοποιώντας τα πιο σύγχρονα και εξελιγμένα συστήματα ασφαλείας, όπως Next-Generation Firewalls, SIEMs, EDRs, IPSs κτλ.

Οι τεχνολογίες αυτές, σε συνδυασμό με άλλες μεθόδους reactive άμυνας, βοηθούν σε ένα βαθμό την προστασία ενάντια σε επιθέσεις, αλλά έχουν αποδειχθεί αναποτελεσματικές στην αντιμετώπιση εξελιγμένων επιτιθεμένων (Advanced Persistent Threat). Τα τελευταία χρόνια νέες τεχνικές, που περιλαμβάνουν proactive defense, όπως το Threat Hunting, έχουν προταθεί ως μία πιθανή λύση σε αυτό το πρόβλημα ώστε να δώσουν τη δυνατότητα στους οργανισμούς να εντοπίζουν έγκαιρα επιθέσεις οι οποίες έχουν περάσει απαρατήρητες τόσο από τα αυτοματοποιημένα συστήματα όσο και από το προσωπικό ασφαλείας τους. Ωστόσο, ακόμα και αυτές οι προσπάθειες από μόνες τους δεν είναι πάντα αρκετές για την αντιμετώπιση των συγχρόνων εξελιγμένων επιτιθεμένων όταν διεξάγουν μια στοχευμένη επίθεση ενάντια σε έναν οργανισμό.

Σε αυτή την εργασία παρουσιάζεται μια hybrid μεθοδολογία για proactive defense ως λύση σε αυτό το πρόβλημα η οποία βασίζεται στο MITRE ATT&CK Framework και συνδυάζει Threat Intelligence, Threat Hunting και Adversary Emulation με στόχο την βελτίωση της ικανότητας των Blue Team να αντιμετωπίζουν εξελιγμένους επιτιθέμενους. Μέσω της μεθοδολογίας αυτής οι οργανισμοί είναι σε θέση να υλοποιήσουν ένα αποτελεσματικό και συνεχές πρόγραμμα για το σχεδιασμό μηχανισμών εντοπισμού κακόβουλης δραστηριότητας οι οποίοι εστιάζουν σε συγκεκριμένα APT groups. Η μεθοδολογία δίνει τη δυνατότητα στις Blue Teams που δεν διαθέτουν την ικανότητα ή τους πόρους να διεξάγουν σύνθετα σενάρια Purple Teaming ή Adversary Emulation από μόνες τους, να παράγουν και να συλλέξουν τα δεδομένα που χρειάζονται ώστε να διαπιστώσουν ποιες ενέργειες ενός συγκεκριμένου επιτιθέμενου δεν μπορούν να εντοπίσουν αλλά και να αξιολογήσουν του μηχανισμούς ασφαλείας που έχουν ήδη υλοποιήσει.

Το τελικό επιδιωκόμενο αποτέλεσμα αυτής της προσέγγισης είναι η εδραίωση μιας συνεχούς διαδικασίας εντός του οργανισμού, που βασίζεται σε αυτή τη μεθοδολογία, υπό τη μορφή ενός προγράμματος Threat Detection Engineering που να έχει ως στόχο τον συνεχή έλεγχο, τη μέτρηση και τη βελτίωση της αποτελεσματικότητας της Blue Team να εντοπίζει και να αποτρέπει εξελιγμένους επιτιθέμενους σε αρχικό στάδιο.

Λέξεις Κλειδιά: Blue Team, Red Team, Advanced Persistent Threats, Threat Intelligence, MITRE ATT&CK Framework, Threat Hunting, Proactive Defense, Adversary Emulation, Attack Coverage Assessment

Abstract

Nowadays attackers are constantly trying to compromise organizations with advanced and stealthy methods. On the other hand, organizations are trying to encounter these threats by employing reactive approaches that focus on responding and preventing immediate incidents by using cutting edge technology solutions such as next Next-Generation Firewalls, SIEMs, EDRs, IPSs etc.

These solutions do help by improving the overall security posture of the organization but still remain ineffective against modern Advanced Persistent Threats (APTs) that are able to perform stealthy and sophisticated attacks. In the recent years, new proactive defense approaches such as Threat Hunting have been introduced as part of a solution to this problem that enable organizations to quickly identify and respond to any potential attacks that have not been identified by the security solutions in use but are still not good enough against APTs.

In this thesis, a proactive defense hybrid methodology is presented as a solution to this problem in order to improve the detection capabilities of a Blue Team by combining Threat Intelligence, Threat Hunting and Adversary Emulation though MITRE ATT&CK Framework. The methodology aims to help Blue Teams build an effective and continuous Detection Engineering process focused on combating APTs. The presented methodology enables Blue Teams that lack the ability or the resources to perform complex Purple Team engagements or Adversary Emulation exercises on their own to produce the necessary adversary behavior telemetry in order to be able to test their existing detection capabilities and tools, to identify visibility gaps within their environment, and to create new detection mechanisms that will help them respond to sophisticated attackers.

The final desired output of this approach would be the establishment of a continuous process within the organization, based on the methodology presented, in order to constantly test, measure and improve the effectiveness of the Threat Detection Engineering program so as to improve the overall security posture of the organization.

Keywords: Blue Team, Red Team, Advanced Persistent Threats, Threat Intelligence, MITRE ATT&CK Framework, Threat Hunting, Proactive Defense, Adversary Emulation, Attack Coverage Assessment

Πίνακας περιεχομένων

Πίνακας σχημάτων

Κεφάλαιο 1

Εισαγωγή

1.1 Σκοπός και στόχοι της εργασίας

Με τη συνεχή εξέλιξη και την αύξηση των επιθέσεων στον κυβερνοχώρο, οι οργανισμοί αναζητούν διαρκώς αποτελεσματικότερους τρόπους ώστε να αμυνθούν ενάντια στις σύγχρονες απειλές. Αντίστοιχα οι επιτιθέμενοι εξελίσσουν τις μεθόδους τους ώστε να γίνονται όλο και πιο αποτελεσματικοί στις επιθέσεις τους και να αποφεύγουν τον εντοπισμό.

Κάθε οργανισμός ανεξάρτητα του μεγέθους του ή της βιομηχανίας στην οποία δραστηριοποιείται προσπαθεί να βρει κάθε δυνατό τρόπο ώστε να προστατευτεί από κυβερνοεπιθέσεις. Για αυτό το λόγο και ένα μεγάλο ποσοστό από τον ετήσιο προϋπολογισμό για το Cyber Security πρόγραμμα του οργανισμού δαπανάται σε state-of-the-art τεχνολογίες και εργαλεία όπως Endpoint Detection and Response (EDR), Intrusion Prevention Systems (IPS), Next Generation Firewalls (NGFW) και Web Application Firewalls (WAF). Ενώ αυτή η στρατηγική τις περισσότερες φορές είναι αρκετή για να αποτρέψει τις περισσότερες από τις κοινές επιθέσεις, τα αυτοματοποιημένα εργαλεία όσο καινοτόμα και αν είναι, δεν είναι αρκετά για να σταματήσουν επιθέσεις από εξελιγμένους επιτιθέμενους όπως APTs (Advanced Persistent Threats). Το γεγονός αυτό δεν οφείλεται σε χαμηλή εξειδίκευση του προσωπικό ασφαλείας, σε ανθρώπινο λάθος ή σε χρήση λανθασμένων διαδικασιών και εργαλείων αλλά στο γεγονός ότι ο επιτιθέμενος συνήθως χρησιμοποιεί μεθόδους και τεχνικές που η ομάδα ασφαλείας του οργανισμού δεν γνωρίζει πως να εντοπίζει ή δεν είχε σχεδιάσει ακόμα τους κατάλληλους μηχανισμούς εντοπισμού αυτής της δραστηριότητας.

Λαμβάνοντας υπόψιν τα παραπάνω, είναι πολύ σημαντικό για τους επαγγελματίες ασφαλείας πριν προσπαθήσουν να οργανώσουν την άμυνα του οργανισμού που καλούνται να προστατεύσουν, να είναι σε θέση να κατανοήσουν όσο το δυνατόν περισσότερο τους επιτιθέμενους που θα κληθούν να αντιμετωπίσουν. Όσο πιο κατανοητός γίνει ο τρόπος με τον οποίο λειτουργούν, τόσο πιο αποτελεσματική και έγκαιρη θα είναι η αντιμετώπιση τους.

Για την αντιμετώπιση ενός συγκεκριμένου εξελιγμένου επιτιθέμενου πρέπει αρχικά να υπάρχουν διαθέσιμες πληροφορίες για τον τρόπο με τον οποίο πραγματοποιεί στις επιθέσεις του. Αυτές οι πληροφορίες μπορεί να είναι διαθέσιμες μέσω αναφορών από προηγούμενες επιθέσεις σε άλλους οργανισμούς αλλά να μην είναι πάντα αρκετές ώστε να μοντελοποιηθεί η συμπεριφορά του και να σχεδιαστούν μηχανισμοί εντοπισμού πάνω σε αυτή. Αυτό συμβαίνει διότι τα στοιχεία που θα αφήσει η διεξαγωγή των ενεργειών μιας επίθεσης (Indicators of Compromise) θα διαφέρουν ανάλογα το περιβάλλον που θα διεξαχθεί η επίθεση ή είναι εύκολο να αλλαχθούν από τον επιτιθέμενο σε επόμενες επιθέσεις, άρα δεν προσφέρουν μεγάλη αξία στην βελτίωση ικανότητας εντοπισμού του. Για τη δημιουργία αποτελεσματικότερων μηχανισμών εντοπισμού απαιτείται η προσομοίωση των ενεργειών του επιτιθέμενου ώστε να υπάρχουν πραγματικά δεδομένα στα οποία μπορεί να στηριχθεί ο σχεδιασμός των αμυντικών μηχανισμών και στη συνέχεια να επαληθευθούν ότι λειτουργούν. Το βασικό πρόβλημα όμως σε αυτή τη διαδικασία είναι πως η αναπαραγωγή της δραστηριότητας του επιτιθέμενου απαιτεί εξειδικευμένες γνώσεις που συνήθως δεν διαθέτει το

προσωπικό ασφαλείας του οργανισμού.

Βασικό κίνητρο και πηγή έμπνευσης για την εκπόνηση αυτής της εργασίας αποτέλεσαν οι δυσκολίες που αντιμετωπίζει το προσωπικό ασφαλείας (Blue Team) στην προσπάθειά του να αναπαράγει τη δραστηριότητα των επιτιθεμένων ώστε να παράξει τα δεδομένα που απαιτούνται για τη μοντελοποίηση της συμπεριφοράς του και για το σχεδιασμών μηχανισμών εντοπισμού.

Απώτερος στόχος της εργασίας είναι η ανάδειξη της αξίας συνδυασμού διαφορετικών proactive μεθόδων άμυνας, υπό ένα κοινό Framework, για τον εντοπισμό και την επαλήθευση κενών στην ικανότητα του οργανισμού να εντοπίζει έγκαιρα τη δραστηριότητα των επιτιθεμένων. Αυτό επιτυγχάνεται μέσω μιας μεθοδολογίας που δεν εξαρτάται από συγκεκριμένα εργαλεία και να μπορεί να αξιοποιηθεί από το προσωπικό ασφαλείας του οργανισμού που δεν διαθέτει εξειδικευμένες γνώσεις και λειτουργεί υπό περιορισμούς.

1.2 Συνεισφορά εργασίας

Η παρούσα εργασία συνεισφέρει αρχικά αναλύοντας σε βάθος έννοιες και οντότητες στον κυβερνοχώρο που συχνά συγχέονται αλλά είναι απαραίτητες για την κατανόηση πιο συνθέτων εννοιών που αξιοποιούνται στα πλαίσια της προτεινόμενης μεθοδολογίας. Παρουσιάζονται οι προκλήσεις που αντιμετωπίζουν οι Blue Teams στη σύγχρονη εποχή και οι λόγοι για τους οποίους είναι αναγκαία η μετάβαση σε proactive μεθόδους άμυνας για την αντιμετώπιση εξελιγμένων επιτιθεμένων (APT groups).

Αναλύονται έννοιες όπως Threat Intelligence, Threat Hunting και Adversary Emulation, παρουσιάζονται οι διαφορετικές τους κατηγορίες αλλά και ο τρόπος με τον οποίο μπορούν να συνδυαστούν με την αξιοποίηση σύγχρονων Framework, όπως το MITRE ATT&CK, για την μοντελοποίηση και την καλύτερη κατανόηση της συμπεριφοράς των επιτιθεμένων. Γίνεται ανάλυση και συγκριτική αξιολόγηση εργαλείων που επιτρέπουν τη διεξαγωγή μερικώς αυτοματοποιημένου Adversary Emulation σε περιβάλλον που είναι ειδικά σχεδιασμένο για τη διεξαγωγή αντίστοιχων δοκιμών.

Τέλος προτείνεται μία μεθοδολογία για τη διεξαγωγή ενός Defensive Gap / Attack Coverage Assessment που βασίζεται στο MITRE ATT&CK Framework και συνδυάζει Threat Intelligence, Threat Hunting και Adversary Emulation. Η μεθοδολογία παρέχει τη δυνατότητα στις Blue Teams που δεν διαθέτουν την ικανότητα ή τους πόρους για να διεξάγουν από μόνες τους σύνθετα σενάρια Purple Teaming ή Adversary Emulation, να παράγουν και να συλλέξουν τα απαραίτητα δεδομένα ώστε να διαπιστώσουν ποιες δραστηριότητες ενός επιτιθέμενου δεν μπορούν να εντοπίσουν, να αξιολογήσουν τους μηχανισμούς ασφαλείας που έχουν ήδη υλοποιήσει αλλά και να δημιουργήσουν νέους.

1.3 Διάρθρωση εργασίας

Η εργασία είναι χωρισμένη σε δέκα κεφάλαια, όπου καθένα από αυτά είναι χωρισμένα σε μικρότερες υπό ενότητες.

Κεφάλαιο 1: Εισαγωγή

Στο πρώτο κεφάλαιο γίνεται μία γρήγορη εισαγωγή στο θέμα της εργασίας που περιλαμβάνει το σκοπό διεξαγωγής και τους στόχους της. Επιπλέον γίνεται αναφορά στη συνεισφορά της εργασίας και στη διάρθρωση των κεφαλαίων.

Κεφάλαιο 2: Βασικές έννοιες και οντότητες

Στο δεύτερο κεφάλαιο γίνεται αναφορά σε βασικές έννοιες και οντότητες οι οποίες θα χρησιμοποιηθούν εκτενώς στα επόμενα κεφάλαια συνεπώς είναι απαραίτητο να έχουν πρώτα αναλυθεί. Δίνεται ο ορισμός ενός Adversary ή Cyber Threat Actor και οι διαφορετικές τους κατηγορίες συνοδευόμενες από παραδείγματα. Στη συνέχεια παρουσιάζονται οι έννοιες της Blue και της Red Team

μαζί με το σκοπό που εξυπηρετεί η κάθε μία αλλά και με τις προκλήσεις που αντιμετωπίζουν στη σύγχρονη εποχή.

Κεφάλαιο 3: Cyber Threat Intelligence

Στο τρίτο κεφάλαιο δίνεται ο ορισμός του Cyber Threat Intelligence (CTI) με τις διαφορετικές κατηγορίες που υπάρχουν, αναλύονται τα βήματα του CTI Life-Cycle και παρουσιάζονται δύο δημοφιλή Frameworks που μπορούν να αξιοποιηθούν για τη δραστηριότητα αυτή. Πιο συγκεκριμένα παρουσιάζεται το Cyber Kill Chain Framework της Lockheed Martin και το ATT&CK της MITRE με έμφαση περισσότερο στο δεύτερο καθώς, πέρα από το ότι είναι το πιο ολοκληρωμένο και ευρέως αποδεκτό, σε αυτό βασίζονται και τα επόμενα κεφάλαια της εργασίας.

Κεφάλαιο 4: Cyber Threat Hunting

Στο τέταρτο κεφάλαιο αναλύονται ο λόγοι για τους οποίους κρίνεται αναγκαία η μετάβαση από reactive σε proactive μεθόδους άμυνας στη σύγχρονη εποχή όπως το Thread Hunting (TH). Δίνεται ο ορισμός του και αναλύονται οι διαφορετικές κατηγορίες που υπάρχουν. Επιπλέον δίνεται ο ορισμός των Indicator of Compromise (IoC), παρουσιάζονται οι διαφορετικές τους κατηγορίες και πώς είναι εφικτό να κατηγοριοποιηθούν μέσω του Pyramid of Pain ανάλογα με την αξία τους. Στο τέλος του κεφαλαίου αναλύονται τα βήματα που απαιτούνται για τη διεξαγωγή μίας ολοκληρωμένης άσκησης TH και γίνεται αναφορά στη σημασία και στα οφέλη διεξαγωγής της.

Κεφάλαιο 5: Adversary Emulation

Το πέμπτο κεφάλαιο εστιάζει στο Adversary Emulation. Προτού δοθεί ο ορισμός του, γίνεται αναφορά στο SCYTHE Ethical Hacking Maturity Model με σκοπό τη σύγκριση του Adversary Emulation με άλλες δραστηριότητες που παρουσιάστηκαν σε προηγούμενα κεφάλαια. Ο σκοπός αυτής της σύγκρισης εξυπηρετεί στο να δοθεί ένας πιο σαφής ορισμός και να αναδειχθεί η αξία του αλλά και οι διαφορές του ανάμεσα στις υπόλοιπες κατηγορίες. Στη συνέχεια γίνεται εισαγωγή στο πώς μπορεί να αξιοποιηθεί το MITRE ATT&CK framework για τη διεξαγωγή Adversary Emulation παρουσιάζοντας τα Adversary Emulation Plans και τα βήματα με τα οποία μπορεί να δημιουργηθεί ένα αντίστοιχο. Τέλος γίνεται αναφορά σε εργαλεία που μπορούν να αξιοποιηθούν για τη διεξαγωγή του Adversary Emulation.

Κεφάλαιο 6: Δημιουργία περιβάλλοντος δοκιμών με τη χρήση του DetectionLab

Στο έκτο κεφάλαιο παρουσιάζεται η διαδικασία δημιουργίας ενός δοκιμαστικού περιβάλλοντος για τη διεξαγωγή των πειραμάτων που θα διεξαχθούν. Αξιοποιείται τον DetectionLab που επιτρέπει την αυτοματοποίηση της διαδικασίας δημιουργίας ενός Active Directory τοπικού δικτύου και αναλύονται τόσο τα χαρακτηριστικά του όσο και η διαδικασία εγκατάστασης του. Τέλος, παρουσιάζεται η διαδικασία προσαρμογής του, με την εισαγωγή κοινών αδυναμιών ώστε να είναι ευάλωτο, βοηθώντας στη διεξαγωγή περισσότερων σεναρίων επιθέσεων.

Κεφάλαιο 7: Adversary Emulation στο DetectionLab

Στο έβδομο κεφάλαιο διεξάγονται τα πειράματα, δηλαδή πραγματοποιείται το Adversary Emulation τόσο ενός συγκεκριμένου APT όσο και προσαρμοσμένων TTPs και Emulation Plans ως παραδείγματα. Γίνεται χρήση διαφορετικών εργαλείων και παρουσιάζονται ενδεικτικά σενάρια ενεργειών που θα πραγματοποιούσε ένας επιτιθέμενος.

Κεφάλαιο 8: Συλλογή αποτελεσμάτων Emulation

Στο όγδοο κεφάλαιο παρουσιάζεται η διαδικασία συλλογής των αποτελεσμάτων από τα πειράματα που διεξήχθησαν στο προηγούμενο κεφάλαιο μέσω του Splunk SIEM που αποτελεί μέρος του DetectionLab. Τα ενδεικτικά δεδομένα που συλλέγονται σε αυτό το κεφάλαιο τροφοδοτούν την ανάλυση που θα πραγματοποιηθεί στο επόμενο κεφάλαιο για την εξαγωγή των συμπερασμάτων.

Κεφάλαιο 9: Αξιολόγηση αποτελεσμάτων

Στο ένατο κεφάλαιο παρουσιάζεται ο τρόπος με τον οποίο τα δεδομένα που συλλέχθηκαν από τη διεξαγωγή του Adversary Emulation μπορούν να αναλυθούν με σκοπό τη διεξαγωγή ενός Defensive GAP / Attack Coverage Assessment. Παρουσιάζονται οι τρόποι με τους οποίους μπορεί να διεξαχθεί μία τέτοια μελέτη και πιο συγκεκριμένα γίνεται η παρουσίαση του VECTR, ενός

εργαλείου το οποίο αυτοματοποιεί σε μεγάλο βαθμό αυτή τη διαδικασία. Επιπλέον, ως τελικό παράγωγο της εργασίας, γίνεται παρουσίαση μιας μεθοδολογίας μέσω της οποίας δίνεται η δυνατότητα σε Blue Teams με περιορισμένους πόρους και μέσα να συνδυάζουν Threat Intelligence, Threat Hunting και Adversary Emulation για τη βελτίωση της ικανότητας τους να αντιμετωπίζουν εξελιγμένους επιτιθέμενους.

Κεφάλαιο 10: Επίλογος

Στο δέκατο και τελευταίο κεφάλαιο γίνεται αναφορά στα συμπεράσματα που μπορούν να εξαχθούν από την εργασία και παρουσιάζονται μελλοντικές επεκτάσεις σχετικά με τους τρόπους με τους οποίους η έρευνα θα μπορούσε να συνεχιστεί.

Κεφάλαιο 2

Βασικές έννοιες και οντότητες

2.1 Adversary - Cyber Threat Actors

Είναι πολύ σημαντικό για τους επαγγελματίες ασφαλείας, πριν προσπαθήσουν να οργανώσουν την άμυνα του οργανισμού που καλούνται να προστατεύσουν, να κατανοήσουν όσο το δυνατόν περισσότερο τους επιτιθέμενους που ενδέχεται να κληθούν να αντιμετωπίσουν. Όσο πιο κατανοητός γίνει ο τρόπος με τον οποίο λειτουργεί ο κάθε επιτιθέμενος, τόσο πιο αποτελεσματική και έγκαιρη θα είναι και η αντιμετώπιση του. Αυτό περιλαμβάνει τόσο τις τεχνικές λεπτομέρειες για τα εργαλεία και τις μεθόδους που χρησιμοποιεί, αλλά και άλλα ιδιαίτερα χαρακτηριστικά του που μπορεί να βοηθήσουν στην μελέτη και την αντιμετώπιση του, όπως τα πιθανά τους κίνητρα, το επίπεδο των ικανοτήτων τους ή το βαθμό οργάνωσης. Ο NIST ορίζει έναν Threat Actor ως «ένα άτομο ή μια ομάδα που αποτελεί μια απειλή». [1]

Αν και ο ορισμός αυτός είναι ακριβής, είναι ταυτόχρονα και αρκετά αόριστος και γενικός. Ένας άλλος κοινός όρος που χρησιμοποιείται όταν προσπαθούμε να περιγράψουμε έναν Threat Actor είναι αυτός του Adversary. Σύμφωνα πάλι με τον ορισμό που δίνει ο NIST, Adversary είναι ένα «άτομο, μια ομάδα, ένας οργανισμός ή μια κυβέρνηση που διεξάγει ή έχει την πρόθεση να διεξάγει κακόβουλες δραστηριότητες» αλλά και ως «μια οντότητα που δεν είναι εξουσιοδοτημένη να έχει πρόσβαση σε πληροφορίες και που προσπαθεί παρ' όλα αυτά να παρακάμψει οποιαδήποτε μέτρο προστατεύει αυτές τις πληροφορίες ώστε να τις αποκτήσει.» [2]

Συνεπώς, με βάση τους ορισμούς αυτούς, θα μπορούσαμε να περιγράψουμε έναν Adversary ή αλλιώς και ένα Cyber Threat Actor (CTA) ως μια οντότητα που λαμβάνει μέρος σε κακόβουλες ενέργειες, χρησιμοποιώντας συστήματα και δίκτυα υπολογιστών. Εάν θέλουμε να το κάνουμε ακόμη πιο συγκεκριμένο, θα μπορούσαμε να περιγράψουμε ένα CTA ως ένα άτομο ή μια ομάδα με κακόβουλες προθέσεις που στοχεύει να εκμεταλλευτεί ευπάθειες ή αδυναμίες ασφαλείας προκειμένου να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφοριών. Κάθε CTA διαφέρει, καθώς διαθέτει τα δικά του ιδιαίτερα χαρακτηριστικά, όπως διαφορετική δομή, μέγεθος, κίνητρο, τεχνογνωσία, οικονομικούς πόρους κ.α. Ένας CTA θα μπορούσε να είναι ένα μεμονωμένο άτομο που ενεργεί μόνο του, δίχως εξειδικευμένες γνώσεις, χρησιμοποιώντας έτοιμα εργαλεία και με βασικό κίνητρο το οικονομικό όφελος. Από την άλλη θα μπορούσε να είναι μια ολόκληρη ομάδα εξειδικευμένων επαγγελματιών ασφαλείας που εργάζεται για μια κυβέρνηση, με πολύ υψηλό επίπεδο τεχνογνωσίας και με μεγάλη χρηματοδότηση, που ως βασικό κίνητρο έχει την κατασκοπία και την συλλογή απορρήτων πληροφοριών σχετικά με το πυρηνικό πρόγραμμα ενός άλλου κράτους.

Είναι εμφανές λοιπόν πως υπάρχουν διαφορετικές κατηγορίες CTA που διαφέρουν σε πολλές παραμέτρους μεταξύ τους. Η κατηγοριοποίηση και η κατανόηση τους δεν είναι απλή διαδικασία αλλά συνήθως χρησιμοποιείται το κίνητρο για τον διαχωρισμό τους σε υποομάδες. Μπορούν επίσης να κατηγοριοποιηθούν σε κάποιο βαθμό, ανάλογα και με το επίπεδο των ικανοτήτων τους, αλλά αυτός ο τύπος κατηγοριοποίησης δεν είναι πάντα τόσο εύστοχος και ακριβής, καθώς δεν

είναι ασυνήθιστο ακόμη και για αρκετά εξελιγμένους CTAs να χρησιμοποιούν ευρέως διαθέσιμα και λιγότερο εξελιγμένα εργαλεία και τεχνικές για να πετύχουν το στόχο τους. [3]

Οι CTAs που διαθέτουν υψηλό επίπεδο οργάνωσης και δεξιοτήτων αλλά και είναι σε θέση να χρησιμοποιήσουν προηγμένες τεχνικές για τη διεξαγωγή σύνθετων αλλά και πολύ αποτελεσματικών επιθέσεων χωρίς να γίνονται αντιληπτοί ονομάζονται Advanced Persistent Threats (APT). Ο όρος αυτός δίνεται συνήθως σε CTAs που αποτελούνται από κυβερνητικές ομάδες ή από πολύ επιτυχημένες και ικανές ομάδες οργανωμένου κυβερνοεγκλήματος. Συνεπώς η κατανόηση των χαρακτηριστικών κάθε CTA θα βοηθήσει τους επαγγελματίες ασφαλείας που προστατεύουν την εκάστοτε επιχείρηση ή οργανισμό να δημιουργήσουν κατάλληλες προστασίες και αντίμετρα ώστε να αμυνθούν όσο το δυνατόν πιο αποτελεσματικά εναντίον τους, αποτρέποντας μια κυβερνοεπίθεση. Επομένως, είναι χρήσιμο στα πλαίσια αυτής εργασίας να αναφέρουμε τις κυριότερες κατηγορίες CTA που ανήκουν στην κατηγορία των Advanced Persistent Threats (APT) και να αναλύσουμε μερικά από τα χαρακτηριστικά τους, καθώς η μελέτη εστιάζει στην προσπάθεια έγκαιρου εντοπισμού αυτών. [4, 5, 6, 7]

Κυβερνητικές ομάδες:

Οι κυβερνητικές ομάδες (Nation-State actors) είναι συνήθως οι πιο εξελιγμένοι και ικανοί CTAs λόγω της ισχυρής χρηματοδότησης που διαθέτουν, του εκτενή σχεδιασμού και συντονισμού αλλά και της ικανότητάς τους να λειτουργούν δίχως τον κίνδυνο νομικών επιπτώσεων, τουλάχιστον εντός της χώρας που ενεργούν, καθώς πρακτικά ενεργούν υπό τις εντολές και την αιγίδα της εκάστοτε κυβέρνησης. Αυτό επιτρέπει την στελέχωση τους με μεγάλο αριθμό εξειδικευμένου προσωπικού με υψηλό επίπεδο τεχνογνωσίας, επιτρέποντας την ανάπτυξη ειδικών εργαλείων και νέων μεθόδων γεγονός που καθιστά τις επιχειρήσεις τους αποτελεσματικές αλλά και ιδιαίτερα δύσκολες να εντοπιστούν.

Βασικά Κίνητρα	Κατασκοπεία, Γεωπολιτικά, Οικονομικά, Στρατιωτικές Επιχειρήσεις
Συνηθισμένες Τεχνικές	Spear-phishing, Social Engineering, 0-day vulnerabilities, Data exfiltration, Persistence

Εικόνα 1. Χαρακτηριστικά Cyber Threat Actor - Κυβερνητικές ομάδες

Οργανωμένο Έγκλημα:

Οι ομάδες από οργανωμένους κυβερνοεγκληματίες αποτελούν την πιο κοινή κατηγορία CTA. Υπάρχει μεγάλη διαβάθμιση στο επίπεδο των ικανοτήτων κάθε ομάδας, καθώς μερικές από αυτές ασχολούνται με μικρότερης κλίμακας οικονομικές απάτες στοχεύοντας μεμονωμένους χρήστες, ενώ άλλες στοχεύουν μεγάλες επιχειρήσεις με πολύτιμα δεδομένα με σκοπό, είτε να τα αποκτήσουν για να τα μεταπωλήσουν, είτε για να τα κρυπτογραφήσουν με χρήση Ransomware, ώστε να ζητήσουν λύτρα για την αποκρυπτογράφηση τους αλλά και για να μην τα διαρρεύσουν. Παρά τις διαφορές τους, όλες αυτές οι ομάδες κυβερνο-εγκληματιών διαθέτουν ως βασικό τους κίνητρο το οικονομικό όφελος. Οι περισσότερες από αυτές διαθέτουν συνήθως από χαμηλό έως μέτριο επίπεδο τεχνογνωσίας και ικανοτήτων. Παρ' όλα αυτά υπάρχουν μερικές ομάδες που έχουν χαρακτηριστεί από τη διεθνή κοινότητα ως APTs λόγω του πολύ υψηλού επιπέδου τεχνογνωσίας που διαθέτουν, φτάνοντας το επίπεδο και την αποτελεσματικότητά κυβερνητικών ομάδων, έχοντας καταφέρει να πλήξουν πολύ υψηλού προφίλ στόχους.

Βασικά Κίνητρα	Οικονομικό όφελος
Συνηθισμένες Τεχνικές	Phishing, Social Engineering, Business email compromise, Botnets, Exploit kits, Malware Infection, Ransomware

Εικόνα 2. Χαρακτηριστικά Cyber Threat Actor - Οργανωμένο Έγκλημα

Χακτιβιστές:

Οι Χακτιβιστές (Hacktivists) είναι μεμονωμένα άτομα ή συνήθως μικρές ομάδες χωρίς αυστηρή δομή ή ιεραρχία που διαθέτουν πολιτικά, κοινωνικά, θρησκευτικά ή ιδεολογικά κίνητρα. Στοχεύουν άτομα, εταιρίες ή οργανισμούς για να περάσουν ένα μήνυμα στο ευρύ κοινό, το οποίο επιθυμούν συνήθως να επιφέρει μια συγκεκριμένη κοινωνικοπολιτική αλλαγή. Από πλευράς ικανοτήτων, συνήθως βρίσκονται σε χαμηλά επίπεδα συγκριτικά με άλλους CTAs, καθώς βασίζονται κυρίως σε ευρέως διαθέσιμα εργαλεία και τεχνικές για την πραγματοποίηση των επιθέσεων τους. Επιπλέον οι ενέργειές τους, τις περισσότερες φορές δεν έχουν σοβαρή επίπτωση στους στόχους τους καθώς λόγω των περιορισμένων ικανοτήτων τους επιλέγουν επιθέσεις όπως DDoS attacks ή Website Defacements για να πετύχουν το στόχο τους.

Βασικά Κίνητρα	Πολιτικά, Κοινωνικά, Θρησκευτικά ή Ιδεολογικά κίνητρα
Συνηθισμένες Τεχνικές	DDoS attacks, Doxing, Website Defacements, Leak of private information

Εικόνα 3. Χαρακτηριστικά Cyber Threat Actor - Χακτιβιστές

Τρομοκρατικές οργανώσεις:

Οι τρομοκρατικές οργανώσεις είναι ίσως από τις πιο σπάνιες κατηγορίες ενός CTA καθώς συνήθως χρησιμοποιούν το διαδίκτυο και γενικότερα την τεχνολογία για επικοινωνία, στρατολόγηση και προπαγάνδα παρά για διαπράξουν επιθετικές επιχειρήσεις με μορφή κυβερνοεπιθέσεων εναντίων των στόχων τους. Ωστόσο αποτελούν πλέον μια υπαρκτή υποκατηγορία CTA που σε καμία περίπτωση δεν θα έπρεπε να υποτιμηθεί, καθώς οι επιθέσεις τους στις κρίσιμες υποδομές ενός κράτους θα μπορούσαν να έχουν πολύ σοβαρές επιπτώσεις. Ως κρίσιμη υποδομή ορίζεται οποιαδήποτε υποδομή ή υπηρεσία της οποίας, εάν η ομαλή της λειτουργία διαταραχθεί, αναμένεται να υπάρξουν σημαντικές αρνητικές επιπτώσεις στην εύρυθμη λειτουργία του κρατικού μηχανισμού και στη ζωή των πολιτών. Τέτοιες υποδομές αποτελούν τα αεροδρόμια, τα ΜΜΜ, εργοστάσια, νοσοκομεία και άλλες κρατικές υποδομές όπου μια επίθεση σε αυτές θα μπορούσε να επιφέρει εξίσου καταστροφικές επιπτώσεις στην κοινωνία όσο ένα φυσικό τρομοκρατικό χτύπημα. Ένα χαρακτηριστικό παράδειγμα αποτελεί μια επίθεση που δέχθηκε η εγκατάσταση επεξεργασίας νερού στην πολιτεία της Φλόριντα των ΗΠΑ. Ο επιτιθέμενος κατάφερε να αλλάξει τα επίπεδα υδροξειδίου του νατρίου στο νερό, καθιστώντας το επικίνδυνο και ακατάλληλο προς κατανάλωση, θέτοντας σε κίνδυνο την υγεία χιλιάδων πολιτών. [8]

Βασικά Κίνητρα	Πολιτικά ή Ιδεολογικά κίνητρα, Οικονομικό όφελος για τη χρηματοδότηση δραστηριοτήτων, Κατασκοπία, Προπαγάνδα, Πρόκληση πανικού ή αποσταθεροποίησης, Εκδίκηση
Συνηθισμένες Τεχνικές	Website Defacements, Ransomware, Καταστροφικό Malware

Εικόνα 4. Χαρακτηριστικά Cyber Threat Actor - Τρομοκρατικές οργανώσεις

2.1.1 APT Groups

Έχοντας παρουσιάσει τις βασικές κατηγορίες των CTAs που διαθέτουν ικανότητες επιπέδου Advanced Persistent Threat (APT) είναι χρήσιμο να αναφερθούν και μερικά από τα πιο γνωστά και επιτυχημένα APT groups που έχουν αναλυθεί εκτενώς από τη διεθνή κοινότητα. [9, 10, 11]

Cozy Bear (APT29)

Η ομάδα Cozy Bear (APT29) είναι ένα APT group με χώρα προέλευσης και βάση τη Ρωσία όπου υπάρχουν ενδείξεις ότι ενεργεί για λογαριασμό των Ρωσικών Υπηρεσιών Πληροφοριών. Η δράση του group ξεκινά το 2008 οπότε εξαπολύει τις πρώτες επιθέσεις, συχνά ενάντια σε κυβερνητικές υποδομές κρατών της ΕΕ ή του ΝΑΤΟ, ερευνητικά ινστιτούτα ή “think tanks”. Ένα από τα

ιδιαίτερα χαρακτηριστικά του mondus operandi του συγκεκριμένου group είναι η ικανότητα της διατήρησης της πρόσβασης (persistence) στα παραβιασμένα συστήματα αλλά και οι επανειλημμένες προσπάθειες για την επανάκτηση της πρόσβασης σε στόχους όπου είχε χαθεί η πρόσβαση. Τον Απρίλιο του 2021 οι κυβερνήσεις των ΗΠΑ και του Ηνωμένου Βασιλείου σε ανεξάρτητες τους ανακοινώσεις συσχέτισαν την επίθεση εφοδιαστικής αλυσίδας στην SolarWinds με του συγκεκριμένο group. Τα θύματα της συγκεκριμένης επίθεσης συμπεριλαμβάνουν κυβερνήσεις αλλά και επιχειρήσεις στον χώρο της τεχνολογίας, της συμβουλευτικής, των τηλεπικοινωνιών ανά τον κόσμο. [12]

Cobalt Group

Το Cobalt Group είναι μια εγκληματική ομάδα με αμιγώς οικονομικά κίνητρα, που δραστηριοποιείται από το 2016 και είναι υπεύθυνη για επιθέσεις κατά χρηματοπιστωτικών ιδρυμάτων σε διάφορες χώρες ανά τον κόσμο. Ενώ το Cobalt Group αρχικά στόχευε τη Ρωσία, από το 2019 οι εκστρατείες του επικεντρώθηκαν σε χρηματοπιστωτικά ιδρύματα στην Ευρώπη, τη Μέση Ανατολή αλλά και την Κεντρική και Νότια Αμερική. Η ομάδα έχει πραγματοποιήσει εισβολές για να αποσπάσει χρηματικά ποσά στοχεύοντας από ATMs, και συστήματα έκδοσης καρτών, μέχρι και συστημάτων πληρωμών SWIFT. Ένας από τους φερόμενους ηγέτες συνελήφθη στην Ισπανία στις αρχές του 2018, αλλά η ομάδα εξακολουθεί να φαίνεται ενεργή. [13]

Lazarus Group

Το Lazarus Group είναι ένα από τα πιο γνωστά APTs της Βόρειας Κορέας και δραστηριοποιείται από το 2009 σε επιχειρήσεις με στόχο τη συλλογή πολιτικών, στρατιωτικών και οικονομικών πληροφοριών για αντίπαλα κράτη αλλά και για τη συγκέντρωση οικονομικών πόρων. Η συγκεκριμένη ομάδα φαίνεται να σχετίζεται με το Reconnaissance General Bureau, μια υπηρεσία πληροφοριών της Βόρειας Κορέας που διαχειρίζεται τις μυστικές επιχειρήσεις του κράτους. Πιο συγκεκριμένα η ομάδα φέρεται να ήταν υπεύθυνη για την καταστροφική επίθεση τον Νοέμβριο του 2014 κατά της Sony Pictures Entertainment ως μέρος μιας καμπάνιας με το όνομα Operation Blockbuster by Novetta. [13]

Wicked Panda (APT41)

Η ομάδα Wicked Panda (APT41) ήταν ένα από τα πιο ενεργά και αποτελεσματικά APT groups με έδρα την Κίνα από τα μέσα της δεκαετίας του 2010 έως τη δεκαετία του 2020. Όσο η ομάδα ήταν ενεργή, εστίαζε διαρκώς σε μεγάλο βαθμό στην επέκταση του εύρους των πιθανών της στόχων, καθώς και των εργαλείων που χρησιμοποιούσε στις επιχειρήσεις της. Ταυτόχρονα, ενώ αρχικά η δραστηριότητα όσο και τα κίνητρα της ομάδας θύμιζαν μια εγκληματική οργάνωση με κίνητρο το οικονομικό όφελος, σταδιακά οι στόχοι αλλά και οι επιχειρήσεις της ομάδας ταυτίστηκαν με επιθέσεις σε οργανισμούς ή επιχειρήσεις που συχνά ευθυγραμμίζονται με τους στόχους της κυβέρνησης. Το APT41 έχει παρατηρηθεί να στοχεύει επιχειρήσεις σε διάφορους κλάδους όπως οι τηλεπικοινωνίες και η τεχνολογία σε περισσότερες από 14 χώρες. [14]

2.2 Blue Team

Είναι εμφανές λοιπόν πως με την πάροδο του χρόνου οι Cyber Threat Actors γίνονται όλο και πιο εξελιγμένοι και καλά οργανωμένοι, αποκτούν ισχυρότερα κίνητρα και διαθέτουν όλο και πιο εξειδικευμένες γνώσεις, καθιστώντας τους μια όλο και πιο σοβαρή απειλή για τις επιχειρήσεις. Το γεγονός αυτό δημιουργεί μια τεράστια ανάγκη στις επιχειρήσεις για την εύρεση εξειδικευμένου προσωπικού που είναι ικανό να κατανοήσει τις τεχνικές και τις μεθόδους των επιτιθέμενων, ώστε και να τις προστατεύσει. Είναι σύνηθες λοιπόν οι εταιρίες που διαθέτουν αντίστοιχες ομάδες από εξειδικευμένο προσωπικό που είναι αποκλειστικά υπεύθυνο για την προστασία του οργανισμού ενάντια σε κυβερνοεπιθέσεις, να χρησιμοποιούν διαφορετικές ορολογίες για την κατηγοριοποίηση τους, ανάλογα με τα καθήκοντα που διαθέτουν.

Οι πιο συνηθισμένοι όροι που χρησιμοποιούνται είναι αυτοί των “Red team” και “Blue team”. Σε αυτό το κεφάλαιο θα αναλύσουμε τον ρόλο ενός Blue Team, τις βασικές του αρμοδιότητες

εντός της εταιρίας, τα καθήκοντα αλλά και τις μεγαλύτερες προκλήσεις που αντιμετωπίζει από σύγχρονες απειλές.

2.2.1 Ορισμός - Ρόλος - Καθήκοντα

Με τον όρο "Blue Team" αναφερόμαστε στο προσωπικό κυβερνοασφάλειας μιας εταιρείας που συνήθως εργάζεται μέσα σε ένα Κέντρο Επιχειρήσεων Ασφαλείας (SOC) το οποίο λειτουργεί αδιάκοπα όλο το χρόνο (24/7/365). Το SOC συνεπώς είναι ένα ξεχωριστό τμήμα εντός του οργανισμού που είναι υπεύθυνο για τη συνεχή παρακολούθηση και τη βελτίωση της ασφάλειας του οργανισμού καθώς βασικό του καθήκον είναι να εντοπίζει, να αναλύει και να αποτρέπει συμβάντα κυβερνοασφάλειας [15].

Αποτελείται από επαγγελματίες ασφαλείας που διαθέτουν διαφορετικούς ρόλους με μεγάλη εξειδίκευση και διαφορετικά επίπεδα εμπειρίας, οι οποίοι διαθέτουν μια ολοκληρωμένη εικόνα για την συνολική εσωτερική δομή του οργανισμό που προστατεύουν. Επιβάλλεται να γνωρίζουν και να κατανοούν καλά τους επιχειρηματικούς στόχους, τις διαδικασίες, την τοπολογία των συστημάτων και τη στρατηγική ασφάλειας του οργανισμού, ώστε να είναι σε θέση να τον προστατεύσουν από εσωτερικές και εξωτερικές απειλές, όταν αυτό κριθεί απαραίτητο. Ως εκ τούτου, το βασικό τους καθήκον είναι να ενισχύσουν την συνολική άμυνα του οργανισμού για την αποτροπή ενός πιθανού περιστατικού ασφαλείας αλλά και η έγκαιρη και αποτελεσματική αντιμετώπισή του, όταν συμβεί, ώστε κανένας κακόβουλος παράγοντας να μην προκαλέσει ανεπιθύμητα αποτελέσματα που θα επηρεάσουν αρνητικά τη λειτουργία του οργανισμού.

Ένα τυπικό Blue Team αποτελείται από αρκετούς Security Analysts μαζί με άλλες ειδικότητες όπως Incident Responders, Forensic και Malware Analysts, Network και Security Engineers που εργάζονται συνεχώς για την υπεράσπιση και τη βελτίωση της άμυνας του οργανισμού. Οι περισσότερες από τις τυπικές απειλές, όπως το κακόβουλο λογισμικό ή τα μηνύματα ηλεκτρονικού ψαρέματος μπορούν εύκολα να εντοπιστούν και να αποκλειστούν από αυτοματοποιημένα εργαλεία όπως AVs, EDRs, IPS πριν προλάβουν να προκαλέσουν κάποια ζημιά. Ωστόσο αντίστοιχες αυτοματοποιημένες λύσεις δεν είναι πάντα αρκετές, επειδή ο ρόλος του Blue Team κρίνεται εξαιρετικά σημαντικός σε πιο σύνθετες και στοχευμένες απειλές που απειλούν τον οργανισμό καθώς προσθέτει την ζωτικής σημασίας ανθρώπινη κρίση και αξιολόγηση που κανένα Security Product δεν έχει καταφέρει ακόμα να αντικαταστήσει. Το εξειδικευμένο προσωπικό θα εντοπίσει και θα εξουδετερώσει τις πιο εξελιγμένες επιθέσεις που πιθανόν να μην αποκλειστούν αυτόματα από τα συστήματα ασφαλείας και θα παρακολουθεί στενά τις τρέχουσες και τις αναδυόμενες απειλές κατά του οργανισμού.

Συνοψίζοντας, οι στόχοι και τα καθήκοντα ενός Blue Team περιλαμβάνουν:

- Συνεχή παρακολούθηση εταιρικών δικτύων, συστημάτων και συσκευών σε πραγματικό χρόνο για τον εντοπισμό ύποπτης ή κακόβουλης δραστηριότητας συνήθως μέσω ενός SIEM (Security Information and Event Management).
- Κατηγοριοποίηση εντοπισμένων απειλών με βάση την κρισιμότητα τους και κατανομή τους στην ομάδα για αντιμετώπιση.
- Συλλογή δεδομένων όπως system logs, network traffic, data flows και alerts από Security Solutions όπως AV, EDR, IPS, IDS για ανάλυση και αξιολόγηση του εκάστοτε περιστατικού ασφαλείας.
- Λήψη απαραίτητων μέτρων ή ενεργειών για την εξάλειψη των εντοπισμένων απειλών και τον μετριασμό της πιθανής ζημίας.
- Διενέργεια προληπτικών ελέγχων και αναζητήσεων βασισμένων σε υποθέσεις (Threat Hunting) για τον έγκαιρο εντοπισμό απειλών που ενδέχεται να υπάρχουν εντός του οργανισμού και δεν έχουν ακόμα εντοπιστεί από τα συστήματα ασφαλείας ή τους αναλυτές.

- Συλλογή πληροφοριών και πραγματοποίηση συνεχούς έρευνας για νέες απειλές ή αδυναμίες (Threat Intelligence).

2.2.2 Προκλήσεις στην σύγχρονη εποχή

Με τη συνεχή εξέλιξη και την αύξηση των απειλών στον κυβερνοχώρο, δεν αποτελεί έκπληξη το γεγονός ότι οι Blue Teams αποτελούν ολοένα και πιο σημαντικό μέρος των προσπαθειών των οργανισμών να αμυνθούν ενάντια στις σύγχρονες απειλές. Παράλληλα οι επιτιθέμενοι επιδιώκουν συνεχώς να εξελίσσουν τις μεθόδους τους ώστε να γίνονται όλο και πιο αποτελεσματικοί στις επιχειρήσεις τους ώστε να πετύχουν τους στόχους τους, είτε αυτοί είναι η υποκλοπή δεδομένων και ο εκβιασμός, είτε είναι το οικονομικό έγκλημα, η βιομηχανική κατασκοπία ή το σαμποτάζ [16].

Όπως μπορούμε να αντιληφθούμε από τα παραπάνω, οι Blue Teams και πιο συγκεκριμένα τα SOC έχουν πολλαπλές αρμοδιότητες και καθήκοντα που είναι αρκετά δύσκολα, χρονοβόρα και περίπλοκα. Πέρα ωστόσο από όσα ήδη αναφέρθηκαν, υπάρχουν και επιπλέον προκλήσεις που κάνουν το έργο τους ακόμα πιο δύσκολο [17]. Μερικές από αυτές είναι οι παρακάτω:

Έλλειψη ορατότητας στην υποδομή:

Ένας από τους πιο σημαντικούς παράγοντες που επηρεάζουν αρνητικά την αποτελεσματικότητα ενός SOC είναι η έλλειψη ορατότητας στην υποδομή που οι αναλυτές προσπαθούν να παρακολουθήσουν και να προστατεύσουν. Είναι πολύ συνηθισμένο για ένα SOC να προσπαθεί να προστατεύσει ένα περιβάλλον για το οποίο δεν έχει πλήρη εικόνα, καθώς η τοπολογία του δικτύου είναι αφηρημένη και κυρίως δεν συλλέγονται όλα τα διαθέσιμα αρχεία καταγραφής από κάθε απαραίτητη πηγή καταγραφής. Αυτό μπορεί να φαίνεται ένα πρόβλημα μικρής σημασίας στην αρχή αλλά η διαφορά ανάμεσα σε μια επιτυχημένη με μια αποτυχημένη επίθεση μπορεί να κριθεί από ένα σύστημα που δεν λαμβάνονται αρχεία καταγραφής άρα το SOC δεν γνωρίζει τι συμβαίνει σε αυτό το σύστημα.

Ελαχιστοποίηση της διαταραχής των επιχειρησιακών λειτουργιών:

Όσο ο κάθε οργανισμός λειτουργεί, υπάρχει έντονη δικτυακή κίνηση και δραστηριότητα σε όλα τα πληροφοριακά του συστήματα που είναι υπεύθυνα να υποστηρίζουν τις επιχειρησιακές του λειτουργίες. Συγκριτικά με τη συνολική δραστηριότητα και τον όγκο της κίνησης που υπάρχει εντός του δικτύου, η δραστηριότητα που πιθανόν να είναι κακόβουλη ή μέρος μιας επίθεσης και να πρέπει να ερευνηθεί είναι ελάχιστη έως μηδαμινή. Οι αναλυτές συνεπώς πρέπει να είναι σε θέση ναι μεν να εντοπίζουν και να αποκλείουν μόνο τις πραγματικές επιθέσεις και απειλές, αλλά παράλληλα να επιτρέπουν και την απροβλημάτιστη συνέχιση των επιχειρησιακών λειτουργιών του οργανισμού, χωρίς να προκαλούν αναστάτωση ή αναιτιολόγητη διακοπή σε αυτές. Ο τεράστιος πλέον όγκος πληροφορίας που τα σύγχρονα SOC καλούνται να αντιμετωπίσουν σε συνδυασμό με την προσπάθεια ελαχιστοποίησης της διαταραχής των επιχειρησιακών λειτουργιών δημιουργεί συχνά προβλήματα αλλά και κενά στην ασφάλεια. Για παράδειγμα, μπορεί να υπάρχουν ενδείξεις πως ένα τερματικό που χρησιμοποιεί το τμήμα του HR είναι μολυσμένο από κακόβουλο λογισμικό. Η ασφαλέστερη επιλογή θα ήταν το τερματικό αυτό να αποκλειστεί αμέσως από το υπόλοιπο δίκτυο μέχρι να γίνουν οι απαραίτητοι έλεγχοι και να διαπιστωθεί αν όντως είναι μολυσμένο από κακόβουλο λογισμικό. Από την άλλη πλευρά, αν αυτή η ενέργεια πραγματοποιηθεί χωρίς να υπάρχει λόγος, οι διαδικασίες του τμήματος του HR που βασίζονται σε αυτό το σύστημα θα διαταραχθούν προκαλώντας καθυστερήσεις και σύγχυση.

Διαχωρισμός πραγματικών συμβάντων από False Positives:

Τα περισσότερα SOC λαμβάνουν δεκάδες χιλιάδες ειδοποιήσεις κάθε μέρα, αλλά μόνο ένα μικρό κομμάτι αυτών αντιστοιχούν σε πραγματικές απειλές. Όπως αναφέρθηκε και πριν στο πρόβλημα ελαχιστοποίησης της διαταραχής των επιχειρησιακών λειτουργιών, δεν γίνεται κάθε πιθανό συμβάν να θεωρείται και πραγματικό, εκτός αν έπειτα απο ανάλυση επιβεβαιωθεί κάτι τέτοιο. Συνεπώς ο ρόλος των αναλυτών είναι να αξιολογούν συνεχώς τις πληροφορίες που συνοδεύουν την κάθε ειδοποίηση για ένα πιθανόν συμβάν, μια χρονοβόρα και κουραστική δραστηριότητα που

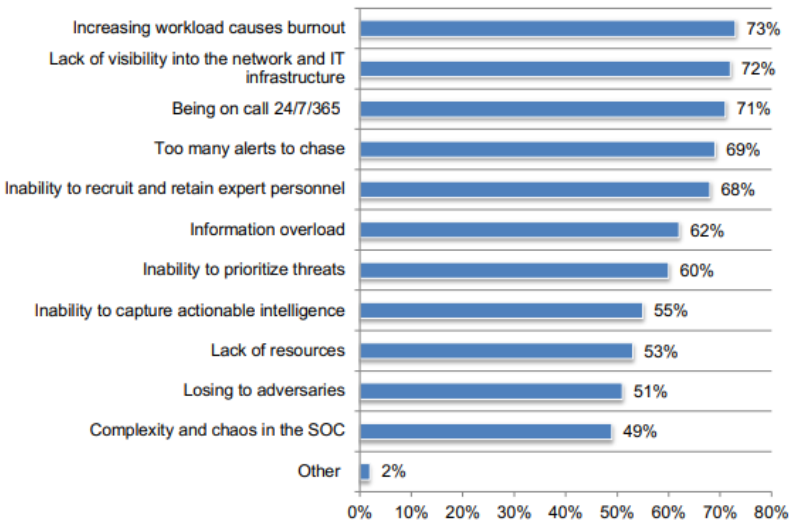
προκαλεί συχνά εξάντληση στους αναλυτές, κάνοντας τους πιο επιρρεπείς σε λάθη.

Alert Fatigue:

Η συνεχής προσπάθεια για το διαχωρισμό των πραγματικών συμβάντων από τα False Positive, σε συνδυασμό με τον υπερβολικά μεγάλο όγκο δεδομένων προς ανάλυση οδηγεί συχνά τους αναλυτές σε μια κατάσταση που έχει ονομαστεί "Alert Fatigue". Με τον όρο αυτό αναφερόμαστε στην κατάσταση που μπορεί να βρεθεί ένας αναλυτής ή και ολόκληρη η ομάδα του SOC όταν κατακλύζονται από ειδοποιήσεις για περιστατικά που οι περισσότερες είναι False Positives. Αυτό έχει ως αποτελέσματα οι αναλυτές να συνηθίζουν να απορρίπτουν ειδοποιήσεις που λαμβάνουν για συμβάντα ως μην πραγματικά, έχοντας χάσει την ευαισθησία τους απέναντι σε φαινομενικά πραγματικές ειδοποιήσεις, καθώς έχουν συνηθίσει να τις αντιμετωπίζουν ως False Positives. Το γεγονός αυτό οδηγεί σε μια επικίνδυνη κατάσταση όπου οι αναλυτές απορρίπτουν τα πιθανά συμβάντα ως μη πραγματικά με ελάχιστη έως καθόλου προσπάθεια για ανάλυση απλά και μόνο για να μπορέσουν να αντεπεξέλθουν στον όγκο εργασίας που καλούνται να αντιμετωπίσουν. Αυτό φυσικά έχει ως αποτέλεσμα πολλά πραγματικά περιστατικά ασφαλείας να περνάνε απαρατήρητα, εκθέτοντας τον οργανισμό σε επιθέσεις.

Υπερκόπωση αναλυτών και έλλειψη προσωπικού:

Έρευνες έχουν δείξει πως το προσωπικό των Blue Teams πιστεύει πως η εργασία στο SOC είναι επώδυνη λόγω του όλο ένα και αυξανόμενου φόρτου εργασίας αλλά και του καθεστώτος αδιάκοπης λειτουργίας του. Σύμφωνα με την ίδια έρευνα, αυτό έχει ως αποτέλεσμα, το 65 τοις εκατό των αναλυτών να δηλώνει πως οι παράγοντες αυτοί θα τους έκαναν να σκεφτούν να αλλάξουν ρόλο ή να εγκαταλείψουν την τωρινή τους θέση, προκαλώντας έτσι μεγάλα προβλήματα υποστελέχωσης σε μια αγορά που ήδη υποφέρει σε μεγάλο βαθμό από την έλλειψη εξειδικευμένου προσωπικού.



Εικόνα 5. Οι μεγαλύτερες προκλήσεις για τους αναλυτές σε ένα σύγχρονο SOC.
Πηγή εικόνας: https://www.devo.com/wp-content/uploads/sites/1/2019/07/2019-Devo-Ponemon-Study-Final.pdf

2.2.3 Ανάγκη για αλλαγή

Πέρα όμως από όλες αυτές τις προκλήσεις που αναφέρθηκαν παραπάνω και που αντιμετωπίζουν καθημερινά τα περισσότερα SOC, άρα και οι Blue Teams συνολικά, υπάρχουν και νέες προκλήσεις που εμφανίζονται εξαιτίας της συνεχόμενης βελτίωσης των ικανοτήτων των επιτιθέμενων που κάνουν το έργο της άμυνας ενός οργανισμού όλο και δύσκολο. Μια από αυτές τις προκλήσεις είναι και η άνοδος της δραστηριότητας του οργανωμένου εγκλήματος κυρίως από ομάδες με ικανότητες ενός APT που πλέον θα στοχεύσουν προσεκτικά επιλεγμένες εταιρίες ή συγκεκριμέ-

νες βιομηχανίες που τους ενδιαφέρουν. Αυτές οι ομάδες έχουν πολύ υψηλά επίπεδα γνώσεων και ικανοτήτων άρα είναι και πολύ αποτελεσματικές στις επιθέσεις τους.

Οι περισσότερες εταιρίες και οργανισμοί έχουν πλέον αντιληφθεί το γεγονός πως εφόσον στοχοποιηθούν από έναν επιτιθέμενο με τέτοιες ικανότητες, είναι αναμενόμενο πως θα δεχθούν μια επίθεση κάποια στιγμή στο μέλλον η οποία θα οδηγήσει σε παραβίαση κάποιων συστημάτων τους. Παλαιότερα ο στόχος της Blue Team ήταν πιο απλός και ξεκάθαρος γιατί στόχευε στο να καταφέρει να αποτρέψει μια επίθεση και αρκετές φορές τα κατάφερνε. Πλέον τα δεδομένα έχουν αλλάξει και το ερώτημα για τις περισσότερες εταιρείες δεν είναι το αν θα πέσουν θύματα μιας επίθεσης και αν θα καταφέρουν να την αποκρούσουν, αλλά το πότε θα πέσουν θύματα επίθεσης και πόσο γρήγορα θα μπορέσουν να αντιδράσουν και να ανακάμψουν.

Παράλληλα οι περισσότερες Blue Teams χρησιμοποιούν ως επί το πλείστον αποτρεπτικές μεθόδους άμυνας (reactive defence). Δηλαδή εστιάζουν περισσότερο στον περιορισμό της ζημιάς από μια απειλή αφού αυτή έχει εκδηλωθεί λειτουργώντας πυροσβεστικά και προσπαθώντας να μειώσουν την εξάπλωση και τις επιπτώσεις της επίθεσης, αντί να προσπαθούν να βελτιώσουν τις ικανότητές τους στο να εντοπίζουν απειλές και επιθέσεις ώστε να τις αποτρέπουν πριν αυτές συμβούν (proactive defence). Οι περισσότερες Blue Teams είναι σε θέση να αντιμετωπίσουν και να αποτρέψουν κοινές απειλές, αλλά το γεγονός ότι πρέπει πάντα να είναι ένα βήμα μπροστά από τους επιτιθέμενους, καθιστά το έργο τους μια τεράστια πρόκληση όταν κληθούν να αντιμετωπίσουν μια επίθεση ενός APT.

Στην σύγχρονη εποχή, η διαφοροποίηση ανάμεσα σε μια αποτελεσματική και μη αποτελεσματική Blue Team δεν κρίνεται μόνο από την ικανότητα της να αποτρέψει ένα περιστατικό ασφαλείας αλλά από το πόσο γρήγορα θα καταφέρει να εντοπίσει μια επίθεση και να τη σταματήσει. Επίσης η επιτυχία της κρίνεται από το πόσο γρήγορα και αποτελεσματικά θα καταφέρει να περιορίσει τη ζημιά αλλά και από το σε τι βαθμό θα βοηθήσει τον οργανισμό να ανακάμψει από την επίθεση με τη λιγότερη δυνατή διαταραχή στην λειτουργία του.

Συνεπώς τα Blue Teams για να παραμένουν αποτελεσματικά ενάντια σε στοχευμένες επιθέσεις από APTs πρέπει συνεχώς να βελτιώνουν τις ικανότητες εντοπισμού τους, και δεν μπορούν να βασίζονται πλέον μόνο σε παραδοσιακά μέσα και εργαλεία, καθώς δεν είναι αρκετά να αποτρέψουν τους εξελιγμένους επιτιθέμενους. Πλέον για τον εντοπισμό τους δεν αρκούν τα παραδοσιακά Indicators of Compromise (IOCs) όπως hashes αρχείων ή διευθύνσεις IPs αλλά η κατανόηση των τακτικών, τεχνικών και των διαδικασιών που ακολουθούν (Tactics, Techniques, Procedures - TTPs).

Τα περισσότερα εργαλεία, όσο προηγμένα και αν είναι, μπορούν να παρακαμφθούν και γι'αυτό πλέον κρίνεται αναγκαία η μετάβαση από reactive σε proactive μεθόδους άμυνας αξιοποιώντας νέες τεχνικές όπως Threat Intelligence και Threat Hunting οι οποίες θα αναλυθούν σε βάθος σε επόμενα κεφάλαια.

Εν συντομία, μέσω του Threat Intelligence ο οργανισμός συλλέγει και επεξεργάζεται δεδομένα που περιλαμβάνουν και τα TTPs των επιθέμενων ώστε να είναι σε θέσει να κατανοήσει καλύτερα τα κίνητρα, τις τεχνικές και τη συμπεριφορά των επιτιθέμενων από τους οποίους πιθανόν θα στοχοποιηθεί αλλά και γενικότερα για τις απειλές στις οποίες είναι είναι εκτεθειμένος. Αυτές οι πληροφορίες αξιοποιούνται ώστε να ληφθούν μέτρα και αποφάσεις που βασίζονται σε δεδομένα με στόχο τη βελτίωση της στρατηγικής άμυνας που ακολουθεί ο οργανισμός. Μέσω του Threat Hunting η Blue Team πραγματοποιεί προληπτικές αναζητήσεις για κακόβουλη δραστηριότητα εντός της υποδομής, ακόμα και χωρίς να υπάρχει κάποια ένδειξη παραβίασης, ώστε να εντοπίσει απειλές που πιθανόν έχουν περάσει απαρατήρητες μέχρι τώρα απο τα συστήματα ασφαλείας. Το Threat Hunting βασίζεται σε υποθετικά σενάρια παραβίασης και πλέον κρίνεται απαραίτητο κομμάτι μιας proactive στρατηγικής άμυνας, καθώς είναι σύνηθες πλέον οι επιτιθέμενοι να παραμένουν αρκετό καιρό εντός ενός δικτύου που έχουν παραβιάσει χωρίς να γίνουν αντιληπτοί.

Οι δυσκολίες και τα προβλήματα που αντιμετωπίζουν οι Blue Teams, και πιο συγκεκριμένα

τα SOCs που δυσκολεύονται να μεταβούν σε proactive μεθόδους άμυνας αλλά και να βελτιώσουν ουσιαστικά τις ικανότητες εντοπισμού APTs, αποτέλεσαν βασικό κίνητρο για την εκπόνηση αυτής της εργασίας. Ένα από τα επιδιωκόμενα αποτελέσματα της εργασίας είναι η ανάδειξη της αναγκαιότητας του proactive defence, για την αποτελεσματική άμυνα, αλλά και η παρουσίαση των μεθόδων με τις οποίες είναι εφικτή η συνεχής βελτίωση της ικανότητας εντοπισμού εξελιγμένων επιτιθέμενων. Αυτό επιτυγχάνεται συνδυάζοντας τεχνικές proactive defence με Adversary Emulation και Purple Teaming, έννοιες που θα αναλυθούν σε επόμενα κεφάλαια.

2.3 Red Team

2.3.1 Ορισμός - Ρόλος - Καθήκοντα

Σε αντίθεση με τη Blue Team που αναλύσαμε σε προηγούμενο κεφάλαιο που έχει αμυντικό ρόλο, η Red Team είναι μια ομάδα τεχνικών ασφαλείας με επιθετικό ρόλο που ο προσπαθεί να εντοπίσει υπάρχουσες αδυναμίες στην υποδομή του οργανισμού ώστε να διορθωθούν πριν κάποιος επιτιθέμενος αποκτήσει την ευκαιρία να τις εκμεταλλευθεί. Αυτό περιλαμβάνει αδυναμίες τόσο στην εξωτερική υποδομή που είναι προσβάσιμη από το διαδίκτυο (external infrastructure / web applications) όσο και στα εσωτερικά συστήματα του οργανισμού (internal infrastructure) καθώς επίσης και αδυναμίες που σχετίζονται με την ανθρώπινη συμπεριφορά (social engineering).

Οι δραστηριότητες της Red Team κυμαίνονται από απλές αξιολογήσεις ευπάθειας (vulnerability assessments) και δοκιμές διείσδυσης (penetration testing) έως πολύπλοκα σενάρια που προσομοιώνουν συνολικά τη συμπεριφορά ενός επιτιθέμενου όσο πιο ρεαλιστικά γίνεται (Red Teaming / Adversary Emulation). Παρά το γεγονός πως όλες αυτές οι δραστηριότητες έχουν μεγάλες διαφορές μεταξύ τους και εφαρμόζονται ανά περίπτωση ανάλογα με το επίπεδο ωριμότητας του κάθε οργανισμού, όλες εκτελούνται με τον ίδιο σκοπό. Ο σκοπός αυτός δεν είναι άλλος από τον έγκαιρο εντοπισμό αδυναμιών και κενών ασφαλείας που υπάρχουν στον οργανισμό με στόχο τη διόρθωσή τους προτού ένας πραγματικός επιτιθέμενος είναι σε θέση να τις εκμεταλλευτεί.

Το Vulnerability Assessment, είναι η πιο επιφανειακή προσέγγιση για την εύρεση αδυναμιών καθώς εκτελείται συνήθως από αυτοματοποιημένα εργαλεία που αξιολογούν εάν ένα σύστημα είναι ευάλωτο σε γνωστές ευπάθειες, κατηγοριοποιώντας τες σύμφωνα με την σοβαρότητά τους και προτείνοντας τρόπους αντιμετώπισης. [18]

Σε αντίθεση με το Vulnerability Assessment, οι δοκιμές διείσδυσης (Penetration Testing) απαιτούν τεχνογνωσία από τη πλευρά του επαγγελματία ασφαλείας που τις πραγματοποιεί, εφόσον δεν μπορούν να γίνουν με αυτοματοποιημένα εργαλεία και περιλαμβάνουν χειροκίνητες δοκιμές για τον εντοπισμό όχι μόνο γνωστών ή άγνωστων αδυναμιών, αλλά κυρίως για την εκμετάλλευσή τους με σκοπό την καλύτερη κατανόηση της ζημιάς που θα μπορούσε να προκληθεί εάν οι ίδιες ενέργειες πραγματοποιούνταν από έναν πραγματικό Threat Actor. Συνεπώς μέσω του Penetration Testing η Red Team πραγματοποιεί μια δοκιμαστική εισβολή για την αξιολόγηση της ασφάλειας του συστήματος ώστε να εντοπιστούν οι αδυναμίες που δεν μπόρεσαν να εντοπιστούν από το Vulnerability Assessment και να διορθωθούν πριν τις εκμεταλλευτεί ένας κακόβουλος χρήστης. [19]

Τέλος, τα Red Team Engagements είναι ολοκληρωμένες επιθέσεις που βασίζονται σε σενάρια και καθοδηγούνται από συγκεκριμένους στόχους ώστε να αξιολογήσουν την συνολική ετοιμότητα του οργανισμού -άρα και του Blue Team- να αντιμετωπίσει μια όσο το δυνατόν πιο ρεαλιστική επίθεση. Τα Red Team Engagements διαφέρουν από το Penetration Testing γιατί δεν εστιάζουν στον εντοπισμό όσο το δυνατόν περισσότερων αδυναμιών υπάρχουν σε ένα σύστημα, αλλά επικεντρώνονται στην επίτευξη ενός συγκεκριμένου στόχου, εκμεταλλευόμενοι οποιαδήποτε αδυναμία είναι διαθέσιμη και εξυπηρετεί την επίτευξη του στόχου. Το Red teaming μπορεί να προσφέρει μια βαθύτερη κατανόηση των αρνητικών επιπτώσεων που μπορεί να έχει ένας εξελιγμένος Threat Actor εναντίον του οργανισμού, καθώς συνδυάζει πολλαπλές τεχνικές που δεν περιλαμβάνονται σε ένα

τυπικό Penetration test, όπως την δοκιμή της ασφάλειας ενός κτηρίου ή την κοινωνική μηχανική (Social Engineering). Επιπλέον το Red Teaming είναι ζωτικής σημασίας καθώς παρέχει ανατροφοδότηση για την ετοιμότητα και την αποτελεσματικότητα της Blue Team [20].

2.3.2 Διαφορές ανάμεσα σε Penetration Testing και Red Teaming

Παρά τις σημαντικές διαφορές που υπάρχουν ανάμεσα σε Penetration Testing και Red Teaming, είναι αρκετά συνηθισμένο οι όροι αυτοί να συγχέονται αλλά είναι σημαντικό να επισημανθούν οι διαφορές τους. Αρχικά, όπως αναφέρθηκε και σε προηγούμενη παράγραφο, το Penetration Testing έχει εντελώς διαφορετικό στόχο από το Red Teaming [21, 22, 23].

Ο στόχος του Penetration Testing είναι να βρεθούν όσο το δυνατόν περισσότερες αδυναμίες είναι εφικτό μέσα σε ένα συγκεκριμένο χρονικό διάστημα, συνήθως μερικών ημερών, με στόχο να διορθωθούν. Η δοκιμή διείσδυσης δεν είναι γενικευμένη προς τον οργανισμό αλλά εστιάζει σε επιλεγμένα σύστημα (συγκεκριμένο scope) που ο οργανισμός ενδιαφέρεται να αξιολογήσει αν είναι ευάλωτα σε επιθέσεις. Ανάλογα με τις αδυναμίες που εντοπιστούν, κάποιες από αυτές θα αξιοποιηθούν ώστε να αναδειχθούν οι επιπτώσεις που προκύπτουν στον οργανισμό από την εκμετάλλευσή τους, αλλά δεν υπάρχει συγκεκριμένος στόχος που πρέπει να επιτευχθεί ώστε η δοκιμή να θεωρηθεί επιτυχής. Τέλος, στις δοκιμές διείσδυσης είναι σύνηθες η Blue Team να είναι εξ αρχής ενημερωμένη για τη δραστηριότητα αυτή και να επιτρέπει την κακόβουλη κίνηση που εντοπίζει ώστε να βοηθήσει τη διεξαγωγή των δοκιμών για να εντοπιστούν όσο το δυνατόν περισσότερες αδυναμίες είναι εφικτό. Συνεπώς το Penetration Testing δεν εστιάζει στο να προσπαθεί να αποκρύψει τη δραστηριότητα ή να αποφύγει τον εντοπισμό από την Blue Team ούτε είναι κατάλληλος τρόπος να αξιολογήσει την ικανότητα του Blue Team να εντοπίζει και να αποκλείει επιθέσεις.

Από την άλλη πλευρά, ο βασικός στόχος του Red Teaming δεν είναι να εντοπιστούν όσο το δυνατόν περισσότερα τρωτά σημεία και αδυναμίες σε ένα σύστημα αλλά η προσπάθεια μίμησης ενός πραγματικού εξελιγμένου επιτιθέμενου και η επίτευξη συγκεκριμένων στόχων, όπως για παράδειγμα η απόκτηση απόρρητων πληροφοριών. Οι ασκήσεις Red Team πραγματοποιούνται συνήθως σε οργανισμούς που έχουν ήδη διεξάγει πολλαπλά Vulnerability Assessments και Penetration Tests στο παρελθόν και διαθέτουν μια καλά οργανωμένη και αποτελεσματική Blue Team και θέλουν να δοκιμάσουν την ετοιμότητα της. Συνεπώς οι ασκήσεις Red Team διαρκούν μεγαλύτερο χρονικό διάστημα και εστιάζουν σε μεγάλο βαθμό στο να προσπαθήσουν να διατηρήσουν χαμηλό προφίλ ώστε να αποφύγουν τον εντοπισμό από την Blue Team. Για να διεξαχθεί μια τέτοια άσκηση και ο οργανισμός να αποκομίσει το μέγιστο δυνατό όφελος από αυτήν, ο οργανισμός θα πρέπει να βρίσκεται ήδη σε ένα αρκετά υψηλό επίπεδο ωριμότητας σε θέματα άμυνας. Θα πρέπει να έχουν θεσπιστεί μέτρα ασφαλείας και η Blue Team να είναι καλά προετοιμασμένη να αντιμετωπίσει εξελιγμένους επιτιθέμενους. Συνεπώς το Red Teaming είναι μια δραστηριότητα που διεξάγεται από εταιρείες και οργανισμούς που θεωρούν ότι η κυβερνοασφάλειά τους είναι αρκετά ώριμη ώστε να θέλουν να δοκιμάσουν τις αντοχές της έναντι σε εξελιγμένους επιτιθέμενους.

	Penetration Testing	Red Team Assessment
Χρονική Διάρκεια	Μερικές μέρες ή εβδομάδες.	Αρκετές εβδομάδες ή και μήνες.
Στόχος	Εντοπισμός όσο το δυνατόν περισσότερων αδυναμιών σε συγκεκριμένα συστήματα και εκμετάλλευση τους για την ανάδειξη των επιπτώσεων αλλά και τη διόρθωση τους.	Ρεαλιστική προσομοίωση μιας επίθεσης από έναν επιτιθέμενο με σκοπό την επίτευξη συγκεκριμένων στόχων και την αξιολόγηση της ετοιμότητας και της αποτελεσματικότητας της Blue Team.
Τακτικές	Εστιάζει σε συγκεκριμένα συστήματα, συνεπώς οι τεχνικές που θα χρησιμοποιηθούν καθορίζονται ανάλογα το σύστημα ή το περιβάλλον, ακολουθώντας διαφορετικές μεθοδολογίες και εργαλεία ανά περίπτωση (External Infrastructure, Web Application, Mobile Application).	Συνδυασμός μεθοδολογίας, εργαλείων, τακτικών, τεχνικών και γενικότερα προσέγγισης που θα χρησιμοποιούσε ένας πραγματικός επιτιθέμενος συμπεριλαμβάνοντας τη συλλογή πληροφοριών και της κοινωνικής μηχανικής.
Επιθυμητό αποτέλεσμα	Οι αδυναμίες που θα εντοπιστούν να διορθωθούν ώστε το σύστημα υπό εξέταση να πάψει να είναι ευάλωτο.	Αξιολόγηση του οργανισμού έναντι σε κυβερνοεπιθέσεις. Αυτό περιλαμβάνει την αξιολόγηση αποτελεσμάτων από ενέργειες όπως Penetration Tests που έχουν πραγματοποιηθεί στο παρελθόν, την κατάσταση της ασφάλειας σε φυσικές υποδομές όπως κτήρια, την ευαισθητοποίηση των υπαλλήλων σε θέματα κυβερνοασφάλειας αλλά και την ετοιμότητα και αποτελεσματικότητα της Blue Team.
Κόστος	Πιο οικονομικό, καθώς διεξάγεται σε λιγότερες μέρες, απαιτείται λιγότερη προεργασία και συνήθως απασχολεί ομάδες 2-3 ατόμων.	Συνήθως πιο ακριβό καθώς απαιτείται μεγάλη προεργασία, είναι μια αρκετά εξειδικευμένη υπηρεσία που απαιτεί αρκετούς πόρους και προσωπικό και η χρονική διάρκεια είναι σαφώς μεγαλύτερη.

Εικόνα 6. Διαφορές ανάμεσα σε Penetration Testing και Red Team Assessment.

2.3.3 Ανάγκη για αλλαγή

Όπως προβλήματα αντιμετωπίζουν οι Blue Teams έτσι αντίστοιχα και οι Red Teams έρχονται αντιμέτωπες με προκλήσεις που αφορούν τη δική τους αποτελεσματικότητα και συνεισφορά στην άμυνα του οργανισμού.

Παρά το γεγονός ότι συνήθως τα ποσοστά επιτυχίας των ασκήσεων που πραγματοποιούνται από τις Red Teams έχουν υψηλά ποσοστά επιτυχίας και είναι σε θέση να δοκιμάσουν αποτελεσματικά την ετοιμότητα μιας Blue Team, συχνά δεν πετυχαίνουν απόλυτα τον απώτερο στόχο τους, δηλαδή την βελτίωση του συνολικού security posture της εταιρίας ενάντια σε εξελιγμένους επιτιθέμενους. Ναι μεν μπορεί να εντοπίστηκαν κενά ασφαλείας που η Blue Team δεν ήταν σε θέση να εντοπίσει και πλέον να διορθώθηκαν, αλλά το βασικό πρόβλημα παραμένει καθώς κάθε εξελιγμένος επιτιθέμενος, ειδικά στην περίπτωση που ανήκει σε μία κατηγορία APT, χρησιμοποιεί δικές του τεχνικές για να επιτεθεί στον οργανισμό.

Όπως παρουσιάστηκε σε προηγούμενο κεφάλαιο, κάθε APT στοχεύει διαφορετικές εταιρείες με βάση τη βιομηχανία που δραστηριοποιούνται. Λαμβάνοντας υπόψιν πως ένας οργανισμός δεν μπορεί να είναι σε θέση να αμυνθεί αποτελεσματικά ενάντια σε κάθε είδους APT, κρίνεται σκόπιμο να προετοιμαστεί ενάντια σε απειλές που είναι πιο πιθανόν να τον στοχεύσουν. Για παράδειγμα αν μία εταιρεία δραστηριοποιείται στον τομέα της ναυτιλίας, μία απλή ad-hoc άσκηση Red Team ενδεχομένως θα τη βοηθήσει να βελτιώσει την κατάσταση ασφαλείας της, αλλά δεν θα την προ-

ετοιμάσει υποχρεωτικά κατάλληλα ενάντια σε μία επίθεση από ένα APT που στοχεύει τον τομέα της ναυτιλίας.

Η κάθε Red Team θα χρησιμοποιήσει τις δικές τις τακτικές για να πετύχει τον στόχο της άσκησης χωρίς να ακολουθήσει υποχρεωτικά τις συγκεκριμένες τεχνικές που θα ακολουθούσε ένα συγκεκριμένο APT group. Το ιδανικό σενάριο θα ήταν η Red Team να προσπαθήσει να πετύχει το στόχο της αλλά ταυτόχρονα να χρησιμοποιήσει τις μεθόδους και τις τακτικές που θα χρησιμοποιούσε ένας πραγματικός APT που στοχεύει τη βιομηχανία της Ναυτιλίας ώστε να δοκιμάσει την ετοιμότητα της εταιρείας να αντιμετωπίσει ένα APT που είναι πιο πιθανό να την στοχεύσει.

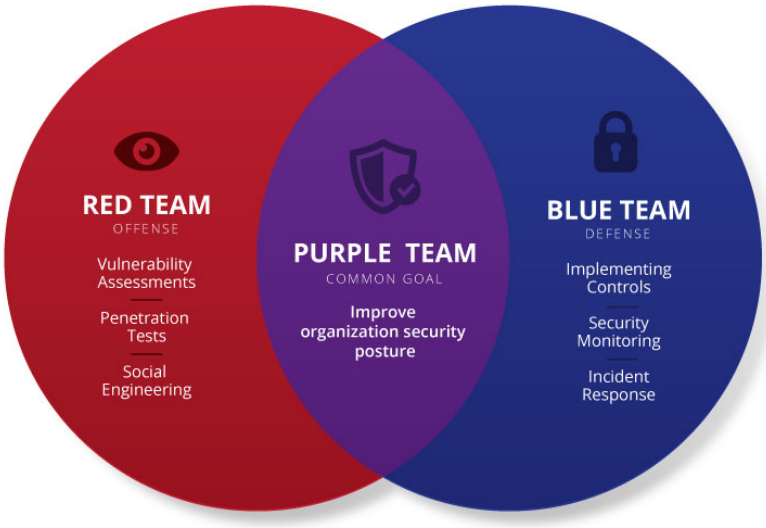
Συνεπώς η αλλαγή που χρειάζεται στη σύγχρονη εποχή για την βελτίωση της αποτελεσματικότητα ενός Red Team επιτυγχάνεται μέσω μιας μεθοδολογίας που ονομάζεται Adversary Emulation όπου προσπαθεί να προσομοιώσει όσο το δυνατόν πιο ρεαλιστικά γίνεται τις μεθόδους με τις οποίες ένας συγκεκριμένος επιτιθέμενος θα πραγματοποιούσε μία επίθεση.

2.4 Purple Teaming

2.4.1 Μεγιστοποιώντας την αποτελεσματικότητα των Blue και των Red Team

Μέχρι τώρα παρουσιάσαμε τι είναι οι Blue και οι Red Teams, ποιος είναι ο ρόλος τους, πώς λειτουργούν και τι προσπαθούν να επιτύχουν. Ανεξάρτητα από το μέγεθος, όλοι οι οργανισμοί χρειάζονται την τεχνογνωσία των επαγγελματιών ασφαλείας και των δύο ομάδων. Παρά τις διαφορές τους και οι δύο ομάδες διαθέτουν κρίσιμο ρόλο και εξυπηρετούν διαφορετικές ανάγκες με απώτερο κοινό στόχο την προστασία του οργανισμού από απειλές. Συνεπώς για να επιτύχουν αυτό το αποτέλεσμα είναι απαραίτητο να επικοινωνούν τακτικά μεταξύ τους, να συνεργάζονται και κυρίως να μοιράζονται τεχνογνωσία για το συνολικό όφελος του οργανισμού.

Ωστόσο σε πολλές περιπτώσεις οι Blue και οι Red Teams λειτουργούν ως ξεχωριστές και ανεξάρτητες οντότητες που λειτουργούν αποσυνδεδεμένες η μία από την άλλη ακόμη κι αν λειτουργούν εντός του ίδιου οργανισμού κάτω από το ίδιο τμήμα. Ειδικά σε μικρότερους οργανισμούς η επικοινωνία είναι ακόμη πιο δύσκολη και αναποτελεσματική καθώς είναι σύνηθες η Blue Team να στελεχώνεται από μόνιμο προσωπικό του οργανισμού, ενώ ο ρόλος της Red Team ανατίθενται σε εξωτερικούς συνεργάτες. Αυτό οφείλεται στο γεγονός πως οι περισσότεροι οργανισμοί έχουν συνεχή ανάγκη των αρμοδιοτήτων μιας Blue Team για την προστασία τους ενώ οι δραστηριότητες που περιλαμβάνονται στα καθήκοντα της Red Team πραγματοποιούνται περιστασιακά ανά μερικούς μήνες το χρόνο, συνεπώς είναι πιο λογικό να ανατίθενται σε τρίτους. Κατά αυτόν τον τρόπο η Red Team, που προσλαμβάνεται για να δοκιμάσει την ετοιμότητα και τις ικανότητες της Blue Team, μπορεί μεν να παρέχει μια τεχνική αναφορά στο τέλος της άσκησης που να περιγράφει τα αποτελέσματα της άσκησης με τεχνικές λεπτομέρειες, αλλά δεν θα μοιραστεί σε βάθος όλες τις τεχνικές που αξιοποίησε για να επιτύχει το στόχο της, ούτε θα ανταλλάξει τεχνογνωσία με την Blue Team. Κατά αυτόν τον τρόπο, ναι μεν αξιολογείται η ετοιμότητα και η ικανότητα της Blue Team να ανιχνεύει και να αποτρέπει επιθέσεις, αλλά χωρίς την αποτελεσματική επικοινωνία ανάμεσα στις δύο ομάδες η άσκηση αυτή δεν θα την βοηθήσει πραγματικά να κατανοήσει σε βάθος τις τεχνικές που χρησιμοποίησε η Red Team σε κάθε βήμα ώστε να μπορέσει να βελτιώσει περαιτέρω τις ικανότητες εντοπισμού της. Αντίστοιχα η Blue Team σε περίπτωσή που καταφέρει και εντοπίσει ή αποτρέψει τη δραστηριότητα της Red Team, πιθανόν δεν θα επικοινωνήσει πλήρως τις τεχνικές λεπτομέρειες, αποτρέποντας έτσι την Red Team από το να βελτιώσει εξίσου τις ικανότητες της. Συνεπώς όταν αυτή η απαραίτητη επικοινωνία ανάμεσα στις δύο ομάδες δεν είναι ποιοτική ή ακόμα χειρότερα δεν συμβαίνει καθόλου, τότε συχνά εξετάζεται η εδραίωση μιας Purple Team. Το Purple Teaming είναι μια μεθοδολογία κατά την οποία οι δύο ομάδες συνεργάζονται στενά για να μεγιστοποιήσουν τις ικανότητές τους μέσω συνεχούς επικοινωνίας ανατροφοδότησης και μεταφοράς γνώσης [24, 25, 26].



Εικόνα 7. Συσχέτηση Red, Blue και Purple Team
Πηγή εικόνας: https://www.schneiderdowns.com/cybersecurity/services/purple-team-assessment

Είναι πολύ συχνό φαινόμενο οι οργανισμοί να παραβιάζονται και η Blue Team να μην καταφέρνει να το αποτρέψει πόσο μάλλον να το εντοπίσει. Αυτό δεν οφείλεται σε άτομα με χαμηλή ειδίκευση, χρήση λανθασμένων διαδικασιών ή εργαλείων. Αυτό συμβαίνει συνήθως διότι ο επιτιθέμενος, είτε με τη μορφή μιας Red Team είτε ως ένας πραγματικός Threat Actor χρησιμοποίησε μια τεχνική που το SOC της Blue Team δεν γνωρίζει πώς να εντοπίζει ή δεν είχε μεριμνήσει ώστε να πράξει τις απαραίτητες ενέργειες για να είναι εφικτός ο εντοπισμός. Μέσω του Purple Teaming και της ανταλλαγής δεδομένων, τεχνικών, πληροφοριών και γενικότερα τεχνογνωσίας η Blue Team έχει τη δυνατότητα να διαμορφώσει, να συντονίσει και να βελτιώσει την ικανότητα ανίχνευσης και απόκρισής της καθιστώντας την εξαιρετικά πιο αποτελεσματική. Αυτός είναι ο λόγος για τον οποίο η εφαρμογή της μεθοδολογίας του Purple Teaming είναι τόσο σημαντική για τα σύγχρονα δεδομένα.

Σε μια Red Team άσκηση η αλληλεπίδραση με την Blue Team είναι περιορισμένη ή και ανύπαρκτη καθώς ο στόχος της άσκησης είναι η αξιολόγηση της ικανότητας της Blue Team να εντοπίζει και να αποτρέπει επιθέσεις από έναν εξελιγμένο επιτιθέμενο. Από την άλλη πλευρά σε μία Purple Team άσκηση επιδιώκεται η μέγιστη δυνατή αλληλεπίδραση ανάμεσα στην Red και την Blue team καθώς ο στόχος είναι η βελτίωση της ικανότητας της Blue την να αποτρέπει επιθέσεις αλλά κυρίως να τις εντοπίζει.

Εφόσον κάθε άσκηση έχει και διαφορετικούς στόχους, η αποτελεσματικότητα της άσκησης θα πρέπει να μετριέται και με διαφορετικούς παράγοντες.

Άσκηση Red Team:

- Ικανότητα εντοπισμού.
- Χρόνος εντοπισμού.
- Ικανότητα αποτροπής επίθεσης.
- Χρόνος αποτροπής επίθεσης.
- Χρόνος παραμονής εντός του δικτύου χωρίς εντοπισμό (dwell time).
- Στόχοι που επιτεύχθηκαν από τη Red Team σύμφωνα με το σενάριο.

Άσκηση Purple Team:

- Πλήθος TTPs (tactics, techniques, procedures) που εντοπίστηκαν.
- Πλήθος TTPs που εντοπίστηκαν αλλά και αποκλείστηκαν.
- Πλήθος TTPs που καταγράφονται από logs αλλά δεν υπάρχουν ακόμα οι κατάλληλοι κανόνες εντοπισμού (Log visibility).
- Πλήθος TTPs που δεν εντοπίστηκαν καθώς δεν συλλέγονται τα logs από τα συστήματα που επηρεάστηκαν.
- Αξιολόγηση πιθανών False Positive ή True Negative.

Τα παραπάνω στοιχεία μπορούν πολύ εύκολα να οπτικοποιηθούν μέσω του MITRE ATT&CK Framework navigator όπως θα παρουσιαστεί σε επόμενα κεφάλαια [27].

Κεφάλαιο 3

Cyber Threat Intelligence

3.1 Ορισμός

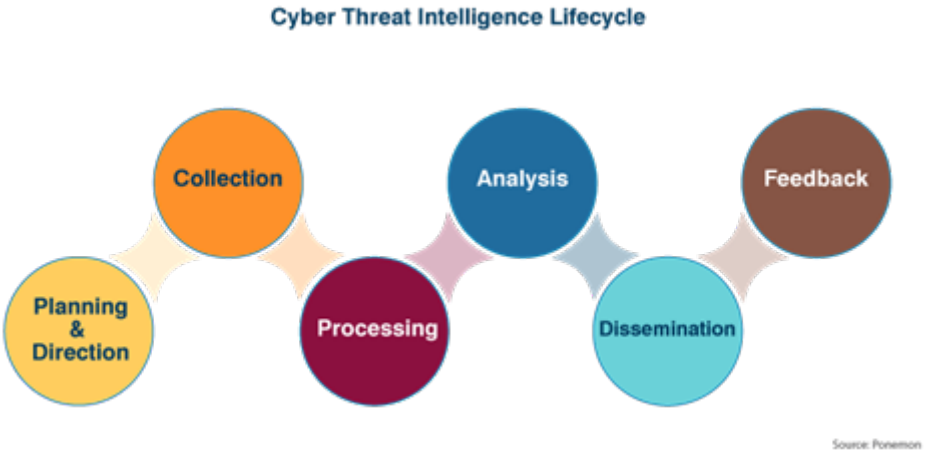
Το Cyber Threat Intelligence (CTI) επικεντρώνεται στη συλλογή και την ανάλυση πληροφοριών σχετικά με τρέχουσες και πιθανές επιθέσεις που απειλούν την ασφάλεια ενός οργανισμού. Με άλλα λόγια, το CTI είναι δεδομένα που συλλέγονται, υποβάλλονται σε επεξεργασία και αναλύονται για να κατανοηθούν τα κίνητρα, οι στόχοι και οι συμπεριφορές ενός Threat Actor. Επιτρέπει στις εταιρείες και τους οργανισμούς να λαμβάνουν ταχύτερες, πιο ενημερωμένες και υποστηριζόμενες από δεδομένα αποφάσεις, καθώς επίσης τους δίνει την δυνατότητα να αποκτούν και μεθόδους proactive defense πέρα από reacrive. Συνεπώς το πλεονέκτημα αξιοποίησης του CTI είναι ότι συνεισφέρει στην αποτροπή πιθανών επιθέσεων αλλά και εξοικονομεί το κόστος που απαιτείται για την αντιμετώπιση ενός συμβάντος ασφάλειας που έχει ήδη εκδηλωθεί. Ο βασικός σκοπός του CTI είναι να βοηθήσει τους οργανισμούς να κατανοήσουν έγκαιρα και σε βάθος τις απειλές που είναι πιθανό να τους στοχεύσουν [28, 29].

Στην σύγχρονη εποχή, οι εξελιγμένοι επιτιθέμενοι επιπέδου APT και από την άλλη πλευρά οι Blue Teams βρίσκονται διαρκώς στην προσπάθεια να ξεπερνούν ο ένας τις τεχνικές του άλλου. Τα αξιόπιστα και λεπτομερή δεδομένα για τις ανερχόμενες απειλές ή τις νέες τεχνικές και μεθόδους που χρησιμοποιεί ένας επιτιθέμενος είναι ζωτικής σημασίας για την οργάνωση της άμυνας του οργανισμού και την πρόληψη μελλοντικών επιθέσεων.

3.2 Threat Intelligence Lifecycle

Το Threat Intel Lifecycle είναι η διαδικασία μετατροπής των δεδομένων που έχουν συλλεχθεί σε χρήσιμες για τον οργανισμό πληροφορίες που είναι ικανές να υποβοηθήσουν στη λήψη αποφάσεων. Υπάρχουν διαφορετικές εκδοχές του Threat Intel Lifecycle που διαφέρουν ελαφρώς μεταξύ τους, αλλά ο στόχος είναι πάντα κοινός, να καθοδηγεί μια ομάδα κυβερνοάμυνας στην ανάπτυξη και εκτέλεση ενός αποτελεσματικού προγράμματος Threat Intelligence.

Το Threat Intelligence είναι μια απαιτητική διαδικασία καθώς οι απειλές και οι επιτιθέμενοι εξελίσσονται συνεχώς με ραγδαίους ρυθμούς, δημιουργώντας την ανάγκη στους οργανισμούς να προσαρμόζονται γρήγορα ώστε να είναι αποτελεσματικοί στην άμυνά τους. Αυτή η διαδικασία αποτελείται από έξι στάδια που αφότου ολοκληρωθούν, η διαδικασία δεν σταματά εκεί αλλά ξεκινά από το πρώτο βήμα ώστε να υπάρχει συνεχής βελτίωση και ανατροφοδότηση [30].



Εικόνα 8. Cyber Threat Intelligence Lifecycle
Πηγή εικόνας: https://www.ethobridge.ca/what-is-threat-intelligence/

1. Planning and Direction

Το πρώτο στάδιο, που ονομάζεται Planning and Direction, είναι ζωτικής σημασίας για το lifecycle καθώς, ως το πρώτο βήμα, καθορίζει το πως θα διεξαχθούν και τα επόμενα βήματα. Η ομάδα που είναι υπεύθυνη για τη διαδικασία αυτή θα καθορίσει τους στόχους, τις απαιτήσεις και τη μεθοδολογία με βάση τις ανάγκες του οργανισμού. Θα πρέπει να θέσει ως στόχους να εντοπιστούν ποιοι είναι οι πιθανοί επιτιθέμενοι, ποια τα κίνητρά τους, ποιο είναι το Attack Surface του οργανισμού και ποιες συγκεκριμένες ενέργειες πρέπει να γίνουν για την ενίσχυση της άμυνας ενάντια σε μια αντίστοιχη μελλοντική επίθεση. Σε αυτό το στάδιο είναι επίσης σημαντικό να προσδιοριστούν τα κρίσιμα assets του οργανισμού που αποτελούν πρωταρχικό στόχο για τους επιτιθέμενους καθώς επίσης ποια μπορεί να είναι τα βασικά τους κίνητρα για την επίθεση.

2. Collection

Στο στάδιο αυτό γίνεται ο καθορισμός και η ανάπτυξη των μεθόδων που θα αξιοποιηθούν για την συλλογή των πληροφοριών, σύμφωνα με όσα ορίστηκαν ως στόχοι στο προηγούμενο βήμα. Δεν είναι πάντα εφικτό να απαντηθούν όλες οι ερωτήσεις που τέθηκαν στο πρώτο βήμα αλλά το στάδιο της συλλογής δεδομένων στοχεύει στην συλλογή όσο το δυνατόν περισσότερων σχετικών πληροφοριών άσχετα με το τελικό αποτέλεσμα. Για παράδειγμα, μπορεί να μην είναι εφικτό μέσω των διαθέσιμων δεδομένων που συλλέχθηκαν να καθοριστεί ποιο είναι το APT group που θα στοχεύσει τον οργανισμό, αλλά να είναι εφικτό να καθοριστεί το πιθανό χρονικό διάστημα. Οι αναλυτές που είναι υπεύθυνοι για την συλλογή των δεδομένων αναζητούν διαφορετικής μορφής δεδομένα που μπορεί να είναι πληροφορίες απο άλλα threat intel reports, IoCs, OSINT data, πληροφορίες απο social media ή forums όπου δραστηριοποιούνται και συνεργάζονται κυβερνοεγκληματίες, Dark Web forums κ.α.

3. Processing

Αφού συλλεχθούν τα δεδομένα, θα πρέπει να υποστούν επεξεργασία ώστε να μετατραπούν σε μορφή κατάλληλη για ανάλυση με στόχο την εξαγωγή χρήσιμων συμπερασμάτων. Ο όγκος των δεδομένων που εν τέλει θα αξιοποιηθεί συνήθως είναι μικρότερος από τον όγκο των δεδομένων που έχουν συλλεχθεί και τα δεδομένα που δεν θα υποβληθούν σε επεξεργασία δεν θα προσφέρουν κάποιο συμπέρασμα.

4. Analysis

Εφόσον έχει ολοκληρωθεί η επεξεργασία των δεδομένων, οι αναλυτές πρέπει να πραγματοποιήσουν ανάλυση για να δώσουν απαντήσεις στα ερωτήματα που τέθηκαν στο πρώτο βήμα του Life Cycle (Planning and Direction). Σημαντική παράμετρο αποτελεί η ικανότητα του κάθε αναλυτή να είναι αντικειμενικός στις απαντήσεις που θα δώσει σε αυτά τα ερωτήματα καθώς θα πρέπει να είναι

σε θέση να μην επηρεάζεται από τις προσωπικές του απόψεις και οπτική ώστε να πραγματοποιήσει την ανάλυση αντικειμενικά και αμερόληπτα.

5. Dissemination

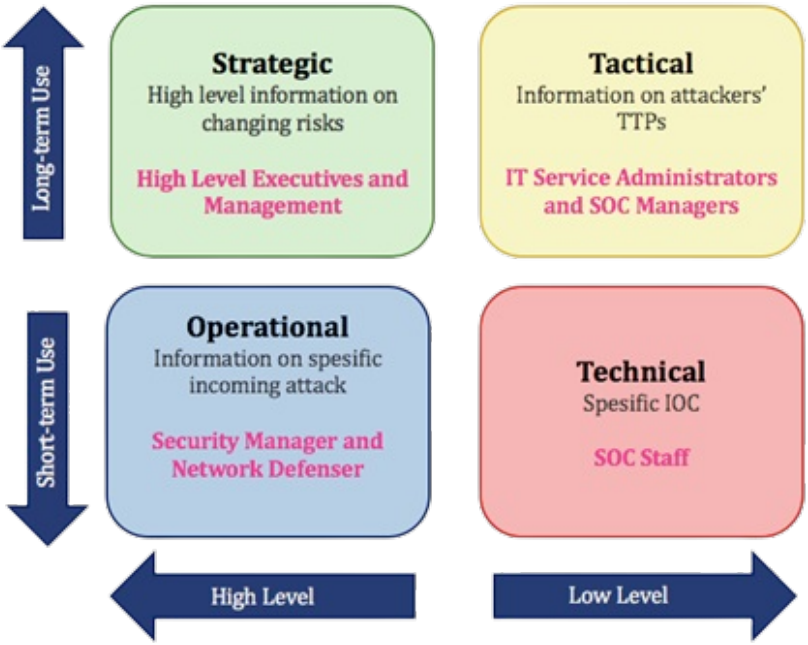
Κάθε οργανισμός έχει διαφορετικές ομάδες που μπορούν να επωφεληθούν από τις πληροφορίες και τα παράγωγα του Threat Intel. Η παράδοση αυτών των πληροφοριών στους ενδιαφερόμενους εντός του οργανισμού ονομάζεται Dissemination. Κατά το στάδιο λοιπόν του Dissemination, η ομάδα που ήταν υπεύθυνη για το Threat Intel καλείται να αποδώσει την ανάλυσή της σε κατανοητή μορφή ανάλογα με τον κάθε αποδέκτη. Οι αναλυτές πρέπει να εξετάσουν διάφορες παραμέτρους, όπως το ποια είναι τα πιο επείγοντα ζητήματα, ποιος πρέπει να λάβει τη συγκεκριμένη πληροφορία και πόσες τεχνικές λεπτομέρειες χρειάζεται ο κάθε παραλήπτης. Για παράδειγμα μια αναφορά των αποτελεσμάτων του Threat Intel που έχει ως αποδέκτη έναν C Level Executive πχ (CEO) θα πρέπει να είναι μικρής έκτασης και αφαιρετικού περιεχομένου, αποφεύγοντας τεχνικές λεπτομέρειες ή αναλύσεις. Από την άλλη πλευρά ένα report που θα απευθύνεται στους αναλυτές του SOC θα πρέπει να είναι όσο το δυνατόν πιο αναλυτικό και περιεκτικό σε τεχνικές λεπτομέρειες, ώστε να τους βοηθήσει να εκμεταλλευθούν στο μέγιστο αυτές τις πληροφορίες στις αναλύσεις που θα πραγματοποιούν.

6. Feedback

Το τελικό στάδιο περιλαμβάνει τη λήψη feedback σχετικά με τις αναφορές που παραδόθηκαν στους ενδιαφερόμενους ώστε να διαπιστωθεί εάν πρέπει να γίνουν προσαρμογές στις μελλοντικές αναφορές που θα πραγματοποιηθούν. Τα ενδιαφερόμενα μέρη ενδέχεται να θέσουν διαφορετικές απαιτήσεις ή προτεραιότητές ή να εκφράσουν την επιθυμία για αλλαγές σε κάποιο από τα υπόλοιπα στάδια. Αυτό το στάδιο είναι ίσως το πιο δύσκολο να επιτευχθεί, καθώς η έλλειψη ουσιαστικού feedback από τους παραλήπτες των αναφορών είναι συχνό φαινόμενο. Η δημιουργία καλών μηχανισμών για τη λήψη feedback βοηθά όσους διεξάγουν την έρευνα να την βελτιώσουν.

3.3 Τύποι Threat Intelligence

Σύμφωνα με το Threat Intel Lifecycle, το τελικό αποτελέσματα, δηλαδή τα Threat Intel reports, θα είναι διαφορετικά ανάλογα με τις αρχικές απαιτήσεις που είχαν τεθεί, τις πηγές πληροφοριών που αξιοποιήθηκαν, αλλά κυρίως και τους παραλήπτες στους οποίους απευθύνονται. Είναι χρήσιμο λοιπόν με βάση αυτά τα κριτήρια να γίνει διαχωρισμός του Threat Intelligence σε διαφορετικές κατηγορίες. [31]



Εικόνα 9. Τύποι Threat Intelligence
Πηγή εικόνας: https://socradar.io/what-is-strategic-cyber-intelligence-and-how-to-use-it/

Strategic

Ευρύτερες τάσεις για απειλές που προορίζονται για ένα μη τεχνικό κοινό, δηλαδή C Level Executives, όπως CEO ή CFO και κάθε άλλον διευθύνοντα σύμβουλο. Οι πληροφορίες που παρέχονται σε αυτό το επίπεδο, πρέπει να βοηθούν τους υπεύθυνους λήψης αποφάσεων να κατανοήσουν σε αφαιρετικό επίπεδο την απειλή όπως τα πιθανά κίνητρα και τις συνέπειες.

Operational

Περιλαμβάνει τεχνικές λεπτομέρειες σχετικά με συγκεκριμένες επιθέσεις ή εκστρατείες που είναι σε εξέλιξη ή πιθανόν να στοχεύσουν τον οργανισμό. Το Operational Intelligence παρέχει χρήσιμες πληροφορίες σε όσους λαμβάνουν καθημερινές αποφάσεις, όπως ο Security Manager, για τον καθορισμό προτεραιοτήτων και την κατανομή των οικονομικών ή ανθρώπινων πόρων. Η αναφορά μπορεί να περιλαμβάνει νέες αδυναμίες ή TTPs που μπορεί να αξιοποιούν οι επιτιθέμενοι γεγονός που θα αποτελέσει καθοριστικό παράγοντα για το ποια συστήματα ενδεχομένως να στοχεύσουν, άρα και να απαιτείται η περαιτέρω παρακολούθηση και προστασία τους.

Tactical

Περιγράφει τα tactics, techniques και procedures (TTPs) του Threat Actor με τεχνικές λεπτομέρειες που απευθύνονται σε άτομα με τεχνικές γνώσεις. Σε αυτή την περίπτωση, το report θα μπορούσε να βοηθήσει τον SOC manager να καθοδηγήσει το προσωπικό του SOC ως προς το πού να εστιάσουν τις αναλύσεις τους.

Technical

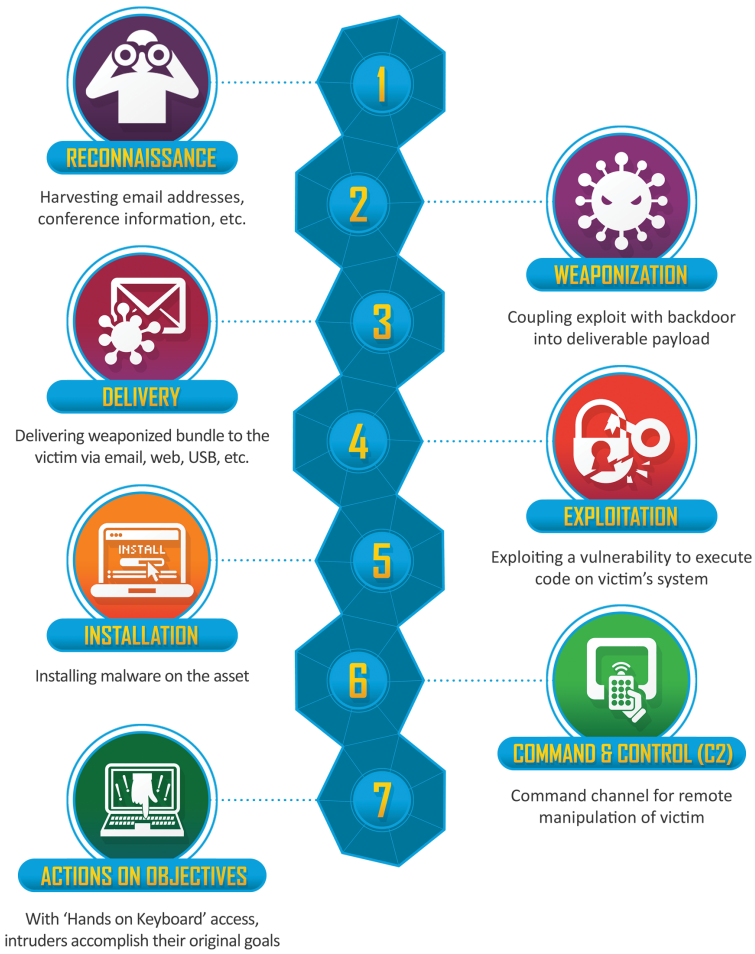
Περιλαμβάνει εξειδικευμένες και αναλυτικές τεχνικές πληροφορίες που παρέχονται σε όσους καλούνται να λάβουν άμεσες αποφάσεις για πιθανά περιστατικά ασφαλείας, όπως οι αναλυτές του SOC ή του IR. Σε αυτήν την περίπτωση, το report θα περιλαμβάνει πληροφορίες όπως IoCs με μορφή hash value, διευθύνσεις IP ή domain names.

3.4 Frameworks

Υπάρχουν διαθέσιμες διάφορες προσεγγίσεις και Frameworks για την προσπάθεια παρακολούθησης, χαρτογράφησης και ανάλυσης των χαρακτηριστικών των APTs στην προσπάθεια καλύτερης κατανόησης και αντιμετώπισης τους. Αυτά τα Frameworks μπορούν να χρησιμοποιηθούν επίσης και για μελέτες Cyber Threat Intelligence, διότι η κατανόηση των μεθόδων που χρησιμοποιεί κάθε APT είναι ζωτικής σημασίας για ένα αποτελεσματικό Threat Intelligence. Σε αυτό το κεφάλαιο θα αναλυθούν δύο από τα πιο διαδεδομένα αντίστοιχα Frameworks, το Cyber Kill Chain από την Lockheed Martin και το MITRE ATT&CK.

3.4.1 Cyber Kill Chain

Το Cyber Kill Chain Framework αναπτύχθηκε από την Lockheed Martin και είναι μέρος του Intelligence Driven Defense model για τον εντοπισμό και την πρόληψη εισβολών. Το μοντέλο ορίζει τα βήματα που πρέπει να πραγματοποιήσει ένας επιτιθέμενος για να επιτύχει τον στόχο του. Τα επτά αυτά βήματα βοηθούν τις Blue Teams να κατανοήσουν καλύτερα τα TTPs του επιτιθέμενου χωρίζοντας τα σε διαφορετικά στάδια και μέσω της καλύτερης κατανόησης αυτών των σταδίων τις βοηθά να εντοπίζουν και να αποτρέπουν τις επιθέσεις σε αρχικό στάδιο [32, 33].



Εικόνα 10. Lockheed Martin - Cyber Kill Chain
Πηγή εικόνας: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

1. Reconnaissance

Κατά τη διάρκεια του πρώτου σταδίου, που ονομάζεται Reconnaissance, ένας Threat Actor έχει ως στόχο να εντοπίζει έναν στόχο και πιθανές ευπάθειες ή αδυναμίες. Ως μέρος αυτής της διαδικασίας, ο Threat Actor συλλέγει κάθε μορφής χρήσιμες πληροφορίες, όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου, κωδικούς πρόσβασης που έχουν διαρρεύσει, πληροφορίες για την υποδομή του οργανισμού, όπως εφαρμογές λογισμικού ή εκδόσεις λειτουργικών συστημάτων που χρησιμοποιεί. Στην συνέχεια αυτές οι πληροφορίες συνήθως αξιοποιούνται για να βρεθεί το πιο αδύνατο σημείο του οργανισμού ώστε και να στοχευθεί. Όσο περισσότερες πληροφορίες μπορεί να συγκεντρώσει ο επιτιθέμενος τόσο πιο εξελιγμένη και αποτελεσματική θα είναι η επίθεση και, ως εκ τούτου, τόσο μεγαλύτερη είναι η πιθανότητα επιτυχίας.

2. Weaponization

Κατά τη διάρκεια του Weaponization, ο επιτιθέμενος δημιουργεί ένα Attack Vector, όπως ένα κακόβουλο λογισμικό απομακρυσμένης πρόσβασης που μπορεί να εκμεταλλευτεί μια ευπάθεια που έχει εντοπίσει στην υποδομή του οργανισμού. Ο επιτιθέμενος αναπτύσσει το κακόβουλο λογισμικό με βάση τις ανάγκες του και προσπαθεί να μειώσει τις πιθανότητες εντοπισμού του από την Blue Team του οργανισμού.

3. Delivery

Σε αυτό το στάδιο ο επιτιθέμενος ξεκινά την επίθεση. Τα συγκεκριμένα βήματα που θα πραγματοποιηθούν εξαρτώνται από το είδος της εκάστοτε επίθεσης. Για παράδειγμα, μια από τις πιο συνηθισμένες μεθόδους είναι η αποστολή συνημμένων κακόβουλων αρχείων μέσω ηλεκτρονικού ταχυδρομείου ώστε ένας από τους υπαλλήλους του οργανισμού να εξαπατηθεί και να εκτελέσει το αρχείο. Αυτή η δραστηριότητα συνήθως συνδυάζεται με τεχνικές κοινωνικής μηχανικής (Social Engineering) ώστε να αυξηθεί η αποτελεσματικότητα της εκστρατείας της επίθεσης.

4. Exploitation

Στη φάση του Exploitation, ο κακόβουλος κώδικας εκτελείται στο σύστημα του θύματος. Στην περίπτωση που είχε σταλεί μέσω συνημμένων κακόβουλων αρχείων μέσω ηλεκτρονικού ταχυδρομείου, όπως αναφέρθηκε προηγουμένως, απαραίτητη είναι η ανθρώπινη αλληλεπίδραση. Η περίμετρος ασφαλείας του οργανισμού παραβιάζεται και οι επιτιθέμενοι έχουν την ευκαιρία να εκμεταλλευτούν τα συστήματά του χρησιμοποιώντας επιπρόσθετα εργαλεία.

5. Installation

Αμέσως μετά τη φάση του Exploitation, το κακόβουλο λογισμικό ή ένα άλλο Attack Vector εγκαθίσταται στο σύστημα του θύματος. Αυτό είναι ένα κομβικό σημείο στον Cyber Kill Chain Lifecycle, καθώς ο επιτιθέμενος μπορεί πλέον να αναλάβει τον πλήρη έλεγχο ενός συστήματος εντός του οργανισμού.

6. Commanda and Control

Στο στάδιο του Command and Control, ο εισβολέας είναι σε θέση να χρησιμοποιήσει το εγκατεστημένο κακόβουλο λογισμικό για να αποκτήσει τον απομακρυσμένο έλεγχο μιας συσκευής μέσα στο δίκτυο του οργανισμού και να πραγματοποιήσει περαιτέρω ενέργειες που επιθυμεί και ταυτίζονται με τον τελικό του στόχο. Για παράδειγμα μπορεί να πραγματοποιήσει Pivoting ή Lateral Movement εντός του δικτύου επεκτείνοντας την πρόσβασή του και φτάνοντας σε πιο κρίσιμα συστήματα και υποδομές. Επιπλέον με αυτό τον τρόπο, εφόσον έχει μολύνει περισσότερα συστήματα, αποκτά και την ικανότητα να έχει περισσότερα σημεία παραβίασης της περιμέτρου του οργανισμού στο μέλλον, σε περίπτωση που του αποκλειστεί η πρόσβαση.

7. Actions on Objectives

Σε αυτό το στάδιο, ο εισβολέας κάνει βήματα για να πετύχει τους επιδιωκόμενους στόχους του, οι οποίοι μπορεί να περιλαμβάνουν κλοπή, καταστροφή, παραποίηση, κρυπτογράφηση ή εξαγωγή δεδομένων. Όσο νωρίτερα ο οργανισμός καταφέρει να σταματήσει την απειλή μέσα στον Cyber Attack Lifecycle, τόσο μικρότερο κίνδυνο και επιπτώσεις θα αντιμετωπίσει. Οι επιθέσεις που φτάνουν στο στάδιο του Command and Control συνήθως απαιτούν πολύ πιο σύνθετες προσπάθειες αποκατάστασης από την πλευρά του οργανισμού καθώς οι επιτιθέμενοι έχουν φτάσει στο στάδιο να έχουν πλήρη έλεγχο σε πολλαπλά εσωτερικά συστήματα και δεδομένα. Ως εκ τούτου, οι οργα-

νισμοί θα πρέπει ιδανικά να λάβουν μέτρα για τον εντοπισμό και την εξουδετέρωση των απειλών όσο το δυνατόν νωρίτερα στον Cyber Attack Lifecycle που περιγράφει το Cyber Kill Chain, προκειμένου να ελαχιστοποιηθούν τόσο οι επιπτώσεις της επίθεσης όσο και το κόστος ανάκαμψης.

Το Cyber Kill Chain της Lockheed Martin είναι αρκετά γραμμικό στην προσέγγισή του, κάτι που μερικές φορές μπορεί να θεωρηθεί ως πλεονέκτημα, καθώς είναι μια πιο ξεκάθαρη προσέγγιση για τους επαγγελματίες ασφαλείας που προσπαθούν να εντοπίσουν μια πιθανή απειλή. Ωστόσο, αυτή η γραμμικότητα μπορεί επίσης να θεωρηθεί και πρόβλημα, επειδή μπορεί να αναγκάσει ή να οδηγήσει τους επαγγελματίες ασφαλείας να υπεραπλουστεύσουν καταστάσεις ή να εξάγουν γρήγορα και αυθαίρετα συμπεράσματα σχετικά με τα στάδια που ακολούθησε ένας επιτιθέμενος σε ένα Attack Chain. Το μοντέλο αυτό έχει επικριθεί αρκετά καθώς δεν πάντα επαρκές για να περιγράψει πλήρως τον τρόπο με τον οποίο λειτουργούν οι σύγχρονοι επιτιθέμενοι, αλλά ταυτόχρονα έχει επαινεθεί για την ικανότητα του να οριοθετεί τα σημεία στα οποία μπορεί να σταματήσει μια επίθεση.

Ενώ το Cyber Kill Chain της Lockheed Martin εξακολουθεί να είναι ένα χρήσιμο εργαλείο για την καλύτερη κατανόηση των διαφορετικών σταδίων μιας επίθεσης, δεν είναι πάντα επαρκές για την περιγραφή ενός κύκλου επίθεσης που θα ακολουθήσει ένας σύγχρονος εξελιγμένος επιτιθέμενος. Για παράδειγμα, δεν είναι ασυνήθιστο για τους επιτιθέμενους να παραλείπουν ή να συνδυάζουν κάποια από τα βήματα που αναλύθηκαν, ειδικά στο πρώτο μισό μέρος του Life Cycle. Το γεγονός αυτό δεν δίνει την ευκαιρία στον οργανισμό να αντιδράσει έγκαιρα με το να αποκλείσει την επίθεση σε αρχικό στάδιο ενώ ταυτόχρονα η επικράτηση του μοντέλου αυτού μπορεί να δώσει και στους επιτιθέμενους κάποια ένδειξη για το πώς ο οργανισμός δομεί την άμυνά του.

3.4.2 MITRE ATT&CK Framework

Εικόνα 11. MITRE ATT&CK Framework
Πηγή εικόνας: https://attack.mitre.org/

Εισαγωγή

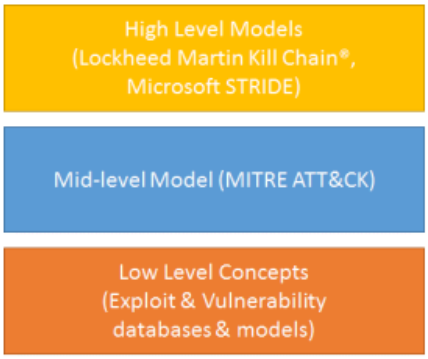
Ενώ το μοντέλο του Cyber Kill Chain και άλλα Frameworks όπως το Diamond Model εξακολουθούν ακόμη και σήμερα να χρησιμοποιούνται, οι περισσότεροι επαγγελματίες ασφαλείας αξιοποιούν το νεότερο MITRE ATT&CK Franework και την ορολογία του. Το ATT&CK προκύπτει από τα αρχικά των λέξεων: Adversarial Tactics, Techniques, and Common Knowledge. Το ATT&CK είναι ένα framework που εξελίσσεται συνεχώς και εμπλουτίζεται διαρκώς με νέα tactics, techniques και procedures (TTPs) που χρησιμοποιούνται από εξελιγμένους επιτιθέμενους (APTs) και άλλους εγκληματίες του κυβερνοχώρου. Το Framework είναι ένας πίνακας ταξινομημένος σε 14 διαφορετικές τακτικές (tactics) και αναλύει τον κύκλο ζωής μιας επίθεσης σε όλα της τα στάδια.

Το πλαίσιο έχει εξελιχθεί με την πάροδο των ετών και πλέον καλύπτει διάφορες τεχνολογίες όπως Windows, macOS, Linux, Android και iOS, συσκευές υποδομής δικτύου, τεχνολογίες Container, συστήματα cloud (IaaS ή SaaS), Office365, Azure Active Directory και Google Workspace.

Το ATT&CK υιοθετήθηκε με γρήγορους ρυθμούς από τους επαγγελματίες ασφαλείας επειδή, σε αντίθεση με άλλα frameworks όπως το Cyber Kill Chain, χαρτογραφεί και δημιουργεί ένα αποθετήριο γνώσης για όλα τα πιθανά βήματα που θα ακολουθήσει ένας επιτιθέμενος αλλά και ένας αμυνόμενος σε κάθε στάδιο της επίθεσης. Περιλαμβάνει δεδομένα σχετικά με τους πιο γνωστούς Threat Actors και APT groups σε αντιστοίχηση με τα TTPs τους και παρέχει ακόμη και αναφορές και παραδείγματα που βασίζονται σε πραγματικές επιθέσεις. Σε αντίθεση με το θεωρητικό μοντέλο Cyber Kill Chain, το MITRE ATT&CK Framewowk βασίζεται απευθείας σε δεδομένα και έρευνα που έχει πραγματοποιηθεί σε εκατομμύρια πραγματικές επιθέσεις και δίνει την δυνατότητα σε διάφορα πραγματικά σενάρια επιθέσεων να χαρτογραφηθούν και να αναπαραχθούν από τις Blue και τις Red teams με στόχο τη βελτίωση της άμυνας του οργανισμού. [34, 35, 36]

Επιπλέον μια σημαντική διαφορά του MITRE ATT&CK Framework ανάμεσα σε άλλα Frameworks είναι το επίπεδο αφαιρετικότητας που διαθέτει για την περιγραφή της συμπεριφορά των επιτιθεμένων. Frameworks όπως το Cyber Kill Chain της Lockheed Marti ή το STRIDE της Microsoft είναι χρήσιμα αλλά μόνο για την κατανόηση των βασικών στόχων και διαδικασιών τον επιτιθεμένων σε υψηλό και αφαιρετικό επίπεδο. Από την άλλη πλευρά, βάσεις δεδομένων που περιέχουν πληροφορίες για συγκεκριμένα exploits ή κακόβουλο λογισμικό περιγράφουν πολύ συγκεκριμένες υλοποιήσεις εργαλείων που ναι μεν μπορεί να χρησιμοποιήθηκαν από έναν Threat Actor αλλά δεν βοηθάνε στην καλύτερη κατανόηση του.

Το MITRE ATT&CK Framework είναι ευρέως αποδεκτό και δημοφιλές γιατί βρίσκεται στο ενδιάμεσο επίπεδο που συνδυάζει ένα αφαιρετικό μοντέλο για την περιγραφή των Threat Actors, διατηρώντας όμως την ικανότητα να παρέχει τεχνικές λεπτομέρειες για τα TTPs του, καθιστώντας το εξαιρετικά εύχρηστο και αποτελεσματικό.



Εικόνα 12. Abstraction Comparison of Models and Threat Knowledge Databases
Πηγή εικόνας: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Για να κατανοήσουμε καλύτερα την ορολογία που χρησιμοποιεί το Framework πρέπει πρώτα να γίνουν κατανοητές οι ακόλουθες έννοιες.

Επιμέρους Στοιχεία

Tactics:

Τα Tactics είναι οι υψηλού επιπέδου στόχοι τους οποίους ένας επιτιθέμενος προσπαθεί να πετύχει κατά τη διάρκεια μιας επίθεσης. Περιλαμβάνουν τα κύρια στάδια μιας επίθεσης, όπως την απόκτηση της αρχικής πρόσβασης, την παραβίαση λογαριασμών χρηστών, το Lateral Movement ή επίτευξη του Persistence εντός του δικτύου. Τα βασικά Tactics είναι τα ακόλουθα και θα αναλυθούν περαιτέρω σε επόμενο στάδιο.

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Collection
12. Command and Control
13. Exfiltration
14. Impact

Techniques:

Τα Techniques περιγράφουν το "πώς", δηλαδή τις μεθόδους που χρησιμοποιούν οι επιτιθέμενοι για να επιτύχουν μια Tactic. Όλα τα Tactics έχουν πολλαπλά Techniques, ενώ ορισμένες Techniques μπορούν να κατηγοριοποιηθούν περαιτέρω σε Sub-Techniques. Έτσι, για κάθε high-level Tactic, το MITRE ATT&CK ορίζει πολλαπλές Techniques για την επίτευξη του στόχου. Για να γίνει πιο κατανοητό το παραπάνω μοντέλο ένα απλό παράδειγμα είναι το Phishing (Technique T1566) που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν Initial Access (Tactic TA0001). Το Phishing Technique μπορεί να χωριστεί σε τρία σχετικά Sub-Techniques: το Spearphishing Attachment (T1566.001), το Spearphishing Link (T1566.002) και το Spearphishing via a Service (T1566.003).

Procedures:

Τα Procedures περιγράφουν τις συγκεκριμένες υλοποιήσεις των Techniques και Sub-Techniques που έχουν χρησιμοποιήσει οι APTs. Περιλαμβάνουν malware, συγκεκριμένα tools και τους Threat Actors/APT groups που είναι γνωστό ότι χρησιμοποιούν ή έχουν χρησιμοποιήσει στο παρελθόν τη συγκεκριμένη Technique.

Detections:

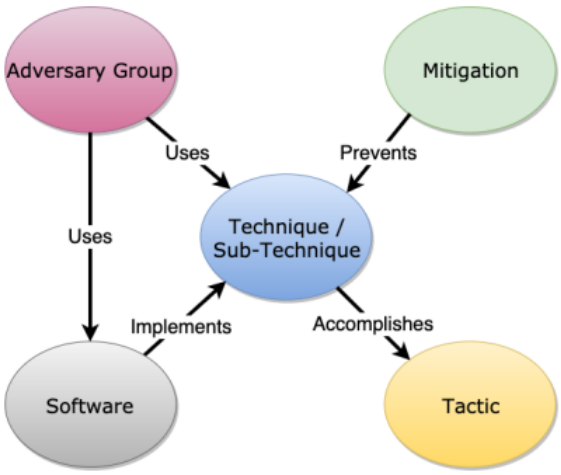
Μέσω των Detections για μια συγκεκριμένη Technique, το MITRE ATT&CK framework προτείνει τις αντίστοιχες μεθόδους ανίχνευσης. Αυτή η ενότητα είναι εξαιρετικά χρήσιμη για το Detection Engineering επειδή περιγράφει τις πληροφορίες και τα δεδομένα που πρέπει να συλλεχθούν για τον εντοπισμό της συγκεκριμένης επίθεσης.

Mitigations:

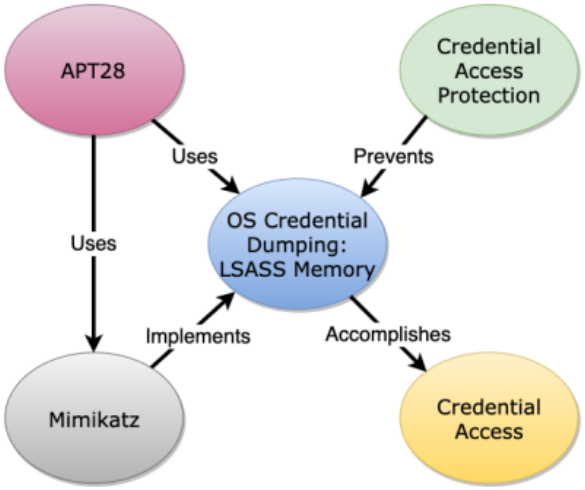
Τέλος στην ενότητα του Mitigation περιγράφονται τα βήματα που μπορεί να ακολουθήσει ένας οργανισμός για να αποτρέψει ή να μειώσει τις επιπτώσεις μιας συγκεκριμένης Technique. Για παράδειγμα, η χρήση Multi-factor Authentication (MFA) είναι ένας συνηθισμένος τρόπος Mitigation για τα Techniques που εκμεταλλεύονται την πρόσβαση σε λογαριασμούς χρηστών μέσω κωδικών πρόσβασης.

Ένα πλήρες παράδειγμα θα ήταν το εξής:

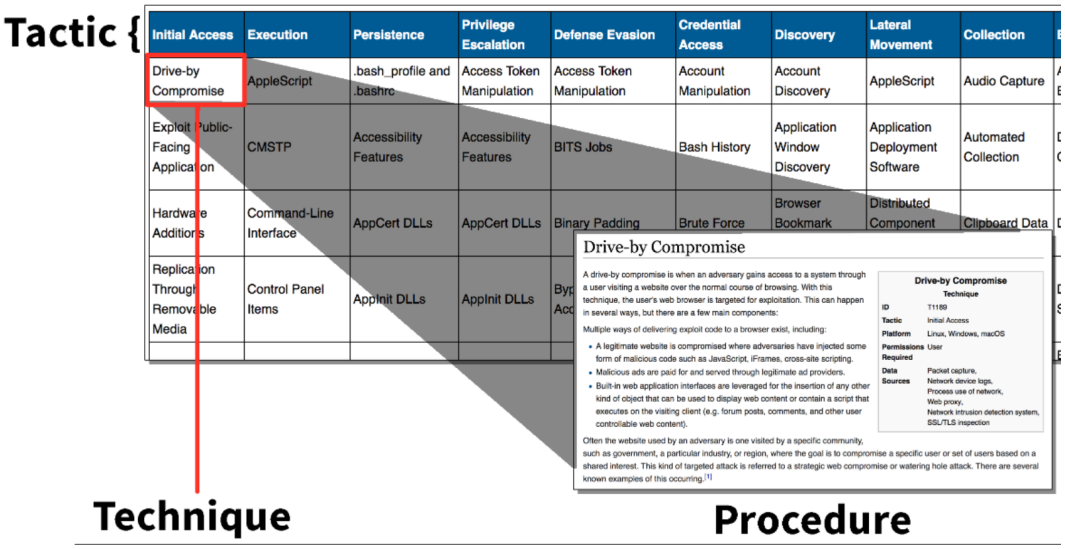
Tactic: Initial Access (TA0001)
Technique: Phishing (T1566)
Procedure: Hikit (S0009)
Sub-Technique: Spearphishing Attachment (T1566.001)
Detection: Network Traffic (DS0029)
Mitigation: User Training (M1017)



Εικόνα 13. ATT&CK Model Relationships
Πηγή εικόνας: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf



Εικόνα 14. ATT&CK Model Relationships παράδειγμα
Πηγή εικόνας: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf



Εικόνα 15. Οπτικοποίηση Tactics, Techniques, Procedures
Πηγή εικόνας: https://threatexpress.com/img/mitre-1.png

Ανάλυση των Tactics

Reconnaissance - Ο επιτιθέμενος προσπαθεί να συλλέξει πληροφορίες που μπορούν να χρησιμοποιηθούν για το σχεδιασμό επιθέσεων.

Στο στάδιο του Reconnaissance (TA0043) ο επιτιθέμενος συλλέγει πληροφορίες που μπορούν να χρησιμοποιηθούν για την υποστήριξη και το σχεδιασμό μελλοντικών επιθέσεων. Οι πληροφορίες αυτές μπορεί να περιλαμβάνουν λεπτομέρειες σχετικά με την οργάνωση, την υποδομή ή το προσωπικό του οργανισμού, και ενδεχομένως να αξιοποιηθούν και σε άλλες φάσεις της επίθεσης.

Resource Development - Ο επιτιθέμενος προσπαθεί να εδραιώσει resources που πιθανόν να χρησιμοποιηθούν για την υποστήριξη της επίθεσης.

Το Resource Development (TA0042) αποτελείται από Techniques που περιλαμβάνουν τη δημιουργία, αγορά ή υποκλοπή resources τα οποία θα χρησιμοποιηθούν για την υποστήριξη των αναγκών της επίθεσης. Τα resources αυτά μπορεί περιλαμβάνουν infrastructure, εργαλεία, domain names, λογαριασμούς σε υπηρεσίες κ.α. και μπορούν να αξιοποιηθούν και σε επόμενα στάδια της επίθεσης. Για παράδειγμα, η χρήση domain names που αγοράστηκαν από τον επιτιθέμενο μπορούν να αξιοποιηθούν στο στάδιο του Command and Control, ενώ παραβιασμένοι λογαριασμοί email στο στάδιο του Initial Access, ως μέρος ενός phishing campaing.

Initial Access - Ο επιτιθέμενος προσπαθεί να παραβιάσει την περίμετρο αποκτώντας αρχική πρόσβαση στο δίκτυο.

Το Initial Access αποτελείται από techniques που χρησιμοποιούν διαφορετικούς τρόπους για την απόκτηση της αρχικής πρόσβασης σε ένα δίκτυο. Τα techniques αυτά μπορεί να περιλαμβάνουν για παράδειγμα spearphishing και εκμετάλλευση αδυναμιών σε public-facing web servers. Η πρόσβαση που θα αποκτηθεί μέσω του Initial Access ανάλογα με το Technique που χρησιμοποιήθηκε μπορεί να προσφέρει συνεχή πρόσβαση, αν για παράδειγμα περιλαμβάνει ενεργά user credentials, ενώ μπορεί να είναι και προσωρινή, αν αποκτήθηκε με άλλο μέσο, όπως ένα webshell σε έναν public-facing web server που μπορεί να τερματιστεί ανά πάσα στιγμή.

Execution - Ο επιτιθέμενος προσπαθεί να εκτελέσει κακόβουλο κώδικα.

Το Execution αποτελείται από techniques που έχουν ως αποτέλεσμα την εκτέλεση κακόβουλου κώδικα. Τα techniques αυτά συχνά συνδυάζονται με techniques από άλλα tactics ώστε να επιτευχθούν ευρύτεροι στόχοι, όπως η εξερεύνηση του δικτύου ή η υποκλοπή δεδομένων. Για παράδειγμα, ο επιτιθέμενος μπορεί να χρησιμοποιήσει ένα remote administration tool για να εκτελέσει ένα PowerShell script που πραγματοποιεί Remote System Discovery.

Persistence - Ο επιτιθέμενος προσπαθεί να διατηρήσει την πρόσβαση του στον στόχο.

Το Persistence αποτελείται από techniques που χρησιμοποιούν οι επιτιθέμενοι για να διατηρήσουν την πρόσβαση τους σε συστήματα, παρά τις αλλαγές που μπορεί να προκύψουν σε αυτά που ενδεχομένως να διέκοπταν την πρόσβαση, όπως επανεκκινήσεις, αλλαγές κωδικών, ενημερώσεις ασφαλείας.

Privilege Escalation - Ο επιτιθέμενος προσπαθεί να αποκτήσει δικαιώματα υψηλότερου επιπέδου.

Το Privilege Escalation αποτελείται από techniques που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν δικαιώματα υψηλότερου επιπέδου σε ένα σύστημα ή δίκτυο σε σχέση με αυτό που διαθέτουν μέχρι τώρα. Οι επιτιθέμενοι μπορούν συχνά να εισέλθουν σε ένα δίκτυο με σκοπό να το εξερευνήσουν διαθέτοντας περιορισμένα δικαιώματα, αλλά στη συνέχεια να απαιτούνται υψηλότερα δικαιώματα ώστε να συνεχίσουν τους στόχους τους, όπως για παράδειγμα την μετάβαση σε άλλα συστήματα ή τη συλλογή ευαίσθητων δεδομένων. Κάτι τέτοιο πραγματοποιείται συνήθως από εκμετάλλευση αδυναμιών ή λανθασμένων παραμετροποιήσεων.

Defense Evasion - Ο επιτιθέμενος προσπαθεί να αποφύγει τον εντοπισμό.

Το Defense Evasion αποτελείται από techniques που χρησιμοποιούν οι επιτιθέμενοι για να αποφύγουν τον εντοπισμό τους από την Blue Team καθ' όλη τη διάρκεια της επίθεσης. Οι τεχνικές που χρησιμοποιούνται για Defense Evasion περιλαμβάνουν την απεγκατάσταση ή την απενεργοποίηση του security software (AV, IPS, EDR, SIEM) ή το obfuscation των script / source code που χρησιμοποιείται.

Credential Access - Ο επιτιθέμενος προσπαθεί να υποκλέψει λογαριασμούς και κωδικούς πρόσβασης.

Το Credential Access αποτελείται από techniques για την υποκλοπή στοιχείων πρόσβασης. Οι τεχνικές που χρησιμοποιούνται περιλαμβάνουν keylogging ή credential dumping μέσω εργαλείων όπως το Mimikatz. Η χρήση πραγματικών στοιχείων πρόσβασης πέρα από το γεγονός ότι παρέχει στους επιτιθέμενους εύκολη πρόσβαση σε συστήματα, καθιστά ιδιαίτερα δύσκολο και τον εντοπισμό τους, καθώς δεν είναι εύκολος ο διαχωρισμός τους από τους πραγματικούς χρήστες, και επιπλέον τους δίνει την ευκαιρία να δημιουργήσουν περισσότερους λογαριασμούς ώστε να πετύχουν τους στόχους τους.

Discovery - Ο επιτιθέμενος προσπαθεί να κατανοήσει το περιβάλλον του οργανισμού.

Το Discovery αποτελείται από techniques που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος για να αποκτήσει πληροφορίες σχετικά με το σύστημα και το εσωτερικό του δίκτυο. Με αυτόν τον τρόπο μπορεί να παρατηρεί το περιβάλλον εντός του οργανισμού και είναι σε θέση να αποφασίσει για το πως θα συνεχίσει την επίθεση.

Lateral Movement - Ο επιτιθέμενος προσπαθεί να κινηθεί σε άλλα συστήματα.

Το Lateral Movement αποτελείται από techniques που χρησιμοποιούν οι επιτιθέμενοι για να εισέλθουν σε απομακρυσμένα συστήματα σε ένα δίκτυο και να τα ελέγξουν. Η επίτευξη του τελικού στόχου του επιτιθέμενου πολλές φορές απαιτεί την εξερεύνηση του δικτύου ώστε να εντοπιστεί ο στόχος και στη συνέχεια να αποκτηθεί πρόσβαση σε αυτόν. Αυτό συχνά περιλαμβάνει το pivoting διαμέσω πολλαπλών συστημάτων και λογαριασμών. Οι επιτιθέμενοι μπορούν να εγκαταστήσουν τα δικά τους εργαλεία απομακρυσμένης πρόσβασης για να επιτύχουν Lateral Movement ή να χρησιμοποιήσουν user crendetials με native tools του κάθε λειτουργικού συστήματος, όπως το PsExec στα Windows, κάτι που μπορεί να τους βοηθήσει να αποφύγουν τον εντοπισμό.

Collection - Ο επιτιθέμενος προσπαθεί να συγκεντρώσει δεδομένα σχετικά με τον στόχο του.

Το Collection αποτελείται από techniques που χρησιμοποιούνται από τον επιτιθέμενο για τη συλλογή πληροφοριών καθώς είναι σύνηθες ο επόμενος στόχος μετά τη συλλογή να είναι το exfiltration των πληροφοριών αυτών. Για παράδειγμα, πολλά Ransomware groups πριν κρυπτογραφήσουν τα δεδομένα, συνηθίζουν να τα κάνουν exfiltrate ώστε να έχουν έναν ακόμα εκβιαστικό μηχανισμό για τη διαπραγμάτευση στην καταβολή των λύτρων.

Command and Control - Ο επιτιθέμενος προσπαθεί να επικοινωνήσει με παραβιασμένα συστήματα για να τα ελέγξει.

Το Command and Control αποτελείται από techniques με τις οποίες οι επιτιθέμενοι επικοινωνούν με συστήματα που είναι υπό τον έλεγχό τους μέσα στο δίκτυο του θύματος. Συνήθως προσπαθούν να μιμηθούν ή αναμείξουν αυτό το traffic μαζί με το κανονικό και αναμενόμενο, για να αποφύγουν τον εντοπισμό.

Exfiltration - Ο επιτιθέμενος προσπαθεί να εξάγει τα δεδομένα που έχει υποκλέψει.

Το Exfiltration αποτελείται από τεχνικές που οι επιτιθέμενοι χρησιμοποιούν για να εξάγουν τα δεδομένα που έχουν υποκλέψει από το δίκτυο που έχουν παραβιάσει. Αφού τα δεδομένα συλλεχθούν, οι επιτιθέμενοι συνήθως τα κατακερματίζουν σε μικρότερα μέρη και τα συνδυάζουν με αναμενόμενο traffic ώστε να αποφύγουν τον εντοπισμό τους κατά την αφαίρεσή τους. Αυτό μπορεί να γίνει με διαχωρισμό σε μικρότερα μέρη, συμπίεση και κρυπτογράφηση.

Impact - Ο επιτιθέμενος προσπαθεί να επιτύχει τον τελικό του στόχο.

Στο τελικό στάδιο της επίθεσης βρίσκεται το Impact το οποίο επιθυμεί να επιτύχει ο επιτιθέμενος. Αυτό αποτελείται από techniques που χρησιμοποιούνται για να επηρεαστεί το CIA triage (Confidentiality, Integrity, Availability) του οργανισμού, διαταράσσοντας τις επιχειρηματικές και τις λειτουργικές διαδικασίες. Οι τεχνικές αυτές μπορεί να περιλαμβάνουν την καταστροφή ή την παραποίηση δεδομένων και τη διαρροή ευαίσθητων πληροφοριών. Σε ορισμένες περιπτώσεις, οι επιχειρηματικές διαδικασίες μπορεί να φαίνονται ανεπηρέαστες, αλλά μπορεί να έχουν τροποποιηθεί προς όφελος των επιτιθεμένων.

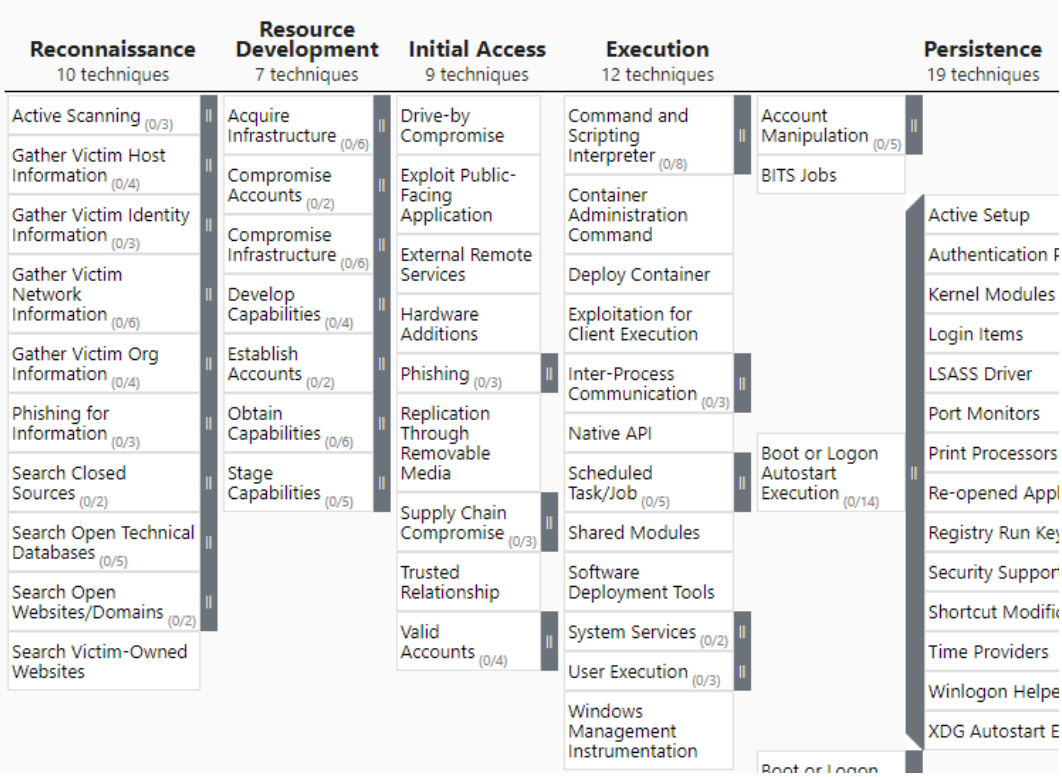
MITRE ATT&CK Framework Navigator & CARET

Ενώ το MITRE ATT&CK Framework είναι πολύ χρήσιμο για την κατανόηση και την χαρτογράφηση ενός επιτιθέμενου, δεν είναι πάντα τόσο εύκολο να γίνει η διαχείριση της καταγραφής και επεξεργασίας των δεδομένων μιας επίθεσης. Όπως φαίνεται στην παρακάτω εικόνα ενώ τα δεδομένα του Framework είναι διαθέσιμα σε spreadsheet (Excel), η μορφή τους είναι δύσχρηστη και όχι ιδιαίτερα βοηθητική.

	A	B	C	D	E	F	G	H	I
1	ID	name	description	url	created	last modified	version	tactics	detection
2	T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent	https://attack.mitre	30 January 2020	21 March 2022	1.0	Defense Evasion,	Monitor th
3	T1548.002	Abuse Elevation Control Mechanism: Byp	Adversaries may bypass UAC	https://attack.mitre	30 January 2020	19 April 2022	2.0	Defense Evasion,	There are
4	T1548.004	Abuse Elevation Control Mechanism: Ele	Adversaries may leverage the	https://attack.mitre	30 January 2020	27 March 2020	1.0	Defense Evasion,	Consider
5	T1548.001	Abuse Elevation Control Mechanism: Set	An adversary may abuse conf	https://attack.mitre	30 January 2020	19 April 2022	1.1	Defense Evasion,	Monitor th
6	T1548.003	Abuse Elevation Control Mechanism: Sud	Adversaries may perform sud	https://attack.mitre	30 January 2020	14 March 2022	1.0	Defense Evasion,	On Linux,
7	T1134	Access Token Manipulation	Adversaries may modify acce	https://attack.mitre	14 December 20	17 October 2021	2.0	Defense Evasion,	If an adve
8	T1134.002	Access Token Manipulation: Create Proce	Adversaries may create a new	https://attack.mitre	18 February 202	17 October 2021	1.1	Defense Evasion,	If an adve
9	T1134.003	Access Token Manipulation: Make and Im	Adversaries may make and im	https://attack.mitre	18 February 202	18 February 202	1.0	Defense Evasion,	If an adve
10	T1134.004	Access Token Manipulation: Parent PID S	Adversaries may spoof the pa	https://attack.mitre	18 February 202	09 February 202	1.0	Defense Evasion,	Look for in
11	T1134.005	Access Token Manipulation: SID-History I	Adversaries may use SID-Hist	https://attack.mitre	18 February 202	09 February 202	1.0	Defense Evasion,	Examine c
12	T1134.001	Access Token Manipulation: Token Impe	Adversaries may duplicate th	https://attack.mitre	18 February 202	26 March 2020	1.0	Defense Evasion,	If an adve
13	T1531	Account Access Removal	Adversaries may interrupt av	https://attack.mitre	09 October 2019	19 April 2022	1.1	Impact	Use proce
14	T1087	Account Discovery	Adversaries may attempt to g	https://attack.mitre	31 May 2017	13 October 2021	2.3	Discovery	System an
15	T1087.004	Account Discovery: Cloud Account	Adversaries may attempt to g	https://attack.mitre	21 February 202	16 March 2021	1.2	Discovery	Monitor p
16	T1087.002	Account Discovery: Domain Account	Adversaries may attempt to g	https://attack.mitre	21 February 202	13 October 2021	1.0	Discovery	System an
17	T1087.003	Account Discovery: Email Account	Adversaries may attempt to g	https://attack.mitre	21 February 202	31 March 2021	1.1	Discovery	System an
18	T1087.001	Account Discovery: Local Account	Adversaries may attempt to g	https://attack.mitre	21 February 202	28 July 2021	1.2	Discovery	System an
19	T1098	Account Manipulation	Adversaries may manipulate	https://attack.mitre	31 May 2017	18 April 2022	2.3	Persistence	Collect ev
20	T1098.001	Account Manipulation: Additional Cloud	Adversaries may add adversa	https://attack.mitre	19 January 2020	19 April 2022	2.3	Persistence	Monitor A
21	T1098.003	Account Manipulation: Additional Cloud	An adversary may add additio	https://attack.mitre	19 January 2020	19 April 2022	2.0	Persistence	Collect act
22	T1098.002	Account Manipulation: Additional Email	Adversaries may grant additic	https://attack.mitre	19 January 2020	19 April 2022	2.0	Persistence	Monitor fo
23	T1098.005	Account Manipulation: Device Registratic	Adversaries may register a de	https://attack.mitre	04 March 2022	20 April 2022	1.0	Persistence	
24	T1098.004	Account Manipulation: SSH Authorized K	Adversaries may modify the S	https://attack.mitre	24 June 2020	20 April 2022	1.1	Persistence	Use file in

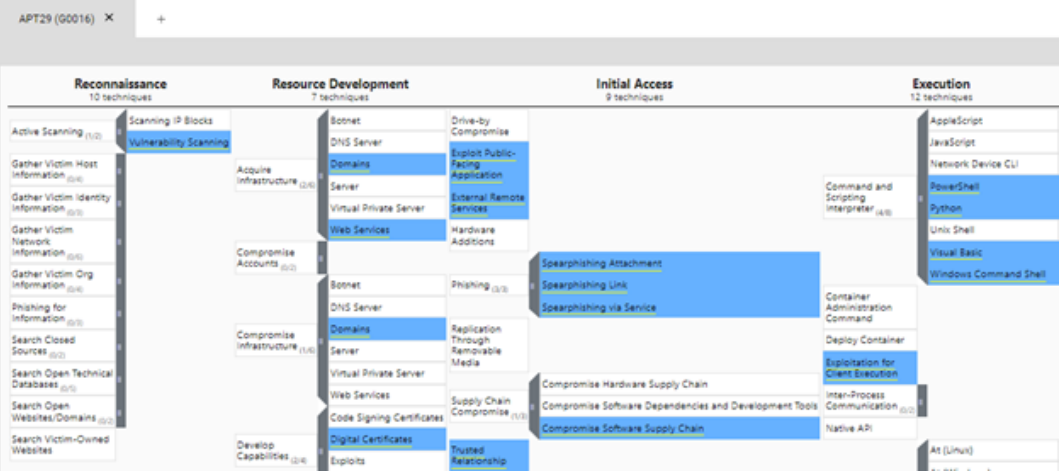
Εικόνα 16. Δεδομένα του MITRE ATT&CK Framework σε spreadsheet.

Λύση σε αυτό το πρόβλημα παρέχει το MITRE ATT&CK Navigator, που είναι ένα web-based tool που επιτρέπει στους επαγγελματίες ασφαλείας να εξερευνήσουν και να αλληλεπιδράσουν με τα στοιχεία του Framework σε οπτικοποιημένη μορφή. Το MITRE Navigator μπορεί επίσης να αξιοποιηθεί για την οπτικοποίηση ενός attack path και να βοηθήσει τις Blue Teams να χαρτογραφήσουν μια επίθεση κατανοώντας καλύτερα τα βήματα του επιτιθέμενου ή τις Red Team να οργανώσουν μια [27].



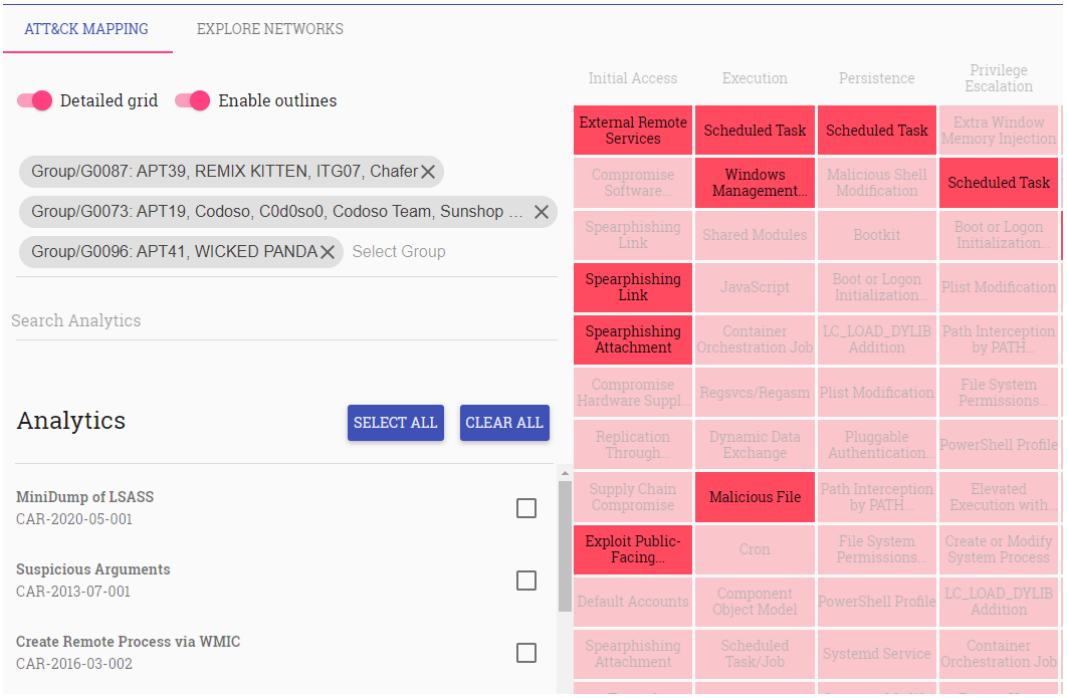
Εικόνα 17. Τα ίδια δεδομένα οπτικοποιημένα με το ATTCK Navigator.

Το συγκεκριμένο εργαλείο είναι επίσης πολύ χρήσιμο καθώς επιτρέπει το mapping ενός συγκεκριμένου APT πάνω στο Framework.



Εικόνα 18. Τα TTPs του APT29 οπτικοποιημένα πάνω στο Navigator

Το Cyber Analytic Repository Exploration Tool (CARET) παρέχει παρόμοιες δυνατότητες, με τη διαφορά ότι προσφέρει τη δυνατότητα επιλογής πολλαπλών APT group ταυτόχρονα, αντιστοιχίζοντάς τα με τα TTPs που αξιοποιούν αλλά και τη σύνδεσή τους με analytics data models και sensors που αναφέρονται στο MITRE's Cyber Analytics Repository (CAR). [37, 38]



Εικόνα 19. Τρία APT groups mapped στο MITRE CARET ταυτόχρονα.

Κεφάλαιο 4

Threat Hunting

4.1 Παραδοσιακές μέθοδοι ανίχνευσης ενός επιτιθέμενου

Κάθε οργανισμός, ανεξάρτητα του μεγέθους του ή της βιομηχανίας στην οποία δραστηριοποιείται, προσπαθεί πάντα να βρει κάθε δυνατό τρόπο ώστε να προστατευτεί από τις πιθανές κυβερνοεπιθέσεις που μπορεί να δεχθεί. Για αυτόν το λόγο άλλωστε και ένα μεγάλο ποσοστό από την ετήσια χρηματοδότηση για το Cyber Security πρόγραμμα του οργανισμού δαπανάται σε διάφορες τεχνολογίες όπως EDR, AV, IPS ώστε να βοηθηθούν οι Blue Teams, και πιο συγκεκριμένα τα SOCs, για να κάνουν πιο αποτελεσματικά τη δουλειά τους. Ωστόσο, τα αυτοματοποιημένα εργαλεία δεν είναι πάντα αρκετά για να σταματήσουν τις εξελιγμένες επιθέσεις, ειδικά στην περίπτωση που τα IOCs δεν είναι απλής μορφής όπως διευθύνσεις IP ή hash values και ο επιτιθέμενος είναι εξελιγμένος όπως ένα APT group. Ωστόσο, όπως αναλύθηκε και σε προηγούμενα κεφάλαια, η αντιμετώπιση κινδύνων αφότου έχουν εκδηλωθεί δεν είναι πάντα ο πιο αποτελεσματικός τρόπος αντιμετώπισης τους.

4.2 Threat Hunting: Μεταβαίνοντας από Reactive σε Proactive μορφές άμυνας

Η παρακολούθηση του δικτύου του οργανισμού και η προσπάθεια αντιμετώπισης απειλών που ήδη έχουν εκδηλωθεί είναι ο μέχρι τώρα γνωστός τρόπος για την προστασία των συστημάτων του οργανισμού και όσων δεδομένων αποθηκεύονται σε αυτά. Ο παραδοσιακός αυτός τρόπος εστιάζει στο να αποτρέψει κακόβουλη δραστηριότητα που ήδη έχει συμβεί ή είναι σε εξέλιξη και επικεντρώνει τις προσπάθειες στο μετριασμό της ζημιάς και της εξάπλωσης της απειλής. Ένα παράδειγμα μιας αντίστοιχης Reactive μεθοδολογίας αντιμετώπισης απειλών θα ήταν ένα Intrusion Detection System ή ένα Antivirus Solution που θα ειδοποιούσε έναν από τους αναλυτές του SOC ότι υπάρχει ένα κακόβουλο αρχείο στον υπολογιστή ενός υπαλλήλου και ότι αφού εντοπίστηκε έχει πλέον αυτόματα αποκλειστεί. Παρά το γεγονός ότι το αυτοματοποιημένο εργαλείο κατάφερε χωρίς την πρωτοβουλία κάποιου αναλυτή να εντοπίσει την απειλή και να την αποκλείσει, αυτό σημαίνει επίσης πως ένα σύστημα μπορεί να είναι ήδη μολυσμένο και ο επιτιθέμενος να έχει καταφέρει να τα μετακινηθεί και σε άλλα συστήματα του οργανισμού.

Λόγω της εξέλιξης των επιτιθεμένων οι Blue Teams δεν έχουν τα περιθώρια να περιμένουν να συμβεί ένα περιστατικό ασφαλείας για αναλάβουν δράση. Από το να αντιδρούν παθητικά περιμένοντας να συμβεί ένα περιστατικό για να το αντιμετωπίσουν, πλέον μπορούν να ακολουθούν Proactive μορφές άμυνας, όπως το Threat Hunting, που εστιάζουν στην προσπάθεια να εντοπίσουν απειλές πριν αυτές εκδηλωθούν. Αυτό επιτυγχάνεται αξιοποιώντας πληροφορίες που έχουν προηγουμένως αποκτηθεί κυρίως μέσω Threat Intelligence σε συνδυασμό με ασκήσεις υποθετικών σεναρίων που πραγματοποιούνται από του Threat Hunters. Αυτά τα υποθετικά σενάρια μπορεί να

διαφέρουν ανά περίπτωση αλλά ένα τυπικό παράδειγμα θα ήταν η υπόθεση ότι ένας επιτιθέμενος έχει πάρει πρόσβαση στον υπολογιστή ενός υπαλλήλου με χρήση κακόβουλου λογισμικού και τον χρησιμοποιεί για να μετακινηθεί εσωτερικά σε άλλα συστήματα, να υποκλέψει δεδομένα και να τα αποσπάσει. Σε περίπτωση λοιπόν που αυτό το κακόβουλο λογισμικό έχει καταφέρει να αποφύγει τον εντοπισμό από τα αυτοματοποιημένα συστήματα, η Blue Team αξιοποιώντας reactive τρόπος άμυνας και εντοπισμού απειλών, δεν θα ήταν σε θέση να εντοπίσει αυτή τη δραστηριότητα. Αντίθετα με τη χρήση πληροφοριών από το Threat Intelligence και αξιοποιώντας το υποθετικό σενάριο ότι ο υπολογιστής ενός υπαλλήλου έχει μολυνθεί από κακόβουλου λογισμικό, οι αναλυτές πραγματοποιούν στοχευμένες αναζητήσεις εντός του δικτύου προσπαθώντας να επιβεβαιώσουν αυτό το σενάριο. Εφόσον το υποθετικό σενάριο επιβεβαιωθεί οι αναλυτές έχουν εντοπίσει μία απειλή η οποία διαφορετικά δεν έχει εντοπιστεί και θα μπορούσε να είχε εξελιχθεί σε ένα πολύ πιο σοβαρό περιστατικό ασφαλείας.

Συνεπώς το Threat Hunting, σύμφωνα και με τον NIST, συνδυάζει εργαλεία ασφαλείας, πληροφορίες από Threat Intelligence και τις ικανότητες και την εμπειρία των αναλυτών ώστε να εντοπίζει απειλές που δεν έχουν εντοπιστεί μέχρι τώρα, μέσω της επαλήθευσης υποθετικών σεναρίων. Η διαδικασία του Threat Hunting ξεκινά με μία υπόθεση που αναπτύχθηκε βασισμένη σε κάποια δεδομένα. Αυτά τα δεδομένα θα μπορούσαν να είναι μια ασυνήθιστη αύξηση στην δραστηριότητα του δικτύου, ένα report απο ένα Penetration Test που εντόπισε ένα σοβαρό κενό ασφαλείας το οποίο είχε περάσει απαρατήρητο για χρόνια, μια πληροφορία για ένα νέο Threat Actor που στοχεύει επιχειρήσεις και οργανισμούς που ανήκουν στην ίδια βιομηχανία. Οι επαγγελματίες ασφαλείας που θα διεξάγουν το Threat Hunting θα διερευνήσουν και θα δοκιμάσουν αυτές τις υποθέσεις προσπαθώντας να βρουν στοιχεία που τις επαληθεύουν ώστε να διαπιστώσουν αν κάποια από αυτές τις απειλές έχει εκδηλωθεί χωρίς να γίνει αντιληπτή. Στην περίπτωση που ένα τέτοιο σενάριο επιβεβαιωθεί σημαίνει ότι έχει υπάρξει ένα περιστατικό ασφαλείας που έχει περάσει απαρατήρητο από τα αυτοματοποιημένα συστήματα ασφάλειας και βρέθηκε μέσω αυτής της μεθοδολογίας [39, 40, 41, 42, 43].

Εφόσον υπάρχει κάποια παραβίαση, ο βασικός στόχος είναι να εντοπιστούν όσο το δυνατόν νωρίτερα οι επιτιθέμενοι και να διακοπεί η δραστηριότητα τους προτού μπορέσουν να εκτελέσουν επιτυχώς μια ολοκληρωμένη επίθεση αλλά και να μειώσουν τον χρόνο παραμονής των επιτιθεμένων μέσα στο δίκτυο του οργανισμού (dwell time).

Με τον όρο dwell time αναφερόμαστε στον χρόνο που μεσολαβεί από τη στιγμή που ο επιτιθέμενος έχει διεισδύσει στο περιβάλλον του οργανισμού και τη στιγμή που εντοπίζεται η παραβίαση αυτή. Είναι πολύ σημαντικό για τους οργανισμούς να καταφέρουν να επιτύχουν όσο το δυνατόν πιο χαμηλό dwell time ενός επιτιθέμενο καθώς όσο ο επιτιθέμενος παραμένει εντός του δικτύου είναι σε θέση να συλλέγει περισσότερες πληροφορίες κάνοντας την επίθεση πιο δύσκολο να αντιμετωπισθεί και να καταπολεμηθεί. Την τελευταία δεκαετία, σημειώθηκε αξιοσημείωτη μείωση του μέσου dwell time, από 12 μήνες το 2011 σε λίγο λιγότερο από έναν μήνα το 2020. Το 2020 μάλιστα ο παγκόσμιος μέσος όρος του dwell time έπεσε για πρώτη φορά κάτω από 30 μέρες και πλέον οι οργανισμοί εντοπίζουν περιστατικά ασφαλείας σε λιγότερο από 24 μέρες, δηλαδή δύο φορές πιο γρήγορα από ότι το 2019 [44].

Εικόνα 20. Διάγραμμα Dwell time

4.3 Τύποι Threat Hunting

Το Threat Hunting μπορεί να χωριστεί σε δύο βασικές κατηγορίες ανάλογα με το πώς πραγματοποιείται, το Structured και το Unstructured Threat Hunting.

Το Structured Theat Hunting βασίζεται σε μία υπόθεση. Η Structured προσέγγιση βασίζεται στα tactics techniques and procedures (TTPs) ενός επιτιθέμενου, συνεπώς μέσω αυτής της διαδικασίας είναι εφικτός ο εντοπισμός ενός Threat Actor πριν αυτός καταφέρει να δημιουργήσει σημαντικό πρόβλημα στον οργανισμό ή να πραγματοποιήσει μια ολοκληρωμένη επίθεση (full chain attack). Αυτός ο τύπος βασίζεται πάνω στο MITRE ATT&CK Framework που αναλύθηκε σε προηγούμενο κεφάλαιο.

Από την άλλη πλευρά, η Unstructured προσέγγιση στο Theat Hunting δεν βασίζεται σε μια υπόθεση αλλά σε ένα IOC που έχει εντοπίσει ο αναλυτής, άρα είναι περισσότερο data-driven. Μια πιθανή κακόβουλη δραστηριότητα μπορεί να εντοπιστεί από έναν αναλυτή ο οποίος αναζητά ενδείξεις που μπορεί να σχετίζονται με μια παραβίαση. Αυτές οι ενδείξεις μπορεί να είναι ασυνήθιστα αυξημένη δικτυακή κίνηση, απόπειρες επικοινωνίας προς κακόβουλες IPs, αρχεία με hash που το Theat Intel τα περιλαμβάνει σε πιθανά IOCs απο έναν Threat Actor κτλ. Εφόσον αυτός ο τύπος Theat Hunting δεν βασίζεται σε ένα υποθετικό σενάριο που η υπόθεση μπορεί να επαληθεύει, δεν ακολουθεί μια προκαθορισμένη μεθοδολογία ή βήματα και σαφώς είναι πιο αυθόρμητο. Βασίζεται περισσότερο στην εμπειρία και το ένστικτο του αναλυτή. Επίσης βασίζεται περισσότερο σε μια ποιοτική αναφορά Theat Intelligence καθώς το οποιασδήποτε μορφής και αν είναι τα IOCs αυτά είναι που θα δώσουν την κατεύθυνση στο τι θα αναζητήσει ο αναλυτής και πως θα κατευθύνει τις αναζητήσεις του [42, 45].

4.4 Indicators of Compromise και Pyramid of Pain

Με τον όρο Indicators of compromise (IoC) αναφερόμαστε σε μοναδικά στοιχεία εντός ενός δικτύου ή ενός λειτουργικού συστήματος τα οποία με μεγάλη βεβαιότητα υποδηλώνουν κακόβουλη δραστηριότητα. Οι πιο συνηθισμένες μορφές IOC είναι διευθύνσεις IP, hashes κακόβουλων αρχείων και URLs ή domain names από C2 (command and control) servers. Αφού τα IOCs έχουν εντοπιστεί απο την Blue Team, μπορούν στη συνέχεια να αξιοποιηθούν για τον έγκαιρο εντοπισμό μελλοντικών επιθέσεων που χρησιμοποιούν τα ίδια στοιχεία [46, 47]. Αν για παράδειγμα, έπειτα από την ανάλυση ενός κακόβουλου αρχείου που εντοπίστηκε στον υπολογιστή ενός υπαλλήλου, εντοπίζεται επικοινωνία με μία συγκεκριμένη κακόβουλη IP, αυτή η διεύθυνση αποτελεί πλέον ένα νέο και μάλιστα πολύτιμο IoC. Συνεπώς, οποιοσδήποτε άλλος υπολογιστής του δικτύου προσπαθεί να επικοινωνήσει με αυτή τη διεύθυνση, αυτό αποτελεί πλέον μία ένδειξη με μεγάλη βεβαιότητα ότι και αυτό το σύστημα έχει παραβιαστεί από το ίδιο κακόβουλο λογισμικό.

Κατά αυτόν τον τρόπο, μόλις η Blue Team ανιχνεύσει έναν ή περισσότερους IoC σε ένα από τα συστήματα του οργανισμού, ξεκινά την αντιμετώπιση του πιθανού περιστατικού ασφαλείας, χρησιμοποιώντας ό,τι σχετικές πληροφορίες έχει διαθέσιμες. Οι πληροφορίες αυτές συνήθως προέρχονται είτε από logs που συγκεντρώνονται σε ένα SIEM είτε από Security Solutions όπως Antivirus EDR ή IPS. Ωστόσο, δεν είναι όλα τα IoC ίδια διότι χωρίζονται σε κατηγορίες. Κάποιες από αυτές τις κατηγορίες είναι πιο εύκολο να εντοπισθούν από τους αμυνόμενους αλλά και να αλλαχθούν από τους επιτιθέμενους, ενώ άλλες είναι πιο δύσκολο τόσο το να εντοπιστούν όσο και να αλλαχθούν. Η όλη ουσία πίσω από τον εντοπισμό και την παρακολούθηση των IOCs είναι η ενσωμάτωση τους στην συνολική στρατηγική άμυνας του οργανισμού ώστε να αποτρέπει τους επιτιθέμενους να χρησιμοποιούν ίδια εργαλεία, υποδομές ή τεχνικές για την διεξαγωγή των επιθέσεων τους. Αυτό κάνει το έργο των επιτιθέμενων σαφώς πιο δύσκολο γιατί θα πρέπει να είναι ιδιαίτερα προσεκτικοί σε κάθε τους κίνηση για να μην χρησιμοποιήσουν κάτι το οποίο έχει εντοπιστεί στο παρελθόν ως IoC και φανερώσει τη δραστηριότητα τους στην Blue Team.

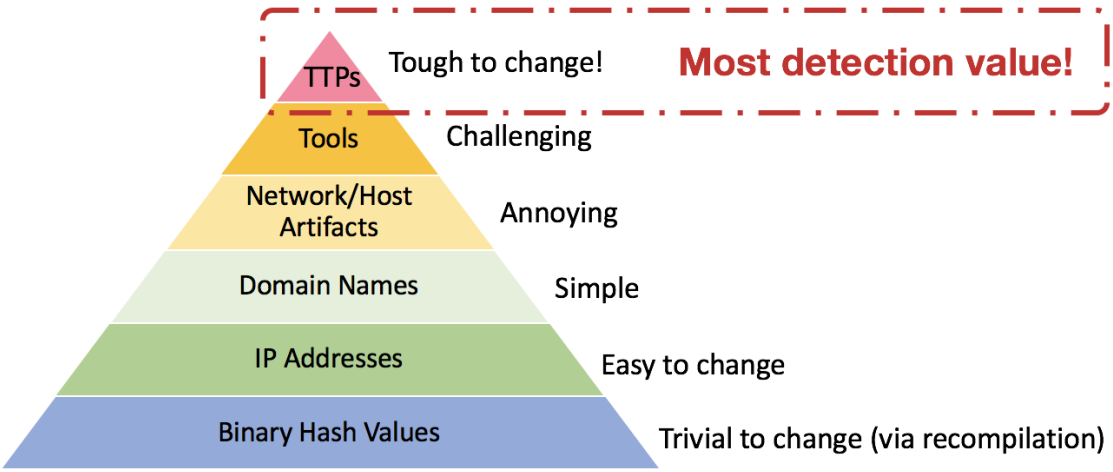
Η σχέση ανάμεσα στις διαφορετικές κατηγορίες IOCs και την δυσκολία που αντιμετωπίζουν

οι επιτιθέμενοι στην διεξαγωγή μιας επίθεσης, ανάλογα με την κατηγορία που καταφέρει η Blue Team να εντοπίσει, μπορεί να γίνει πιο κατανοητή με την έννοια του Pyramid of Pain. Η Pyramid of Pain είναι μια αναπαράσταση των διαφορετικών κατηγοριών IOC σε μορφή πυραμίδας οι οποίες είναι χωρισμένες σε αύξουσα σειρά, ανάλογα με το πόσο δύσκολο είναι να εντοπιστούν από τους αμυνόμενους αλλά και αντίστοιχα πόσο δύσκολο να αλλαχθούν από τους επιτιθέμενους. [48, 49]

Κάθε επίπεδο της πυραμίδας απεικονίζει διαφορετικούς τύπους IOC που μπορούν να αξιοποιηθούν για τον εντοπισμό της δραστηριότητας ενός επιτιθέμενου. Συνεπώς μια Blue Team, για να βελτιώσει την ικανότητα της να εντοπίζει εξελιγμένους επιτιθέμενους, πρέπει να εστιάζει της προσπάθειες της στον εντοπισμό όσο το δυνατών υψηλότερων κατηγοριών IOC στην κλίμακα που παρέχει η Pyramid of Pain.

Οι παραπάνω έννοιες μπορούν να γίνουν πιο κατανοητές μέσω ενός παραδείγματος. Όταν ένας επιτιθέμενος στείλει ένα phishing mail που περιέχει ένα εκτελέσιμο αρχείο, η Blue Team μπορεί να αναλύσει αυτό το αρχείο και εφόσον διαπιστώσει ότι είναι κακόβουλο, να πάρει το hash του και να το μετατρέψει σε ένα IOC. Κατά αυτό τον τρόπο, οποιοδήποτε e-mail σταλθεί εκ νέου και περιέχει ένα αρχείο με το ίδιο hash θα μπορεί αυτόματα να αποκλειστεί με ένα αυτοματοποιημένο εργαλείο που εκμεταλλεύεται αυτό το IOC αποτρέποντας έτσι περαιτέρω στόχευση υπαλλήλων του οργανισμού. Παρά το γεγονός ότι η δημιουργία αυτής της κατηγορίας IOC, είναι εύκολη και φαινομενικά αποτελεσματική για τους αμυνόμενους, οι επιτιθέμενοι μπορούν πολύ εύκολα να ξεπεράσουν αυτόν τον περιορισμό. Το κακόβουλο αρχείο μπορεί να δημιουργηθεί ξανά μέσα σε μερικά δευτερόλεπτα με μία πολύ μικρή και ασήμαντη αλλαγή στον κώδικα του η οποία θα έχει ως αποτέλεσμα να δημιουργηθεί ένα αρχείο με εντελώς διαφορετικό αριθμό hash. Το γεγονός αυτό καθιστά αναποτελεσματική την προηγούμενη μορφή άμυνας πού βασίζεται στην απλοϊκή μορφή IOC μέσω hash. Συνεπώς καταλαβαίνουμε ότι όσο εύκολος είναι ο εντοπισμός και δημιουργία ενός IOC άλλο τόσο εύκολο είναι και οι επιτιθέμενοι να παρακάμψουν αυτό τον εντοπισμό.

Οι τρεις πρώτες κατηγορίες IOC στην Pyramid of Pain περιλαμβάνουν (hash values, IP addresses, domain names) που μπορούν εύκολα να εντοπιστούν και να αποκλειστούν ακόμα και από αυτοματοποιημένα εργαλεία, αλλά ταυτόχρονα και οι επιτιθέμενοι είναι σε θέση να αλλάξουν τα στοιχεία αυτά σε μικρό χρονικό διάστημα και με λιγοστό κόπο. Αυτός είναι και ο βασικός σκοπός της Pyramid of Pain. Να κατηγοριοποιήσει τα IOCs ώστε να αναδείξει τη δυσκολία δημιουργίας και εντοπισμού της κάθε κατηγορίας και να βοηθήσει τις Blue Teams να εστιάσουν σε IOCs που τις βοηθάνε πραγματικά να δυσκολέψουν το έργο των επιτιθέμενων.



Εικόνα 21. Pyramid of Pain
Πηγή εικόνας: https://redcanary.com/blog/detection-engineering/

Hash Values

Οι τιμές Hashe αρχείων είναι η πιο διαδεδομένη κατηγορία IOCs καθώς είναι πολύ εύκολο να δημιουργηθούν αλλά και να ενσωματωθούν σε αυτοματοποιημένα εργαλεία όπως IDS/IPS, Antivirus. Ωστόσο, όπως αναφέρθηκε και προηγουμένως, παρέχουν τη λιγότερη αξία σε σχέση με άλλες κατηγορίες καθώς είναι πολύ εύκολο για τους επιτιθέμενους να δημιουργήσουν ένα καινούργιο κακόβουλο αρχείο το οποίο έχει την ίδια λειτουργικότητα αλλά διαφορετικό hash, πραγματοποιώντας μόνο μία μικρή αλλαγή σε αυτό και αποφεύγοντας έτσι τον εντοπισμό.

IP Addresses

Η επόμενη κατηγορία είναι οι διευθύνσεις IP, οι οποίες είναι επίσης μία πολύ δημοφιλής κατηγορία IOC, καθώς από τη φύση τους είναι ένα πολύ βασικό στοιχείο για το χαρακτηρισμό μιας δραστηριότητας, κακόβουλης ή μη. Κάθε δραστηριότητα που συμβαίνει είτε εντός είτε εκτός του δικτύου προέρχεται και καταλήγει σε μία διεύθυνση IP. Έτσι λοιπόν, είναι εύκολο για τους αμυνόμενους, εφόσον εντοπίσουν κακόβουλη δραστηριότητα η οποία προέρχεται από μία συγκεκριμένη IP, να την μετατρέψουν σε IOC και να την ενσωματώσουν σε αυτοματοποιημένα εργαλεία, όπως προηγουμένως με τα hashes.

Παρά το γεγονός ότι πλέον ένας εξελιγμένος επιτιθέμενος είναι σπάνιο να χρησιμοποιεί την ίδια IP σε πολλαπλές στοχευμένες επιθέσεις, δεν είναι και ασυνήθιστο κάποια κακόβουλη δραστηριότητα να εντοπίζεται εύκολα από την Blue Team καθώς προέρχεται από μία διεύθυνση IP που έχει αναφερθεί στο παρελθόν να διεξάγει κακόβουλες δραστηριότητες. Ωστόσο, είναι αρκετά εύκολο για τους επιτιθέμενους να αλλάζουν τη διεύθυνση IP από την οποία διεξάγουν τη δραστηριότητά τους για να αποφύγουν τον εντοπισμό. Συνεπώς και αυτή η κατηγορία IOC δεν προσφέρει πολλά στον αποτελεσματικό εντοπισμό των επιτιθεμένων.

Domain Names

Σε ένα επίπεδο παραπάνω στην πυραμίδα συναντάμε την κατηγορία των Domain Name. Σε αντίθεση με τις διευθύνσεις IP, τα domain names είναι πιο δύσκολο να αλλαχθούν απο τους επιτιθέμενους εφόσον για τη δημιουργία τους συνήθως απαιτείται η εγγραφή σε κάποια υπηρεσία, πραγματοποίηση πληρωμής και επαλήθευση των στοιχείων του αγοραστή. Όλα αυτά φυσικά για τους επιτιθέμενους δεν αποτελούν σημαντικό πρόβλημα, γιατί η αγορά μπορεί να γίνει με έναν τρόπο πληρωμής που προσφέρει ανωνυμία, όπως τα Cryptocurrencies, και να χρησιμοποιηθούν ψευδή στοιχεία αγοραστή. Από την άλλη πλευρά, τα domain names συνήθως χρειάζονται μερικές ώρες ή μέρες να τεθούν σε λειτουργία και ταυτόχρονα είναι εύκολο να διαπιστωθεί αν έχουν δημιουργηθεί πρόσφατα, άρα και να είναι πιο ύποπτα σε σχέση με άλλα domain names που είναι ενεργά για χρόνια.

Αυτοί οι παράγοντες σαφώς δημιουργούν μία περαιτέρω δυσκολία στους επιτιθέμενους επειδή απαιτούν χρόνο και περαιτέρω ενασχόληση για να αλλαχθούν αν μετατραπούν σε IOC, αλλά και πάλι υπάρχουν μέσα όπως οι domain-generated algorithms (DGA) που αυτοματοποιούν τη διαδικασία δημιουργίας νέων domain name που δεν έχουν χρησιμοποιηθεί στο παρελθόν, άρα δεν υπάρχει και κίνδυνος να έχουν εντοπιστεί ως IOC.

Network/Host Artifacts

Στην επόμενη κατηγορία στο Pyramid of Pain βρίσκονται τα Network / Host Artifacts. Τα artifacts είναι στοιχεία μιας δραστηριότητας τα οποία χαρακτηρίζουν μία κακόβουλη δραστηριότητα, διαφοροποιώντας την από μία μη κακόβουλη δραστηριότητα. Αυτά τα Artifacts μπορεί να είναι μοτίβα σε διευθύνσεις URL, user-agents, ονόματα αρχείων, ακόμα και σχόλια σε πηγαίο κώδικα. Σε αυτό το σημείο οι αμυνόμενοι, εφόσον καταφέρουν να δημιουργήσουν IOCs που βασίζονται σε Network/Host Artifacts, είναι σε θέση να δημιουργήσουν σημαντική διατάραξη στη δραστηριότητα των επιτιθεμένων. Μέσω αντίστοιχων IOCs οι αμυνόμενοι μπορεί να καταφέρουν να αναγκάσουν τους επιτιθέμενους να διακόψουν τη δραστηριότητά τους και να ξεκινήσουν έρευνα ώστε να διαπιστώσουν πως έγιναν αντιληπτοί και να αλλάξουν τα εργαλεία ή τις μεθόδους που χρησιμοποιούσαν ως τώρα.

Για παράδειγμα, αν γίνει αντιληπτό ότι οι επιτιθέμενοι χρησιμοποιούν ένα HTTP web scanner όπως το Nikto, το οποίο χρησιμοποιεί τον ίδιο User-Agent όσο ψάχνει για web content ή αδυνα-

μίες, η Blue Team μπορεί να δημιουργήσει έναν κανόνα που μπλοκάρει κάθε δικτυακή κίνηση που προέρχεται από κάθε συσκευή με το συγκεκριμένο User-Agent. Αντίστοιχα, όταν οι αμυνόμενοι αναλύσουν ένα κακόβουλο αρχείο και εντοπίσουν συγκεκριμένο τρόπο ονομασίας των μεταβλητών που χρησιμοποίησαν οι προγραμματιστές αυτού του κακόβουλου προγράμματος, θα τους είναι εύκολο να αναλύσουν και άλλα αρχεία, τα οποία μπορεί να μην τα έχουν κατηγοριοποιήσει μέχρι τώρα ως κακόβουλα, αλλά επειδή οι μεταβλητές μέσα στο πρόγραμμα ακολουθούν την ίδια ξεχωριστή μορφή, να δημιουργήσουν την αναγκαία συσχέτιση. Και στις δύο περιπτώσεις οι επιτιθέμενοι θα πρέπει να ξοδέψουν χρόνο και κόπο για να αντιληφθούν αρχικά το πώς εντοπίστηκε η δραστηριότητά τους αλλά και στη συνέχεια να αλλάξουν τα στοιχεία τα οποία τους πρόδωσαν. Στην περίπτωση του User-Agent η αλλαγή σε διαφορετικό User-Agent είναι δύσκολη όμως το να αντιληφθούν οι επιτιθέμενοι ότι το συγκεκριμένο στοιχείο είναι αυτό που πρόδωσε τη δραστηριότητά τους μπορεί να τους πάρει μεγάλο χρονικό διάστημα. Αντίθετα, στην περίπτωση που τα ίδια μοτίβα για την ονομασία μεταβλητών στον πηγαίο κώδικα έχουν χρησιμοποιηθεί στην ανάπτυξη πολλαπλών διαφορετικών κακόβουλων αρχείων, θα ήταν εξαιρετικά χρονοβόρο για τους επιτιθέμενους να προβούν σε αλλαγές. Ένα IOC αυτής της κατηγορίας και τέτοιας σημαντικότητας θα ήταν εξαιρετικής σημασίας για την άμυνα του οργανισμού.

Tools

Στην κατηγορία των εργαλείων εντάσσονται όλα τα εργαλεία τα οποία μπορεί να χρησιμοποιεί ο επιτιθέμενος για να πετύχει το στόχο του. Αυτό αφορά κυρίως εργαλεία τα οποία χρησιμοποιούνται για πολύ συγκεκριμένο σκοπό σε διαφορετικά στάδια μιας επίθεσης. Ένα πολύ κοινό παράδειγμα είναι το Mimikatz. Το Mimikatz είναι ένα open-source εργαλείο με πολλές δυνατότητες και μια από αυτές επιτρέπει σε έναν επιτιθέμενο να ανακτήσει από τη μνήμη συστημάτων Windows κωδικούς χρηστών σε plaintext μορφή. Εδώ υπάρχει μία σημαντική διαφορά ανάμεσα στην κατηγορία IOC αρχείων και εργαλείων. Δεν θα είχε νόημα ο εντοπισμός της χρήσης του προγράμματος Mimikatz με βάση το hash του γιατί όπως αναφέρθηκε, θα ήταν πολύ εύκολο να αλλάξει. Ωστόσο η δημιουργία IOC που βασίζεται στον εντοπισμό της δραστηριότητας που προκύπτει έπειτα από τη χρήση ενός συγκεκριμένου προγράμματος, όπως του Mimikatz, είναι εξαιρετικής αξίας για την Blue Team γιατί μπορεί να δημιουργήσει πολύ μεγάλο πρόβλημα σε έναν επιτιθέμενο, διαταράσσοντας τις διαδικασίες που έχει συνηθίσει να ακολουθεί. Ο εντοπισμός της χρήσης ενός συγκεκριμένου εργαλείου που είναι σημαντικό για τους επιτιθέμενους θα τους αναγκάσει να επενδύσουν περισσότερο χρόνο για την έρευνα και τον εντοπισμό ενός εναλλακτικού εργαλείου με παρόμοιες δυνατότητες και στην περίπτωση που δεν υπάρχει να φτιάξουν το δικό τους. Δεν είναι όλοι οι επιτιθέμενοι το ίδιο εξελιγμένοι, συνεπώς αν ο επιτιθέμενος που στοχεύει τον οργανισμό δεν έχει την ικανότητα και την τεχνογνωσία να δημιουργήσει ένα δικό του εργαλείο που αντικαθιστά αυτό που είναι open-source και έχει μετατραπεί σε IOC, τότε μία επίθεσή του μπορεί να αποκλειστεί πετυχαίνοντας τον επιθυμητό στόχο για την Blue Team.

Tactics, Techniques, and Procedures

Η τελευταία κατηγορία του Pyramid of Pain είναι τα Tactics, Techniques και Procedures ενός επιτιθέμενου που αναφέρθηκαν και προηγουμένως, στο κεφάλαιο που αναλύθηκε το MITRE ATT&CK Framework. Τα TTPS είναι τα ιδιαίτερα χαρακτηριστικά του επιτιθέμενου που καθορίζουν τη συμπεριφορά του και τον τρόπο που ενεργεί. Τα Tactics είναι οι βασικοί στόχοι του όπως για παράδειγμα το να αποκτήσει initial access, ή να επιτύχει privilage escalation ή persistence. Τα Techniques περιγράφουν τις μεθόδους που χρησιμοποιεί για να επιτύχει ένα tactic και τέλος τα Procedures περιγράφουν την συγκεκριμένη υλοποίηση ενός Tactic. Όταν οι αμυνόμενοι προσπαθούν να εντοπίσουν TTPS δεν εστιάζουν στα εργαλεία ή στην υποδομή αλλά στην κατανόηση της συμπεριφοράς του επιτιθέμενου για τον οποίο είναι δύσκολο να επιτύχει το στόχο του με έναν εντελώς διαφορετικό τρόπο από αυτόν που γνωρίζει. Εντοπίζοντας τα TTPS, δηλαδή χαρτογραφώντας τον τρόπο λειτουργίας και συμπεριφοράς και μετατρέποντας τα σε IOCs, η Blue Team είναι σε θέση να επιτύχει τη μεγαλύτερη δυνατή διατάραξη στον επιτιθέμενο αλλά και να αυξήσει σημαντικά τις πιθανότητες εντοπισμού του. Αυτό συμβαίνει επειδή τον αναγκάζει να αλλάξει τον

τρόπο με τον οποίο λειτουργεί και να ξοδέψει περισσότερο χρόνο, κόπο και πόρους για να επιτύχει το ίδιο αποτέλεσμα αλλά με διαφορετικό τρόπο.

4.5 Μεθοδολογία Threat Hunting

Αφού λοιπόν έγινε αναφορά στο τι είναι το Threat Hunting, αλλά και στις διαφορές ανάμεσα στα IOCs σύμφωνα με την προσέγγιση του Pyramid of Pain, μπορούμε πλέον να αναλύσουμε σε βάθος και τα βασικά βήματα και τις διαδικασίες που ακολουθούνται για τη διεξαγωγή του Threat Hunting. Η μεθοδολογία που ακολουθείται στο Threat Hunting βασίζεται στην επιστημονική μέθοδο. Για να πραγματοποιηθεί δηλαδή το Threat Hunting, ο αναλυτής πρέπει να ορίσει μία υπόθεση βάση κάποιων δεδομένων που έχει συλλέξει και στη συνέχεια να προσπαθήσει να την επαληθεύσει μέσω αναζητήσεων που θα πραγματοποιήσει. Η επιτυχία του Threat Hunting αλλά και η ποιότητα των αποτελεσμάτων που θα επιφέρει εξαρτάται σε πολύ μεγάλο βαθμό από το πόσο εύστοχη και στοχευμένη θα είναι υπόθεση που θα ορίσει ο αναλυτής αλλά και το πόσο θα είναι εφικτό να επαληθευθεί [50].

Εικόνα 22. Διάγραμμα μεθοδολογίας Threat Hunting

1) Αναζήτηση του ερωτήματος

Το πρώτο στάδιο λοιπόν του Threat Hunting είναι η εύρεση της ερώτησης που θέλουμε να απαντηθεί μέσω αυτού. Αξιοποιώντας το MITRE ATT&CK Framework που περιγράφει τα διαφορετικά στάδια μιας επίθεσης είναι αρκετά εύκολο για τον Threat Hunter να επιλέξει μία από αυτές τις τακτικές και να προσπαθήσει να εντοπίσει αν κάτι τέτοιο συμβαίνει εντός του δικτύου. Το πρώτο λοιπόν στάδιο μπορεί να ακούγεται απλό και κάπως αφηρημένο, αλλά μπορεί να γίνει πολύ ειδικό και συγκεκριμένο αν τεθεί το κατάλληλο ερώτημα με την κατάλληλη μορφή. Για παράδειγμα, ένα ερώτημα που δεν είναι ιδανικό για αυτό το στάδιο θα είχε την εξής μορφή. - "Έχει κάποιος επιτιθέμενος παραβιάσει τον υπολογιστή ενός υπαλλήλου και κατάφερε να αποκτήσει δικαιώματα διαχειριστή;" Το ίδιο ερώτημα θα μπορούσε να εκφραστεί με διαφορετικό τρόπο σύμ-

φωνα με το MITRE ATT&CK Framework ώστε να βοηθήσει τον Threat Hunter να το διερευνήσει αποτελεσματικότερα και με μεγαλύτερη πιθανότητα επιτυχίας. - "Έχει καταφέρει κάποιος επιτιθέμενος να επιτύχει privilege escalation (tactic TA0004) στο X σύστημα μέσω της τεχνικής Abuse Elevation Control Mechanism (technique T1548) και πιο συγκεκριμένα μέσω Setuid και Setgid (subtechnique T1548.001);"

2) Έρευνα πηγών πληροφοριών

Μόλις η ερώτηση έχει τεθεί, επόμενο βήμα είναι η διενέργεια ενός background check για τα στοιχεία που θα χρειαστούν για την διεξαγωγή του Threat Hunting. Σε αυτό το στάδιο ο αναλυτής προσπαθεί να εντοπίσει ποιες είναι οι πηγές δεδομένων που θα πρέπει να έχει πρόσβαση αλλά και ποια εργαλεία θα χρειαστεί για να διεξάγει την έρευνα. Στην προκειμένη περίπτωση για τη διερεύνηση του παραδείγματος που τέθηκε παραπάνω, απαιτούνται αρχεία καταγραφής (logs) από το μηχάνημα στο οποίο πραγματοποιήθηκε το συγκεκριμένο συμβάν, τη συγκεκριμένη χρονική περίοδο. Αυτές οι πληροφορίες είναι διαθέσιμες τόσο μέσω του ίδιου του μηχανήματος όσο και από το SIEM. Χάριν ευκολίας το συγκεκριμένο παράδειγμα είναι απλό, αλλά στην περίπτωση πιο σύνθετων σεναρίων με πιο δύσκολες ερωτήσεις, το στάδιο αυτό μπορεί να αποδειχθεί χρονοβόρο και απαιτητικό διότι τα δεδομένα που χρειάζεται να συγκεντρωθούν μπορεί να προέρχονται από πολλαπλά διαφορετικά συστήματα ή να βρίσκονται σε μορφή που δεν είναι ανακτήσιμη η εύκολα προσβάσιμη. Επίσης πηγές πληροφορίας θα μπορούσε να είναι Threat Intel reports ή πληροφορίες από παρόμοια περιστατικά που έχουν συμβεί στον οργανισμό στο παρελθόν.

3) Δημιουργία ενός υποθετικού σεναρίου

Σε αυτό το στάδιο δημιουργείται μία υπόθεση η οποία μπορεί να επαληθευτεί και θα βοηθήσει τους αναλυτές να διαπιστώσουν αν το συγκεκριμένο σενάριο που βασίζεται στο MITRE ATT&CK Framwork εντοπίζεται εντός του δικτύου. Αυτή η υπόθεση θα μπορούσε να έχει την παρακάτω μορφή:

Σύμφωνα με ένα πρόσφατο Threat Intelligence report το οποίο λάβαμε από το τμήμα Threat Intel τμήμα του οργανισμού, ένας νέος Threat Actor που στοχεύει επιχειρήσεις στη βιομηχανία που δραστηριοποιείται ο οργανισμός μας, χρησιμοποιεί στοχευμένα και καλοσχεδιασμένα phishing mails ώστε να διαμοιράσει ένα άγνωστο μέχρι τώρα ransomware το οποίο δεν ανιχνεύεται απο τα automated security solutions. Σύμφωνα με τις πληροφορίες που έχουν συλλεχθεί, οι επιτιθέμενοι φαίνεται να χρησιμοποιούν την ίδια υποδομή που χρησιμοποιούσαν στο παρελθόν για να διαμοιράσουν άλλης μορφής ransomware. Μέσα στο report περιλαμβάνονται IOCs όπως διευθύνσεις IP και domain names. Αν κάποια από τις αναζητήσεις που θα πραγματοποιηθούν κατά τη διάρκεια του Threat Hunt επιστρέψουν κάποιους από αυτούς τους IOCs, τότε πιθανόν κάποιος από τους υπαλλήλους να έχει λάβει ένα αντίστοιχο phishing email και να έχει ήδη εκτελέσει το κακόβουλο εκτελέσιμο αρχείο. Αυτό το υποθετικό σενάριο στη συνέχεια μπορεί να μετατραπεί σύμφωνα με το MITRE ATT&CK Framework και το threat Intelligence report σε συγκεκριμένα TTPs που ακολουθεί ο επιτιθέμενος. Το MITRE ATT&CK Framework και σε αυτή την περίπτωση είναι εξαιρετικά χρήσιμο καθώς μαζί με κάθε τεχνική περιλαμβάνει και τους τρόπους εντοπισμού της.

4) Έλεγχος της υπόθεσης με αναζήτηση σχετικών δεδομένων

Σε αυτό το στάδιο είναι το σημείο που συμβαίνει πρακτικά το Thread Hunting καθώς η ομάδα που είναι υπεύθυνη για αυτό συλλέγει δεδομένα από διάφορες πηγές εντός του δικτύου όπως SIEM, Antivirus, IPS, EDR, προσπαθώντας να επαληθεύσει ή να καταρρίψει την υπόθεση που ορίστηκε. Τα δεδομένα τα οποία συλλέγονται θα πρέπει να σχετίζονται άμεσα με το αν το συγκεκριμένο γεγονός συμβαίνει ή όχι εντός του δικτύου και να μπορούν να παρέχουν αδιάσειστες αποδείξεις για αυτό.

5) Επεξεργασία και ανάλυση δεδομένων

Τα σχετικά δεδομένα που συλλέχθηκαν, δεν είναι αρκετά από μόνα τους για να επαληθεύσουν ή να καταρρίψουν την υπόθεση. Χρειάζονται περαιτέρω επεξεργασία και ανάλυση από τους αναλυτές ώστε να μπορέσουν να εξαχθούν χρήσιμα συμπεράσματα από αυτά που θα οδηγήσουν στην επαλήθευση ή την κατάρριψη της υπόθεσης.

6) Εξαγωγή συμπερασμάτων και επικοινωνία των αποτελεσμάτων

Βασιζόμενοι πάντα στα δεδομένα τα οποία συλλέχθηκαν και σχετίζονται με τη δραστηριότητα που έχει οριστεί στην υπόθεση, οι αναλυτές είναι σε θέση να επαληθεύσουν ή να διαψεύσουν την υπόθεση. Στην περίπτωση που η υπόθεση επαληθεύεται, ξεκινάει αμέσως η διαδικασία του Incident Response καθώς μέσω του Threat Hunting ανιχνεύθηκε μία πραγματική απειλή η οποία είχε περάσει απαρατήρητη. Από την άλλη πλευρά, αν η υπόθεση καταρριφθεί, τότε δεν έχει υπάρξει κάποια παραβίαση και η ομάδα του Threat Hunter μπορεί να επικοινωνήσει τα αποτελέσματα στα υπόλοιπα τμήματα του Blue Team και κυρίως στην ομάδα που ασχολείται με το Threat Intelligence. Πέρα από αυτά τα δύο σενάρια υπάρχει και το ενδεχόμενο η υπόθεση να μην ήταν σωστά διατυπωμένη και συνεπώς να μην ήταν εφικτό να εξεταστεί με απόλυτη βεβαιότητα. Σε αυτή την περίπτωση η ομάδα του Threat Hunt θα χρειαστεί να επαναδιατυπώσει την υπόθεση με διαφορετικό τρόπο ώστε να είναι επαληθεύσιμη ή όχι και να ξεκινήσει τη διαδικασία από την αρχή.

4.6 Σημασία και οφέλη διεξαγωγής

Έπειτα από την ανάλυση των βημάτων που απαιτούνται για τη διενέργεια ενός Threat Hunt βασισμένο στο MITRE ATT&CK Framework, μπορούμε να αντιληφθούμε και τα οφέλη τα οποία προσφέρει στην περίπτωση που ο οργανισμός επιθυμεί και είναι σε θέση να διενεργήσει proactive μεθόδους άμυνας.

Αρχικά, κατά αυτόν τον τρόπο ο οργανισμός είναι σε θέση να εντοπίσει εξελιγμένους επιτιθέμενους οι οποίοι έχουν παραβιάσει τα συστήματα του και μέχρι τώρα δεν έχουν γίνει αντιληπτοί είτε από τα αυτοματοποιημένα συστήματα είτε από τους αναλυτές του SOC. Αυτό δίνει τη δυνατότητα στον οργανισμό να μην ενεργεί με παθητικό τρόπο άμυνας αλλά να είναι σε θέση να εντοπίζει επιτιθέμενους σε ένα πολύ πιο αρχικό στάδιο σε σχέση με το όταν αυτοί θα είχαν καταφέρει να κάνουν μεγάλη ζημιά και βρίσκονταν σε ένα από τα τελευταία στάδια του Attack Chain που ήθελαν να ακολουθήσουν (Lateral Movement ή Exfiltration). Κατά αυτό τον τρόπο μειώνεται σε πολύ μεγάλο βαθμό και ο χρόνος που παραμένουν εντός του δικτύου χωρίς να έχουν εντοπιστεί (dwell time) μειώνοντας τις επιπτώσεις της παραβίασης στον οργανισμό. Για παράδειγμα μέσω του Threat Hunting μπορεί να εντοπιστεί μία επίθεση που είχε στόχο την εγκατάσταση Ransomware σε κρίσιμα υπολογιστικά συστήματα του οργανισμού αλλά, επειδή εντοπίστηκε σε αρχικό στάδιο, οι επιτιθέμενοι να μην πρόλαβαν να ολοκληρώσουν την επίθεσή τους. Συνεπώς η ζημιά θα είναι μικρότερη και η διαταραχή των επιχειρησιακών λειτουργιών του οργανισμού σαφώς μειωμένη.

Επιπλέον, διενεργώντας συχνά Theat Hunting, η Blue Team μπορεί να εντοπίσει κενά στο visibility των συστημάτων εντός του οργανισμού αλλά και να πραγματοποιεί συνεχή επαλήθευση για την ορθή λειτουργία συστημάτων ασφαλείας όπως του SIEM. Για παράδειγμα, αν κατά τη διάρκεια ενός Theat Hunt χρειαστούν logs από έναν Domain Controller που δεν έχει ρυθμιστεί ώστε να προωθεί τα αρχεία καταγραφής του στο SIEM, τότε αυτό το πρόβλημα μπορεί να διορθωθεί επιτόπου.

Κεφάλαιο 5

Adversary Emulation

5.1 Αντιμετώπιση APT group στη σύγχρονη εποχή

Στα προηγούμενα κεφάλαια αναλύσαμε το ρόλο και τα καθήκοντα της Blue Team, της Red Team αλλά και πώς αυτές οι δύο συνεργάζονται ώστε να μεγιστοποιηθεί η αποτελεσματικότητα τους άρα και η συνολική ικανότητα του οργανισμού να αμύνεται ενάντια σε εξελιγμένους επιτιθέμενους μέσω του Purple Teaming. Ένα ερώτημα που τίθεται σε αυτό το σημείο θα ήταν αν όλα αυτά είναι αρκετά για την αντιμετώπιση των εξελιγμένων επιτιθεμένων. Μια απόλυτη απάντηση σε αυτό το ερώτημα δεν θα ήταν ούτε εύκολο ούτε σκόπιμο να δοθεί καθώς εξαρτάται από πολλαπλούς παράγοντες όπως το πόσο εξελιγμένος θα ήταν ο επιτιθέμενος που θα στόχευε τον κάθε οργανισμό αλλά και τον βαθμό ωριμότητας της κυβερνοάμυνας του κάθε οργανισμού. Στην περίπτωση ενός πολύ εξελιγμένου επιτιθέμενου επιπέδου Advance Persistent Threat ή Nation State, η ύπαρξη μιας Blue team που συνεργάζεται αποτελεσματικά με την Red Team, ακόμα και με την αξιοποίηση μεθοδολογίας Purple Teaming, μπορεί να μην ήταν αρκετά για την αποτροπή μιας αντίστοιχης επίθεσης. Αυτό οφείλεται και στο γεγονός πως υπάρχουν τόσα πολλά διαφορετικά APT groups και Cyber Threat Actors που χρησιμοποιούν διαφορετικά Tactics, Techniques, και Procedures (TTPs) με διαφορετικά mondus operandi που είναι αδύνατο για έναν οργανισμό να είναι κατάλληλα προετοιμασμένος ενάντια σε όλες αυτές απειλές. Παρά το γεγονός λοιπόν ότι δεν θα ήταν εφικτό ένας οργανισμός να προετοιμαστεί για να αμυνθεί ενάντια σε όλους αυτούς τους εξελιγμένους επιτιθέμενους, δεν θα είχε και νόημα να σπαταλήσει τόσους πόρους σε μια αντίστοιχη προσπάθεια καθώς κάθε APT δεν θα στοχεύσει τους ίδιους οργανισμούς καθώς έχει διαφορετικά κίνητρα και στόχους.

Συνεπώς δεν υπάρχει όφελος στην προσπάθεια δημιουργίας ενός πλάνου άμυνας ενάντια σε οποιαδήποτε APT αλλά στην προετοιμασία ενάντια σε συγκεκριμένους CTA που σύμφωνα με δεδομένα που παρέχονται από το Cyber Threat Intelligence έχουν κριθεί ως πιο πιθανό να στοχεύσουν τον οργανισμό. Στην περίπτωσή που ένα τέτοιο ενδεχόμενο πραγματοποιηθεί, θα ήταν εξαιρετικά ωφέλιμο για τον οργανισμό να έχει δοκιμαστεί και να είναι έτοιμος για μια τέτοια επίθεση έχοντας δοκιμάσει ήδη τα TTP και το mondus perandi εναντίον του.

Σε αυτό το σημείο λοιπόν παρατηρούμε την ανάγκη για μετάβαση από πιο απλές δραστηριότητες που αναλύθηκαν σε προηγούμενα κεφάλαια, όπως το Vulnerability Assesment ή το Penetration Testing, στην έννοια του Adversary Emulation που θα αναλυθεί σε αυτό το κεφάλαιο.

5.2 SCYTHE Ethical Hacking Maturity Mode

Πριν γίνει αναφορά στο Adversary Emulation είναι χρήσιμη η αναφορά στο SCYTHE Ethical Hacking Maturity Model το οποίο κατηγοριοποιεί όλες τις δραστηριότητες που αναφέρθηκαν μέχρι τώρα με βάση την ωριμότητα που χρειάζεται να έχει ο οργανισμός για να τις αξιοποιήσει,

ξεκινώντας από την πιο απλή που είναι το Vulnerability Scanning και καταλήγοντας στην πιο σύνθετη που είναι το Adversary Emulation. Οι δραστηριότητες αυτές ακολουθούν μια γραμμική σειρά καθώς για παράδειγμα, είναι άσκοπη η πραγματοποίηση ενός Penetration Test αν πρώτα δεν έχουν πραγματοποιηθεί Vulnerability Scanning και Assesment όπως και είναι αδύνατο να διεξαχθεί ουσιαστικό και ποιοτικό Adversary Emulation αν πρώτα δεν έχουν προηγηθεί τα προηγούμενά στάδια [51].

Εικόνα 23. Scythe Ethical Hacking Maturity model
Πηγή εικόνας: https://www.scythe.io/library/scythes-ethical-hacking-maturity-model

Vulnerability Scanning: Το Vulnerability Scanning αφορά τη χρήση automated εργαλείων για τον εντοπισμό γνωστών αδυναμιών σε συστήματα του εκάστοτε οργανισμού. Η διαδικασία είναι συνήθως εντελώς αυτοματοποιημένη και χρειάζεται ελάχιστη ανθρώπινη παρέμβαση για την ολοκλήρωση της. Τα αποτελέσματα που παρέχει ενδέχεται να περιέχουν false positive και είναι η ελάχιστη δραστηριότητα που μπορεί να πραγματοποιεί ένας οργανισμός για τον εντοπισμό και την διόρθωση ευρέως γνωστών αδυναμιών.

Vulnerability Assessment: Αφού ένα Vulnerability Scan έχει ολοκληρωθεί, οι επαγγελματίες ασφαλείας μπορούν στη συνέχεια μέσω του Vulnerability Assessment να επαληθεύσουν τις αδυναμίες που εντοπίστηκαν και να αφαιρέσουν πιθανά false positives αποτελέσματα αλλά και να υπολογίσουν και να αξιολογήσουν τις αδυναμίες με βάση το ρίσκο τους ώστε να δρομολογηθεί η διόρθωση τους με αντίστοιχη προτεραιότητα.

Penetration Testing: Σε αντίθεση με το Vulnerability Assessment, το Penetration Testing δεν μπορεί να πραγματοποιηθεί με αυτοματοποιημένα εργαλεία καθώς περιλαμβάνει χειροκίνητες δοκιμές για τον εντοπισμό όσο το δυνατόν περισσότερων αδυναμιών. Οι αδυναμίες σε αυτή την περίπτωση μπορεί να είναι και άγνωστες μέχρι τώρα και ο στόχος είναι η εκμετάλλευσή τους για την καλύτερη κατανόηση της ζημιάς που θα μπορούσε να προκληθεί, εάν οι ίδιες ενέργειες πραγματοποιούνταν από έναν πραγματικό επιτιθέμενο. Η βασική διαφορά στο Penetration Testing είναι ότι οι αδυναμίες πού εντοπίζονται, γνωστές ή μη, αξιοποιούνται στην πράξη και πολλές φορές συνδυάζονται μεταξύ τους ώστε να αναδειχθεί η επίπτωση της εκμετάλλευσης τους.

Red Team Engagements: Τα Red Team Engagements είναι ολοκληρωμένες επιθέσεις που βασίζονται σε σενάρια και καθοδηγούνται από συγκεκριμένους στόχους ώστε να αξιολογήσουν την συνολική ετοιμότητα του οργανισμού και κυρίως της Blue Team σε μια ρεαλιστική επίθεση. Τα Red Team Engagements διαφέρουν από το Penetration Testing καθώς δεν εστιάζουν στον εντοπισμό όσο το δυνατόν περισσότερων αδυναμιών υπάρχουν σε ένα σύστημα, αλλά επικεντρώνονται στην επίτευξη ενός συγκεκριμένου στόχου, αξιοποιώντας οποιαδήποτε αδυναμία είναι διαθέσιμη. Επιπλέον, είναι ολοκληρωμένες επιθέσεις που δεν εστιάζουν μόνο σε ένα σύστημα και αποκλειστικά στην τεχνική του πλευρά αλλά περιλαμβάνουν δοκιμές ενάντια σε διαδικασίες, τεχνολογίες ακόμα και ανθρώπους και φυσικές υποδομές όπως κτήρια. Τέλος σε αντίθεση με το Penetration Testing αξιοποιούν Tactics, Techniques, και Procedures (TTPs).

Purple Team Exercises: Στο Purple teaming ο στόχος είναι η επίτευξη της αποτελεσματικής συνεργασίας ανάμεσα στη Red Team και την Blue Team σε μία ανοιχτή άσκηση όπου οι λεπτομέρειες της δραστηριότητας της Red team αποκαλύπτονται πλήρως στην Blue Team με στόχο την καλύτερη κατανόηση των μεθόδων που χρησιμοποίησε και την δημιουργία των αντίστοιχων μηχανισμών εντοπισμού από την Blue Team. Οι ασκήσεις Purple Team βασίζονται σε μεγάλο βαθμό σε πληροφορίες που προέρχονται από Cyber Threat Intelligence και περιλαμβάνουν όπως και στο Red Teaming τα Tactics, Techniques, και Procedures (TTPs) επιτιθεμένων αλλά με τη διαφορά ότι

εστιάζουν σε ευρέως γνωστούς CTA και APT Groups με στόχο την συνεργασία των δύο ομάδων για τη δημιουργία αποτελεσματικότερων μηχανισμών εντοπισμού.

Adversary Emulation: Στο τελευταίο στάδιο του Scythe Ethical Hacking Maturity model βρίσκεται το Adversary Emulation, η πιο εξελιγμένη δραστηριότητα σε αυτό το μοντέλο, που αφορά οργανισμούς που έχουν ολοκληρώσει στο παρελθόν τις προηγούμενες δραστηριότητες. Στο επόμενα υποκεφάλαια θα δοθεί ο ορισμός του Adversary Emulation, θα παρουσιαστούν τα στοιχεία που το διαφοροποιούν ανάμεσα σε άλλες δραστηριότητες όπως το Red Teaming/Purple Teaming, θα γίνει αναφορά στις προκλήσεις κατά την προσπάθεια αξιοποίησης του, στα οφέλη που προκύπτουν από την αξιοποίηση του αλλά και στη σημαντική διαφορά ανάμεσα στους όρους Emulation και Simulation.

5.3 Ορισμός Adversary Emulation

Το Adversary Emulation είναι ένας ειδικός τύπος Red Team engagement που μιμείται ένα γνωστό Threat Actor ή APT group συνδυάζοντας πηγές Threat Intelligence που βασίζονται σε Frameworks όπως το MITRE ATT&CK με στόχο τη χρήση των συγκεκριμένων tactics, techniques και procedures (TTPs) που θα χρησιμοποιούσε ο πραγματικός επιτιθέμενος ενάντια στον οργανισμό. Κατά αυτόν τον τρόπο η Red Team θα προσπαθεί να επιτύχει τους στόχους της αλλά ενεργώντας όπως θα ενεργούσε ο συγκεκριμένος επιτιθέμενος. Δεδομένου του ότι το MITRE ATT&CK Framework περιέχει ένα τεράστιο όγκο πληροφοριών από TTPs γνωστών APT group, είναι ιδανικό για χρήση σε Adversary Emulation engagements [36, 52].

Η βασική διαφορά ανάμεσα στο τυπικό Red Teaming με το Adversary Emulation είναι πως στο τυπικό Red Teaming ο βασικός σκοπός είναι η επίτευξη συγκεκριμένων στόχων, όπως για παράδειγμα να αποκτηθεί πρόσβαση σε ένα συγκεκριμένο σύστημα εντός του οργανισμού, ενώ στο Adversary Emulation ο βασικός σκοπός είναι η προσομοίωση ενός συγκεκριμένου Threat Actor με τα TTPs που χρησιμοποιεί για την επίτευξη του ίδιου στόχου [53].

Είναι προφανές πως με τόσους διαφορετικούς Threat Actors και APT groups, είναι αδύνατο ένας οργανισμός να είναι κατάλληλα προετοιμασμένος για όλους και να έχει μηχανισμούς εντοπισμού για όλα τα TTPs κάθε επιτιθέμενου. Συνεπώς μέσω του Threat Intelligence ο οργανισμός μπορεί να εντοπίσει τα APT groups που στοχεύουν οργανισμούς σε ίδιο κλάδο/βιομηχανία και έχουν το κίνητρο και την ικανότητα άρα και είναι πιο πιθανό να στοχεύσουν τον οργανισμό. Με αυτήν την πληροφορία και σε συνδυασμό με το Adversary Emulation, η red team έχει τη δυνατότητα να προσομοιώσει μια επίθεση σύμφωνα με τα TTPs του συγκεκριμένου APT group προετοιμάζοντας τον οργανισμό για ένα τέτοιο ενδεχόμενο.

Σημαντική λεπτομέρεια αποτελεί το γεγονός πως ένας οργανισμός μπορεί να παραβιαστεί από ένα τυπικό Red Team engagement το οποίο αξιοποίησε μια ad-hoc προσέγγιση για την επίτευξη του στόχου ενώ αν είχε στοχευθεί από ένα συγκεκριμένο APT group, το οποίο προηγουμένως είχε διεξάγει μια άσκηση Adversary Emualtion που προσημείωνε τα TTPs του, με σκοπό να δοκιμάσει και να βελτιώσεις τις ικανότητες εντοπισμού του, τότε θα ήταν πολύ πιθανό να κατάφερνε να εντοπίσει την επίθεση σε αρχικό στάδιο άρα και να την περιόριζε έγκαιρα. Επιπλέον το Adversary Emulation συχνά θεωρείται αποκλειστικά ως μια Red Team δραστηριότητα αλλά στην πραγματικότητα αποτελεί ένα αναπόσπαστο και σημαντικό μέρος και της διαδικασίας του Threat Hunting. Μέσω του Adversary Emulation και προσομοιώνοντας την δραστηριότητα και τα TTPs ενός Threat Actor η Blue Team έχει τη δυνατότητα να συλλέξει όσο το δυνατόν περισσότερα δεδομένα μπορεί και να προσπαθεί να εντοπίσει τη δραστηριότητα μέσω του Threat Hunting. Απώτερος στόχος άλλωστε του Adversary Emulation είναι η βελτίωση της άμυνας του οργανισμού ενάντια σε εξελιγμένους επιτιθέμενους μέσω της αξιολόγηση της ικανότητας του Blue Team να εντοπίζει και να περιορίζει αντίστοιχες επιθέσεις αλλά και της δημιουργίας αποτελεσματικότερων μηχανισμών εντοπισμού με μεγαλύτερη κάλυψη.

Τέλος, τα Adversary Emulation engagements μπορούν να πραγματοποιηθούν χωρίς η Blue Team να γνωρίζει τις λεπτομέρειες της άσκησης, ώστε να δοκιμαστεί η ετοιμότητά της ενάντια σε συγκεκριμένο APT group αλλά με διαφάνεια και συνεργασία ανάμεσα στις δύο ομάδες (Blue/Red), ως ένα Purple Team engagement. Στο επόμενο υποκεφάλαιο γίνεται αναφορά σε αυτές τις διαφοροποιήσεις ώστε να γίνουν πιο κατανοητές οι διάφορές τους, να αναδειχθεί η αξία της κάθε μιας άλλα και να καθοριστεί σε ποια διαφοροποίηση εστιάζει η εργασία.

5.4 Διαφορές ανάμεσα σε Adversary Emulation και Simulation

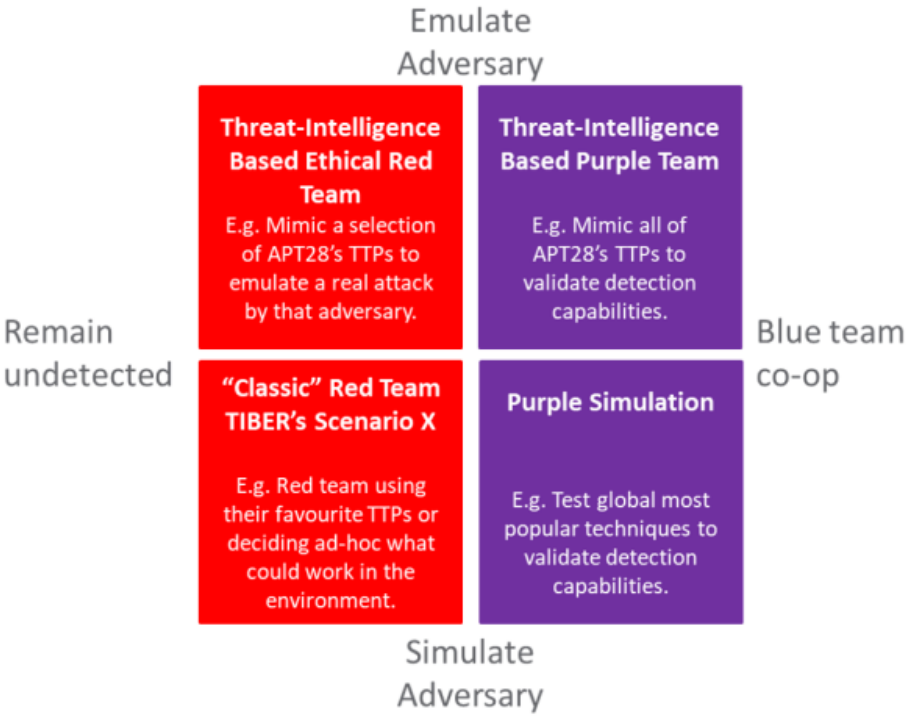
Ενώ οι έννοιες Emulation και Simulation ακούγονται παρόμοιες, υπάρχει διαφοροποίηση ανάμεσα τους η οποία είναι ιδιαίτερα σημαντική καθώς καθορίζει τον τρόπο διεξαγωγής των engagements αλλά και των επιδιωκόμενων αποτελεσμάτων τους. [54]

Ο όρος Emulate χρησιμοποιείται για την περιγραφή ενός συστήματος που έχει σχεδιαστεί έτσι ώστε να συμπεριφέρεται και λειτουργεί με τον ίδιο τρόπο που θα συμπεριφερόταν ένα άλλο. Για παράδειγμα, στην επιστήμη της πληροφορικής, ένας Emulator είναι το hardware ή το software που επιτρέπει σε ένα σύστημα να συμπεριφέρεται όπως ένα άλλο, όπως ένα Android Emulator που εκτελείται σε περιβάλλον Windows, αλλά επιτρέπει στους χρήστες να εκτελούν εφαρμογές που προορίζονται για κινητές συσκευές Android.

Από την άλλη πλευρά ο όρος Simulate χρησιμοποιείται για την περιγραφή ενός συστήματος που δεν είναι πραγματικό αλλά συμπεριφέρεται ή λειτουργεί σαν να είναι πραγματικό. Για παράδειγμα είναι πολύ συχνό κατά τα πρώτα στάδια της εκπαίδευσης ενός πιλότου να γίνεται χρήση ενός συστήματος Flight Simulator (προσομοιωτής πτήσης). Έτσι οι πιλότοι έχουν την ευκαιρία να εκπαιδευτούν σε ένα σύστημα που λειτουργεί και συμπεριφέρεται όπως ένα πραγματικό αεροσκάφος χωρίς ωστόσο να διατρέχουν τον παραμικρό κίνδυνο λόγω της απειρίας τους.

Συνεπώς ο όρος Adversary Emulation αφορά τη δραστηριότητα όπου η Red Team μιμείται τη συμπεριφορά ενός APT αξιοποιώντας τα ίδια TTPs για την πραγματοποίηση μιας επίθεσης. Από την άλλη πλευρά ο όρος Adversary Simulation χρησιμοποιείται όταν η Red Team αντιγράφει τη συμπεριφορά και τις ενέργειες του APT group με τη μέγιστη δυνατή ακρίβεια. Αυτό θα μπορούσε να είναι η ακριβής επανάληψη των TTPs του APT με τα ίδια ακριβώς εργαλεία και μεθόδους που είχαν χρησιμοποιηθεί σε μια πραγματική επίθεση. Σε ένα Adversary Emulation engagement η Red Team μπορεί να χρησιμοποιήσει δικά της custom-made εργαλεία για να πετύχει τα ίδια TTPs αλλά με διαφορετικό τρόπο από αυτό που θα χρησιμοποιούσε το συγκεκριμένο APT group που θα έκανε emulate. Αντιθέτως στο Adversary Simulation, στην περίπτωση που το engagement δεν εστιάζει σε συγκεκριμένο APT group τότε ο στόχος είναι να φανεί ότι συμβαίνει μια πραγματική επίθεση ενώ δεν υπάρχει πραγματικός επιτιθέμενος, επομένως είναι πιο κοντά στη λογική του τυπικού Red Team engagement και μπορούν να χρησιμοποιηθούν τα πιο κοινά TTPs για λόγους ευκολίας. Σε περίπτωση που το Adversary Simulation engagement εστιάζει σε συγκεκριμένο APT group, τότε γίνεται προσπάθεια για την ακριβή επανάληψη των TTPs του συγκεκριμένου APT group με τα ίδια ακριβώς εργαλεία και μεθόδους που είχαν χρησιμοποιηθεί σε μια πραγματική επίθεση σύμφωνα με διαθέσιμες πληροφορίες απο Threat Intelligence reports και άλλων resources.

Ο διαφορές που αναφέρθηκαν παραπάνω μπορούν να γίνουν πιο κατανοητές μέσω του παρακάτω σχεδιαγράμματος.



Εικόνα 24. Διαφορές ανάμεσα σε Emulation/Simulation, Red/Purple Teaming
Πηγή εικόνας: https://blog.nviso.eu/2020/01/23/thoughts-on-red-team-nomenclature/

Η εργασία αυτή εστιάζει στην βελτίωση της ικανότητας του οργανισμού να εντοπίζει εξελιγμένους επιτιθέμενους και όχι στην αξιολόγηση της Blue Team, συνεπώς εμπίπτει στο δεξί μέρος του σχεδιαγράμματος καθώς απαιτείται η ενεργή συμμετοχή και συνεργασία της Blue Team με τη Red Team αξιοποιώντας Purple Team μεθοδολογία. Ανάλογα με τις ανάγκες, τη στρατηγική αλλά και την ωριμότητα του κάθε οργανισμού, είναι εφικτό να πραγματοποιηθούν engagements και υπό τη μορφή του Emulation αλλά και του Simulation. Ωστόσο η παρούσα εργασία εστιάζει στο Emulation ενός συγκεκριμένου APT group, συνεπώς εμπίπτει στην κατηγορία του Threat-Intelligence Based Purple Team Engagement (Emulate Adversay με Blue Team co-op).

5.5 Προκλήσεις

Το Adversary Emulation είναι μία εξαιρετικά χρήσιμη δραστηριότητα για τους οργανισμούς που είναι πιθανόν να δεχθούν επίθεση από εξελιγμένους επιτιθέμενους αλλά από την άλλη είναι και αρκετά δύσκολο να οργανωθεί και να πραγματοποιηθεί διότι απαιτεί τη συνεργασία διαφορετικών ομάδων εντός του οργανισμού και αρκετή προεργασία.

Αρχικά δεν υπάρχουν πάντα διαθέσιμες και πρόσφατες πληροφορίες για όλους τους εξελιγμένους επιτιθέμενους υπό τη μορφή ενός Theat Intelligence Report το οποίο κάνει αντιστοίχηση των μεθόδων που χρησιμοποιούν οι επιτιθέμενοι πάνω σε Frameworks όπως το MITRE ATT&CK. Παρά το γεγονός ότι το MITRE ATT&CK Framework περιέχει παραπάνω από 130 διαφορετικά APT groups είναι ότι προφανές δεν είναι τα μοναδικά που υπάρχουν και είναι ενεργά ανά τον κόσμο. Επιπλέον πολλές από τις δραστηριότητες που θα ακολουθήσει ένας εξελιγμένος επιτιθέμενος σε μία πραγματική επίθεση ενάντια σε έναν οργανισμό δεν είναι πάντα εύκολο η και νόμιμο να αναπαραχθούν από μία Red team. Για παράδειγμα μία επίθεση μπορεί να βασίζεται σε ένα Supply Chain Attack ή στην παραβίαση μιας υποδομής που δεν ανήκει στον οργανισμό αλλά σε κάποιον τρίτο. Ένα άλλο παράδειγμα θα μπορούσε να είναι άλλες μη ηθικές, ανορθόδοξες ή και παράνο-

μες δραστηριότητες που σαφώς οι επαγγελματίες ασφαλείας που είναι μέρος της Red Team δεν θα μπορούσαν σε καμιά περίπτωση να πραγματοποιήσουν. Συνεπώς η δραστηριότητα ενός APT Group, ακόμα και πλήρως χαρτογραφημένη να είναι πάνω σε ένα Framework χάρη σε ένα πρόσφατο Thread Intelligence report, δεν είναι πάντα εύκολο να αναπαραχθεί πλήρως στο πλαίσιο μιας άσκησης.

Επιπλέον, όπως οι Blue Teams εξελίσσονται διαρκώς για να βελτιώνουν τις ικανότητες εντοπισμού τους, έτσι και οι επιτιθέμενοι αλλάζουν, μετασχηματίζουν και βελτιώνουν διαρκώς τις μεθόδους και τις τεχνικές που χρησιμοποιούν αλλά και τα TTPs τους ώστε να παραμένουν ικανοί να πραγματοποιούν επιτυχημένες επιθέσεις. Για παράδειγμα, ένας εξελιγμένος επιτιθέμενος μπορεί να χρησιμοποιήσει μία αδυναμία 0-day σε μία επίθεση και μετά να μην την χρησιμοποιήσει ξανά εφόσον θα έχει γίνει γνωστή και θα έχει διορθωθεί. Συνεπώς η αναπαραγωγή της συγκεκριμένης αδυναμίας με ακρίβεια σε μία άσκηση δεν θα είχε τόσο μεγάλο όφελος για την Blue Team σε επίπεδο βελτίωσης των ικανοτήτων εντοπισμού εξελιγμένων επιτιθέμενων. Για αυτό άλλωστε είναι σημαντικό το Adversary Emulation να βασίζεται πάντα στα TTPs που σύμφωνα και με την Pyramid Of Pain είναι πιο δύσκολο ένας επιτιθέμενος να αλλάξει και όχι υπό άλλης μορφής IOCs που βρίσκονται πιο χαμηλά στην ιεραρχία της πυραμίδας, άρα έχουν και χαμηλότερη αξία για την Blue Team καθώς μπορούν να αλλαχθούν πιο εύκολα από τον επιτιθέμενο.

Τέλος, το γεγονός ότι το Adversary Emulation είναι μία δύσκολη διαδικασία δεν σημαίνει ότι δεν αξίζει να πραγματοποιείτε από τους οργανισμούς στην περίπτωση που έχουν φτάσει στο επίπεδο ωριμότητας όπου να μπορούν να το διεξάγουν σύμφωνα με το Scythe Ethical Hacking maturity model που παρουσιάστηκε σε προηγούμενο κεφάλαιο.

5.6 Σημασία και οφέλη διεξαγωγής

Εφόσον έγινε αναφορά στο τι είναι Adversary Emulation, στις διαφορετικές του κατηγορίες αλλά και στις προκλήσεις που υπάρχουν κατά τη πραγματοποίησή του, αξίζει να αναφερθούν και τα οφέλη και να αναδειχθεί η σημασία διεξαγωγής του.

1) Βελτιώνει την επικοινωνία ανάμεσα σε Blue και Red Team

Δεδομένου του ότι ένα Adversary Emulation engagement απαιτεί τη συμμετοχή και της Blue Team και της Red Team, είναι ένας τρόπος και μια αφορμή να βελτιωθεί η επικοινωνία και η συνεργασία ανάμεσα στις δύο ομάδες. Μέσω της ανταλλαγής γνώσης αλλά και της καλύτερης επικοινωνίας των δύο ομάδων, ο οργανισμός βελτιώνει σημαντικά την ικανότητα του να αμύνεται ενάντια σε πραγματικούς και εξελιγμένους επιτιθέμενους.

2) Επαλήθευση ορατότητας

Είναι σύνηθες φαινόμενο αρκετά από τα συστήματα του οργανισμού να μην είναι ορατά από τα Security Solutions και να αποτελούν τα λεγόμενα "τυφλά σημεία" (Blind Spots). Αυτό μπορεί να οφείλεται σε ένα πρόβλημα τεχνικής φύσεως που δεν έγινε ποτέ αντιληπτό ή σε ανθρώπινο λάθος. Είναι προφανές πως ένα σύστημα για το οποίο δεν υπάρχει Visitibily από τα Secuirty Solutions του οργανισμού είναι αυτομάτως πιο ευάλωτο και εκτεθειμένο στους επιτιθέμενους, εφόσον η παραβίασή του δεν είναι εφικτό να γίνει αντιληπτή, μπορεί να οδηγήσει σε ένα πιο σοβαρό περιστατικό ασφαλείας. Μέσω του Adversary Emulation η Blue Team μπορεί να διαπιστώσει από ποια σημεία στις υποδομές του δεν λαμβάνονται καθόλου ή ικανοποιητικά αρχεία καταγραφής (logs). Έτσι είναι πιο εύκολο να δοθεί προτεραιότητα σε αυτά και ταυτόχρονα να μετρηθεί αξιόπιστα η βελτίωση του Visitibility σε βάθος χρόνου.

3) Δημιουργία αποτελεσματικότερων μεθόδων εντοπισμού (Threat Detection Engineering)

Η δραστηριότητα του Threat Detection Engineering περιλαμβάνει την ικανότητα της Blue Team όχι απλά να φτιάχνει ένα κανόνα εντοπισμού μιας επίθεσης στο SIEM ή σε ένα άλλο Security Solution αλλά να ερμηνεύει και να μοντελοποιεί απειλές για την παροχή σύγχρονων και αποτελεσματικών μεθόδων ανίχνευσης σύνθετων απειλών. Μέσω του Adversary Emulation οι οργανισμοί μπορούν παράγουν τα απαραίτητα δεδομένα που χρειάζονται ώστε να διαπιστώσουν ποια TTPs

ενός επιτιθέμενους δεν είναι σε θέση να εντοπίσουν, να επαληθεύσουν πως οι μέθοδοι εντοπισμού που έχουν υλοποιήσει πράγματι λειτουργούν όπως θα έπρεπε και να δημιουργήσουν νέους μηχανισμούς εντοπισμού που θα βασίζονται σε πραγματικά δεδομένα.

4) Συνεχής αξιολόγηση και επαλήθευση μεθόδων και τεχνικών εντοπισμού

Μέσω του Adversary Emulation η Blue Team μπορεί ανά πάσα στιγμή να δοκιμάσει αν ένας μηχανισμός εντοπισμού λειτουργεί όπως έχει σχεδιαστεί. Ένας μηχανισμός εντοπισμού μπορεί να φαίνεται ότι έχει σχεδιαστεί σωστά και να είναι αναμενόμενο να λειτουργεί αλλά πολλές φορές μπορεί να επηρεαστεί από αλλαγές που θα συμβούν σε ένα από τα συστήματα που λαμβάνει δεδομένα και να πάψει λειτουργεί. Συνεπώς υπάρχει το ενδεχόμενο στη περίπτωση μιας πραγματικής επίθεσης να μην λειτουργήσουν με τον αναμενόμενο τρόπο εκθέτοντας σε κίνδυνο τον οργανισμό.

5) Καλύτερη προετοιμασία από υπαρκτά APT groups

Μέσω του Adversary Emulation ο οργανισμός μπορεί να αξιολογήσει την ικανότητα του να αντιμετωπίσει έναν πραγματικό επιτιθέμενο και όχι μια Red Team που θα χρησιμοποιούσε ad-hoc μεθόδους ή τεχνικές για να πετύχει το στόχο της. Αξιοποιώντας εργαλεία για Adversary Emulation που επιτρέπουν την διεξαγωγή επιθέσεων που βασίζονται στα TTPs πραγματικών Threat Actor και APT group είναι εφικτή η προσομοίωση μιας πραγματικής επίθεσης από συγκεκριμένο APT group και η αξιολόγηση της ικανότητας της Blue Team να ανταποκρίνεται σε αυτό.

5.7 Πλάνα Adversary Emulation

5.7.1 Ορισμός

Για την ανάδειξη της πρακτικής χρήσης και αξίας του MITRE ATT&CK Framework τόσο για τις Blue όσο και για τις Red Teams, η MITRE Corporation δημιούργησε τα Adversary Emulation Plans. Τα Adversary Emulation Plans (AEPs) είναι λεπτομερείς αναφορές που αποτελούν ένα παράδειγμα του τι μπορεί να δημιουργηθεί συνδυάζοντας και αξιοποιώντας cyber threat reports και το MITRE ATT&CK Framework για τη χαρτογράφηση ενός Cyber Threat Actor. Κάθε AEP έχει βασιστεί σε πραγματικά Threat Intelligence reports που περιγράφουν σε βάθος επιθέσεις που έχει πραγματοποιήσει ο Threat Actor στο παρελθόν, εστιάζοντας όχι μόνο στο τι ενέργειες πραγματοποίησε αλλά και σε ποιο στάδιο της επίθεσης και με ποιο τρόπο [55].

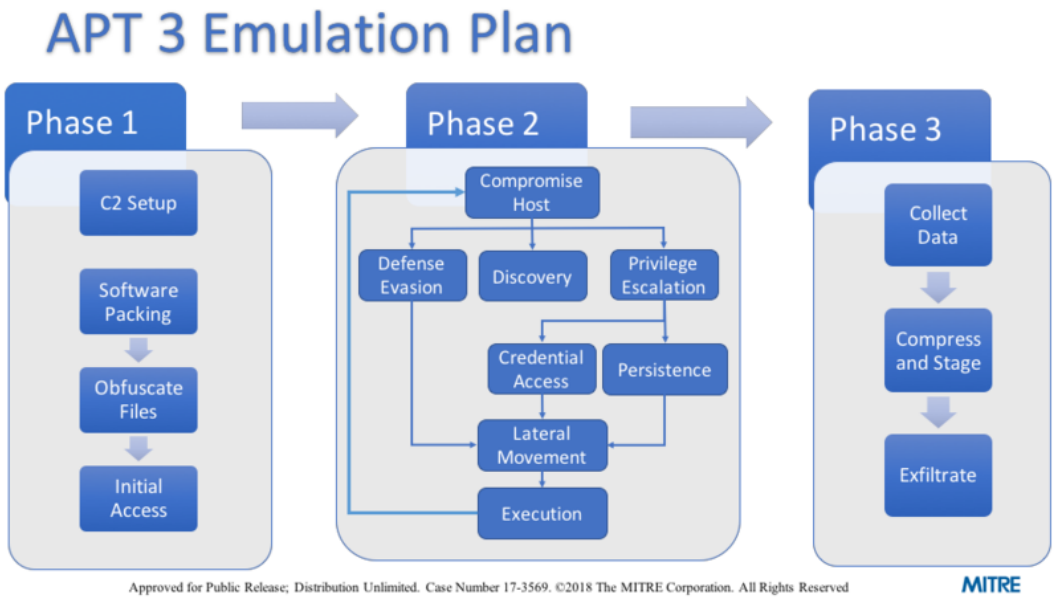
Ο σκοπός των Adversary Emulation Plans είναι να δώσουν τη δυνατότητα στις Blue Teams να αξιολογήσουν αποτελεσματικότερα τους μηχανισμούς εντοπισμού τους, παρέχοντας τις απαραίτητες πληροφορίες στις Red Teams ώστε να πραγματοποιήσουν ένα όσο το δυνατόν πιο ρεαλιστικό Adversary Emulation ενός συγκεκριμένου APT group. Τα Adversary Emulation Plans αποτελούν ένα μέρος μιας μεγαλύτερης προσπάθειας μετάβασης απο reactive σε proactive defense και την εστίαση σε υψηλότερης αξίας IoCs όπως τα TTPs σε αντίθεση με hash values, IP addresses ή συγκεκριμένα εργαλεία.

Για παράδειγμα η MITRE έχει αναπτύξει το AEP για το APT3 group για να παρουσιάσει πώς οι ενέργειές του μπορούν να μοντελοποιηθούν σε ένα AEP.

Table of Contents

Εικόνα 25. Περιεχόμενα APT3 Emulation Plan
Πηγή εικόνας: https://attack.mitre.org/resources/adversary-emulation-plans/

Ένα από τα πιο κρίσιμα στοιχεία ενός AEP είναι η ενότητα με τα Emulation Phases. Τα Emulation Phases περιλαμβάνουν μια λεπτομερή ανάλυση των τακτικών που χρησιμοποιεί το Adversary group.



Εικόνα 26. APT3 Emulation Phases
Πηγή εικόνας: https://attack.mitre.org/resources/adversary-emulation-plans/

Τέλος, το Adversary Emulation Field Manual περιλαμβάνει τις ίδιες τις εντολές που χρησιμοποίησε το APT group ή εντολές που έχουν παρόμοιο αποτέλεσμα για τη διεξαγωγή κάθε Technique που περιλαμβάνεται μέσα στο Emulation Plan. Στην προκειμένη περίπτωση οι εντολές παρέχονται τόσο σε Native Windows μορφή όσο και σε δημορφιλή Adversary Emulation Frameworks, όπως το Cobalt Strike και το Metasploit.

	A	B	C	D	E
1		Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved			
2	**Category**	**Built-in Windows Command**	**Cobalt Strike**	**Metasploit**	**Description**
3	**Discovery**				
4	**T1082**	ver	shell ver		Get the Windows OS version that's running
5	**T1082**	set	shell set	get_env.rb	Print all of the environment variables
6	**T1033**	whoami /all /fo list	shell whoami /all /fo list	getuid	Get current user information, SID, domain, groups the user belongs to, security privs of the user
7	**T1082**	net config workstation net config server	shell net config workstation shell net config server		Get computer name, username, OS software version, domain information, DNS, logon domain
8	**T1016**	ipconfig /all	shell ipconfig	ipconfig post/windows/gather/enum_domains	Get information about the domain, network adapters, DNS / WSUS servers
9	**T1082**	systeminfo [/s COMPNAME] [/u DOMAIN\user] [/p password]	systemprofiler tool if no access yet (victim browses to website) or shell systeminfo (if you already have a beacon)	sysinfo, run winenum, get_env.rb	Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties, such as RAM, disk space, and network cards
10	**T1012**	reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections	shell reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections	reg queryval -k "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" -v fDenyTSConnections post/windows/gather/enum_termserv	Check for the current registry value for terminal services, if it's 0, then terminal services are enabled. If it's 1, then they're disabled
11	**T1016**	arp -a route print	shell arp -a	route	Display the ARP table
12	**T1049**	netstat -ano[b]	shell c:\windows\sysnative\netstat.exe -ano[b]	post/windows/gather/tcpnetstat	Display current TCP/IP network connections (b requires elevated privs so you can see the process that opened the connection)
13	**T1057**	tasklist /v [/svc] net start qprocess *	ps shell tasklist /v [/svc] shell net start	ps post/windows/gather/enum_services	Display list of currently running processes and services on the system
14	**T1069**	net localgroup "Administrators"	shell net localgroup "Administrators"	post/windows/gather/local_admin_search_enum	Display the list of local administrator accounts on the workstation
15	**T1069**	net group ["Domain Admins"] /domain[DOMAIN]	net group ["Domain Admins"] /domain	domain_list_gen.rb post/windows/gather/enum_domain_group_users	Display the list of domain administrator accounts
16	**T1087**	net user [username] [/domain]	shell net user [username] [/domain]	post/windows/gather/enum_ad_users auxiliary/scanner/smb/smb_enumusers	Used to add, delete, and manage the users on the computer. Run this command on the users discovered from the previous two commands to gather more information on targeted users.
17	**T1018**	net group "Domain Computers" /domain[DOMAIN]	net group "Domain Computers" /domain	post/windows/gather/enum_ad_computers post/windows/gather/enum_computers	Display the list of domain computers in the domain by showing their computer accounts (COMP_NAME$)
18	**T1018**	net group "Domain Controllers" /domain[DOMAIN]	net group "Domain Controllers" /domain		Display the list of domain controllers in the network
		net use [\\ip\path] [password] [/user:DOMAIN\user] net use \\COMP\ADMIN$ password /user:COMP\Administrator (checking password			Used to view network shared resource information, add a new network resource, and remove an old network resource from the computer. Run this against computers discovered from the

Εικόνα 27. APT3 Emulation Commands
Πηγή εικόνας: https://attack.mitre.org/resources/adversary-emulation-plans/

5.7.2 Έτοιμα Community Emulation Plans

Πολλά έτοιμα Emulation Plans υπάρχουν διαθέσιμα σε αποθετήρια όπως το Scythe Community Threats ή το Adversary Emulation Library που φιλοξενούνται στον GitHub. Ο σχεδιασμός ενός Emulation Plan είναι μία απαιτητική και χρονοβόρα διαδικασία συνεπώς η αξιοποίηση έτοιμων Emulation Plan είναι ιδιαίτερα χρήσιμη [56, 57]. Τα repositories εμπλουτίζονται διαρκώς με νέα APT Groups και αποτελούν μία πολύ χρήσιμη πηγή πληροφορίας που διευκολύνει σε μεγάλο βαθμό τη διεξαγωγή ενός Adversary EMulation σε συγκεκριμένο APT group.

APT19	Create README (#53)	12 months ago
APT33	Update APT33v2	8 months ago
APT35	Add files via upload (#81)	3 months ago
APT41	Updated README.md	4 days ago
BazarLoader	Change scythe.phollowing	17 days ago
BerserkBear	Create README.md (#61)	12 months ago
BoratRAT	Audio.dll cleanup (#91)	18 days ago
Buhtrap	Organized	2 years ago
Conti	Create Conti_VECTR_Import.json	10 days ago
CozyBear	Organized	2 years ago
DEV-0322	Fixed typo	10 months ago
DarkSide	added step to delete exfil.zip (#95)	8 days ago
DazzleSpy	Patching path for VFS	3 months ago
DeepPanda	Patching path for VFS	3 months ago
Diavol	Change scythe.phollowing	17 days ago
Egregor	Patching path for VFS	3 months ago
EvilCorp	Create README.md (#60)	12 months ago
FIN13	Add FIN13	last month
FIN6	Patching path for VFS	3 months ago
FloridaWater	Create README (#57)	12 months ago
Hive	Patching path for VFS	3 months ago

Εικόνα 28. Έτοιμα Community Emulation Plans
Πηγή εικόνας: https://github.com/scythe-io/community-threats

5.7.3 Δημιουργία Emulation Plan

Πολλές φορές τα έτοιμα Emulation Plans μπορεί να είναι αρκετά για το την προσομοίωση ενός συγκεκριμένου APT Group ειδικά στην περίπτωση που είναι αρκετά δημοφιλές οπότε υπάρχουν αρκετοί οργανισμοί που έχουν ασχοληθεί με τη δημιουργία ενός πλάνου. Στην περίπτωση ωστόσο που ένας επιτιθέμενος δεν έχει ακόμα μοντεολοποιηθεί η συμπεριφορά του πλήρως, είναι νέος η δεν έχει στοχοποιήσει πολλούς οργανισμούς ώστε να υπάρχουν Community Emulation Plans πότε μπορεί να δημιουργηθεί ένα νέο. Σύμφωνα με το MITRE ATT&CK Framework η δημιουργία ενός Emulation Plan μπορεί να ολοκληρωθεί ακολουθώντας τα πέντε βήματα που αναλύονται στη συνέχεια [58].

Εικόνα 29. Βήματα για τη δημιουργία ενός Emulation Plan
Πηγή εικόνας: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3

1. Gather threat intel

Επιλογή ενός Adversary / APT group που είναι πιθανό να στοχεύσει τον οργανισμό και συλλογή όλων των διαθέσιμων πληροφοριών που περιγράφουν προηγούμενες επιθέσεις, τα κίνητρα

και τον τρόπο λειτουργίας του.

2. Extract techniques

Από τα δεδομένα που συλλέχθηκαν μπορούν τώρα να εξαχθούν συγκεκριμένες techniques που χρησιμοποιεί ο Threat Actor για να πετύχει τους στόχους του και να γίνουν αντιστοίχηση στο MITRE ATT&CK Framework.

3. Analyze and organize

Τώρα που οι απαραίτητες πληροφορίες για τον τρόπο δράσης, τους στόχους και τα κίνητρα έχουν συλλεχθεί και έχουν μετατραπεί σε TTPs μπορεί να καθοριστεί και ο τελικός στόχος. Για παράδειγμα, αν ο τελικός στόχος είναι το Exfiltration όπως και στο παράδειγμα με το AEP του APT3, τότε πρέπει να δημιουργηθεί και ένα αντίστοιχο Attack Chain path που να αξιοποιεί τα TTPs που ανιχνεύθηκαν στα προηγούμενα βήματα ώστε να επιτευχθεί αυτός ο στόχος.

4. Develop tools and procedures

Το στάδιο αυτό περιλαμβάνεται τη διαδικασία δημιουργίας ή εύρεσης των απαραίτητων εργαλείων ή διαδικασιών που θα είναι σε θέση να αναπαραστήσουν τα TTPs του AEP. Για παράδειγμα κάποια από τα TTPs μπορεί να είναι εφικτό να γίνουν Emulate έτοιμα open-source tools (πχ Mimikatz) ή με Windows Native tools (PsExec) ενώ άλλα να βασίζονται σε tools/infrastructue που πρέπει να σχεδιαστούν ειδικά για τις ανάγκες του συγκεκριμένου AEP.

5. Emulate the adversary

Στο τελευταίο στάδιο, η Red Team διαθέτει πλέον ένα ολοκληρωμένο AEP και είναι σε θέση να διεξάγει το Adversary Emulation engagement. Σε αυτό το στάδιο αξίζει να επισημανθεί το γεγονός πως, εφόσον ο στόχος του Adversary Emulation είναι η βελτίωση της ικανότητας της Blue Team να εντοπίζει εξελιγμένους επιτιθέμενους, είναι θεμιτή η στενή συνεργασία ανάμεσα στις δύο ομάδες ώστε να εντοπιστούν τα κενά που υπάρχουν τόσο visibility όσο και στο Detection της δραστηριότητας του Emulated APT.

5.8 Εργαλεία για Adversary Emulation

Για τις ανάγκες του διεξαγωγής του Adventure Emulation υπάρχουν πολλά διαφορετικά εργαλεία που μπορούν να αξιοποιηθούν. Στην ουσία τα Adventure Emulation Tools χρησιμοποιούνται στο 5ο στάδιο της διεξαγωγής ενός Adversary Emulation Plan, όπως αναφέρθηκε παραπάνω, με στόχο την προσομοίωση του εξελιγμένου επιτιθέμενου και δημιουργίας του απαιτουμένου telemetry για το Blue Team. Κάποια από αυτά έχουν τη μορφή ενός απλού εκτελέσιμου αρχείου .exe ενώ άλλα μπορεί να αποτελούν ολόκληρα σύνθετα Frameworks με πολλαπλές δυνατότητες. Κάποια από αυτά αφορούν την αναπαραγωγή μόνο μερικών συγκεκριμένων τεχνικών ενώ αλλά έχουν ευρεία κάλυψη και είναι σε θέση να εκτελέσουν σύνθετα και πολλαπλών σταδίων σενάρια επίθεσης. Επίσης κάποια από αυτά είναι ανοιχτού κώδικα (open-source) και δωρεάν στη χρήση ενώ αλλά είναι εμπορικές λύσεις κλειστού κώδικα (closed-source).

Για τις ανάγκες της παρούσας εργασίας ορίστηκαν κάποια συγκεκριμένα κριτήρια επιλογής για τα εργαλεία που θα αξιοποιηθούν, τα οποία είναι τα παρακάτω:

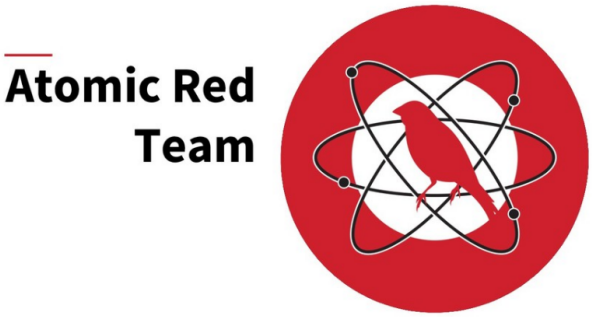
1. Αξιοποιούν το MITRE ATT&CK Framework
2. Μη εμπορικά (Free)
3. Ανοιχτού Κώδικα (Open-Source)
4. Automated / Scripted (όχι Cobalt Strike/Metasploit ή άλλα C2 Frameworks που χρησιμοποιούνται από Red Teams)

Η πρώτη απαίτηση αφορά στη δυνατότητα του εργαλείου να αξιοποιεί το mapping που παρέχει το MITRE ATT&CK Framework εφόσον, πέρα το γεγονός ότι είναι ευρέως διαδεδομένο και εξαιρετικά αποτελεσματικό, η εργασία βασίζεται σε αυτό.

Στη συνέχεια ορίστηκε ως απαίτηση τα εργαλεία που θα επιλεχθούν να είναι open-source και δωρεάν στη χρήση ώστε να μπορούν να χρησιμοποιηθούν από Blue Teams πού ενδέχεται να έχουν περιορισμούς σε θέματα οικονομικών πόρων για την αγορά εμπορικών λύσεων που συνήθως είναι ιδιαίτερα ακριβές. Επιπλέον το γεγονός ότι είναι open-source παρέχει ένα επιπλέον πλεονέκτημα τόσο για την επαλήθευση των ενεργειών που εκτελούνται κατά τη διάρκεια του emulation όσο και της ικανότητας αλλαγής και προσαρμογής των ενεργειών που πραγματοποιούν σε περίπτωση που αυτό είναι αναγκαίο.

Τέλος, η σημαντικότερη ίσως παράμετρος επιλογής είναι ότι τα εργαλεία θα πρέπει να είναι Automated / Scripted ώστε να δίνουν τη δυνατότητα στις Blue Teams, που δεν διαθέτουν τις τεχνικές γνώσεις και ικανότητες που διαθέτει μία Red Team, να αναπαράγουν επιτυχώς τις μεθόδους και τις τεχνικές που θα χρησιμοποιούσε ένας εξελιγμένος επιτιθέμενος χωρίς τη χρήση σύνθετων Red Teaming (C2) Frameworks όπως Cobalt Strike ή Metasploit.

5.8.1 Atomic Red Team



Εικόνα 30. Atomic Red Team Logo

Το Atomic Red Team είναι ένα δημοφιλές εργαλείο για Adversary Emulation που έχει αναπτυχθεί από την εταιρία Red Canary. Είναι open source και παρέχει τη δυνατότητα εκτέλεσης scripted atomic tests που βασίζονται στο MITRE ATT&CK Framework. Ο όρος scripted atomic tests αφορά ολοκληρωμένα και αυτοματοποιημένα test τεχνικών που είναι σχεδιασμένα έτσι ώστε να εκτελούνται με μια απλή εντολή [59].

Για παράδειγμα στην παρακάτω εικόνα με τη χρήση της παρακάτω εντολής γίνεται αυτοματοποιημένη εκτέλεση της τεχνικής T1053.005 ”Scheduled Task/Job: Scheduled Task”.

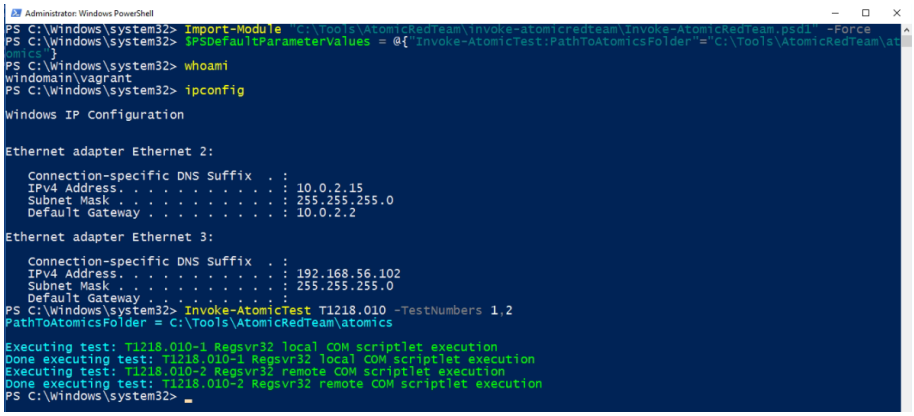
```
Invoke-AtomicTest T1053.005 -TestNumbers 2
```

```
PS C:\WINDOWS\system32> Invoke-AtomicTest T1053.005 -TestNumbers 2
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-2 Scheduled task Local
Done executing test: T1053.005-2 Scheduled task Local
SUCCESS: The scheduled task "spawn" has successfully been created.
```

Εικόνα 31. Ενδεικτική χρήση Atomic Red Team - Scheduled Task/Job: Scheduled Task

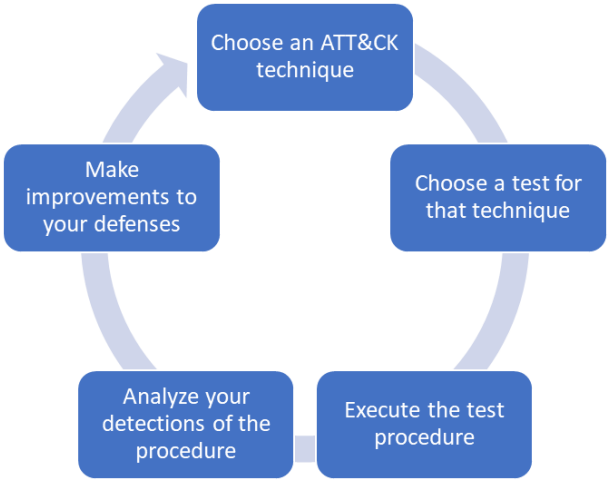
Η ίδια διαδικασία θα ήταν αρκετά πιο περιπλοκή και χρονοβόρα να εκτελεστεί χρησιμοποιώντας ένα Red Teaming Framework όπως το Cobalt Strike ή Metasploit. Συνεπώς το Atomic Red Team είναι ιδιαίτερα χρήσιμο επειδή πέρα από την ευκολία χρήσης που παρέχει, διαθέτει και μεγάλη κάλυψη στα techniques που συμπεριλαμβάνονται στο MITRE ATT&CK Framework. Επιπλέον δεν απαιτείται εγκατάσταση παρά μόνο η εισαγωγή ενός PowerShell module όπως φαίνεται και στην παρακάτω εικόνα. Τέλος, τα Atomic Tests εκτελούνται κατευθείαν στον κάθε host

machine χωρίς να απαιτούν την εγκατάσταση ενός C2 agent/server ή την εκτέλεση προσαρμοσμένου payload.



Εικόνα 32. Ενδεικτική χρήση Atomic Red Team

Η παρακάτω εικόνα παρέχει μια οπτικοποίηση των βημάτων που προτείνει η Red Canary για την αποτελεσματική χρήση του Atomic Red Team εργαλείου.

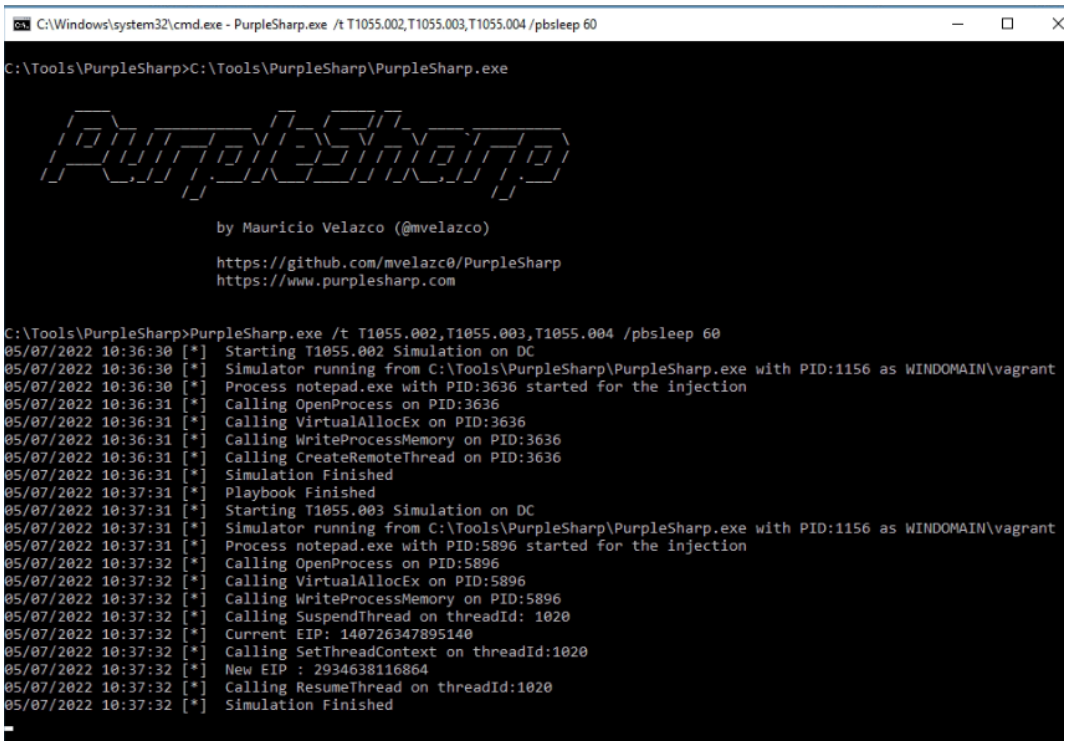


Εικόνα 33. Atomic Testing Lifecycle
Πηγή εικόνας: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3

5.8.2 PurpleSharp

Εικόνα 34. PurpleSharp Logo

Το εργαλείο PurpleSharp διαθέτει παρόμοια λογική με το Atomic Red Team, είναι επίσης free, opensource και βασίζεται στο MITRE ATT&CK Framework. Είναι σχεδιασμένο σε C# και μια από τις διαφορές του και βασικό πλεονέκτημα είναι το γεγονός ότι η χρήση του είναι ακόμα πιο απλή μιας και βασίζεται σε ένα μόνο εκτελέσιμο αρχείο, συνεπώς αποτελεί μια πιο portable λύση. Από την άλλη πλευρά ως μειονέκτημά του σε σχέση με το Atomic Red Team είναι το ότι διαθέτει σαφώς μικρότερη κάλυψη σε ATT&CK techniques και αφορά μόνο Active Directory περιβάλλον [60, 61].



Εικόνα 35. Ενδεικτική χρήση PurpleSharp

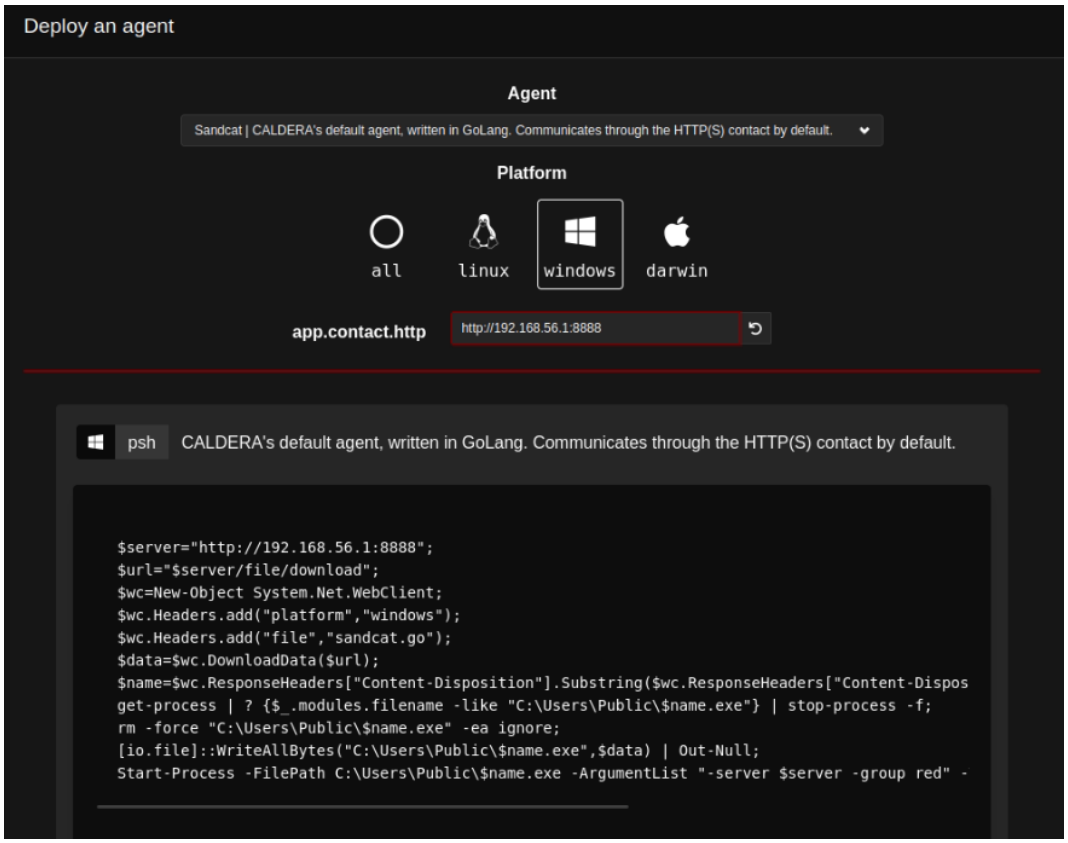
5.8.3 Caldera

Εικόνα 36. Caldera Logo

Το CALDERA (Cyber Adversary Language & Decision Engine) είναι ένα cybersecurity framework που σχεδιάστηκε ώστε να παρέχει την δυνατότητα εκτέλεσης breach & simulation ασκήσεων με αυτοματοποιημένο τρόπο. Συνεπώς, είναι ιδανικό για χρήση σε περιπτώσεις Adversary Emulation όπου υπάρχουν ανάγκες για αυτοματοποίηση και ελαχιστοποίηση των χειροκίνητων βημάτων που πρέπει να πραγματοποιηθούν [62, 63, 64].

Συγκριτικά με τα προηγμένα εργαλεία είναι πιο σύνθετο στη χρήση του και παρέχει περισσότερες δυνατότητες αλλά δεν παύει να είναι μία automated λύση για Adversary Emulation που προσφέρει δυνατότητες οι οποίες είναι διαθέσιμες μόνο σε πιο σύνθετα Red Team Frameworks χωρίς να διαθέτει την αντίστοιχη πολυπλοκότητά τους. Ένα άλλο ιδιαίτερα σημαντικό χαρακτηριστικό και μεγάλο πλεονέκτημα του CALDERA είναι το γεγονός ότι έχει κάποια βασικά στοιχεία και λειτουργίες τα οποία όμως μπορούν πολύ εύκολα να επεκταθούν με την προσθήκη plugin. Το γεγονός ότι είναι free και open source καθιστά πολύ εύκολη τη διαδικασία προσθήκης νέων χαρακτηριστικών και δυνατοτήτων μέσω αυτής της λειτουργίας.

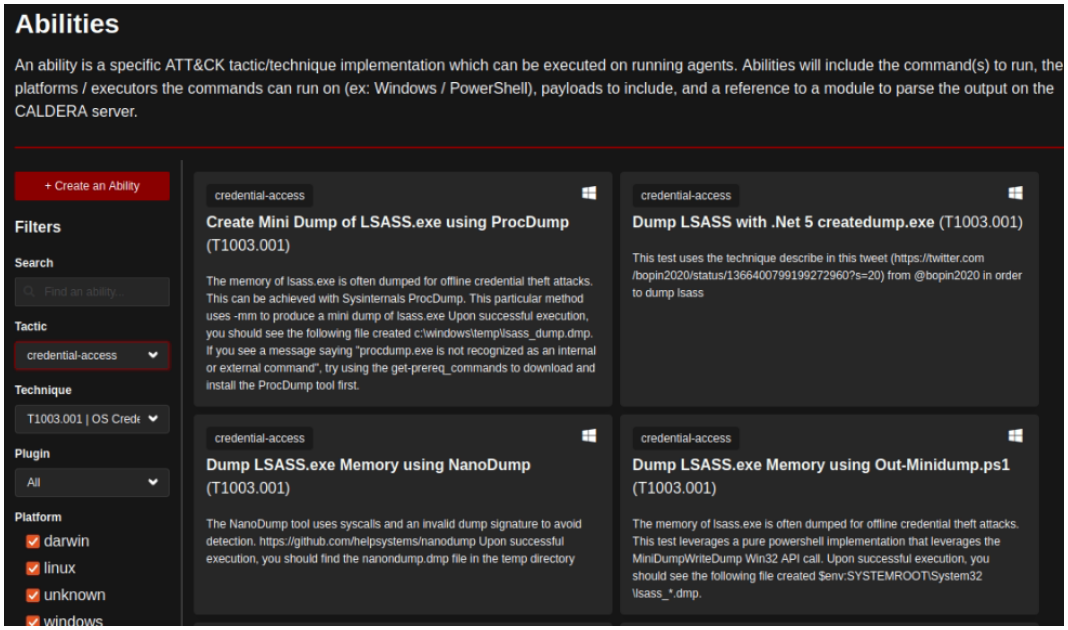
Το Caldera διαθέτει τις δυνατότητες ενός C2 server εφόσον για την έναρξη της εκτέλεσης των ενεργειών που θα έκανε ένας επιτιθέμενος απαιτείται η εγκατάσταση ενός agent στο μηχάνημα του θύματος το οποίο στη συνέχεια συνδέεται με το CALDERA. Μέσω αυτής της σύνδεσης είναι εφικτή η επικοινωνία με το σύστημα που ξεκινά το Emulation Plan.



Εικόνα 37. Caldera C2 Agent

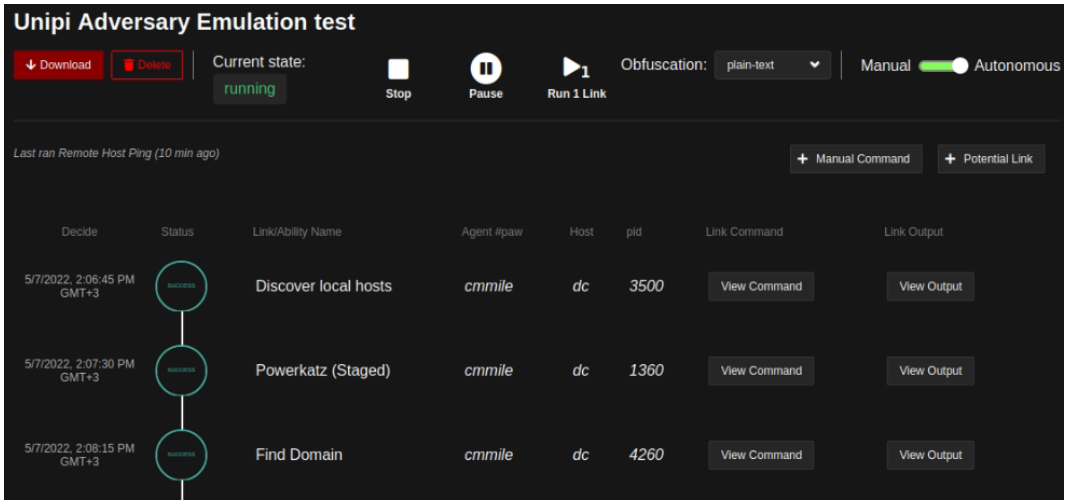
Επιπλέον, ένα από τα πιο σημαντικά πλεονεκτήματα του, που δεν διαθέτουν τα υπόλοιπα εργαλεία που παρουσιάστηκαν, είναι το ότι επιτρέπει το συνδυασμό πολλών τεχνικών ταυτόχρονα ώστε να σχεδιαστεί και να εκτελεστεί ένα ολοκληρωμένο adversary emulation test αυτόματα. Υπάρχουν προσχεδιασμένα έτοιμα σενάρια αλλά μπορούν να δημιουργηθούν και προσαρμοσμένα ανάλογα με τις ανάγκες του κάθε engagement.

Τα Atomic Tests στο Caldera ονομάζονται “Abilities” και μπορούν να συνδυαστούν σε ένα Attack Chain Path που εκτελείται αυτόματα.



Εικόνα 38. Atomic Tests στο Caldera (Abilities)

Όταν όλα τα επιθυμητά “Abilities” (Atomic Tests) συνδυαστούν σε ένα “Operation” (δηλαδή ένα ολοκληρωμένο test) τότε μπορεί να εκτελεστούν αυτόματα από το CALDERA και να παρουσιαστούν τα αποτελέσματα από κάθε στάδιο μέσω του Web Interface.



Εικόνα 39. Πλήρες Emulation test στο Caldera

5.8.4 Stratus Red team

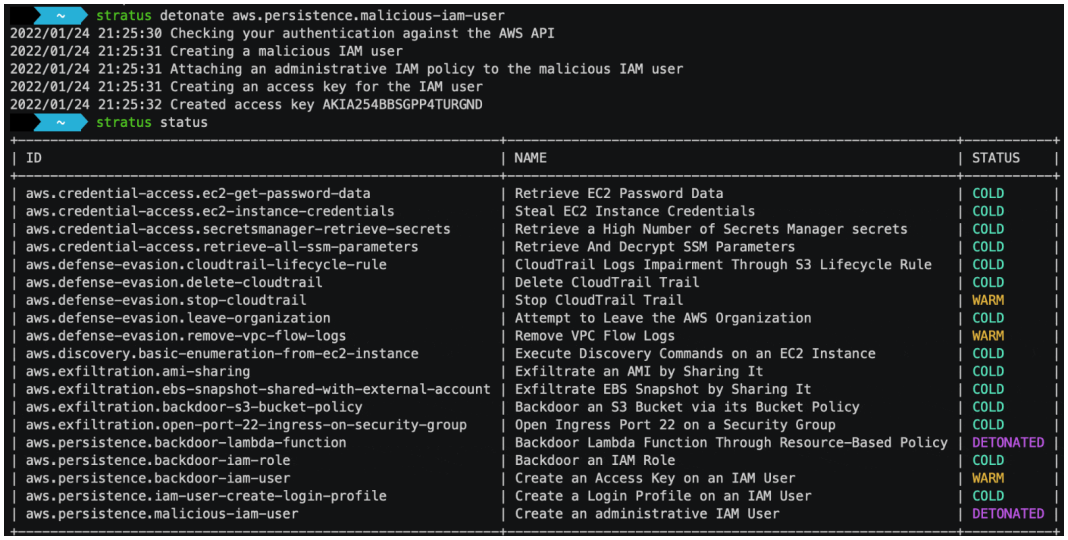
Εικόνα 40. Stratus Red team - logo

Το τελευταίο εργαλείο ονομάζεται Stratus Red team και η βασική του διαφορά είναι πως εστιάζει σε περιβάλλον Cloud. Ενώ υπάρχουν αρκετά εργαλεία για την πραγματοποίηση scripted/automated Adversary emulation σε on-premise / local περιβάλλον, λίγα από αυτά διαθέτουν Atomic Tests για το Cloud. Πρόσφατα το Atomic Red Team εισήγαγε κάποια Atomic Tests που περιλαμβάνουν Cloud ωστόσο, επειδή δεν έχει σχεδιαστεί για Cloud testing, δεν διαχειρίζεται αυτόματα τις προαπαιτήσεις για την εκτέλεση των TTPs, αφήνοντας τες στον χρήστη [65, 66]. Για παράδειγμα, το Atomic Test T1098.001 (AWS - Create Access Key and Secret Key) απαιτεί από τον χρήστη τη δημιουργία ενός IAM user πριν την έναρξη της επίθεσης. Το Stratus Red Team διαθέτει την ικανότητα να αυτοματοποιεί αυτές τις διαδικασίες πριν την έναρξη μιας επίθεσης, απλοποιώντας κατά πολύ τη διαδικασία.

Μερικά παραδείγματα για Cloud (AWS) Atomic Test που περιλαμβάνει είναι τα παρακάτω:

Name	Platform	MITRE ATT&CK Tactics
Retrieve EC2 Password Data	AWS	Credential Access
Steal EC2 Instance Credentials	AWS	Credential Access
Retrieve a High Number of Secrets Manager secrets	AWS	Credential Access
Retrieve And Decrypt SSM Parameters	AWS	Credential Access
Delete CloudTrail Trail	AWS	Defense Evasion
Disable CloudTrail Logging Through Event Selectors	AWS	Defense Evasion
CloudTrail Logs Impairment Through S3 Lifecycle Rule	AWS	Defense Evasion
Stop CloudTrail Trail	AWS	Defense Evasion

Εικόνα 41. Stratus Supported AWS attacks
Πηγή εικόνας: https://stratus-red-team.cloud/attack-techniques/list/



```
~ stratus detonate aws.persistence.malicious-iam-user
2022/01/24 21:25:30 Checking your authentication against the AWS API
2022/01/24 21:25:31 Creating a malicious IAM user
2022/01/24 21:25:31 Attaching an administrative IAM policy to the malicious IAM user
2022/01/24 21:25:31 Creating an access key for the IAM user
2022/01/24 21:25:32 Created access key AKIA254BBSGPP4TURGND
~ stratus status
+-----------------------------------------------------------+-----------------------------------------------------------+------------+
| ID                                                        | NAME                                                      | STATUS     |
+-----------------------------------------------------------+-----------------------------------------------------------+------------+
| aws.credential-access.ec2-get-password-data               | Retrieve EC2 Password Data                                | COLD       |
| aws.credential-access.ec2-instance-credentials            | Steal EC2 Instance Credentials                            | COLD       |
| aws.credential-access.secretsmanager-retrieve-secrets     | Retrieve a High Number of Secrets Manager secrets         | COLD       |
| aws.credential-access.retrieve-all-ssm-parameters         | Retrieve And Decrypt SSM Parameters                       | COLD       |
| aws.defense-evasion.cloudtrail-lifecycle-rule             | CloudTrail Logs Impairment Through S3 Lifecycle Rule      | COLD       |
| aws.defense-evasion.delete-cloudtrail                     | Delete CloudTrail Trail                                   | COLD       |
| aws.defense-evasion.stop-cloudtrail                       | Stop CloudTrail Trail                                     | WARM       |
| aws.defense-evasion.leave-organization                    | Attempt to Leave the AWS Organization                     | COLD       |
| aws.defense-evasion.remove-vpc-flow-logs                  | Remove VPC Flow Logs                                      | WARM       |
| aws.discovery.basic-enumeration-from-ec2-instance         | Execute Discovery Commands on an EC2 Instance             | COLD       |
| aws.exfiltration.ami-sharing                              | Exfiltrate an AMI by Sharing It                           | COLD       |
| aws.exfiltration.ebs-snapshot-shared-with-external-account | Exfiltrate EBS Snapshot by Sharing It                     | COLD       |
| aws.exfiltration.backdoor-s3-bucket-policy                | Backdoor an S3 Bucket via its Bucket Policy               | COLD       |
| aws.exfiltration.open-port-22-ingress-on-security-group   | Open Ingress Port 22 on a Security Group                  | COLD       |
| aws.persistence.backdoor-lambda-function                  | Backdoor Lambda Function Through Resource-Based Policy    | DETONATED  |
| aws.persistence.backdoor-iam-role                         | Backdoor an IAM Role                                      | COLD       |
| aws.persistence.backdoor-iam-user                         | Create an Access Key on an IAM User                       | WARM       |
| aws.persistence.iam-user-create-login-profile             | Create a Login Profile on an IAM User                     | COLD       |
| aws.persistence.malicious-iam-user                        | Create an administrative IAM User                         | DETONATED  |
+-----------------------------------------------------------+-----------------------------------------------------------+------------+
```

Εικόνα 42. Stratus Supported AWS attacks

Παρά το γεγονός ότι το συγκεκριμένο εργαλείο δεν χρησιμοποιήθηκε στα πλαίσια αυτής της εργασίας, είναι άξιο αναφοράς, καθώς πλέον πολλοί οργανισμοί διαθέτουν ένα Hybrid μοντέλο που συνδυάζει Infrastructure τόσο σε on-premise όσο και Cloud περιβάλλον συνεπώς μπορεί να φανεί χρήσιμο σε κάποιες περιπτώσεις λόγω των ιδιαίτερων χαρακτηριστικών του.

5.8.5 Συγκριτική Αξιολόγηση Εργαλείων

Για τις ανάγκες της παρούσας εργασίας ορίστηκαν κάποια συγκεκριμένα κριτήρια επιλογής για τα εργαλεία που θα αξιοποιηθούν όπως το να αξιοποιούν, το MITRE ATT&CK Framework, να είναι μη εμπορικά (Free) και ανοιχτού κώδικα (Open-Source) αλλά κυρίως να είναι Automated / Scripted, ώστε να είναι εφικτό να χρησιμοποιηθούν από Blue Teams χωρίς εξειδικευμένες γνώσεις σε περίπλοκα Adversary Emulation Tools. Ωστόσο, παρά τα κοινά τους χαρακτηριστικά έχουν σημαντικές διαφορές που κάνουν το κάθε ένα από αυτά ξεχωριστό και καταλληλότερο ανά περίπτωση. Για αυτό το λόγο ο παρακάτω πίνακας λειτουργεί ως μία σύνοψη των διαφορετικών τους χαρακτηριστικών ανάλογα με τις δυνατότητες που προσφέρουν.

	Atomic Red Team	PurpleSharp	Caldera	Stratus Red Team
MITRE ATT&CK Mapping	YES	YES	YES	YES
Automated / Scripted	YES	YES	YES	YES
Platform Coverage	Multiple	Windows	Windows, Linux, Darwin	Cloud
Open Source / Free	YES / YES	YES / YES	YES / YES	YES / YES
Installation required	NO	NO	YES	NO
Ease of use	Easy	Trivial	Moderate	Easy
Interface / GUI	CLI	CLI	Web-based	CLI
Cloud support	Partial	NO	NO	Extensive
Extensibility	NO	NO	YES (plugins)	NO
C2 Capabilities	NO	NO	YES	NO
Obfuscation / Stealth	NO	NO	YES	NO
Autonomous Plan Emulation	NO	NO	YES	NO
Reporting	NO	NO	YES	NO

Εικόνα 43. Πίνακας συγκριτικής αξιολόγησης εργαλείων

Κεφάλαιο 6

Δημιουργία περιβάλλοντος δοκιμών με τη χρήση του DetectionLab

Εικόνα 44. DetectionLab Logo

6.1 Εισαγωγή

Για τις ανάγκες της εργασίας απαιτείται ο σχεδιασμός ενός περιβάλλοντος το οποίο να προσομοιώνει το δίκτυο ενός οργανισμού και να συμπεριλαμβάνει τα εργαλεία τα οποία είναι απαραίτητα για τη διεξαγωγή των πειραμάτων και για τη συλλογή των αποτελεσμάτων. Κάθε οργανισμός διαθέτει διαφορετικό περιβάλλον και αξιοποιεί διαφορετικές τεχνολογίες και security tools, συνεπώς μια μεθοδολογία που θα εξαρτώταν σε συγκεκριμένο περιβάλλον και τεχνολογίες δεν θα ήταν ιδανική. Επιπλέον η δημιουργία ενός δοκιμαστικού περιβάλλοντος το οποίο να συνδυάζει τις τεχνολογίες αλλά και το configuration που απαιτείται για τη διεξαγωγή τόσο του Threat Hunting όσο και του Adversary Emulation είναι μία δύσκολη και χρονοβόρα διαδικασία.

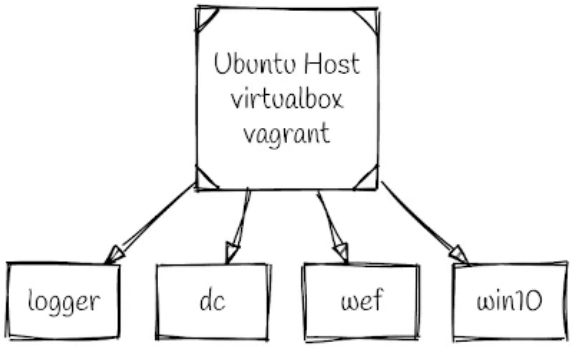
6.2 Παρουσίαση DetectionLab

Για τους παραπάνω λόγους επιλέχθηκε η χρήση του DetectionLab. Το DetectionLab είναι ένα σύνολο από εργαλεία και scripts τα οποία επιτρέπουν την αυτοματοποίηση της διαδικασίας δημιουργίας ενός Windows Active Directory Lab που να διαθέτει πλήρες logging σε SIEM (Splunk) και χρήσιμα εργαλεία όπως osquery, Zeek, Suricata. Ο βασικός σκοπός δημιουργίας του ήταν η παροχή μιας εύκολης και αυτοματοποιημένης λύσης για τις Blue Team που επιθυμούν να δημιουργήσουν γρήγορα και εύκολα ένα πλήρες περιβάλλον Active Directory με όλα τα απαιτού-

μενα εργαλεία για την διεξαγωγή σχετικών πειραμάτων. Συνεπώς, για τις ανάγκες τις εργασίας είναι μια ιδανική λύση, γι' αυτό και επιλέχθηκε. Το DetectionLab αυτοματοποιεί πλήρως τη διαδικασία δημιουργίας των Virtual Machine, του Active Directory και των παραμετροποιήσεων που απαιτούνται για το πλήρες logging. [67]

6.3 Τοπολογία δικτύου

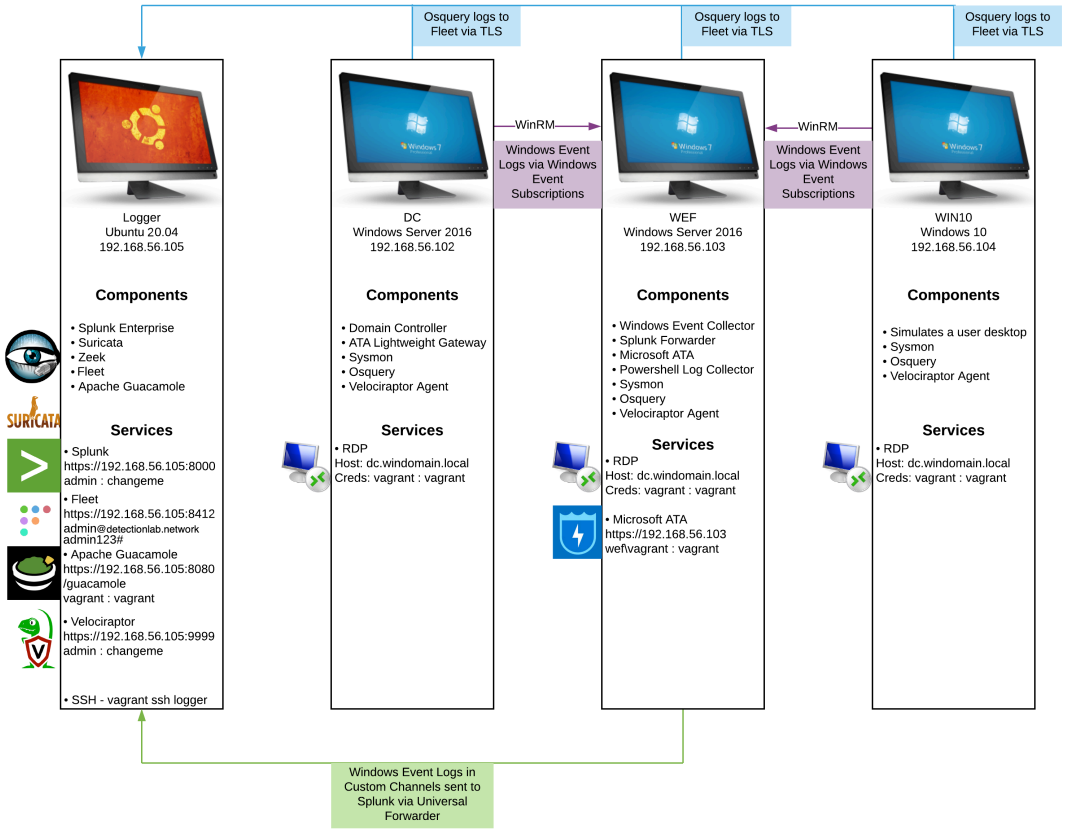
Το Detection Lab μπορεί να εγκατασταθεί με πολλούς διαφορετικούς τρόπους σχεδόν σε όλα τα λειτουργικά συστήματα. Για τις ανάγκες της εργασίας χρησιμοποιήθηκε ως βάση το λειτουργικό σύστημα Ubuntu με Hypervisor το VirtualBox όπως φαίνεται και στο παρακάτω σχεδιάγραμμα. Μέσω του Vagrant ήταν εφικτό το provisioning των VMs που αποτελούνται από τέσσερις διαφορετικούς hosts όπου κάθε ένας εξυπηρετεί διαφορετικό σκοπό.



Εικόνα 45. Τοπολογία δικτύου DetectionLab σε αφαιρετικό επίπεδο
Πηγή εικόνας: https://detectionlab.network/introduction/packerandvagrant/

Πιο συγκεκριμένα, ο host "Logger" έχει ως βάση το λειτουργικό σύστημα Ubuntu και αποτελεί το σημείο όπου συγκεντρώνονται όλα τα logs από τους υπόλοιπους hosts που αποτελούν μέρος του δικτύου. Τα επιμέρους στοιχεία τα οποία εκτελούνται στο Logger Host περιλαμβάνουν το Splunk SIEM, τα IDS Suricata και Zeek και άλλα βοηθητικά εργαλεία όπως το Fleet, το οποίο επιτρέπει την διαχείριση πολλαπλών host από έναν κεντρικό server και το Apache Guacamole που βοήθα στη διαχείριση και στη σύνδεση με τους υπόλοιπους hosts.

Το υπόλοιπο δίκτυο αποτελείται από τρεις Windows hosts που ο καθένας τους εξυπηρετεί διαφορετικό σκοπό. Αρχικά ο Domain controller (Windows Server 2016) είναι υπεύθυνος για τη διαχείριση του Active directory, κι έπειτα ο host WEF (Windows Event Forwarding - Windows server 2016) είναι υπεύθυνος για τη συγκέντρωση και την προώθηση των logs από όλο το Active directory σε συστήματα όπως το Splunk ή το Suricata. Τέλος, υπάρχει ο host WIN10 (Windows 10) ο οποίος έχει ως σκοπό το να προσομοιώνει ένα απλό endpoint που χρησιμοποιεί ένας υπάλληλος. Το δίκτυο του DetectionLab περιέχει τους βασικούς hosts που χρειάζονται για να διεξαχθούν απλά σενάρια και πειράματα αλλά παρέχει τη δυνατότητα να προστεθούν επιπλέον hosts ώστε το Active Directory περιβάλλον να επεκταθεί και να προσαρμοστεί ώστε να προσομοιώνει σε καλύτερο βαθμό την τοπολογία του κάθε οργανισμού.



Εικόνα 46. Αναλυτική τοπολογία δικτύου DetectionLab
Πηγή εικόνας: https://detectionlab.network/introduction/

Η παρακάτω λίστα παρουσιάζει όλα τα στοιχεία που περιλαμβάνει ο κάθε host.
DC - Windows 2016 Domain Controller

- WEF Server Configuration GPO
- Powershell logging GPO
- Enhanced Windows Auditing policy GPO
- Sysmon
- Velociraptor
- osquery
- Splunk Universal Forwarder (Forwards Sysmon & osquery)
- Sysinternals Tools
- Microsft Advanced Threat Analytics Lightweight Gateway

WEF - Windows 2016 Server

- Microsoft Advanced Threat Analytics
- Windows Event Collector

- Windows Event Subscription Creation
- Powershell transcription logging share
- Sysmon
- Velociraptor
- osquery
- Splunk Universal Forwarder (Forwards WinEventLog & Powershell & Sysmon & osquery)
- Sysinternals tools

Win10 - Windows 10 Workstation

- Employee workstation
- Sysmon
- Velociraptor
- osquery
- Splunk Universal Forwarder (Forwards Sysmon & osquery)
- Sysinternals Tools

Logger - Ubuntu 16.04

- Splunk Enterprise
- Fleet osquery Manager
- Zeek
- Suricata
- Guacamole
- Velociraptor server

6.4 Εγκατάσταση

Πριν παρουσιαστούν τα βήματα της εγκατάστασης του DetectionLab, για να γίνουν πιο κατανοητές οι τεχνολογίες και τα εργαλεία που χρησιμοποιούνται κατά την εγκατάσταση, είναι σημαντική η ανάλυση των εργαλείων Packer και Vagrant. Και τα δύο εργαλεία εξυπηρετούν παρόμοιο σκοπό: την αυτοματοποίηση διαδικασιών που διαφορετικά θα έπρεπε να πραγματοποιηθούν χειροκίνητα για την επίτευξη του ίδιου αποτελέσματος. Για παράδειγμα, δίχως Packer και Vagrant, για να επιτύχουμε τον σχεδιασμό ενός αντίστοιχου δοκιμαστικού περιβάλλοντος, θα έπρεπε να πραγματοποιηθούν οι παρακάτω ενέργειες.

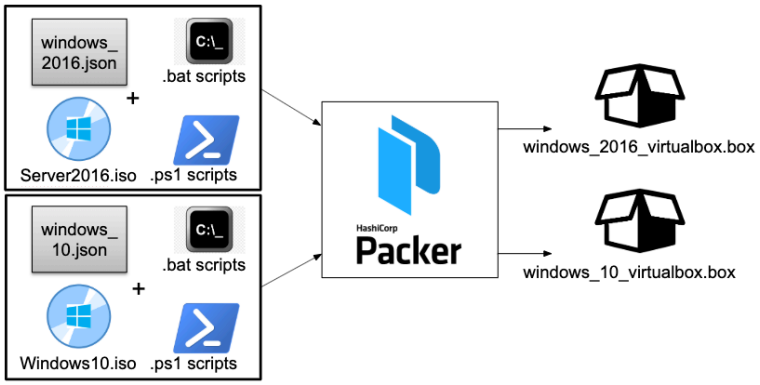
- Απόκτηση αρχείων ISO για τα λειτουργικά συστήματα Ubuntu, Windows Server 2016 και Windows 10.
- Χρήση ενός Hypervisor όπως Virtualbox ή VMware για την εγκατάσταση των λειτουργικών συστημάτων.

- Βασικές παραμετροποιήσεις ανά Host ώστε να διαθέτει τις σωστές ρυθμίσεις σε πόρους hardware (CPU cores, Disk, RAM κτλ).
- Λήψη snapshot για κάθε VM όταν έχει ολοκληρωθεί η εγκατάσταση και η παραμετροποίηση.
- Εγκατάσταση και παραμετροποίηση των απαραίτητων επιμέρους στοιχείων όπως Splunk, Active Directory Domain Services, Windows Event Forwarding και πολλών ακόμα εργαλείων που απαιτούνται.
- Σύνδεση κάθε host με το Active Directory domain και πραγματοποίηση δοκιμών ώστε να είναι βέβαιη η ορθή λειτουργεία τους.

Προφανώς αυτή η διαδικασία είναι εξαιρετικά χρονοβόρα και επίπονη, ιδιαίτερα αν χρειάζεται να επαναλαμβάνεται συχνά, όπως στην περίπτωση ενός δοκιμαστικού περιβάλλοντος. Τα εργαλεία Packer, Vagrant βοηθούν στην αυτοματοποίηση όλων των βημάτων που αναφέρθηκαν παραπάνω και όχι μόνο εξοικονομούν χρόνο αλλά διασφαλίζουν και πως το τελικό αποτέλεσμα θα είναι κάθε φορά το επιθυμητό.

6.4.1 Packer

Το εργαλείο Packer έχει σχεδιαστεί έτσι ώστε να λαμβάνει ως κύρια είσοδο ένα αρχείο ISO με το επιθυμητό λειτουργικό σύστημα, πχ Windows 10, και επιπλέον αρχεία με τη μορφή .json (JavaScript Object Notation), .ps1 (Windows PowerShell), .bat (Windows Batch file) που περιλαμβάνει προκαθορισμένες ρυθμίσεις για την προσαρμογή του λειτουργικού συστήματος. Το τελικό αποτέλεσμα είναι ένα ”Box” που στην ουσία είναι μια τροποποιημένη έκδοση του επιλεγμένου λειτουργικού συστήματος. Συνεπώς το Packer, όπως φαίνεται και στην παρακάτω εικόνα, επιτρέπει την αυτοματοποιημένη εγκατάσταση και διαμόρφωση του λειτουργικού συστήματος.

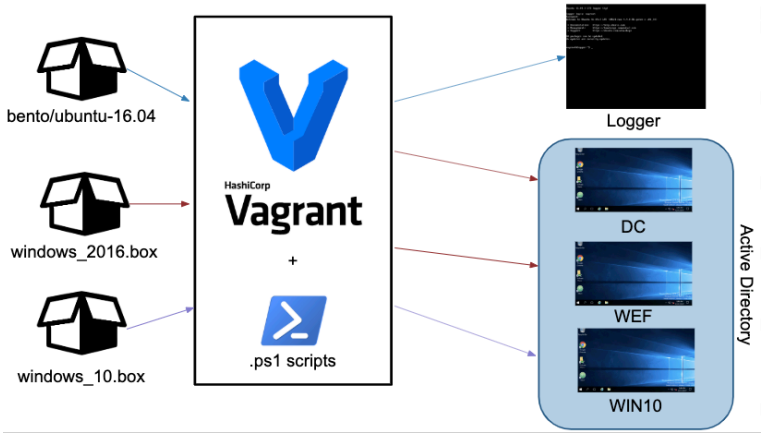


Εικόνα 47. Εγκατάσταση DetectionLab μέσω Packer και VirtualBox σε Ubuntu
Πηγή εικόνας: https://detectionlab.network/introduction/packerandvagrant/

6.4.2 Vagrant

Το Vagrant είναι ένας command line client για virtualization hypervisor όπως το VirtualBox και το VMware. Όπως για παράδειγμα το Docker μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός container, έτσι και το Vagrant μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός ολόκληρου Virtual Machine. Το Vagrant είναι υπεύθυνο να διαχειριστεί το output (.box) που δημιουργήθηκε προηγουμένως από το Packer. Το Vagrant, λαμβάνοντας ως input το “box” αναλαμβάνει να το ενσωματώσει στον επιλεγμένο hypervisor χωρίς να χρειάζεται η χρήση το graphic user interface λόγω

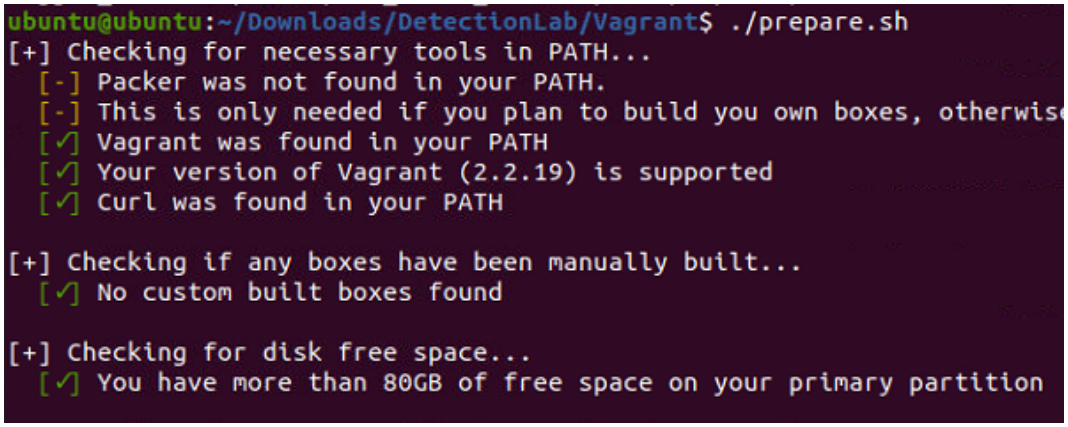
του ότι η διαδικασία μπορεί να πραγματοποιηθεί μέσω command line. Συνεπώς τα Vagrantfiles περιλαμβάνουν πληροφορίες για το πως τα virtual machines μπορούν να ρυθμιστούν αυτόματα σύμφωνα με προκαθορισμένες ρυθμίσεις σχετικά με CPU/memory specifications, networking options, και φυσικά να εκτελέσουν όποια scripts ή εντολές χρειάζονται. Στην περίπτωση του DetectionLab αυτά τα scripts αναλαμβάνουν την εγκατάσταση των Splunk, Active Directory, Windows Event Forwarding, Security Tooling κτλ.



Εικόνα 48. Εγκατάσταση DetectionLab μέσω Vagrant και VirtualBox σε Ubuntu
Πηγή εικόνας: https://detectionlab.network/introduction/packerandvagrant/

Εφόσον οι δύσκολες διαδικασίες είναι αυτοματοποιημένες από το Packer και το Vagrant, η εγκατάσταση του DetectionLab αποτελεί μία πολύ απλή διαδικασία που απαιτεί τη χρήση ελάχιστων και πολύ απλών εντολών. Με τη χρήση των παρακάτω εντολών γίνεται η ενημέρωση του λειτουργικού συστήματος Ubuntu και η εγκατάσταση των εργαλείων που θα χρειαστούν για την εγκατάσταση του DetectionLab όπως το git το curl το Vagrant (ως provisioner) και το VirtualBox (ως Hypervisor). Στη συνέχεια γίνεται clone το repository του DetectionLab από το GitHub και εκτελείται το αρχείο prepare.sh που πραγματοποιεί τους απαραίτητους ελέγχους ώστε να διαπιστωθεί αν το περιβάλλον απαιτεί όλες τις προϋποθέσεις για την έναρξη της εγκατάστασης.

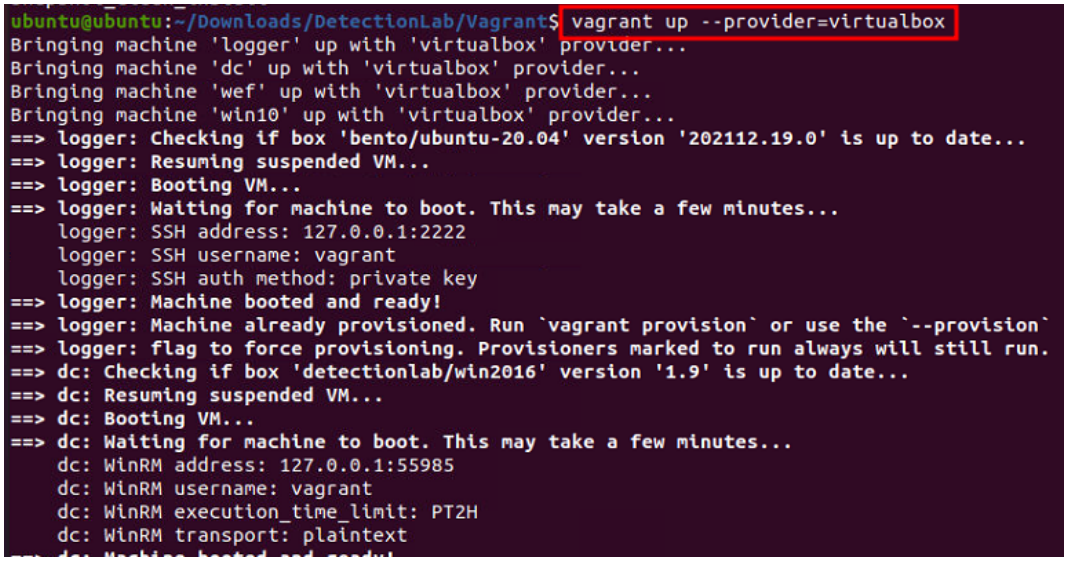
```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install git curl virtualbox
curl -fsSL https://apt.releases.hashicorp.com/gpg | sudo apt-key add -
sudo apt-add-repository "deb [arch=amd64] https://apt.releases.hashi
corp.com $(lsb_release -cs) main"
sudo apt-get update
sudo apt-get install vagrant
cd Downloads/
git clone https://github.com/clong/DetectionLab.git
cd DetectionLab/
cd Vagrant/
./prepare.sh
```



Εικόνα 49. Έλεγχος απαιτήσεων περιβάλλοντος για εγκατάσταση DetectionLab

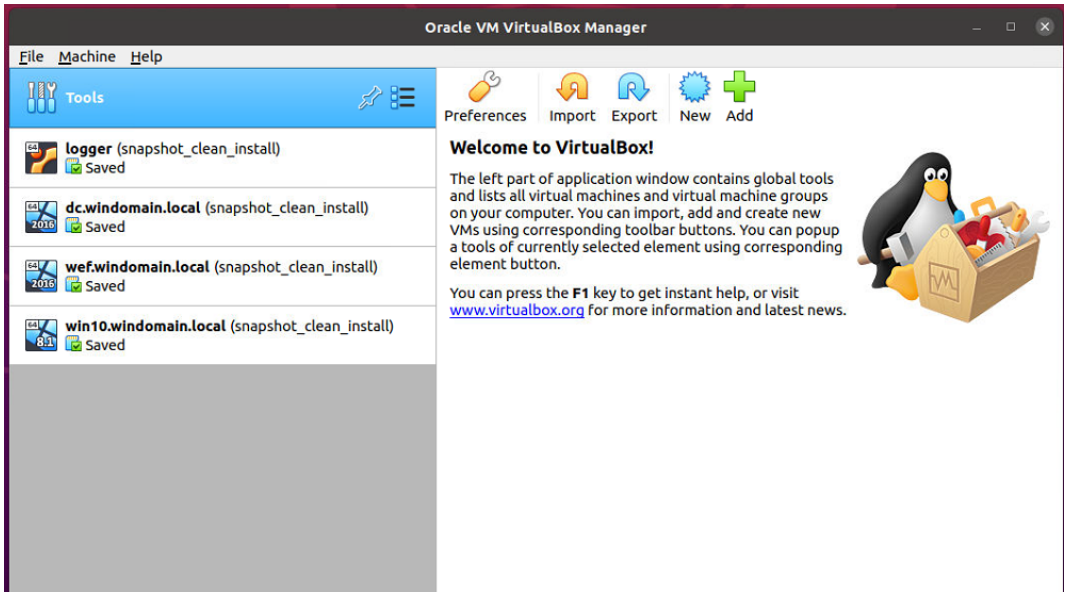
Εφόσον όλοι οι έλεγχοι είναι επιτυχείς, μπορεί να ξεκινήσει η εγκατάσταση του DetectionLab με την παρακάτω εντολή.

```
vagrant up --provider=virtualbox
```



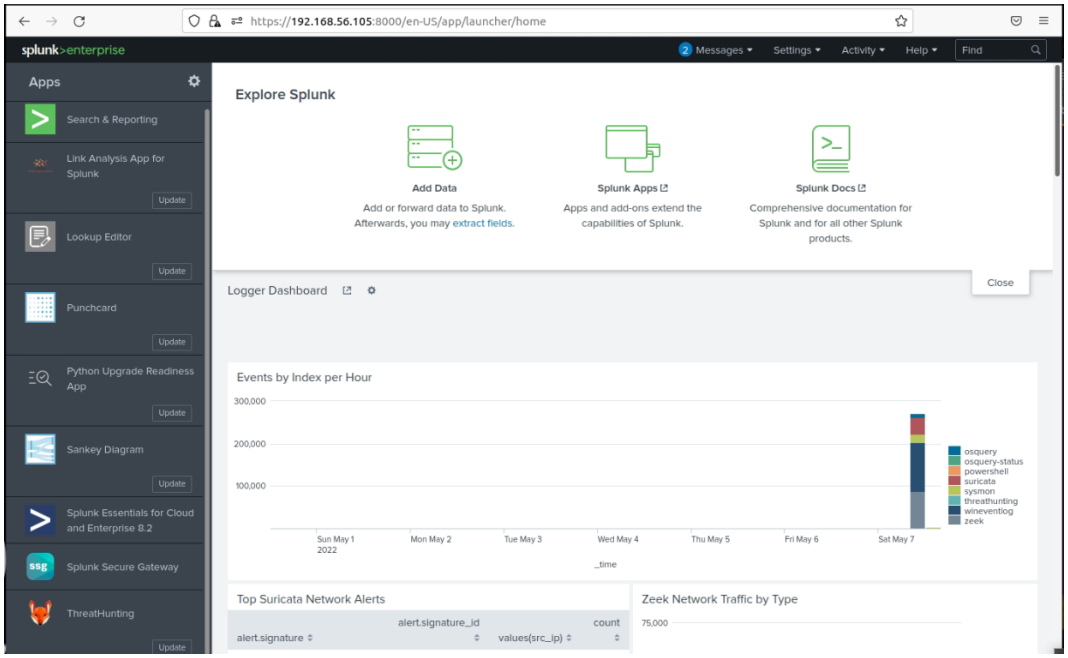
Εικόνα 50. Εγκατάσταση DetectionLab μέσω Vagrant

Όπως φαίνεται στην παρακάτω εικόνα, κατά την ολοκλήρωση της εγκατάστασης τα virtual machines έχουν εμφανιστεί στο interface του VirtualBox και είναι έτοιμα προς χρήση.



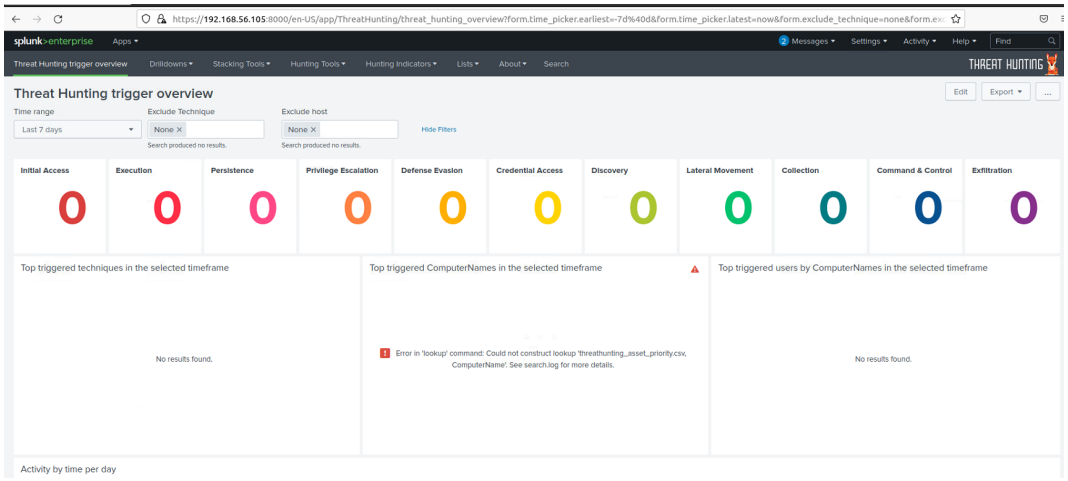
Εικόνα 51. Ενεργοί hosts στο VirtualBox Hypervisor

Εφόσον έχει ολοκληρωθεί η εγκατάσταση, τα επιμέρους στοιχεία του DetectionLab, όπως το Splunk SIEM, είναι έτοιμα προς χρήση.



Εικόνα 52. Ενεργή εγκατάσταση Splunk SIEM

Συγκεκριμένα, το Splunk SIEM έρχεται προ-εγκατεστημένο με ένα πολύ χρήσιμο plugin το οποίο και είναι ιδανικό για τα πειράματα που θα διεξαχθούν στο επόμενο κεφάλαιο καθώς, είναι σε θέση να κάνει MAP διάφορα events πάνω στο MITRE ATT&CK Framework βοηθώντας σημαντικά τους αναλυτές να διεξαγάγουν το Theat Hunting μετά το Adversary Emulation.



Εικόνα 53. Splunk SIEM με Threat Hunting Plugin βασισμένο στο MITRE ATT&CK

6.5 Προσαρμογή περιβάλλοντος και εισαγωγή αδυναμιών

Αφού είχε ολοκληρωθεί η εγκατάσταση το Detection Lab έχουμε στη διάθεσή μας ένα ολοκληρωμένο Active Directory περιβάλλον για να διεξαχθούν τα πειράματα και οι δοκιμές που σχετίζονται με το Adversary Emulation. Ωστόσο, πολλά από τα σενάρια και τα επιθυμητά πειράματα, για να πραγματοποιηθούν, απαιτούν συγκεκριμένες προϋποθέσεις που βασίζονται σε ρυθμίσεις εντός του Active Directory. Για παράδειγμα, η διεξαγωγή συγκεκριμένων επιθέσεων όπως DCSync ή Kerberoasting απαιτεί προηγουμένως να έχουν γίνει συγκεκριμένες παραμετροποίησεις στο Active Directory. Αυτές οι ρυθμίσεις μπορούν να πραγματοποιηθούν χειροκίνητα αλλά και πάλι απαιτούν αρκετό κόπο και χρόνο. Η διαδικασία αυτή μπορεί να αυτοματοποιηθεί μέσω της χρήσης του Vuln-AD που δεν είναι τίποτα άλλο παρά ένα PowerShell script το οποίο αναλαμβάνει την παραμετροποίηση του Active Directory περιβάλλοντος έτσι ώστε να εισάγει τις παρακάτω επιθέσεις [68].

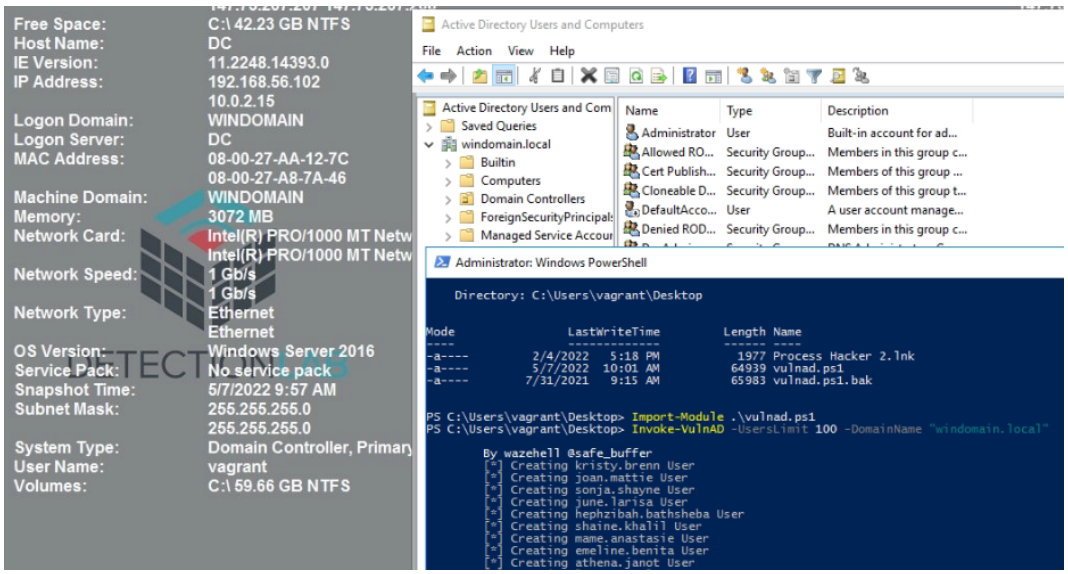
- Abusing ACLs/ACEs
- Kerberoasting
- AS-REP Roasting
- Abuse DnsAdmins
- Password in Object Description
- User Objects With Default password (Changeme123!)
- Password Spraying
- DCSync
- Silver Ticket
- Golden Ticket
- Pass-the-Hash
- Pass-the-Ticket

- SMB Signing Disabled

Εφόσον η εγκατάσταση του Active Directory έχει ήδη ολοκληρωθεί από το Detection Lab, αρκεί η εισαγωγή του Vuln-AD script στο PowerShell και η εκτέλεση του με τα επιθυμητά arguments. Στην προκειμένη περίπτωση τα arguments περιλαμβάνουν τον αριθμό των χρηστών που θα εισαχθούν (100) και το domain name που έχει δημιουργηθεί (windomain.local).

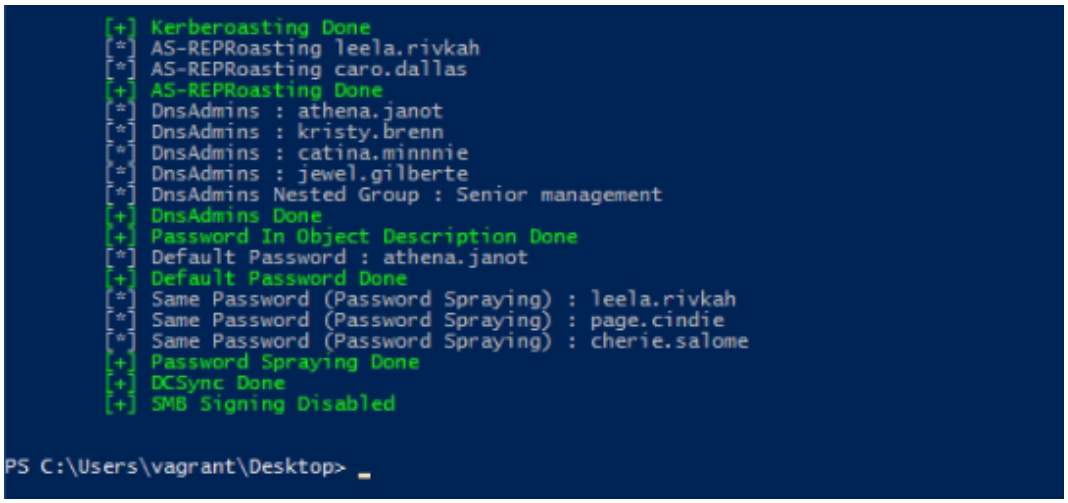
```
https://raw.githubusercontent.com/wazehell/vulnerable-AD/master/vulnad.ps1
Import-Module .\\vulnad.ps1
Invoke-VulnAD -UsersLimit 100 -DomainName "windomain.local"
```

Όπως φαίνεται στην παρακάτω εικόνα, το Vuln-AD script εκτελείται μέσω PowerShell και ξεκινά τη δημιουργία των χρηστών και την εισαγωγή των αδυναμιών.



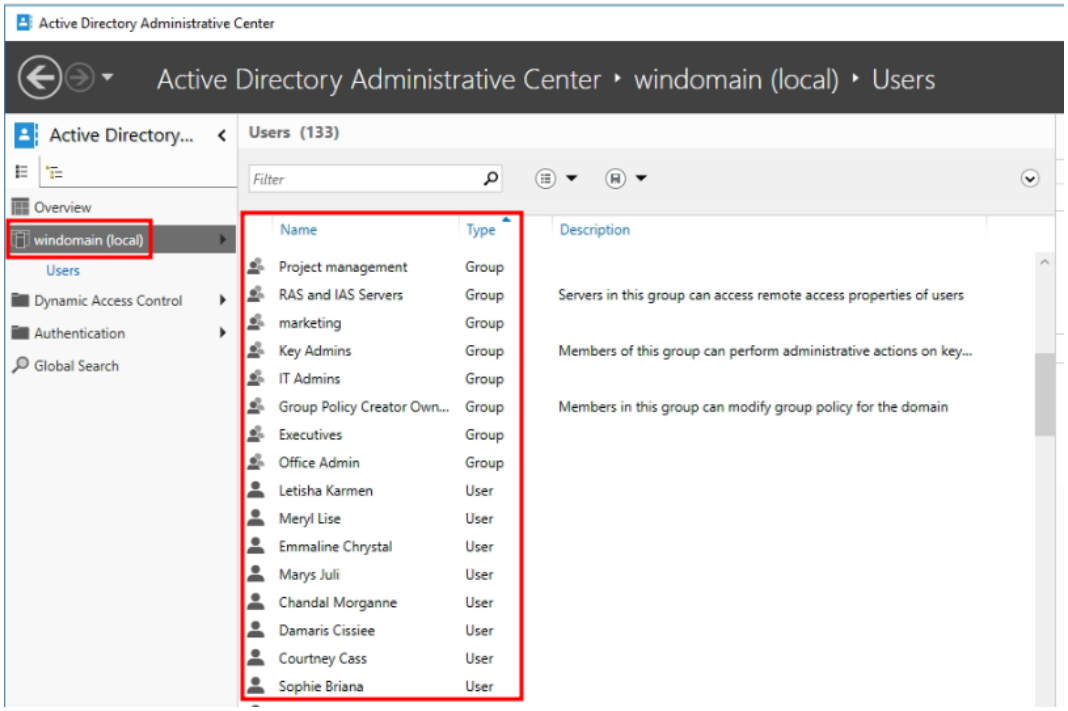
Εικόνα 54. Χρήση vulnerable-AD για την εισαγωγή αδυναμιών στο Active Directory

Κατά την ολοκλήρωση της εκτέλεσης του script, τα αποτελέσματα εμφανίζονται στο terminal και φανερώνουν πως οι αδυναμίες εισήχθησαν επιτυχώς στο περιβάλλον.



Εικόνα 55. Αποτελέσματα έπειτα απο την εκτέλεση του Vulnerable-AD

Το γεγονός αυτό μπορεί να επαληθευτεί πολύ εύκολα παρατηρώντας τους νέους χρήστες που έχουν δημιουργηθεί στο Active Directory περιβάλλον από το Administrative Center του Domain Controller.



Εικόνα 56. Νέοι χρήστες και Groups έχουν εισαχθεί στο Active Directory

Κεφάλαιο 7

Adversary Emulation στο DetectionLab

7.1 Προσομοίωση TTPs του APT29 μέσω του Invoke-APT29

Για την προσομοίωση ενός Adversary μπορούν να χρησιμοποιηθούν διαφορετικά εργαλεία όπου το κάθε ένα, διαθέτοντας διαφορετικά χαρακτηριστικά και έχοντας σχεδιαστεί με διαφορετικό σκοπό μπορεί να προσφέρει ποικίλα πλεονεκτήματα. Κάποια εργαλεία έχουν σχεδιαστεί ώστε να έχουν μεγάλη κάλυψη από TTPs ώστε να μπορούν να χρησιμοποιηθούν σε ad-hoc σενάρια, ενώ άλλα μπορεί να εστιάζουν στην προσομοίωση ενός συγκεκριμένου Threat Actor ή APT Group. Στο πρώτο μέρος αυτού του κεφαλαίου θα διεξαχθούν πειράματα στον DetectioLab που έχουν στόχο την προσομοίωση των TTPs του APT-29 μέσω ενός PowerShell script που έχει σχεδιαστεί ακριβώς για αυτό το σκοπό.

Η ομάδα Cozy Bear, γνωστή και ως APT29, είναι ένα APT group με χώρα προέλευσης και βάση τη Ρωσία όπου υπάρχουν ενδείξεις ότι ενεργεί για λογαριασμό των Ρωσικών Υπηρεσιών Πληροφοριών. Η δράση του group ξεκίνησε το 2008 οπότε και εξαπολύει τις πρώτες επιθέσεις, συχνά ενάντια σε κυβερνητικές υποδομές κρατών της ΕΕ ή του NATO, ερευνητικά ινστιτούτα ή “think tanks”. Ένα από τα ιδιαίτερα χαρακτηριστικά του mondus operandi του συγκεκριμένου group είναι η ικανότητα της διατήρησης της πρόσβασης (persistence) στα παραβιασμένα συστήματα αλλά και οι επανειλημμένες προσπάθειες για την επανάκτηση της πρόσβασης σε στόχους που είχε χαθεί η πρόσβαση. Τον Απρίλιο του 2021 οι κυβερνήσεις των ΗΠΑ και του Ηνωμένου Βασιλείου σε ανεξάρτητές τους ανακοινώσεις συσχέτισαν την επίθεση εφοδιαστικής αλυσίδας στη SolarWinds με το συγκεκριμένο group [12].

Το Invoke-APT29 PowerShell script δίνει τη δυνατότητα για τη γρήγορη και εύκολη διεξαγωγή των TTPs που σχετίζονται με τις επιθέσεις του APT29 (Cozy Bear). Αξιοποιεί Atomic Tests από το Atomic Red Team tool που παρουσιάστηκε σε προηγούμενο κεφάλαιο μαζί με άλλες custom made τεχνικές εστιασμένες στον τρόπο ενέργειας και συμπεριφοράς του APT29. [69]

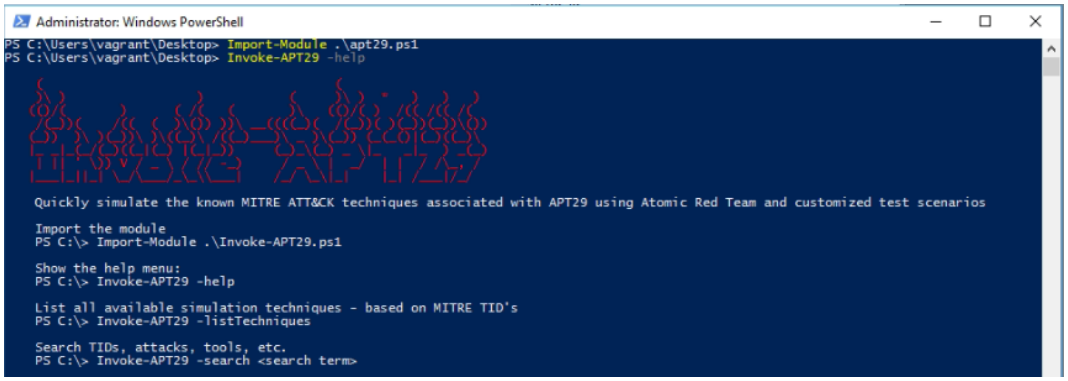
Η χρήση του είναι ιδιαίτερα εύκολη και απλή και παρουσιάζεται συνοπτικά παρακάτω.

Εισαγωγή του Powershell module

```
PS C:\> Import-Module .\\apt29.ps1
```

Προβολή του Menu

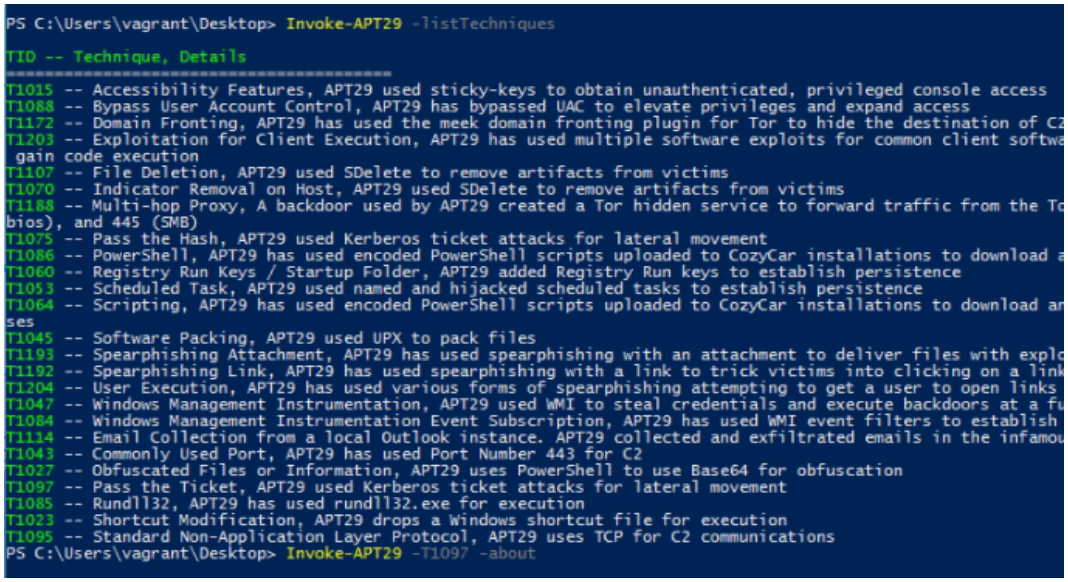
```
PS C:\> Invoke-APT29 -help
```



Εικόνα 57. Εισαγωγή του Powershell Module

Προβολή των TTPs σύμφωνα με τα MITRE ATT&CK TID's

```
PS C:\> Invoke-APT29 -listTechniques
```



Εικόνα 58. Προβολή των διαθέσιμων TTPs

Προβολή των λεπτομερειών μιας τεχνικής και των διαθέσιμων variants

```
PS C:\> Invoke-APT29 -<MITRE TID> -listVariants
```

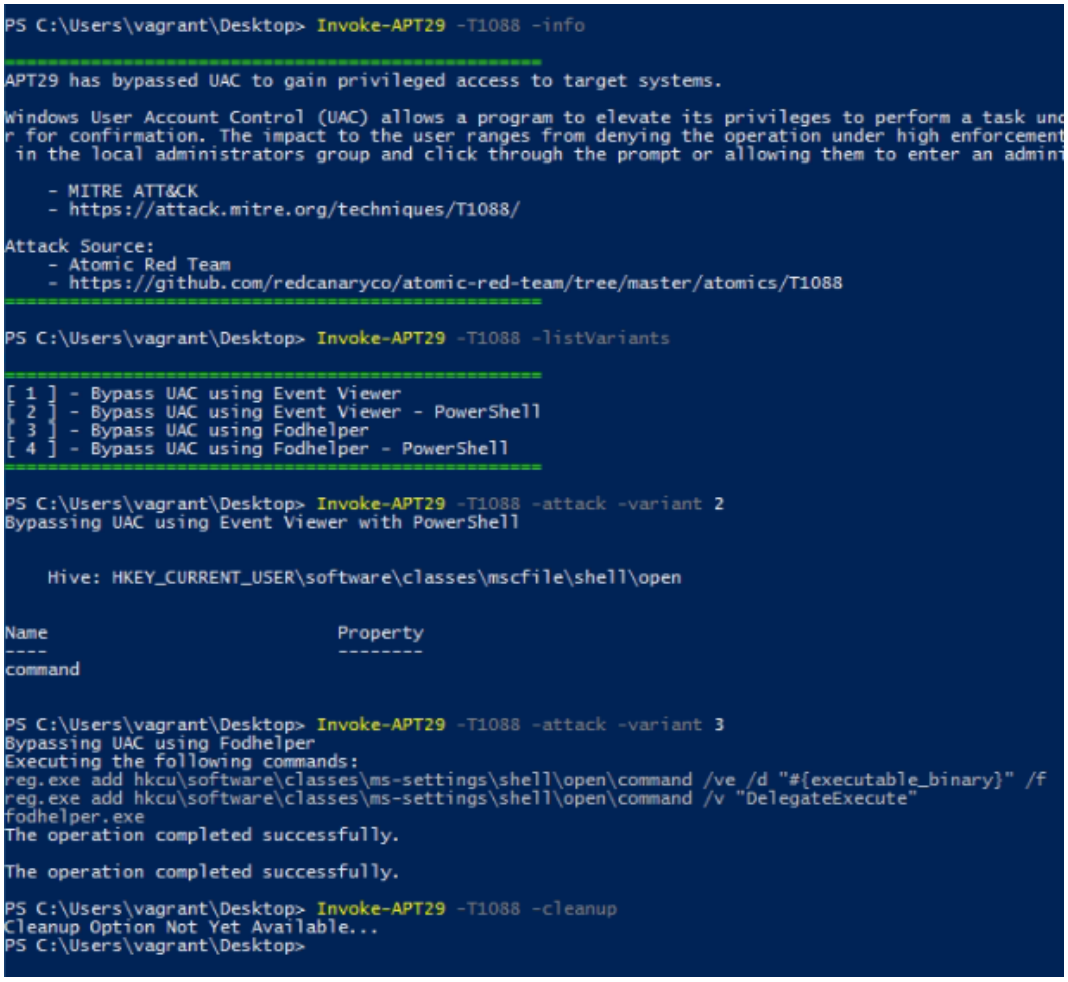
Εκτέλεση συγκεκριμένης επίθεσης με επιλεγμένη μέθοδο

```
PS C:\> Invoke-APT29 -<MITRE TID> -attack -variant <number>
```

Διεξαγωγή cleanup εφόσον είναι διαθέσιμο για τη συγκεκριμένη επίθεση

```
PS C:\> Invoke-APT29 -<MITRE TID> -cleanup
```

Εικόνα 59. Πληροφορίες για Technique -T1097 (Pass the Ticket)



Εικόνα 60. Διεξαγωγή πειραμάτων με Invoke-APT29

7.2 Διεξαγωγή πειραμάτων με Atomic Red Team

Όπως παρουσιάστηκε και σε προηγούμενο κεφάλαιο, το Atomic Red Team είναι ένα δημοφιλές εργαλείο για Adversary Emulation που παρέχει τη δυνατότητα εκτέλεσης scripted atomic test, δηλαδή αυτοματοποιημένων TTPs που είναι σχεδιασμένα έτσι ώστε να εκτελούνται με μια απλή εντολή [59]. Το Atomic Red Team, παρά το γεγονός ότι δεν εστιάζει στο Adversary Emulation συγκεκριμένων APT Group και δεν παρέχει έτοιμα templates, είναι πολύ εύκολο να χρησιμοποιηθεί

τόσο για Ad-Hoc Adversary Emulation Plans όσο και για συγκεκριμένα APTs. Συνεπώς, όπως και με τη χρήση InvokeAPT-29 έτσι το Atomic Red Team είναι εφικτή και πολύ εύκολη η προσομοίωση του APT29 εφόσον το MITRE ATT&CK framework παρέχει ξεκάθαρο mapping στα TTPs του όπως φαίνεται και στην παρακάτω εικόνα.

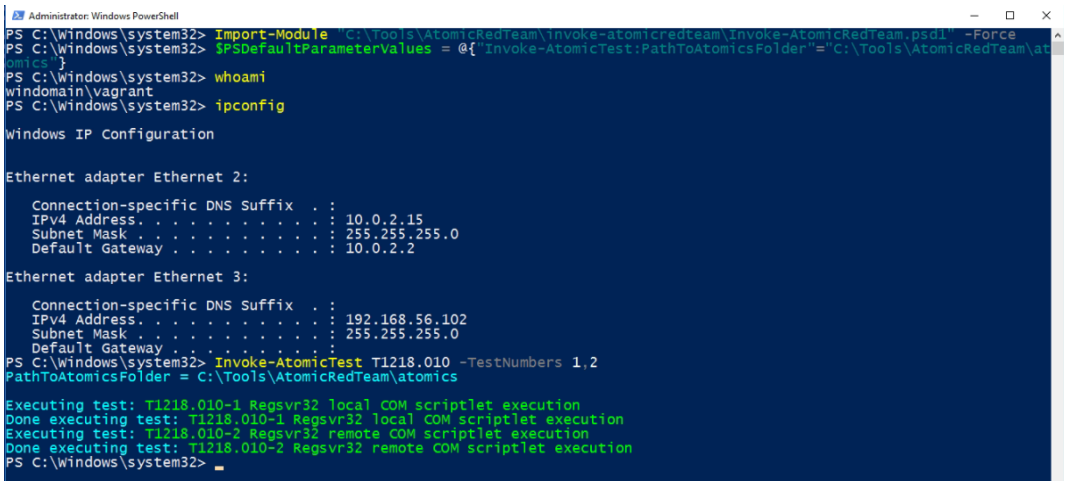
Techniques Used

ATT&CK® Navigator Layers

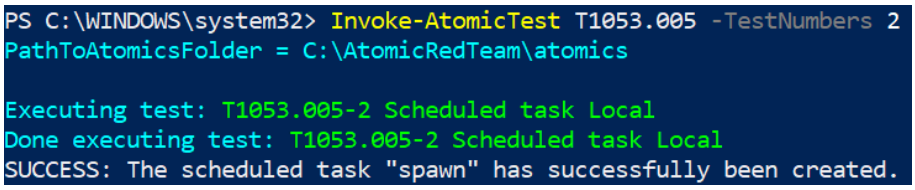
Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	APT29 has bypassed UAC.[24]
Enterprise	T1087		Account Discovery	APT29 obtained a list of users and their roles from an Exchange server using `Get-ManagementRoleAssignment`.[12]
		.002	Domain Account	APT29 has used PowerShell to discover domain accounts by executing `Get-ADUser` and `Get-DGroupMember`.[17][14]
		.004	Cloud Account	APT29 has conducted enumeration of Azure AD accounts.[25]
Enterprise	T1098	.001	Account Manipulation: Additional Cloud Credentials	APT29 has added credentials to OAuth Applications and Service Principals.[26][17]
		.002	Account Manipulation: Additional Email Delegate Permissions	APT29 added their own devices as allowed IDs for active sync using `Set-CASMailbox`, allowing it to obtain copies of victim mailboxes. It also added additional permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals.[12][26][25]
		.003	Account Manipulation: Additional Cloud Roles	APT29 has granted `company administrator` privileges to a newly created service principal.[17]
		.005	Account Manipulation: Device Registration	APT29 registered devices in order to enable mailbox syncing via the `Set-CASMailbox` command.[12]

Εικόνα 61. APT29 TTPs mapped στο MITRE ATT&CK Framework

Το Atomic Red Team έρχεται προεγκατεστημένο στο DetectionLab και για την χρήση του αρκεί η χρήση των παρακάτω εντολών όπως φαίνεται και στην εικόνα.



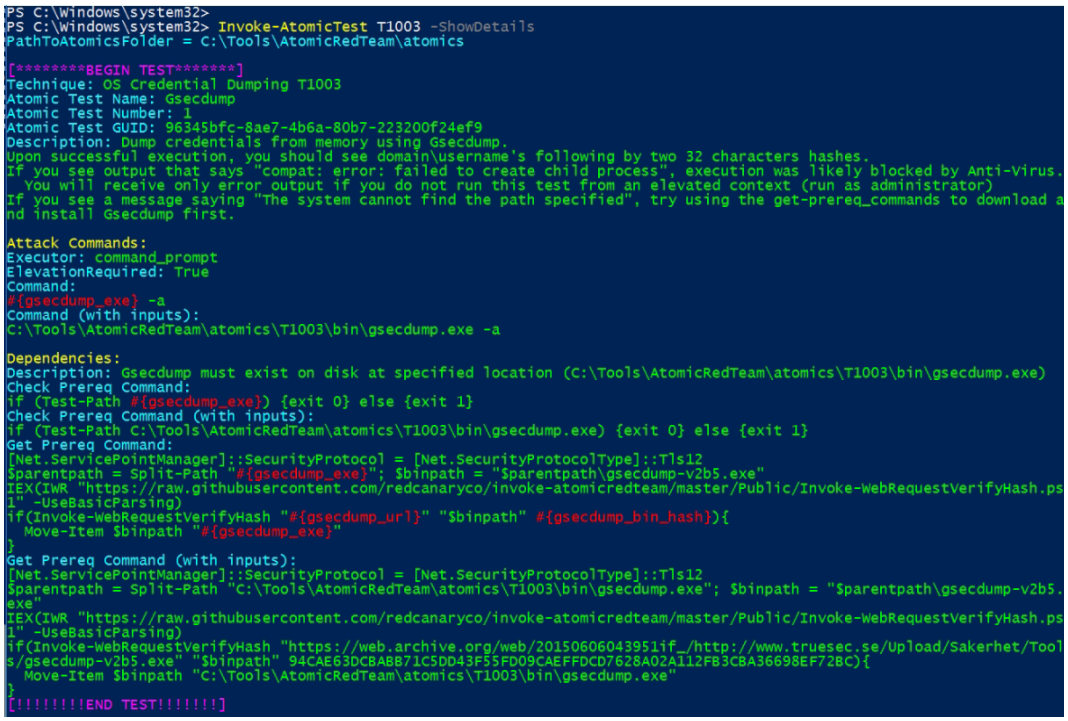
Εικόνα 62. Εισαγωγή Atomic Red Team και εκτέλεση πειραμάτων



Εικόνα 63. Ενδεικτική χρήση Atomic Red Team - Scheduled Task/Job: Scheduled Task

Η ίδια διαδικασία θα ήταν αρκετά πιο περιπλοκή και χρονοβόρα να εκτελεστεί χρησιμοποιώντας Red Teaming (C2) Frameworks. Συνεπώς το Atomic Red Team είναι ιδιαίτερα χρήσιμο καθώς, πέρα από την ευκολία χρήσης του, παρέχει διαθέτει και μεγάλη κάλυψη στα techniques που

συμπεριλαμβάνονται στο MITRE ATT&CK Framework. Επιπλέον, τα Atomic Tests εκτελούνται κατευθείαν στο κάθε host machine, χωρίς να απαιτούν την εγκατάσταση ενός C2 agent/server ή την εκτέλεση προσαρμοσμένου payload.

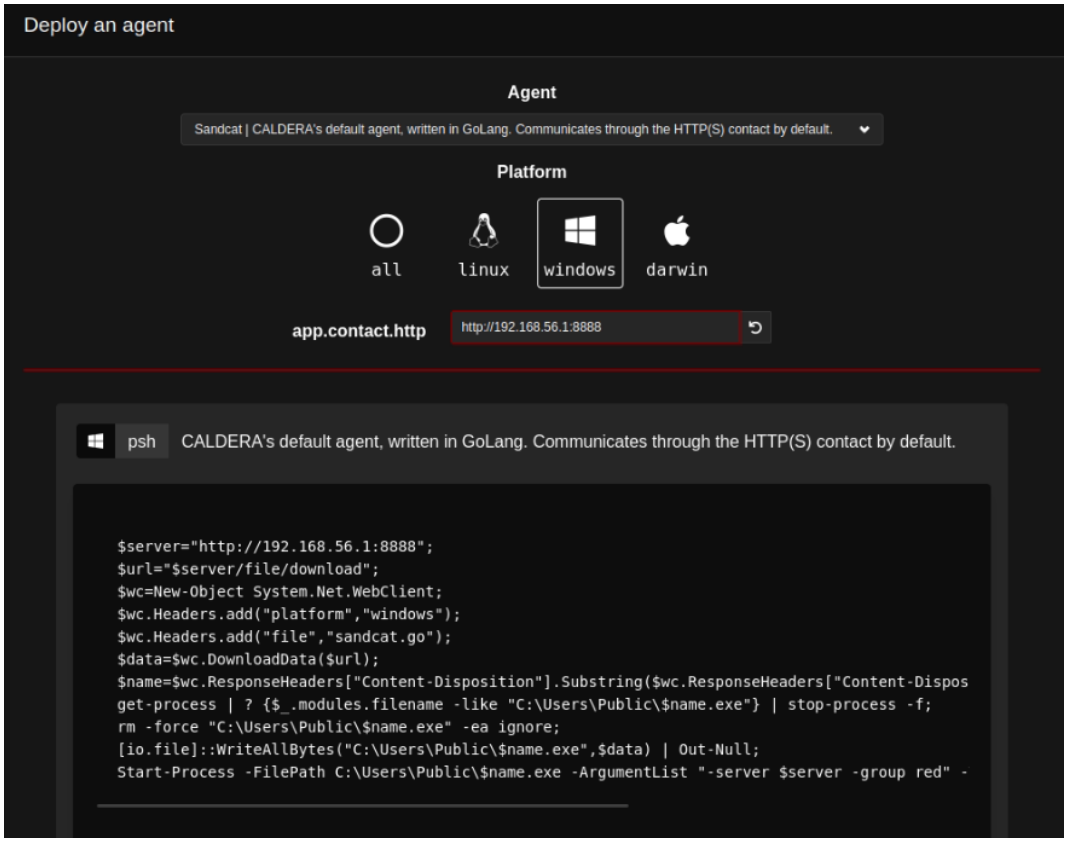


Εικόνα 64. Προβολή λεπτομερειών Technique T1003 (OS Credential Dumping)

7.3 Διεξαγωγή πειραμάτων με Caldera

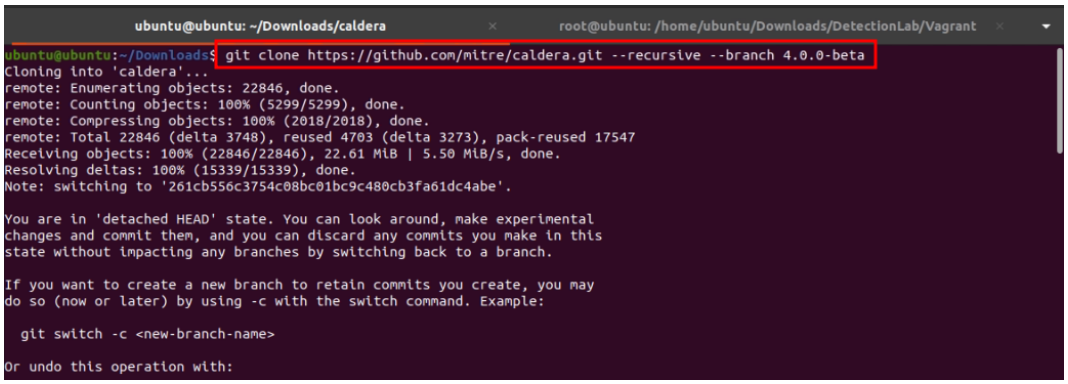
Όπως παρουσιάστηκε και σε προηγούμενο κεφάλαιο, το CALDERA (Cyber Adversary Language & Decision Engine) είναι ένα Framework που σχεδιάστηκε ώστε να παρέχει την δυνατότητα εκτέλεσης breach & simulation ασκήσεων με αυτοματοποιημένο τρόπο. Συνεπώς, είναι ιδανικό για χρήση σε περιπτώσεις Adversary Emulation, όπου υπάρχουν ανάγκες για αυτοματοποίηση και ελαχιστοποίησης των χειροκίνητων βημάτων που πρέπει να πραγματοποιηθούν [62, 63, 64]. Το Caldera μπορεί να χρησιμοποιηθεί τόσο για την προσομοίωση ενός συγκεκριμένου APT group όσο και για το σχεδιασμό custom-made adventure emulation plans που επιτρέπει το συνδυασμό πολλών τεχνικών ταυτόχρονα ώστε να σχεδιαστεί και να εκτελεστεί ένα ολοκληρωμένο adversary emulation test αυτόματα. Υπάρχουν προσχεδιασμένα έτοιμα σενάρια αλλά μπορούν να δημιουργηθούν και προσαρμοσμένα, ανάλογα με τις ανάγκες του κάθε engagement.

Σε αντίθεση με τα υπόλοιπα εργαλεία που χρησιμοποιούν scripted atomic tests, το Caldera χρησιμοποιεί C2 agent που πρέπει να εκτελεστεί στον host όπου θα διεξαχθούν τα πειράματα. Όπως φαίνεται και στην παρακάτω εικόνα, παρέχονται διαφορετικοί τύποι agent, ανάλογα με το λειτουργικό σύστημα που θα εκτελεστεί. Εφόσον παρακάτω κώδικας εκτελεστεί στον Windows Host του DetectionLab, έπειτα θα είναι εφικτή η αποστολή εντολών για την εκτέλεση συγκεκριμένων TTPs.



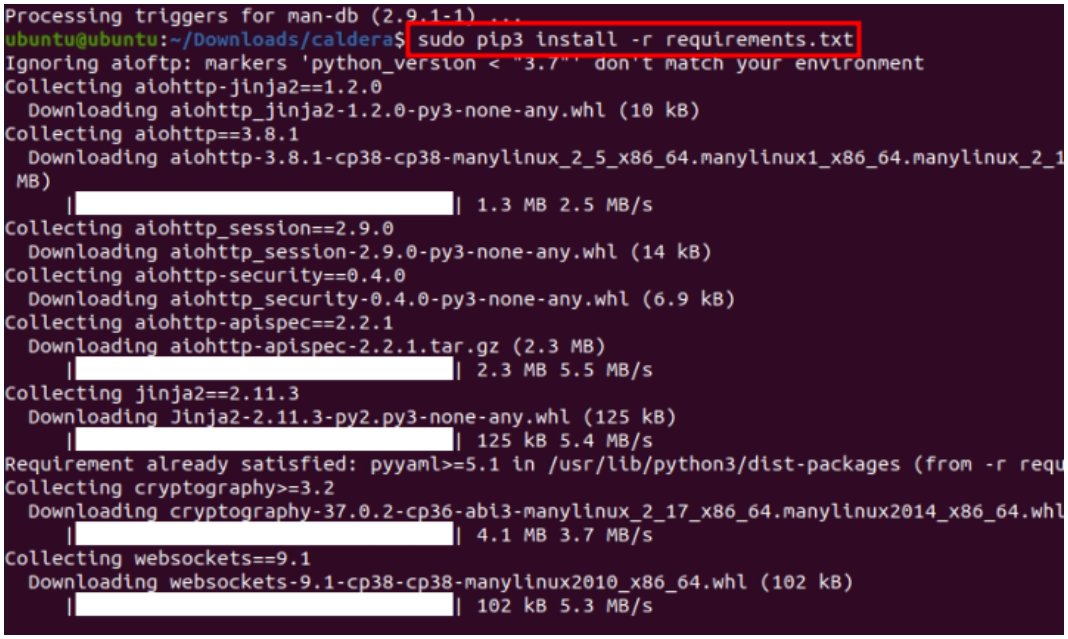
Εικόνα 65. Caldera C2 Agent

Το Caldera δεν έρχεται προεγκατεστημένο στο DetectionLab, οπότε θα πρέπει να εγκατασταθεί χειροκίνητα. Το πρώτο βήμα για την εγκατάσταση είναι το clone του repository από το GitHub.



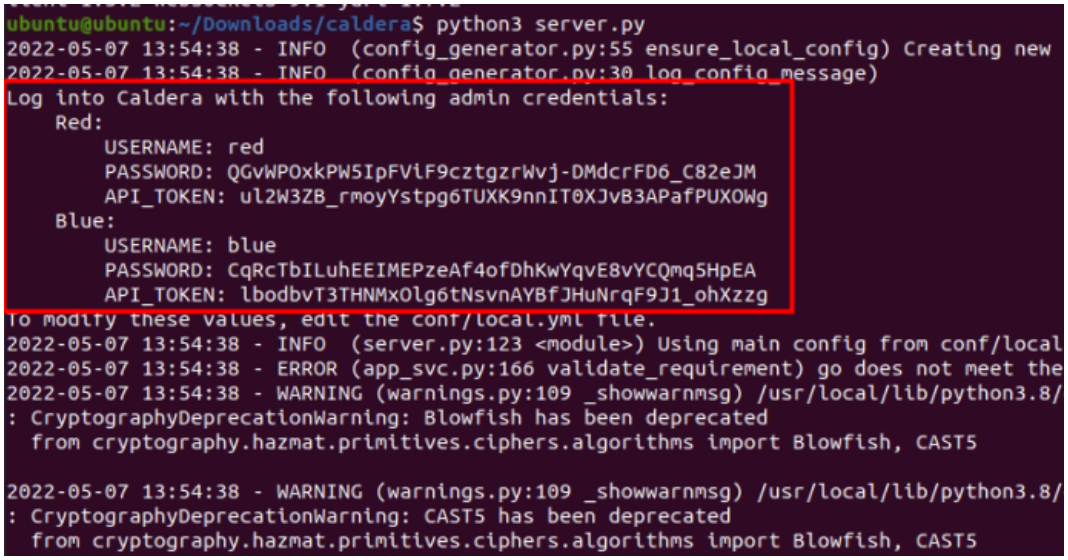
Εικόνα 66. Λήψη Caldera απο Github repo

Στη συνέχεια γίνεται η εγκατάσταση των Python dependencies.



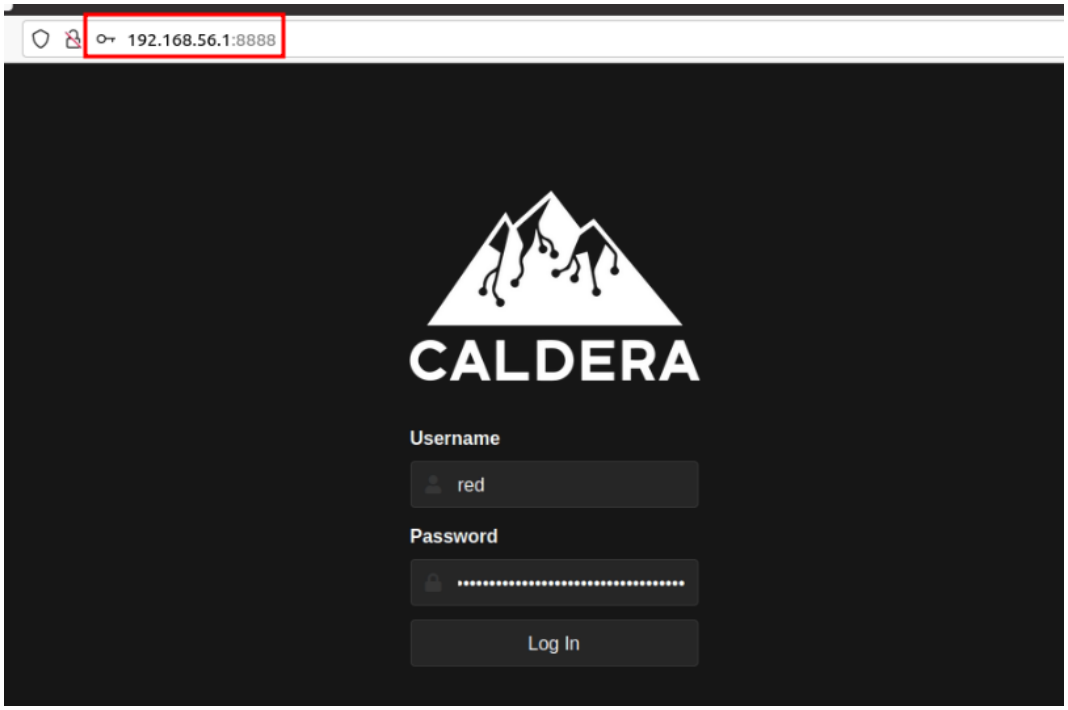
Εικόνα 67. Caldera - Εγκατάσταση dependencies

Αφού ολοκληρωθεί η εγκατάσταση των Python dependencies και εκτελεστεί το αρχείο server.py που εκκινεί τον Caldera web server, εμφανίζονται και στο terminal τα administration credentials.



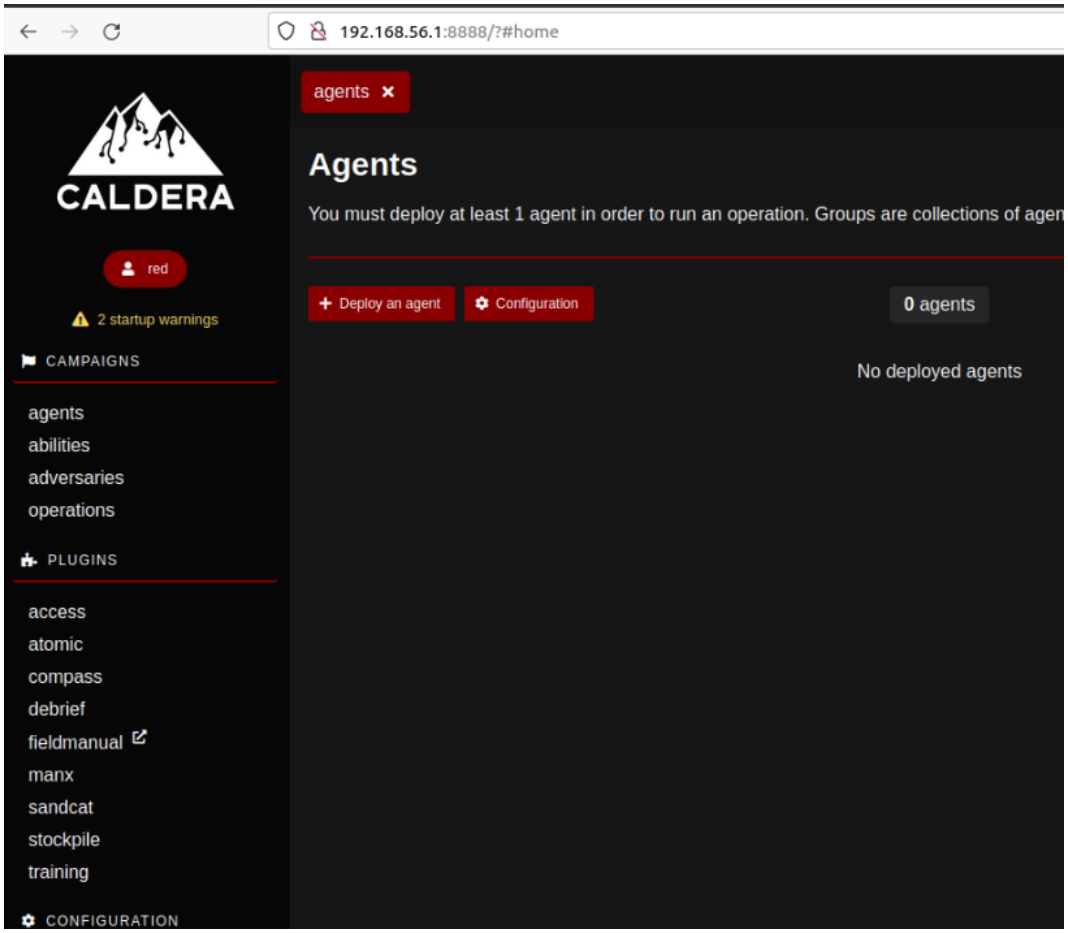
Εικόνα 68. Caldera - Εκκίνηση server και απόκτηση credential

Έπειτα στην τοπική διεύθυνση IP και στο Port 8888 είναι διαθέσιμο το web interface διαχείρησης του Caldera.



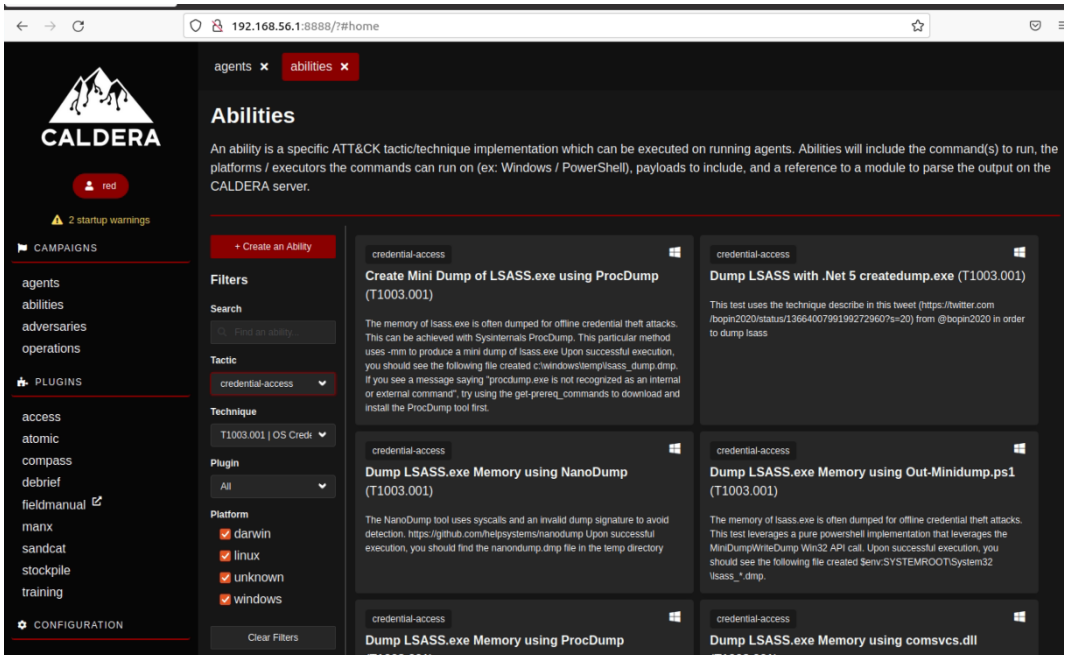
Εικόνα 69. Caldera - Web Interface

Αφού πραγματοποιηθεί σύνδεση με τα administrator credentials, εμφανίζεται το κεντρικό menu διαχείρισης.



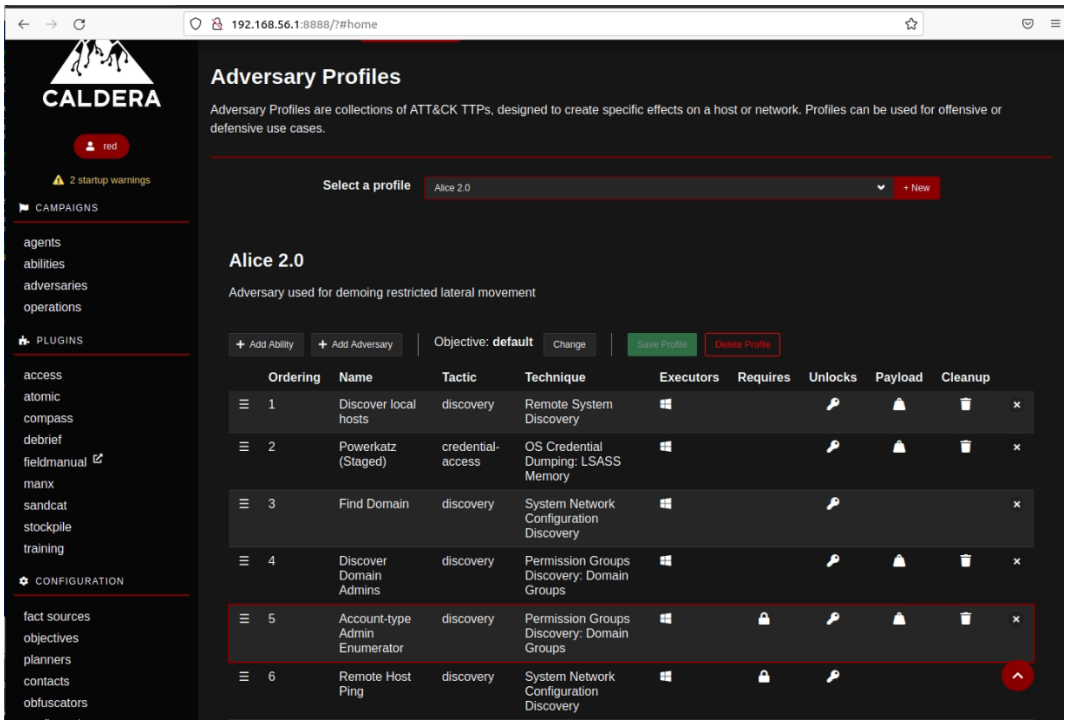
Εικόνα 70. Caldera - Κεντρικό Interface ως Red User

Το Caldera ονομάζει τα MITRE ATTCK Techniques ως “Abilities”.



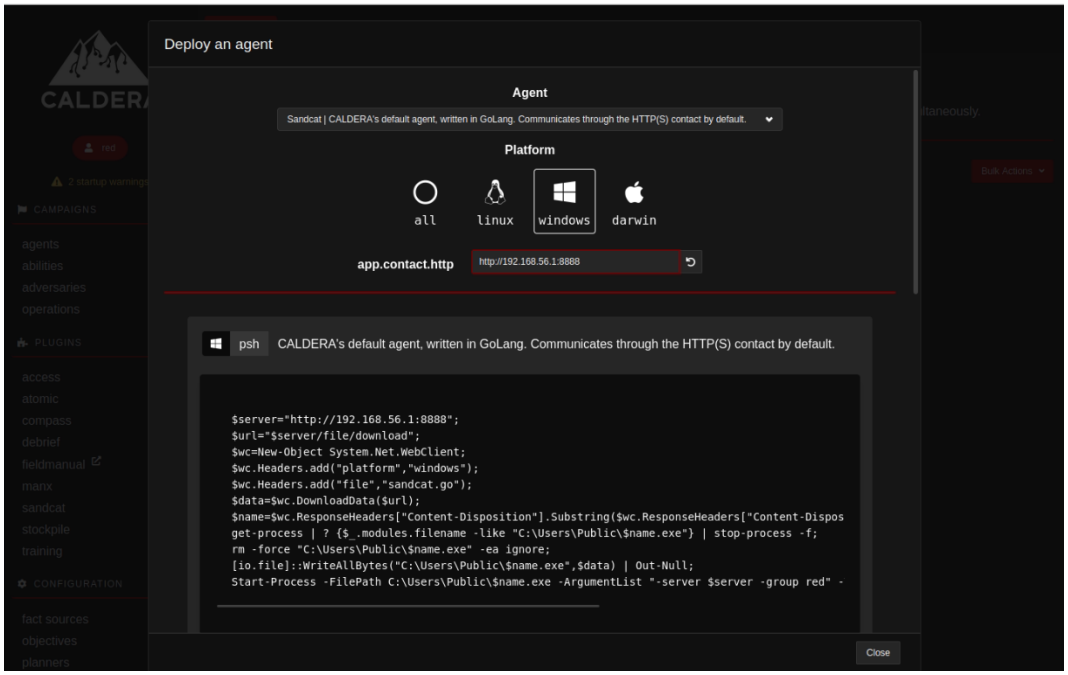
Εικόνα 71. Caldera - Abilities

Επιπλέον το Caldera διαθέτει προκαθορισμένα templates που τα ονομάζει adversary profiles τα οποία είναι μικρά Adversary Emulation plans, καθώς περιλαμβάνουν μια σειρά από προκαθορισμένα TTPs που θα εκτελεστούν αυτόματα στον host που έχει εκτελεστεί ο C2 Agent.



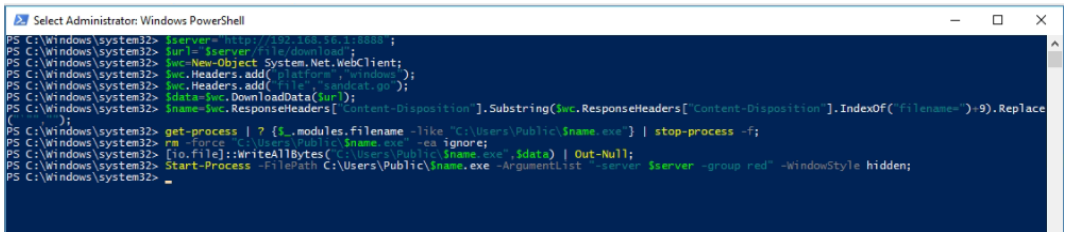
Εικόνα 72. Caldera - Adversary Profiles

Στην προκειμένη περίπτωση, εφόσον το DetectionLab αποτελείται από Windows hosts, θα δημιουργηθεί ένας Powershell Windows Agent που θα εκτελεστεί στο windows host machine.



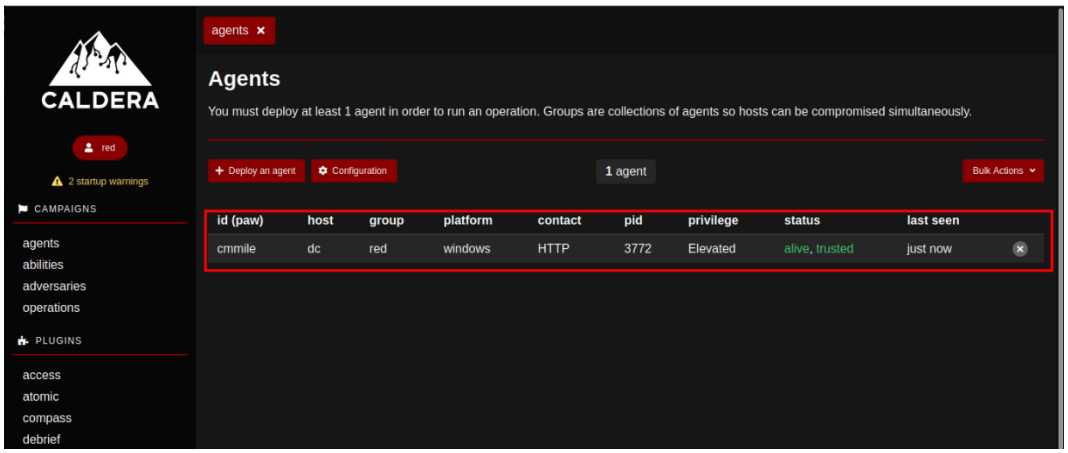
Εικόνα 73. Caldera - Δημιουργία Windows Agent

Για την εκτέλεση του agent αρκεί να εκτελεστεί ο κώδικας του παρέχει το Caldera σε ένα PowerShell terminal.



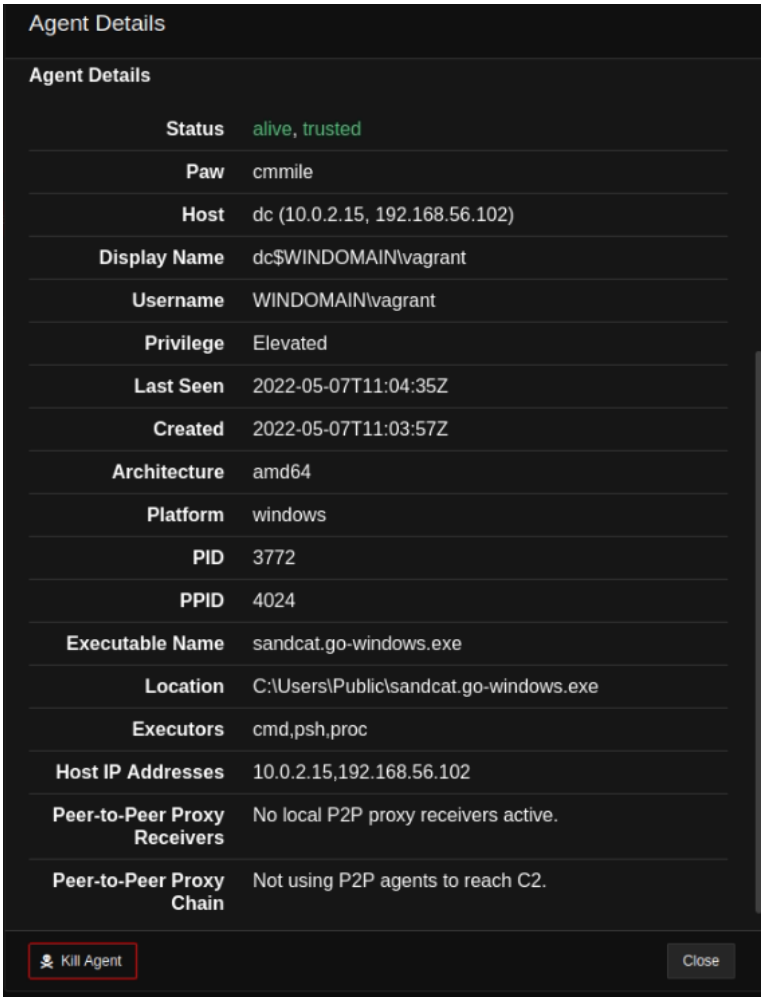
Εικόνα 74. Caldera - Εκτέλεση Agent σε Windows host

Μερικά δευτερόλεπτα αφότου εκτελεστεί η εντολή στην καρτέλα agents του Caldera εμφανίζεται ο πρώτος agent που στην ουσία δεν είναι τίποτα άλλο από την ενεργή σύνδεση που επιτρέπει στο Καλντέρα να στέλνει τα επιθυμητά TTPs προς εκτέλεση στο Windows host.



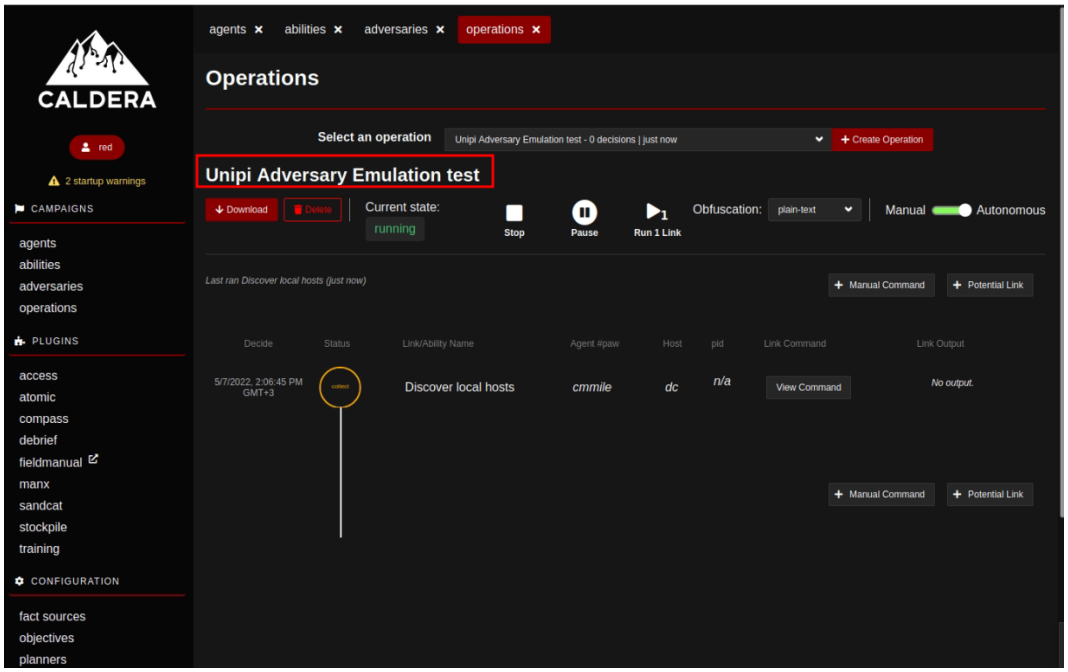
Εικόνα 75. Caldera - Εμφάνιση ενεργού agent

Αφού εκτελεσθεί ο Agent, μπορούμε να δούμε και αναλυτικότερα στοιχεία για τον compromised host, όπως τη διεύθυνση IP, τον χρήστη των Windows, τα δικαιώματα που διαθέτει, το χρόνο εκτέλεσης, την αρχιτεκτονική του λειτουργικού συστήματος, το process ID και άλλες χρήσιμες πληροφορίες.

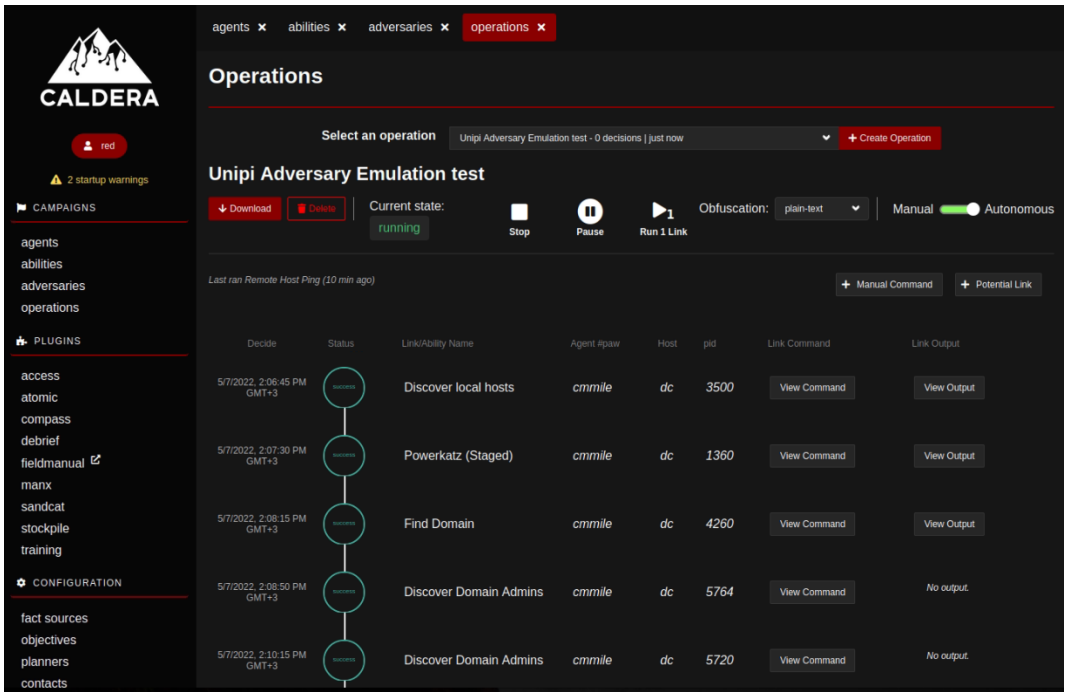


Εικόνα 76. Caldera - Πληροφορίες agent

Στην καρτέλα operations είναι εφικτή η δημιουργία ενός operation προς εκτέλεση που στην ουσία είναι Emulation Plan με πολλαπλά βήματα. Όπως φαίνεται στις παρακάτω εικόνες ένα ολοκληρωμένο Emualtion Plan εκτελέσθηκε αυτόματα και επιτυχώς στον host.

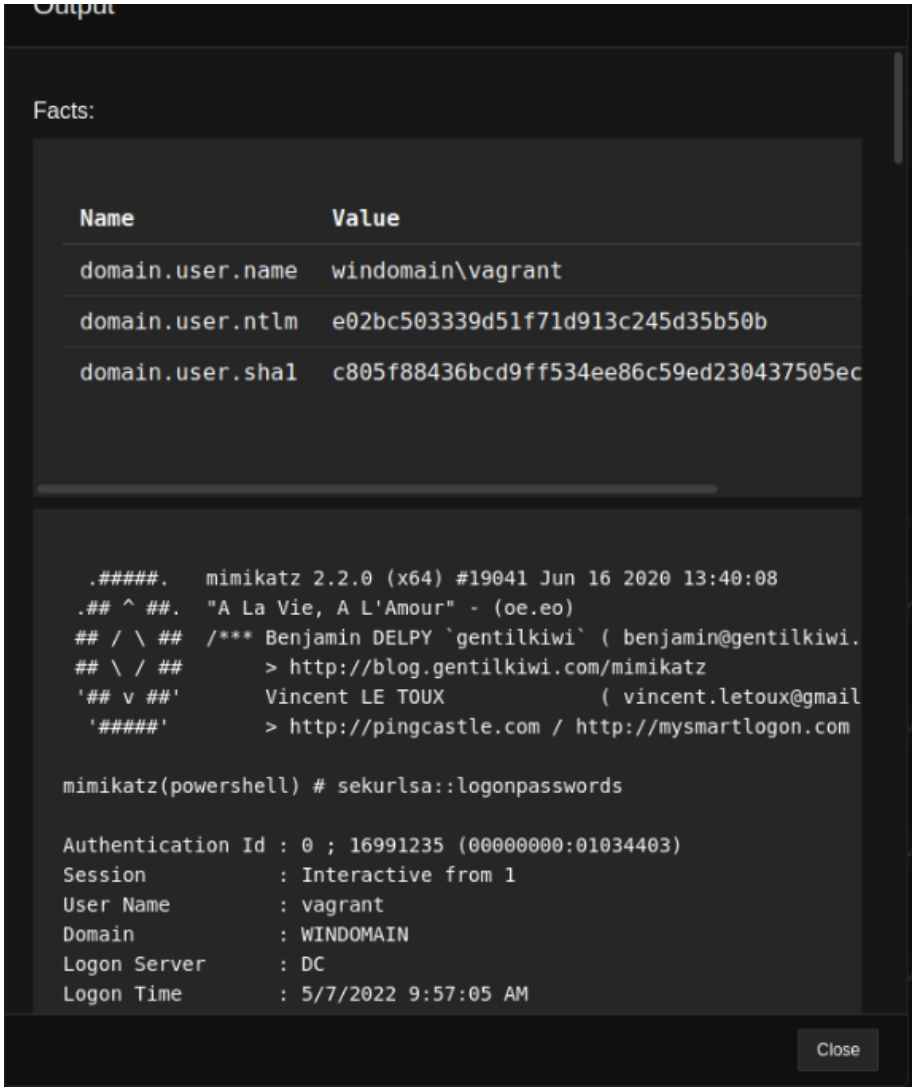


Εικόνα 77. Caldera - Adversary Emulation test



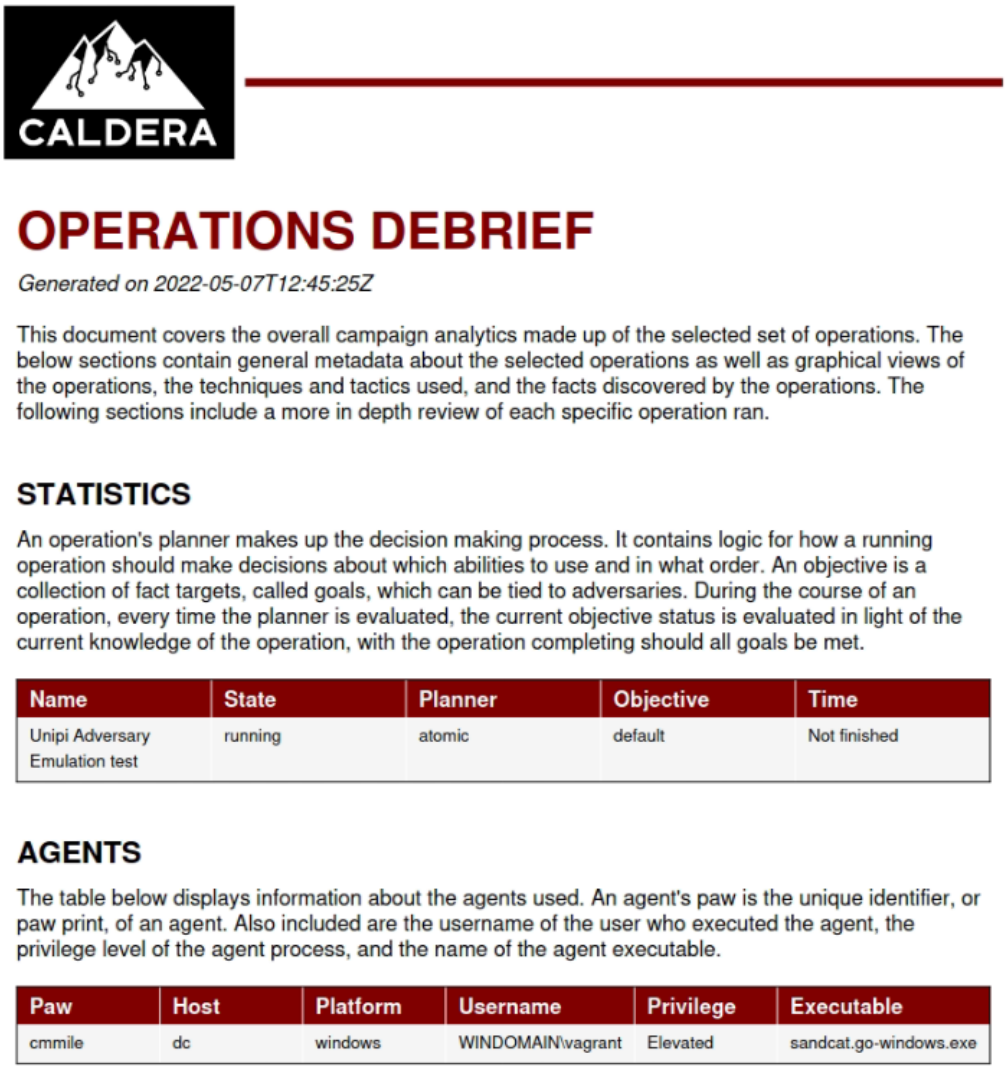
Εικόνα 78. Caldera - Adversary Emulation test ολοκλήρωση

Σε κάθε βήμα που εκτελείται εντός συγκεκριμένου operation μπορεί να προβληθούν όχι μόνον εντολές που εκτελέσθηκαν αλλά και το output που προέκυψε από τη συγκεκριμένη ενέργεια.



Εικόνα 79. Caldera - Προβολή output από συγκεκριμένο action

Επιπλέον, το Caldera διαθέτει πολλές άλλες δυνατότητες μία εκ των οποίων είναι και η δημιουργία ενός Report που περιλαμβάνει την ανάλυση του Emulation που εκτελέσθηκε και των αποτελεσμάτων που προέκυψαν.



CALDERA

OPERATIONS DEBRIEF

Generated on 2022-05-07T12:45:25Z

This document covers the overall campaign analytics made up of the selected set of operations. The below sections contain general metadata about the selected operations as well as graphical views of the operations, the techniques and tactics used, and the facts discovered by the operations. The following sections include a more in depth review of each specific operation ran.

STATISTICS

An operation's planner makes up the decision making process. It contains logic for how a running operation should make decisions about which abilities to use and in what order. An objective is a collection of fact targets, called goals, which can be tied to adversaries. During the course of an operation, every time the planner is evaluated, the current objective status is evaluated in light of the current knowledge of the operation, with the operation completing should all goals be met.

Name	State	Planner	Objective	Time
Unipi Adversary Emulation test	running	atomic	default	Not finished

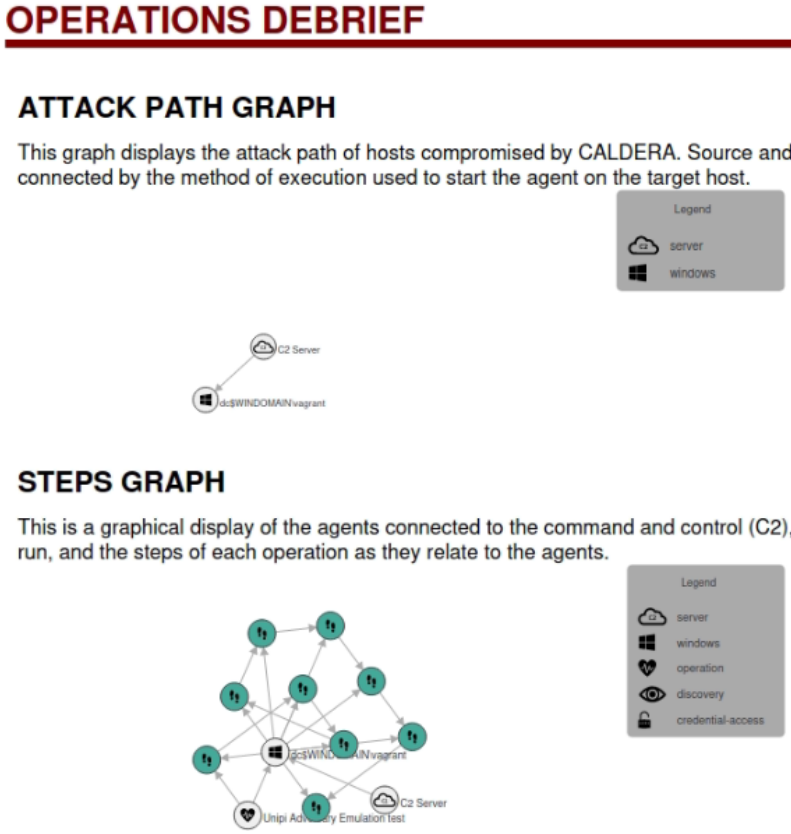
AGENTS

The table below displays information about the agents used. An agent's paw is the unique identifier, or paw print, of an agent. Also included are the username of the user who executed the agent, the privilege level of the agent process, and the name of the agent executable.

Paw	Host	Platform	Username	Privilege	Executable
cmmile	dc	windows	WINDOMAIN\vagrant	Elevated	sandcat.go-windows.exe

Εικόνα 80. Caldera - Εξαγωγή Report - Operation Debrief

Όπως φαίνεται και στις παρακάτω εικόνες, αναλύονται τα Attack Paths και όλα τα βήματα που εκτελέσθηκαν για την επίτευξη του στόχου, σε συνδυασμό με τις εντολές που χρησιμοποιήθηκαν, και κατά πόσο εκτελέστηκαν επιτυχώς.



Εικόνα 81. Caldera - Εξαγωγή Report - Attack Path

OPERATIONS DEBRIEF

STEPS IN OPERATION UNIPI ADVERSARY EMULATION TEST

The table below shows detailed information about the steps taken in an operation and whether the command run discovered any facts.

Time	Status	Agent	Name	Command	Facts
2022-05-07 T11:07:30Z	success	cmmile	Discover local hosts	Import-Module .\powerview.ps1;Get-DomainComputer	Yes
2022-05-07 T11:08:14Z	success	cmmile	Powerkatz (Staged)	Import-Module .\invoke-mimi.ps1;Invoke-Mimikatz -DumpCreds	Yes
2022-05-07 T11:08:47Z	success	cmmile	Find Domain	nbtstat -n	Yes
2022-05-07 T11:10:15Z	success	cmmile	Discover Domain Admins	Import-Module .\powerview.ps1;Get-NetLocalGroupMember -ComputerName win10.windomain.local	No
2022-05-07 T11:10:48Z	success	cmmile	Discover Domain Admins	Import-Module .\powerview.ps1;Get-NetLocalGroupMember -ComputerName wef.windomain.local	No
2022-05-07 T11:11:22Z	success	cmmile	Discover Domain Admins	Import-Module .\powerview.ps1;Get-NetLocalGroupMember -ComputerName dc.windomain.local	Yes
2022-05-07 T11:12:11Z	success	cmmile	Remote Host Ping	ping win10.windomain.local	Yes
2022-05-07 T11:12:51Z	success	cmmile	Remote Host Ping	ping wef.windomain.local	Yes
2022-05-07 T11:13:42Z	success	cmmile	Remote Host Ping	ping dc.windomain.local	Yes

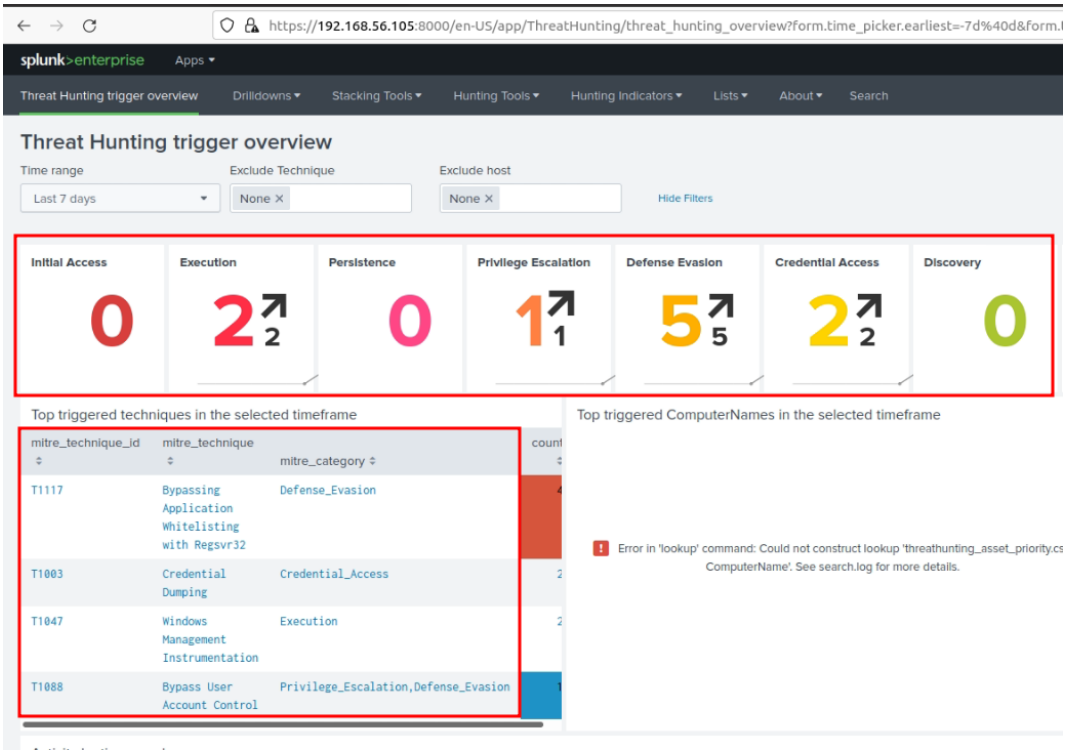
Εικόνα 82. Caldera - Εξαγωγή Report - Βήματα που εκτελέστηκαν

Κεφάλαιο 8

Συλλογή αποτελεσμάτων Emulation

Όπως αναφέρθηκε στην εισαγωγή αλλά και σε προηγούμενα κεφαλαία, ο σκοπός της εργασίας αυτής δεν είναι η διεξαγωγή και η παρουσίαση ενός ad-hoc σεναρίου Threat Hunting και Adversary Emulation βασισμένο στο MITRE ATT&CK Framework. Το επιδιωκόμενο αποτέλεσμα είναι η βελτίωση της ικανότητας της Blue Team, συνδυάζοντας Threat Intelligence, Threat Hunting, Adversary Emulation και το MITRE ATT&CK Framework, να εντοπίζει και να αντιμετωπίζει εξελιγμένους επιτιθέμενους. Κάθε οργανισμός έχει διαφορετικές ανάγκες, προτεραιότητες και προβλήματα προς επίλυση καθώς δεν θα στοχευθεί από τους ίδιους Threat Actors. Επιπλέον, διαθέτει διαφορετικό επίπεδο οργάνωσης και ωριμότητας σε θέματα ασφάλειας, διαφορετική τοπολογία δικτύου και αξιοποιεί διαφορετικά Security Solutions. Τέλος, η κάθε Blue Team, ανάλογα τον οργανισμό, μπορεί να διαθέτει διαφορετικές ικανότητες ή περιορισμούς και η ύπαρξη μιας Red ή Purple Team εντός του ίδιου οργανισμού να μην είναι πάντα δεδομένη. Κατά αυτόν τον τρόπο μια προκαθορισμένη λύση ή η παρουσίαση ενός συγκεκριμένου σεναρίου δεν θα παρείχε κάποιο ιδιαίτερο όφελος προς κάθε Blue Team.

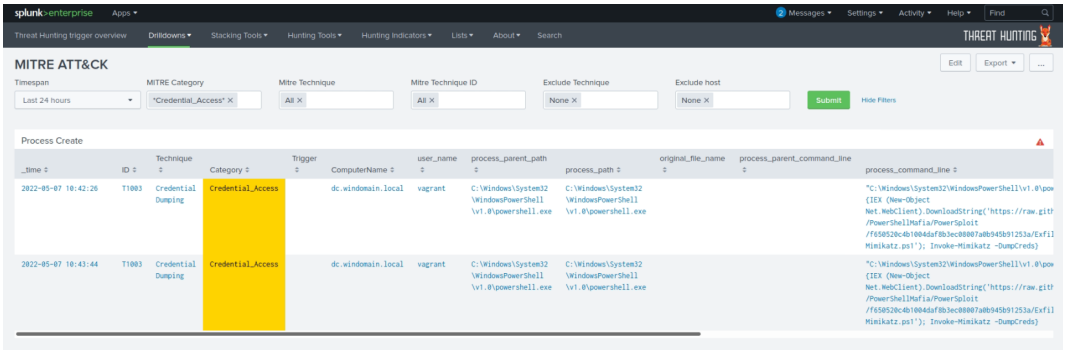
Λαμβάνοντας υπόψιν τα παραπάνω, η εργασία σχεδιάστηκε έτσι ώστε να μην εστιάζει στην αναπαραγωγή ενός συγκεκριμένου Adversary Emulation Plan. Κατά αντιστοιχία σε αυτό το κεφάλαιο δεν θα διεξαχθεί συγκεκριμένο σενάριο Threat Hunting. Το κεφάλαιο εστιάζει στην παρουσίαση μιας high-level προσέγγισης στην συλλογή και στην επισκόπηση των αποτελεσμάτων με στόχο την ανάδειξη της αξίας διεξαγωγής της διαδικασίας αυτής, ασχέτως του Adversary, των TTPs, των Security εργαλείων, του SIEM κτλ. Κατά αυτόν τον τρόπο, η μεθοδολογία που προτείνεται στο επόμενο κεφάλαιο είναι ικανή να εφαρμοστεί σε κάθε περιβάλλον ανεξαρτήτως των ιδιαίτερων χαρακτηριστικών του και να βοηθήσει κάθε Blue Team να βελτιώσει σημαντικά την αποτελεσματικότητα της. Ως ενδεικτικό παράδειγμα για της ανάγκες της εργασίας γίνεται χρήση του Splunk SIEM στο DetectionLab. Μέσω του Threat Hunting extension είναι πολύ εύκολη η κατηγοριοποίηση διαφόρων σεναρίων που εκτελέστηκαν στο προηγούμενο κεφάλαιο. Όπως φαίνεται και στην εικόνα, πολλά από τα logs που παρήχθησαν κατά το Adversary Emulation έχουν δημιουργήσει τα αντίστοιχα alerts και έχουν αυτομάτως αντιστοιχηθεί πάνω στο MTRE ATT&CK Framework και σε συγκεκριμένα Techniques.



Εικόνα 83. Splunk Threat Hunting plugin - Αποτελέσματα

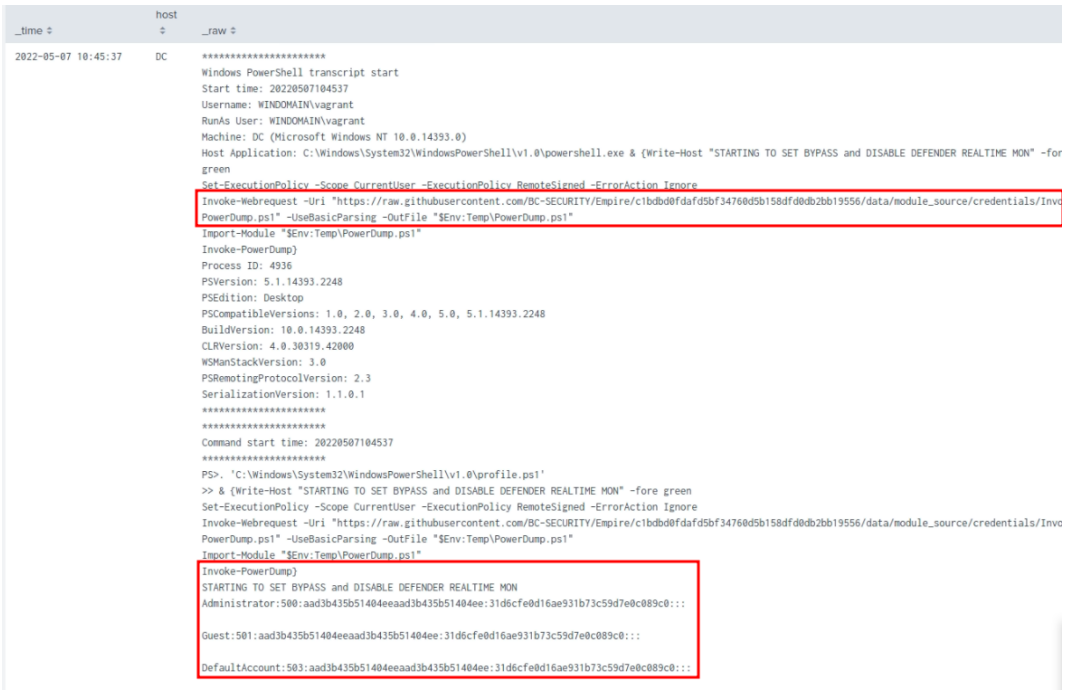
Εικόνα 84. Splunk - Δραστηριότητα που εντοπίστηκε μετά το Emulation

Επιλέγοντας μία συγκεκριμένη κατηγορία Tactic, όπως για παράδειγμα το Credential Access, εμφανίζονται τα αντίστοιχα events. Κατά αυτό τον τρόπο είναι πολύ εύκολη η συσχέτιση ενός συγκεκριμένου Technique όπως το Credential Dumping (T1003) με συγκεκριμένα logs, events, log sources και να επαληθευτεί τόσο το visibility αλλά και η ικανότητα εντοπισμού.



Εικόνα 85. Splunk - Παράδειγμα από εντοπισμένα Techniques

Για παράδειγμα τα παρακάτω logs φανερώνουν τη λήψη και την εκτέλεση ενός PowerShell script που πραγματοποιεί OS Credential Dumping.



Εικόνα 86. Splunk - Logs που σχετίζονται με Techniques απο το Emulation

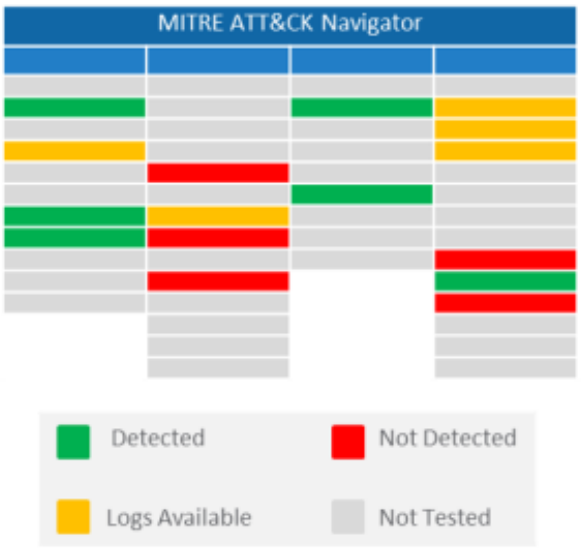
Φυσικά, αυτή η δραστηριότητα θα διαφέρει σε μεγάλο βαθμό ανάλογα το περιβάλλον, την τοπολογία του δικτύου, τα security solutions και το SIEM όπου συγκεντρώνονται τα logs, ωστόσο η λογική παραμένει η ίδια. Έπειτα από κάθε Adversary Emulation Activity, είτε αυτό είναι ένα απλό Atomic Test, είτε ένα ολόκληρο Adversary Emulation Plan, γίνεται προσπάθεια για την συλλογή των σχετικών logs έπειτα από Threat Hunting ή απλό εντοπισμό των logs μέσω του SIEM. Απώτερος στόχος είναι ο εντοπισμό των κενών στη συλλογή των logs, η επαλήθευση των μηχανισμών εντοπισμού που ήδη υπάρχουν και η δημιουργία νέων για τη δραστηριότητα που δεν εντοπίστηκε.

Κεφάλαιο 9

Αξιολόγηση αποτελεσμάτων

9.1 Σκοπός διεξαγωγής Defensive Gap / Attack Coverage Assessment

Το Defensive Gap / Attack Coverage Assessment δίνει τη δυνατότητα σε έναν οργανισμό να διαπιστώσει τα σημεία του περιβάλλοντός του που υστερούν σε αμυντικούς μηχανισμούς ή visibility. Αυτά τα κενά είναι "τυφλά σημεία" άρα και περιοχές όπου ένας επιτιθέμενος θα μπορούσε να αποκτήσει αρχική πρόσβαση και στη συνέχεια να επεκταθεί μέσα στο δίκτυο χωρίς να γίνει αντιληπτός [36]. Η λογική του Defensive GAP / Attack Coverage Assessment μπορεί να οπτικοποιηθεί μέσω της παρακάτω εικόνας που κατηγοριοποιεί τα TTPs που έγιναν Emulate κατά αντιστοιχία με το MITRE ATT&CK Framework. Με πράσινο χρώμα καταγράφονται όσα TTPs εντοπίστηκαν, με κόκκινο όσα δεν εντοπίστηκαν ούτε καταγράφηκαν σε logs, με κίτρινο όσα δεν εντοπίστηκαν αλλά η σχετική δραστηριότητα έχει καταγραφεί σε logs, συνεπώς υπάρχει visibility αλλά όχι μηχανισμός εντοπισμού, και τέλος με γκρι όσα δεν εκτελέστηκαν.

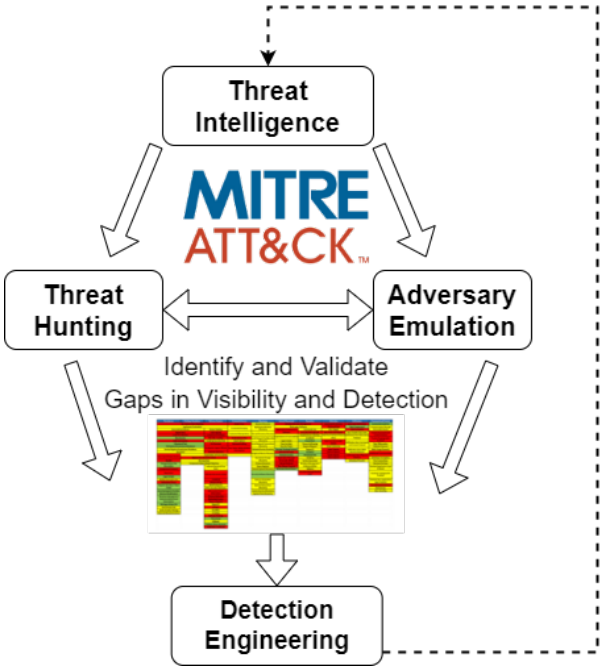


Εικόνα 87. Οπτικοποίηση Detection/Visibility στο MITRE ATT&CK Framework

Για να διεξαχθεί το συγκεκριμένο Assessment απαιτείται η αναπαραγωγή των ενεργειών του Threat Actor μέσω του Adversary Elumation και η διεξαγωγή του Threat Hunting για τη συλλογή των αποτελεσμάτων. Ένα αντίστοιχο Assessment θα μπορούσε να πραγματοποιηθεί και σε μια συνηθισμένη άσκηση Red Team με μια Ad-Hoc προσέγγιση και να δώσει κάποια αποτελέσματα. Ωστόσο στόχος αυτής της εργασίας είναι η ανάδειξη της αξίας συνδυασμού του Threat Intelligence

με Threat Hunting και Adversary Emulation για τον εντοπισμό και την επαλήθευση κενών στην ικανότητα της Blue Team να εντοπίζει δραστηριότητα συγκεκριμένων εξελιγμένων επιτιθεμένων αλλά και της δημιουργίας ενός αποτελεσματικού προγράμματος Threat Detection Engineering.

Ο συνδυασμός των παραπάνω διαδικασιών αναπαρίσταται στην παρακάτω εικόνα.



Εικόνα 88. Συνδυασμός διαδικασιών που συνεισφέρουν σε αποτελεσματικό Threat Detection Engineering

9.2 Εργαλεία διεξαγωγής Defensive GAP / Attack Coverage Assessment

Όπως και το Adversary Emulation που παρουσιάστηκε σε προηγούμενο κεφάλαιο μπορεί να πραγματοποιηθεί χωρίς τη χρήση ενός συγκεκριμένου μόνο εργαλείου, έτσι και η διεξαγωγή ενός Defensive GAP / Attack Coverage Assessment και η καταγραφή των σχετικών δεδομένων που θα παραχθούν μπορεί να πραγματοποιηθεί χωρίς κάποιο συγκεκριμένου εργαλείο. Ωστόσο, και στις δύο περιπτώσεις η αξιοποίηση εργαλείων που είναι σε ένα βαθμό αυτοματοποιημένα διευκολύνουν τη διαδικασία εξοικονομώντας χρόνο, μειώνοντας την πολυπλοκότητα και παρέχοντας επιπλέον εργαλεία που βοηθούν στην εξαγωγή ποιοτικότερων συμπερασμάτων. Η παρούσα εργασία έχει ως στόχο την παρουσίαση μιας μεθοδολογίας η οποία δεν βασίζεται σε συγκεκριμένα εργαλεία ωστόσο κάποια από αυτά θα αναφερθούν και θα παρουσιαστούν ως προτεινόμενες λύσεις. Με την πάροδο του χρόνου τα εργαλεία εξελίσσονται, βελτιώνονται, αλλάζουν ή δημιουργούνται νέα, συνεπώς μία μεθοδολογία δεν μπορεί να βασίζεται σε συγκεκριμένα εργαλεία. Κατά αυτόν τον τρόπο, όπως και στο κεφάλαιο με το Adversary Emulation, όπου αναφέρθηκαν ορισμένα εργαλεία που βοηθούν μια Blue Team να κάνει Emulate ένα APT χωρίς εξειδικευμένες γνώσεις, έτσι και στο Defensive GAP / Attack Coverage Assessment η διαδικασία μπορεί να πραγματοποιηθεί με διαφορετικούς τρόπους, ανάλογα τις ανάγκες του κάθε οργανισμού.

9.2.1 AttackCoverage SpreadSheet

Ο απλούστερη μέθοδος για την καταγραφή των αποτελεσμάτων ενός Defensive Gap / Attack Coverage Assessment είναι μέσω ενός απλού Excel spreadsheet. Πιο συγκεκριμένα, υπάρχει διαθέσιμο το AttackCoverage spreadsheet που εξυπηρετεί ακριβώς αυτό το σκοπό. Μέσω αυτού εί-

ναι πολύ εύκολη η διεξαγωγή ενός αντίστοιχου Assessment βασισμένο στο MITRE ATT&CK Framework [70]. Όπως φαίνεται και στις παρακάτω εικόνες, το spreadsheet είναι διαμορφωμένο έτσι ώστε να περιέχει όλα τα Tactics, Techniques και Procedures που θα μπορούσε να χρησιμοποιήσει ο επιτιθέμενος, έτσι ώστε να μπορεί να γίνει η καταγραφή των αποτελεσμάτων και οπτικοποίηση των δεδομένων. Κατά αυτό τον τρόπο είναι πολύ εύκολη η παρακολούθηση της πορείας των πειραμάτων και η εξαγωγή των επιθυμητών συμπερασμάτων για την κάλυψη που διαθέτει ο οργανισμός.

O	P	Q	R	S	T	U	V	W	X	Y	Z
Credential Access	**1**	**Discovery**	**0**	**Lateral Movement**	**0**	**Collection**	**0**	**Command & Control**	**1**	**Exfiltration**	0
OS Credential Dumping (T1003)		System Service Discovery (T1007)		Remote Services (T1021)		Data from Local System (T1005)		Data Obfuscation (T1001)	1	Exfiltration Over Other Network Medium (T1011)	
LSASS Memory (T1003.001)	1	Application Window Discovery (T1010)		Remote Desktop Protocol (T1021.001)		Data from Removable Media (T1025)		Junk Data (T1001.001)		Exfiltration Over Bluetooth (T1011.001)	
Security Account Manager (T1003.002)		Query Registry (T1012)		SMB/Windows Admin Shares (T1021.002)		Data from Network Shared Drive (T1039)		Steganography (T1001.002)		Automated Exfiltration (T1020)	
NTDS (T1003.003)		System Network Configuration Discovery (T1016)		Distributed Component Object Model (T1021.003)		Input Capture (T1056)		Protocol Impersonation (T1001.003)		Traffic Duplication (T1020.001)	
LSA Secrets (T1003.004)		Internet Connection Discovery (T1016.001)		SSH (T1021.004)		Keylogging (T1056.001)		Fallback Channels (T1008)		Scheduled Transfer (T1029)	
Cached Domain Credentials (T1003.005)		Remote System Discovery (T1018)		VNC (T1021.005)		GUI Input Capture (T1056.002)		Multiband Communication (T1026)		Data Transfer Size Limits (T1030)	
DCSync (T1003.006)		System Owner/User Discovery (T1033)		Windows Remote Management (T1021.006)		Web Portal Capture (T1056.003)		Commonly Used Port (T1043)		Exfiltration Over C2 Channel (T1041)	
Proc Filesystem (T1003.007)		Network Sniffing (T1040)		Shared Webroot (T1051)		Credential API Hooking (T1056.004)		Application Layer Protocol (T1071)		Exfiltration Over Alternative Protocol (T1048)	
/etc/passwd and /etc/shadow (T1003.008)		Network Service Scanning (T1046)		Software Deployment Tools (T1072)		Data Staged (T1074)		Web Protocols (T1071.001)		Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1048.001)	
Network Sniffing (T1040)		System Network Connections Discovery (T1049)		Taint Shared Content (T1080)		Local Data Staging (T1074.001)		File Transfer Protocols (T1071.002)		Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002)	
Input Capture (T1056)		Process Discovery (T1057)		Replication Through Removable Media (T1091)		Remote Data Staging (T1074.002)		Mail Protocols (T1071.003)		Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol (T1048.003)	

Εικόνα 89. Καταγραφή εντοπισμού MITRE ATT&CK TTPs σε spreadsheet 1

technique	id	name	tactics	data sources	data sources numbe	data source availabl	number of sub techniqu	detection rules for techique	detection rules for subtec	minimum detection rules	detection rules modifie	expected detection rules	detection rules	coverage	technique status
T1001	T1001	Data Obfuscation (T1001)	command-and-control	Network Traffic: Netw	1	1	3	1	0	3		3	1	33%	detect
T1001	T1001.001	Junk Data (T1001.001)	command-and-control	Network Traffic: Netw	1	1				1		1	0	0%	no detect
T1001	T1001.002	Steganography (T1001.002)	command-and-control	Network Traffic: Netw	1	1				1		1	0	0%	no detect
T1001	T1001.003	Protocol Impersonation (T1001.003	command-and-control	Network Traffic: Netw	1	1				1		1	0	0%	no detect
T1002	T1002	Data Compressed (T1002)	unspecified		0	0	0			1		1	0	0%	no sources
T1003	T1003	OS Credential Dumping (T1003)	credential-access	Process: Process Crea	9	1	8		1	8		8	1	13%	detect
T1003	T1003.001	LSASS Memory (T1003.001)	credential-access	Process: Process Crea	4	0		1		1		1	1	100%	inconsistent
T1003	T1003.002	Security Account Manager (T1003.0	credential-access	Command: Command	3	0				1		1	0	0%	no sources
T1003	T1003.003	NTDS (T1003.003)	credential-access	File: File Access|Com	2	0				1		1	0	0%	no sources
T1003	T1003.004	LSA Secrets (T1003.004)	credential-access	Windows Registry: W	2	0				1		1	0	0%	no sources
T1003	T1003.005	Cached Domain Credentials (T1003.	credential-access	Command: Command	1	0				1		1	0	0%	no sources
T1003	T1003.006	DCSync (T1003.006)	credential-access	Active Directory: Activ	3	1				1		1	0	0%	no detect
T1003	T1003.007	Proc Filesystem (T1003.007)	credential-access	Command: Command	2	0				1		1	0	0%	no sources
T1003	T1003.008	/etc/passwd and /etc/shadow (T100	credential-access	Command: Command	2	0				1		1	0	0%	no sources
T1004	T1004	Winlogon Helper DLL (T1004)	unspecified		0	0	0			1		1	0	0%	no sources
T1005	T1005	Data from Local System (T1005)	collection	Script: Script Executio	3	0	0			1		1	0	0%	no sources
T1006	T1006	Direct Volume Access (T1006)	defense-evasion	Command: Command	2	0	0			1		1	0	0%	no sources
T1007	T1007	System Service Discovery (T1007)	discovery	Process: Process Crea	2	0	0			1		1	0	0%	no sources
T1008	T1008	Fallback Channels (T1008)	command-and-control	Network Traffic: Netw	2	0	0			1		1	0	0%	no sources
T1009	T1009	Binary Padding (T1009)	unspecified		0	0	0			1		1	0	0%	no sources
T1010	T1010	Application Window Discovery (T1(	discovery	Process: Process Crea	3	0	0			1		1	0	0%	no sources
T1011	T1011	Exfiltration Over Other Network Me	exfiltration	Network Traffic: Netw	5	1	1		0	1		1	0	0%	no detect
T1011	T1011.001	Exfiltration Over Bluetooth (T1011.(	exfiltration	Network Traffic: Netw	5	1				1		1	0	0%	no detect
T1012	T1012	Query Registry (T1012)	discovery	Process: Process Crea	4	0	0			1		1	0	0%	no sources
T1013	T1013	Port Monitors (T1013)	unspecified		0	0	0			1		1	0	0%	no sources
T1014	T1014	Rootkit (T1014)	defense-evasion	Drive: Drive Modifica	2	0	0			1		1	0	0%	no sources
T1015	T1015	Accessibility Features (T1015)	unspecified		0	0	0			1		1	0	0%	no sources
T1016	T1016	System Network Configuration Disc	discovery	Process: Process Crea	4	0	1		0	1		1	0	0%	no sources
T1016	T1016.001	Internet Connection Discovery (T10	discovery	Process: Process Crea	2	0				1		1	0	0%	no sources
T1017	T1017	Application Deployment Software (	unspecified		0	0	0			1		1	0	0%	no sources
T1018	T1018	Remote System Discovery (T1018)	discovery	Process: Process Crea	4	0	0			1		1	0	0%	no sources
T1019	T1019	System Firmware (T1019)	unspecified		0	0	0			1		1	0	0%	no sources
T1020	T1020	Automated Exfiltration (T1020)	exfiltration	Command: Command	6	1	1		0	1		1	0	0%	no detect
T1020	T1020.001	Traffic Duplication (T1020.001)	exfiltration	Network Traffic: Netw	2	0				1		1	0	0%	no sources
T1021	T1021	Remote Services (T1021)	lateral-movement	Process: Process Crea	7	0	6		0	6		6	0	0%	no sources
T1021	T1021.001	Remote Desktop Protocol (T1021.00	lateral-movement	Process: Process Crea	4	0				1		1	0	0%	no sources

Εικόνα 90. Καταγραφή εντοπισμού MITRE ATT&CK TTPs σε spreadsheet 2

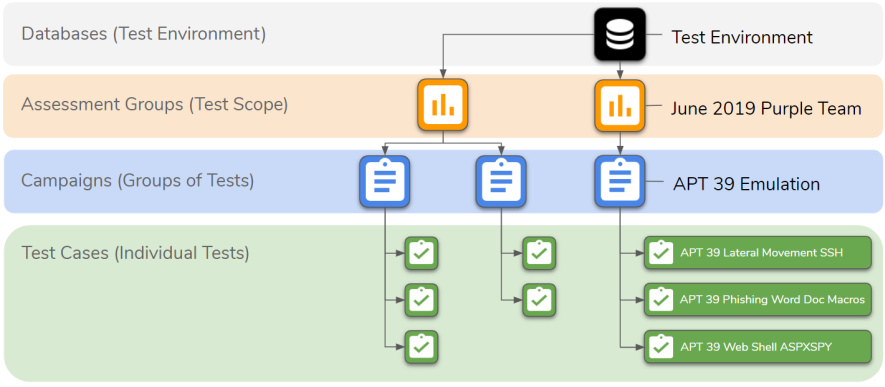
Παρά το γεγονός ότι το AttackCoverage spreadsheet μπορεί να βοηθήσει στην καταγραφή και να παρέχει μια σύνοψη των αποτελεσμάτων, δεν παύει να είναι μία λύση με πολύ περιορισμένες δυνατότητες και μειωμένη ευχρηστία. Οι περιορισμοί αυτοί μπορούν να ξεπεραστούν με τη χρήση ενός πιο εξειδικευμένου open-source και free λογισμικού όπως το VECTR που θα αναλυθεί στη συνέχεια.

9.2.2 VECTR

Εικόνα 91. VECTR Logo

Το VECTR είναι ένα εργαλείο που διευκολύνει τη διεξαγωγή ενός Defensive GAP / Attack Coverage Assessment, καθώς βοηθά στην παρακολούθηση των ενεργειών τόσο της Red όσο και της Blue Team σε μια κοινή άσκηση που περιλαμβάνει Adversary Emulation και Threat Hunting. Έχει σχεδιαστεί έτσι ώστε να παρέχει πλήρη διαφάνεια και να βοηθά στην ανταλλαγή δεδομένων και πληροφοριών ανάμεσα στις δύο ομάδες κατά την κοινή άσκηση, με απώτερο στόχο την καταγραφή των αποτελεσμάτων αυτής. Τα αποτελέσματα αυτά στη συνέχεια αξιοποιούνται για τον εντοπισμό και την επαλήθευση κενών στην ικανότητα της Blue Team να εντοπίζει τη δραστηριότητα των εξελιγμένων επιτιθεμένων που έγιναν Emulate, αλλά και της δημιουργίας ενός αποτελεσματικού προγράμματος Threat Detection Engineering βασισμένο σε αυτά [71].

Όπως φαίνεται στο παρακάτω σχήμα, η ιεραρχική δομή του VECTR είναι απλή, αλλά ταυτόχρονα παρέχει μεγάλη ευελιξία γιατί δίνει τη δυνατότητα δημιουργίας διαφορετικών Test Environment. Κάθε Test Environment μπορεί να χωριστεί σε διαφορετικά Assessment Groups ανάλογα το scope ή την χρονική περίοδο διεξαγωγής, όπως φαίνεται στο παράδειγμα της εικόνας (June 2019 Purple Team). Το κάθε Assessment Group στη συνέχεια μπορεί να χωριστεί σε μικρότερα campaigns ανάλογα το APT group (παράδειγμα εικόνας APT 39 Emulation). Τέλος το κάθε campaign μπορεί να χωριστεί σε ξεχωριστά test cases που αφορούν σε συγκεκριμένα TTPs.



Εικόνα 92. Ιεραρχική Δομή VECTR
Πηγή εικόνας: https://docs.vectr.io/user/important-concepts/

9.2.3 Defensive GAP / Attack Coverage Assessment με χρήση του Vectr

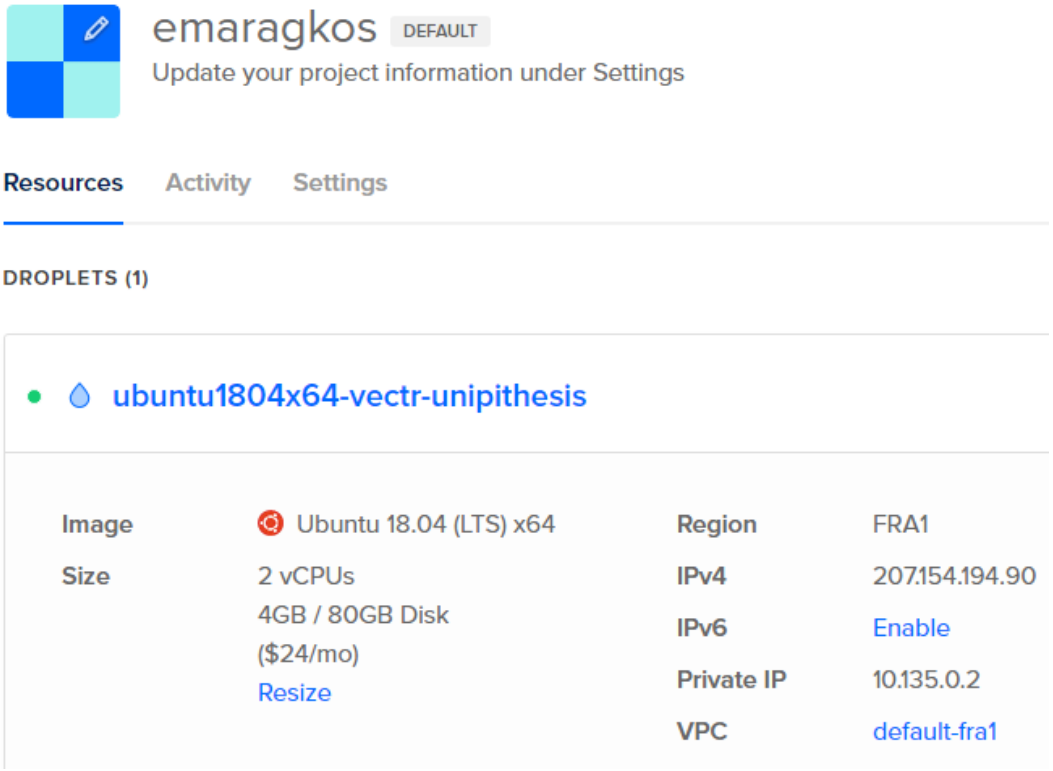
Απαιτήσεις Συστήματος

Για τη χρήση του VECTR απαιτείται η εγκατάσταση του σε ένα σύστημα το οποίο πληρεί τις παρακάτω απαιτήσεις.

- Internet access to GitHub and DockerHub
- 2+ CPU cores recommended

- Minimum 4GB RAM
- 100+ GB of free space

Για τις ανάγκες της εργασίας χρησιμοποιήθηκε ένα VM (Droplet) στο Digital Ocean, ωστόσο η εγκατάσταση μπορεί να πραγματοποιηθεί και σε ένα virtual machine που εκτελείται τοπικά σε έναν hypervisor όπως το VirtualBox.



Εικόνα 93. VECTR - Προετοιμασία περιβάλλοντος εγκατάστασης σε Cloud Provider (Digital Ocean)

Διαδικασία εγκατάστασης

Η διαδικασία εγκατάστασης του VECTR είναι ιδιαίτερα απλή διότι πέρα από το ότι υπάρχουν αναλυτικές οδηγίες και documentation, παρέχεται και η δυνατότητα εγκατάστασής του μέσω Docker που απλουστεύει και αυτοματοποιεί σε μεγάλο βαθμό τη διαδικασία. Ωστόσο, πριν την εγκατάσταση του σε Ubuntu 18.04 απαιτείται η εγκατάσταση ενός επιπλέον repository και των απαιτούμενων πακέτων λογισμικού που θα χρησιμοποιηθούν στη συνέχεια.

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

sudo add-apt-repository \
   "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
   $(lsb_release -cs) \
   stable"

sudo apt update

sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose unzip
```

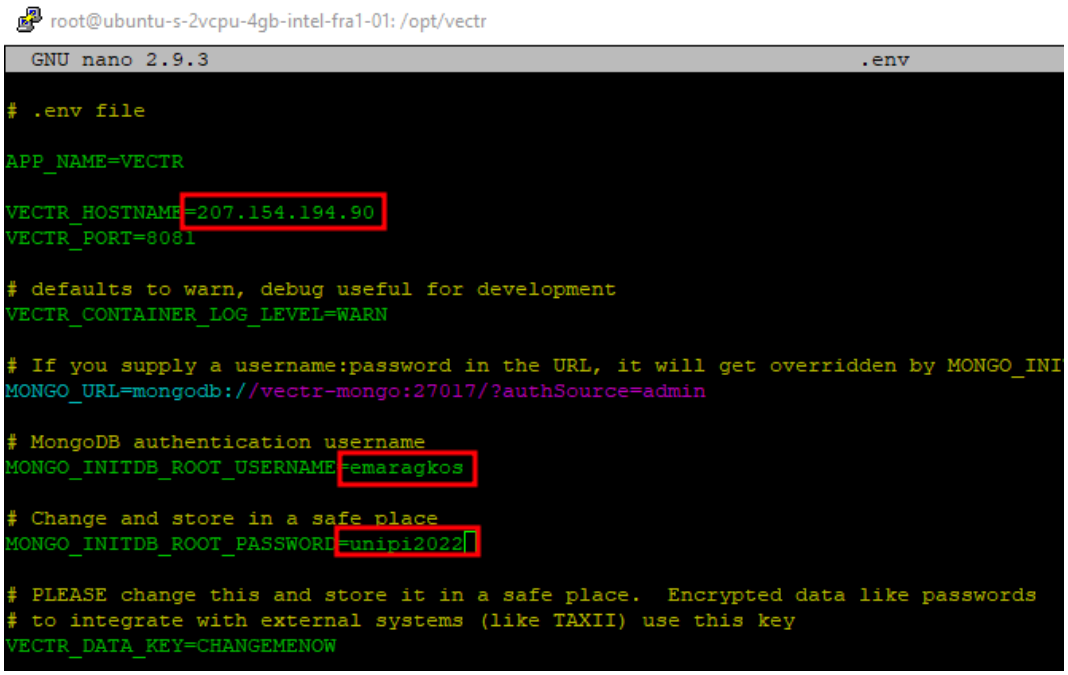
```
sudo apt upgrade

sudo systemctl enable docker
```

Αφού ολοκληρωθούν τα παραπάνω βήματα απομένει η λήψη του VECTR απο το GitHub repository και η αποσυμπίεση του σε έναν νέο φάκελο.

```
mkdir -p /opt/vectr

cd /opt/vectr

wget https://github.com/SecurityRiskAdvisors/VECTR/releases/down
load/ce-8.3.2/sra-vectr-runtime-8.3.2-ce.zip -P /opt/vectr

unzip sra-vectr-runtime-8.3.2-ce.zip
```

Το επόμενο βήμα είναι η επεξεργασία του αρχείου .env ώστε να προσαρμοστεί κατάλληλα για τη συγκεκριμένη εγκατάσταση προσθέτοντας τη διεύθυνση IP του Digital Ocean Droplet που δημιουργήθηκε αλλά και των credential της MongoDB βάσης δεδομένων που αποθηκεύουν τα δεδομένα της εφαρμογής.

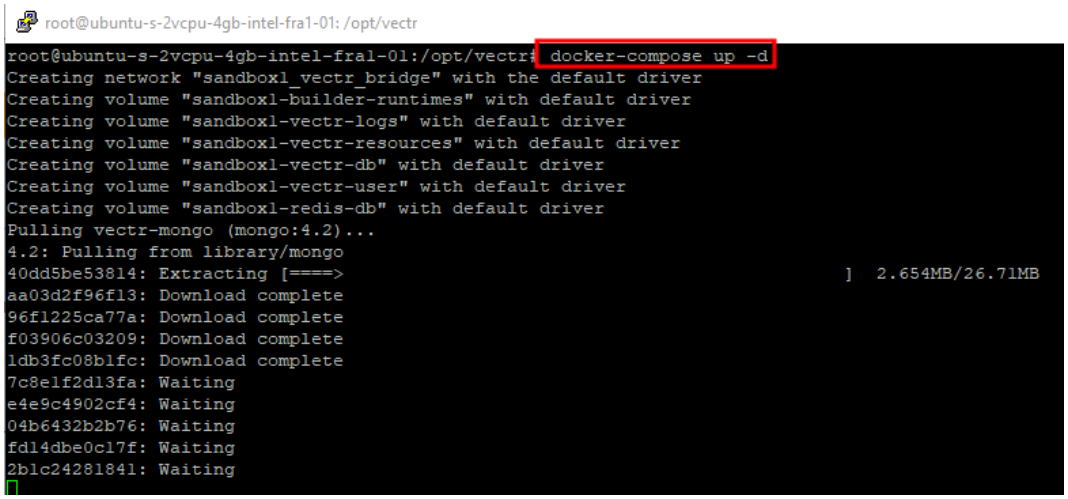
```
sudo nano .env
```



Εικόνα 94. Vectr - Παραμετροποίηση αρχείου config

Τέλος μέσω της παρακάτω εντολής του Docker ξεκινά η εγκατάσταση του VECTR που ολοκληρώνεται αυτόματα εντός μερικών λεπτών.

```
docker-compose up -d
```

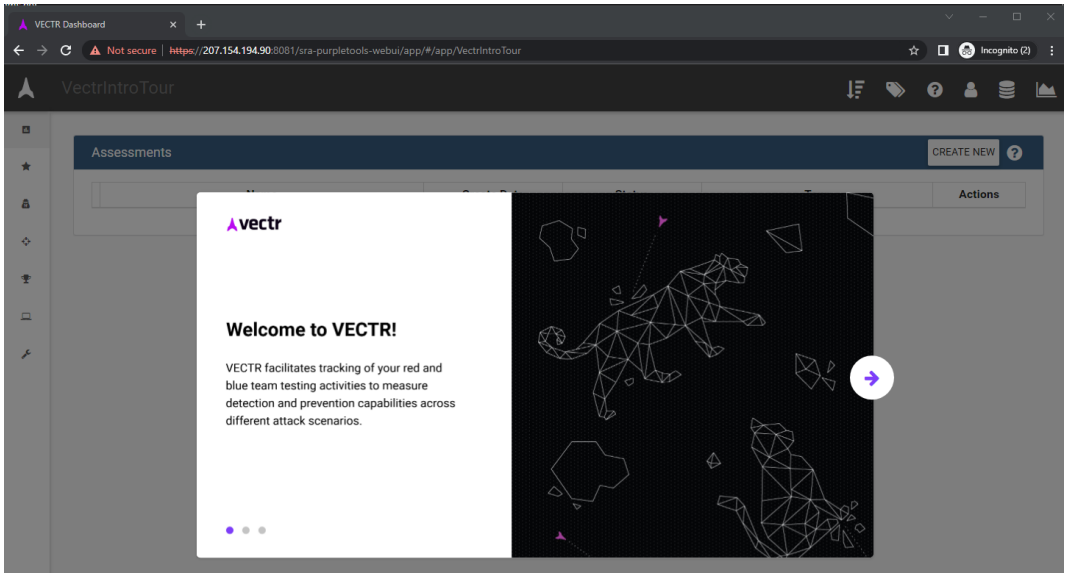


Εικόνα 95. VECTR - Εγκατάσταση μέσω Docker

Αφότου ολοκληρωθεί η εγκατάσταση, το Web Interface του VECTR είναι διαθέσιμο στο Port 8081 (https://IP:8081/) όπου IP είναι η διεύθυνση του Digital Ocean droplet που προστέθηκε στο .env file κατά την εγκατάσταση. Η σύνδεση με δικαιώματα διαχειριστή μπορεί να πραγματοποιηθεί με τα παρακάτω default credentials:

```
User: admin
Password: 11_ThisIsTheFirstPassword_11
```

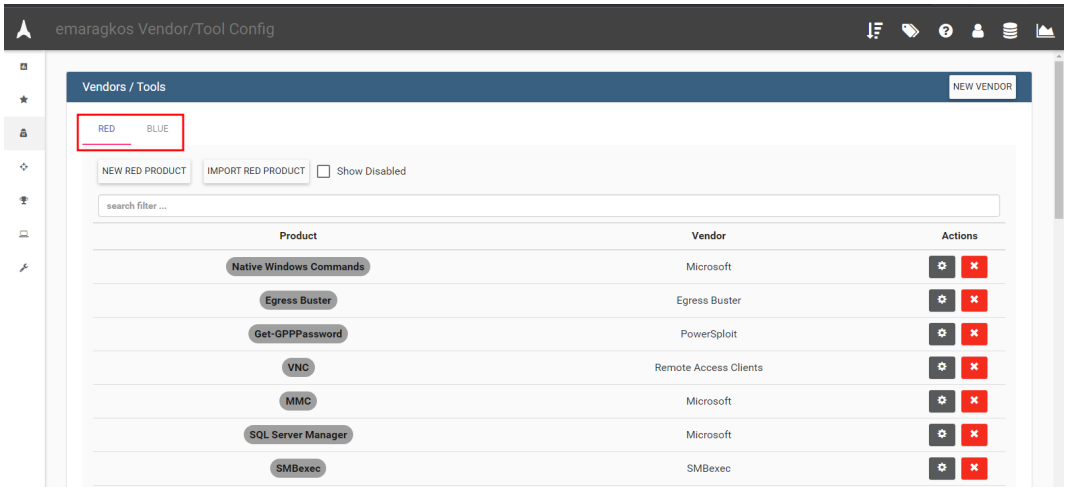
Κατά την πρώτη σύνδεση στο VECTR εμφανίζεται η παρακάτω εικόνα που παρουσιάζει μερικά από τα βασικά χαρακτηριστικά του λογισμικού.



Εικόνα 96. VECTR - Web Interface

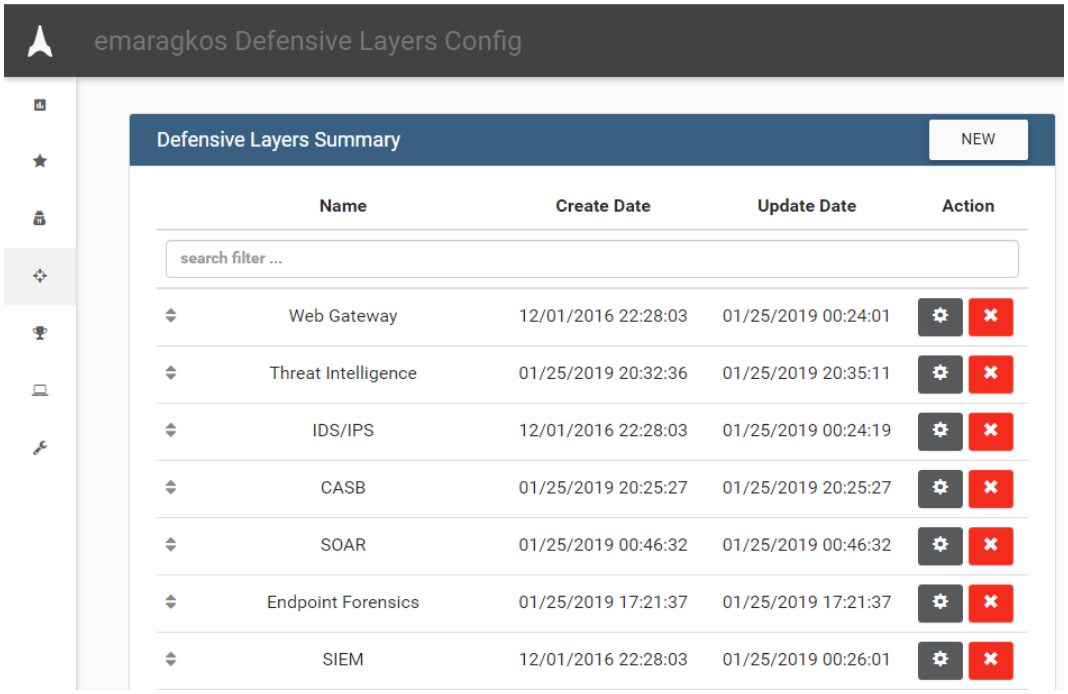
Για να αξιοποιηθούν οι πλήρεις δυνατότητες του VECTR απαιτείται πρώτα η προσαρμογή του ανάλογα με την υποδομή που θα διεξαχθούν τα πειράματα και τα Security Solutions που διαθέτει ο κάθε οργανισμός. Για παράδειγμα, στην παρακάτω εικόνα εμφανίζονται τα εργαλεία που είναι διαθέσιμα τόσο για τη Red όσο και για την Blue team με τη δυνατότητα προσθήκης νέων ανάλογα με το τι διαθέτει ο κάθε οργανισμός. Αυτά τα εργαλεία θα χρησιμοποιηθούν στην πορεία για να

χαρακτηρίσουν και να συνοδεύσουν τα αποτελέσματα που θα προκύψουν από το Threat Hunting και το Adversary Emulation. Για παράδειγμα αν κατά τη διάρκεια του Emulation Plan χρησιμοποιηθεί το Mimikatz από την Red Team και η δραστηριότητα εντοπιστεί μέσω του EDR από την Blue Team, τα εργαλεία αυτά θα πρέπει να έχουν προστεθεί εκ των προτέρων στη βάση δεδομένων του VECTR για να χρησιμοποιηθούν.



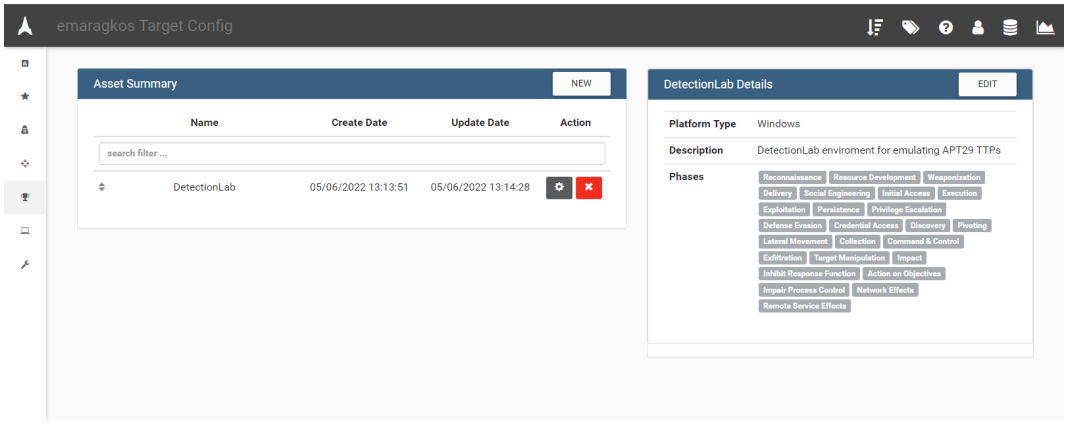
Εικόνα 97. VECTR - Δυνατότητα προσθήκης εργαλείων για Blue και Red Team

Το ίδιο ισχύει και στην περίπτωση των Defensive Layer που περιλαμβάνουν κατηγορίες συγκεκριμένων Security Solutions όπως SIEM, IPS, EDR SOAR κτλ.



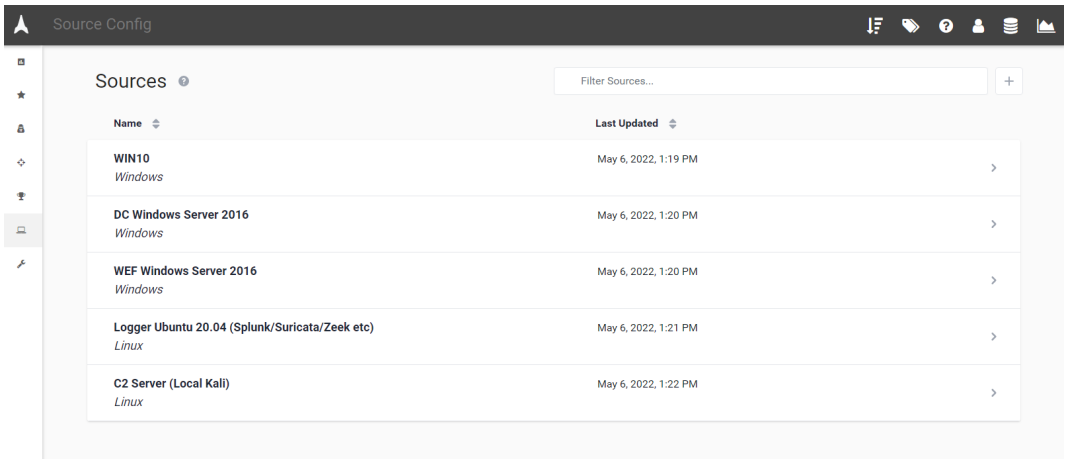
Εικόνα 98. VECTR - Δυνατότητα εισαγωγής custom Defensive Layers

Αφού προστεθούν και προσαρμοστούν τα εργαλεία που θα χρησιμοποιηθούν στις ασκήσεις και τα Defensive Layers που είναι διαθέσιμα στον οργανισμό, στη συνέχεια θα πρέπει να δημιουργηθεί ένα νέο Asset που στην προκειμένη περίπτωση θα ονομαστεί Detection Lab, καθώς σε αυτό θα διεξαχθούν τα πειράματα.



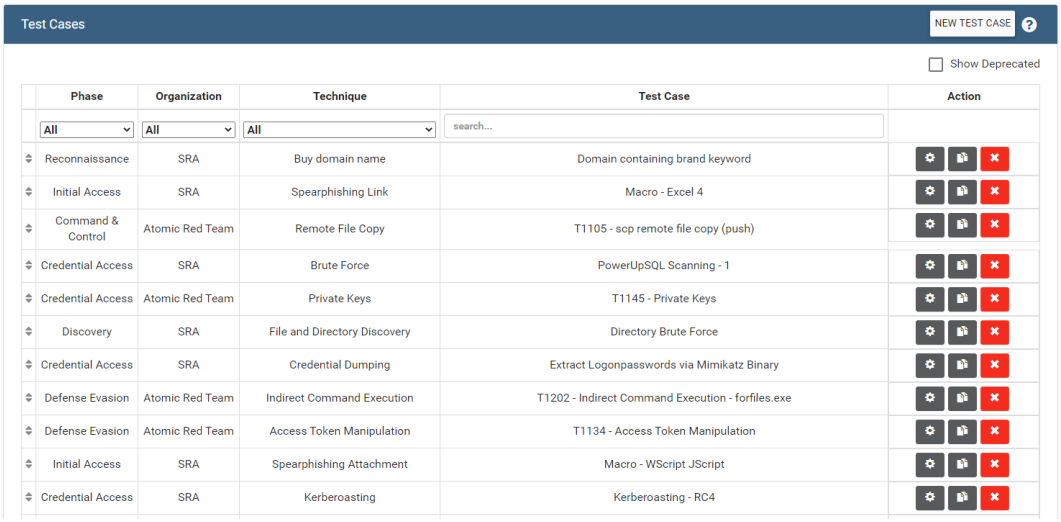
Εικόνα 99. VECTR - Δημιουργία DetectionLab ως νέου asset

Εντός του Detection Lab Asset θα προστεθούν τα υπό-στοιχεία της τοπολογίας του δικτύου που στην προκειμένη περίπτωση είναι τα τρία Windows VMs, ένα Ubuntu VM και ένα Kali Linux VM. Ανάλογα την τοπολογία του κάθε δικτύου προσαρμόζονται και όλα τα assets που περιλαμβάνονται εντός του scope της άσκησης, είτε αποτελούν μέρος ενός δοκιμαστικού περιβάλλοντος είτε ενός production περιβάλλοντος του οργανισμού.



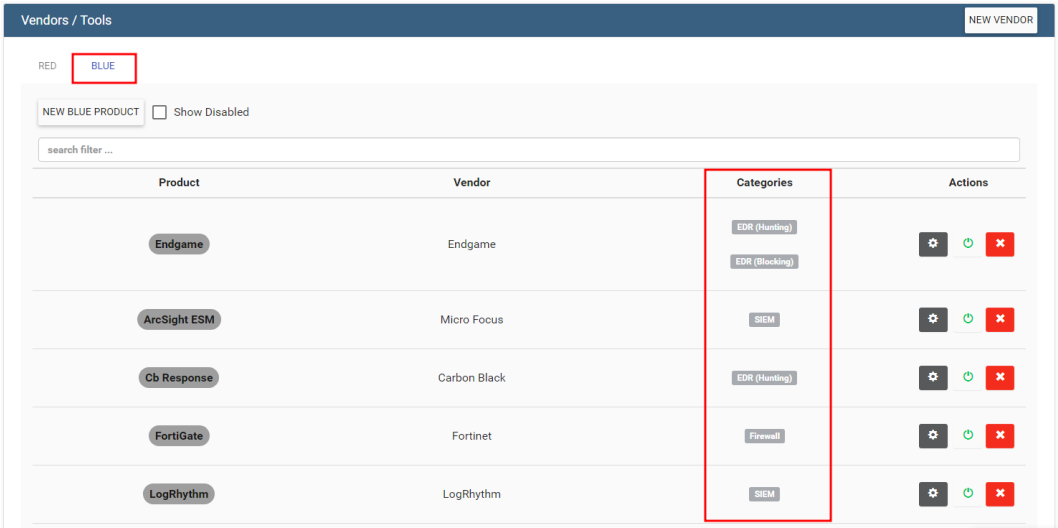
Εικόνα 100. VECTR - Εισαγωγή υποστοιχείων του DetectionLab

Στη συνέχεια, ανάλογα με το κάθε phase, μπορούν να δημιουργηθούν test cases που αφορούν συγκεκριμένες δοκιμές που θα διεξαχθούν ανάλογα την επιλεγμένη τεχνική (Tactic) βασισμένη στο MITRE ATT&CK Framework.



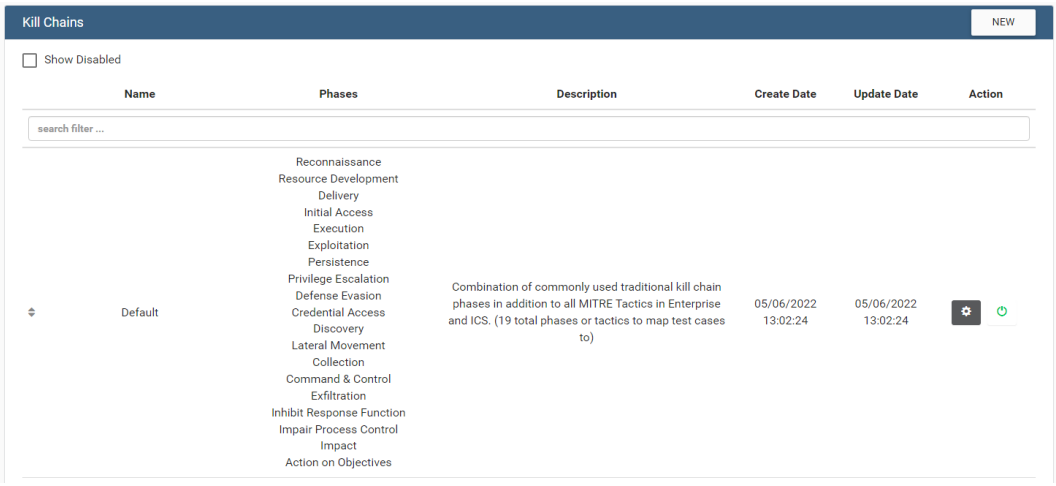
Εικόνα 101. VECTR - Παραδείγματα απο Test Cases

Σε αυτό το σημείο γίνεται η επιλογή των Security Solutions που υπάρχουν στο επιλεγμένο περιβάλλον από αυτά που δημιουργήθηκαν σε προηγούμενο στάδιο. Για παράδειγμα, σε ένα test case το οποίο αφορά τη δοκιμή επιθέσεων σε έναν webserver πιθανόν να υπάρχει WAF αλλά όχι ένα EDR.



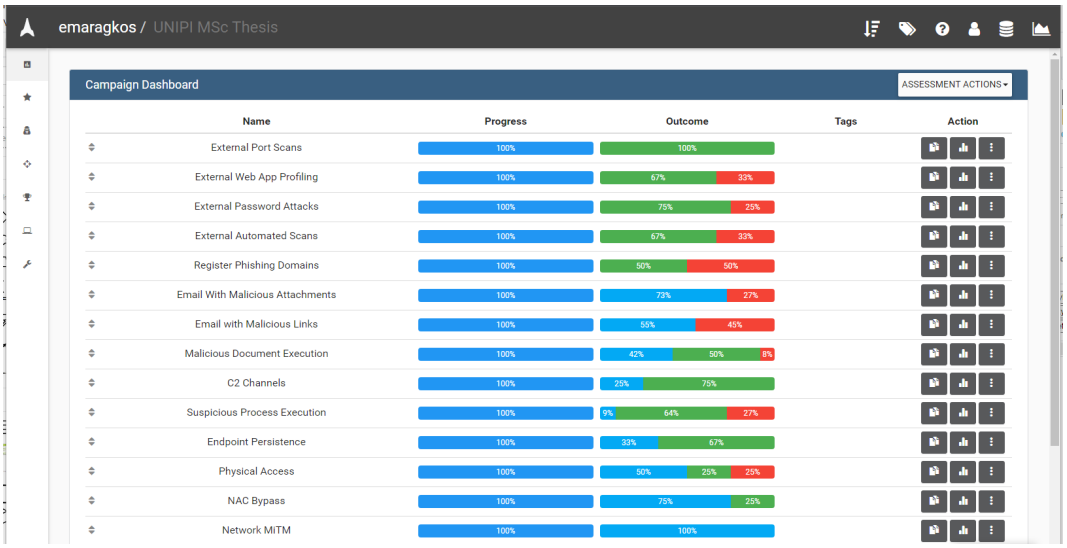
Εικόνα 102. VECTR - Εισαγωγή εργαλείων ασφαλείας που περιέχει το κάθε περιβάλλον

Στη συνέχεια γίνεται η επιλογή ενός Attack Kill-Chain. Αυτό μπορεί να είναι ένα προκαθορισμένο, όπως αυτό που χρησιμοποιεί το MITRE ATT&CK Framework και περιλαμβάνει όλα τα Tactics από το Reconnaissance μέχρι και το Impact, ή ένα προσαρμοσμένου σύμφωνα με τις ανάγκες της άσκησης. Για παράδειγμα αν η άσκηση περιλαμβάνει μόνο τις δοκιμές που αφορούν το Tactic του Exfiltration δεν υπάρχει λόγος να χρησιμοποιηθεί ένα πλήρες Attack Kill-Chain.



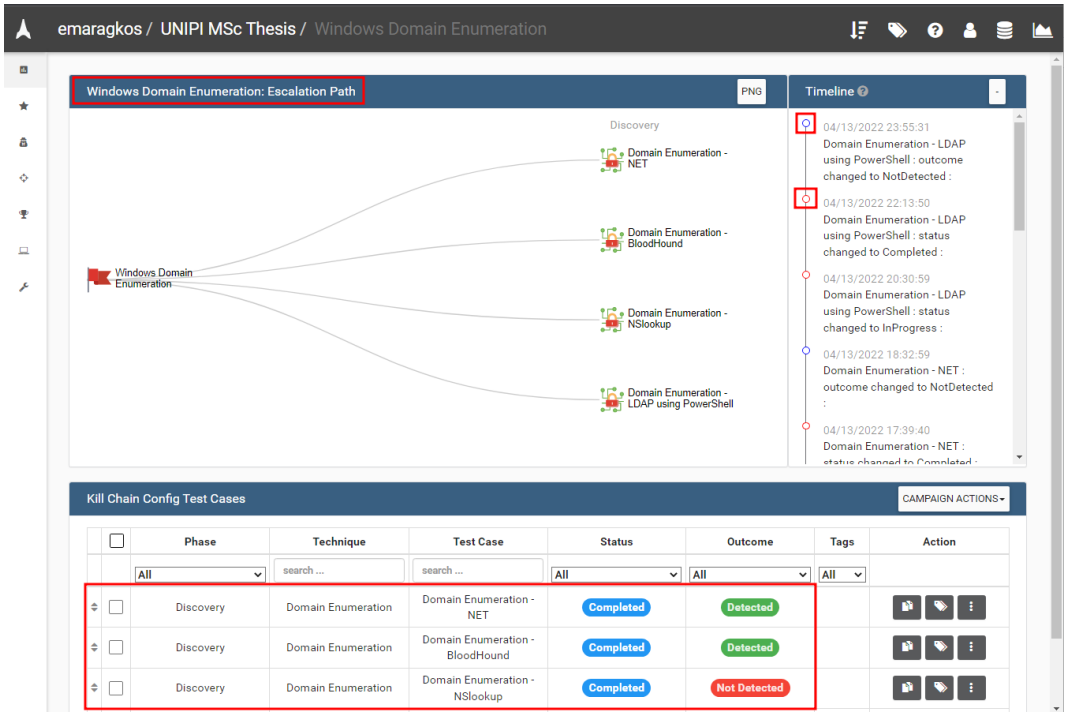
Εικόνα 103. VECTR - Επιλογή Attack Kill Chain ή δημιουργία προσαρμοσμένου

Έχοντας λοιπόν δημιουργήσει διαφορετικά use cases είναι είναι πολύ εύκολη η εκτέλεση των αντίστοιχων πειραμάτων μέσω των εργαλείων του Adversary Emulation που παρουσιάστηκαν στο πέμπτο κεφάλαιο και να δοκιμαστεί η ικανότητα εντοπισμού της δραστηριότητας αυτής από την Blue Team. Για παράδειγμα, στην παρακάτω εικόνα έχουν εκτελεστεί διαφορετικά Campaigns τα οποία εστιάζουν σε διαφορετικές περιπτώσεις.



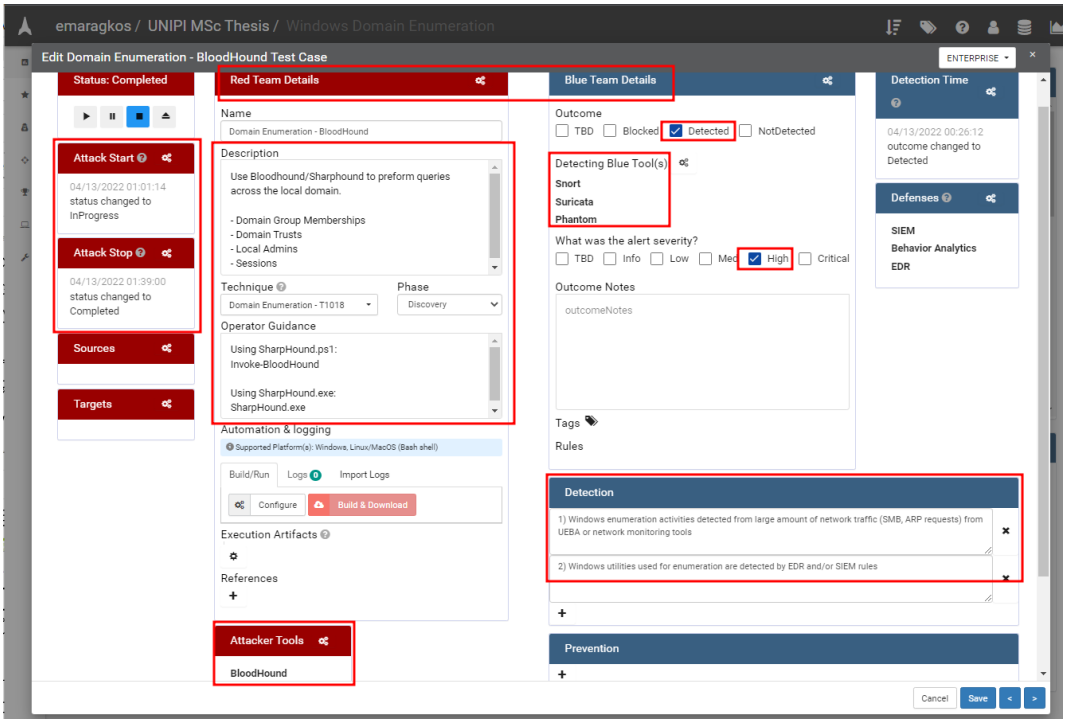
Εικόνα 104. VECTR - Επισκόπηση διαφορετικών Campaigns που έχουν εκτελεστεί

Πιο συγκεκριμένα στο παρακάτω Use Case που αφορά δοκιμές για Windows Domain Enumeration, εμφανίζονται τα βήματα που εκτέλεσε η Red team, το timeline των ενεργειών, η κατάσταση του test, δηλαδή αν έχει ολοκληρωθεί ή όχι και αν η Blue Team κατάφερε να εντοπίσει την δραστηριότητα αυτή.



Εικόνα 105. VECTR - Windows Domain Enumeration test cases

Παρακολουθώντας ακόμα πιο λεπτομερώς ένα συγκεκριμένο use case, και οι δύο ομάδες μπορούν να εισάγουν στοιχεία τα οποία περιγράφουν τα αποτελέσματα των δοκιμών. Στη συγκεκριμένη περίπτωση η Red team ξεκίνησε μία επίθεση η οποία έχει ως στόχο να πραγματοποιήσει Windows Domain Enumeration χρησιμοποιώντας τα εργαλεία Bloodhound και SharpHound (Technique Domain Enumeration - T1018). Αντίστοιχα η Blue απο την δική της πλευρά αναφέρει την έκβαση του πειράματος, δηλαδή το ότι κατάφερε να εντοπίσει τη δραστηριότητα με τρία διαφορετικά εργαλεία περιγράφοντας και τον τρόπο.



Εικόνα 106. VECTR - BloodHound Test Case

Συνοψίζοντας, το VECTR μπορεί να βοηθήσει έναν οργανισμό με τους παρακάτω τρόπους:

- Βοηθά στη διεξαγωγή κοινών ασκήσεων της Blue και της Red Team συλλέγοντας τα αντίστοιχα δεδομένα από τις ενέργειες και των δύο ομάδων.
- Βοηθά στον εντοπισμό των κενών στην ικανότητα εντοπισμού επιθέσεων εντός του περιβάλλοντος του οργανισμού χρησιμοποιώντας το MITRE ATT&CK Framework.
- Βοηθά στην δοκιμή των Security Solutions (IPS/IDS, EDR) που χρησιμοποιούνται και στην αξιολόγηση της αποτελεσματικότητας τους σε διαφορετικά στάδια ενός Attack Path.
- Παρέχει χρήσιμα συμπεράσματα τα οποία βοηθούν στο να οριστεί προτεραιότητα στις ενέργειες που πρέπει να πραγματοποιηθούν για τη βελτίωση της ικανότητας εντοπισμού κακόβουλης δραστηριότητας.
- Καταγράφει τα TTPs που χρησιμοποιεί ένας επιτιθέμενος ώστε να μπορεί να μετρηθεί η ικανότητα της Blue Team να εντοπίζει την αντίστοιχη δραστηριότητα σε βάθος χρόνου.
- Παρέχει ιστορικά δεδομένα για την πορεία των ασκήσεων και τη βελτίωση του εντοπισμού της κακόβουλης δραστηριότητας.
- Παρέχει οπτικοποίηση δεδομένων μέσω του MITRE ATT&CK Framework heatmap.
- Παρέχει τη δυνατότητα δημιουργίας αναλυτικών αναφορών οι οποίες μπορούν να συνοψίσουν τα αποτελέσματα των ασκήσεων βοηθώντας την παρουσίαση τους σε μη τεχνικό ακροατήριο όπως C Level Executives.

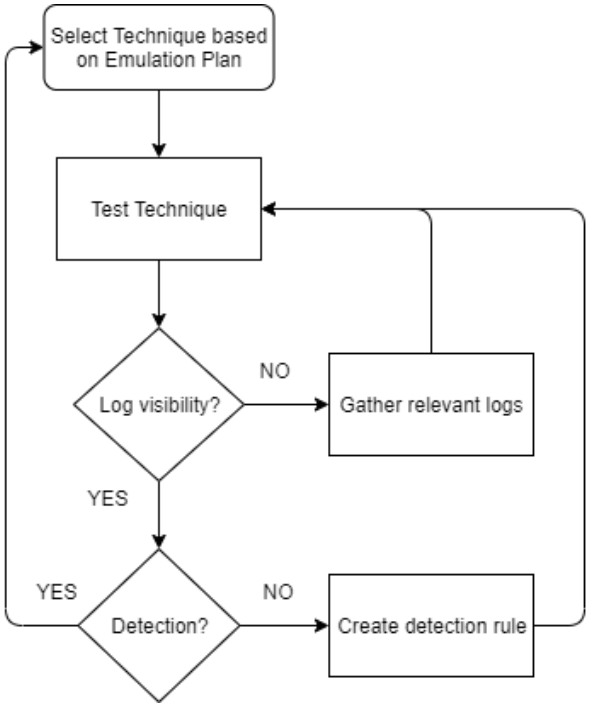
9.3 Threat Detection Engineering

Το επιδιωκόμενο αποτέλεσμα από τη χρήση του VECTR είναι αφενός η διευκόλυνση της διεξαγωγής του Gap Analysis και της συνεργασίας ανάμεσα στη Blue και στη Red team υπό την

μορφή μιας Purple Team άσκησης και αφετέρου η διευκόλυνση δημιουργίας μηχανισμών εντοπισμού για τη δραστηριότητα του Threat Actor η οποία δεν εντοπίστηκε. Άλλωστε αυτό είναι και το τελικό επιδιωκόμενο αποτέλεσμα της εργασίας, ο εντοπισμός δηλαδή των κενών στην ικανότητα εντοπισμού δραστηριότητας εξελιγμένων επιτιθεμένων για τη δημιουργία των απαραίτητων μηχανισμών εντοπισμού. Αυτή η διαδικασία ονομάζεται και Threat Detection Engineering. Συνεπώς, το Threat Detection Engineering είναι η ικανότητα των αναλυτών της Blue Team να μοντελοποιούν τη δραστηριότητα ενός επιτιθέμενου ώστε να παρέχουν αποτελεσματικούς μηχανισμούς εντοπισμού αυτής. Το βασικό output από τη διαδικασία αυτή είναι τα λεγόμενα Detectors που είναι σε θέση να εντοπίζουν τα TTPs του επιτιθέμενου. Αυτά τα Detectors μπορεί να είναι υπό τη μορφή Yara rules, Sigma rules, SIEM rules ή IPS rules. Σε όποια κατηγορία και αν ανήκει ένας Detector πρακτικά είναι ένας "κανόνας" που περιγράφει το πώς να εντοπιστεί η συγκεκριμένη δραστηριότητα.

Εικόνα 107. Συνδυασμός δεδομένων για Threat Detection Engineering
Πηγή εικόνας:
https://medium.com/mitre-attack/getting-started-with-attack-assessment-cc0b01769cb4

Όπως φαίνεται και στην παρακάτω εικόνα, η λογική πίσω από τη διαδικασία του Threat Detection Engineering είναι απλή και ξεκινά από την επιλογή της τεχνικής που θα γίνει Emulate ή ακόμα και ενός ολοκληρωμένου Emulation Plan. Στη συνέχεια πραγματοποιείται το Emulation της τεχνικής με σκοπό να διαπιστωθεί αν υπάρχει visibility, δηλαδή αν συλλέγονται τα απαραίτητα logs από τα συστήματα τα οποία επηρεάστηκαν. Αν δεν συλλέχθηκαν τα απαραίτητα logs, η διαδικασία επαναλαμβάνεται μέχρι τα logs να συγκεντρώνονται στα Security Solutions που απαιτούνται για τον εντοπισμό αυτής της δραστηριότητας. Ένα παράδειγμα είναι η περίπτωση στην οποία υπάρχει ένα Public-Facing Web Application και το Emulation Plan που πραγματοποιείται περιλαμβάνει τη διεξαγωγή του Technique "Public-Facing Application (ID: T1190)" για την επίτευξη του Tactic: "Initial Access Exploit". Στην περίπτωση που η επίθεση εκμεταλλεύεται μια αδυναμία SQL Injection στο web application, και τα logs του Web Server δεν μεταφέρονται σε ένα Security Solution (WAF/SIEM) τότε η δραστηριότητα αυτή δεν θα είναι εφικτό να εντοπιστεί εφόσον πρακτικά δεν υπάρχει visibility σε αυτό το σύστημα. Το επόμενο βήμα, εφόσον τα logs πλέον συλλέγονται είναι η διαπίστωση του αν η δραστηριότητα αυτή είναι ικανή να εντοπιστεί ως κακόβουλη από τα διαθέσιμα Security Solutions. Για παράδειγμα τα logs απο τον web server μπορεί να συλλέγονται και να αποστέλλονται στο SIEM αλλά να μην υπάρχει μηχανισμός εντοπισμού της συγκεκριμένης δραστηριότητας (SQL Injection). Εφόσον δεν εντοπίζεται, πρέπει να δημιουργηθεί ο αντίστοιχος κανόνας/μηχανισμός εντοπισμού. Κατά αυτό τον τρόπο υπάρχει μία προκαθορισμένη διαδικασία η οποία είναι σε θέση να δημιουργεί κανόνες εντοπισμού με βάση τα δεδομένα που παρήχθησαν από το Adversary Emulation. Όσο αυτή η διαδικασία επαναλαμβάνεται σε τακτά χρονικά διαστήματα, η Blue Team είναι σε θέση να επαληθεύει ότι οι μηχανισμοί εντοπισμού που ήδη υπάρχουν λειτουργούν, να τους βελτιώνει αλλά και να δημιουργεί νέους.



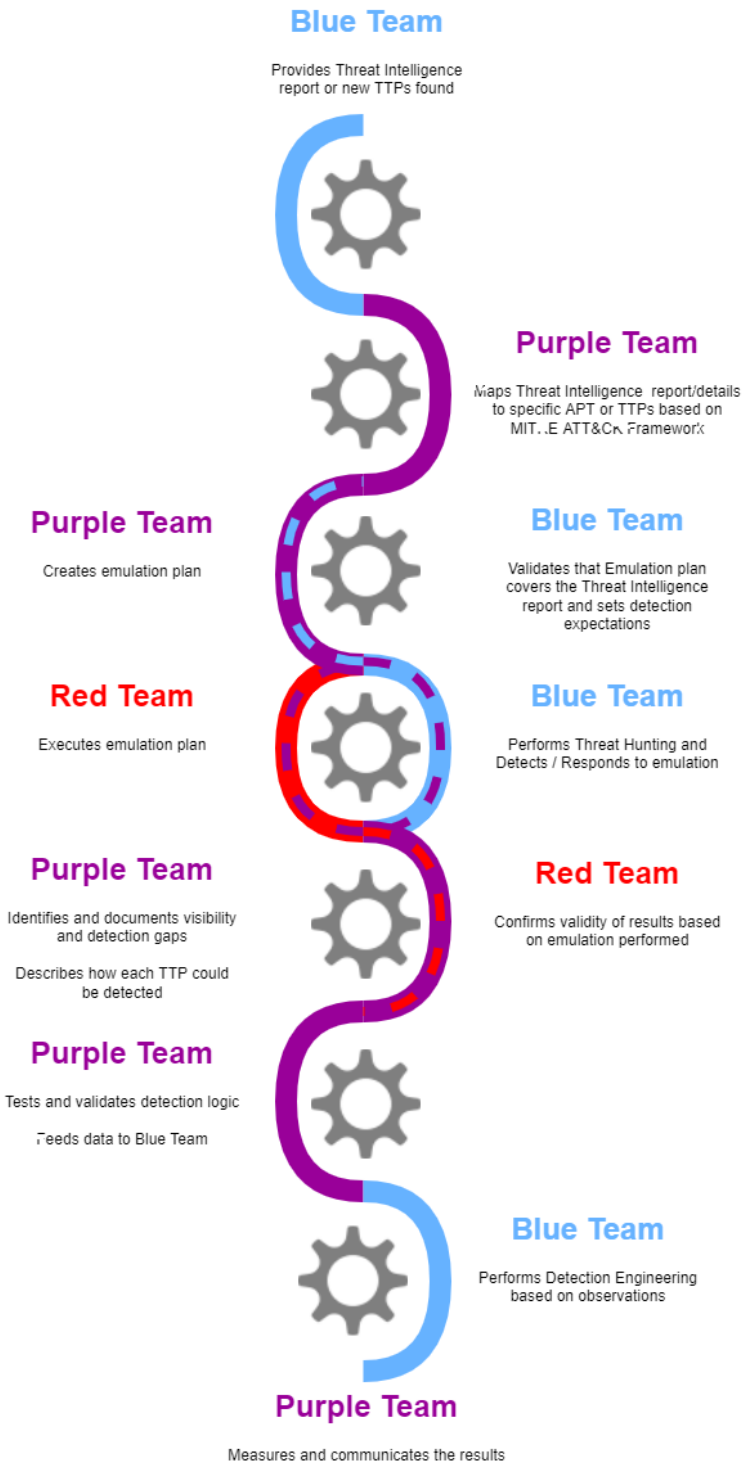
Εικόνα 108. Βήματα διεξαγωγής δοκιμής Technique

9.4 Προτεινόμενη μεθοδολογία συνεχούς βελτίωσης

Όλα όσα αναφέρθηκαν στα προηγούμενα κεφάλαια αποσκοπούν στη βελτίωση της ικανότητας της Blue Team να εντοπίζει έγκαιρα εξελιγμένους επιτιθέμενους. Ωστόσο ο συνδυασμός και η διασύνδεση των ενεργειών αυτών ενδέχεται να μην απόλυτα ξεκάθαρη. Σε αυτό το υπό-κεφάλαιο αναλύεται μια προτεινόμενη μεθοδολογία η οποία συνοψίζει τα βήματα που πραγματοποιήθηκαν στα προηγούμενα κεφάλαια και διευκρινίζει πως συνδυάζονται. Το επιδιωκόμενο αποτελέσματα της μεθοδολογίας αυτής είναι να παρέχει τη δυνατότητα σε Blue Teams να κάνουν Emulate τα TTPs που χρησιμοποιεί ένα εξελιγμένος επιτηθέμενος και με τα διαθέσιμα detection mechanisms, logs, rules, security solutions που ήδη υπάρχουν στον οργανισμό να διαπιστώνει τυχόν κενά τόσο στο visibility αλλά και σε ότι αφορά τους μηχανισμών detection που έχουν ήδη υλοποιηθεί. Η μεθοδολογία εστιάζει στο να μην εξαρτάται από συγκεκριμένα Threat Hunting / Adversary Emulation Tools και να μπορεί να διεξαχθεί από Blue Teams που δεν έχουν εξειδικευμένες γνώσεις στο Adversary Emulation όπως μια Red Team. Συνεπώς μια Blue Team με περιορισμούς, όπως μικρό αριθμό προσωπικού, μικρό προϋπολογισμό, χωρίς γνώσεις Adversary Emulation και Purple Teaming και χωρίς την ύπαρξη Red/Purple Team στον οργανισμό, να μπορεί να πραγματοποιήσει Automated / Scripted Adversary Emulation με τελικό στόχο τη διεξαγωγή ενός Defensive Gap / Attack coverage Assessment επαναλαμβάνοντας αυτή τη διαδικασία σε βάθος χρόνου για τη συνεχή βελτίωση.

Η προτεινόμενη μεθοδολογία παρουσιάζεται μέσω της παρακάτω εικόνας. Αξίζει να σημειωθεί πως τα βήματα είναι χωρισμένα ανά ομάδες (Blue, Purple, Red), συνεπώς η κάθε ομάδα εκτελεί τα στάδια της μεθοδολογίας που της αντιστοιχούν εφόσον υπάρχουν ή μπορούν να δημιουργηθούν για της ανάγκες της άσκησης. Ωστόσο, στην περίπτωση που λόγω περιορισμένων πόρων η Blue Team αναγκάζεται να ενεργήσει μόνη της, η διεξαγωγή των βημάτων είναι και πάλι εφικτή, καθώς εξειδικευμένες ενέργειες όπως η εκτέλεση του Emulation Plan, που θα διεκπεραίωνε η Red Team, μπορούν να πραγματοποιηθούν μέσω Automated / Scripted Atomic Tests με τα εργαλεία που παρουσιάστηκαν. Επιπλέον οι δραστηριότητες που θα αναλάμβανε η Purple Team όπως η καταγραφή

και η εξαγωγή των συμπερασμάτων σχετικά με το Emulation μπορούν να πραγματοποιηθούν πολύ εύκολα με τη χρήση εργαλείων όπως το VECTR.



Εικόνα 109. Διάγραμμα Μεθοδολογίας

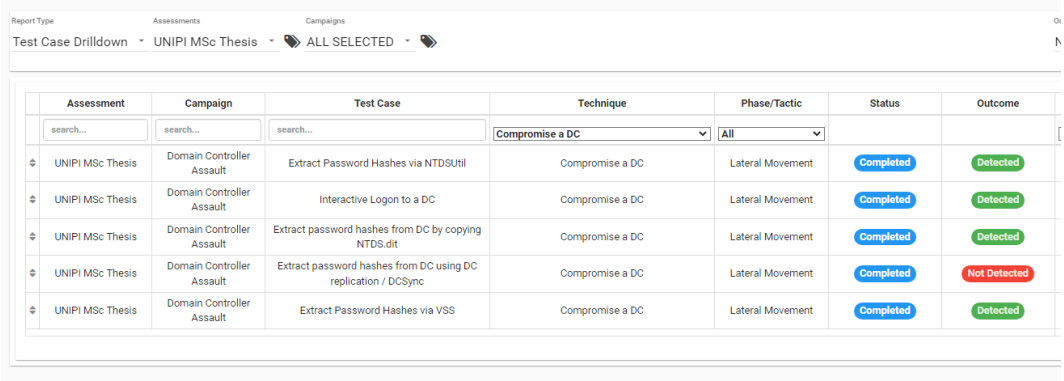
- Το πρώτο βήμα ξεκινά με την Blue Team να διαθέτει πληροφορίες που προέρχονται από ένα Threat Intelligence Report για έναν εξελιγμένο επιτιθέμενο που ενδέχεται να στοχεύσει τον

οργανισμό ή για νέα TTPs που χρησιμοποιούνται απο Threat Actors.

- Στο επόμενο βήμα η Purple Team, εξετάζοντας το Threat Intelligence Report, είναι σε θέση να συνδέσει τις πληροφορίες με συγκεκριμένα APT Groups / Threat Actors ή TTPs βασιζόμενη στο MITRE ATT&CK Framework.
- Στη συνέχεια, η Purple Team αξιοποιώντας αυτές τις πληροφορίες και εκμεταλευόμενη τις δυνατότητες του MITRE ATT&CK Framework είναι σε θέση να δημιουργήσει ένα ολοκληρωμένο Emulation Plan. Ταυτόχρονα η Blue team εξετάζει τον Emulation Plan και επιβεβαιώνει πως καλύπτει τις απαιτήσεις του Threat Intelligence Report στο οποίο βασίστηκε.
- Στο επόμενο βήμα η Red Team λαμβάνει Emulation Plan και το εκτελεί ενώ παράλληλα η Blue Team πραγματοποιεί Threat Hunting και Incident Response.
- Αφού το Emulation Plan έχει ολοκληρωθεί, η Purple team καταγράφει τις ενέργειες και των δύο ομάδων εντοπίζοντας τα κενά που υπάρχουν σε visibility και detection προτείνοντας παράλληλα και τρόπους ώστε να εντοπιστούν βοηθώντας την Blue να κατανοήσει καλύτερα τις ενέργειες που πραγματοποίησε η Red team. Επίσης σε αυτό το στάδιο η Red team εξετάζει τα αποτελέσματα που συλλέχθηκαν από το emulation ώστε να επαληθεύσει την ορθότητα τους σύμφωνα με τις ενέργειες που πραγματοποίησε για την αποφυγή false positive.
- Στο επόμενο βήμα η Purple Team δοκιμάζει και επαληθεύει την προτεινόμενη λύση για το Detection Mechanism που η Blue Team θα κληθεί να υλοποιήσει.
- Στη συνέχεια, η Blue team, εξετάζοντας τα δεδομένα που παρέχει η Purple team, είναι σε θέση να σχεδιάσει νέους μηχανισμούς εντοπισμού ώστε να εντοπίζει τη δραστηριότητα που πραγματοποίησε η Red team στο συγκεκριμένο adventure simulation πραγματοποιήθηκε.
- Τέλος η Purple Team είναι υπεύθυνη για την μέτρηση της απόδοσης και των δύο ομάδων και την επικοινωνία των αποτελεσμάτων.

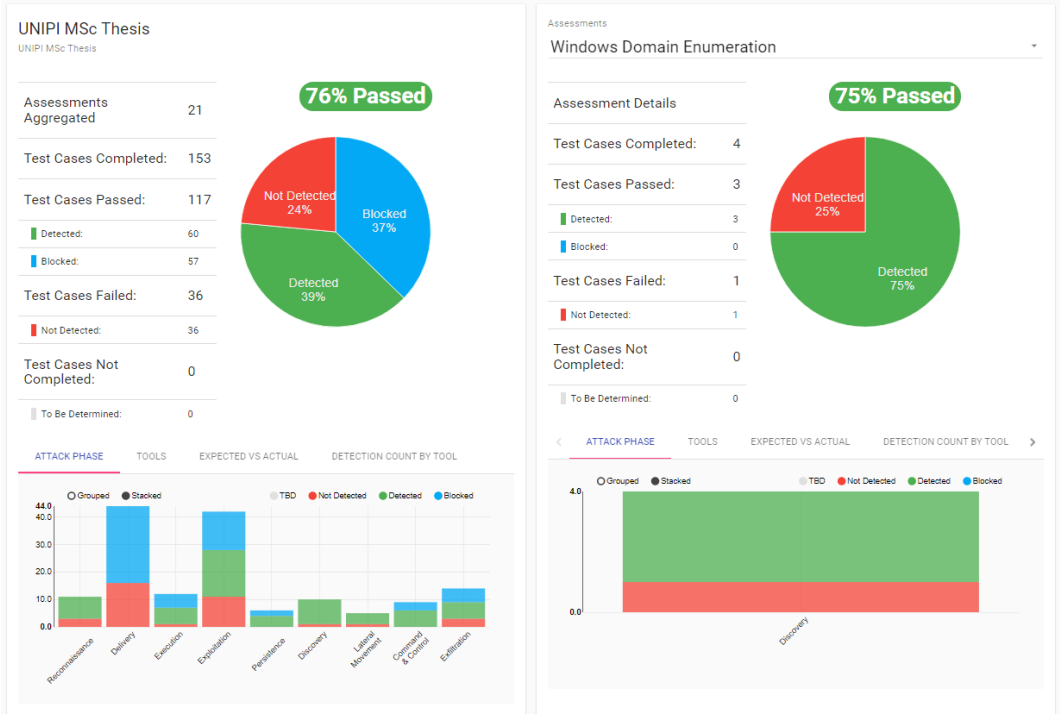
9.5 Ανατροφοδότηση

Πολύ σημαντική διαδικασία είναι και η διαδικασία της ανατροφοδότησης, δηλαδή η επικοινωνία των αποτελεσμάτων και η συνεχής επανάληψη της μεθοδολογίας σε βάθος χρόνου. Η παραπάνω διαδικασία είναι ιδιαίτερα σημαντική επειδή επιτρέπει τη μεταφορά των αποτελεσμάτων στην Blue Team για την διεξαγωγή των επόμενων πειραμάτων αλλά και για την παρακολούθηση της βελτίωσης ικανότητας εντοπισμού σε βάθος χρόνου. Το VECTR παρέχει πολλαπλούς τρόπους εξαγωγής στατιστικών που να απευθύνονται και σε μη τεχνικό ακροατήριο, μέσω της μορφής διαγραμμάτων ή Heat Maps με ώστε να είναι κατανοητά σε C Level executives εντός του οργανισμού. Όπως φαίνεται στην παρακάτω εικόνα μπορεί να γίνει επισκόπηση όλων των assessments και των campaings που έχουν διεξαχθεί.



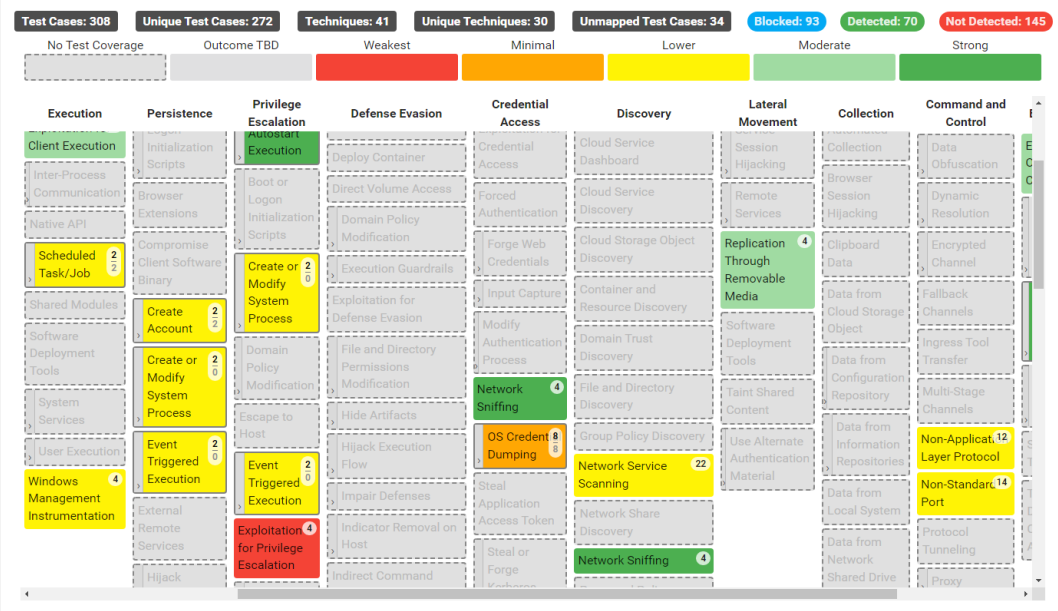
Εικόνα 110. Vectr Reporting - Επισκόπηση ολοκλήρωσης δοκιμών ανά Technique

Για παράδειγμα, στην παρακάτω εικόνα εμφανίζεται σε μορφή διαγραμμάτων η επισκόπηση των αποτελεσμάτων ενός ολοκληρωμένου Emulation Plan το οποίο αναφέρει τον αριθμό των cases τα οποία εκτελέστηκαν και τα ποσοστά όσων εντοπίστηκαν ή όχι. Επιπλέον, μπορούν να εμφανιστούν περισσότερες πληροφορίες ανάλογα με τα εργαλεία ή το κάθε assesment.



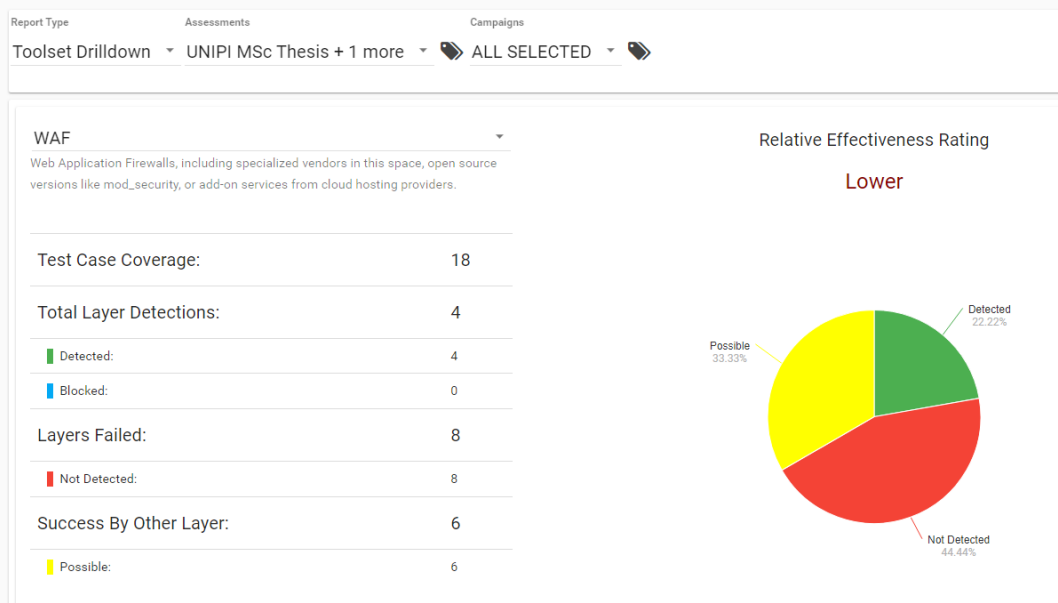
Εικόνα 111. Vectr Reporting - Επισκόπηση αποτελεσμάτων Emulation

Ιδιαίτερα χρήσιμη είναι και η επισκόπηση των αποτελεσμάτων μέσω του MITRE ATT&CK Framework HeatMap.



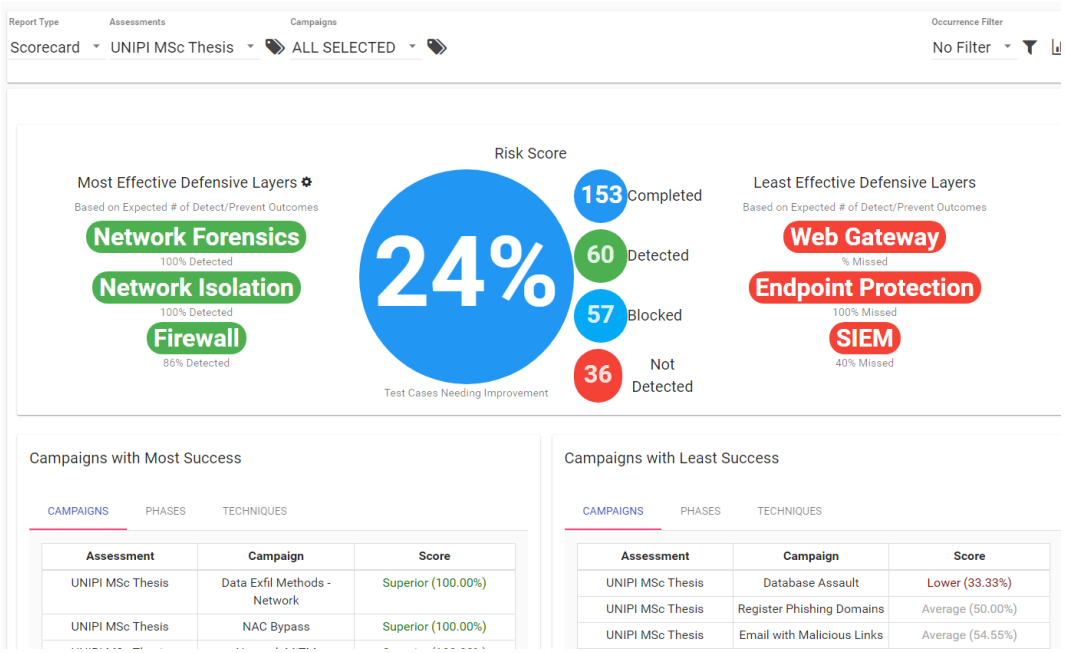
Εικόνα 112. Vectr Reporting - Επισκόπηση αποτελεσμάτων κάλυψης με μορφή Heat Map

Χρήσιμα στατιστικά παρέχονται επίσης και για κάθε ξεχωριστό εργαλείο. Για παράδειγμα, στην προκειμένη περίπτωση το WAF φαίνεται να έχει χαμηλό effectiveness rating σε σχέση με Security Solutions. Μία αντίστοιχη πληροφορία είναι ιδιαίτερα χρήσιμη σε όσους είναι υπεύθυνοι για τη λήψη των αποφάσεων σχετικά με τα εργαλεία τα οποία αποτελούν μέρος του προϋπολογισμού για την άμυνα του οργανισμού.



Εικόνα 113. Vectr Reporting - Επισκόπηση αποτελεσμάτων αποτελεσματικότητας ανά Security Solution

Τέλος παρέχονται στατιστικά ως γενική επισκόπηση των αποτελεσμάτων των δοκιμών.



Εικόνα 114. VECTR Reporting - Επισκόπηση αποτελεσμάτων ως Scoreboard

Κεφάλαιο 10

Επίλογος

10.1 Συμπεράσματα

Η αντιμετώπιση εξελιγμένων επιτιθέμενων θα αποτελεί πάντα μία πρόκληση για τις Blue Teams. Όσο καλά προετοιμασμένη και αν είναι η άμυνα ενός οργανισμού, με state-of-the-art security solutions και εξειδικευμένο προσωπικό, οι επιτιθέμενοι θα είναι πάντα ένα βήμα μπροστά. Ωστόσο, αξιοποιώντας proactive μεθόδους άμυνας και αξιοποιώντας μεθοδολογίες όπως αυτή που παρουσιάστηκε στην εργασία, οι οργανισμοί μπορούν να επιτύχουν σε βάθος χρόνου σημαντικές βελτιώσεις στην ικανότητα τους να εντοπίζουν και να αποτρέπουν επιθέσεις σε αρχικό στάδιο.

10.2 Μελλοντικές επεκτάσεις

Η παρούσα εργασία θα μπορούσε να επεκταθεί διενεργώντας περαιτέρω έρευνα σε επιπλέον εργαλεία τόσο για Adversary Emulation όσο και για Detection Gap Analysis. Επίσης θα μπορούσε να διεξαχθεί επιπρόσθετη έρευνα σε τρόπους βελτίωσης της μεθοδολογίας, δημιουργώντας παραλλαγές ανάλογα με τους πιθανούς περιορισμούς που μπορεί να διαθέτει η Blue Team ανά περίπτωση.

Βιβλιογραφικές Αναφορές

[1] NIST. *Glossary - Threat actor*. 2022. URL: https://csrc.nist.gov/glossary/term/threat_actor (επίσκεψη 25/05/2022).

[2] NIST. *Glossary - Adversary*. URL: https://csrc.nist.gov/glossary/term/adversary (επίσκεψη 25/05/2022).

[3] NIST. *Glossary - Advanced Persistent Threat*. URL: https://csrc.nist.gov/glossary/term/advanced%5C_persistent%5C_threat (επίσκεψη 25/05/2022).

[4] Nonprofit organization Center for Internet Security. *Election Security Spotlight – Cyber Threat Actors*. URL: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors (επίσκεψη 25/05/2022).

[5] Aleksandra Pawlicka, Michał Choraś και Marek Pawlicki. «The stray sheep of cyberspace aka the actors who claim they break the law for the greater good». Στο: *Personal and Ubiquitous Computing* 25.5 (2021), σσ. 843–852.

[6] Mirko Sailio, Outi-Marja Latvala και Alexander Szanto. «Cyber threat actors for the factory of the future». Στο: *Applied Sciences* 10.12 (2020), σ. 4334.

[7] Canadian Centre for Cyber Security. *Cyber threat and cyber threat actors*. URL: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors (επίσκεψη 25/05/2022).

[8] The Washington Post. *A hacker broke into a Florida town's water supply and tried to poison it with lye, police said*. 2021. URL: https://www.washingtonpost.com/nation/2021/02/09/oldsmar-water-supply-hack-florida/ (επίσκεψη 25/05/2022).

[9] Crowd Strike. *Adapt and Persevere: In-depth analysis of the most significant cybersecurity events and trends (2022)*. URL: https://www.crowdstrike.com/resources/reports/global-threat-report/ (επίσκεψη 25/05/2022).

[10] MITRE Corporation. *APT Groups*. URL: https://attack.mitre.org/groups/ (επίσκεψη 25/05/2022).

[11] U.S. General Services Administration. *GSA's Advanced Persistent Threat (APT) Buyer's Guide*. URL: https://interact.gsa.gov/document/gsas-advanced-persistent-threat-apt-buyers-guide (επίσκεψη 25/05/2022).

[12] MITRE Corporation. *APT29 Group (Cozy Bear) - ID: G0016*. URL: https://attack.mitre.org/groups/G0016/ (επίσκεψη 25/05/2022).

[13] MITRE Corporation. *Cobalt Group - ID: G0080*. URL: https://attack.mitre.org/groups/G0080/ (επίσκεψη 25/05/2022).

[14] MITRE Corporation. *APT41 Group (Wicked Panda) - ID: G0096*. URL: https://attack.mitre.org/groups/G0096/ (επίσκεψη 25/05/2022).

[15] NIST. *Glossary - Blue Team*. URL: https://csrc.nist.gov/glossary/term/blue_team (επίσκεψη 25/05/2022).

[16] ENISA. *ENISA Threat Landscape 2021*. 2021. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (επίσκεψη 25/05/2022).

[17] Ponemon Institute LLC. *Improving the Effectiveness of the Security Operations Center*. 2019. URL: https://www.devo.com/wp-content/uploads/2019/07/2019-Devo-Ponemon-Study-Final.pdf (επίσκεψη 25/05/2022).

[18] NIST. *Glossary - Red Team*. URL: https://csrc.nist.gov/glossary/term/red_team (επίσκεψη 25/05/2022).

[19] Patrick Engebretson. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier, 2013.

[20] Bradley J Wood και Ruth A Duggan. «Red teaming of advanced information assurance concepts». Στο: *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*. Τόμ. 2. IEEE. 2000, σσ. 112–118.

[21] Steve Mansfield-Devine. «The best form of defence–the benefits of red teaming». Στο: *Computer Fraud & Security* 2018.10 (2018), σσ. 8–12.

[22] Ville Saarainen. «Red Teaming: Regulatory and non-regulatory frameworks used in adversarial simulations». Στο: (2021).

[23] Ivan Kovacevic και Stjepan Gros. «Red Teams-Pentesters, APTs, or Neither.» Στο: *MIPRO*. 2020, σσ. 1242–1249.

[24] Jacob G Oakley. «Purple Teaming». Στο: *Professional Red Teaming*. Springer, 2019, σσ. 105–115.

[25] Matthew Hickey και Jennifer Arcuri. *Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming*. John Wiley & Sons, 2020.

[26] Siddharth Chowdhury. «PERCEPTIONS OF PURPLE TEAMS AMONG CYBERSECURITY PROFESSIONALS». Διδακτορική διατρ. Purdue University Graduate School, 2019.

[27] MITRE Corporation. *MITRE ATT&CK Navigator*. URL: https://mitre-attack.github.io/attack-navigator/ (επίσκεψη 25/05/2022).

[28] Matt Bromiley. «Threat intelligence: What it is, and how to use it effectively». Στο: *SANS Institute InfoSec Reading Room* 15 (2016), σ. 172.

[29] Vasileios Mavroeidis και Siri Bromander. «Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence». Στο: *2017 European Intelligence and Security Informatics Conference (EISIC)*. IEEE. 2017, σσ. 91–98.

[30] Crowd Strike. *WHAT IS CYBER THREAT INTELLIGENCE?* URL: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (επίσκεψη 25/05/2022).

[31] SOCRadar.io. *What is Strategic Cyber Intelligence and How to Use it*. URL: https://socradar.io/what-is-strategic-cyber-intelligence-and-how-to-use-it/ (επίσκεψη 25/05/2022).

[32] Lockheed Martin. *Lockheed Martin - The Cyber Kill Chain*. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (επίσκεψη 25/05/2022).

[33] Tarun Yadav και Arvind Mallari Rao. «Technical aspects of cyber kill chain». Στο: *International Symposium on Security in Computing and Communication*. Springer. 2015, σσ. 438–452.

[34] MITRE Corporation. *MITRE ATT&CK Framework Homepage*. URL: https://attack.mitre.org/ (επίσκεψη 25/05/2022).

[35] MITRE Corporation. *GETTING STARTED WITH ATT&CK*. URL: https://www.mitre.org/publications/technical-papers/getting-started-with-attack (επίσκεψη 25/05/2022).

[36] MITRE Corporation. *MITRE ATT&CK : DESIGN AND PHILOSOPHY*. URL: https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy (επίσκεψη 25/05/2022).

[37] MITRE Corporation. *MITRE Cyber Analytics Repository*. URL: https://car.mitre.org/ (επίσκεψη 25/05/2022).

[38] MITRE Corporation. *MITRE Caret*. URL: https://mitre-attack.github.io/caret/ (επίσκεψη 25/05/2022).

[39] ChaosSearch. *The Threat Hunter's Handbook: Using Log Analytics to Find and Neutralize Hidden Threats in Your Environment*. URL: https://www.chaossearch.io/hubfs/ChaosSearch%5C%20Threat%5C%20Hunters%5C%20Handbook.pdf (επίσκεψη 25/05/2022).

[40] Nataliia Lukova-Chuiko, Andriy Fesenko, Hanna Papirna και Sergiy Gnatyuk. «Threat Hunting as a Method of Protection Against Cyber Threats.» Στο: *IT&I*. 2020, σσ. 103–113.

[41] Eric C Thompson. «Threat hunting». Στο: *Designing a HIPAA-Compliant Security Operations Center*. Springer, 2020, σσ. 205–212.

[42] Dutch Payments Association. *TaHiTI Threat Hunting Methodology*. URL: https://www.betaalvereniging.nl/en/safety/tahiti/ (επίσκεψη 25/05/2022).

[43] SQRRL. *A Framework for Cyber Threat Hunting*. URL: https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf (επίσκεψη 25/05/2022).

[44] Mandiant. *M-trends 2021: Insights into Today's Top Cyber Trends and Attacks*. URL: https://www.mandiant.com/sites/default/files/2021-09/rpt-mtrends-2021-3.pdf (επίσκεψη 25/05/2022).

[45] IBM. *What is threat hunting?* URL: https://www.ibm.com/topics/threat-hunting (επίσκεψη 25/05/2022).

[46] Crowd Strike. *INDICATORS OF COMPROMISE (IOC) SECURITY*. 2021. URL: https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ (επίσκεψη 25/05/2022).

[47] RSA.com. *UNDERSTANDING INDICATORS OF COMPROMISE (IOC) PART I*. 2012. URL: https://web.archive.org/web/20170914034202/https://blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i/ (επίσκεψη 25/05/2022).

[48] Arun Warikoo. «The Triangle Model for Cyber Threat Attribution». Στο: *Journal of Cyber Security Technology* (2021), σσ. 1–18.

[49] David J. Bianco. *The Pyramid of Pain*. 2014. URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (επίσκεψη 25/05/2022).

[50] Jeremy Kerwin. *"Applying the scientific method to threat hunting*. Αδημοσίευτη ερευνητική εργασία. Tech. Rep., 2020.[Online]. Available: https://www. sans. org/reading-room …, 2020.

[51] Jorge Orchilles. *SCYTHE's Ethical Hacking Maturity Model*. 2020. URL: https://www.scythe.io/library/scythes-ethical-hacking-maturity-model (επίσκεψη 25/05/2022).

[52] NVISO. *Adversary Emulation*. URL: https://www.nviso.eu/en/service/21/adversary-emulation (επίσκεψη 25/05/2022).

[53] Erik Van Buggenhout - NVISO. *Automated Adversary Emulation using Caldera*. URL: https://www.nviso.eu/en/service/21/adversary-emulation (επίσκεψη 25/05/2022).

[54] Jonas Bauters - NVISO Labs. *What's in a name? Thoughts on Red Team nomenclature*. URL: https://blog.nviso.eu/2020/01/23/thoughts-on-red-team-nomenclature/ (επίσκεψη 25/05/2022).

[55] MITRE Corporation. *Adversary Emulation Plans*. URL: https://attack.mitre.org/resources/adversary-emulation-plans/ (επίσκεψη 25/05/2022).

[56] The Center for Threat-Informed Defense. *Adversary Emulation Library*. URL: https://github.com/center-for-threat-informed-defense/adversary_emulation_library (επίσκεψη 25/05/2022).

[57] Scythe. *Community Threats Library*. URL: https://github.com/scythe-io/community-threats (επίσκεψη 25/05/2022).

[58] Blake Strom - MITRE Corporation. *Getting Started with ATT&CK: Adversary Emulation and Red Teaming*. URL: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3 (επίσκεψη 25/05/2022).

[59] Red Canary. *Atomic Red Team Homepage*. URL: https://atomicredteam.io/ (επίσκεψη 25/05/2022).

[60] Red Canary. *Atomic Red Team Homepage*. URL: https://atomicredteam.io/ (επίσκεψη 25/05/2022).

[61] Mauricio Velazco. *PurpleSharp - Homepage*. URL: https://www.purplesharp.com/en/latest/home/purplesharp.html (επίσκεψη 25/05/2022).

[62] MITRE Corporation. *CALDERA - GitHub repository*. URL: https://github.com/mitre/caldera (επίσκεψη 25/05/2022).

[63] Doug Miller - MITRE Corporation Andy Applebaum. *CALDERA - Automating Adversary Emulation*. URL: https://www.blackhat.com/docs/eu-17/materials/eu-17-Miller-CALDERA-Automating-Adversary-Emulation.pdf (επίσκεψη 25/05/2022).

[64] MITRE Corporation. *CALDERA - Homepage*. URL: https://caldera.readthedocs.io/en/latest/ (επίσκεψη 25/05/2022).

[65] DataDog. *Stratus Red Team - Homepage*. URL: https://stratus-red-team.cloud/ (επίσκεψη 25/05/2022).

[66] DataDog. *Stratus Red Team - Github*. URL: https://github.com/datadog/stratus-red-team (επίσκεψη 25/05/2022).

[67] Chris Long. *DetectionLab - Homepage*. URL: https://www.detectionlab.network/ (επίσκεψη 25/05/2022).

[68] WazeHell. *vulnerable-AD - Github repository*. URL: https://github.com/WazeHell/vulnerable-AD (επίσκεψη 25/05/2022).

[69] Carbon Black. *Invoke-APT29 - Github repository*. URL: https://github.com/carbonblack/tau-tools/tree/master/threat%5C_emulation/Invoke-APT29 (επίσκεψη 25/05/2022).

[70] RealityNet. *Attack-Coverage - Github repository*. URL: https://github.com/RealityNet/attack-coverage (επίσκεψη 25/05/2022).

[71] Security Risk Advisors. *Vectr - Homepage*. URL: https://docs.vectr.io/.