ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

Μεταπτυχιακό Πρόγραμμα

Τμήμα: Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακό Διατριβή

Εγχειρίδιο Μπλε Ομάδας

ΓΕΩΡΓΙΟΣ ΜΑΚΡΗΣ

ΜΤΕ1723

g.makris91@ssl-unipi.gr

Υπό την επίβλεψη του καθηγητή:

Κωνσταντίνος Λαμπρινουδάκης,

clam@unipi.gr

Περιεχόμενα

Εισαγωγή

Η εξέλιξη της τεχνολογίας μεγάλωνε ραγδαία και για αυτόν τον λόγο υπήρχε ραγδαία αύξηση των απειλών και τον επιθέσεων στον κυβερνοχώρο. Οι χρήστες με κακόβουλη πρόθεση, άρχισαν να χρησιμοποιούν εξελιγμένα εργαλεία και τεχνολογίες, έτσι ώστε να εκτελέσουν στοχευμένες επιθέσεις με πιο γρήγορο ρυθμό ή για να συλλέξουν τεράστιο όγκο δεδομένων ή να προκαλέσουν μεγαλύτερη ζημία σε έναν οργανισμό. Για την άμυνα αυτών των επιθέσεων έχουν αναπτυχθεί ήδη εργαλεία και τεχνολογίες.

Για την άμυνα των επιθέσεων άλλα και για την αποφυγή των καταστροφών δημιουργήθηκε το πρώτο SOC το 1975 και λειτουργούσε κυρίως για την άμυνα των οργανισμών και για κυβερνητικές υπηρεσίες. Καθώς το διαδίκτυο και η τεχνολογία εξελίχθηκε, ιοί ξεκίνησαν να εισβάλλον στα πληροφοριακά συστήματα και οι ανάγκες για ανίχνευση εισβολών και απειλών αυξήθηκαν. Το 1996 η δεύτερα γενιά SOC ικανοποίησε αυτήν την ανάγκη. Οι hackers συνέχισαν να βελτιώνουν τις μεθοδολογίες επίθεσης και αρχίσαν να πραγματοποιούν Denial of Services επιθέσεις χρησιμοποιώντας Bots και botnets μέχρι που το SOC εξελίχθηκε και απέκτησε την ικανότητα πρόληψης.

Οι επιτιθέμενοι άλλαξαν την μεθοδολογία και τις στρατηγικές τους και οι επιθέσεις που πραγματοποιήσουν θα παρέμειναν μη ανιχνεύσιμες από την υποδομή ασφάλειας ενός οργανισμού. Οι επιθέσεις του συγκεκριμένου τύπου ονομάζονται επίμονες(persistent). Το SOC διαθέτοντας τεχνολογίες APT(Advance persistence threat detection technologies)όπου τις απέκτησε το 2007 πραγματοποίησε μια άνοδο ως προς την πρόληψη και ανίχνευση των μη ανιχνεύσιμων επιθέσεων. Η τρίτη γενιά του SOC όπου ξεκίνησε με την τεχνολογία του APT, διέθετε ένα σημαντικό εργαλείο τεχνολογίας, το SIEM(Security Incidents and Event Management). Το SIEM συλλέγει αρχεία καταγραφών από πηγές, δημιουργεί ειδοποιήσεις σύμφωνα με κανόνες και σε γενικές γραμμές ευθύνεται για την διαχείριση των incidents και των event. Με το εργαλείο αυτό οι αναλυτές πραγματοποιούν ανάλυση και ανίχνευση για events και incident σε πραγματικό χρόνο Το 2013, οι ειδήμονες της ασφάλειας, συνειδητοποίησαν ότι με την προσθήκη feeds από threat intelligence με συνδυασμό της heuristic ανάλυσης του SIEM, θα υπάρξει έγκυρη ενημέρωση από παραβίαση ασφάλειας στην υποδομή του οργανισμού η ακόμα σε ένα σύστημα.

Παραπάνω περιεγράφηκε μια σύντομη αναδρομή στην ιστορία του SOC τμήματος, δηλαδή της μπλε ομάδας. Παρακάτω όμως θα αναλυθούν θέματα όπως αυτά που προαναφέραμε όπως λειτουργίες και μέλη ενός SOC τμήματος, λειτουργία ενός εργαλείου SIEM, threat hunting, αλλά και θέματα που αφορούν τον τρόπο σκέψης και την λειτουργικότητα μιας επίθεσης ενός επιτιθέμενου όπως το Cyber Kill Chain SOC και ένα diamond model που αφορά το σωστό tracking ενός incident ή event.

Κόκκινη, Μπλε και Μωβ Ομάδα

Στο χώρο της Κυβερνοασφάλειας (cybersecurity) υπάρχουν κατηγορίες ομάδων οι οποίες δεν αλληλοεπιδρούν πάντα μεταξύ τους. Συγκεκριμένα οι ομάδες αυτά συμβολίζουν τρία χρώματα, το μπλε, το κόκκινο και το μωβ. Η μπλε ομάδα αναφέρεται στην αμυνόμενη ομάδα δηλαδή το SOC. Η κόκκινη στην ethical team, δηλαδή penetration team. Η μωβ τοποθετείται ανάμεσα στην κόκκινη και στην μπλε, κυρίως σε στρατιωτικούς τομείς.

Σχετικά με την κόκκινη και μπλε ομάδα επικρατεί μια άσκηση προσομοίωσης. Η ιδέα πρωτοεμφανίστηκε πριν από καιρό, κατά την διάρκεια του πρώτου παγκοσμίου πόλεμου. Η γενική ιδέα αποτελούσε την επίδειξη μιας επίθεσης αποτελεσματικής μέσω προσομοιώσεων. Για παράδειγμα, το 1932 ο Rear Admiral Harry E. Yarnell απέδειξε την αποτελεσματικότητα μια επίθεσης στο Pearl Harbor. Εννέα χρόνια αργότερα, χρησιμοποιήθηκαν παρόμοιες τακτικές επίθεσης των Ιαπώνων στο Pearl Harbor. Η αποτελεσματικότητα των προσομοιώσεων βασίζονται σε πραγματικές τακτικές. Οι συγκεκριμένες τακτικές μπορούν να χρησιμοποιηθούν από κακόβουλο χρήστη στον στρατιωτικό τομέα. Το πανεπιστήμιο Foreign Military and CulturalStudies έχει ειδικευμένα μαθήματα για να προετοιμάσει τους συμμετέχοντες της Red Team.

Στο κομμάτι της ασφάλειας στον κυβερνοχώρο, η υιοθέτηση της προσέγγισης της κόκκινης ομάδας βοήθησε επίσης τον οργανισμό να διατηρήσει τα περιουσιακά του στοιχεία(assets) ασφαλή. Στο κομμάτι τώρα της κόκκινης ομάδας, τα μέλη πρέπει να έχουν υψηλή κατάρτιση, με πολλαπλές δεξιότητες και πλήρη επίγνωση της τρέχοντας απειλής. Επίσης τα μέλη, πρέπει να κατέχουν δεξιότητες προγραμματισμού, για να δημιουργούν δικό τους exploit, να πειραματίζονται έτσι ώστε να εκμεταλλευτούν καλύτερα τις ευπάθειες που θα μπορούν να επηρεάσουν τον οργανισμό.

Η μπλε ομάδα από την αντίθετη βοηθάει στην άμυνα ενός οργανισμού ή στην ασφάλειας μια υποδομής ή συστήματος. Το SOC περιέχει μέλη καταρτισμένα με ιεραρχική δομή με ποικίλες δεξιότητες έτσι ώστε να ανταποκριθούν αποτελεσματικά σε ένα incident. Βασική δραστηριότητα ενός SOC τμήματος είναι το monitoring(παρακολούθηση) της ασφάλειας μιας υποδομής δικτύου ή ενός συστήματος. Επίσης υπάρχουν και άλλες δραστηριότητες όπως η διαχείριση ενός incident, η παραμετροποίηση και η διαχείριση του εργαλείου SIEM. Όλα αυτά όμως θα εξηγηθούν παρακάτω.

Η μωβ ομάδα εντάσσεται ανάμεσα από την κόκκινη και την μπλε ομάδα .Ο ρόλος της μωβ ομάδας, είναι λιγότερο γνωστός αλλά εξίσου σημαντικός με τις υπόλοιπες ομάδες. Η μωβ ομάδα συνήθως αποτελείται από προσωπικό υψηλά καταρτισμένο, το οποίο. αναλαμβάνει καθήκοντα τα οποία υφίστανται τόσο στην κόκκινη όσο και στην μπλε. Δηλαδή η ομάδα της μωβ ομάδα αναλαμβάνει καθήκοντα επιθετικού άλλα και αμυντικού περιεχομένου. Συνήθως λειτουργούν ως εξωτερική ομάδα σε έναν οργανισμό, σε ιδανικές περιπτώσεις όμως ένας οργανισμός έχει την δυνατότητα να δημιουργήσει την δικιά του μωβ ομάδα.

Security Operation Center

Η μπλε ομάδα λεγόμενη ως soc, περιέχει πολλούς τομείς δραστηριότητας και πολλές ευθύνες. Μια σημαντική δραστηριότητα του είναι η παρακολούθηση ασφάλειας της υποδομής ή του συστήματος του πελάτη ή ακόμα και του ίδιου οργανισμού. Για να πραγματοποιηθεί η παρακολούθηση, τα μέλη της ομάδας του SOC, χωρίζονται σε βάρδιες 24 ωρών. Τα μέλη εργάζονται συνήθως ανά δυάδες σε 3 βάρδιες σε καθημερινή βάση. Εάν δεν υπήρχε το monitoring ως διαδικασία, η ανάλυση ενός περιστατικού ασφάλειας θα είναι δυσκολότερη καθώς η διαδικασία της ανάλυσης θα πρέπει να ξεκινήσει χειροκίνητα από τα αρχεία καταγραφής στο εργαλείο SIEM.

Το monitoring λαμβάνει χώρο σε 2 τμήματα της πληροφορικής, στο NOC και στο SOC
Το NOC(Network Operation Center) αποτελείται από ένα τμήμα, όπου κύρια αρμοδιότητα του είναι η παρακολούθηση και η συντήρηση της δικτυακής υποδομής ενός η πολλών οργανισμών.

Παρακάτω αποτυπώνεται η μορφή ενός SOC/NOC κατά την διάρκεια του monitoring.

ΜΕΛΗ

Πρώτού αναλυθούν τα μέλη του τμήματος SOC, σημαντικό είναι να αναφερθεί ο ορισμός ενός SOC.
ΤΟ SOC ορίζεται σαν μια κεντρικοποιημένη (centralized) ομάδα, αποτελούμενή από έμπειρους ανθρώπους, διαδικασίες και τεχνολογίες με σκοπό την παράδοση υπηρεσιών δυνατότητων ασφάλειας. Κύριες λειτουργίες του είναι η παρακολούθηση(monitoring), ο έλεγχος για alarms (ειδοποιήσεις).

Για την σωστή λειτουργία ενός Security Operation Center, τα μέλη του θα πρέπει να αποτελούνται από μια ιεραρχική δομή. Υπάρχουν πολλές αναφορές για τον αριθμό των μελών και τους ρόλους του SOC. Συνήθως όμως το τμήμα του SOC αποτελείται από πέντε μέλη, τα οποία είναι:

- Αναλυτής επιπέδου ένα
- Αναλυτής επιπέδου δυο
- Αναλυτής επιπέδου τρία
- Τεχνικός-Μηχανικός
- Soc Manager

Ο αναλυτής επιπέδου ένα, έχει ρόλο εκπαιδευτικής φύσης. Τις περισσότερες φορές προσλαμβάνεται για την διαδικασία του monitoring. Πέρα από την διαδικασία αυτή πολλές φορές θα χρειαστούν δεξιότητες όπως:

- Προγραμματιστικές δεξιότητες(Python, PHP and more
- Sysadmin δεξιότητες
- Δεξιότητες ασφάλειας(GCIA and more)

Το πραγματικό κομμάτι της εργασίας του είναι η ανασκόπηση στα alerts από το εργαλείο SIEM και ο καθορισμός ενός incident, δηλαδή το πόσο σημαντικό είναι ώστε να το αναθέσει στους ανώτερους του.
Σαν δεύτερο βήμα, θα πρέπει να δημιουργήσει αναφορές, τα λεγόμενα tickets για τα alerts, τα οποία χρήζουν ανασκόπηση από τους αναλυτές του επόμενου επιπέδου.
Οι αναλυτές επιπέδου ένα πραγματοποιούν σε ορισμένες συνθήκες σαρώσεις για τυχόν ευπάθειες, έτσι ώστε να παραδώσουν μια αναφορά διαφορετικού τύπου στους ανωτέρους.

Η επόμενη θέση αφορά τον αναλυτή επιπέδου δυο. Ο τίτλος του είναι incident responder και αναφέρεται στην άμεση ανταπόκριση σε incidents.
Εκτελεί όλα τα προηγούμενα καθήκοντα του αναλυτή επιπέδου ένα ά σε μειωμένο βαθμό καθώς έχει αρμοδιότητες που επισκοπούν στην βαθύτερη ανάλυση ενός Incident.
Το κύριο χαρακτηριστικό του αποτελεί την περιέργεια του και την φυσική του ικανότητα για την εξερεύνηση της βασική αιτία ενός incident. Του προσάπτεται ακόμα η ικανότητα της ψυχραιμίας κάτω από συνθήκες πίεσης.
Επιπλέον αναθεωρεί τα tickets τα οποία έχουν αναπαραχθεί από τον αναλυτή επιπέδου ένα. Χρησιμοποιεί το threat intelligence και ανασκοπεί και συλλέγει τα δεδομένα όπως configs και running processes σε συστήματα όπου χρειάζονται περαιτέρω investigation.

Ο αναλυτής επιπέδου 3 δημιουργεί αναφορές με περιεχόμενο τις ευπάθειες που υπάρχουν σε μια υποδομή δικτύου ή σε ένα σύστημα και πραγματοποιεί ανασκόπηση στα assets. Χρησιμοποιεί προηγμένο threat intelligence για την αναγνώριση των τύπων των επιθέσεων και για αυτό τον λόγο ο τίτλος του δικαιωματικά αποτελεί τον threat hunter.Επίσης κάνει χρήση pen testing για να προσδώσει αυθεντικότητα και ερευνήσει ευάλωτα σημεία εισόδου.

Ο μηχανικός είναι υπεύθυνος για την σωστή λειτουργεία όλων των εργαλείων. Διαχειρίζεται και ρυθμίζει τις παράμετρούς από διάφορα εργαλεία ασφαλείας όπως IDS,NetFlow και κανόνες συσχέτισης του SIEM.

Υπεύθυνος ενός SOC τμήματος είναι ο SOC Manager. Οι δεξιότητες που έχει είναι της επικοινωνίας και της ισχυρής ηγεσίας. Σκοπός του είναι να επιτηρεί την δραστηριότητα της ομάδας του SOC. Προσλαμβάνει, εκπαιδεύει και αξιολογεί την ομάδα. Διαχειρίζεται την διαδικασία του escalation και αναθεωρεί όλα τα incident report. Επίσης εμπλέκεται με τα ενδιαφερόμενα μέλη και τον CISO. Τέλος Πραγματοποιεί compliance reports και audit process.

Το Soc σύμφωνα με το NIST θεωρείται ως Incident Response Team. Οι κατηγορίες από την ομάδα αυτή αναλύονται ως Central Incident Response Team, ως Distributed Incident Response Team και ως Coordination Team.

Η Central Incident Response Team αποτελεί μια ομάδα εντός οργανισμού όπου διαχειρίζεται τα συμβάντα μέσα σε αυτόν τον οργανισμό. Distributed incident Response team αφορά ομάδες ανεξάρτητες όπου διαχειρίζονται πολλαπλά incidents. Η Coordination Team αφορά μια incident response ομάδα που παρέχει συμβουλές σε άλλες ομάδες. Μια ομάδα Incident Response team μπορεί είναι μια ομάδα SOC εσωτερικά σε έναν οργανισμό ή μπορεί ο οργανισμός να αναθέσει σε εξωτερική incident response ομάδα την λειτουργεία του SOC ή εν μέρη.

Μια μέρα στην ζωή του αναλυτή

Ένα πράγμα που μπορεί να χαρακτηρίσει την ζωή του αναλυτή, είναι το πόσο απρόβλεπτη μπορεί να είναι. Η εργασία του είναι επίπονη, εφόσον εργάζεται σε ένα περιβάλλον με κυλιόμενες βάρδιες. Το πρώτο του καθήκον είναι η πλήρη αναφορά της της βάρδιας του στους επόμενους αναλυτές. Σε αυτό το σημείο θα πρέπει να αναλύσει τα incidents, τα alarms ή οτιδήποτε σημαντικό έγινε στην διάρκεια της βάρδιας, έτσι ώστε οι αναλυτές της επόμενης βάρδια να έχουν μια ετκίμηση και μια ενημέρωση ως προς τα καθήκοντα τους. Η παράδοση των πληροφοριών από τον προηγούμενο αναλυτή είναι ανεκτίμητη

Κατά την διάρκεια πιο ήσυχων στιγμών τους, οι αναλυτές θα μεταβούν στο στάδιο της ανάλυσης, με σκοπό να «πιάσουν» κάποια επίθεση όπου θα παραβιάσει την ασφάλεια του συστήματος ή της υποδομής ενός οργανισμού. Υπάρχουν περιπτώσεις όπου δεν θα παραχθεί κάποια ειδοποίηση από το εργαλείο SIEM. Σε μια τέτοια περίπτωση, ο αναλυτής μπορεί να το καταλάβει ανιχνεύοντας τα αρχεία καταγραφών. Θα πρέπει να παραμείνει ψύχραιμος καθώς το event αυτό μπορεί να οδηγήσει σε false positive δηλαδή σε λάθος

εκτίμηση. Στις πιο δύσκολες μέρες, θα πρέπει να επικοινωνούν με τον προϊστάμενο τους ή ακόμα καλύτερα με τον manager τους για τυχόν configuration στα device τους, για incidents, Reports και με πελάτες για κάποια παραμετροποίηση των συστημάτων τους ή για κάποιο incident.

Ένας αναλυτής διαρκώς σκέφτεται και αναζητά στα αρχεία καταγραφών για περισσότερες πληροφορίες εφόσον έχει εξαντλήσει όλες τις αναζητήσεις στις προκαθορισμένες διαδικασίες. Όπως προαναφέρθηκε ο αναλυτής πρέπει να διαθέτει πολλές δεξιότητες και ικανότητες έτσι ώστε να ανταποκριθεί άμεσα και η εργασία του να αποδώσει καρπούς.

Ένας αναλυτής πρέπει να διαθέτει συγκεκριμένα χαρακτηριστικά όπως η επικοινωνία, η αφαιρετική σκέψη και η φυσική περιέργεια.

Η επικοινωνία θεωρείται ως σημαντικό προσόν του αναλυτή καθώς όταν κάποιο incident λάβει χώρα τότε ο αναλυτής θα πρέπει να επικοινωνήσει με τα αρμόδια μέλη για την άμεση λύση του. Η αφαιρετική σκέψη βοηθάει στην ανάλυση ενός incident, παραδείγματος χάρη η σκέψη έξω από το κουτί (out of the box) και η αναζήτηση σε αρχεία καταγραφών τα οποία δεν είναι άμεσα συ σχετιζόμενα με το incident. Η φυσική περιέργεια, ίσως εκ τω πλείστων να είναι η πιο σημαντική. Ο αναλυτής τις περισσότερες φόρες θα αναζητήσει αρχεία καταγραφών όπου του διακινούν την περιέργεια του έτσι ώστε να δημιουργήσει κανόνες για την διαχείριση ενός event.

Τα μέλη του SOC πρέπει να κατανοούν βασικούς ορισμούς έτσι ώστε να λειτουργούν αποτελεσματικά. Βασικοί ορισμοί θεωρούνται το event και το incident. Ένα event αποτελείται από οποιοδήποτε περιστατικό, το οποίο καταγράφεται σε ένα σύστημα ή σε ένα δίκτυο. Παραδείγματα από τα event μπορούν να αποτελέσουν τα εξής:

- Ένας χρήστης που συνδέεται με ένα κοινόχρηστο χώρο αρχείων,
- Έναν διακομιστή που λαμβάνει ένα email με περιεχόμενο μια ιστοσελίδα,
- Ένα τείχος προστασίας που αποκλείει μια προσπάθεια σύνδεσης.

Τα ανεπιθύμητα event όπου μπορούν να αποτελέσουν ένα incident είναι event με αρνητική συνέπεια, όπως:

- Σφάλματα συστήματος
- Αυξημένος αριθμός πακέτων
- Μη εξουσιοδοτημένη χρήση προνομίων συστήματος
- Μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα
- Εκτέλεση κακόβουλου λογισμικού

Ένα incident καθορίζεται από τον χρόνο που εμφανίζεται. Σε αυτήν την περίπτωση τα incident κατηγοριοποιούνται σε Precursor και indicator. Το incident που αποκαλείται Precursor συμβολίζει ένα incident το οποίο μπορεί να πραγματοποιηθεί στο μέλλον ενώ το incident που ονομάζεται indicator αφορά το incident στην τρέχουσα χρονική στιγμή.

Οι Precursors και οι indicators χρησιμοποιούνται σε πολλές πηγές, με τις πιο συνηθισμένες να αποτελούν λογισμικό ασφάλειας υπολογιστή και αρχεία καταγραφής.

Ένας αναλυτής θα πρέπει να είναι γνώστης και εφάμιλλος με τους δείκτες αυτές, σαφώς και με τις συσκευές-τεχνολογείς που αποτελούν τους δείκτες αυτούς.

Παρακάτω υπάρχει μία ενδεικτική λίστα με τεχνολογίες, και αρχεία καταγραφών οι ειδοποιήσεις περιγράφουν τους Precursors και τους indicators.

Ειδοποιήσεις(Alerts):

- IDPSs
- SIEMs
- Antivirus and antispam software

Αρχεία καταγραφών(Logs):

- Operating System. Service and application logs
- Network device logs

Computer security incident:

Όταν ένα event είναι υψίστης σημασίας(severity:critical), το SIEM συνήθως παράγει μια ειδοποίηση(alert). Το αποτέλεσμα της ειδοποίηση αυτής, δηλαδή η πληροφορία που παράγεται από το alert ονομάζεται περιστατικό ασφάλειας(incident). Συνήθως αποτελείται από μια παραβίαση ή μια επικείμενη απειλή παραβίασης των πολιτικών ασφάλειας των υπολογιστών. Παρακάτω περιγράφονται μερικά παραδείγματα που συντελούν ένα incident.

Παραδείγματα:

- Ένας επιτιθέμενος στέλνει ένα botnet με υψηλά αιτήματα σύνδεσης σε ένα διακομιστή ιστοσελίδας, με την προϋπόθεση να προκαλέσει "κόλλημα" της ιστοσελίδας.
- Ένας χρήστης μπορεί να παραβιάσει τα ευαίσθητα δεδομένα των χρηστών μέσα από υπηρεσίες διαμοίρασης αρχείων.
- Ένας επιτιθέμενος υποκλέβει τα στοιχεία και της πληροφορίες μια πιστωτικής κάρτας.

Δυνατότητες ενός SOC

Καθώς αναλύθηκαν οι ορισμοί που διέπουν το SOC τμήμα, σε επόμενο στάδιο θα περιγράφουν οι δυνατότητες που παρέχει ένα SOC. Εκτός από τα καθήκοντα του κάθε αναλυτή, σημαντικές είναι και οι δυνατότητες που παρέχει το SOC. Παρακάτω αναγράφονται οι δυνατότητες:

Δυνατότητες:

- Ανίχνευση και ανταπόκριση απειλών σε πραγματικό χρόνο.
  Την κατάλληλη τεχνολογία και τον βέλτιστο μέθοδο για τον εντοπισμό και ανάλυση απειλών ορίζεται από τα μέλη του SOC.
- Παρακολούθηση δεδομένων καταγραφής συστημάτων και δικτυακής κυκλοφορίας σε πλαίσιο χρόνου 24X7(24 ώρες επι 7 μέρες)
  Σε ένα soc, συχνά τα μέλη αντιμετωπίζουν καταστάσεις όπως κακόβουλη και ανώμαλή δραστηριότητα. Για να διασφαλιστεί ότι αντιμετωπίζεται σε πραγματικό χρόνο, το soc τις παρακολουθεί συνεχώς. Η παρακολούθηση αυτή ονομάζεται monitoring

- Ολοκληρωμένη και centralized ορατότητα της ασφάλειας της εταιρίας.
- Threat hunting και έρευνα απειλών(investigation).
  Τα μέλη του Soc πραγματοποιούν διαρκή, προληπτική και ενδελεχής αναζήτηση στα συστήματα και στις υποδομείς των δικτυών ώστε να αντιμετωπισθούν απειλές, οι οποίες έχουν αποκρυφθεί από τα περιμετρικά στοιχεία ελέγχου.

Τις κύριες λειτουργίες του SOC διαχειρίζονται μέσω ενός εργαλείου που ονομάζεται SIEM (System Information and Event Management).Μια siem τεχνολογία είναι ένα σύστημα λογισμικού, το οποίο αποτελείται από δυο τεχνολογίες, Το SIM και το SEM. Τα αρχικά του SIM μεταφράζονται ως Security information management System και του SEM ως Security management System. Το Sim παρέχει δυνατότητες για διαχείριση αρχείων καταγραφών όπως real-time monitoring και ανάλυση. Το Sem, λειτουργεί ως correlation μηχανή. ΤΟ Siem, με την συμβολή των SEM και SIM, προσφέρει visibility, event correlation και alerting system.

Υπηρεσίες ενός SOC

Το Soc ενός οργανισμού δεν έχει ολιγάριθμες υπηρεσίες. Οι υπηρεσίες που προσφέρει το SOC διαχωρίζονται σε reactive και proactive υπηρεσίες.
Οι Proactive υπηρεσίες προσφέρουν υπηρεσίες πρόληψης των incident και αποτελούνται από:

- Network Security Monitoring
- Threat Hunting
- Platform Health Monitoring
- Cyber Threat Intelligence
- Threat Intelligence Integration

Network Security Monitoring

Αφορά την ανάλυση, την ανίχνευση που πραγματοποιεί ένας αναλυτής καθώς και την ανασκόπηση των indicators και των alerts όπου υποδεικνύον ένα πιθανό Incident.

Threat Hunting

Το Threat hunting είναι μια διαδικασία προληπτική η οποία διερευνά εάν θα υπάρξει κάποιο intrusion ή breach. Επίσης εντοπίζει απειλές ασφάλειας, intrusions, κακή χρήση και breaches από data mining.

Platform Health Monitoring

Για την παρακολούθηση της υγείας συστημάτων, ο αναλυτής χρησιμοποιεί το εργαλείο SIEM. Στο εργαλείο SIEM η ομάδα του SOC μπορούν να δημιουργήσουν διάφορα ταμπλό (dashboard) τα οποία θα περιέχουν πληροφορίες για την υγεία των συστημάτων ενός οργανισμού άλλα και του SIEM. Το alerting σύστημα μπορεί να δημιουργηθεί μέσα από κανόνες συσχέτισης (correlation rules) του QRadar έτσι ώστε μέσα από τα ταμπλό να απεικονίζεται ως μια ένδειξη σήματος. Η παρακολούθηση των συστημάτων μέσα από

την SIEM πλατφόρμα βοηθά τον αναλυτή, να ανιχνεύσει θέματα που δημιουργούνται σε επίπεδο συντήρησης αλλά και διαθεσιμότητας συστημάτων.

Cyber Threat Intelligence

Το cyber Threat Intelligence αποσκοπεί στην ανάλυση των adversaries, των δυνατοτήτων, των κίνητρων του και των στόχων του. Ο τρόπος των advesaries που χρησιμοποιούν το cyber domain για να επιτύχουν τον στόχο τους μπορεί να ανιχνευθεί από το CTI ή αλλιώς Cyber Threat Intelligence. Ένα cyber domain αποτελείται από έναν global domain με πληροφορίες από ανεξάρτητα δίκτυα πληροφοριών τεχνολογικές υποδομές και υπολογιστικά συστήματα. Ο αναλυτής μέσω του CTI ενημερώνεται για φορείς επίθεσης, και IOC (indicators of compromise). Η ενημέρωση του πραγματοποιείται απο δικτυακές πηγές όπως SANS, TrustW Ave, CrowdStrike και όχι μόνο.

Threat Intelligence Integration

Το threat Intelligence Integration αφορά την ενσωμάτωση από πηγές threat intelligence (feeds) σε διάφορα συστήματα όπως ένα NGFW (next generation firewall). Στο τμήμα του SOC σημαντική είναι η προσεκτική επιλογή των threat intelligence feeds στο εργαλείο SIEM. Τα threat intelligence feeds ενσωματώνονται στο σύστημα του SIEM για να βελτιώσουν το alerting σύστημα και την αναγνώριση malicious sources, destinations, domains και άλλα. Με την συγκεκριμένη ενσωμάτωση και το cyber threat intelligence ο αναλυτής έχει την δυνατότητα να ανταποκριθεί άμεσα σε ένα incident άλλα και να ενημερώσει τα αρμόδια μέλη και τμήματα για την αντιμετώπιση του.

Reactive Services

Τα Reactive Services αφορούν υπηρεσίες όπου έχουν αντιδραστικό παράγοντα. Δηλαδή είναι υπηρεσίες ενεργητικού χαρακτήρα οι οποίες αποσκοπούν στην άμεση ανταπόκριση των incidents.

Παρακάτω αναφέρονται επιγραμματικά και αναλυτικά οι reactive υπηρεσίες:

- Monitor Alerts
- Analysis
- Manage Incident Response
- Vulnerability Management
- Forensics
- Reporting
- Malware Analysis
- Intrusion Detection
- Audit
- Notification Refinement

Monitor Alerts

Η παρακολούθηση των alerts είναι λειτουργεία όπου εντάσσεται σε καθημερινό επίπεδο και αποτελεί τον σκελετό του τμήματος SOC. Οι αναλυτές παρακολουθούν την υποδομή του πελάτη για alarms, incidents, την υγεία της ασφάλειας μιας πλατφόρμας, ενός συστήματος ή ακόμα μια υποδομής δικτύου ή συστημάτων με απώτερο σκοπό την ενημέρωση για τυχόν αποκλείσεις, παραμετροποιήσεις ή incidents στον κατάλληλο οργανισμό. Φυσικά η εταιρία που στεγάζεται συνήθως προσφέρει λύσεις τεχνολογικές

για την αντιμετώπιση προβλήματος. Μια επιπλέον λύση εκτός από τις υπηρεσίες του SOC θα μπορούσε να προσφέρει ένας οργανισμός σε έναν πελάτη όσο αφορά την ασφάλεια, θα ήταν η πώληση ενός πακέτου Advance Malware Protection. Φυσικά θα μπορούσε να πωληθεί η συγκεκριμένη υπηρεσία μέσω του τμήματος SOC, όμως συνήθως υπάρχει συγκεκριμένο τμήμα σε έναν οργανισμό που διαχειρίζεται και πουλάει πακέτα ασφάλειας, τα Presales όπου αποτελείται από τον Manager και τους μηχανικούς Presales

Analysis

Όσο σημαντικές είναι οι διεργασίες του SOC όπως το alarm response, incident response και forensic άλλο τόσο είναι η ανάλυση. Όσο αφορά την ανάλυση τα μέλη του SOC θα ανιχνεύσουν events τα οποία κατηγοριοποιούνται ως incidents, θα συντονίσουν λειτουργίες αναφοράς και θα βοηθήσουν στις προσπάθειες εξάλειψης(eradication). Για την βελτίωση των συστημάτων ασφαλείας, θα πληροφορήσουν όσο καλύτερα γίνεται το κατάλληλο τμήμα με τις κατάλληλες πληροφορίες.

Manage Incident Response

Τα μέλη του SOC διαχειρίζονται τα incidents μέσω του εργαλείου SIEM. Για να διαχειριστούν τα incidents τα μέλη θα πρέπει να έχουν αρχειοθετημένες πολιτικές διαχείρισης κατηγοριοποιημένες ανά τύπο incident, έτσι ώστε να μπορούν να ανταποκριθούν στο κάθε ένα ξεχωριστά. Συνήθως ο Soc manager είναι υπεύθυνος για την επεξήγηση διαδικασιών ανταπόκρισης περαστικών στους αναλυτές.

Vulnerability Management

Ο SOC Manager έχει την δυνατότητα να εκτελέσει και να τρέξει ένα πρόγραμμα ευπαθειών. Δεν θα πρέπει να αναθέσει το έργο αυτό στο τμήμα του SOC και θα πρέπει να είναι πολύ προσεχτικός στο τι μπορεί να χειριστεί το τμήμα του SOC. Επίσης ο ρόλος του, τον καθιστά υπεύθυνο για τον σχεδιασμό και το deployment ενός full scope Vulnerability Assessment και Vulnerability Management πρόγραμμα. Μόλις το πρόγραμμα είναι έτοιμο για deployment, οι αναλυτές μετά το στάδιο αυτό θα μπορέσουν να πραγματοποιήσουν αναζητήσεις, να ενημερωθούν και να εντοπίσουν τις ευπάθειες του κάθε συστήματος και να ενημερώσουν τον αντίστοιχο διαχειριστή ασφάλειας.

Forensics

Συνήθως τα Forensics απασχολούν τις κόκκινες ομάδες όπως μια penetration testing ομάδα. Σε κάθε άλλη περίπτωση εάν ο οργανισμός περιέχει την ομάδα του SOC ως ενσωματωμένο τμήμα της και εμπεριέχει διαδικασίες για forensic τότε το τμήμα του SOC είναι σε θέση να υλοποιήσει τις διαδικασίες αυτές. Εάν ο οργανισμός δεν διαθέτει κόκκινη η μπλε ομάδα τότε μπορεί να αναθέσει το Forensic support σε έναν τρίτο οργανισμό. Οι διαδικασίες του forensic support αποσκοπούν στον έλεγχο των αρχείων από ένα σύστημα αρχείων το οποίο βρίσκεται σε ένα τερματικό, σε ένα σύστημα ή σε ένα σύστημα. Τα αρχεία αυτά μπορεί να περιέχουν κακόβουλο λογισμικό ή διαγραμμένα δεδομένα από τον δίσκο. Στο εργαλείο του SIEM υπάρχει η δυνατότητα της ανάλυσης των forensics. Οι αναλυτές μπορούν να εξάγουν σημαντικά στοιχεία όπως τους χρόνους εκτέλεσης του κάθε αρχείου, την αλλαγή ή την εκτέλεση από κάποιον χρήστη, την

ανίχνευση κακόβουλων λογισμικών στα αρχεία αυτά και άλλα πολλα τα οποια μπορούν να συντελέσουν μια αναφορά ως προς τον manager.

Reporting

Οι αναφορές μπορούν να έχουν περιεχόμενο όπως alerts, incidents ή ακόμα να περιέχουν απαιτήσεις συμμόρφωσης η γενικούς IT ελέγχους για το monitoring. Οι αναφορές που αφορούν τα incidents συνήθους στέλνονται σε πελάτες σε εβδομαδιαία ή μηνιαία βάση. Οι αναλυτές μέσω του ticketing system όπου ανασκοπεί στην ενημέρωση του πελάτη για incidents εξάγουν σημαντικές πληροφορίες, έτσι ώστε να τις εξάγουν στις αναφορές που στέλνουν.

Malware Analysis

Το εργαλείο SIEM έχει την δυνατότητα λήψης αρχείων καταγραφών και feeds από το Advance Malware Protection (AMP). Ο αναλυτής επιπέδου δυο και τρία μπορεί να περιηγηθεί στο interface του AMP και να κατεβάσει από εκεί ένα αρχείο που κατηγοριοποιείται σαν malware. Δεν είναι η βέλτιστή τεχνική καθώς το AMP περιέχει δικιά του βάση δεδομένων ή κάποια γνωστή όπως Virus total με την προϋπόθεση να ελέγχει εάν ένα αρχείο είναι κακόβουλο ή όχι.

Intrusion Detection

Υπάρχουν πολλά συστήματα ανίχνευσης όπως Snort, Suricata τα οποία μπορούν να γίνουν deploy πάνω σε ένα δίκτυο ή σε έναν host. Φυσικά αυτές οι τεχνολογίες μπορούν να λειτουργήσουν μαζί με ένα τοίχος προστασίας έτσι ώστε να προσφέρουν πλήρη ενημέρωση στον αναλυτή μέσω του εργαλείου SIEM.

Audit

Ο έλεγχος των αρχείων καταγραφών του εργαλείου SIEM αφορά την διαδικασία του audit. Ο τεχνικός ή ο αναλυτής επιπέδου δυο η τρία περιηγείται στην κονσόλα και αναλύει τα αρχεία καταγραφών ελέγχου. Στο σημείο εκείνο μπορεί να επιβεβαιώσει τις χρονικές στιγμές εισόδου κάθε χρήστη, τις ενέργειες τους άλλα μπορεί να επιβεβαιώσει τον έλεγχο και την διαθεσιμότητα του εργαλείου SIEM

Notifications

Οι ειδοποιήσεις αποτελούν ένα κομμάτι αρκετά χρήσιμο για την ομάδα του SOC. Παραδείγματος χάρη η ομάδα του Soc στέλνει κάποια threat detected, τα οποία περιέχουν αρχεία υπολογιστή ή συστήματος. Τα αρχεία αυτά μπορούν να θεωρηθούν κακόβουλα και να αποτελούν ένα malware ή ένα adware. Στην συνέχεια ο αναλυτής μετά από ανάλυση, θα στείλει μια αναφορά με το κακόβουλο αρχείο στον αντίστοιχο πελάτη με τις απαραίτητες πληροφορίες. Η διαδικασία αυτή μπορεί να αυτοματοποιηθεί μέσα από το εργαλείο SIEM και τα threat detected events να αποστέλλονται κάθε φορά αυτόματα.

Attack vector

Σύμφωνα με το NIST καθώς είναι ο επίσημος οδηγός στον τομέα της ασφάλειας, attack vector ονομάζουμε ένα τμήμα ενός μονοπατιού μιας επίθεσης. Η επίθεση αυτή εκμεταλλεύεται μια ευπάθεια έτσι ώστε να αποκτήσει πρόσβαση στο στοχευμένο σύστημα. Ένα attack vector μπορεί να περιλαμβάνει μια πηγή κακόβουλου περιεχομένου όπως, ένα επεξεργαστή ο οποίος κατά πάσα πιθανότητα διαθέτει ευπάθειες και περιέχει κακόβουλο περιεχόμενο. Παρακάτω αναγράφονται τα attack vector επιγραμματικά.

Attack vector μπορεί να αποτελεί:

- Ένα κακόβουλο συνημμένο email ή ένας κακόβουλος σύνδεσμος σε ένα email
- Κακόβουλο περιεχόμενο ιστοσελίδας
- Μια υπηρεσία δικτύου η οποία είναι ευάλωτη σε επιθέσεις ή παραβιασμένη(compromised)
- Μια συνομιλία η οποία έχει υποστεί social engineering από έναν κακόβουλο επιτιθέμενο. Δηλαδή ο κακόβουλος χρήστης έχει χρησιμοποιήσει τρόπους επικοινωνίας όπως τηλέφωνο και email για υποκλοπή ευαίσθητων δεδομένων από τον χρήστη. Στα ευαίσθητα δεδομένα συμπεριλαμβάνονται στοιχεία όπως τα credential, ημερομηνία γέννησης, αριθμοί κοινωνικής ασφάλισης, πληροφορίες λογαριασμού και άλλα
- Δεδομένα προσωπικού χαρακτήρα από τα κοινωνικά μέσα τα οποία συλλέγονται από τον κακόβουλο χρήστη για την εκτέλεση μιας στοχευμένης επίθεσης
- Μια δικτυακή πόρτα συστήματος, η οποία θα μπορούσε να οδηγήσει σε υπηρεσίες οι οποίες είναι εκτεθειμένες, έτσι ώστε να οδηγήσει τον επιτιθέμενο στην εκμετάλλευση της πληροφορίας αυτήν
- Μια βάση δεδομένων με προεπιλεγμένα credential ή χωρίς credential.
- Μια συσκευή η οποία υπάγεται σε μια υποδομή δικτύου με προεπιλεγμένα credential ή ο επιτιθέμενος να πραγματοποιήσει εικασίες με εύκολες επιλογές.

Use cases

Οι περισσότεροι οργανισμοί στην σημερινή μέρα, έχουν ανάγκη να αναπτύξουν μια λύση διαχείρισης συμβάντων και συμβάντων ασφαλείας (SIEM) ως προληπτικό μέτρο για την διαχείριση απειλών(threat management), έτσι ώστε να αποκτήσουν ένα visibility της ασφάλειας του οργανισμού. Αυτή η ανάγκη προκύπτει από τις αυξανόμενες τάσεις και μορφές επιθέσεων που ανανεώνονται μέρα με την μέρα και διαθέτουν ποικιλομορφία.

Στην ουσία use case θεωρείται ένα συγκεκριμένο event ή μια συγκεκριμένη κατάσταση στην οποία συνήθως σχετίζεται μια συγκεκριμένη απειλή. Το use case ανιχνεύεται και αναφέρεται από ένα εργαλείο ασφάλειας. Στην ουσία αποτελεί μια μεθοδολογία που χρησιμοποιείται από το τμήμα του SOC για τον προσδιορισμό και την οργάνωση τεχνικών και οργανωτικών απαιτήσεων για τον εντοπισμό και την αντιμετώπιση συγκεκριμένων απειλών.

Τα use cases αποτελούν βάση για την ανάλυση αρχείων καταγραφής σε κάθε SIEM και προσδιορίζουν τα αρχεία καταγραφών που έχουν αναλυθεί και τον τύπο της ανάλυσης πάνω στα αρχεία καταγραφών.

Παρακάτω αναγράφονται παραδείγματα από use cases ενός οργανισμού, τα οποία είναι χρήσιμα για την βελτίωση και την ανίχνευση ενός εργαλείου SIEM.

Παραδείγματα:

- **DOS**

Το DOS αποτελεί μια επίθεση εναντίων ενός υπολογιστικού συστήματος ή μια υπηρεσίας που έχουν ως σκοπό να καταστήσουν το υπολογιστικό σύστημα ανίκανο ή την υπηρεσία ανίκανη να δεχτούν άλλα αιτήματα σύνδεσης. Ένας μέθοδος επίθεσης είναι η αποστολή υπερβολικού μεγάλου αριθμού ψεύτικων αιτήσεων, με απώτερο σκοπό την μη διαθεσιμότητα και εξυπηρετικότατα των συστημάτων σε συστήματα που χρειάζονται την υπηρεσία αυτή. Το SIEM περιέχει τα αρχεία καταγραφής της κίνησης του δικτύου, έτσι ώστε να ενημερώνει για κακόβολους αποκλίσεις ή αυξήσεις σε σχέση με το ομοιόμορφη κίνηση δικτύου(baseline)..

- **Εντοπισμός κακόβουλου λογισμικού**
  Καθώς οι επιθέσεις αυξάνονται σε αριθμό και είναι οι μορφές από αυτές είναι ποικίλες, για την αντιμετώπιση τους σημαντικό ρόλο αποτελούν τα εργαλεία του network monitoring και οι threat detection λύσεις για την ανίχνευση απειλών. Το SIEM καθώς μπορεί να διαθέσει αυτές τις λειτουργίες χρησιμοποιεί επίσης machine learning δυνατότητες για να εντοπίσει το κακόβουλο λογισμικό στην υποδομή του δικτύου, σε ένα τερματικό ή σε ένα σύστημα.

- **Προστασία από απώλεια δεδομένων**
  Στον Γενικό Κανονισμό Προστασίας Δεδομένων ιδιαίτερη σημασία έχει η προστασία των ευαίσθητων δεδομένων. Για τον μη παραβιάσιμό των δεδομένων αυτών υπάρχουν άρθρα και διατάξεις. Για έναν οργανισμό οπού συμμορφώνεται με τον ΓΚΠΔ πρέπει να εκτελέσει ορισμένες ενέργειες για την προστασία των δεδομένων αυτών. Σε πρώτο στάδιο πρέπει να προστατεύσει τις πληροφορίες ευαίσθητου τύπου και να μην αποκαλύψει σε τρίτους τα δεδομένα αυτά. Επίσης απαραίτητη είναι η παρακολούθηση των συστημάτων που ορίζονται ως critical για την αποφυγή απώλεια δεδομένων. Οι διαχειριστές πρέπει να εκτελέσουν ενέργειες αποκλεισμού, δικαιωμάτων και πρόσβασης στους χρήστες που χρησιμοποιούν τις υπηρεσίες διαμοιρασμού δεδομένων εκτός οργανισμού

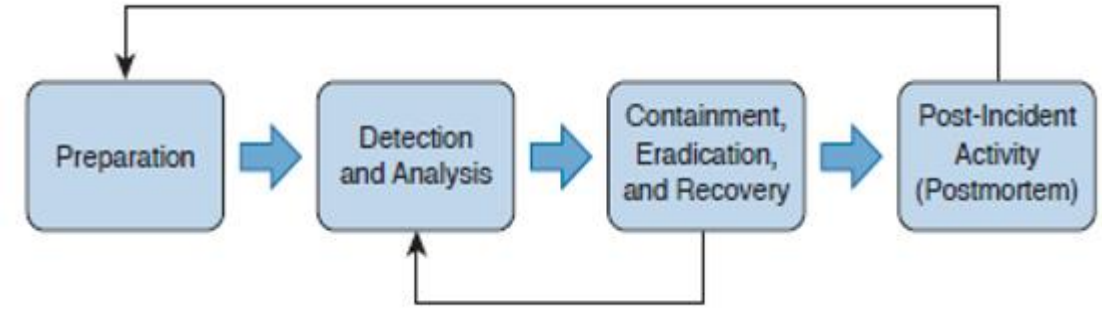
Διαχείριση συμβάντος

Οι αναλυτές καθώς έχουν πραγματοποιήσει investigation και monitoring, θα ανιχνεύσουν κάποιο incident. Η κυριότερη διαδικασία που αφορά όλη την δραστηριοποίηση του SOC γύρω από ένα Incident είναι η διαχείριση συμβάντος. Ο οδηγός NIST εμβαθύνει λεπτομερώς σε ότι αφορά την διαχείριση συμβάντος. Στην περίπτωση όπου μια εταιρία θέλει να επιτύχει στην διαμόρφωση και στην δημιουργία

ενός SOC περιβάλλοντος, θα πρέπει να είναι ενήμερη σύμφωνα με την δημοσίευσή του NIST 800-61.

ΤΟ NIST σε ένα κομμάτι του αναφέρεται στην διαχείριση συμβάντος μιας CSIRT ομάδας. Μια ομάδα CSIRT αναφέρεται ως μια ομάδα Infosec ή μια ομάδα SOC. Η ομάδα αυτή πρέπει να είναι εφάμιλλή με τις τέσσερις φάσεις της διαχείρισης συμβάντος.

Παρακάτω στο σχήμα αποτυπώνονται οι τέσσερείς φάσεις της διαχείρισης συμβάντος.



Τέσσερις φάσεις:

- Προετοιμασία
- Ανίχνευση και Ανάλυση
- Περιορισμός, εξάλειψη και αποκατάσταση
- Post Incident Activity (

Προετοιμασία

Η φάση της προετοιμασίας παίζει σημαντικό ρόλο, καθώς οι μεθοδολογίες απόκρισης περιστατικών δίνουν έμφαση στην προετοιμασία.
Με τον τρόπο αυτό, ο οργανισμός είναι έτοιμος να ανταποκριθεί σε περιστατικά ασφάλειας, αλλά και να προλάβει, προτρέψει συμβάντα ασφάλειας διασφαλίζοντας ότι τα συστήματα, οι εφαρμογές και τα δίκτυα λειτουργούν σε ασφαλής υποδομή.
Η φάση της προετοιμασίας, εμπεριέχει επίσης τα ακόλουθα βήματα:

- Δημιουργία διαδικασιών για την επικοινωνία του SOC με τα υπόλοιπα μέλη. Ο σκοπός είναι ενημέρωση για τον τρόπο διαχείριση συμβάντων και την αποφυγή λαθών ως προς αυτήν.
- Διασφάλιση ότι ο οργανισμός διαθέτει κατάλληλο υλικό(hardware) και λογισμικό για ανάλυση συμβάντων
- Δημιουργία πολιτικών για εκτίμηση κινδύνων εντός του οργανισμού
- Διασφάλιση ότι ο οργανισμός έχει υλοποιήσει κατάλληλα το host και network security και τις λύσεις πρόβλεψης malware(κακόβουλου λογισμικού)
- Ανάπτυξη της εκπαίδευσης των εργαζομένων

Ο οργανισμός πρέπει να λάβει υπόψιν του, τα διαθέσιμα εργαλεία και τους πόρους που θα προσαρμόσει στο τμήμα του SOC. Το SOC επιπλέον μπορεί να χρησιμοποιήσει με την έγκριση του οργανισμού δικούς τους πόρους όπως μηχανές αναζήτησης για την ανάλυση μιας IP ή ενός αρχείου.

Ανίχνευση και Ανάλυση

Πολλά incident και πολλά breaches συμβαίνουν σε μια υποδομή ενός οργανισμού. Κάποια από αυτά είναι ανιχνεύσιμα για αρκετό διάστημα. Η δικτυακή υποδομή είναι γεμάτη από «κρυφά σημεία», όπου η ανώμαλη κίνηση παραμένει μη ανιχνεύσιμη. Απαραίτητη είναι εδώ η φάση της ανίχνευσης και της ανάλυσης

Η incident response ομάδα πρέπει να αντιδράσει γρήγορα έτσι ώστε να αναλύσει και να επικυρώσει το περιστατικό(incident). Σύμφωνα με το NIST υπάρχουν προκαθορισμένες διαδικασίες όπου θα πρέπει να ακολουθήσει κάποιος αναλυτής. Οι διαδικασίες αυτές αναφέρονται επιγραμματικά παρακάτω:

Διαδικασίες

- Κατανόηση κανονικής συμπεριφοράς δικτύου
- Χρησιμοποίηση search engine
- Φιλτράρισμα δεδομένων
- Δημιουργία πολιτικής διατήρησης αρχείων καταγραφών
- Εκτέλεση sniffer πακέτων για την συλλογή επιπλέον δεδομένων
- Γνώμη διαφορετικών τύπων επιθέσεων και attack vector.
- Διατήρηση συγχρονισμένων ρολογιών όλων των συστημάτων

Περιορισμός, εξάλειψη και αποκατάσταση

Εφόσον έχουμε ανιχνεύσει και αναλύσει τα περιστατικά ασφαλείας, ο οργανισμός περνάει στην επόμενη φάση όπου είναι η φάση του περιορισμού, της εξάλειψης και της αποκατάστασης. Η συλλογή και η διαχείριση αποδεικτικών στοιχείων, ο προσδιορισμός των μέσων επίθεσης και η επιλογή στρατηγικής για την ύπαρξη αποτελεσματικού περιορισμού, η εξάλειψης μιας επίθεσης άλλα και ανάκαμψη από αυτήν αποτελούν την φάση του περιορισμού, εξάλειψης και αποκατάστασης.

Τα Κριτήρια για προσδιορισμό κατάλληλής στρατηγικής περιορισμού, εξάλειψης και αποκατάστασης είναι:

- Πιθανή ζημία ή κλοπή πόρων
- Ανάγκη διατήρησης αποδεικτικών στοιχείων
- Διαθεσιμότητα υπηρεσιών
- Χρόνος και πόροι που απαιτούνται για την εφαρμογή της στρατηγικής
- Αποτελεσματικότητα στατηγικής
- Διάρκεια της λύσης, για παράδειγμα πόσο χρονικό διάστημα χρειάζεται ή λύση έκτακτης ανάγκης;

Post Incident Activity

Η τελική φάση ονομάζεται post incident activity, η οποία αποτελεί την δραστηριότητα της ομάδας μέτα το incident. Από το περιστατικό οι αναλυτές διδαχθήκανε κάποια μαθήματα όσο αφορά την διαχείριση πληροφοριών και την άντληση τους από πηγές. Τα μαθήματα αυτά πρέπει να τα μεταφέρουν στον manager τους έτσι ώστε να αλληλοεπιδρούν και να ανταλλάσσουν απόψεις. Ο Manager θα συμβουλέψει τους αναλυτές και θα μεταφέρει τα λόγια τους στα ανώτερα στελέχη. Η διατήρηση αποδεικτικών στοιχείων και η σωστή χρησιμοποίηση δεδομένων που αφορούσαν το περιστικό αποτελούν στοιχεία του post incident activity.

Όπως προαναφέρθηκε, σημαντικές είναι οι συναντήσεις μετά το incident. Στην συνάντηση θα διεξαχθούν θέματα και ερωτήσεις όπως:

- Τι ακριβώς έγινε, και σε ποια χρονική στιγμή;
- Πόσο καλά αντιμετώπισε το περιστατικό η διεύθυνση;
- Ακολούθησαν τεκμηριωμένες διαδικασίες; Ήταν επαρκείς;
- Ποιες διορθωτικές ενέργειες μπορούν να αποτρέψουν παρόμοια συμβάντα στο μέλλον;
- Ποια indicators και ποια processors πρέπει να παρακολουθούνται τακτικά;

Alerting

Στην διάρκεια της μέρας του, καθώς ο αναλυτής διερευνά incident μπορεί να παρατηρήσει και πολλά εσφαλμένα incident όπου παράχθηκαν από ψευδείς συναγερμούς. Για τον λόγο αυτό πρέπει να είναι εφάμιλλος με τέσσερις έννοιες:

- False positive
- False negative
- True positive
- True negative

False postive

Περιγράφει μια κατάσταση στην οποία μια συσκευή ασφαλείας (security device) ενεργοποιεί έναν alarm ή ένα offense αλλά στην ουσία δεν υπάρχει κακόβουλη δραστηριότητα ή πραγματική επίθεση. Με άλλες λέξεις, η κατάσταση αυτή θα μπορούσε να ονομαστεί "ψευδής συναγερμός"

False negative

Περιγράφει την ανικανότητα της συσκευής π.χ τείχος προστασίας, να εντοπίσει αληθινά συμβάντα ασφαλείας.

True Positive

Η επιτυχής αναγνώριση μια επίθεσης ή ενός κακόβουλου συμβάντος.

True negative

Intrusion detection device αναγνωρίζει μια συμπεριφορά ή οποία είναι πραγματικά αποδεκτή

Ο αναλυτής εννοείται πρέπει να είναι σε θέση να ξεχωρίζει εάν προέκυψε ένας ψευδής συναγερμός ή όχι. Πολλές φορές, υπάρχει περίπτωση να μπερδευτεί με τους ορισμούς αυτούς. Με την εξοικείωση όμως και την συνεχή παρακολούθηση και ανάλυση των incident θα είναι σε θέσει να τα ξεχωρίσει. Ένα παράδειγμα, το οποίο βοηθάει τον αναλυτή, ειδικά επιπέδου ένα είναι το εξής:

True Positive (TP): • Πραγματικότητα: Ο λύκος απείλησε • Ο βοσκός είπε: "Λύκος" • Αποτέλεσμα: Ο βοσκός είναι ήρωας	**False Postive (FP):** • **Πραγματικότητα: Κανένας λύκος δεν απείλησε** • **Ο βοσκός είπε: " Λύκος"** • **Αποτέλεσμα: Οι κάτοικοι νεύριασαν επειδή ο βοσκός τους ξύπνησε**
False Negative (FN): • **Πραγματικότητα: Ο λύκος απείλησε** • **Ο βοσκός είπε: "Δεν υπάρχει λύκος"** • **Αποτέλεσμα: Ο λύκος έφαγε όλα τα πρόβατα**	True Negative (TN): • Πραγματικότητα: Κανένας λύκος δεν απείλησε • Ο βοσκός είπε: "Δεν υπάρχει λύκος" • Αποτέλεσμα: Όλοι είναι καλά

IBM QRadar

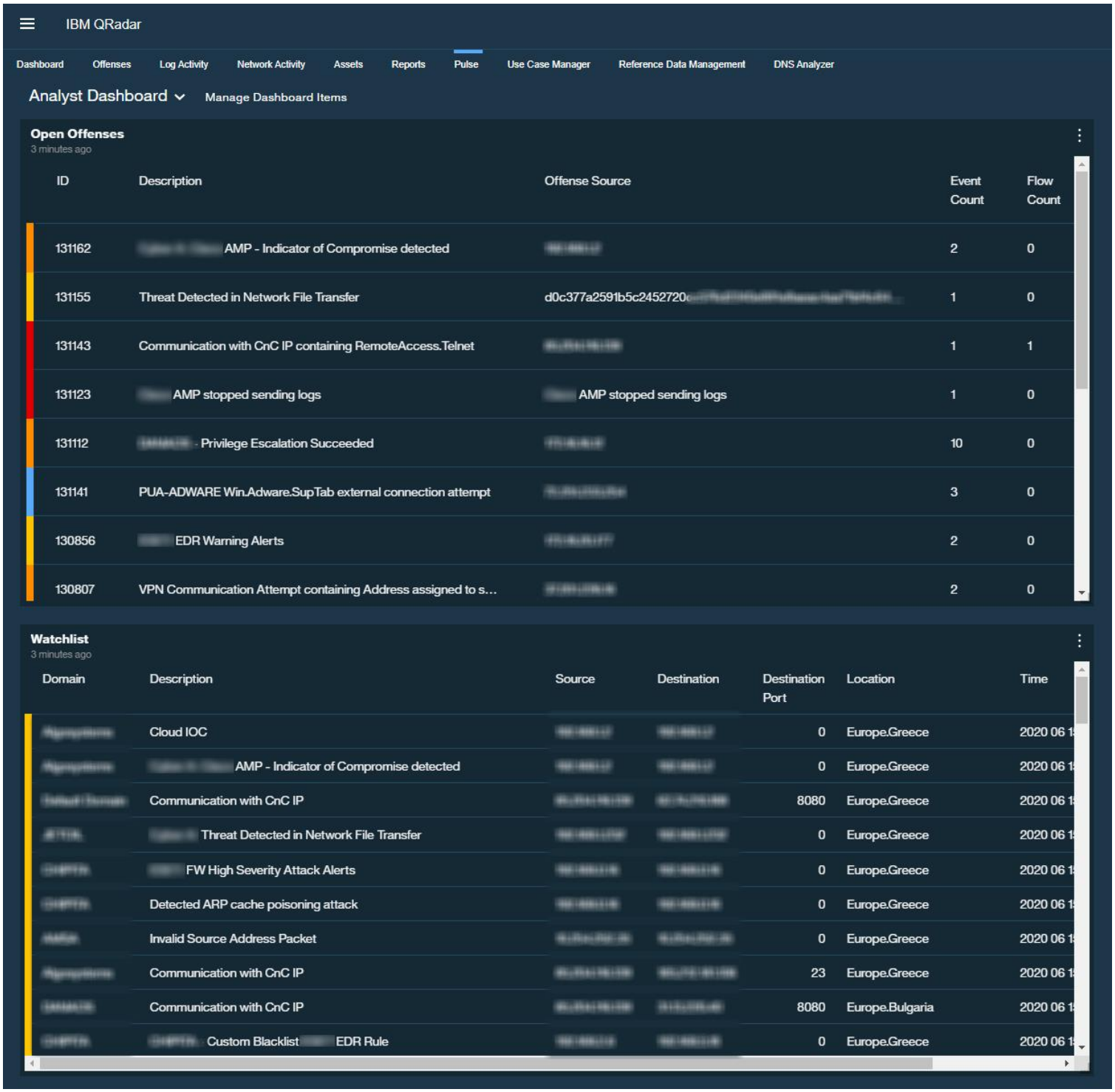
Στα πλαίσια της εργασίας χρησιμοποιήθηκε το εργαλείο IBM QRadar όπου είναι ένα εργαλείο SIEM. Ο αναλυτής μέσα από αυτό το εργαλείο μπορεί να πραγματοποιήσει ανάλυση, παρακολούθηση των alerts και άλλα.

Στην πρώτη εικόνα του κειμένου αποτυπώνεται η βασική διαδικασία ενός αναλυτή το monitoring. Η διαδικασία αυτή αφορά την παρακολούθηση ασφάλειας των συστημάτων και των υποδομών ενός δικτύου. Σε έναν χώρο του soc, υπάρχουν οθόνες μεγάλου μεγέθους ώστε οι αναλυτές να πραγματοποιήσουν το λεγόμενο monitoring. Οι τρεις παρακάτω εικόνες μπορούν να προβληθούν στις τηλεοράσεις. Ο αναλυτής καθώς εκτελεί την ανάλυση ή πραγματοποιεί έρευνα στο εργαλείο SIEM, θα πρέπει ανά τακτά διαστήματα να παρακολουθεί το monitoring 1,2,3 (αντίστοιχες εικόνες παρακάτω). Ο αναλυτής πρέπει να διακρίνει γρήγορα και εύκολα την σημαντικότητα του κάθε incident. Στις εικόνες monitoring 1,3 ο αναλυτής αναγνωρίζει την σημαντικότητα από τον χρωματισμό των πεδίων. Στο ταμπλό του αναλυτή στις εικόνες Monitoring 1,2 αναπαρίσταται η εξής βαθμολόγηση.

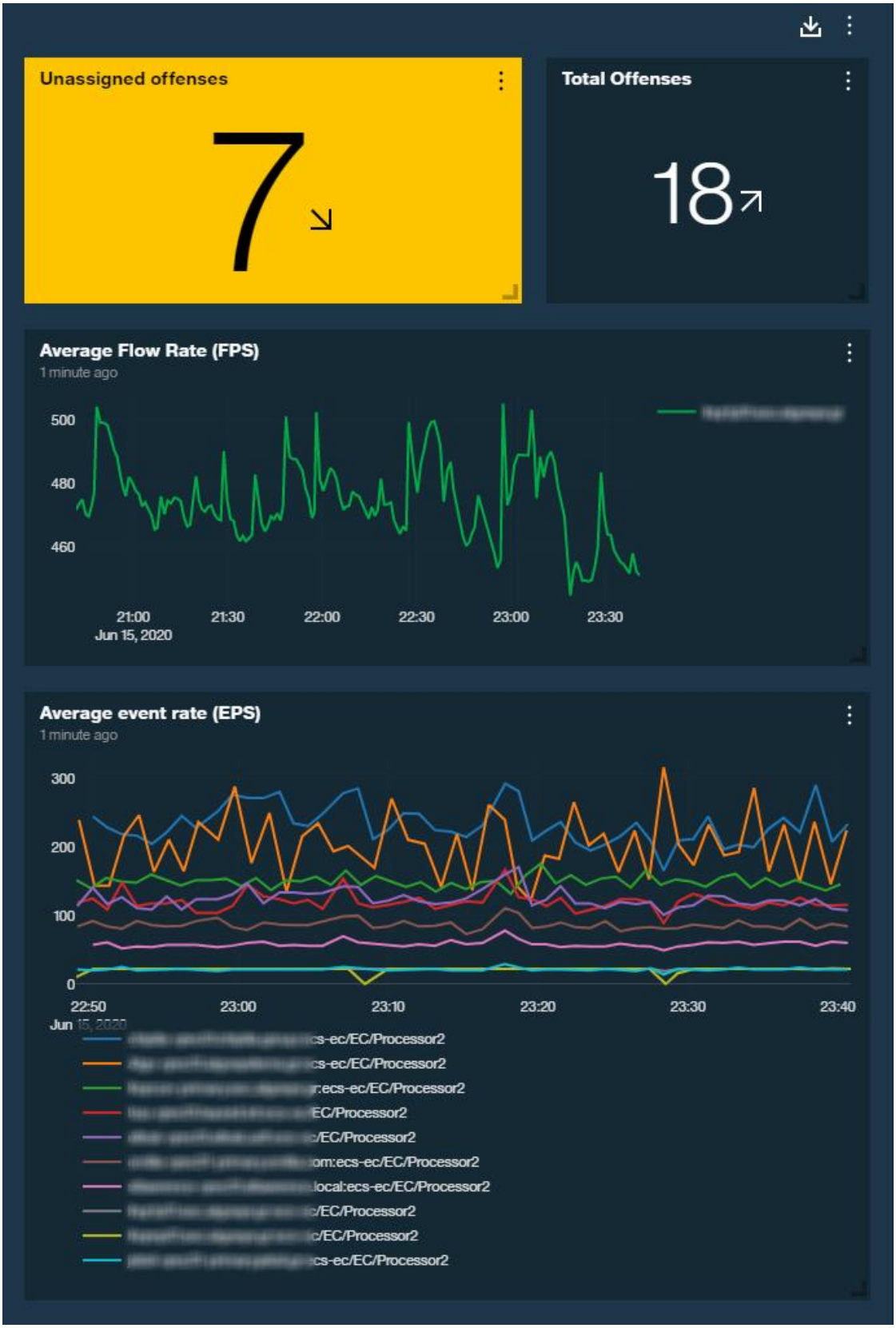
- 8-10 Κόκκινο
- 6-8 Πορτοκαλί
- 4-6 κίτρινο
- 1-4 μπλε

Ο αριθμήσιμός σχετίζεται με το severity του κάθε alert, δηλαδή με την σημαντικότητα του. Η βαθμολόγηση που αναφέρθηκε γίνεται με φθίνουσα σειρά ως προς το επίπεδο επικινδυνότητας. Το κόκκινο θεωρείται το πιο κρίσιμο(critical) και είναι το πρώτο πράγμα που ερευνά ο αναλυτής. Στην εικόνα Monitoring1 ως κόκκινη ειδοποίηση(alert) παρατηρείται το event:Communication with CnC IP containing RemoteAccess Telnet.

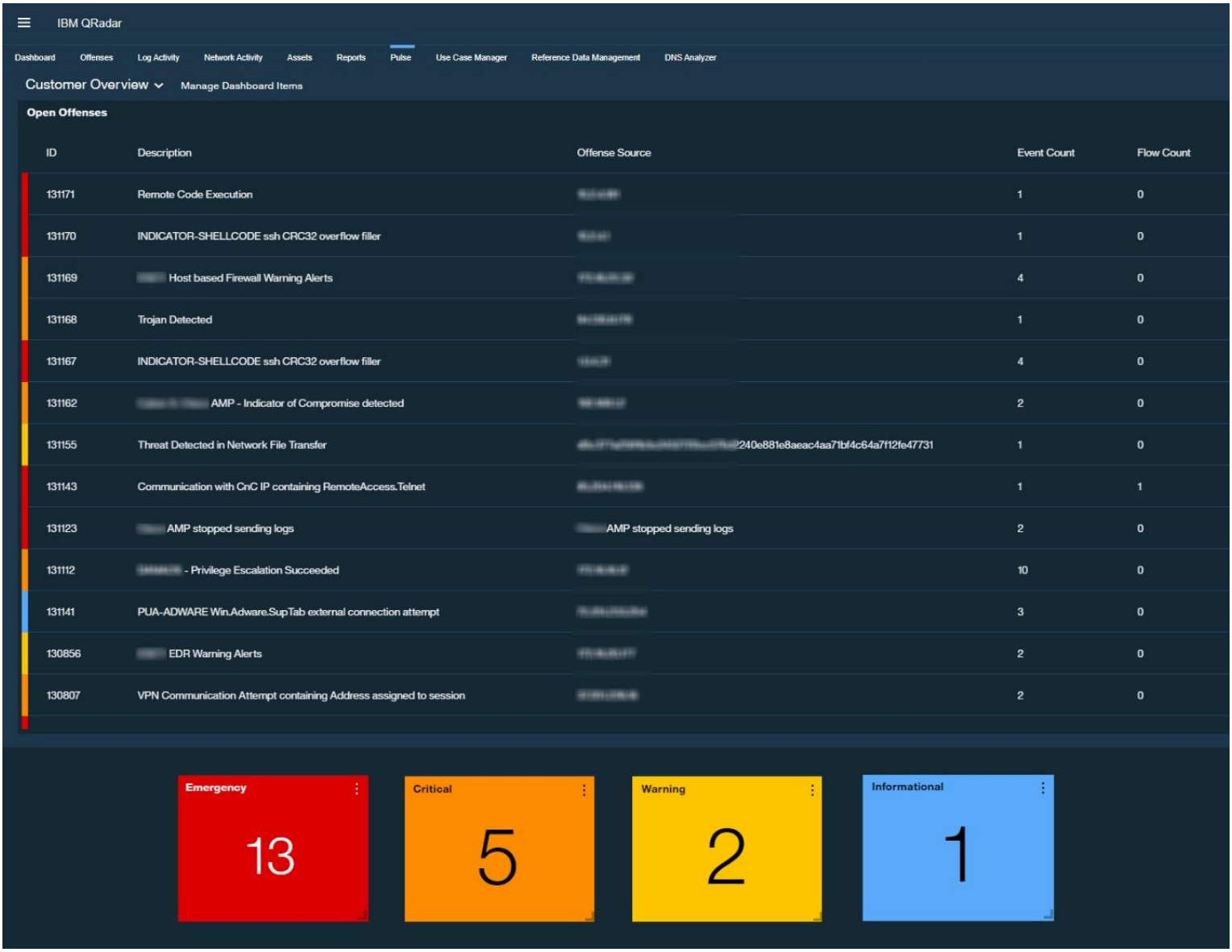
Το event αφορά μια επικοινωνία με botnet cnc server remote to local. Η source IP κατηγοριοποιείται από xforce ως botnet cnc με confidence value >60



Monitoring1



Monitoring2



Monitoring3

Οι αναλυτές ανεξαρτήτου επιπέδου χρησιμοποιούν το παράθυρο των offenses.Συγκεκριμένα ο αναλυτής επιπέδου ένα αξιοποιεί την χρησιμότητα του παραθύρου αυτού, περισσότερο από τους υπόλοιπους αναλυτές επιπέδου δυο και τρία. Στο παράθυρο offenses, ο αναλυτής έχει την δυνατότητα να παρακολουθήσει το κάθε alert ή offense. Με τον τρόπο αυτό ανιχνεύει στην υποδομή του δικτύου κάθε οργανισμού, incident που προκύπτουν. Τα incident που θα προκύψουν θα ανήκουν στις κατηγορίες False Positive-Negative, True Positive-Negative. Τα alerts/offenses μπορούν να περιέχουν events ή flows δηλαδή μπορούν να εμπεριέχουν αρχεία καταγραφών ή/και πακέτα δικτυακού περιεχομένου. Στο πρώτο πεδίο μπορούμε να δούμε τα αποτελέσματα λειτουργιών των αναλυτών όπως:

- Σε ποιο όνομα έχει αναθέτει το offense
- Σημειώσεις με κείμενο
- Σημαιάκι ώστε να αναγνωρίζουμε ότι το offense είναι υψίστης σημασία
- Προστατευόμενα offenses ώστε οι αναλυτές να προσέχουν για την μη διαγράφη του συγκεκριμένου καθώς χρήζει περαιτέρω διερεύνηση.

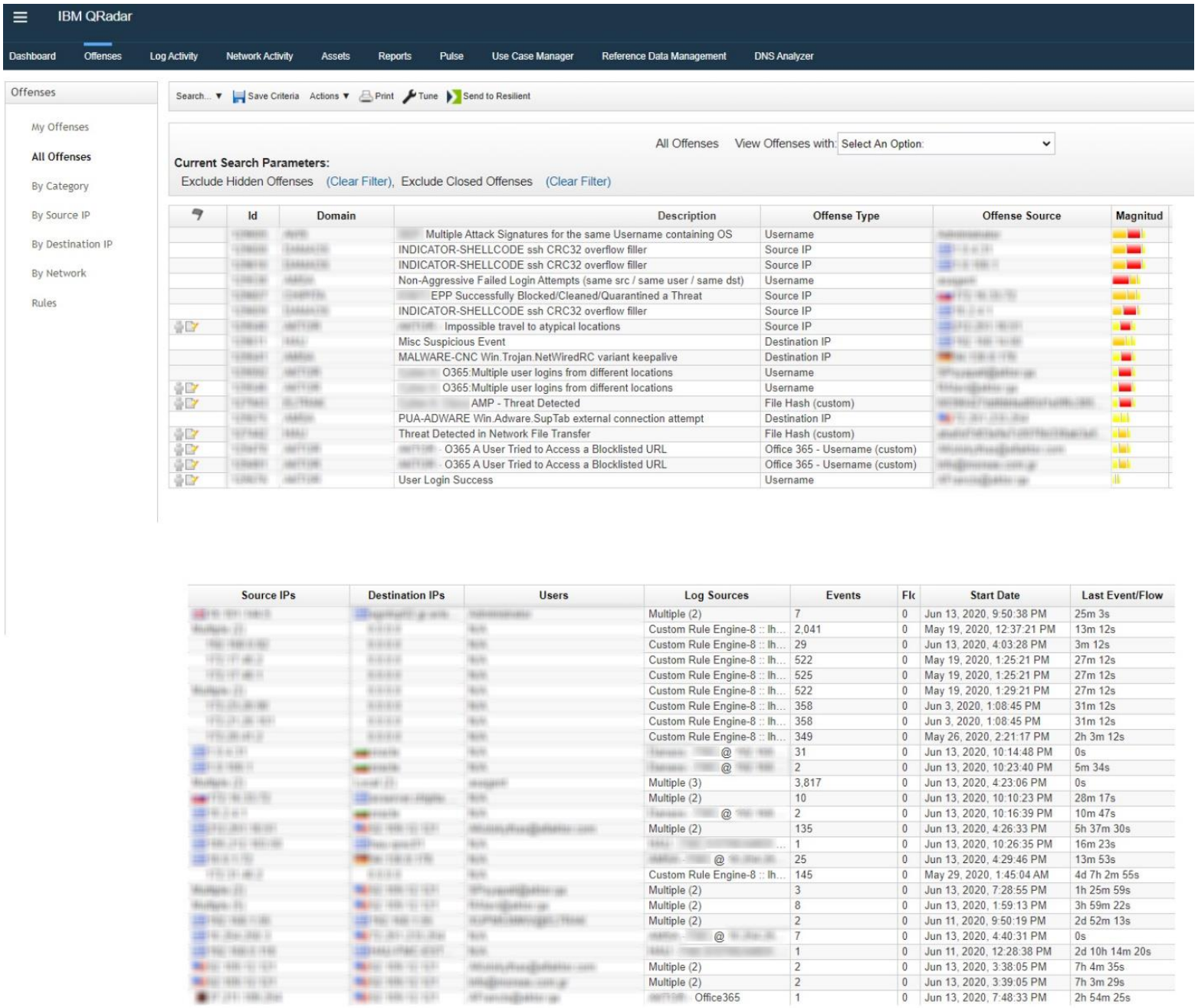
Όπως παρατηρεί κάποιος στην εικόνα των offenses υπάρχουν πεδία όπως το ID, το Domain, η περιγραφή και άλλα.

- Το πεδίο ID αποτελεί τον μοναδικό αριθμό των offenses.
- Το πεδίο Domain αφορά τον οργανισμό που παρακολουθεί το τμήμα SOC.
- Το πεδίο Description αφορά την περιγραφή του κάθε offense.
- Το πεδίο offense type αφορά την κατηγοριοποίηση του offense σύμφωνα με τον κανόνα που έχει δημιουργήσει η ομάδα του soc. Εάν η ομάδα έχει φτιάξει έναν κανόνα ο οποίος θα εμφανίζει το offense σύμφωνα με την source IP, τότε στο πεδίο offense Source θα εμφανίζεται η source IP. Στο πεδίο magnitude απεικονίζεται το severity(επικινδυνότητα) του κάθε offense.
- Στα πεδία source IP, Destination IP αναγράφονται οι IP από εξωτερικό δίκτυο προς εσωτερικό ή αλλιώς Remote to Local(R2L) ή από εσωτερική σύνδεση προς εξωτερική σύνδεση (Local το Remote). Επίσης υπάρχει και η περίπτωση εσωτερικής σύνδεσης προς εσωτερική σύνδεση (Local to Local). Ανάλογα πως έχουμε διαμορφώσει τους κανόνες για να παραχθεί το συγκεκριμένο offense. Στο πεδίο users φαίνεται ο χρήστης που έχει άμεση επαφή με το offense.
- Στο πεδίο log source παρατηρεί κανείς την πηγή προέλευσης των αρχείων καταγραφών παραδείγματος χάρη Log source = Microsoft Office 365.
- Στο πεδίο event και flows παρατηρούνται τα events και τα flows που είναι άμεσα σχετιζόμενα με το παραγόμενο offense.
- Στο πεδίο Start Date εμφανίζεται η ημερομηνία στην οποία παράχθηκε ένα offense
- Στο πεδίο Last Event/Flow εμφανίζεται η τελευταία χρονική στιγμή που εμφανίστηκε το τελευταίο event/flow

Υπάρχουν κάποια buttons όπως το print για την εκτύπωση του περιεχομένου ενός offense η την αποθήκευση του σε μορφη pdf. Επίσης υπάρχει και το button της αναζήτησης όπου στην συγκεκριμένη περίπτωση ο αναλυτής αναζητά ένα offense με συγκεκριμένα κριτήρια.

Αριστερά υπάρχουν κάποιες κατηγορίες όπως my offense κ.α. στις οποίες τα offense ομαδοποιούνται σύμφωνα με την κατηγορία που επιλέξει ο αναλυτής.Στην κατηγορία rule ο αναλυτής μαζί με τον technician προσαρμόζουν κανόνες για τα offenses ή και ακόμα αυτοματοποιούν διαδικασίες που αφορούν την ανάλυση από incident έτσι ώστε ο πελάτης να δέχεται email όταν παράγεται κάποιο incident.

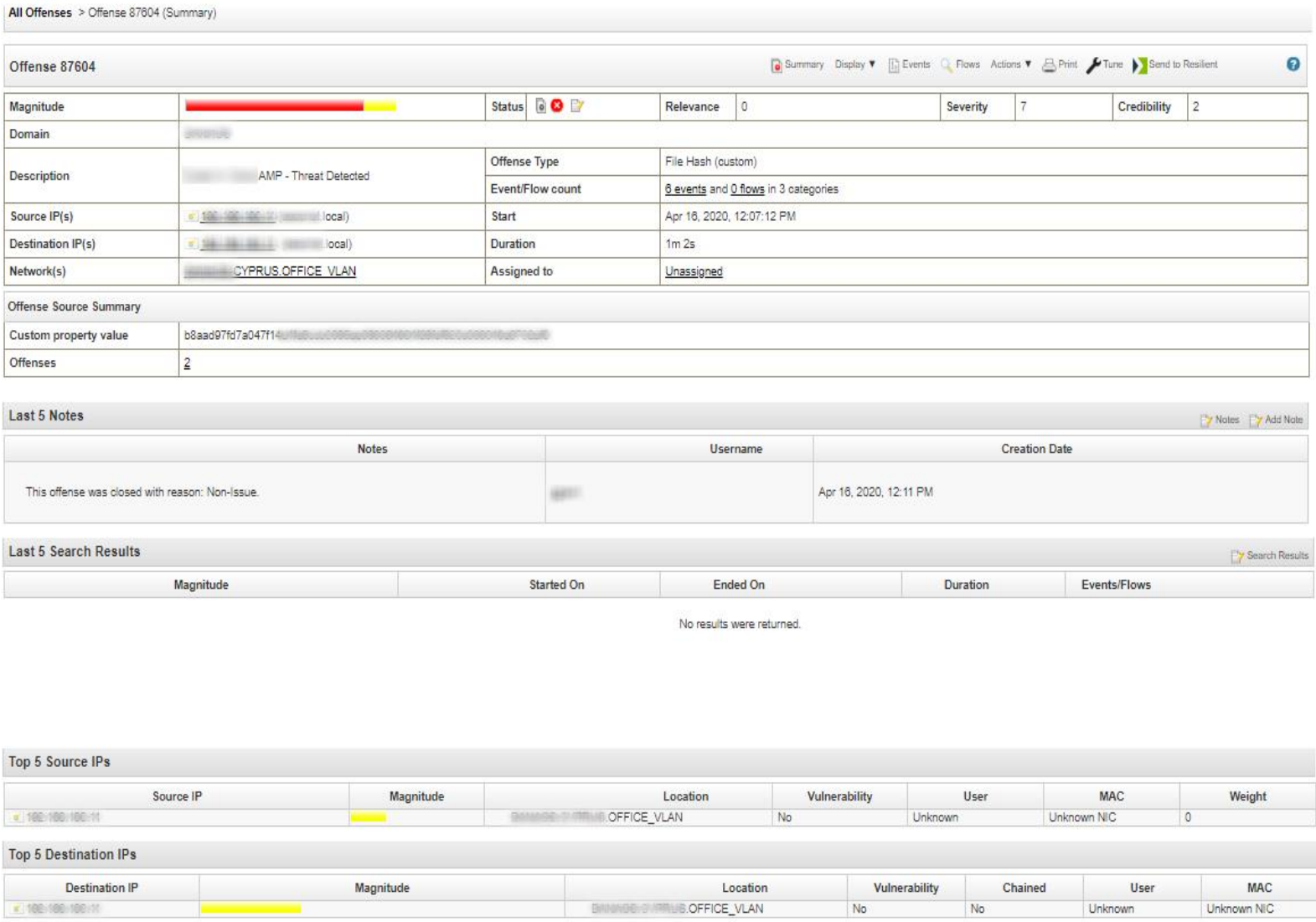
Αυτή είναι η γενική εικόνα των offenses που έχει ο αναλυτής όταν ξεκινήσει την βάρδια του



Source IPs	Destination IPs	Users	Log Sources	Events	Flc	Start Date	Last Event/Flow
			Multiple (2)	7	0	Jun 13, 2020, 9:50:38 PM	25m 3s
			Custom Rule Engine-8 :: lh...	2,041	0	May 19, 2020, 12:37:21 PM	13m 12s
			Custom Rule Engine-8 :: lh...	29	0	Jun 13, 2020, 4:03:28 PM	3m 12s
			Custom Rule Engine-8 :: lh...	522	0	May 19, 2020, 1:25:21 PM	27m 12s
			Custom Rule Engine-8 :: lh...	525	0	May 19, 2020, 1:25:21 PM	27m 12s
			Custom Rule Engine-8 :: lh...	522	0	May 19, 2020, 1:29:21 PM	27m 12s
			Custom Rule Engine-8 :: lh...	358	0	Jun 3, 2020, 1:08:45 PM	31m 12s
			Custom Rule Engine-8 :: lh...	358	0	Jun 3, 2020, 1:08:45 PM	31m 12s
			Custom Rule Engine-8 :: lh...	349	0	May 26, 2020, 2:21:17 PM	2h 3m 12s
				31	0	Jun 13, 2020, 10:14:48 PM	0s
				2	0	Jun 13, 2020, 10:23:40 PM	5m 34s
			Multiple (3)	3,817	0	Jun 13, 2020, 4:23:06 PM	0s
			Multiple (2)	10	0	Jun 13, 2020, 10:10:23 PM	28m 17s
				2	0	Jun 13, 2020, 10:16:39 PM	10m 47s
			Multiple (2)	135	0	Jun 13, 2020, 4:26:33 PM	5h 37m 30s
				1	0	Jun 13, 2020, 10:26:35 PM	16m 23s
				25	0	Jun 13, 2020, 4:29:46 PM	13m 53s
			Custom Rule Engine-8 :: lh...	145	0	May 29, 2020, 1:45:04 AM	4d 7h 2m 55s
			Multiple (2)	3	0	Jun 13, 2020, 7:28:55 PM	1h 25m 59s
			Multiple (2)	8	0	Jun 13, 2020, 1:59:13 PM	3h 59m 22s
			Multiple (2)	2	0	Jun 11, 2020, 9:50:19 PM	2d 52m 13s
				7	0	Jun 13, 2020, 4:40:31 PM	0s
				1	0	Jun 11, 2020, 12:28:38 PM	2d 10h 14m 20s
			Multiple (2)	2	0	Jun 13, 2020, 3:38:05 PM	7h 4m 35s
			Multiple (2)	2	0	Jun 13, 2020, 3:39:05 PM	7h 3m 29s
			Office365	1	0	Jun 13, 2020, 7:48:33 PM	2h 54m 25s

Offense

Ο αναλυτής καθώς διεξάγει την παρακολούθηση των offense, θα παρατηρήσει κάποιο offense το οποίο θα του κεντράρει το ενδιαφέρον. Ένα offense όπου θα παρατηρήσει είναι το threat detected. Στην εικόνα threat detected1 ο αναλυτής έχει ανοίξει το παράθυρο με το συγκεκριμένο offense ώστε να προχωρήσει στην διεξαγωγή της ανάλυσης (investigation). Τα πεδία είναι ξεκάθαρα, καθώς αναλύθηκαν για την εικόνα offense



Threat Detected 1

Το μέλος της ομάδας του SOC καθώς ανοίξει το event που αφορά το offense αυτό θα βρεί πολύτιμα στοιχεία για την διεξαγωγή της έρευνας του. Από την εικόνα threat detected 2 αναλύονται χαρακτηριστικά που συσχετίζονται με το offense. Μια λίστα ενδεικτική είναι:

- Event Name
- Username
- SHA-256
- File name
- File path
- Threat Name
- File Directory
- Computer Name

Στο πεδίο payload υπάρχει όλη η πληροφορία από τα δεδομένα που στέλνει το συγκεκριμένο log source. Από τις πληροφορίες αυτές μπορούμε να κάνουμε extract και να εξάγουμε custom properties όπως παραπάνω(username κ.α)

Η εξαγωγή συνήθως γίνεται από τον αναλυτή και προϋποθέτει γνώσεις regex και Jason εκ των πλείστων.

Event Information

Event Name	Threat Detected						
Low Level Category	Malicious Software						
Event Description	A threat was found on this system.						
Magnitude	(7)	**Relevance**	8	**Severity**	6	**Credibility**	5
Username	N/A						
Start Time	Apr 16, 2020, 12:08:12 PM	**Storage Time**	Apr 16, 2020, 12:07:12 PM	**Log Source Time**	Apr 16, 2020, 12:10:07 PM		
Archived File Disposition (custom)	N/A						
Archived File SHA256 Hash (custom)	N/A						
Computer Name (custom)	dc [redacted].local						
Disposition (custom)	Allowed						
EventID (custom)	1090519054						
FMC - Application Name (custom)	null						
FMC - Blocked Value (custom)	null						
FMC - Client App Name (custom)	null						
FMC - Disposition Value (custom)	null						
FMC - Impact Value (custom)	null						
FMC - Network Protocol Name (custom)	null						
FMC - Retrospective Disposition (custom)	null						
FMC Action (custom)	null						
File Directory (custom)	\\\?\C:\Windows\\Sys[redacted]W64\\						
File Extension (custom)	exe						
File Hash (custom)	b8aad97fd7a047f14e[redacted]						
File Path (custom)	\\\?\C:\Windows\\Sys[redacted]W64\\RemComSvc.exe						
Filename (custom)	RemComSvc.exe						
Geographic Location (custom)	{}						
MD5 Hash (custom)	3384be4f48f[redacted]						
Office 365 - Action Value (custom)	null						
Parent Disposition (custom)	N/A						
Parent Filename (custom)	N/A						
Parent Hash (custom)	N/A						
Parent MD5 (custom)	N/A						
Parent Process ID (custom)	N/A						
Parent SHA1 Hash (custom)	N/A						
Parent SHA256 Hash (custom)	N/A						
Reference Link (custom)	https://api.amp.[redacted].com/v1/computers/e3bca77d-8664-[redacted]0c6dd/trajectory						
SHA1 Hash (custom)	367d57d239d27c5320ae5229543[redacted]						
SHA256 Hash (custom)	b8aad97fd7a047f14e[redacted]						
Threat Name (custom)	PUA.Win.File.Remcom::in03.talos						
UploadRatio (custom)	N/A						
dns_event_flag (custom)	0						
test_username (custom)	null						

Source and Destination Information

Source IP	[redacted]	**Destination IP**	[redacted]
Source Asset Name	[redacted].local	**Destination Asset Name**	[redacted].local
Source Port	0	**Destination Port**	0
Pre NAT Source IP		**Pre NAT Destination IP**	
Pre NAT Source Port	0	**Pre NAT Destination Port**	0
Post NAT Source IP		**Post NAT Destination IP**	
Post NAT Source Port	0	**Post NAT Destination Port**	0
Source IPv6	0:0:0:0:0:0:0:0	**Destination IPv6**	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	**Destination MAC**	00:00:00:00:00:00

Payload Information

utf | hex | base64

Wrap Text


```
{"id":6816238408717828106,"timestamp":1587028207,"timestamp_nanoseconds":102039932,"date":"2020-04-16T09:10:07+00:00","event_type":"Threat
Detected","event_type_id":1090519054,"detection":"PUA.Win.File.Remcom::in03.talos","detection_id":"6816238[redacted]",
"connector_guid":"e3bca77d-8664-[redacted]","group_guids":["620fcdee-425b-[redacted]
[redacted]"],"severity":"Medium","computer":{"connector_guid":"e3bca77d-8664-[redacted]",
"hostname":"dc.[redacted].local","external_ip":"[redacted]","user":"","active":true,"network_addresses":
[{"ip":"[redacted]","mac":"[redacted]"}],"links":{"computer":"https://api.amp.[redacted].com/v1/computers/e3bca77d-8664-[redacted]",
"trajectory":"https://api.amp.cisco.com/v1/computers/e3bca77d-8664-[redacted]
[redacted]/trajectory","group":"https://api.amp.[redacted].com/v1/groups/620fcdee-425b-[redacted]"},
"file":{"disposition":"Allowed","file name":"RemComSvc.exe","file_path":"\\\\?\\C:\\Windows\\Sys[redacted]64\\RemComSvc.exe","identity":
{"sha256":"b8aad97fd7a047f1[redacted]",
"sha1":"367d57d239d27c5320ae52295[redacted]","md5":"3384be[redacted]"}}}
```


Additional Information

Protocol	255	**QID**	111250007
Log Source	[redacted] - AMP4E @ Cloud	**Event Count**	1

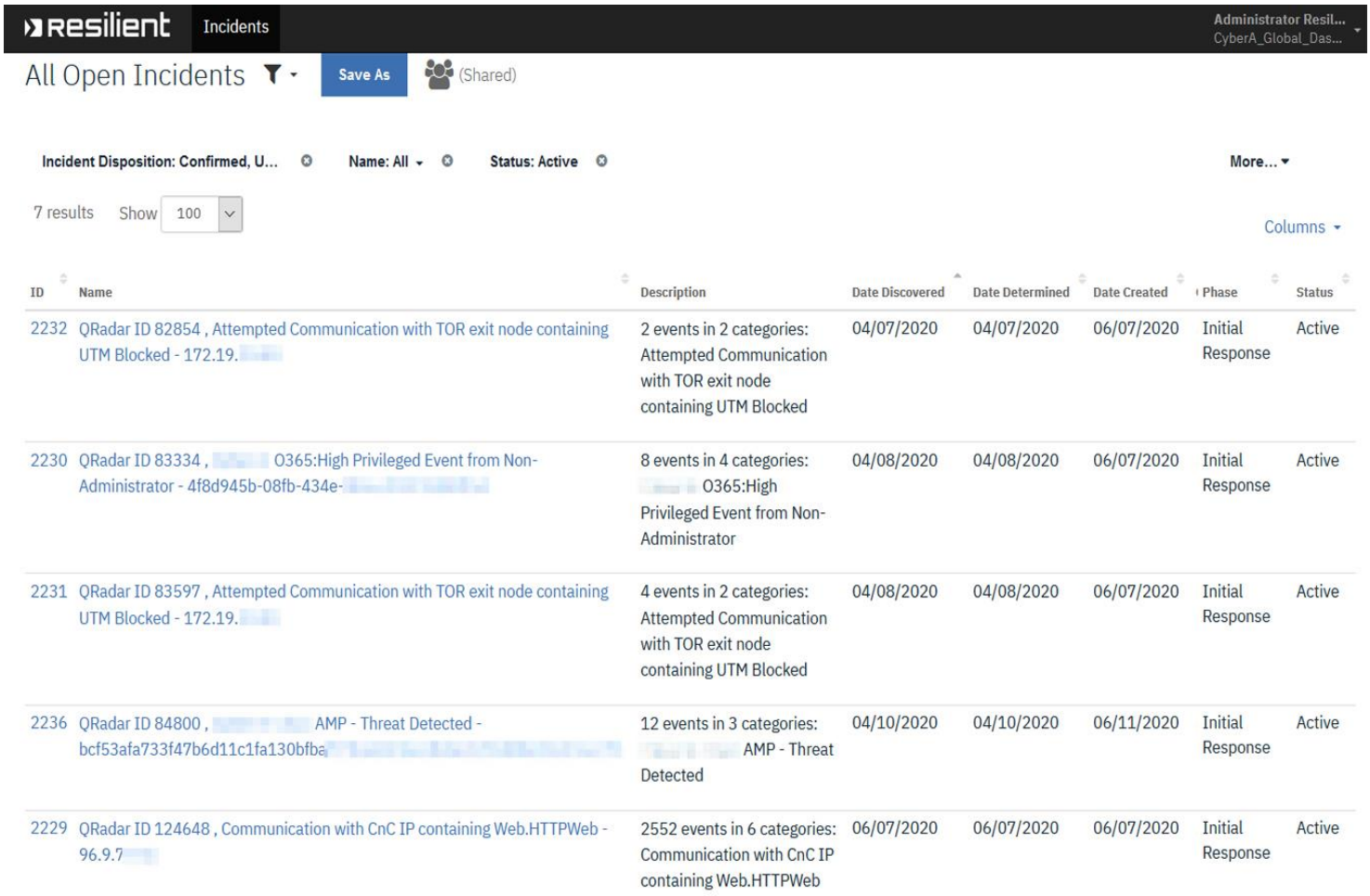
Threat Detected 2

Μετά από αναλύσεις που πραγματοποίησε ο αναλυτής, το event αυτό πιθανότατα να είναι adware. Για επιβεβαίωση ανοίγει ticket στον πελάτη με σκοπό την αναφορά του και την περεταίρω διερεύνηση στο τερματικό. Σε περίπτωση που διαχειρίζεται η εταιρία του αναλυτή τις δικτυακές του υποδομές μπορούν να πραγματοποιήσουν οι ίδιοι τον αποκλεισμό της κίνησης αυτή ρωτώντας πελάτη, αλλιώς ο οργανισμός του πελάτη είναι υπεύθυνος για τον αποκλεισμό.

IBM Resilient

Αξίζει να αναφερθεί ότι υπάρχουν incident tracking εργαλεία, τα οποία περιέχουν playbooks. Τα εργαλεία αυτά δίνουν μια κατά μια έννοια, μια ανάλυση και ένα reporting σε χρόνο σύντομο. Οι αναλυτές έχουν την δυνατότητα να τρέξουν αυτοματοποιημένες διεργασίες όπως να αναζητήσουν εάν ένα αρχείο είναι κακόβουλο πατώντας ένα κουμπί. Σε την περίπτωση αυτή θα χρησιμοποιηθεί το IBM Resilient. Σε πρώτο στάδιο για την ορθή λειτουργία του IBM Resilient θα πρέπει να πραγματοποιηθούν κάποια βήματα. Το πρώτο βήμα αφορά την εγκατάσταση του Resilient και την άμεσα σύνδεση του με το εργαλείο SIEM, σε αυτήν εδώ την περίπτωση το IBM QRadar. Σε δεύτερο στάδιο ο μηχανικός θα ρυθμίσει και θα εγκαταστήσει τις απαραίτητες λειτουργείες στο Resilient έτσι ώστε να δέχεται τα σωστά feed και να είναι πλήρως συγχρονισμένο με το QRadar. Όταν όλα τελειοποιηθούν και το IBM Resilient είναι πλήρως λειτουργικό τότε ο αναλυτής μπορεί να κάνει escalate(στείλει) το πρώτο offense στο QRadar.

Στην εικόνα dashboard ο αναλυτής έχει ορατότητα των offenses που έχει κάνει escalate στο Resilient. Ο αναλυτής μπορεί να προσαρμόσει τις στήλες σύμφωνα με την ευκολία του ώστε να μπορεί άμεσα να αντλήσει τις πληροφορίες που χρειάζεται. Στην στήλη name αναγράφονται τα offense από το QRadar. Με μια πρώτη ματιά τα offense τα οποία θα σημειώσει ο αναλυτής ως σημαντικά είναι το attempted communication with Tor exit node, το AMP – Threat Detected και το Communication with CnC IP. Στην δεύτερη στήλη υπάρχει η περιγραφή του event, ιincident. Στην Τρίτη, τέταρτη και Πέμπτη μέρα αναγράφεται η ημερομηνία που ανακαλύφθηκε, προσδιορίσθηκε και δημιουργήθηκε το συγκεκριμένο incident ή event στο Resilient. Το Phase δηλώνει σε ποια φάση βρίσκεται το συγκεκριμένο incident, θα εξηγηθεί παρακάτω και τέλος το status δηλώνει εάν είναι σε ενεργή κατάσταση.



ID	Name	Description	Date Discovered	Date Determined	Date Created	Phase	Status
2232	QRadar ID 82854 , Attempted Communication with TOR exit node containing UTM Blocked - 172.19.	2 events in 2 categories: Attempted Communication with TOR exit node containing UTM Blocked	04/07/2020	04/07/2020	06/07/2020	Initial Response	Active
2230	QRadar ID 83334 , O365:High Privileged Event from Non-Administrator - 4f8d945b-08fb-434e-	8 events in 4 categories: O365:High Privileged Event from Non-Administrator	04/08/2020	04/08/2020	06/07/2020	Initial Response	Active
2231	QRadar ID 83597 , Attempted Communication with TOR exit node containing UTM Blocked - 172.19.	4 events in 2 categories: Attempted Communication with TOR exit node containing UTM Blocked	04/08/2020	04/08/2020	06/07/2020	Initial Response	Active
2236	QRadar ID 84800 , AMP - Threat Detected - bcf53afa733f47b6d11c1fa130bfba	12 events in 3 categories: AMP - Threat Detected	04/10/2020	04/10/2020	06/11/2020	Initial Response	Active
2229	QRadar ID 124648 , Communication with CnC IP containing Web.HTTPWeb - 96.9.7	2552 events in 6 categories: Communication with CnC IP containing Web.HTTPWeb	06/07/2020	06/07/2020	06/07/2020	Initial Response	Active

Dashboard

Στο πεδίο tasks ο αναλυτής έχει πλήρη εικόνα των λειτουργιών και ενεργειών που πρέπει να εκτελέσει. Στην εικόνα tasks αναλύεται ένα μέρος ενός playbook.

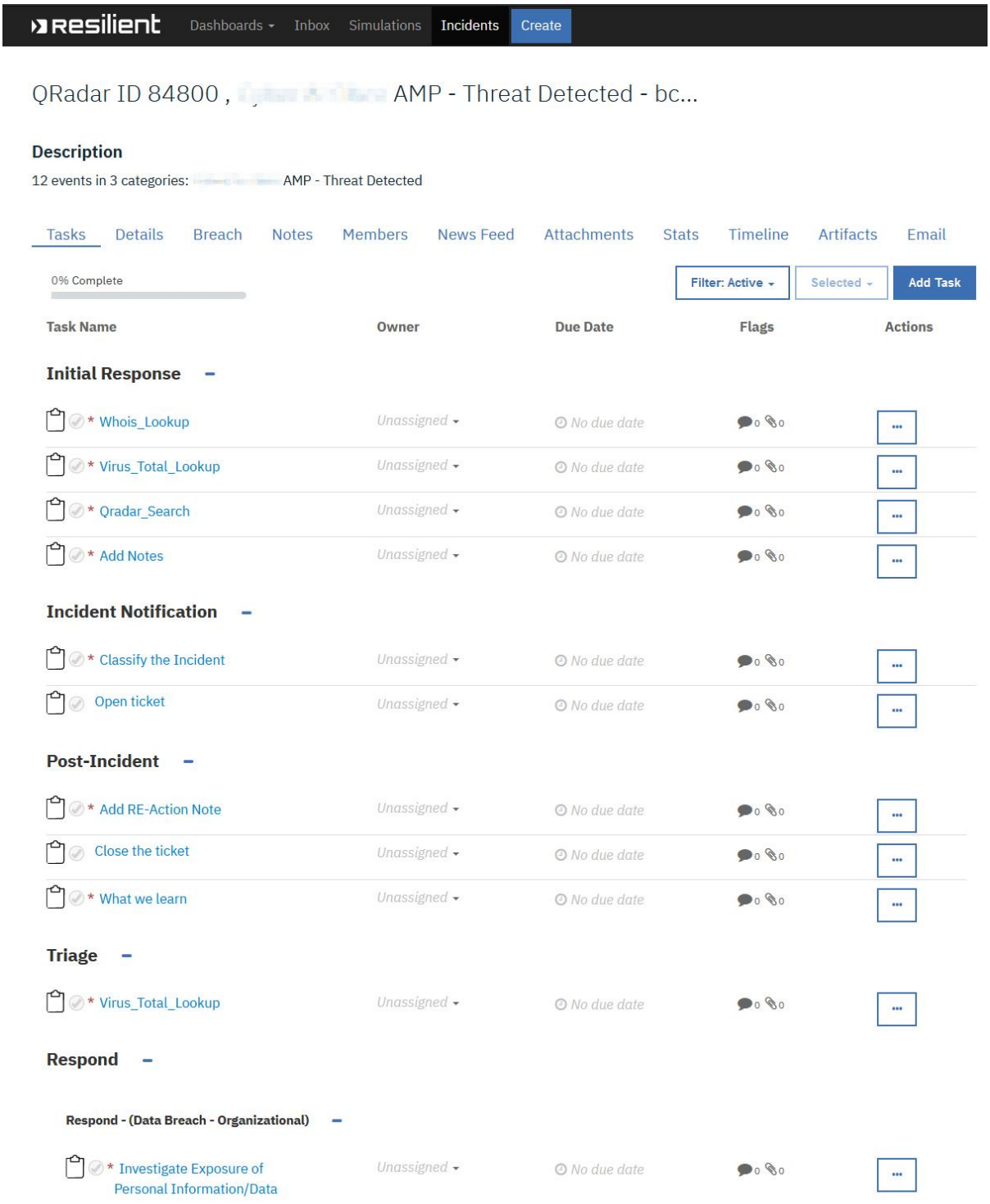
Ένα playbook μπορεί να εμπεριέχει Rules, Workflow, Fields, Artifacts, Data Tables, Blocks, Scripts, Widgets, Dashboard, Messages, Notification, Wiki Pages, Incident Tabs, Groups, Messages Destinations, Phases, Tasks, Incident Types, Workspaces, Roles, Functions. Στην ουσία είναι κανόνες που διέπουν την σωστή λειτουργία ενός incident έτσι ώστε ο αναλυτής να παρέχει την πλήρη πληροφόρηση του.

Τα tasks εδώ χωρίζονται σε τρεις φάσεις. Στην πρώτη φάση initial response, ο αναλυτής είναι υπεύθυνος έτσι ώστε η ανταπόκριση του αναλυτή στο incident να είναι άμεση. Ο αναλυτής χωρίς την χρήση του Resilient πρέπει να πραγματοποιήσει βασικές λειτουργίες όπως να ερευνήσει τα αρχεία καταγραφών του εργαλείου SIEM που διαθέτει, να αναζητήσει εάν η IP που εμπεριέχεται στο συγκεκριμένο event είναι κακόβουλη. Οι διαδικασίες αυτές μπορούν να αυτοματοποιηθούν στο εργαλείο του Resilient. Παραδείγματος χάριν έχει την δυνατότητα να πατήσει ένα κουμπί και να εκτελέσει την

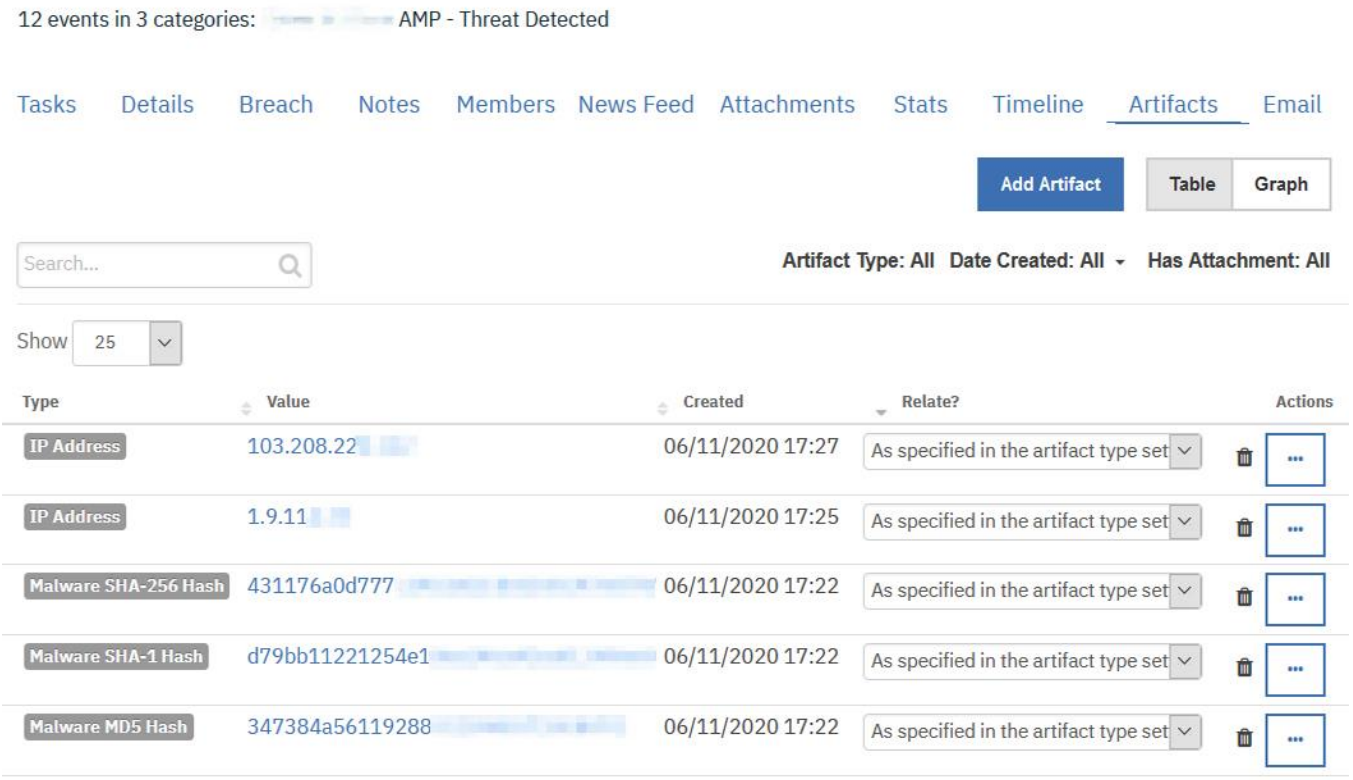
αναζήτηση της IP στο virus total ώστε να ενημερωθεί εάν είναι κακόβουλη ή όχι. Επίσης μια άλλη λειτουργεία είναι ο αυτοματοποιημένος έλεγχος μιας IP στο TOR δίκτυο.

Σε δεύτερη φάση είναι το incident notification όπου εκεί υπάρχει classify the incident και open ticket όπου ο αναλυτής θα προσδιορίσει το incident, Πχ εάν είναι false positive ή malicious και θα ανοίξει ένα ticket εσωτερικά ή στον πελάτη για να τον ενημερώσει ή για ενέργειες.

Στην επόμενη φάση υπάρχει το post incident όπου ο αναλυτής μπορεί να προσθέσει σημειώσεις, να κλείσει ένα ticket και να προσθέσει σε σημειώσεις τι μαθήματα πήραν ή τι πληροφορίες διοχέτευσαν για το συγκεκριμένο incident.


Resilient
Dashboards
Inbox
Simulations
Incidents
Create
QRadar ID 84800 , AMP - Threat Detected - bc...
Description
12 events in 3 categories: AMP - Threat Detected
Tasks
Details
Breach
Notes
Members
News Feed
Attachments
Stats
Timeline
Artifacts
Email
0% Complete
Filter: Active
Selected
Add Task
Task Name
Owner
Due Date
Flags
Actions
Initial Response
* Whois_Lookup
* Virus_Total_Lookup
* Qradar_Search
* Add Notes
Incident Notification
* Classify the Incident
Open ticket
Post-Incident
* Add RE-Action Note
Close the ticket
* What we learn
Triage
* Virus_Total_Lookup
Respond
Respond - (Data Breach - Organizational)
* Investigate Exposure of Personal Information/Data
Unassigned
No due date

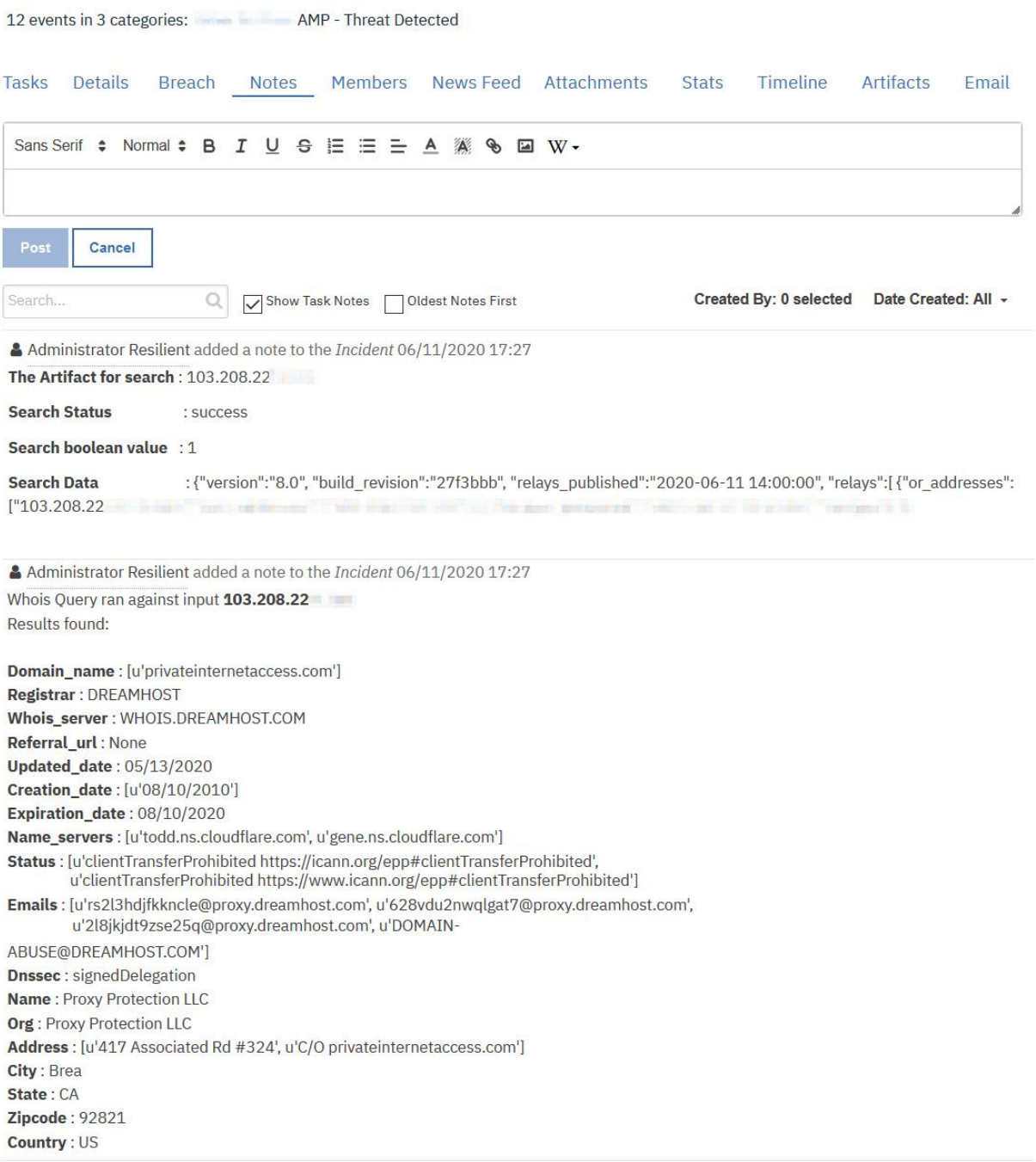
Tasks



Artifacts

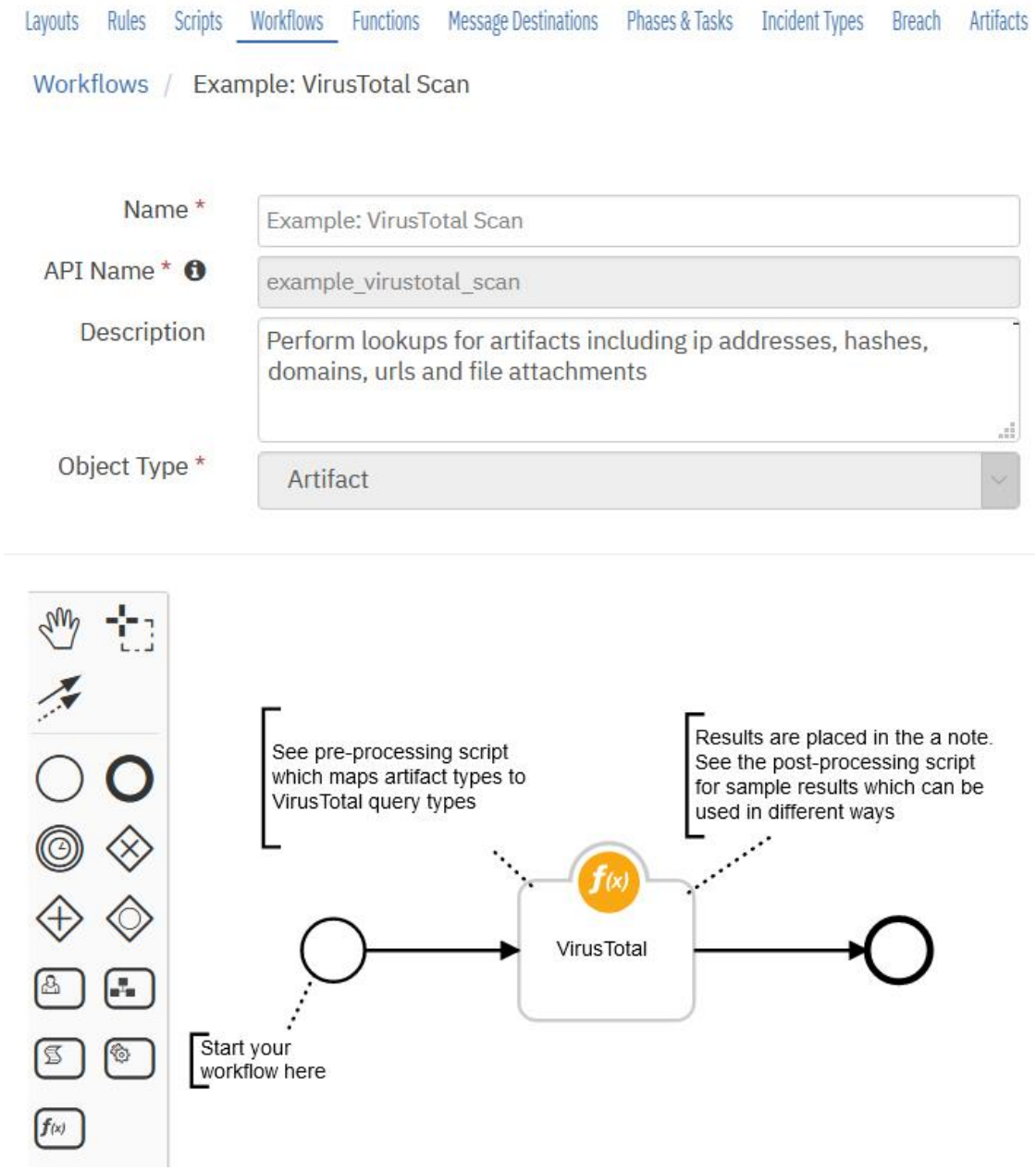
Στο παραπάνω παράθυρο φαίνονται τα στοιχεία ενος incident όπως IP, ονόματα υπολογιστών, hash, file name. Τα στοιχεία αυτά βρίσκονται μέσα στο event. Στην περίπτωση μη ύπαρξης των στοιχείων αυτών, ευθύνεται ή πραγματοποίηση κάποιο misconfiguration. Τότε ο αναλυτής έχει την δυνατότητα της χειροκίνητης προσθήκες των στοιχείων αυτών (artifacts). Στην συνέχεια μπορεί να εκτελέσει κάποιες ενέργειες μέσω του AMP. Το AMP μεταφράζεται ως Advance Malware Protection και ο σκοπός του είναι η προστασία του χρήστη από κακόβουλα λογισμικά ή εφαρμογές. Ο οργανισμός που περιέχει το AMP, προστατεύεται από όλες τις μορφές κακόβουλου περιεχομένου . Επίσης για να λειτουργήσει πλήρως η πλατφόρμα του AMP, πρέπει να εγκαταστήσει στα τερματικά του, το AMP for endpoints. Σε επόμενη φάση τα αρχεία καταγραφούν θα σταλθούν στο IBM Reseilient ή QRadar. Ο αναλυτής όταν αναλύει στο incident response system τα στοιχεία από το AMP μπορεί να πραγματοποιήσει ενέργειες όπως την εκτέλεση εντολής για την αναζήτηση εάν το hash ή ip είναι είναι κακόβουλα στην βάση δεδομένων του AMP. Ο αναλυτής έχει την ορατότητα της δικτυακής και συστηματικής κίνησης ενός αρχείου, δηλαδή σε ποιο τερματικό εγκαταστάθηκε το συγκεκριμένο αρχείο, από ποιον χρήστη, ποιες διεργασίες του αρχείου εκτελέστηκαν και άλλα.

Παρακάτω ο αναλυτής εκτελεί δυο ενέργειες. Η πρώτη αφορά την αναζήτηση μιας κακόβουλης Ip στο virus total και η δεύτερη αφορά μια who is λειτουργία.



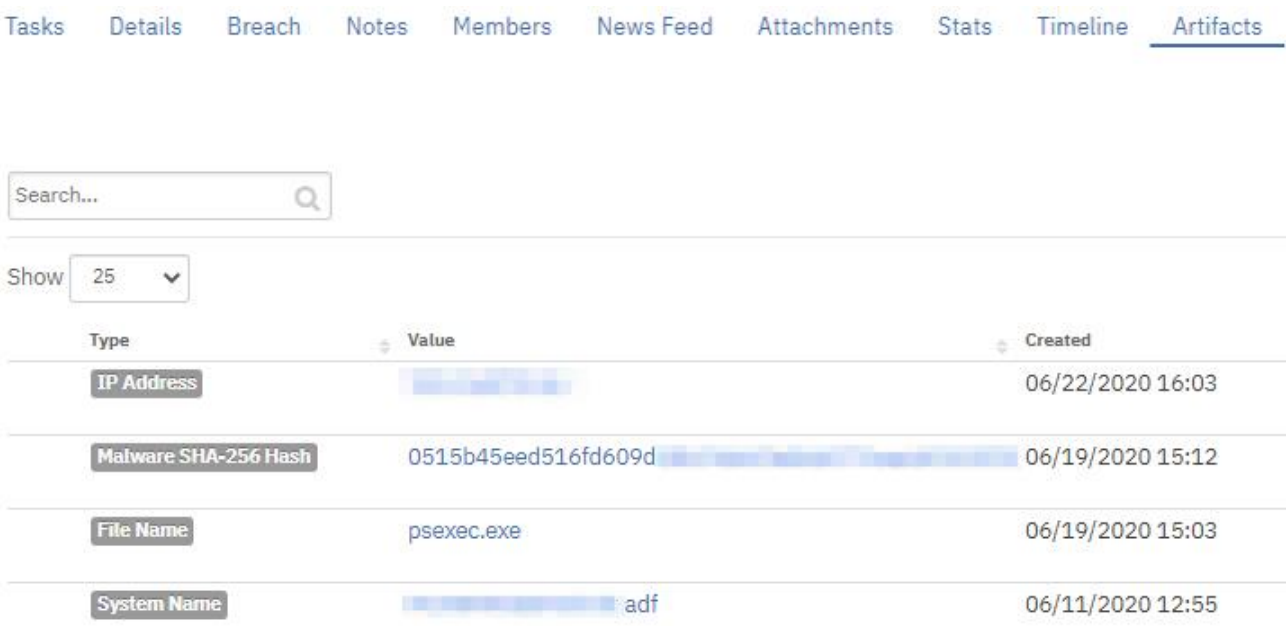
Notes

Ένα χαρακτηριστικό η στοιχείο ενός playbook είναι το workflow. Το workflow είναι μια γραφικά σχεδιασμένο από activities οι οποίες σου επιτρέπουν να δημιουργήσεις ένα σετ από οδηγίες. Παραδείγματος χάρη παρακάτω φαίνεται πως λειτουργεί το workflow του virus total



Workflow

Παρακάτω αναλύονται οι λειτουργίες του amp σύμφωνα με τις πληροφορίες της εικόνας Artifacts2. Ο αναλυτής εκτελεί τις απαιτούμενες ενέργειες, έτσι ώστε το AMP να τροφοδοτήσει το Resilient με τις κατάλληλες πληροφορίες.



Artifacts2

Στην εικόνα AMP παρατηρείται πληροφορίες για ένα σύστημα (System name/ Hostname). Στο πεδίο AMP computers αναλύονται τα στοιχεία ενός υπολογιστικού συστήματος όπως το λειτουργικό του σύστημα, οι εξωτερικές και εσωτερικές IP όπου έχουν χρησιμοποιηθεί.

Στο πεδίο AMP activity ο αναλυτής παρατηρεί το χρόνο που εκτέλεσε ο υπολογιστής το query. Στον πίνακα Simple Custom Detection file lists παρατηρείται εάν το όνομα αρχείου είναι σε blacklist.

AMP computers

Hostname	Operating system	Connector guid	Connector version	Group name	Group guid	External ip	Internal ips	Install date	Last seen
PC a df	Windows 7 Professional	eedf8fb2-2087-4aa3-8ff5-	7.2.7.11687	Protection -Group	c7034a08-db49-4e77-88f4-			2017-09-13T12:38:09Z	2020-06-18T11:45:09Z

AMP activity

Query execution time	Query string	Active	Hostname	Connector guid
2020-06-19 15:02:11	psexec.exe	Yes	PC adf	24a6b49e-c987-4893-b67f-

AMP Simple Custom Detections file lists

Query execution time	List name	List guid	List type
2020-06-19 15:03:43	File Blacklist	1cc259cb-af06-4ed8-8a70-	simple_custom_detections

AMP

Στο πεδίο AMP groups ο αναλυτής μπορεί να δει σε ποια ομάδα δικτύου ανήκει ο συγκεκριμένος υπολογιστής.

AMP groups

Search... Print Export

Query execution time	Name	Description	Group guid	
2020-06-19 15:03:38	Audit	Audit Group for SA	98adb2e9-576a-46d4-b571-08305	...
2020-06-19 15:03:38	Domain Controller	Domain Controller Group for SA	fb7b071b-4d96-4dc7-ac8d-2e7	...
2020-06-19 15:03:38	Audit-Group	—	9df8f840-4529-42e9-b650-62	...
2020-06-19 15:03:38	Protect-Group	group	5c718082-e393-4337-aa4c-411	...
2020-06-19 15:03:38	Domain-Controller-Group	—	ec3758b3-ff38-4d96-b5e7-f04	...
2020-06-19 15:03:38	Protection-Group	—	c7034a08-db49-4e77-88f4-6f7f7	...
2020-06-19 15:03:38	-Server-Group	—	08e36a14-1cc7-4860-a963-6a	...
2020-06-19 15:03:38	NeedToBeUpgraded	—	b983b0b9-fdd8-4bee-82f4-6a4	...
2020-06-19 15:03:38	Protect	Protect Group for SA	9615f948-603c-4c44-9efb-2a	...
2020-06-19 15:03:38	Server	Server Group for SA	f50bf280-ef2b-4cc4-8a01-bd22	...

AMP groups

Στο πεδίο AMP event types κατατάσσονται σε χρονική διάρκεια τα events. Στο πεδίο name αναγράφονται οι ενέργειες που πραγματοποιήθηκαν από τον συγκεκριμένο υπολογιστικό μηχάνημα και ανιχνεύθηκαν από το AMP. Το policy update αφορά κάποια ενημέρωση πολιτικής, παραδείγματος χάρη σε ποιο domain group θα ανήκει ένας χρήστης. Συνήθως η αλλαγή αυτή πραγματοποιείται από το IT τμήμα. Μια ενέργεια ή οποία μπορεί να είναι αυτόματη ή χειροκίνητη. Η ενέργεια threat detected είναι αυτόματη, καθώς το AMP εντόπισε μια απειλή η οποία μπορεί να αποτελείται από ένα κακόβουλο λογισμικό ή από ένα adware. Ο αναλυτής παρατηρεί ότι ο χρόνος του threat detected και του threat Quarantine failure είναι ο ίδιος. Για αυτόν τον λόγο πρέπει να περιηγηθεί στο εργαλείο QRadar ή στο ίδιο AMP ώστε να δει το file trajectory του συγκεκριμένου υπολογιστικού συστήματος.

AMP event types

Search... Print Export

Query execution time	Event type name	Event type description	Event type id	
2020-06-19 15:03:35	Policy Update	An agent has been told to fetch policy.	553648130	...
2020-06-19 15:03:35	Policy Update Failure	A policy update failed, and the policy was not successfully applied.	2164260866	...
2020-06-19 15:03:35	Scan Started	An agent has started scanning.	554696714	...
2020-06-19 15:03:35	Scan Completed, No Detections	A scan has completed without detecting anything malicious.	554696715	...
2020-06-19 15:03:35	Scan Completed With Detections	A scan has completed and detected malicious items.	1091567628	...
2020-06-19 15:03:35	Scan Failed	A scan has been attempted, and failed to run.	2165309453	...
2020-06-19 15:03:35	Threat Detected	A threat was found on this system.	1090519054	...
2020-06-19 15:03:35	Threat Quarantined	A threat was successfully quarantined.	553648143	...
2020-06-19 15:03:35	Quarantine Failure	A detected threat was not successfully quarantined.	2164260880	...
2020-06-19 15:03:35	Quarantine Restore Requested	A request has been made to move a file from Quarantine back to its original location.	570425394	...

Amp event types

Threat Hunting

Μια θεμελιώδης λύση για την αύξηση της άμυνας στον κυβερνοχώρο απέναντι σε adversaries είναι το threat hunt. Ο ορισμός ορίζεται ως εξής: Είναι μια διαδικασία προληπτική, καθοδηγούμενη από τους αναλυτές για την αναζήτηση τακτικών, τεχνικών και διαδικασιών ενός adversary σε ένα περιβάλλον. Ο ορισμός αυτός είναι ο πιο κοντινός που υπάρχει, καθώς δεν υπάρχει επίσημος ακαδημαϊκός ορισμός. Στα αγγλικά υπάρχει συντομογραφία, το TTP(tactics, techniques and procedures. Το TTP πρέπει να ερευνηθεί και να γίνει κατανοητό ως προς τον τρόπο συλλογής δεδομένων. Οι πληροφορίες σχετικά με το TTP του adversary προέρχονται συνήθως από υπογραφές, δείκτες(indicators) και συμπεριφορές, οι οποίες παρατηρούνται από threat intelligences πήγες. Το threat hunting χρειάζεται συγκεκριμένες αναλυτικές δεξιότητες, όπως η εξοικείωση με τις threat hunting τεχνικές και την ικανότητα να δημιουργεί και να διερευνά ο αναλυτής υποθετικά σενάρια σχετικά με τον adversary.

Οι threat hunters δεν περιμένουν την κατάλληλη στιγμή για να ανταποκριθούν σε alerts ή indicators of compromise (IoCs). Συνεχώς αναζητούν για απειλές έτσι ώστε να

προτρέψουν ή να μειώσουν την ζημία από έναν επιτιθέμενο. Στο threat hunting δεν είναι απαραίτητο να βρεθούν αποτελέσματα από threats έτσι ώστε να θεωρηθεί η διαδικασία threat hunting επιτυχής. Οι απειλές (threats), συχνά αναγνωρίζονται ως advance persistent threats (APTs), όχι για τις δυνατότητες των adversaries άλλα για την ικανότητά να διατηρούν λειτουργίες ενεργές και επίμονες εναντίων των στόχων τους.

Μια έρευνα του 2018 του SANS παρουσιάζει την ακριβέστατη χρήστη του threat hunting σε οργανισμούς. Η χρήστη αυτή είχε αυξηθεί από το 2017, στην οποία έρευνα πολλοί οργανισμοί χρησιμοποιούσαν την παραδοσιακή μέθοδο του intrusion detection. Στην έρευνά του 2018 πολλοί οργανισμοί χρησιμοποιούσαν το κατάλληλο threat intelligence, έτσι ώστε να αναγνωρίσουν τις πιο αποτελεσματικά σημεία μέσα σε ένα δίκτυο ενός οργανισμού για ανώμαλες συμπεριφορές οι οποίες είναι δείκτες (indicator) απειλών.

Το threat hunting γενικά βοηθάει πολύ τον οργανισμό με πολλούς τρόπους. Πρώτα από όλα το threat hunting μεγιστοποιεί την ασφάλεια μέσω της ανάλυσης, του reporting και της βελτιστοποιημένης ειδοποίησης του alerting system. Το threat hunting έχει την δυνατότητα να εντοπίσει αποκλίσεις ανάμεσα σε normal system operation και error conditions. Όπως έχει προαναφερθεί ο αναλυτής του SOC εποπτεύει και παρακολουθεί συνεχώς την υποδομή και τα συστήματα ενός ή περισσότερων οργανισμών, ως προς την ασφάλεια. Με το threat hunting οι adversaries μπορούν να ανιχνευτούν σε χρόνο μικρότερης διάρκειας από ότι πριν. Με αυτόν τον τρόπο θα μειωθεί ο χρόνος παραμονής του adversary και ο έλεγχος των ζημιών που προκάλεσε ο ίδιος θα είναι πιο αποτελεσματικός. Η δημιουργία μιας ομάδας threat hunting είναι ένας τέλειος τρόπος έτσι ώστε να παρέχεται εναλλαγή στην ζωή των αναλυτών του SOC και για να μην περάσουν την υπόλοιπη ζωή τους επιβλέποντας alerts.

Παρακάτω αποτυπώνονται μερικές πρακτικές του threat hunting, κάποιες είναι καλές και κάποιες όχι. Οι κακές πρακτικές συνήθως ενεργούν ως intrusion detection και όχι σαν threat hunting.

Καλές Πρακτικές:

- Συλλογή πληροφοριών, ανάπτυξη μιας υπόθεσης, δημιουργία ενός σκοπού και εκτέλεση του κυνηγιού(hunt)
- Σχηματισμός μιας υπόθεσης ή χρησιμοποίηση πληροφοριών από την πηγή (threat intelligence feed), και προσδιορισμός των καλύτερων μεθόδων έτσι ώστε να βρεθεί η δραστηριότητα των adversaries την κατάλληλη χρονική στιγμή ή για την αξιοποίηση τους σε μελλοντικά event.

Κακές Πρακτικές:

- Παρατήρηση ενός alert στο σύστημα έτσι ώστε με αργούς μεθόδους να αποχωριστεί από τερματικό σε τερματικό.
- Πολύωρη επισκόπηση και ανάλυση αρχείων καταγραφών στο SIEM και χρησιμοποίηση custom queries.
- Οι αναλυτές παρακολουθούν τα αρχεία καταγραφής και τα event από τα τερματικά. Οι αναλυτές πραγματοποιούν αναθεώρηση και ανασκόπηση στην κίνηση του δικτύου και απομονώνουν συστήματα που έχουν μολυνθεί.
- Η ιδέα ότι το antivirus σε τερματικά είναι η ασφαλέστερη λύση.
- Η φήμη ότι το Threat hunting ανιχνεύεται από τα alerts του SIEM ή από AV alerts

MITRE ATT&CK Framework

Το MITRE's Adversarial Tactics, Techniques and Common Knowledge αποτελεί μια βάση δεδομένων και ένα μοντέλο για συμπεριφορά ενός adversary στον κυβερνοχώρο, αντικατοπτρίζοντας σημαντικές φάσεις κύκλου ενός advesary. Το ATT&CCK είναι χρήσιμο για την κατανόηση του ρίσκου ασφαλείας εναντίων γνωστών συμπεριφορών adversary και για την σχεδίαση τρόπων βελτιστοποίησης ασφάλειας. Το ATT&CK framework παρέχει μια βάση έτσι ώστε να κατανοήσει κάποιος, τον τρόπο εισβολής του επιτιθέμενο.

Παράδειγμα:

Υπάρχουν διαφορετικοί τύποι spearfishing μέθοδοι επίθεσης οι οποίοι μπορούν να εφοδιάσουν τον επιτεθειμένο με άμεση πρόσβαση στο δίκτυο. Το Spear phishing ορίζεται ως ένας κοινός τύπος μιας κυβερνο-επίθεσης, στην οποία οι επιτιθέμενοι εστιάζουν σε λεπτομερή και στοχευμένα μηνύματα ενός συγκεκριμένου παραλήπτη ή μιας ομάδας παραληπτών. Η συγκεκριμένη επίθεση προϋποθέτει την λεπτομερή έρευνα από τον επιτιθέμενο στον πιθανό θύμα ώστε να βρει τις κατάλληλες πληροφορίες, οι οποίες μπορούν να χρησιμοποιηθούν έτσι ώστε να ξεγελάσουν το θύμα. Ο σκοπός είναι να περιηγηθεί ο χρήστης στο κακόβουλο mail που το ήρθε, να κάνει «κλικ» και να κατεβάσει το κακόβουλο payload ή αρχείο έτσι ώστε ο επιτιθέμενος να ξεκινήσει μια ανεπιθύμητη ενέργεια όπως μεταφορά στον λογαριασμό του ή ένα τραπεζικό έμβασμα.

Ο οργανισμός κατανοώντας το attack vector και μαθαίνοντας από αυτόν, θα εκπαιδεύσει τους πελάτες ως προς το θέμα της επίγνωσης ασφάλειας του email. Επιπλέον σημαντική ενέργεια του οργανισμού μετά από την προηγούμενη, είναι η βελτίωση των τεχνικών ανίχνευσης όπως η παραμετροποίηση του sysmon σε ένα Windows σύστημα για την ανίχνευση scripting γλωσσών όπου ανακαλούνται από εφαρμογές παραγωγικότητας. Επίσης ο οργανισμός τίθεται να επιβεβαιώσει την σωστή λειτουργία των τεχνικών συστημάτων προστασίας όπως web filtering proxy και anti spam λύσεις.. Εάν ο οργανισμός έχει ολοκληρώσει αυτά τα βήματα, τότε θα πρέπει να σιγουρευτεί ότι τα συστήματα λειτουργούν αποτελεσματικά. Το SOC πρέπει να κατανοήσει μέσα από όλα αυτά τα βήματα πως δουλεύουν τα data sources.

Παρακάτω αναλύονται παραδείγματα threat hunting ή αλλιώς παραδείγματα Threat Hunt Check List.

1. Ο threat hunter ή αλλιώς ο αναλυτής επιπέδου τρία σε πρώτο στάδιο θα προετοιμάσει και θα εκτελέσει το threat hunting.
   Αρχικά αναζητά για σημάδια command and control. Δηλαδή αναζητά για beacons χρησιμοποιώντας για παράδειγμα Real Intelligence Threat Analytics (RITA) από την Black Hills Information Security, η οποία έχει μηχανισμό ανάλυσης. Εάν δεν υπάρχει μηχανισμό ανάλυσης θα πρέπει ο αναλυτής να αναθεωρήσει τις κορυφαίες IP σε τα μεγαλύτερα νούμερα συνδέσεων, τον μεγαλύτερο χρόνο σύνδεσης και τα περισσότερα δεδομένα που έχουν μετακινηθεί. Εννοείται ότι το SIEM διαθέτει μηχανισμό ανάλυσης και τις προηγούμενες ενέργειες ο αναλυτής μπορεί να τις πραγματοποιήσει μέσα από το εργαλείο SIEM για διευκόλυνση. Επίσης μπορεί να ελέγξει τα μεγαλύτερα σε διάρκεια τρεχούμενα transaction, να ελέγξει τα DNS responses, τους ανώνυμους user agents και άλλα.

2. Σε δεύτερο στάδιο ο threat hunter παρατηρεί για δυνητικούς advesaries ή αλλιώς επιτιθέμενους. Ο αναλυτής πραγματοποιεί ανασκόπηση των event και των alert όπου έχουν παραχθεί από συστήματα τα οποία εμπεριέχουν ευαίσθητα δεδομένα. Φυσικά όλα τα event έχουν την δυνατότητα αποστολής μέσω syslog στο εργαλείο SIEM. Οπότε τα alerts και τα events, ο αναλυτής μπορεί να τα ελέγξει από εκεί. Μια άλλη περίπτωση αποτελεί το φαινόμενο live of the land, όπου σημαίνει ότι ο επιτιθέμενος μπορεί να μοχλεύσει τις ενσωματωμένες εντολές του PowerShell. Ο αναλυτής εξετάζει τα αποτελέσματα του sysmon και το windows security log event ID 4888 για την ανάκληση της διεργασίας, τη διεργασία cmd.exe και την χρησιμοποίηση του command line από το PowerShell.
3. Σε επόμενο στάδιο αρχειοθετεί τα συστήματα τα οποία θα έπρεπε να χρησιμοποιούνται για συγκεκριμένες υπηρεσίες και αναζητά συστήματα τα οποία παραβιάζουν κανόνες όπου διέπουν τα πρωτόκολλα DNS, FTP, email. Επιπλέον παρακολουθεί, δηλαδή πραγματοποιεί την διαδικασία monitoring για όλα τα αγαθά που ανήκουν στο DMZ για εξωτερικές προσπάθειες σύνδεσης. Κανονικά θα πρέπει να απαντούν στα εσωτερικά αιτήματα.
4. Ο αναλυτής πρέπει να παρακολουθεί τα accounts όπου περιέχουν υψηλά δικαιώματα έτσι ώστε να παρακολουθεί τις κινήσεις που γίνονται από αυτούς τους χρήστες

Diamond Model

Ένας αναλυτής πρέπει να γνωρίζει το Diamond model, έτσι ώστε να κατασκευάσει ένα μοτίβο άμυνας για να αμυνθεί στις επόμενες επιθέσεις. Το Diamond model έχει σχεδιαστεί για να αντιπροσωπεύει ένα περιστατικό(event).

Χωρίζεται σε 4 μέρη.

- Adversary
- Capabilities
- Infrastructure
- Victim

Ως advesary θεωρείται ο επιτιθέμενος, ένας hacktivist ή ακόμα και ένας δυσαρεστημένος υπάλληλος. Ο επιτεθειμένος αυτός, θα χρησιμοποιήσει διάφορες ικανότητες ή μέσα επίθεσης όπως exploits, malware, hacker tools. Τα μέσα επίθεσης θα χρησιμοποιηθούν πάνω στην υποδομή (infrastructure) του θύματος ή του οργανισμού.

Η υποδομή εμπεριέχει τα ακόλουθα στοιχεία:

- IP διεύθυνση
- Domain
- Email

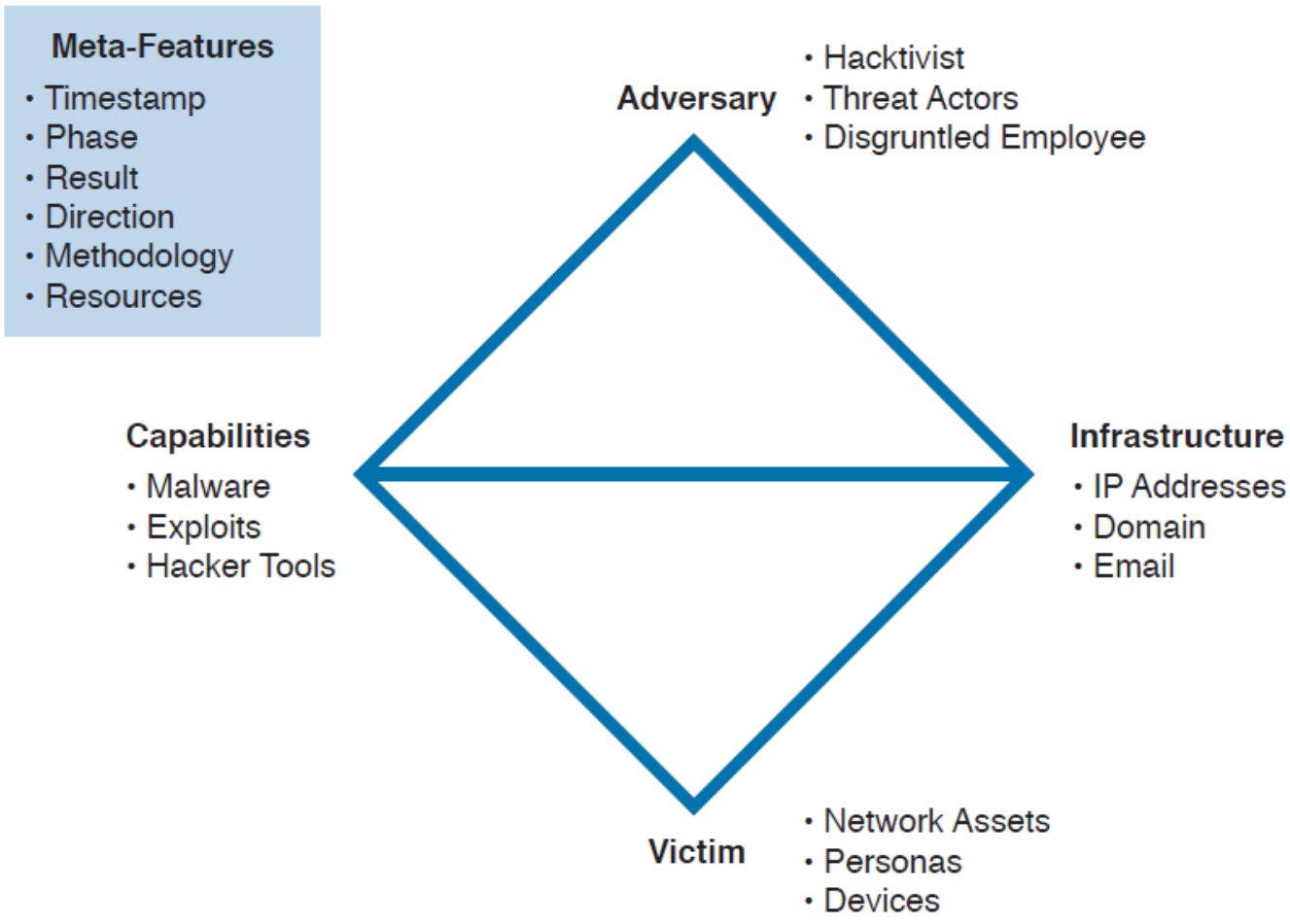
Όσο αφορά το victim, αναλύεται στα εξής χαρακτηριστικά:

- Δικτυακή διεύθυνση
- Personas
- Συσκευές

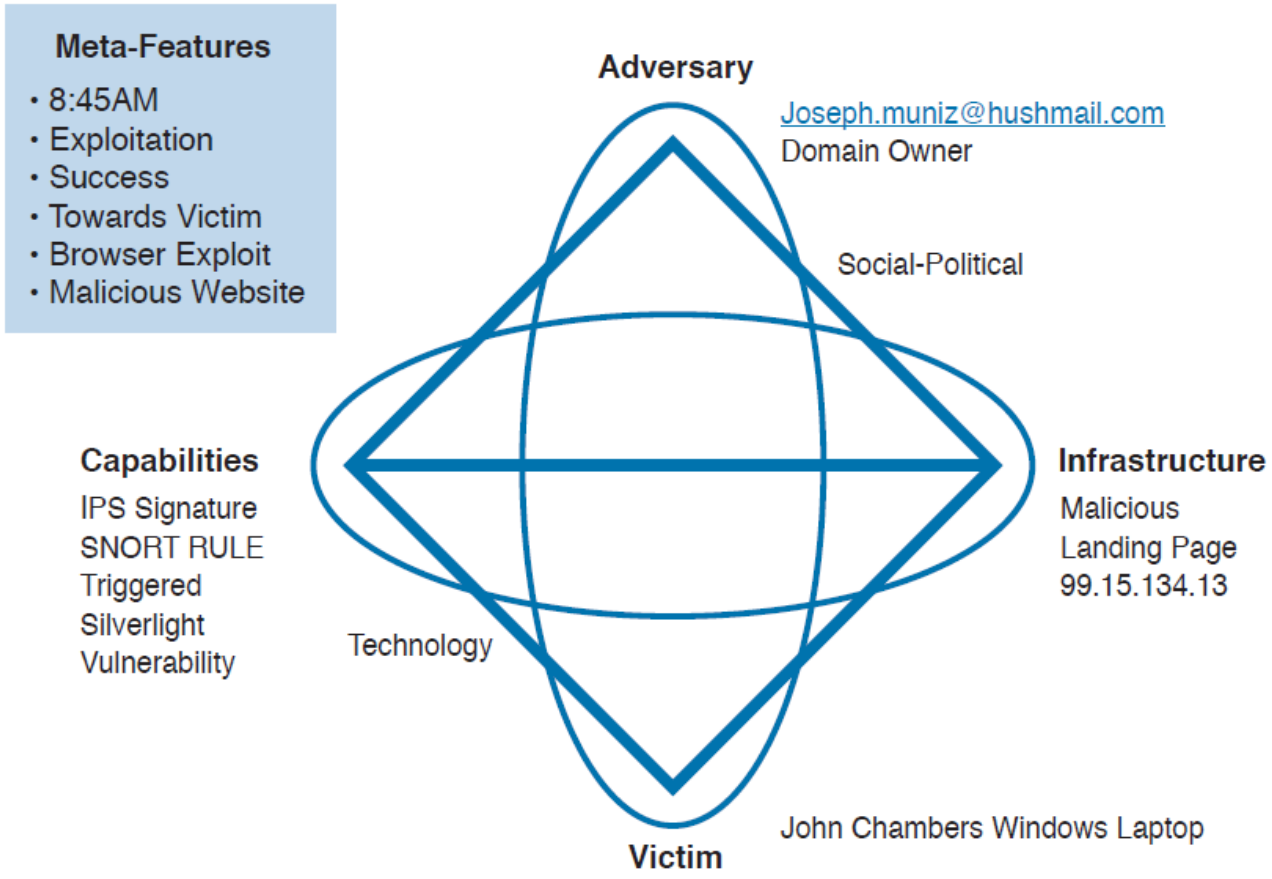
Οι γραμμές που συνδέουν τα μέρη του μοντέλου, απεικονίζουν το πως ένα σημείο έφτασε ένα άλλο. Για παράδειγμα ο αναλυτής μπορεί να δει τον τρόπο σύνδεσης ενός capability με την υποδομή(infrastructure) Το diamond model χρησιμοποιεί ένα επιπλέον πεδίο, το οποίο δεν είναι υποχρεωτικό, τα meta-features. Περιέχουν χρήσιμο περιεχόμενο και μπορούν να δώσουν στον αναλυτή, λεπτομερή στοιχεία.

Meta-Features:

- Timestamp
- Phase
- Result
- Direction
- Methodology
- Resources



Diamond Model 1



Diamond Model 2

Cyber Kill Chain

Η αλυσίδα του cyber kill χρησιμοποιείται στο diamond model και βοηθάει τους αναλυτές και ομάδες infosec να κατηγοριοποιήσουν τις επιθέσεις αλλά και αν συνδέσουν τομείς όπως τρόπο επίθεσης και άλλα.

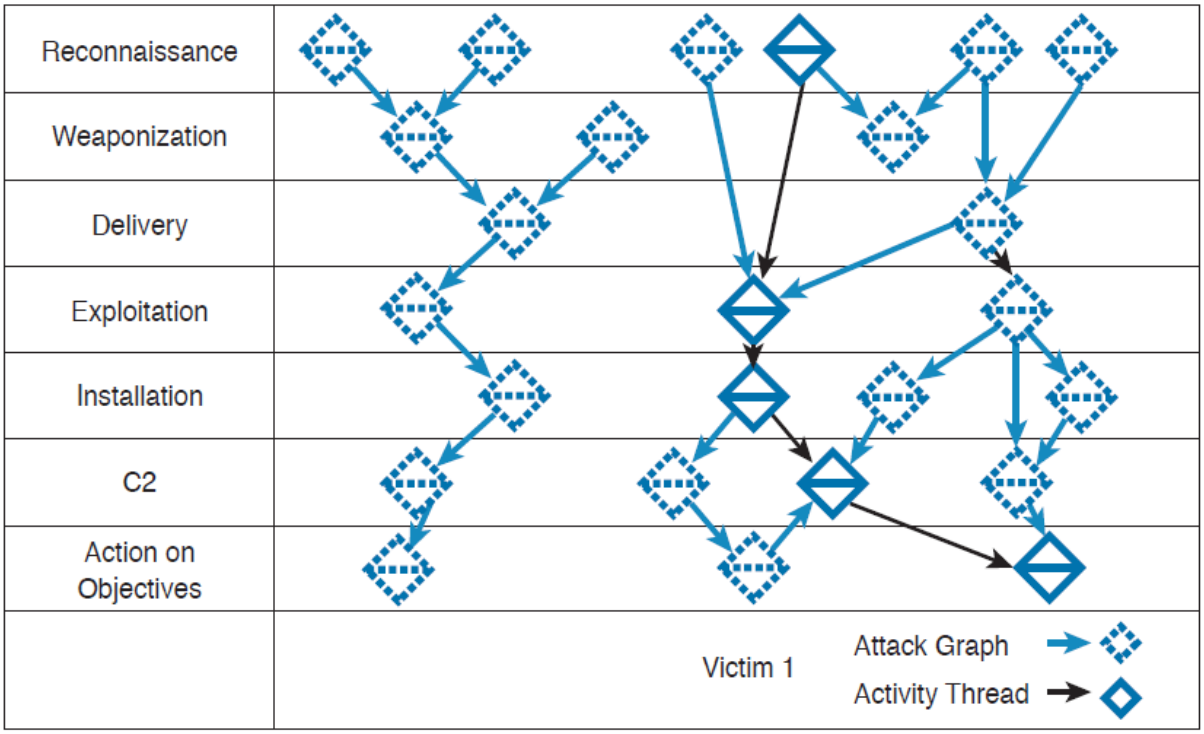
Στην ουσία αποτυπώνει τα βήματα του adversary έτσι ώστε να πραγματοποιήσει μια εισβολή. Η αλυσίδα εμπεριέχει κάποια στάδια, τα οποία είναι σημεία αναφοράς για το SOC. Είναι πολύ χρήσιμα, έτσι ώστε να καταλάβουν τα στάδια επίθεσης. Έτσι θα μπορούν να αποτρέψουν ή να σταματήσουν την επίθεση πριν φτάσει στο τελικό στάδιο δηλαδή στον σκοπό της,

Παρακάτω αναφέρονται τα στάδια του cyber kill chain:

- Reconnaissance (Αναγνώριση)
  Στην αναγνώριση πραγματοποιείται η συλλογή πληροφοριών. Η συλλογή αυτή βοηθάει τον adversary να ερευνήσει τον στόχο επίθεσης του καλύτερα.

- Weaponization (Οπλισμού)
  Η φάση του οπλισμού ορίζεται ώς την ανάπτυξη και σχεδιασμό των επιθέσεων βάση των δεδομένων που εντοπίστηκαν κατά την διάρκεια της φάσης της αναγνώρισης.
- Delivery
  Στη φάση της παράδοσης, καθορίζεται το πως θα αναπτυχθεί η επίθεση βάση το στάδιο του οπλισμού.
- Exploitation
  Όταν η επίθεση έχει γίνει launched εναντίων μιας ευπάθειας εννοείται πάντα στην υποδομή του στόχου, τότε έχει πραγματοποιηθεί η φάση του exploitation.
- Command and control
  Όταν ο advesary συνδεθεί στο compromised σύστημα, τότε επιτελείται η cnc φάση.
- Action and objectives (Δράση και στόχοι)
  Καθώς έχει συνδεθεί στο σύστημα και έχει προχωρήσει τον στόχο του, ο adversary ξεκινάει την επίθεση. Αυτό αντιπροσωπεύει την φάση δράση και στόχοι.

  Παρακάτω απεικονίζεται η εικόνα της συσχέτισης του Diamond Model με το Cyber Kill Chain



ΠΗΓΕΣ

[1] Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases – Notes from the Field (V1.02)
Don Murdoch

[2] BTFM Blue Team Field Manual Version 1 – ALAN WHITE, BEN CLARK. Copyright ©2017

[3] Cybersecurity – Attack and Defense Strategies

[4] Wikipedia

[5] CCNA – Cyber Ops 210-255

[6] NIST Computer Security Incident Handling Guide – Special Publication 800-61

[7] https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493840947.pdf

[8] https://www.bluesec.pl/wp-content/uploads/2017/03/SecurityOperationsCenter_eBook.pdf

[9] https://stratsolutions.com/wp-content/uploads/2018/06/AWN_Definitive-Guide-to-SOCaaS-ebook-final.pdf

[10] https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf

[11] https://developers.google.com/machine-learning/crash-course/classification/true-false-positive-negative

[12] https://www.careersincyber.com/article-details/8/a-day-in-the-life-of-a-security-analyst/

[13] https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

[14] https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf

[15] https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

[16] https://digital-forensics.sans.org/media/Targeted-SOC-Use-Cases-for-effective-Incident-Detection-and-Response-Angelo-Perniola-David-Gray.pdf

[17] https://www.capgemini.com/2019/05/how-to-define-complex-use-cases-and-implement-them-in-your-siem-soc-project/

[18] https://resources.infosecinstitute.com/top-6-seim-use-cases/

[19] https://www.sumologic.com/blog/why-modern-siem/

[20] Nadean H. Tanner - Cybersecurity Blue Team Toolkit (2019, Wiley)

[21] SANS Institute - A Practical Model for Conducting Cyber Threat Hunting

[22] SANS Analyst Program - SANS 2018 Threat Hunting

Survey Results

[23] Threat hunting and active cyber defense – Anthony Paris, Jr.

[24] https://medium.com/taslet-security/the-rise-of-next-generation-security-operation-center-ng-soc-266d0522681b

[25] https://xmcyber.com/purple-team/

[26] https://www.rapid7.com/fundamentals/spear-phishing-attacks/