Πανεπιστήμιο Πειραιώς

Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνίων

Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών

«Ασφάλεια Ψηφιακών Συστημάτων»

Μεταπτυχιακή Διπλωματική Εργασία

Open-source Security Orchestration, Automation and Response (SOAR) platform deployment and use

Επιβλέπον Καθηγητής: Χρήστος Ξενάκης

Ονοματεπώνυμο	E-mail	A.M.
Νικόλαος Τσιλίκας	nikolaos.tsilikas@ssl-unipi.gr	MTE2130

Πειραιάς

05/04/2023

Περίληψη

Με την αυξανόμενη εξάρτηση της σύγχρονης κοινωνίας από την υποδομή πληροφορικής, η σημασία της ασφάλειας στον κυβερνοχώρο αυξάνεται επίσης. Τα εργαλεία που χρησιμοποιούνται από τους εισβολείς χρησιμοποιούν συχνά την αυτοματοποίηση για να βρουν και να εκμεταλλευτούν τρωτά σημεία στα συστήματα ενός οργανισμού, ενώ οι επιθέσεις έχουν γίνει επίσης πιο εξελιγμένες και χρονοβόρες για την πρόληψη, επομένως απαιτείται αυτοματοποίηση και στην ασφάλεια στον κυβερνοχώρο.

Σκοπός της παρούσης εργασίας είναι η περιγραφή της τεχνολογίας Security Orchestration, Automation and Response (SOAR) καθώς και η εξέταση του τι αυτή εξυπηρετεί και τι προβλήματα επιλύει. Στα πρώτα κεφάλαια δίνεται μια περιγραφή του προβλήματος και της ανάγκης που υπάρχει για αυτοματοποίηση καθώς επίσης παρουσιάζεται η λειτουργία του Security Operation Center (SOC) και των κυριότερων εργαλείων ασφαλείας που χρησιμοποιούνται στις μέρες μας. Στην συνέχεια, στο κεφάλαιο 4, γίνεται περιγραφή της τεχνολογίας SOAR και των συστατικών αυτής καθώς επίσης παρουσιάζονται τα πλεονεκτήματα χρήσης των πλατφορμών SOAR και τι προβλήματα επιλύονται από την χρήση τους. Στο επόμενο κεφάλαιο 5 παρουσιάζονται τέσσερις από τις πιο γνωστές πλατφόρμες SOAR και γίνεται μια σύγκριση μεταξύ τους. Τέλος, στο κεφάλαιο 6, περιγράφεται η εγκατάσταση και λειτουργία μέσα από usecases της πλατφόρμας SOAR ανοικτού κώδικα Shuffle.

Τσιλίκας Νικόλαος
ΑΜ. MTE2130

Λέξεις κλειδιά: αυτοματισμός, ενορχήστρωση, SOAR, κυβερνοασφάλεια, απειλές, απόκριση, ασφάλεια, τεχνολογία, Shuffle.

Περιεχόμενα

Πίνακας Εικόνων

1. Εισαγωγή

Η ασφάλεια στον κυβερνοχώρο είναι ένα σημαντικό θέμα από την εποχή δημιουργίας του Διαδικτύου. Η σημασία της ασφάλειας έχει αυξηθεί τα τελευταία χρόνια λόγω της αυξανόμενης εξάρτησης από τις υποδομές πληροφορικής λόγω της τηλεργασίας, της διαδικτυακής ψυχαγωγίας και των διαδικτυακών επιχειρήσεων. Με ταχύτερες συνδέσεις στο Διαδίκτυο, περισσότερους χρήστες και περισσότερες συσκευές, ο όγκος των δεδομένων που κινούνται στα δίκτυα έχει σημειώσει τεράστια αύξηση. Οι διακοπές στη ροή των δεδομένων μπορεί να είναι πολύ δαπανηρές για τις επιχειρήσεις και την κοινωνία.

Οι οργανισμοί αντιμετωπίζουν μια συνεχή απειλή καθώς οι απειλές και οι επιθέσεις για την ασφάλεια γίνονται όλο και πιο περίπλοκες και οι εισβολείς χρησιμοποιούν αυτοματοποίηση. Η διατήρηση των εφαρμογών, των λειτουργικών συστημάτων και των συσκευών με ασφάλεια και ο εντοπισμός, η ανάλυση και η απόκριση σε απειλές είναι χρονοβόρα για τους ειδικούς σε θέματα ασφάλειας και η αυτοματοποίηση αυτών των διαδικασιών είναι ένας τρόπος να γίνουν τα συστήματα πιο ανθεκτικά και ασφαλή έναντι πολλών απειλών.

Η αυτοματοποίηση πολύπλοκων εργασιών ασφαλείας είναι ένας νέος τομέας, με πολλά περιθώρια ανάπτυξης. Ο αυτοματισμός στην ασφάλεια χρησιμοποιείται από τη χρήση βασικών σεναρίων έως πιο σύνθετες διαδικασίες, όπως η ενσωμάτωση μηχανικής μάθησης και τεχνητής νοημοσύνης σε λογισμικό ασφαλείας.

Οι οργανισμοί χρησιμοποιούν διάφορες λύσεις ασφαλείας για να αποτρέψουν γνωστές και άγνωστες επιθέσεις και να αποφύγουν τις συνέπειες που συνήθως συνδέονται με τρωτά σημεία και απειλές ασφαλείας [1]. Μερικές από τις ευρέως χρησιμοποιούμενες λύσεις ασφαλείας είναι τα προγράμματα προστασίας από ιούς, Firewall, Intrusion Detection Systems and Instruction Prevention Systems (IDS/IPS), και Security Information and Events Management (SIEM).[2] Οι πάροχοι λύσεων ασφαλείας χρησιμοποιούν διαφορετικές τεχνολογίες και πρότυπα για την ανάπτυξη, την υλοποίηση και τη λειτουργία των λύσεων ασφαλείας τους, οι οποίες δεν μπορούν εύκολα να ενοποιηθούν και να λειτουργήσουν συνδυαστικά μεταξύ τους για την

[1] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques, Journal of Network and Computer Applications", vol. 60, pp. 19-31, 2016.
[2] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," Journal of Network and Computer Applications, vol. 101, pp. 18-54, 2018.

αποτελεσματική και αποδοτική υποστήριξη του Κέντρου Επιχειρήσεων Ασφαλείας (Security Operation Centre – SOC).

Η τεχνολογία Security orchestration, automation, and response (SOAR) είναι μια τεχνολογία που συνδυάζει διάφορα εργαλεία και διαδικασίες ασφαλείας για την αυτοματοποίηση και την βελτιστοποίηση της απόκρισης συμβάντων. Επιτρέπει στις ομάδες ασφαλείας να ανταποκρίνονται γρήγορα και αποτελεσματικά σε συμβάντα ασφαλείας αυτοματοποιώντας επαναλαμβανόμενες εργασίες, όπως συλλογή δεδομένων, ανάλυση και επικοινωνία, και παρέχοντας μια ενοποιημένη άποψη της ασφάλειας ενός οργανισμού. Τα συστήματα SOAR περιλαμβάνουν συνήθως δυνατότητες όπως διαχείριση συμβάντων, threat intelligence, αυτοματοποίηση απόκρισης περιστατικών και δημιουργία αναφοράς. Αυτή η τεχνολογία έχει σχεδιαστεί για να βελτιώνει τους χρόνους απόκρισης συμβάντων, να αυξάνει την αποτελεσματικότητα της ομάδας ασφαλείας και να μειώνει τον κίνδυνο παραβιάσεων, αυτοματοποιώντας τη διαδικασία απόκρισης σε περιστατικά ασφαλείας, παρέχοντας ευέλικτες πληροφορίες και συντονίζοντας τα διαφορετικά εργαλεία ασφαλείας σε έναν οργανισμό. Οι οργανισμοί υιοθετούν ολοένα και περισσότερο πλατφόρμες SOAR οι οποίες αποτελούν proactive, αυτόνομες και συνεργατικές λύσεις που επιτρέπουν στο προσωπικό ασφαλείας να εκτελεί τις ευθύνες του αποτελεσματικά και αποδοτικά.[3]

Σκοπός αυτής της εργασίας είναι να γίνει περιγραφή της τεχνολογίας “Security Orchestration, Automation and Response (SOAR)” και στην συνέχεια υλοποίηση μιας open source πλατφόρμας, ονόματι Shuffle. Στα επόμενα κεφάλαια θα γίνει αρχικά μια περιγραφή του θεωρητικού υποβάθρου ώστε να γίνει κατανοητό τι εξυπηρετεί και τι προβλήματα επιλύει η τεχνολογία SOAR. Για το σκοπό αυτό θα δοθούν πληροφορίες για τα Security Operation Centres (SOCs) καθώς και εργαλείων που χρησιμοποιούνται, όπως των λογισμικών Security Information and Event Management (SIEM). Στην συνέχεια θα γίνει παρουσίαση της τεχνολογίας SOAR, θα αναφερθούν κάποιες από τις σημαντικότερες υλοποιήσεις ανοικτού κώδικα SOAR πλατφορμών και θα γίνει μια σύγκριση αυτών. Τέλος, θα παρουσιαστεί η εγκατάσταση και βασική λειτουργία της πλατφόρμας Shuffle.

[3] B. Schneier, “Security Orchestration for an Uncertain World”, 2017, https://securityintelligence.com/security-orchestration-for-an-uncertain-world/ , Accessed on: February 4, 2023.

2. Θεωρητικό υπόβαθρο

2-1. SOC

Στη σύγχρονη εποχή των υπολογιστών, υπάρχουν διάφορες απειλές στον κυβερνοχώρο που στοχεύουν οργανισμούς όλων των μεγεθών. Στη χειρότερη περίπτωση, κακόβουλοι παράγοντες εισβάλλουν στον οργανισμό και μπορεί να προκαλέσουν τεράστιες απώλειες δεδομένων και χρημάτων. Οι κυβερνοεπιθέσεις, οι παραβιάσεις δεδομένων και οι μολύνσεις από κακόβουλο λογισμικό έχουν γίνει τόσο συνηθισμένες που τα περισσότερα τμήματα πληροφορικής πρέπει να εντοπίζουν και να μετριάζουν αυτές τις απειλές καθημερινά προτού προκαλέσουν επικίνδυνα αποτελέσματα.

Ένα Security Operation Centre (SOC) παρέχει συνεχή παρακολούθηση για τους οργανισμούς με σκοπό να βελτιώσει την ασφάλεια του οργανισμού αναλύοντας και δρώντας ενάντια στις απειλές που εντοπίζονται ως περιστατικά ασφάλειας στον κυβερνοχώρο.[4]

Εν ολίγοις, ένα SOC είναι μια ομάδα αναλυτών ασφάλειας, των οποίων η δουλειά είναι να ανιχνεύει, να αναλύει, να ανταποκρίνεται, να αναφέρει και να αποτρέπει περιστατικά ασφάλειας στον κυβερνοχώρο.[5] Υπάρχουν δύο τύποι SOC, ένα εσωτερικό SOC που υπάρχει σε έναν οργανισμό και είναι υπεύθυνο για τις λειτουργίες ασφαλείας αυτού του οργανισμού και το μοντέλο SOC-as-a-service που ανατίθεται σε εξωτερικούς συνεργάτες και προσφέρεται από διαχειριζόμενους παρόχους υπηρεσιών ασφαλείας (managed security service providers - MSSP). Οι μεγαλύτερες επιχειρήσεις έχουν συχνά εσωτερικά SOC, ενώ οι μεσαίες επιχειρήσεις συχνά εξετάζουν υβριδικές λύσεις ή αναθέτουν σε εξωτερικούς συνεργάτες τις λειτουργίες ασφαλείας τους με MSSP.

Το SOC είναι το μέρος όπου παρακολουθούνται όλα τα καταγεγραμμένα συμβάντα στο δίκτυο και είναι υπεύθυνο για τη λήψη μέτρων όταν χρειάζεται. Ο στόχος ενός SOC είναι να κατανοήσει ολόκληρο το εύρος των απειλών του οργανισμού και να κάνει ό,τι καλύτερο μπορεί για την προστασία της εσωτερικής υποδομής πληροφορικής, καθώς και των υπηρεσιών τρίτων, όπως οι υπηρεσίες cloud.

Για την επίτευξη αυτού του στόχου, διεξάγεται συνεχής παρακολούθηση με εργαλεία που σαρώνουν το δίκτυο όλο το εικοσιτετράωρο. Το κέντρο ασφαλείας ειδοποιείται αμέσως για ανώμαλη δραστηριότητα και απειλές, επομένως τα περισσότερα προβλήματα μπορούν να

[4] Aher, B., “Importance of a Security Operations Center”, 2018, https://dzone.com/articles/importance-of-security-operations-center , Accessed on: February 4, 2023

[5] Zimmerman C. “Ten Strategies of a World-Class Cybersecurity Operations Center.” McLean, USA: MITRE Corporation, 2014. p. 8-9.: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.545&rep=rep1&type=pdf , Accessed on: February 4, 2023

αποφευχθούν ή να μετριαστούν πριν γίνουν σοβαρά περιστατικά. Οι αναλυτές δεν χρειάζεται να ερευνούν κάθε ειδοποίηση επειδή φιλτράρονται τα false alerts, οι περιττές ειδοποιήσεις και οι μη κρίσιμες ειδοποιήσεις. Στην περίπτωση πραγματικών απειλών, το SOC θα καθορίσει τη σημασία και θα ανταποκριθεί στην απειλή αναλόγως απομονώνοντας τα endpoints γύρω από το συμβάν εάν χρειαστεί και διενεργώντας έρευνα, διασφαλίζοντας παράλληλα ότι το συμβάν θα έχει ελάχιστο αντίκτυπο στον οργανισμό.

Μετά την απόκριση σε μια απειλή, πραγματοποιείται ανάκτηση και αποκατάσταση. Ο καθαρισμός των συσκευών, η επαναφορά αντιγράφων ασφαλείας και η επαναδιαμόρφωση των συστημάτων είναι ορισμένες πτυχές ανάκτησης και αποκατάστασης. Η εύρεση της βασικής αιτίας είναι σημαντική για την αποτροπή τέτοιων επιθέσεων στο μέλλον, επομένως τα αρχεία καταγραφής της δραστηριότητας του δικτύου διερευνώνται για να εντοπιστεί η πηγή του προβλήματος και να ληφθούν μέτρα εάν χρειάζεται για να διορθωθούν τυχόν «τρύπες» που εντοπίστηκαν στην ασφάλεια

Ακριβώς όπως σε κάθε άλλη οργανωτική μονάδα, υπάρχουν αρκετοί διαφορετικοί ρόλοι και αρμοδιότητες σε ένα SOC. Ανάλογα με το εύρος και το μέγεθος, χρειάζονται διαφορετικές ομάδες σε διαφορετικούς αριθμούς. Τυπικοί βασικοί ρόλοι σε ένα SOC είναι διαφορετικά επίπεδα αναλυτών καθώς και διευθυντών. Μπορούμε να ξεχωρίσουμε τρεις ρόλους με αντίστοιχες αρμοδιότητες: [6]

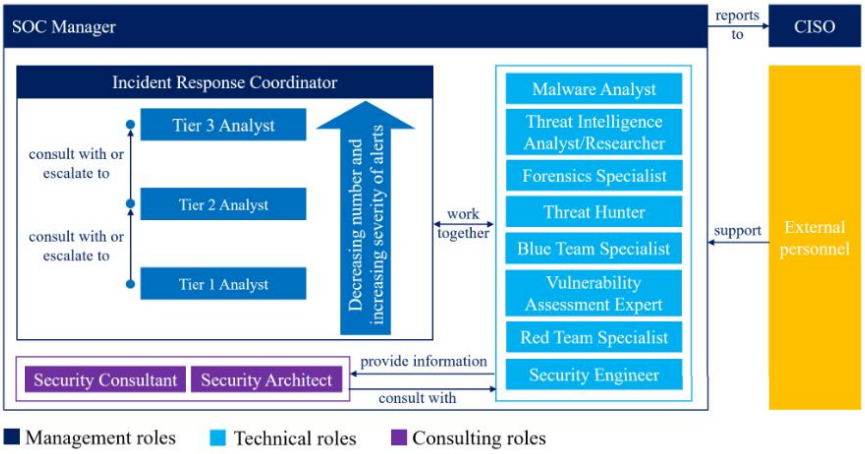
- **Tier 1 (Triage Specialist):** Οι αναλυτές της βαθμίδας 1 είναι κυρίως υπεύθυνοι για τη συλλογή ανεπεξέργαστων δεδομένων, καθώς και για τον έλεγχο alarm και alert. Πρέπει να επιβεβαιώσουν, να καθορίσουν ή να προσαρμόσουν την κρισιμότητα των ειδοποιήσεων και να τις εμπλουτίσουν με σχετικά δεδομένα. Για κάθε ειδοποίηση, ο ειδικός διαλογής πρέπει να προσδιορίσει εάν είναι δικαιολογημένη ή false positive. Μια πρόσθετη ευθύνη σε αυτό το επίπεδο είναι ο εντοπισμός άλλων γεγονότων υψηλού κινδύνου και πιθανών συμβάντων. Όλα αυτά πρέπει να ιεραρχηθούν ανάλογα με την κρισιμότητα τους. Εάν τα προβλήματα που εμφανίζονται δεν μπορούν να επιλυθούν σε αυτό το επίπεδο, προωθούνται σε αναλυτές της βαθμίδας 2. Επιπλέον, οι ειδικοί διαλογής συχνά διαχειρίζονται και διαμορφώνουν τα εργαλεία παρακολούθησης.
- **Tier 2 (Incident Responder):** Στη βαθμίδα 2, οι αναλυτές εξετάζουν τα πιο κρίσιμα περιστατικά ασφαλείας που κλιμακώνονται από τους ειδικούς διαλογής της βαθμίδας 1 και κάνουν μια πιο εις βάθος αξιολόγηση χρησιμοποιώντας threat intelligence.

[6] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul, "Security Operations Center: A Systematic Study and Open Challenges", p.7-9, 2020.

Πρέπει να κατανοήσουν το εύρος μιας επίθεσης και να γνωρίζουν τα επηρεαζόμενα συστήματα. Οι υπεύθυνοι αντιμετώπισης περιστατικών είναι υπεύθυνοι για το σχεδιασμό και την εφαρμογή στρατηγικών για τον περιορισμό και την ανάκαμψη από ένα περιστατικό. Εάν ένας αναλυτής επιπέδου 2 αντιμετωπίζει σημαντικά προβλήματα με τον εντοπισμό ή τον μετριασμό μιας επίθεσης, ζητείται η γνώμη επιπλέον αναλυτών της βαθμίδας 2 ή το περιστατικό κλιμακώνεται στο επίπεδο 3.

- **Tier 3 (Threat Hunter):** Οι αναλυτές της βαθμίδας 3 είναι το πιο έμπειρο εργατικό δυναμικό σε ενα SOC. Χειρίζονται μεγάλα περιστατικά που προωθήθηκαν από τους Incident Responders. Εκτελούν επίσης ή τουλάχιστον επιβλέπουν τις αξιολογήσεις ευπάθειας και τις δοκιμές διείσδυσης για τον εντοπισμό πιθανών φορέων επίθεσης. Η σημαντικότερη ευθύνη τους είναι να εντοπίζουν προληπτικά πιθανές απειλές, κενά ασφαλείας και τρωτά σημεία που μπορεί να είναι άγνωστα. Καθώς αποκτούν εύλογες γνώσεις σχετικά με μια πιθανή απειλή για τα συστήματα, θα πρέπει επίσης να προτείνουν τρόπους βελτιστοποίησης των αναπτυγμένων εργαλείων παρακολούθησης ασφάλειας. Επίσης, τυχόν κρίσιμες ειδοποιήσεις ασφαλείας, πληροφορίες απειλών και άλλα δεδομένα ασφαλείας που παρέχονται από αναλυτές βαθμίδας 1 και 2 πρέπει να επανεξεταστούν σε αυτό το επίπεδο.

Άλλοι κοινοί βασικοί ρόλοι που περιέχει το SOC είναι Malware Analyst, Digital Forensics Analyst, Threat Intelligence Analyst, SOC System Admin, SOC Manager. Ανάλογα με το μέγεθος του SOC ένα άτομο μπορεί να είναι υπεύθυνο για πολλούς ρόλους. Στην παρακάτω εικόνα φαίνεται η αλληλεπίδραση μεταξύ των διαφορετικών ρόλων σε ένα SOC.[7]



Εικόνα 1. Αλληλεπίδραση μεταξύ των διαφορετικών ρόλων σε ένα SOC.

[7] C. Olt, "Establishing security operation centers for connected cars," ATZelectronics worldwide, vol. 14, no. 5, pp. 40–43, May 2019.

2-2. SIEM

Ένα Security Information and Event Management (SIEM) βοηθά στη συγκέντρωση δεδομένων από όλο το περιβάλλον πληροφορικής σε ένα κεντρικό αποθετήριο για περαιτέρω ανάλυση. Τα δεδομένα που συλλέγονται περιλαμβάνουν πληροφορίες ασφαλείας, αρχεία καταγραφής, δεδομένα των endpoints και δεδομένα δικτύου. Αυτά τα δεδομένα μπορούν να συσχετιστούν ιστορικά και σε πραγματικό χρόνο για τον εντοπισμό ανωμαλιών, τρωτών σημείων και περιστατικών. Κυρίως η εστίαση επικεντρώνεται σε δεδομένα που σχετίζονται με την ασφάλεια, για παράδειγμα πληροφορίες σύνδεσης, ανιχνεύσεις κακόβουλου λογισμικού και privilege escalation. Το SIEM προσφέρει επίσης οπτικοποίηση και dashboard για ευκολότερη ανάλυση.

Η μηχανική μάθηση (ML) χρησιμοποιείται για την περαιτέρω βελτίωση των δυνατοτήτων των SIEM. Οι λύσεις SIEM επόμενης γενιάς ενσωματώνουν τεχνικές μηχανικής μάθησης για την καλύτερη ανάλυση του τεράστιου όγκου δεδομένων που χειρίζονται τα συστήματα και αυτά τα μοντέλα ML εκπαιδεύονται να βρίσκουν τόσο γνωστές όσο και άγνωστες απειλές και περιλαμβάνουν επίσης ανάλυση συμπεριφοράς. Τα αναλυτικά στοιχεία συμπεριφοράς χρηστών και οντοτήτων (User and entity behavior analytics – UEBA) παρακολουθούν και μοντελοποιούν την κανονική συμπεριφορά οντοτήτων και χρηστών για να δημιουργήσουν μια γραμμή βάσης. Η γραμμή βάσης περιλαμβάνει πού και πότε ο χρήστης συνδέεται στα συστήματα, σε ποια αρχεία και διακομιστές έχει συνήθως πρόσβαση και ποιες συσκευές χρησιμοποιεί. Όταν ανιχνεύονται ανωμαλίες και ύποπτη δραστηριότητα, ειδοποιείται το SOC. Η UEBA μπορεί να βοηθήσει στην άμυνα ενάντια σε εσωτερικές απειλές, καθώς και σε περιπτώσεις όπου τα διαπιστευτήρια ενός υπαλλήλου κλαπούν και χρησιμοποιούνται με κακόβουλο τρόπο.

2-3. IDS / IPS

Τα Intrusion Detection Systems (IDS) και τα Intrusion Prevention Systems (IPS) παρακολουθούν την κυκλοφορία του δικτύου και συγκρίνουν τα περιεχόμενα των πακέτων με μια βάση δεδομένων γνωστών απειλών. Η διαφορά μεταξύ τους είναι ότι το IDS είναι ένα παθητικό σύστημα που λειτουργεί μόνο σε ανίχνευση και παρακολούθηση και δεν αναλαμβάνει δράση από μόνο του, ενώ το IPS είναι ένα σύστημα ελέγχου που μπορεί να απορρίψει πακέτα εάν το περιεχόμενό τους βρεθεί κακόβουλο.[8]

[8] Petters J. “IDS vs. IPS: What is the Difference?” , 2020. https://www.varonis.com/blog/ids-vs-ips/ , Accessed on: February 4, 2023

Υπάρχουν δύο κατηγορίες συστημάτων IDS και IPS ανάλογα με την τεχνική ανίχνευσης: ανίχνευση βάσει υπογραφών και ανίχνευση βάσει στατιστικών ανωμαλιών. Η ανίχνευση που βασίζεται σε υπογραφές είναι ευάλωτη σε επιθέσεις zero-day, επειδή δεν βρίσκονται ακόμη σε μια βάση δεδομένων γνωστών απειλών. Η ανίχνευση βάσει ανωμαλιών δημιουργεί μια γραμμή βάσης δικτύου και όταν υπάρχει απόκλιση, ειδοποιείται ο διαχειριστής. Η ανίχνευση που βασίζεται σε ανωμαλίες είναι ισχυρότερη έναντι νέων τύπων επιθέσεων, αλλά έχει υψηλότερο ποσοστό false positive αποτελεσμάτων. Τα σύγχρονα συστήματα IDS και IPS χρησιμοποιούν συνδυασμό των δύο τεχνικών.[9]

Τα IPS είναι ένα καλό παράδειγμα αυτοματισμού στην ασφάλεια. Αυτά τα συστήματα απαιτούν μόνο να διατηρούνται ενημερωμένες οι βάσεις δεδομένων απειλών και χειρίζονται από μόνα τους τον εντοπισμό και την απόκριση σε απειλές και επιθέσεις. Τα IPS έχουν αντικαταστήσει τα IDS σε κάποιο βαθμό λόγω των χαρακτηριστικών αυτόματης απόκρισης που διαθέτουν τα IPS.

2-4. Firewall

Τα παραδοσιακά port-based firewall είναι αναποτελεσματικά για την προστασία των εταιρικών δικτύων, επειδή μια προσέγγιση port-based περιορίζεται στον έλεγχο της TCP ή UPD header ενός πακέτου για τον προσδιορισμό του πρωτοκόλλου εφαρμογής και στη συνέχεια είτε επιτρέπει είτε αποκλείει την κυκλοφορία μέσω μιας θύρας. Για την αντιμετώπιση αυτού του προβλήματος, εφαρμόζονται IDS/IPS, φιλτράρισμα διευθύνσεων URL και άλλες λύσεις ασφαλείας, που οδήγησαν σε πιο περίπλοκα και δυσκολότερα στη διαμόρφωση συστήματα.

Τα next generation firewalls (NGFW) αναπτύχθηκαν για να «αποκαταστήσουν τα τείχη προστασίας ως τον ακρογωνιαίο λίθο της ασφάλειας του εταιρικού δικτύου».[10] Τα NGFW ρυθμίζονται με βάση τον χρήστη και τις εφαρμογές τους και ενσωματώνουν λειτουργίες IPS και παραδοσιακά τείχη προστασίας. Τα κύρια χαρακτηριστικά των παραδοσιακών firewall είναι το φιλτράρισμα πακέτων, η μετάφραση διευθύνσεων δικτύου και θύρας, ο έλεγχος κατάστασης και η υποστήριξη VPN. Το NGFW ήταν μια από τις πρώτες τεχνολογίες που εκμεταλλεύτηκε μια αρχιτεκτονική zero-trust. Η zero-trust λειτουργεί με βάση το «ποτέ μην εμπιστεύεστε, πάντα επαληθεύστε», σε αντίθεση με την «πάντα εμπιστοσύνη» στην

[9] Nilă C, Apostol I, Patriciu V. "Machine learning approach to quick incident response." In: 2020 13th International Conference on Communications, 2020. p. 291-292. https://doi.org/10.1109/COMM48946.2020.9141989 , Accessed on: February 4, 2023

[10] Miller L. "Next-Generation Firewalls For Dummies." New Jersey: John Wiley & Sons; 2019. p. 3-5. https://incom.co.uk/wp-content/uploads/2020/10/Next-Generation-Firewalls-For-Dummies.pdf , Accessed on: February 4, 2023

κυκλοφορία δικτύου που προέρχεται από το εσωτερικό του δικτύου, γεγονός που αφήνει το δίκτυο ευάλωτο σε επιθέσεις lateral movement.

Τα NGFW ενσωματώνουν αυτοματισμό ροής εργασιών, αυτοματισμό πολιτικής και αυτοματισμό ασφάλειας. Ο αυτοματισμός ροής εργασίας περιλαμβάνει API, έτσι ώστε το τείχος προστασίας να μπορεί να προγραμματιστεί με άλλα εργαλεία και σενάρια που μπορεί να χρησιμοποιήσει ο χρήστης. Τα NGFW μπορούν επίσης να χρησιμοποιούν τα API άλλων συσκευών για να κάνουν αλλαγές πολιτικής όταν είναι απαραίτητο. Η αυτοματοποίηση πολιτικής σημαίνει ότι το τείχος προστασίας είναι σε θέση να προσαρμόζεται στις αλλαγές στο περιβάλλον και μπορεί να λάβει πληροφορίες για τις απειλές από τρίτες πηγές και να ενεργεί αυτόματα σε αυτές τις πληροφορίες. Ο αυτοματισμός ασφαλείας επιτρέπει στο τείχος προστασίας να αποκλείει νέες απειλές όταν οι πληροφορίες τους παραδίδονται στο τείχος προστασίας από άλλα εργαλεία ασφαλείας.

2-5. EDR

Ο όρος Endpoint Detection and Response (EDR), επινοήθηκε από τον A. Chuvakin [11] το 2013. Τα EDR συλλέγουν δεδομένα από endpoints και τα στέλνουν για αποθήκευση και επεξεργασία σε μια κεντρική βάση δεδομένων. Εκεί, τα συλλεχθέντα συμβάντα, τα δυαδικά αρχεία κ.λπ., θα συσχετιστούν σε πραγματικό χρόνο για τον εντοπισμό και την ανάλυση ύποπτων δραστηριοτήτων στους υπολογιστές που παρακολουθούνται. Έτσι, τα EDR ενισχύουν τις δυνατότητες των SOC καθώς ανακαλύπτουν και ειδοποιούν τόσο τον χρήστη όσο και τις ομάδες απόκρισης έκτακτης ανάγκης για αναδυόμενες απειλές στον κυβερνοχώρο.

Οι κύριες λειτουργίες ενός συστήματος ασφαλείας EDR είναι:

- Παρακολούθηση και συλλογή δεδομένων δραστηριότητας από endpoints που θα μπορούσαν να υποδηλώνουν απειλή.
- Ανάλυση αυτών των δεδομένων για να εντοπιστούν μοτίβα απειλών.
- Αυτόματη απάντηση σε εντοπισμένες απειλές για την αφαίρεση ή τον περιορισμό τους και ειδοποίηση προσωπικού ασφαλείας.
- Εγκληματολογία και εργαλεία ανάλυσης για την έρευνα των εντοπισμένων απειλών και αναζήτηση ύποπτων δραστηριοτήτων.

[11] Hutchins, E.M., Cloppert, M.J., Amin, R.M. “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead. Issues” Inf. Warf. Secur. Res. 2011.

Οι βασικές δυνατότητες των EDR είναι:

Detection

Η ανίχνευση απειλών είναι μια θεμελιώδης ικανότητα των EDR. Το θέμα δεν είναι αν θα «επιτεθεί» μια προηγμένη απειλή, το θέμα είναι το πότε. Κατά την είσοδο στο περιβάλλον λειτουργίας, πρέπει να είμαστε σε θέση να ανιχνεύουμε με ακρίβεια την απειλή, ώστε να μπορούμε να την περιορίσουμε, να την αξιολογήσουμε και να την εξουδετερώσουμε. Αυτό δεν είναι εύκολη υπόθεση όταν αντιμετωπίζουμε εξελιγμένο κακόβουλο λογισμικό που μπορεί να είναι εξαιρετικά κρυφό και ικανό να μεταμορφωθεί από μια καλοήθη σε μια κακόβουλη κατάσταση αφού περάσει το σημείο εισόδου.

Με τη συνεχή ανάλυση αρχείων, το EDR μπορεί να επισημαίνει τα μολυσμένα αρχεία με την πρώτη ένδειξη κακόβουλης συμπεριφοράς. Εάν ένα αρχείο θεωρείται αρχικά ασφαλές, αλλά μετά από μερικές εβδομάδες αρχίσει να εμφανίζει δραστηριότητα ransomware, το EDR θα εντοπίσει το αρχείο και θα ξεκινήσει τη διαδικασία αξιολόγησης και ανάλυσης, ενώ θα ειδοποιήσει τον οργανισμό να ενεργήσει.

Containment

Μετά τον εντοπισμό ενός κακόβουλου αρχείου, το EDR πρέπει να μπορεί να περιορίσει την απειλή. Τα κακόβουλα αρχεία στοχεύουν να μολύνουν όσο το δυνατόν περισσότερες διεργασίες, εφαρμογές και χρήστες. Η τμηματοποίηση μπορεί να είναι μια εξαιρετική άμυνα στο data center για να αποφύγουμε την πλευρική μετακίνηση (lateral movement) προηγμένων απειλών. Ενώ η τμηματοποίηση είναι χρήσιμη, ένα ισχυρό EDR μπορεί να βοηθήσει να περιοριστεί ένα κακόβουλο αρχείο πριν ελέγξουμε τις άκρες των τμηματοποιημένων περιοχών του δικτύου. Το Ransomware είναι ένα τεράστιο παράδειγμα του γιατί πρέπει να περιορίζονται οι απειλές. Το ransomware μπορεί να είναι δύσκολο να αφαιρεθεί και από την στιγμή που έχει κρυπτογραφήσει τα δεδομένα, το εργαλείο EDR μπορεί να περιορίσει πλήρως το ransomware για να μετριάσει την βλάβη. Ως πρόσθετο στοιχείο, η ασφάλεια EDR παρέχει τη δυνατότητα απομόνωσης παραβιασμένων endpoints, αποτρέποντας περαιτέρω κρυπτογράφηση μέσω του δικτύου.

Investigation

Μόλις εντοπιστεί και περιοριστεί το κακόβουλο αρχείο, το EDR θα πρέπει να διερευνήσει το περιστατικό. Εάν το αρχείο πέρασε κρυφά στην περίμετρο με την πρώτη προσπάθεια, υπάρχει μια ευπάθεια. Είναι πιθανό η ομάδα πληροφοριών απειλών να μην έχει ξαναδεί τέτοιου είδους προηγμένη απειλή. Ίσως μια συσκευή ή μια εφαρμογή να είναι ξεπερασμένη και να πρέπει να ενημερωθεί. Χωρίς τις κατάλληλες δυνατότητες διερεύνησης,

δεν θα αποκτηθεί εικόνα για το πώς πέρασε μια απειλή το δίκτυο. Ως αποτέλεσμα, το δίκτυο είναι πιθανό να αντιμετωπίσει ξανά τις ίδιες απειλές και προβλήματα. Το EDR παρέχει ανά περιστατικό το είδος της ανάλυσης που απαιτείται για την αποκάλυψη αυτών των ζητημάτων και την αποτροπή μελλοντικής εκμετάλλευσης μέσω του ίδιου φορέα απειλής.

Στη διαδικασία έρευνας, το sandboxing είναι μια άλλη κρίσιμη ικανότητα. Το Sandboxing μπορεί να χρησιμοποιηθεί στην περίμετρο, για να βοηθήσει στην παραχώρηση ή άρνηση πρόσβασης, αλλά μπορεί επίσης να χρησιμοποιηθεί αποτελεσματικά μετά το σημείο εισόδου. Sandboxing είναι όταν το αρχείο απομονώνεται σε ένα προσομοιωμένο περιβάλλον και δοκιμάζεται και παρακολουθείται. Το EDR μπορεί να παρέχει sandboxing.

Μέσα σε αυτό το προσομοιωμένο, απομονωμένο περιβάλλον, το EDR θα προσπαθήσει να προσδιορίσει τη φύση του αρχείου χωρίς να διακινδυνεύει ενδεχομένως την ασφάλεια του ευρύτερου περιβάλλοντος. Σε αυτή τη διαδικασία, το EDR μπορεί να κατανοήσει τα χαρακτηριστικά και τη φύση αυτού του κακόβουλου αρχείου, στη συνέχεια να μάθει από αυτό και να προσαρμοστεί για καλύτερη άμυνα έναντι μελλοντικών απειλών.

Elimination

Το πιο προφανές στοιχείο ενός EDR πρέπει να είναι η ικανότητά του να εξαλείφει την απειλή. Ο εντοπισμός, ο περιορισμός και η διερεύνηση μιας απειλής είναι μια καλή αρχή, αλλά αν δεν μπορούμε να την εξαλείψουμε, τότε απλώς συνεχίζουμε να γνωρίζουμε ότι το σύστημά μας έχει παραβιαστεί. Για να εξαλειφθούν σωστά οι απειλές, το EDR χρειάζεται να απαντήσει σε ερωτήσεις όπως:

- Από πού ξεκίνησε το αρχείο;
- Με ποια διαφορετικά δεδομένα και εφαρμογές αλληλεπίδρασε αυτό το αρχείο;
- Έχει γίνει αναπαραγωγή του αρχείου;

Το να μπορεί να δεί ολόκληρο το χρονοδιάγραμμα ενός αρχείου είναι το κλειδί. Δεν είναι τόσο εύκολο όσο απλά να αφαιρέσουμε το αρχείο που έχουμε παρατηρήσει. Όταν καταργείται το αρχείο, πιθανόν να χρειαστεί να διορθωθούν αυτόματα πολλά μέρη του δικτύου. Για αυτόν τον λόγο, ένα EDR θα πρέπει να παρέχει δεδομένα με δυνατότητα ενέργειας σχετικά με τη διάρκεια ζωής του αρχείου. Εάν ένα εργαλείο EDR έχει αναδρομικές δυνατότητες, αυτά τα δεδομένα με δυνατότητα ενέργειας θα πρέπει να χρησιμοποιηθούν για την αυτόματη αποκατάσταση των συστημάτων στην κατάστασή τους πριν από τη μόλυνση.

2-6. TIP

Η threat intelligence είναι πληροφορίες που βασίζονται σε στοιχεία ή γνώση του πλαισίου, των μηχανισμών, των ενδείξεων και των επιπτώσεων υφιστάμενων ή αναδυόμενων απειλών.[12] Οι ροές πληροφοριών απειλών είναι ροές δεδομένων που μοιράζονται πληροφορίες σχετικά με τις συλλεγμένες απειλές, επιτρέποντας στους οργανισμούς να χρησιμοποιούν κοινή γνώση για την ασφάλειά τους. Συχνά αυτές οι ροές είναι δωρεάν και χρησιμοποιούν μια συλλογή πληροφοριών ανοιχτού κώδικα, αλλά υπάρχουν επίσης ροές επί πληρωμή που συνδυάζουν ανοιχτές και κλειστές πηγές πληροφοριών. Μια ροή πληροφοριών απειλών μπορεί επίσης να προέρχεται από δεδομένα που συλλέγονται και αναλύονται εσωτερικά μέσα σε έναν οργανισμό.

Οι πλατφόρμες πληροφοριών απειλών (Threat Intelligence Platform – TIP) συνδυάζουν πολλαπλές πηγές πληροφοριών για τις απειλές για να θέσουν σε χρήση σχετικές πληροφορίες, ενισχύοντας τα SIEM, τα endpoints, τα τείχη προστασίας και άλλα συστήματα ασφαλείας με ενημερωμένη threat intelligence. [13]

2-7. Ανάγκη για αυτοματοποίηση

Καθημερινά, οι αναλυτές ασφαλείας πρέπει να λαμβάνουν γρήγορα αποφάσεις για τον εντοπισμό ειδοποιήσεων που είναι πραγματικές απειλές έναντι false positives. Αν και οι αναλυτές λαμβάνουν σημαντικές αποφάσεις πολλές φορές την ημέρα, δεν είναι πάντα σε θέση να ολοκληρώσουν τις έρευνες απειλών. Πολλοί αναλυτές απλώς κατακλύζονται από τον τεράστιο αριθμό ειδοποιήσεων. Περισσότερο από το 50% των οργανισμών λαμβάνει 5.000 ειδοποιήσεις την ημέρα και το 17% έχει 100.000 την ημέρα.[14] Τα προβλήματα επιδεινώνονται από τον εκτεταμένο αριθμό τεχνολογιών που χρησιμοποιούνται για την αντιμετώπιση των απειλών στον κυβερνοχώρο. Η χρήση ενός SIEM σε σύγχρονα SOC, παρόλο που θεωρείται αξιόπιστο μέτρο μετριασμού, έχει γίνει προβληματική. Η δυσκολία ενσωμάτωσης νέων λύσεων παρακολούθησης σε υπάρχουσες τεχνολογίες SIEM προκειμένου να καταστούν αποτελεσματικές είναι ένας από τους λόγους πίσω από το ζήτημα. Ένας αναλυτής πρέπει να έχει την απαιτούμενη εμπειρία και επάρκεια γνώσεων για να πραγματοποιήσει

[12] Gartner Research. “Definition: Threat Intelligence”. Stamford, USA: Gartner Research, 2013 https://www.gartner.com/en/documents/2487216/definition-threat-intelligence , Accessed on: February 4, 2023
[13] Palo Alto Networks. “What is a Threat Intelligence Platform.” Santa Clara, USA: Palo Alto Networks, 2021 https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform , Accessed on: February 4, 2023
[14] “Securing What’s Now and What’s Next: 20 Cybersecurity Considerations for 2020,” Cisco, 2020 https://ebooks.cisco.com/story/2020-ciso-benchmark/page/4/13 , Accessed on: February 9, 2023

αποτελεσματική αναγνώριση των false positive στοιχείων, κάτι που γίνεται ακόμη πιο δύσκολο με τον υπάρχοντα όγκο ειδοποιήσεων.

Μια λύση που έχει προταθεί και χρησιμοποιηθεί σε πολλές περιπτώσεις είναι αυτή του αυτοματισμού. Χρησιμοποιώντας την αυτοματοποίηση σε έρευνες ασφαλείας και προτείνοντας μέτρα μετριασμού που βασίζονται στην αυτοματοποίηση των διαδικασιών, μπορεί να μειωθεί δραστικά ο χρόνος απόκρισης από τους αναλυτές, καθιστώντας τους πιο αποτελεσματικούς. Το όνομα του λογισμικού που έχει εισαχθεί για το σκοπό αυτό είναι S.O.A.R. (Security Orchestration Automation and Response).

3. Ιστορική Αναδρομή / Άλλες Έρευνες

Καθώς ο αριθμός και η πολυπλοκότητα των κυβερνοεπιθέσεων συνέχισαν να αυξάνονται με την πάροδο των ετών, ορισμένοι προμηθευτές συνειδητοποίησαν ότι οι παραδοσιακές προσεγγίσεις και τα εργαλεία της κυβερνοασφάλειας επίσης απέτυχαν να συμβαδίσουν. Πριν από είκοσι πέντε χρόνια, ένα μόνο τείχος προστασίας μπορεί να ήταν αρκετό για την προστασία ευαίσθητων πόρων εντός του εταιρικού δικτύου, αλλά αυτό δεν ισχύει πλέον. Πολλοί οργανισμοί που συνειδητοποιούν την ασφάλεια μπορούν να βρουν τους εαυτούς τους να διαχειρίζονται περισσότερα από 50 διαφορετικά και ασύνδετα εργαλεία ασφαλείας.

Μόλις πριν από μια δεκαετία, τα προϊόντα Security Information and Event Management (SIEM) θεωρούνταν ως η απόλυτη λύση για τη διαχείριση λειτουργιών ασφαλείας. Σε πολλούς οργανισμούς, εξακολουθούν να αποτελούν τα θεμέλια των σύγχρονων SOCs. Ωστόσο, η ορατότητα πιθανών γεγονότων ασφαλείας από μόνη της δεν βοηθά τους αναλυτές να αξιολογήσουν κάθε απειλή που ανακαλύφθηκε, ούτε μειώνει τον χρόνο που αφιερώνεται σε επαναλαμβανόμενες χειροκίνητες εργασίες που αποτελούν μια διαδικασία απόκρισης περιστατικού.

Τα SIEM πρώτης γενιάς παρείχαν αξία, αλλά πολλοί πρώτοι χρήστες του SIEM αναφέρουν ότι ο όγκος των false alarms προκάλεσε προβλήματα στην προσπάθεια να ξεχωρίσουν τι αξίζει προσοχής και παρακολούθησης και τι όχι. Τα SIEM δεύτερης γενιάς συνήθως ενσωματώνουν μοντέλα ανίχνευσης μηχανικής μάθησης (ML) ως μέσο για τη μείωση των false alarms στοιχείων και την παροχή περισσότερης ευφυΐας με δυνατότητα δράσης σε αναλυτές και διαχειριστές.

Παράλληλα με αυτές τις νεότερες λύσεις SIEM, έχει εμφανιστεί μια κατηγορία πλατφορμών απόκρισης συμβάντων που επικεντρώνονται στη δημιουργία πιο βελτιστοποιημένων και αυτοματοποιημένων ροών εργασιών για την αντιμετώπιση συμβάντων ασφαλείας.

Τα προϊόντα SOAR είναι η πιο πρόσφατη επανάληψη αυτής της εξέλιξης. Καθοδηγούμενοι από την αυξανόμενη ζήτηση για εφαρμογή κεντρικού, αυτοματοποιημένου ελέγχου επί της ανάλυσης συμβάντων και των ροών εργασιών απόκρισης σε διαφορετικές λύσεις ασφάλειας, οι προμηθευτές επεκτείνουν τις υπάρχουσες πλατφόρμες πληροφοριών ασφαλείας, ενορχήστρωσης ασφαλείας ή απόκρισης συμβάντων για να συνδυάσουν τις βασικές δυνατότητες και στα τρία αυτά τμήματα της αγοράς. Συμπληρώνοντας ή ενοποιώντας

άμεσα με τα SIEM, οι πλατφόρμες SOAR στοχεύουν να γίνουν το θεμέλιο των σύγχρονων Κέντρων Επιχειρήσεων Ασφαλείας (SOC).

Αρχικά, το 2015, ο Gartner προσδιόρισε τη Διαχείριση απειλών και ευπάθειας, την απόκριση συμβάντων ασφαλείας και τον αυτοματισμό λειτουργιών ασφαλείας ως τρεις βασικές δυνατότητες της τεχνολογίας SOAR. Ο όρος security orchestration εισήχθη για πρώτη φορά από τον Gartner το 2017 για να περιγράψει τις λειτουργίες που εκτελούνται από το πρόσφατα αναπτυγμένο λογισμικό για την αντιμετώπιση περιστατικών, την αυτοματοποίηση ασφαλείας, τη διαχείριση υποθέσεων και επίσης άλλες ενοποιήσεις. Ο Gartner όρισε το S.O.A.R. ως τεχνολογίες που επιτρέπουν στους οργανισμούς να συλλέγουν δεδομένα από διάφορες πηγές, όπου μπορεί να εκτελεστεί ανάλυση και διαλογή συμβάντων, προκειμένου να αξιοποιηθεί ο συνδυασμός ανθρώπου-μηχανής, προκειμένου να βοηθήσει στον καθορισμό, την ιεράρχηση και την προώθηση τυποποιημένων δραστηριοτήτων απόκρισης περιστατικών.[15]

Το 2022, ο Gartner ενημέρωσε περαιτέρω τον ορισμό της ασφάλειας SOAR και τον ορίζει ως λύσεις που συνδυάζουν την απόκριση περιστατικών, την ενορχήστρωση και την αυτοματοποίηση και τις δυνατότητες διαχείρισης πλατφόρμας πληροφοριών απειλών σε μια ενιαία πλατφόρμα. Σύμφωνα με τον Οδηγό Αγοράς 2022 του Gartner για Λύσεις SOAR, οι σύγχρονες επιχειρήσεις αξιοποιούν τα εργαλεία SOAR για να τεκμηριώσουν και να εφαρμόσουν διαδικασίες ασφαλείας, να υποστηρίξουν τη διαχείριση συμβάντων ασφαλείας, να παρέχουν βοήθεια στις ομάδες ασφαλείας και να λειτουργήσουν καλύτερα το threat intelligence.

Ο επόμενος που αναφέρθηκε στην εξέλιξη της S.O.A.R. πλατφόρμας ήταν ο Jon Oltsik, αναφέροντας την ταχεία υιοθέτηση των S.O.A.R. λύσεων από πολλούς προμηθευτές συστημάτων ασφάλειας τα τελευταία χρόνια. [16] Η ανάλυσή του παρείχε το νέο πλαίσιο σχετικά με τις λειτουργίες ασφάλειας, ένα πλαίσιο που παραμένει ακόμη και σήμερα. Περιέγραψε πώς οι λειτουργίες ασφαλείας μεταπήδησαν από ένα SIEM σύστημα και γενικά, μια πιο λογισμική προσέγγιση, σε μια προσέγγιση με κέντρο τον αναλυτή.[17] Παρόλο που πολλοί έχουν υποστηρίξει ότι οι S.O.A.R. τεχνολογίες θα οδηγήσουν στην αυτοματοποίηση των εργασιών του επιπέδου 1 σε ένα SOC, οδηγώντας τελικά στην απασχόληση λιγότερων αναλυτών, ο

[15] Gartner, “Security Orchestration, Automation and Response (SOAR)”, 2017 https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar , Accessed on: February 9, 2023

[16] Jon Oltsik, “The evolution of security operations, automation and orchestration”, CSO, 2018, https://www.csoonline.com/article/3270957/the-evolution-of-security-operations-automation-and-orchestration.html , Accessed on: February 9, 2023

[17] Jon Oltsik, “The rise of analyst-centric security operations technologies”, CSO, 2018 https://www.csoonline.com/article/3276463/the-rise-of-analyst-centric-security-operations-technologies.html , Accessed on: February 9, 2023

Oltsik υποστηρίζει ότι οι S.O.A.R. τεχνολογίες θα ενδυναμώσουν και θα εξελίξουν τους αναλυτές επιπέδου 1, προσφέροντας νέα όπλα για την αντιμετώπιση των εξελισσόμενων απειλών. Μερικά από αυτά τα όπλα περιλαμβάνουν noise cancelling assistance που παρέχει λύση κλιμάκωσης και ενεργεί ως proxy για τον αναλυτή, ενοποιημένα δεδομένα που μπορούν να προβληθούν μόνο από μία κονσόλα, μοντέλα και ρουτίνες με εξαιρετικά προσαρμόσιμα πρότυπα και επίσης συνεχή εκμάθηση που με την πάροδο του χρόνου θα μπορεί να αναγνωρίζει τα μοτίβα μιας επίθεσης και να προτείνει εργασίες και διαδικασίες που ήταν πιο αποτελεσματικές στο παρελθόν. Ως αποτέλεσμα, μια S.O.A.R. πλατφόρμα μπορεί να γίνει πιο προσιτή και φιλική σε άπειρους αναλυτές και μπορεί να βοηθήσει στην ανάπτυξη των ικανοτήτων έμπειρων αναλυτών.

4. S.O.A.R.

4-1. Περιγραφή τεχνολογίας SOAR

Οι υπάρχουσες λύσεις ασφάλειας έχουν σχεδιαστεί για την παρακολούθηση των υποδομών πληροφορικής και των δραστηριοτήτων δικτύου ενός οργανισμού, τη δημιουργία ειδοποιήσεων ασφαλείας και την εκτέλεση των απαραίτητων ενεργειών κατά τον εντοπισμό απειλών ασφαλείας. Οι λύσεις κυβερνοασφάλειας ενός οργανισμού παράγουν χιλιάδες ειδοποιήσεις, οι οποίες συνήθως παρακολουθούνται και επεξεργάζονται από το προσωπικό ασφαλείας, κυρίως χρησιμοποιώντας μη αυτόματες ή ημιαυτόματες διαδικασίες και πρακτικές. Μια αναφορά της Verizon δείχνει ότι το 93% των περιπτώσεων παραβίασης δεδομένων απαιτούν λίγα λεπτά για να εκτελεστούν, αλλά χρειάστηκαν εβδομάδες ή μήνες οι εταιρείες για να ανακαλύψουν τις επιθέσεις.[18] Για παράδειγμα, αφού λάβει ειδοποιήσεις από το IDS για κακόβουλες συμπεριφορές, ένας εμπειρογνώμονας ασφαλείας μπορεί να μεταβεί σε ένα τερματικό αμυντικό σύστημα για να συγκεντρώσει περισσότερες σχετικές πληροφορίες αναζητώντας πόρους δικτύου και επιβεβαιώνοντας την απειλή. Αφού επιβεβαιώσει την απειλή, ένας εμπειρογνώμονας ασφαλείας δίνει εντολή σε ένα firewall να απομονώσει ή να αποκλείσει την κυκλοφορία από την πληγείσα περιοχή και να ενημερώσει τις πληροφορίες απειλής στη threat intelligence. Σύμφωνα με την BakerHostetler[19], οι ειδικοί ασφαλείας χρειάστηκαν κατά μέσο όρο 61 ημέρες για να ανακαλύψουν την εμφάνιση ενός περιστατικού και μετά τις ανακαλύψεις 41 ακόμη ημέρες για να λάβουν διορθωτικά μέτρα.

Μια λύση SOAR έχει τη δυνατότητα να αντιμετωπίσει τις δυσχέρειες της χειροκίνητης ανάλυσης απειλών, τις καθυστερήσεις στις αποκρίσεις σε συμβάντα ασφαλείας καθώς και να παρέχει ασφάλεια στις ICT υποδομές ενός οργανισμού. Οι λύσεις SOAR είναι σε θέση να εντοπίζουν αυτόματα ύποπτες δραστηριότητες σε ένα περιβάλλον ενός οργανισμού και να ενεργούν προληπτικά για τον μετριασμό μιας κυβερνοεπίθεσης.

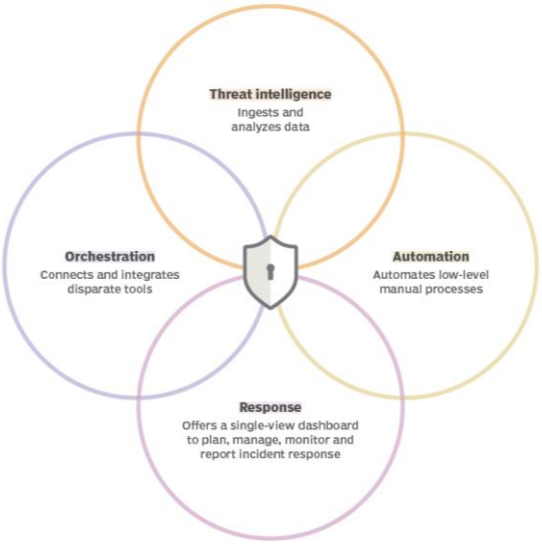
Το SOAR σημαίνει Security Orchestration, Automation και Response. Ο Gartner ορίζει το SOAR ως «τεχνολογίες που επιτρέπουν στους οργανισμούς να συλλέγουν εισόδους που παρακολουθούνται από την ομάδα λειτουργιών ασφαλείας. Τα εργαλεία SOAR επιτρέπουν σε έναν οργανισμό να ορίζει διαδικασίες ανάλυσης περιστατικών και απόκρισης (incident response playbooks) σε μορφή ψηφιακής ροής εργασιών (workflow)». Με άλλα λόγια, το

[18] Verizon "2016 Data Breach Investigations Report", 2016 http://www.verizonenterprise.com/verizon-insights-lab/dbir/ , Accessed on: February 13, 2023.

[19] BakerHosteller, "Be Compromise Ready: Go Back to the Basics - 2017 Data Security Incident Response Report", 2017, https://www.bakerlaw.com/events/webinar-be-compromise-ready-go-back-to-the-basics , Accessed on: February 13, 2023.

SOAR αναφέρεται σε μια τεχνολογία ασφαλείας που επιτρέπει την αυτοματοποιημένη συσσώρευση και ροή δεδομένων απειλών ασφαλείας μεταξύ διαφορετικών τεχνολογιών ασφαλείας (όπως SIEM, threat intelligence platform, firewall, incident response platform κ.λπ.) που αναπτύσσονται σε διαφορετικά περιβάλλοντα (cloud και εσωτερική εγκατάσταση) και διευκολύνει τις αυτοματοποιημένες απαντήσεις σε απειλές ασφαλείας. Ο στόχος του SOAR είναι να βελτιστοποιήσει τις λειτουργίες ασφάλειας.

Οι πλατφόρμες SOAR συγκεντρώνουν εργαλεία, συστήματα, ανθρώπους και διαδικασίες σε ένα μέρος για να επιτρέψουν στις ομάδες ασφαλείας να αυτοματοποιήσουν τις ροές εργασιών ασφαλείας. Με άλλα λόγια, οι λύσεις SOAR επιτρέπουν στους οργανισμούς να εντοπίζουν τα προβλήματα, να περιγράφουν τις λύσεις και να αυτοματοποιούν την απόκριση.



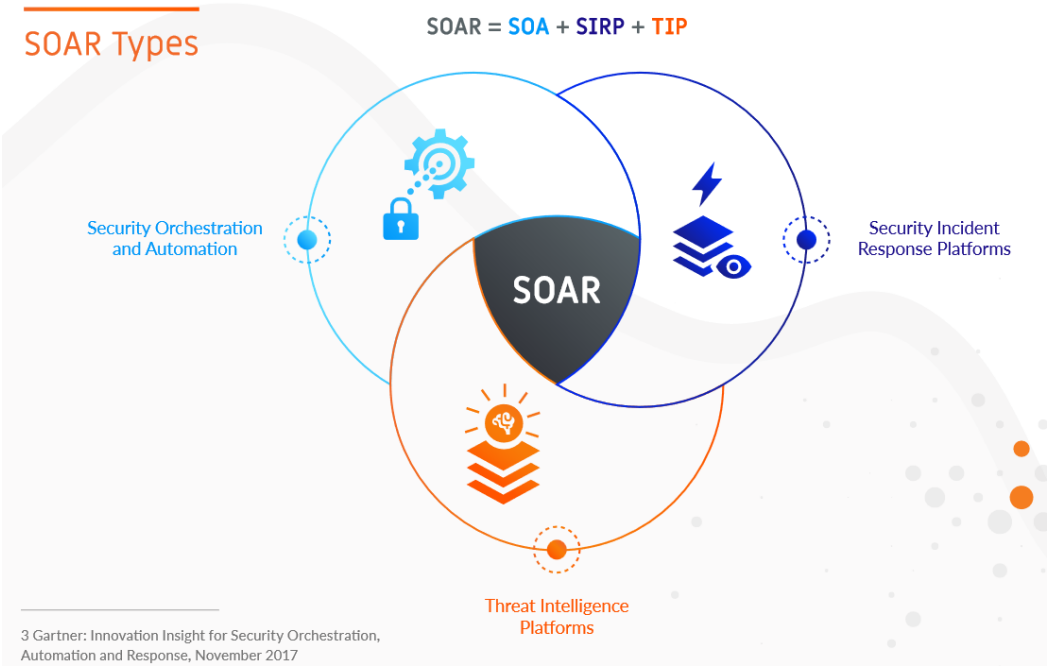
Εικόνα 2. Τα στοιχεία της τεχνολογίας SOAR.[20]

Μια ολοκληρωμένη λύση SOAR θα αποτελείται από τρεις ενοποιημένες λειτουργίες:

- Security Orchestration and Automation (SOA) - παρέχει δυνατότητες αυτοματοποίησης και ενορχήστρωσης ροών εργασιών σε πολλά εργαλεία, συστήματα και εφαρμογές
- Security Incident Response Platform (SIRP) - παρέχει δυνατότητες για διαχείριση περιστατικών και υποθέσεων, συμπεριλαμβανομένης της διαλογής και της απόκρισης.
- Threat Intelligence Platform (TIP) - παρέχει δυνατότητες απόκτησης πληροφοριών για τους επιτιθέμενους σχετικά με τους γνωστούς δείκτες συμβιβασμού (indicators of

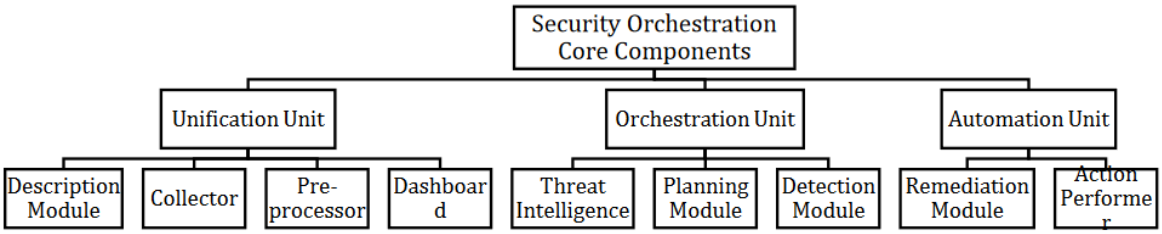
[20] Sharon Shea, "SOAR (security orchestration, automation and response)", 2021 https://www.techtarget.com/searchsecurity/definition/SOAR , Accessed on: February 13, 2023.

compromise – IOC) και τις τακτικές, τις τεχνικές και τις διαδικασίες (tactics, techniques, and procedures – TTP) μέσω της πρόσληψης, ανάλυσης και διάδοσης δεδομένων απειλών και πληροφοριών.



Εικόνα 3. Λειτουργίες τεχνολογίας SOAR

Υπάρχουν διαφορετικές κατηγοριοποιήσεις των βασικών στοιχείων μιας πλατφόρμας SOAR, οι περισσότερες από τις οποίες προτείνουν έναν συνδυασμό των ανωτέρω. Άλλη μια κατηγοριοποίηση που γίνεται είναι αυτή της πρώτης λειτουργίας Security Orchestration and Automation (SOA), η οποία θα μπορούσε να χωριστεί σε τρία βασικά στοιχεία, unification, orchestration και automation.



Εικόνα 4. Κατηγοριοποίηση των βασικών στοιχείων μιας SOA πλατφόρμας.

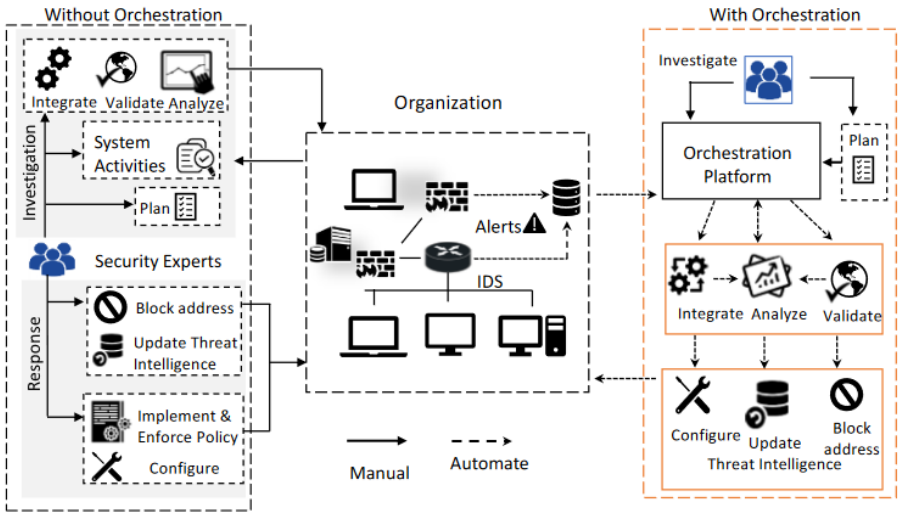
4-1-1. Orchestration

Ενώ οι διαφορετικές λύσεις ασφαλείας αποτελούν μεγάλο «οπλοστάσιο» για το SOC, κάθε μία από τις λύσεις χρησιμοποιεί διαφορετικές τεχνολογίες και πρότυπα για την ανάπτυξη

και τη λειτουργία. Αυτές οι διαφορές δυσκολεύουν το SOC να ενοποιήσει και να λειτουργήσει σε συνδυασμό όλα τα εργαλεία. Η ενορχήστρωση ασφαλείας χρησιμοποιείται όταν οι λύσεις εργαλείων ασφάλειας διαφορετικών προμηθευτών συγχωνεύονται για να υποστηρίξουν το SOC.

Η εργασία των αναλυτών ασφαλείας γίνεται πολύ πιο αποτελεσματική όταν οι δραστηριότητες μπορούν να συγχωνευθούν από διαφορετικές λύσεις ασφάλειας. Αυτές οι συνδυασμένες δραστηριότητες παρουσιάζονται σε μια ενιαία κονσόλα ή πλατφόρμα. Με την ενορχήστρωση, τα δεδομένα πληροφοριών απειλών συλλέγονται από πολλαπλές πηγές σε μια μοναδική βάση δεδομένων. Το πλαίσιο μπορεί να προσφέρει πληροφορίες για τους αναλυτές ασφαλείας που καθιστούν πολύ ευκολότερη και ταχύτερη την αντίδραση στις απειλές. Όταν εμφανίζεται μια ειδοποίηση, ο αναλυτής πρέπει να συλλέγει δεδομένα χειροκίνητα μέσω πολύπλοκων διαδικασιών, να ερευνά και να σχεδιάζει την αντιμετώπιση.

Στην εικόνα 4 φαίνονται ορισμένες από τις ρυθμίσεις ενός οργανισμού όπου διάφοροι τύποι λύσεων ασφαλείας δημιουργούν ειδοποιήσεις που πρέπει να αναλυθούν χειροκίνητα από το προσωπικό ασφαλείας απουσία πλατφόρμας SOAR που μπορεί να αυτοματοποιήσει το μεγαλύτερο μέρος της διαδικασίας μη αυτόματης λήψης αποφάσεων έναντι ενός περιστατικού απειλής. Η πλατφόρμα SOAR ενοποιεί εργαλεία ασφαλείας για να επιταχύνει την απόκριση περιστατικού μειώνοντας τις μη αυτόματες και επαναλαμβανόμενες δραστηριότητες. Η ενορχήστρωση και η αυτοματοποίηση των δραστηριοτήτων των λύσεων ασφαλείας από πολλούς διαφορετικούς προμηθευτές απαιτούν μια ολοκληρωμένη εικόνα της πλατφόρμας ενορχήστρωσης, καθώς αυτές οι λύσεις έχουν τον δικό τους τρόπο λειτουργίας και παράγουν διαφορετικές μορφές ειδοποιήσεων. Δεδομένης της αυξανόμενης ζήτησης για ενορχήστρωση ασφαλείας, απαιτείται σημαντικός όγκος έρευνας για να βοηθήσει στην κατανόηση των προκλήσεων στην ενορχήστρωση ασφαλείας, των υπαρχουσών λύσεων και πρακτικών για την αντιμετώπιση των προκλήσεων.



Εικόνα 5. Επισκόπηση των διαδικασιών ασφαλείας ενός οργανισμού έναντι μιας ειδοποίησης απειλής χωρίς και με orchestration.

4-1-2. Automation

Μοναδικός σκοπός του αυτοματισμού ασφαλείας είναι η εκτέλεση εργασιών που σχετίζονται με την ασφάλεια χωρίς καμία ανθρώπινη αλληλεπίδραση. Ο αυτοματισμός μπορεί να εφαρμοστεί και στις δύο πλευρές της ασφάλειας του υπολογιστή. Οι Blue Teams μπορούν να αξιοποιήσουν την αυτοματοποίηση για την πρόληψη, τον εντοπισμό και την αποκατάσταση απειλών. Από την άλλη πλευρά, οι Red Teams μπορούν να εφαρμόσουν αυτοματοποίηση σε αξιολογήσεις ευπάθειας και να εκτελέσουν διαφορετικούς τύπους επίθεσης. Το βασικό πλεονέκτημα των αυτοματισμών ασφαλείας είναι η απελευθέρωση των αναλυτών ασφαλείας από χρονοβόρες εργασίες, ώστε να γίνουν πολύ πιο αποτελεσματικοί στην εργασία τους και να μπορούν να επικεντρωθούν σε πιο ενδιαφέρουσες εργασίες.

Διαφορά orchestration - automation

Η κατανόηση των ροών εργασίας SOAR θα πρέπει να παραμένει πάντα προτεραιότητα για τις ομάδες ασφαλείας που θέλουν να ενορχηστρώσουν και να αυτοματοποιήσουν τις διαδικασίες ασφαλείας τους. Συχνά οι όροι ενορχήστρωση ασφαλείας και αυτοματισμός χρησιμοποιούνται εναλλακτικά στο τοπίο της κυβερνοασφάλειας. Ωστόσο, είναι επιτακτική ανάγκη να κατανοήσουμε ότι και οι δύο όροι έχουν διαφορετικές έννοιες και στόχους. Όταν εμφανίστηκε η αυτοματοποίηση, αποτέλεσε ένα σημαντικό πλεονέκτημα για τις ομάδες ασφαλείας που είχαν κουραστεί από τις κοινότυπες, χρονοβόρες και χαμηλού επιπέδου εργασίες. Μετά από αυτό, η ενορχήστρωση ήρθε στο προσκήνιο, ενισχύοντας τη διαχείριση

χρόνου και πόρων για τις ομάδες ασφαλείας, βοηθώντας τις να ανταποκρίνονται ταχύτερα σε περιστατικά και δίνοντας προτεραιότητα σε σημαντικές εργασίες.

Ο αυτοματισμός ασφαλείας είναι ο αυτόματος χειρισμός εργασιών σε συστήματα κυβερνοασφάλειας χωρίς την ανάγκη ανθρώπινης παρέμβασης. Αντίθετα, η ενορχήστρωση ασφαλείας αναφέρεται στην χρησιμοποίηση πολλών εργασιών αυτοματισμού σε διαφορετικές πλατφόρμες. Οι εργασίες αυτοματισμού αποτελούν μέρος της συνολικής διαδικασίας ενορχήστρωσης, η οποία περιλαμβάνει πιο πολύπλοκα σχήματα και εργασίες. Με λίγα λόγια, η ενορχήστρωση δεν είναι παρά ο αυτοματοποιημένος συντονισμός και διαχείριση διαφορετικών συστημάτων, υπηρεσιών και ενδιάμεσων λογισμικών. Η ενορχήστρωση ασφαλείας χρησιμοποιεί αρκετές αυτοματοποιημένες αλλά και ημι-αυτόματες ενέργειες για την υλοποίηση μιας πολύπλοκης διαδικασίας, η οποία μπορεί να περιλαμβάνει πολλαπλές αυτοματοποιημένες εργασίες ή συστήματα. Επικεντρώνεται στη βελτιστοποίηση επαναλαμβανόμενων διαδικασιών και διασφαλίζει την ακριβή εκτέλεση των εργασιών.

Ο αυτοματισμός και η ενορχήστρωση μπορούν να κατανοηθούν καλύτερα με τη διάκριση μεταξύ μιας μεμονωμένης λειτουργίας και μιας πλήρους διαδικασίας. Ενώ η αυτοματοποίηση χειρίζεται μόνο μία εργασία, η ενορχήστρωση χρησιμοποιεί ένα σύνθετο σύνολο εργασιών καθώς και διεργασιών. Ο αυτοματισμός επιτρέπει στις ομάδες ασφαλείας να εκτελούν ομαλά χρονοβόρες εργασίες χωρίς ανθρώπινη παρέμβαση, δίνοντάς τους τη δυνατότητα να υιοθετήσουν μια πιο προληπτική προσέγγιση απέναντι σε πιθανές απειλές. Ο στόχος της ενορχήστρωσης είναι να βελτιστοποιήσει μια διαδικασία.

Η ενορχήστρωση ασφαλείας αποτελεί προϋπόθεση για την αυτοματοποίηση ασφαλείας, η οποία είναι η διαδικασία αυτόματης ανίχνευσης, πρόληψης και ανάκτησης από επιθέσεις στον κυβερνοχώρο χωρίς ανθρώπινη παρέμβαση χρησιμοποιώντας τεχνολογία πληροφοριών, αλγόριθμο αυτοματισμού και τεχνητή νοημοσύνη.[21]

4-1-3. Response

Όταν έχει συμβεί ένα συμβάν ασφαλείας, εφαρμόζεται η λειτουργία Response προκειμένου να βοηθηθούν οι αναλυτές ασφαλείας να διαχειρίζονται, να συνεργάζονται και να μοιράζονται δεδομένα. Το SOAR εκτελεί διαλογή και επεξεργασία των alarm συλλέγοντας δεδομένα που σχετίζονται με την πιθανή απειλή. Ο ρόλος του αναλυτή ασφαλείας είναι να εκτελεί ανάλυση με βάση τα δεδομένα. Εάν επαληθευτεί μια απειλή, διενεργείται βαθύτερη

[21] J. TRULL, “Top 5 best practices to automate security operations”, 2017, https://cloudblogs.microsoft.com/microsoftsecure/2017/08/03/top-5-best-practices-to-automate-security-operations/ , Accessed on: February 13, 2023.

ανάλυση σε περίπτωση άλλων πιθανών απειλών, ώστε να μπορούν να σταματήσουν περαιτέρω επιθέσεις. Το περιστατικό ασφαλείας επιλύεται μετά την εκτέλεση της διαδικασίας αποκατάστασης. Διαφορετικές μονάδες χρησιμοποιούνται με τα συμβάντα ασφαλείας, έτσι ώστε η επικοινωνία και η διαχείριση εργασιών να μπορούν να γίνουν εντός ή εκτός του SOC. Τα δεδομένα που σχετίζονται με το περιστατικό ασφαλείας μπορούν να συλλεχθούν και να υποβληθούν σε επεξεργασία για πληροφορίες απειλών, ώστε να μπορούν να εφαρμοστούν προληπτικά μέτρα στο μέλλον.

4-1-4. Playbooks

Η χρήση ενός playbook (μερικές φορές αναφέρεται ως runbook) βοηθά να διασφαλιστεί ότι το SOC ανταποκρίνεται σε συγκεκριμένες απειλές με τον ίδιο τρόπο κάθε φορά. Το playbook είναι μια τυπική, τεκμηριωμένη διαδικασία που περιγράφει λεπτομερώς επαναλαμβανόμενα βήματα για την απόκριση σε συγκεκριμένους τύπους περιστατικών. Ένα playbook μπορεί να θεωρηθεί ως μια λίστα ελέγχου (checklist).

Τα Playbooks επιτρέπουν συνεπείς, προκαθορισμένες απαντήσεις σε απειλές, παρέχοντας μια καθοδηγούμενη ροή διεργασιών και εκτέλεση βέλτιστων πρακτικών για τη μείωση του φόρτου εργασίας των αναλυτών και τη βελτίωση της αποδοτικότητας και της αποτελεσματικότητας SOC.

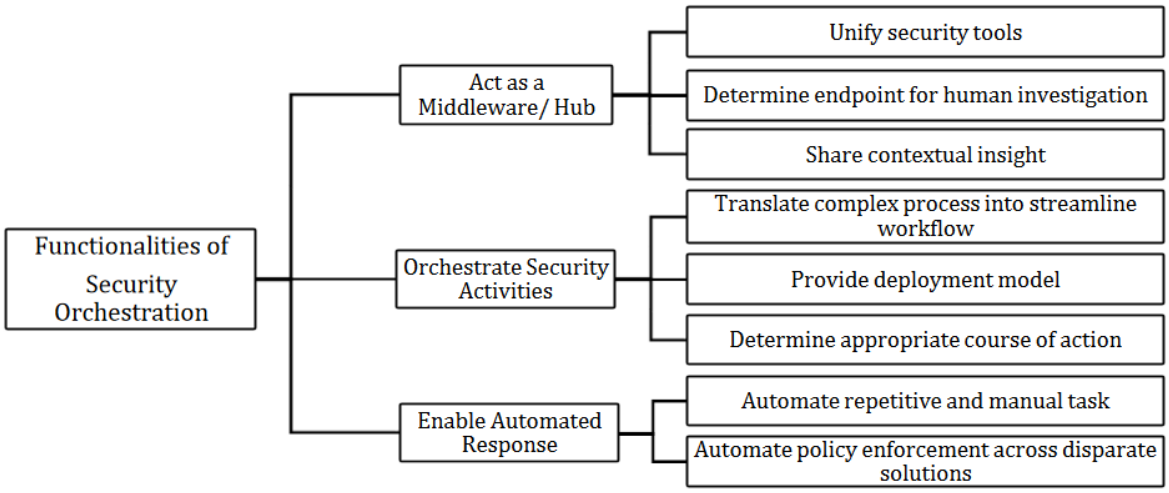
Οι πλατφόρμες SOAR συνοδεύονται από prebuilt playbooks για κοινές απειλές. Ωστόσο, αυτά τα playbook συχνά απαιτούν προσαρμογή από τους αναλυτές για να ευθυγραμμιστούν με τις εσωτερικές διαδικασίες λειτουργίας του οργανισμού τους. Οι αναλυτές μπορούν επίσης να δημιουργήσουν τα δικά τους playbooks από την αρχή ή να υιοθετήσουν playbooks που έχουν αναπτυχθεί και κοινοποιούνται από άλλους οργανισμούς.

4-1-5. Workflows

Οι καλά καθορισμένες διεργασίες και διαδικασίες είναι χαρακτηριστικά γνωρίσματα ενός SOC. Μια μηχανή ροής εργασιών και συνεργασίας (workflow and collaboration engine) ορίζει τις επιχειρησιακές διαδικασίες και διασφαλίζει τη συνεπή εκτέλεση των διαδικασιών. Οι επίσημες διαδικασίες του workflow and collaboration engine μπορούν να έχουν τόσο χειροκίνητα όσο και αυτοματοποιημένα βήματα. Όπου οι εργασίες δεν είναι αυτοματοποιημένες, το εργαλείο θα πρέπει να καθοδηγεί τους αναλυτές να εκτελούν τις σωστές εργασίες με τη σωστή σειρά για να διασφαλιστεί η συνέπεια. Όπου οι εργασίες είναι αυτοματοποιημένες, η πλατφόρμα θα πρέπει να διασφαλίζει την επιτυχή εκτέλεση, την κατάλληλη έγκριση και επίβλεψη και την επίσημη συλλογή των αποτελεσμάτων της αυτοματοποιημένης εργασίας.

4-2. Λειτουργίες τεχνολογίας SOAR

Μια από τις προκλήσεις της ενορχήστρωσης ασφαλείας είναι να γεφυρωθεί το χάσμα μεταξύ του εντοπισμού και της αποκατάστασης περιστατικών ασφαλείας[22]. Οι περισσότερες από τις λύσεις ανίχνευσης είναι αυτοματοποιημένες όπου οι διαδικασίες απόκρισης εξακολουθούν να εξαρτώνται από τον άνθρωπο. Για να γεφυρωθεί αυτό το χάσμα, υπάρχει ανάγκη να ενοποιηθούν οι δραστηριότητες των εργαλείων ασφαλείας, να βελτιστοποιηθούν οι ροές εργασίας και να επιλεγεί η σωστή πορεία ενεργειών. Μια ολοκληρωμένη πλατφόρμα ενορχήστρωσης ασφάλειας πρέπει να μπορεί να αυτοματοποιεί τις δραστηριότητες των εργαλείων ασφαλείας, να δημιουργεί playbook με περίπλοκη λογική και να παρακολουθεί και να ενορχηστρώνει τις εργασίες που έχουν ανατεθεί σε έναν αναλυτή. Η εικόνα 5 υπογραμμίζει τις βασικές λειτουργίες της ενορχήστρωσης ασφαλείας σε τρία υποδείγματα: α) ενοποίηση όπου μια ενορχήστρωση ασφαλείας λειτουργεί ως ενδιάμεσο λογισμικό, β) ενορχήστρωση που είναι η διαδικασία μετατροπής πολύπλοκης διαδικασίας σε βελτιστοποίηση της ροής εργασιών και γ) αυτοματοποίηση που επιτρέπει μια αυτοματοποιημένη απόκριση. [23]



Εικόνα 6. Βασικές λειτουργίες της τεχνολογίας SOAR.

Middleware / Hub

- **Unify Security Tools:** Η ενορχήστρωση ασφαλείας ενοποιεί ανόμοια εργαλεία και διαδικασίες ασφαλείας, ενσωματώνει την αρχιτεκτονική ασφάλειας επιχειρήσεων, συνδέει συστήματα ανίχνευσης, δικτύων και endpoints και πραγματοποιεί συντονισμό μεταξύ των διαφορετικών εργαλείων ασφαλείας. Η σύνδεση των δραστηριοτήτων

[22] ForeScout, "ForeScout Agentless Visibility and Control, White Paper", https://www.forescout.com/wp-content/uploads/2018/08/Agentless-Visibility-and-Control-ForeScout-White-Paper.pdf Accesed on: February 13, 2023.
[23] C. Islam, M.A. Babar, S. Nepal, "A Multi-Vocal Review of Security Orchestration", 2017 https://arxiv.org/abs/2002.09190 , Accessed on: January 12, 2023.

διαφορετικών εργαλείων ασφαλείας καθιστά τη διαδικασία χειρισμού περιστατικών αποτελεσματική για τον αναλυτή ασφαλείας. Η ενοποίηση των πληροφοριών αναλόγως της ευπάθειας ελαχιστοποιεί επίσης τη συνολική πολυπλοκότητα της διαδικασίας απόκρισης περιστατικού. Μέσω της πλατφόρμας, τα εργαλεία ασφαλείας μπορούν να συνεργάζονται μεταξύ τους ώστε να ενισχυθεί η αποτελεσματικότητα των συστημάτων προστασίας και άμυνας του οργανισμού.

- **Determine endpoint for human investigation:** Μια πλατφόρμα SOAR μπορεί να επιτρέψει στους ειδικούς σε θέματα ασφάλειας να αποκτήσουν πληροφορίες για διάφορες δραστηριότητες ελέγχου ασφαλείας, να λειτουργήσουν διαφορετικά εργαλεία ως ενοποιημένο σύστημα και να συνεργαστούν με άλλους ειδικούς για τον σχεδιασμό και τη λήψη αποφάσεων. Η λύση SOAR ενημερώνει και εκπαιδεύει τον αναλυτή ασφαλείας σχετικά με συμπεριφορές απειλών και ειδοποιεί για τις υποστηριζόμενες πολιτικές. Ενορχηστρώνοντας διάφορες δραστηριότητες, ένα σύστημα μπορεί να αποφασίσει πότε απαιτείται ανθρώπινη γνώση. Το κίνητρο είναι να διατηρηθεί η εστίαση του αναλυτή σε απειλές που απαιτούν την άμεση προσοχή και την τεχνογνωσία του.
- **Share contextual insight:** Ένα απλό σύστημα πρόληψης και ανίχνευσης ασφάλειας συνήθως πάσχει από το tunnel vision syndrome που οδηγεί σε αδυναμία εντοπισμού ορισμένων τύπων επιθέσεων, όπως η Distributed Denial of Service (DDoS). Μια πλατφόρμα ενορχήστρωσης ασφαλείας συλλέγει πληροφορίες απειλών από διάφορες εξωτερικές πηγές (π.χ. ιστοσελίδες και blogs), εξάγει βασικά χαρακτηριστικά από έναν τεράστιο όγκο δεδομένων πληροφοριών απειλών και παρέχει την πληροφόρηση σχετικά με ειδοποιήσεις ή επιθέσεις σε έναν αναλυτή ασφαλείας. Επιπλέον, χρησιμοποιεί εργαλεία ασφαλείας για την εκτέλεση πλήρους παρακολούθησης του endpoint, συσχετίζει τις δραστηριότητές τους και παρέχει σε πραγματικό χρόνο πληροφόρηση γνωστών και άγνωστων απειλών στον αναλυτή ασφαλείας. Ένας οργανισμός μπορεί να μοιράζεται δεδομένα με το σύστημα τρίτων. Βοηθά τον αναλυτή ασφαλείας να μειώσει και να μετριάσει την έκθεση στον κίνδυνο, να λάβει μια ταχύτερη απόφαση και να συγκεντρώσει μια επισκόπηση του τι συμβαίνει σε διάφορα υποδίκτυα μέσα σε έναν οργανισμό. Μοιράζοντας την ολική γνώση, μια πλατφόρμα ενορχήστρωσης λειτουργεί ως μια συνεργατική πλατφόρμα που επιτρέπει επίσης την εκπαίδευση του αναλυτή με βάση προηγούμενες έρευνες.

Orchestrate Security Activities

- **Translate complex process into streamline workflow**: Μετά τη λήψη ειδοποιήσεων, οι ειδικοί σε θέματα ασφάλειας πρέπει να εκτελέσουν πολλά βήματα για να εντοπίσουν τις επιθέσεις, τα τρωτά σημεία, τα επηρεαζόμενα endpoints και τις λύσεις μετριασμού. Αυτά τα βήματα περιλαμβάνουν τη σύνθετη διαδικασία συλλογής δεδομένων, διερεύνησης, αποκατάστασης, αξιολόγησης των ενεργειών και απόφασης της κατάλληλης πορείας ενεργειών. Μια απλοποιημένη ροή εργασιών απαιτεί μια τυποποιημένη διαδικασία που περιλαμβάνει σωστό σχεδιασμό για την απόκριση σε περιστατικό, την εκτέλεση πολιτικής, τη διερεύνηση, τη δράση απόκρισης και τη διαδικασία αποκατάστασης. Η ροή εργασίας έχει σχεδιαστεί για να μιμείται τις ανθρώπινες δραστηριότητες διερεύνησης απειλών για να μειώσει τη δυσκολία της χειροκίνητης διαδικασία, τα ανθρώπινα λάθη και να βελτιώσει τις δυνατότητες του προσωπικού για την απόκριση σε περιστατικά. Η ενορχήστρωση και η ενοποίηση των δραστηριοτήτων των εργαλείων ασφαλείας επιτρέπουν στους ειδικούς να απλοποιούν τη σύνθετη ροή εργασιών, να συντονίζουν τη ροή δεδομένων και εργασιών και να επιτρέπουν την ισχυρή αυτοματοποίηση από μηχανή σε μηχανή. Η εργασία μπορεί να αυτοματοποιηθεί πλήρως ή εν μέρει με βάση την πολυπλοκότητα των απειλών.
- **Provide deployment model:** Αρκετοί προμηθευτές συστημάτων ασφάλειας παρέχουν υπηρεσίες υλοποίησης SOAR που απαιτούν κατάλληλη ενορχήστρωση και αυτοματοποίηση των υπαρχόντων εργαλείων ασφαλείας μαζί με εξωτερικές και εσωτερικές υποδομές του οργανισμού. Το μοντέλο ανάπτυξης εξαρτάται από την κλίμακα, την πολυπλοκότητα και την πορεία των ενεργειών του οργανισμού. Οι οργανισμοί μπορούν να επιλέξουν πολιτικές ασφαλείας με βάση την ανάγκη τους να περιορίσουν την πρόσβαση και να προσαρμόσουν τις διαμορφώσεις ασφαλείας.
- **Determine appropriate course of actions:** Μια πλατφόρμα SOAR μπορεί να βοηθήσει στην άμεση επίλυση ενός περιστατικού και να καθορίσει την κατάλληλη και αποτελεσματική πορεία ενεργειών. Επιλέγοντας την κατάλληλη πορεία ενεργειών, η ενορχήστρωση ασφαλείας διατηρεί τη συνοχή της διαδικασίας σε ένα πρόγραμμα ασφαλείας. Επίσης, απαιτούνται διάφορα είδη ειδοποιήσεων (δηλαδή, phishing και μόλυνση endpoint) για τη διάκριση των δραστηριοτήτων αποκατάστασης με διαφορετικές πορείες ενεργειών. Κατά τη διερεύνηση μιας ειδοποίησης, μια πλατφόρμα ενορχήστρωσης μπορεί να καθορίσει την προληπτική απόκριση σε απειλές ή μπορεί να ξεκινήσει μια πρόσθετη έρευνα με βάση την πολυπλοκότητα μιας

επίθεσης. Σε πολλές περιπτώσεις, μπορεί επίσης να δημιουργηθεί μια εργασία έρευνας ή αξιολόγησης μετά την επίθεση. Οι Feitosa et al.[24] έχουν προτείνει ένα πλαίσιο, «Orchestration-oriented Anomaly Detection System (OADS)», το οποίο εκτελεί συντονισμό και συνεργασία μεταξύ διαφορετικών τεχνικών ανίχνευσης ανωμαλιών για τον εντοπισμό και την αξιολόγηση απειλών και την επιλογή των σωστών ενεργειών. Οι ειδικοί ασφαλείας πραγματοποιούν πολλαπλές έρευνες ως απάντηση σε μια ειδοποίηση. Στη διαδικασία της ενορχήστρωσης, μια έρευνα συνήθως ενεργοποιεί πολλαπλές έρευνες. Οι ροές εργασίας έχουν σχεδιαστεί για να επιλέγουν την κατάλληλη πορεία ενεργειών, να απλοποιούν την απόκριση σε απειλές μέσω ενοποίησης και αυτοματοποίησης, να εκτελούν την απαραίτητη αποκατάσταση, να αποφασίζουν πρόσθετη έρευνα, να σχεδιάζουν έγγραφα για την αναθεώρηση των βιβλίων στρατηγικής και να ορίζουν πηγές πληροφοριών για να βοηθήσουν τους ειδικούς στην επίλυση των προβλημάτων που έχουν εντοπιστεί.

Enable Automated Response

Τα συστήματα SOAR αυτοματοποιούν τις δράσεις αντιμετώπισης περιστατικών. Η ενορχήστρωση των δραστηριοτήτων απόκρισης περιστατικού επιτρέπει την αυτοματοποιημένη απόκριση χωρίς την ανάγκη για δεξιότητες γραφής κώδικα.

- **Automate repetitive manual task:** Οι προμηθευτές χρησιμοποιούν μια πλατφόρμα SOAR για να αυτοματοποιήσουν επαναλαμβανόμενες εργασίες και να αφαιρέσουν διπλά συμβάντα για να βελτιστοποιήσουν την ικανότητα του προσωπικού ασφαλείας και να μειώσουν το συνολικό κόστος. Η αυτοματοποίηση των εργασιών ρουτίνας βοηθά τους ειδικούς σε θέματα ασφάλειας να αντιμετωπίσουν πιο κρίσιμα προβλήματα. Σύμφωνα με το Swimlane, το 80% έως το 90% όλων των λειτουργιών ασφαλείας μιας απόκρισης συμβάντος μπορεί να αυτοματοποιηθεί σε κάποιο βαθμό.[25]
- **Automate policy enforcement:** Η επιβολή της πολιτικής ασφαλείας επωφελείται σε μεγάλο βαθμό από την αυτοματοποίηση που λαμβάνει υπόψη όλα τα εργαλεία, τις συσκευές και τα μέτρα που απαιτούνται για την εφαρμογή μιας πολιτικής ασφάλειας. Η ενορχήστρωση ασφαλείας δίνει τη δυνατότητα σε έναν οργανισμό να αυτοματοποιεί την επιβολή και τη διαμόρφωση πολιτικών κατά το χρόνο εκτέλεσης.

[24] E. Feitosa, E. Souto, and D. H. Sadok, "An orchestration approach for unwanted Internet traffic identification, Computer Networks", vol. 56, no. 12, pp. 2805-2831, 2012.
[25]SWIMLANE, "Security Orchestration | What is Security Orchestration?" https://swimlane.com/solutions/security-automation-and-orchestration/security-orchestration/ , Accessed on: February 13, 2023.

4-3. Χρήσεις τεχνολογίας SOAR και προβλήματα που επιλύει

Οι πλατφόρμες SOAR χρησιμοποιούνται για την αυτοματοποίηση και την βελτιστοποίηση των διαδικασιών απόκρισης συμβάντων. Έχουν σχεδιαστεί για να βοηθούν τις ομάδες ασφαλείας να ανταποκρίνονται γρήγορα και αποτελεσματικά σε συμβάντα ασφαλείας παρέχοντας μια ενοποιημένη εικόνα της ασφάλειας ενός οργανισμού, αυτοματοποιώντας επαναλαμβανόμενες εργασίες και παρέχοντας πληροφορίες που μπορούν να αξιοποιηθούν. Μερικές από τις βασικές χρήσεις των συστημάτων SOAR περιλαμβάνουν:

1. **Incident management**: Τα συστήματα SOAR παρέχουν μια κεντρική πλατφόρμα για τη διαχείριση συμβάντων, επιτρέποντας στις ομάδες ασφαλείας να παρακολουθούν και να διαχειρίζονται συμβάντα ασφαλείας από την αρχή μέχρι το τέλος.
2. **Threat intelligence**: Τα συστήματα SOAR ενοποιούνται με διάφορες τροφοδοσίες πληροφοριών απειλών για να παρέχουν στις ομάδες ασφαλείας αξιόπιστες πληροφορίες σχετικά με τις απειλές που αντιμετωπίζει ο οργανισμός τους.
3. **Incident response automation**: Τα συστήματα SOAR αυτοματοποιούν επαναλαμβανόμενες εργασίες απόκρισης συμβάντων, όπως συλλογή δεδομένων, ανάλυση και επικοινωνία, για να βελτιώσουν τους χρόνους απόκρισης συμβάντων.
4. **Coordination of security tools**: Τα συστήματα SOAR μπορούν να ενοποιηθούν με διάφορα εργαλεία ασφαλείας, όπως firewalls, intrusion detection systems, και endpoint protection, για να συντονίσουν τις αποκρίσεις τους σε συμβάντα.
5. **Reporting and compliance**: Τα συστήματα SOAR μπορούν να παρέχουν λεπτομερείς δυνατότητες αναφοράς και συμμόρφωσης για να βοηθήσουν τους οργανισμούς να ανταποκριθούν στις κανονιστικές απαιτήσεις.
6. **Automated incident handling**: Τα συστήματα SOAR μπορούν να προγραμματιστούν ώστε να χειρίζονται αυτόματα ορισμένους τύπους συμβάντων, όπως ο αποκλεισμός μιας διεύθυνσης IP ή ο τερματισμός μιας συγκεκριμένης υπηρεσίας.
7. **Automated incident investigation**: Τα συστήματα SOAR μπορούν να χρησιμοποιηθούν για την αυτόματη συλλογή και ανάλυση δεδομένων από διάφορες πηγές για να βοηθήσουν τους ερευνητές να κατανοήσουν το εύρος και την αιτία ενός συμβάντος.

Τα συστήματα SOAR έχουν σχεδιαστεί για να επιλύουν μια ποικιλία προβλημάτων που αντιμετωπίζουν οι ομάδες ασφαλείας, όπως:

1. **Αργοί χρόνοι incident response**: Τα συστήματα SOAR αυτοματοποιούν επαναλαμβανόμενες εργασίες απόκρισης περιστατικού για να βελτιώσουν τους χρόνους απόκρισης περιστατικού και να μειώσουν τον κίνδυνο παραβιάσεων.
2. **Έλλειψη συνολικής εικόνας**: Τα συστήματα SOAR παρέχουν μια ενοποιημένη εικόνα της ασφάλειας ενός οργανισμού, δίνοντας στις ομάδες ασφαλείας μια σαφή και ολοκληρωμένη κατανόηση των κινδύνων ασφαλείας που αντιμετωπίζει ο οργανισμός τους.
3. **Περιορισμένοι πόροι**: Τα συστήματα SOAR μπορούν να βοηθήσουν τις ομάδες ασφαλείας να λειτουργούν πιο αποτελεσματικά αυτοματοποιώντας επαναλαμβανόμενες εργασίες, ελευθερώνοντας πόρους για να επικεντρωθούν σε πιο περίπλοκα και κρίσιμα συμβάντα.
4. **Περιορισμένο threat intelligence**: Τα συστήματα SOAR ενοποιούνται με διάφορες πηγές πληροφοριών απειλών για να παρέχουν στις ομάδες ασφαλείας αξιόπιστες πληροφορίες σχετικά με τις απειλές που αντιμετωπίζει ο οργανισμός τους.
5. **Αδυναμία συντονισμού εργαλείων ασφαλείας**: Τα συστήματα SOAR μπορούν να ενοποιηθούν με διάφορα εργαλεία ασφαλείας, όπως firewalls, intrusion detection systems, και endpoint protection, για να συντονίσουν τις αποκρίσεις τους σε συμβάντα.
6. **Δυσκολία ικανοποίησης των κανονιστικών απαιτήσεων**: Τα συστήματα SOAR μπορούν να παρέχουν λεπτομερείς δυνατότητες αναφοράς και συμμόρφωσης για να βοηθήσουν τους οργανισμούς να ανταποκριθούν στις κανονιστικές απαιτήσεις.
7. **Πολυπλοκότητα χειρισμού συμβάντων**: Τα συστήματα SOAR μπορούν να αυτοματοποιήσουν τη διαχείριση περιστατικών, βοηθώντας τις ομάδες ασφαλείας να χειριστούν μεγάλο όγκο συμβάντων και να μειώσουν την πολυπλοκότητα της διαδικασίας χειρισμού περιστατικών.
8. **Δυσκολία στη διερεύνηση περιστατικού**: Τα συστήματα SOAR μπορούν να χρησιμοποιηθούν για την αυτόματη συλλογή και ανάλυση δεδομένων από διάφορες πηγές για να βοηθήσουν τους ερευνητές να κατανοήσουν το εύρος και την αιτία ενός συμβάντος, καθιστώντας την έρευνα περιστατικού πιο αποτελεσματική.

4-4. Πλεονεκτήματα τεχνολογίας SOAR

Από την εμφάνιση της τεχνολογίας SOAR, μεγάλες επιχειρήσεις, προμηθευτές ασφάλειας και πάροχοι υπηρεσιών ασφαλείας (MSSP) έχουν αναπτύξει ένα ευρύ φάσμα

περιπτώσεων χρήσης SOAR, αναζητώντας τα οφέλη τους καθώς η αγορά συνεχίζει να ευδοκιμεί. Μερικά από τα οφέλη που προσφέρει μια λύση SOAR είναι:[26]

1. **Ταχύτεροι χρόνοι απόκρισης**: Η ενορχήστρωση ασφαλείας συγκεντρώνει πολλαπλές σχετιζόμενες ειδοποιήσεις από διαφορετικά συστήματα σε ένα μόνο περιστατικό. Εξοικονομώντας ακόμη περισσότερο χρόνο, ο αυτοματισμός ασφαλείας επιτρέπει στο σύστημα να ανταποκρίνεται σε ειδοποιήσεις χωρίς ανθρώπινη παρέμβαση όποτε είναι δυνατόν.
2. **Βελτιωμένο Threat Intelligence:** Οι οργανισμοί μπορούν να βελτιστοποιήσουν τη ροή εργασιών πληροφοριών απειλών (threat intelligence workflow), ενοποιώντας τα υπάρχοντα εργαλεία ασφαλείας τους σε μία πλατφόρμα SOAR. Οι αναλυτές SOC αντιμετωπίζουν συνεχώς υπερφόρτωση πληροφοριών. Οι καλύτερες πλατφόρμες SOAR μπορούν να προσλάβουν πληροφορίες απειλών και να τις συσχετίσουν αυτόματα με γεγονότα σε πραγματικό χρόνο. Αυτό αφαιρεί το βάρος των αναλυτών SOC και παρέχει άμεσα πρακτικές πληροφορίες για τις ομάδες αντιμετώπισης περιστατικών.
3. **Βελτιωμένα SOC με τυποποιημένες διαδικασίες:** Η αυτοματοποίηση ασφαλείας απαλλάσσει τους αναλυτές SOC από κοινότοπες, επαναλαμβανόμενες εργασίες και τους συμπεριλαμβάνει σε μια συνολική διαδικασία για το πώς να χειριστούν οποιοδήποτε περιστατικό. Μια καλή πλατφόρμα SOAR θα ενοποιήσει αυτές τις διαδικασίες σε playbook που παρουσιάζουν όλα τα βήματα για την απόκριση σε ένα συμβάν.
4. **Βελτιστοποιημένες διαδικασίες:** Κάθε στοιχείο του SOAR συμβάλλει στην βελτιστοποίηση των λειτουργιών ασφαλείας. Η ενορχήστρωση ασφαλείας συγκεντρώνει δεδομένα που προέρχονται από διάφορες πηγές. Ο αυτοματισμός ασφαλείας, μπορεί εύκολα να χειριστεί ειδοποιήσεις και συμβάντα χαμηλής προτεραιότητας μέσω της χρήσης αυτοματοποιημένων playbook. Η απόκριση περιστατικών περιορίζει τον χρόνο παραμονής των επιθέσεων στον κυβερνοχώρο και τον συνολικό αντίκτυπο στην επιχείρηση.
5. **Μειωμένος αντίκτυπος των κυβερνοεπιθέσεων:** Ο μέσος χρόνος εντοπισμού (MTTD) και ο μέσος χρόνος απόκρισης (MTTR) είναι κρίσιμες μετρήσεις που

[26] Dan Kaplan, "9 security orchestration and automation benefits: How SOAR helps improve incident response", 2021 https://chronicle.security/blog/posts/security-orchestration-automation-response-benefits/ , Accessed on: February 13, 2023.

επηρεάζουν τον αντίκτυπο που έχει μια κυβερνοεπίθεση σε έναν οργανισμό. Όσο περισσότερος χρόνος χρειάζεται για να εντοπιστεί και να ανταποκριθεί σε μια επίθεση, τόσο μεγαλύτερη ζημιά μπορεί να προκληθεί και τόσο μεγαλύτερος είναι ο αντίκτυπος στον οργανισμό. Το SOAR ελαχιστοποιεί τόσο το MTTD όσο και το MTTR. Η ενορχήστρωση ασφαλείας μειώνει το MTTD παρέχοντας λεπτομέρειες για κάθε περιστατικό, δίνοντας τη δυνατότητα στους αναλυτές να αφιερώνουν λιγότερο χρόνο στη συλλογή πληροφοριών και περισσότερο χρόνο στη διερεύνηση της ειδοποίησης. Ο αυτοματισμός ασφαλείας μειώνει το MTTR απαντώντας σε ειδοποιήσεις και συμβάντα αυτόματα σε πραγματικό χρόνο.

6. **Εύκολη ενοποίηση εργαλείων και τεχνολογιών**: Ένα από τα οφέλη της τεχνολογίας SOAR είναι η δυνατότητα συσχέτισης ειδοποιήσεων από μια μεγάλη ποικιλία προϊόντων και τεχνολογιών. Μια πλατφόρμα SOAR θα πρέπει να μπορεί να ενοποιηθεί με προϊόντα σε διάφορες τεχνολογίες ασφάλειας, όπως Cloud Security, Data Enrichment, Email Security, Endpoint Security, Forensics & Malware Analysis, Identity and Access Management, IT and Infrastructure, Network Security, SIEM & Log Management, Threat Intelligence, Vulnerability & Risk Management. Η ενοποίηση αυτών των προϊόντων στην πλατφόρμα SOAR είναι εύκολη.
7. **Χαμηλότερα κόστη:** Μια τυπική επιχείρηση θα έχει σημαντική εξοικονόμηση πόρων ενσωματώνοντας μια πλατφόρμα SOAR στο επιχειρηματικό της μοντέλο**.**
8. **Δυνατότητες αυτοματοποιημένης αναφοράς και μετρήσεων:** Η αυτοματοποιημένη αναφορά όχι μόνο διευκολύνει τη ζωή, αλλά εξαλείφει την ανάγκη για μετρήσεις που παράγονται με μη αυτόματο τρόπο. Επιτρέποντας στο προσωπικό του SOC να αντλεί αναφορές κατά παραγγελία — κατά προτίμηση με ένα κλικ — ή αυτόματα σε ένα χρονοδιάγραμμα, οι επιχειρήσεις λαμβάνουν αξιόπιστες και έγκαιρες μετρήσεις για κάθε περίοδο αναφοράς. Για να απλοποιηθεί περαιτέρω αυτή η διαδικασία, τα περισσότερα εργαλεία SOAR παρέχουν πρότυπα αναφοράς και τη δυνατότητα δημιουργίας προσαρμοσμένων αναφορών.
9. **Τυποποιημένη επικοινωνία κατά το Incident Response**: Ο χειρισμός και η απόκριση συμβάντων συχνά απαιτούν πρόσβαση εκτός του SOC, ειδικά για μεγάλα περιστατικά. Αυτό σημαίνει ότι οι ομάδες αντιμετώπισης συμβάντων μπορούν να περιλαμβάνουν ενδιαφερόμενους τόσο εντός όσο και εκτός του. Για τον μετριασμό αυτού του ζητήματος, οι επιχειρήσεις συχνά σχηματίζουν έναν mission control hub για να χειρίζονται συμβάντα κορυφαίας προτεραιότητας. Μια πλατφόρμα SOAR θα έχει μια λειτουργία " virtual war room" για να διασφαλίσει ότι η κρίσιμη επικοινωνία είναι

τυποποιημένη και να αποτρέψει οποιοδήποτε μέλος της ομάδας να χάσει κρίσιμες πληροφορίες κατά τη διάρκεια μιας απόκρισης περιστατικού.

4-5. Διαφορές SOAR και SIEM

Τόσο το SOAR όσο και το SIEM ασχολούνται με δεδομένα γύρω από απειλές ασφαλείας και επιτρέπουν πολύ καλύτερες απαντήσεις σε περιστατικά ασφαλείας. Ωστόσο, το SIEM συγκεντρώνει και συσχετίζει δεδομένα από πολλαπλά συστήματα ασφαλείας για τη δημιουργία ειδοποιήσεων, ενώ το SOAR λειτουργεί ως η μηχανή αποκατάστασης και απόκρισης σε αυτές τις ειδοποιήσεις.

Οι λύσεις κυβερνοασφάλειας SOAR και SIEM μπορούν να συλλέγουν δεδομένα από τις ίδιες πηγές, αν και το εύρος του SOAR είναι ευρύτερο, καθώς μπορεί να συλλέγει δεδομένα από εξωτερικές εφαρμογές. Η διαφορά μεταξύ SOAR και SIEM βασίζεται στις ενέργειες που μπορεί να κάνει κάθε είδος εργαλείου όταν ανακαλύπτει μια πιθανή απειλή ή ευπάθεια. Το SOAR χρησιμοποιεί AI bots και playbooks που είναι προσαρμοσμένα για να κάνουν μια συγκεκριμένη ενέργεια μόλις εντοπιστεί μια απειλή. Οι προσαρμοσμένες ενέργειες αποτελούν μέρος μιας αυτοματοποιημένης ροής εργασιών (workflow) που καταγράφει και παρακολουθεί τα βήματα για την επίλυση μιας αναγνωρισμένης απειλής. Αυτό δημιουργεί μεγαλύτερη αποτελεσματικότητα στη διαδικασία απόκρισης περιστατικού.

Από την άλλη πλευρά, το SIEM χρησιμοποιεί αντιστοίχιση pattern για να δημιουργήσει ειδοποιήσεις που μπορεί να διερευνήσει το προσωπικό ασφαλείας IT. Το SIEM χρησιμοποιεί επίσης τεχνολογία AI για να μειώσει τον αριθμό των false positives που μπορούν να αποσπάσουν την προσοχή των ομάδων ασφαλείας από την αντιμετώπιση απειλών για την ασφάλεια στον κυβερνοχώρο. Επιπλέον, ο ρόλος ενός εργαλείου SIEM σταματά στον εντοπισμό μιας απειλής, ενώ μια πλατφόρμα SOAR κάνει το επόμενο βήμα για να βοηθήσει τους διαχειριστές να αναλάβουν δράση.

Το SOAR έχει θεωρηθεί ως ένα τέλειο συμπλήρωμα σε ένα SIEM. Για παράδειγμα, ο Gartner χρησιμοποιεί τον συνδυασμό SIEM και SOAR ως παράδειγμα κοινής προσέγγισης για τον εντοπισμό και την απόκριση. Παρόλο που έχουν εμφανιστεί άλλα εργαλεία που παρέχουν εναλλακτικές λύσεις στο SOC με επίκεντρο το SIEM, ένα SIEM εξακολουθεί να είναι μια ιδανική πηγή ειδοποίησης, με την ικανότητά του να συγκεντρώνει και να επισημαίνει κακόβουλη δραστηριότητα. Αυτές οι ειδοποιήσεις μπορούν στη συνέχεια να παραπεμφθούν σε μια ενοποιημένη πλατφόρμα SOAR, είτε χειροκίνητα είτε αυτόματα με βάση τους κανόνες SIEM.

Η πλατφόρμα SOAR μπορεί να χρησιμοποιηθεί για την ανάλυση του alert, για τον προσδιορισμό του αν πρόκειται για αληθινό περιστατικό και για την ενορχήστρωση της απαραίτητης απόκρισης σε άλλα ολοκληρωμένα συστήματα. [27]

[27] Ina Nikolova, "What Are the Main Differences Between SIEM and SOAR?", 2022, https://www.linkedin.com/pulse/what-main-differences-between-siem-soar-ina-nikolova-ph-d-?trk=pulse-article_more-articles_related-content-card , Accessed on: February 13, 2023.

5. Σημαντικότερες υλοποιήσεις SOAR ανοικτού κώδικα και σύγκριση

5-1. Ποιοτικά χαρακτηριστικά

Οι πλατφόρμες SOAR ανοιχτού κώδικα γίνονται όλο και πιο δημοφιλείς λόγω της οικονομικής αποδοτικότητάς τους και της ευελιξίας τους. Κάθε πλατφόρμα έχει τα δικά της δυνατά και αδύνατα σημεία, επομένως είναι σημαντικό να αξιολογούμε την καθεμία με βάση τις συγκεκριμένες ανάγκες και απαιτήσεις του κάθε οργανισμού.

Οι οργανισμοί έχουν μια ποικιλία επιλογών όσον αφορά την αξιοποίηση των δυνατοτήτων SOAR. Η επιλογή μεταξύ τους θα εξαρτηθεί από τις συγκεκριμένες απαιτήσεις του κάθε οργανισμού, καθώς και από παράγοντες όπως η ευκολία χρήσης, η ενοποίηση με άλλα εργαλεία ασφαλείας και το community support. Αξίζει επίσης να σημειωθεί ότι ορισμένες από αυτές τις πλατφόρμες μπορεί να ταιριάζουν καλύτερα σε συγκεκριμένους τύπους οργανισμών, όπως εκείνοι με μεγάλο πρόγραμμα threat intelligence, ενώ άλλες μπορεί να είναι πιο κατάλληλες για εκείνους με μικρότερη ομάδα και λιγότερα εργαλεία ασφαλείας.

Σε αυτήν την ενότητα, θα παρουσιάσουμε κάποια κρίσιμα ποιοτικά χαρακτηριστικά για μια λύση SOAR, έτσι ώστε παρακάτω να παρουσιάσουμε τέσσερις από τις σημαντικότερες υλοποιήσεις SOAR πλατφορμών ανοικτού κώδικα και να τις συγκρίνουμε με βάση αυτά τα χαρακτηριστικά.[28]

Dashboard

Οι incident responders και οι security analysts αλληλεπιδρούν με το SOAR μέσω του dashboard. Αυτό πρέπει να είναι εξελιγμένο, αλλά εύκολο στη χρήση. Τα workflows θα πρέπει να καθοδηγούν τους αναλυτές χωρίς να απαιτείται από αυτούς να κατανοήσουν την αρχιτεκτονική δεδομένων που κρύβεται από πίσω. Το προσωπικό του SOC θα πρέπει να μπορεί να λειτουργεί φυσικά, να αναθέτει και να εργάζεται μέσα από εργασίες χωρίς να σκέφτεται το ίδιο το εργαλείο. Θα πρέπει να είναι διαθέσιμες ισχυρές δυνατότητες αναζήτησης και λειτουργικότητας με ένα κλικ για να βοηθήσουν στη διερεύνηση συμβάντων. Μια εστιασμένη προβολή εργασιών μπορεί να βοηθήσει να διασφαλιστεί ότι οι χρήστες δεν χάνουν κάποιο βήμα και γνωρίζουν πάντα σε τι να δώσουν προτεραιότητα, οδηγώντας έτσι σε χαμηλότερο MTTR (mean time to respond).

[28] Crystal Bedell, “Definitive guide to SOAR. How to stop threats faster with security orchestration, automation and response”, 2019, p. 51-56.
https://gallery.logrhythm.com/white-papers-and-e-books/definitive-guide-to-soar.pdf

Κεντρικό Αποθετήριο Τεκμηρίων

Ένα κεντρικό αποθετήριο αποδεικτικών στοιχείων διευκολύνει τους αναλυτές να μοιράζονται αποδεικτικά στοιχεία μεταξύ τους, ενώ αποτρέπει την τυχαία έκθεση πληροφοριών σε επιτιθέμενους.

Χωρίς ένα κεντρικό αποθετήριο αποδεικτικών στοιχείων, οι αναλυτές ξοδεύουν πολύτιμο χρόνο και διακινδυνεύουν να μοιράζονται αποδεικτικά στοιχεία μέσω μη ασφαλών καναλιών όπως το email, τα άμεσα μηνύματα και οι πλατφόρμες συνεργασίας όπως το Slack. Όταν οι αναλυτές χρειάζεται να ανατρέξουν σε ένα συγκεκριμένο αποδεικτικό στοιχείο, πρέπει να το αναζητήσουν σε πολλά κανάλια, με κίνδυνο να χάσουν κάτι εντελώς.

Ένα κεντρικό αποθετήριο είναι επίσης κρίσιμο για την υποστήριξη οποιασδήποτε διαδικασίας συμμόρφωσης. Οι περισσότερες έρευνες μιας παραβίασης διαρκούν χρόνια και τα στοιχεία για το τι έγινε μπορεί να κάνουν τη διαφορά μεταξύ της διαπίστωσης «εσκεμμένης αμέλειας» και της «τυχαίας έκθεσης».

Για να είναι αποτελεσματική, μια πλατφόρμα SOAR πρέπει να δέχεται στοιχεία από διάφορες πηγές που μπορούν να αναζητηθούν. Εάν ένας αναλυτής πρέπει να μεταβεί σε διαφορετικά συστήματα για να ανακτήσει ένα αρχείο καταγραφής, ένα μολυσμένο αρχείο και μια αναφορά, ο χρόνος που αφιερώνεται στην εναλλαγή περιβάλλοντος αυξάνει άμεσα τον χρόνο εντοπισμού και απόκρισης. Η λύση SOAR θα πρέπει επίσης να διασφαλίζει τη συνοχή των οπτικοποιήσεων διαφορετικών δεδομένων ανεξάρτητα από την πηγή.

Προσαρμόσιμα Workflows

Ενώ οι βέλτιστες πρακτικές ασφαλείας θα πρέπει να χρησιμοποιούνται για τη διαμόρφωση και την τυποποίηση των workflows, αυτά τα workflows πρέπει επίσης να είναι συμβατά με μοναδικά περιβάλλοντα. Μια πλατφόρμα SOAR θα πρέπει να ενοποιηθεί με τα υπάρχοντα στοιχεία της υποδομής του οργανισμού, επιτρέποντας στις ομάδες να αναπτύξουν προσαρμοσμένα workflows που αποτυπώνουν τις ιδιοσυγκρασίες που κρύβονται μέσα στον οργανισμό.

Επιπλέον, τα workflows πρέπει να επικεντρώνονται πλήρως και να υποστηρίζουν τις λειτουργίες ασφάλειας. Μια πλατφόρμα SOAR δεν θα πρέπει να εκθέτει στοιχεία για ένα κρίσιμο περιστατικό, π.χ. τον IT administrator, απλώς και μόνο επειδή η πλατφόρμα SOAR μοιράζεται τη διαχείριση υποθέσεων μέσα στο σύστημα πληροφορικής που λειτουργεί από αυτόν τον administrator. Τα workflows πρέπει να υποστηρίζουν την απομόνωση των χρηστών και τα κατάλληλα μέτρα ασφαλείας.

Playbooks και οδηγίες

Τα καθοδηγούμενα workflows — playbooks — σε μια πλατφόρμα SOAR επιτρέπουν γρήγορη, ακριβή και προβλέψιμη απόκριση περιστατικού, ανεξάρτητα από το επίπεδο δεξιοτήτων του αναλυτή. Τα Playbook περιγράφουν ακριβώς τι πρέπει να κάνει ο αναλυτής σε ένα δεδομένο σενάριο απειλής και πότε να το κάνει. Καθοδηγώντας τους αναλυτές μέσα από ένα καθορισμένο σύνολο βημάτων, τα playbook αυξάνουν την αποτελεσματικότητά τους, βελτιώνουν την ποιότητα της απόκρισής τους σε περιστατικά και βελτιστοποιούν τον φόρτο εργασίας τους.

Με βάση τις γνώσεις των ειδικών σε θέματα ασφάλειας, τα playbooks καταγράφουν τη θεσμική γνώση που διαφορετικά μπορεί να εξαφανιστεί όταν ένας ανώτερος αναλυτής αποχωρήσει από τον οργανισμό. Δίνουν χρόνο στους ανώτερους αναλυτές για πιο σύνθετες έρευνες, threat hunting κ.λπ., επιτρέποντας στους κατώτερους αναλυτές να αναλάβουν περισσότερες δραστηριότητες αντιμετώπισης περιστατικών.

Επιπλέον, μια πλατφόρμα SOAR με playbooks δίνει τη δυνατότητα στους αναλυτές να ανταποκρίνονται και να αποκαθιστούν απειλές μέσα από μια ενιαία πλατφόρμα για βέλτιστη απόδοση και αποτελεσματικότητα.

Εμπλουτισμός Δεδομένων

Όσο περισσότερα δεδομένα υψηλής ποιότητας έχουν οι αναλυτές δεδομένων, τόσο καλύτερα ενημερωμένοι θα είναι και τόσο μεγαλύτερη είναι η πιθανότητα να λάβουν ακριβείς αποφάσεις. Επομένως, μια πλατφόρμα SOAR θα πρέπει να έχει εκτεταμένες δυνατότητες εμπλουτισμού δεδομένων για μια έρευνα ώστε να διευκολύνει τη λήψη αποφάσεων. Για παράδειγμα, τα δεδομένα alert θα πρέπει να διαβιβάζονται από τις συσκευές δικτύου στο SOAR. Σε περίπτωση πιθανής μόλυνσης από κακόβουλο λογισμικό, η πλατφόρμα SOAR θα πρέπει να συλλέγει εγκληματολογικά δεδομένα από το ύποπτο endpoint. Στο μέτρο του δυνατού, η συλλογή δεδομένων θα πρέπει να είναι αυτοματοποιημένη.

Βιβλιοθήκη αυτοματοποιημένων αποκρίσεων

Μια εκτεταμένη βιβλιοθήκη με αυτοματοποιημένες απαντήσεις σε απειλές παρέχει συνέχεια σε όλη τη ροή εργασιών ανίχνευσης απειλών και απόκρισης χωρίς την ανάγκη για API ή προσαρμοσμένη εργασία ενοποίησης. Αυτά τα πρότυπα (template) workflow μειώνουν το TCO (Total Cost of Ownership) για μια πλατφόρμα SOAR, ειδικά σε μεγάλα περιβάλλοντα.

Εκτός από την εξάλειψη κοινότυπων και κουραστικών εργασιών, τα αυτοματοποιημένα αντίμετρα δρουν για να περιορίσουν τις απειλές ή να περιορίσουν την εξέλιξη της απειλής.

APIs και μια ποικιλία ενσωματώσεων

Ως κεντρικός κόμβος για ένα SOC, ένα SIEM με δυνατότητες SOAR πρέπει να μπορεί να ενοποιηθεί τόσο με τις τρέχουσες όσο και με τις μελλοντικές τεχνολογίες εντός και εκτός του περιβάλλοντος IT. Έτσι, μια λύση SOAR θα πρέπει να παρέχει API και ένα ευρύ φάσμα ενσωματώσεων από πολλούς προμηθευτές και τεχνολογίες.

Οι οργανισμοί θα πρέπει να μπορούν να ενοποιήσουν εύκολα το αποθετήριο αποδεικτικών τεκμηρίων με άλλες εταιρικές εφαρμογές, χωρίς σημαντικές ρυθμίσεις παραμέτρων σε πολλαπλά συστήματα. Αυτή η ενοποίηση βοηθά στην επιτάχυνση του μετριασμού της απειλής και της απόκρισης συμβάντων.

Ο προμηθευτής SOAR θα πρέπει επίσης να παρέχει ένα REST API για ενσωματώσεις τρίτων. Εκτός από την υποστήριξη της ενοποίησης του συστήματος ticketing, το API μπορεί να χρησιμοποιηθεί για τη διαχείριση των playbook και την αυτόματη ανάθεση εργασιών σε έναν αναλυτή.

Ευκολία χρήσης και δυνατότητα υποστήριξης

Οι αποδόσεις που επιτυγχάνονται με το SOAR θα πρέπει να επεκταθούν στη χρήση και την υποστήριξη του ίδιου του εργαλείου. Η πλατφόρμα θα πρέπει να είναι εύκολη στη χρήση και τη διαχείριση, με λειτουργία one-click για κοινότυπες εργασίες όπως η δημιουργία case και οι αναζητήσεις πληροφοριών απειλών.

Ενσωματωμένες δυνατότητες SOAR

Είναι σημαντικό να επιλεγεί μια λύση SIEM με ενσωματωμένες δυνατότητες SOAR έναντι μιας αυτόνομης λύσης SOAR. Ένα SIEM με ενσωματωμένο SOAR θα επιτρέψει σε ένα SOC να βελτιστοποιήσει την απόδοση που κερδίζει από το SOAR. Ωστόσο, είναι σημαντικό οι δυνατότητες SOAR να είναι εγγενώς ενσωματωμένες στο σύστημα SIEM —όχι να προστίθενται μετά την ανάπτυξη του SIEM— για τον ίδιο ακριβώς λόγο.

Ενώ ορισμένοι προμηθευτές προσφέρουν δυνατότητες SIEM και SOAR, αυτές ενδέχεται να εξακολουθούν να λειτουργούν ως ανεξάρτητες λύσεις με μόνο ελαφρές

ενσωματώσεις. Οι λύσεις που προκύπτουν δεν είναι βασικά σχεδιασμένες για να λειτουργούν με συνοχή. Η εμπειρία χρήστη και τα workflows είναι συνήθως λιγότερο αποτελεσματικά.

Αναζητούμε μια λύση SIEM με δυνατότητες SOAR που είναι άμεσα ενσωματωμένες στο σύνολο χαρακτηριστικών της πλατφόρμας, με workflows διαχείρισης απειλών και framework ανίχνευσης και απόκρισης για το SOC.

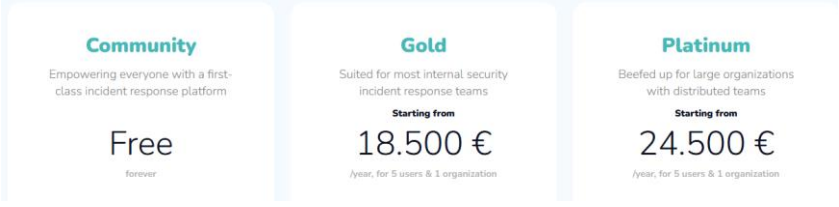
5-2. Σημαντικότερες υλοποιήσεις SOAR ανοικτού κώδικα

Υπάρχουν πολλά διαθέσιμα συστήματα SOAR ανοιχτού κώδικα, το καθένα με τα δικά του πλεονεκτήματα και αδυναμίες. Μερικά από τα πιο δημοφιλή συστήματα SOAR ανοιχτού κώδικα περιλαμβάνουν: TheHive, MISP, Cortex XSOAR, OpenSOAR (υπό ανάπτυξη), OpenCTI, Chronicle SOAR (Siemplify), Shuffle κ.α. Παρακάτω θα δούμε και θα συγκρίνουμε τέσσερα από αυτά τα συστήματα SOAR, και πιο συγκεκριμένα τα TheHive, Cortex XSOAR, Chronicle SOAR και Shuffle.

5-2-1. TheHive[29]

Η πλατφόρμα TheHive είναι μια δωρεάν, επεκτάσιμη και ανοιχτού κώδικα πλατφόρμα αντιμετώπισης περιστατικών ασφαλείας (Security Incident Response Platform). Είναι ενοποιημένο με το MISP (Malware Information Sharing Platform) και έχει σχεδιαστεί για να διευκολύνει τη ζωή των SOC, CSIRT, CERT και κάθε επαγγελματία ασφάλειας πληροφοριών που ασχολείται με περιστατικά ασφάλειας που πρέπει να διερευνηθούν και να αντιμετωπιστούν γρήγορα. Αν και δεν πωλείται ρητά ως SOAR, έχει όλα τα στοιχεία για να λειτουργήσει ως τέτοιο.

Διατίθεται σε δωρεάν έκδοση (Community) καθώς και σε δύο επί πληρωμή εκδόσεις (Gold και Platinum).



Εικόνα 7. Διαθέσιμες εκδόσεις TheHive.

Το Thehive έχει δύο βασικά στοιχεία, το Thehive που θα λειτουργήσει ως orchestrator και το Cortex που θα χειριστεί όλη την ανάλυση και την αυτόματη απόκριση. Επειδή είναι ένα

[29] TheHive, https://thehive-project.org/ , Accessed on: Feb 24, 2023.

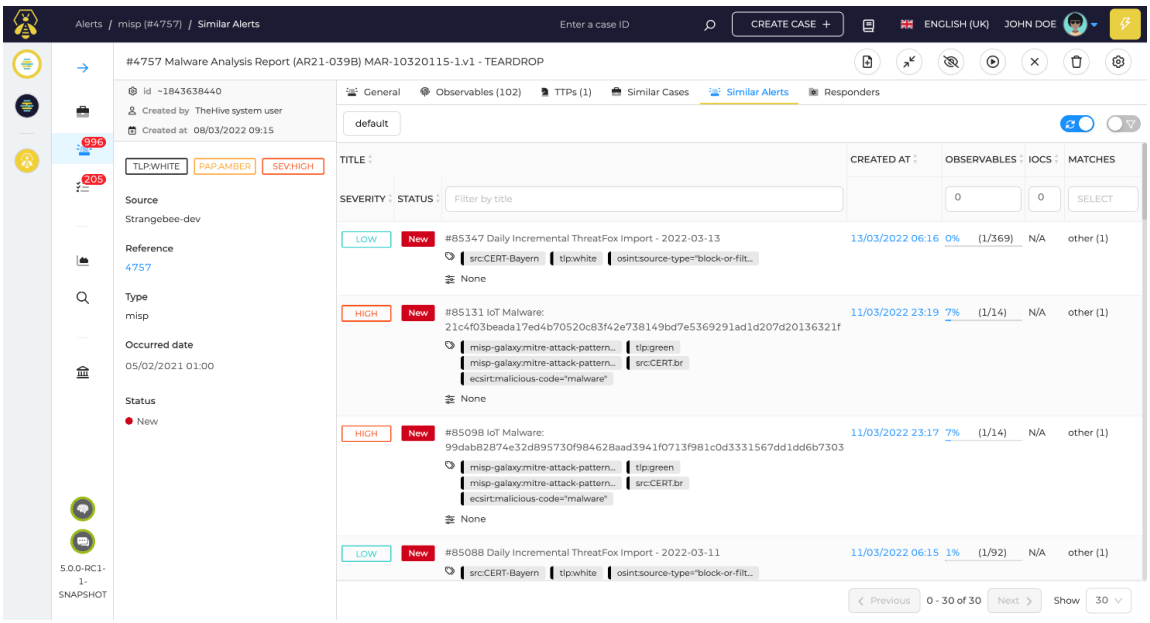
εργαλείο ανοιχτού κώδικα, δεν έχει τον προϋπολογισμό των εργαλείων premium και αυτό έχει αντίκτυπο στο τελικό προϊόν, καθώς η αυτοματοποίηση δεν είναι τόσο εύκολη και απλή όσο με τα premium εργαλεία.

Από την άλλη πλευρά, το ότι είναι ένα εργαλείο ανοιχτού κώδικα θα μπορούσε να μας επιτρέψει να το τροποποιήσουμε και να προσθέσουμε λειτουργίες σε αυτό με πιο απλό τρόπο. Επιπλέον, χάρη στο API μπορεί να αυτοματοποιηθεί σχεδόν οποιαδήποτε εργασία χρησιμοποιώντας απλά σενάρια python και τη βιβλιοθήκη που παρέχουν.

Παρόλο που είναι ένα πολύ πλήρες εργαλείο, είναι πολύ πιο δύσκολο να λειτουργήσει και απαιτεί περισσότερη επεξεργασία από τον χρήστη για να λειτουργήσει ως SOAR. Αυτό συμβαίνει γιατί σε αυτή την περίπτωση όλοι οι αυτοματισμοί γίνονται μέσω του API και πρέπει να κωδικοποιηθεί αντί να χρησιμοποιούνται απλές πλατφόρμες χωρίς κώδικα.

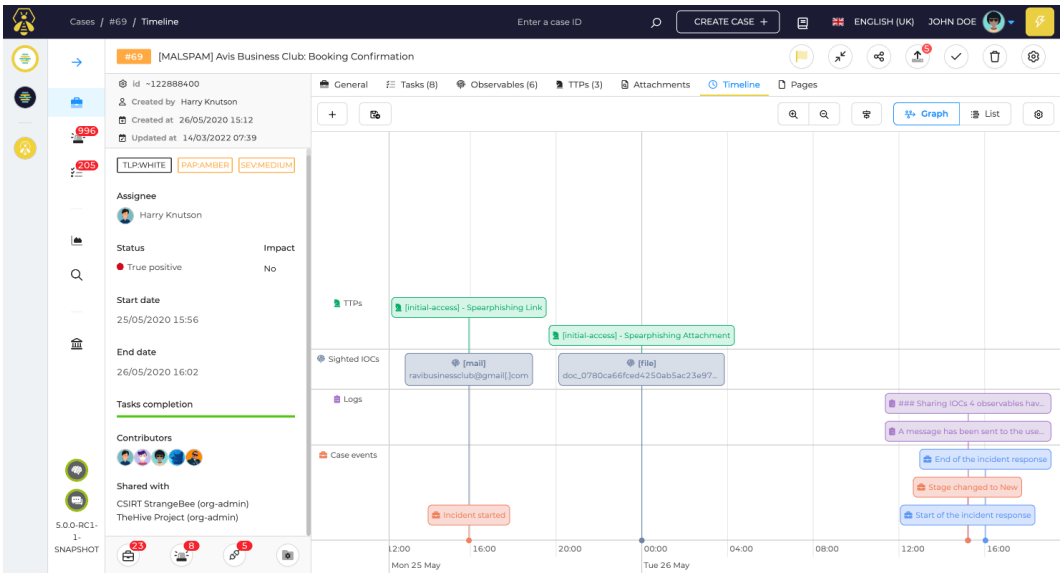
Τα κυριότερα χαρακτηριστικά που προσφέρει είναι:

- Alert management: Μπορεί κάποιος να μεταβεί στην ειδική και λεπτομερή σελίδα Alert, να κάνει σχόλια, να εντοπίσει παρόμοια alert, να ορίσει προσαρμοσμένες καταστάσεις και πεδία. Στη συνέχεια, μπορεί να αποφασίσει εάν θα πρέπει ή όχι να κλιμακωθούν σε investigation ή σε incident response.



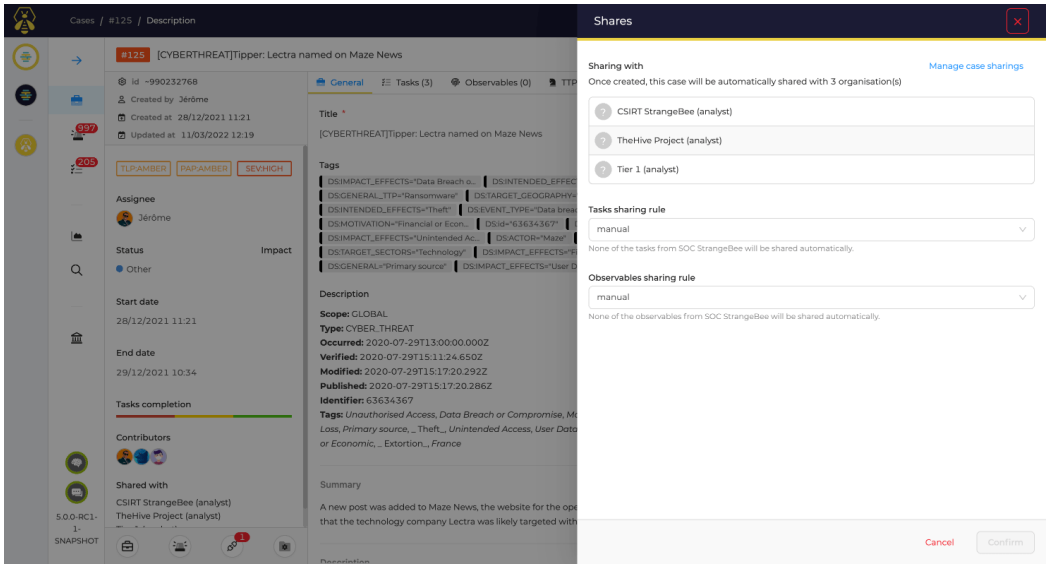
Εικόνα 8. Alerts στο TheHive.

- Case management: Είναι δυνατή η δημιουργία cases και σχετικών εργασιών.



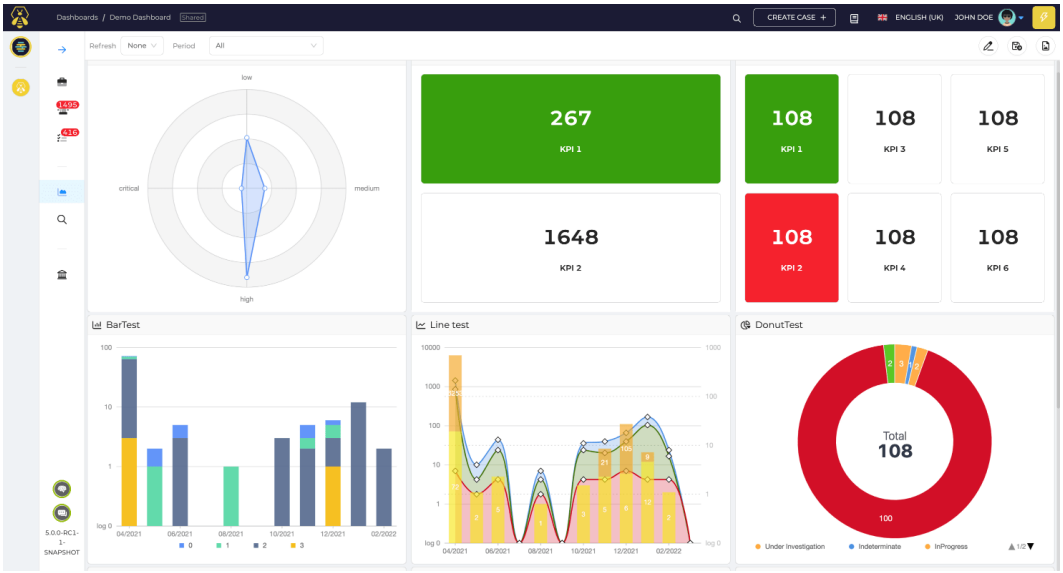
Εικόνα 9. Case management στο TheHive.

- Περιβάλλον Multi tenant: Μπορούν να προσδιοριστούν διαφορετικοί οργανισμοί και ομάδες και να εργαστούν με έναν αποκλειστικό ή συλλογικό τρόπο: τα cases των ξεχωριστών χρηστών μπορούν να απομονωθούν ή να διερευνηθούν από χρήστες από διαφορετικούς οργανισμούς με βάση προσαρμόσιμους ρόλους και δικαιώματα.



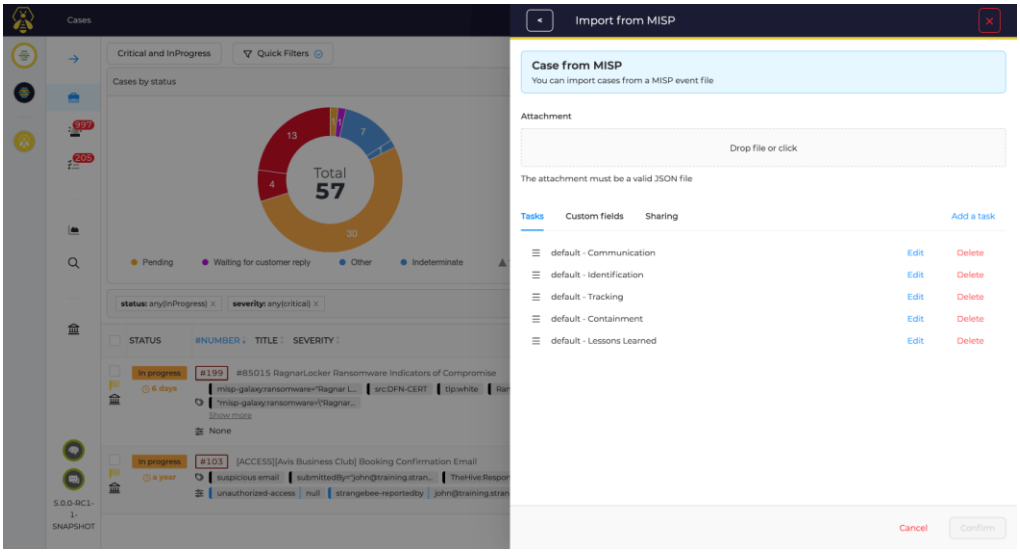
Εικόνα 10. Multi tenant περιβάλλον του TheHive.

- Dashboard και μετρήσεις: Παρέχει ένα δυναμικό dashboard μέσω του οποίου συγκεντρώνονται και συσχετίζονται στατιστικά στοιχεία για cases, εργασίες, παρατηρήσιμα στοιχεία, μετρήσεις και άλλα.

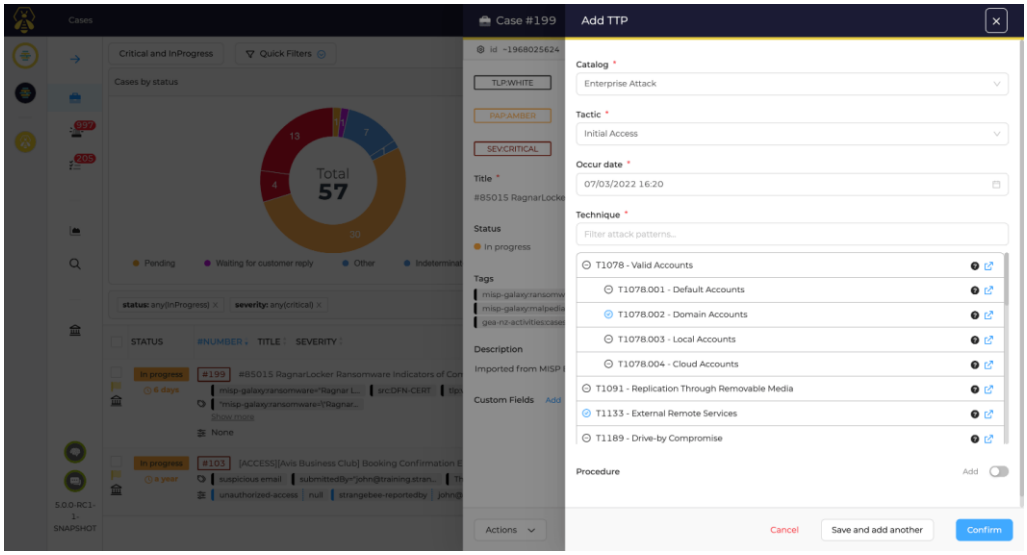


Εικόνα 11. Dashboard του TheHive.

- Ενοποίηση με το MISP και Mitre Att&ck: Συνδέοντας το TheHive με το MISP είναι δυνατή η λήψη και γρήγορη εισαγωγή κοινόχρηστων Indicator of compromise ή ο διαμοιρασμός των δικών μας εύκολα με τις κοινότητες στις οποίες ανήκουμε. Επίσης, είναι δυνατή η εισαγωγή όλων των TTP του MITER ATT&CK Framework στο TheHive Alert management.



Εικόνα 12. MISP Integration.



Εικόνα 13. Mitre Att&ck Integration.

Τα κυριότερα πλεονεκτήματα και μειονεκτήματα του Cortex XSOAR συνοψίζονται στον παρακάτω πίνακα.

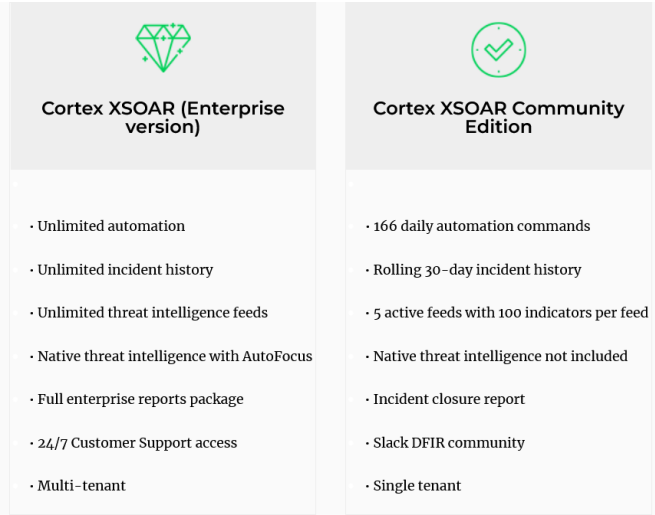
Μειονεκτήματα	Πλεονεκτήματα
Λιγότερο εύχρηστο	Υποστηρίζει πολλαπλούς χρήστες
Στην δωρεάν έκδοση δεν παρέχεται υποστήριξη	Αρκετά προσαρμόσιμο με API
Συμπεριλαμβάνει μόνο έναν οργανισμό στην δωρεάν έκδοση	Ενοποίηση με Cortex, MISP και Mitre Att&ck

5-2-2. Cortex XSOAR[30]

Το Cortex XSOAR είναι μια ισχυρή πλατφόρμα που διαθέτει ένα πλούσιο σύνολο χαρακτηριστικών και λειτουργιών που επιτρέπουν υψηλό βαθμό προσαρμογής.

Διατίθεται σε δωρεάν έκδοση Cortex XSOAR Community Edition με κάποιους περιορισμούς, καθώς και σε επί πληρωμή έκδοση Enterprise version. Οι διαφορές μεταξύ των δύο εκδόσεων φαίνονται στην παρακάτω εικόνα 14.

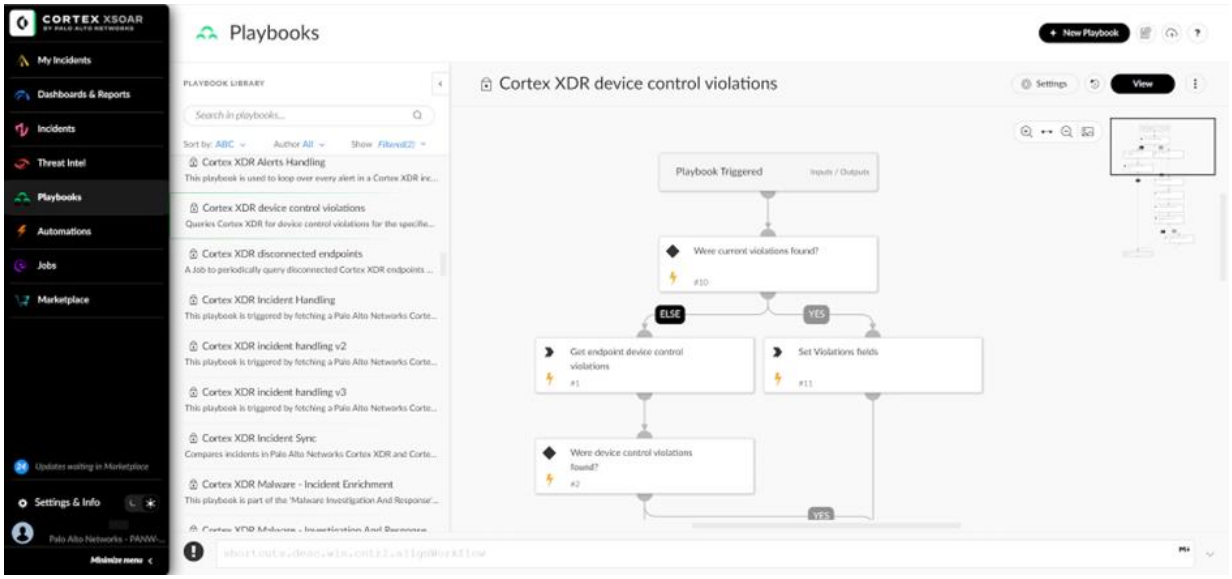
[30] Cortex XSOAR, https://www.paloaltonetworks.com/cortex/cortex-xsoar , Accessed on: Feb 24, 2023.



Εικόνα 14. Διαφορές Cortex XSOAR Enterprise και Community edition.

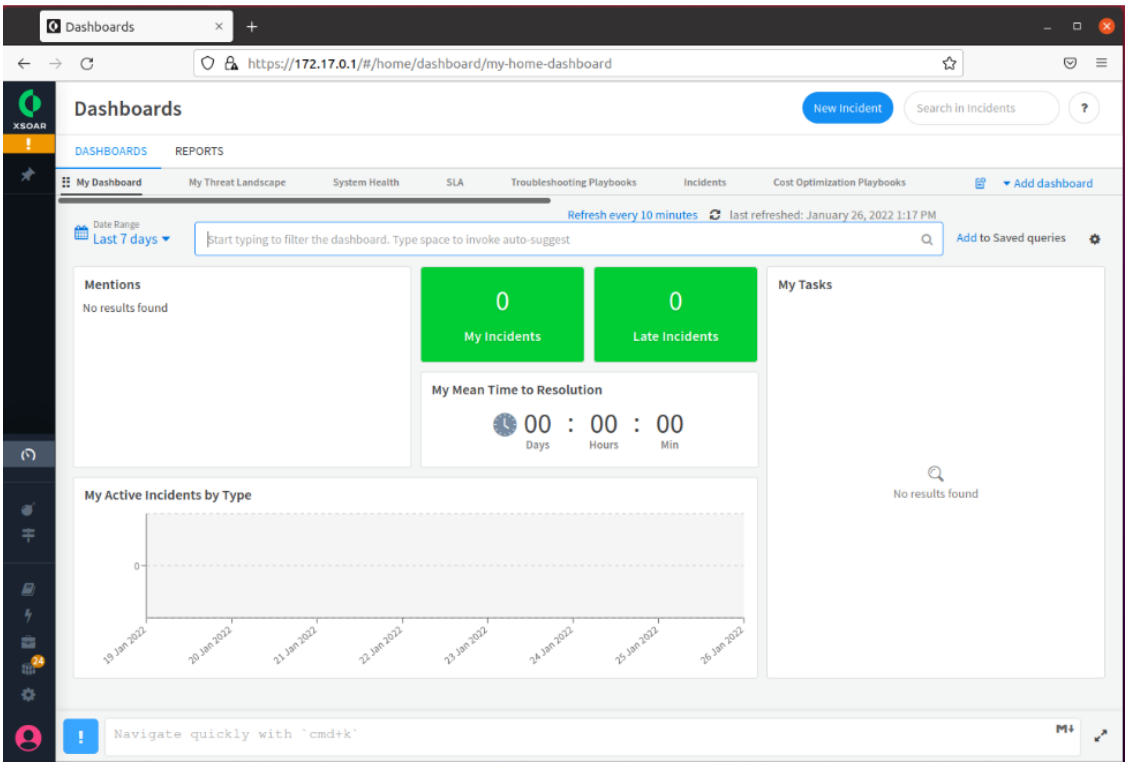
Το Cortex XSOAR μπορεί να αναπτυχθεί είτε στις εγκαταστάσεις του οργανισμού, είτε σε ιδιωτικό cloud ή ως μια πλήρως hosted λύση. Επίσης, διατίθεται και σαν εφαρμογή για κινητές συσκευές.

Μπορούμε να δούμε ότι, προσφέρει μια προβολή playbook που ενεργοποιείται όταν ένα περιστατικό ταιριάζει με ένα συγκεκριμένο κριτήριο και περιέχει ένα σύνολο βημάτων που πρέπει να ακολουθηθούν προκειμένου να μετριαστεί και να εμπλουτιστεί η γνώση του περιστατικού. Η community edition συνοδεύεται από μια μεγάλη γκάμα από προκαθορισμένα playbooks και πολλές ενσωματώσεις για τους πιο γνωστούς κατασκευαστές συστημάτων ασφαλείας.



Εικόνα 15. Cortex XSOAR Playbook view.

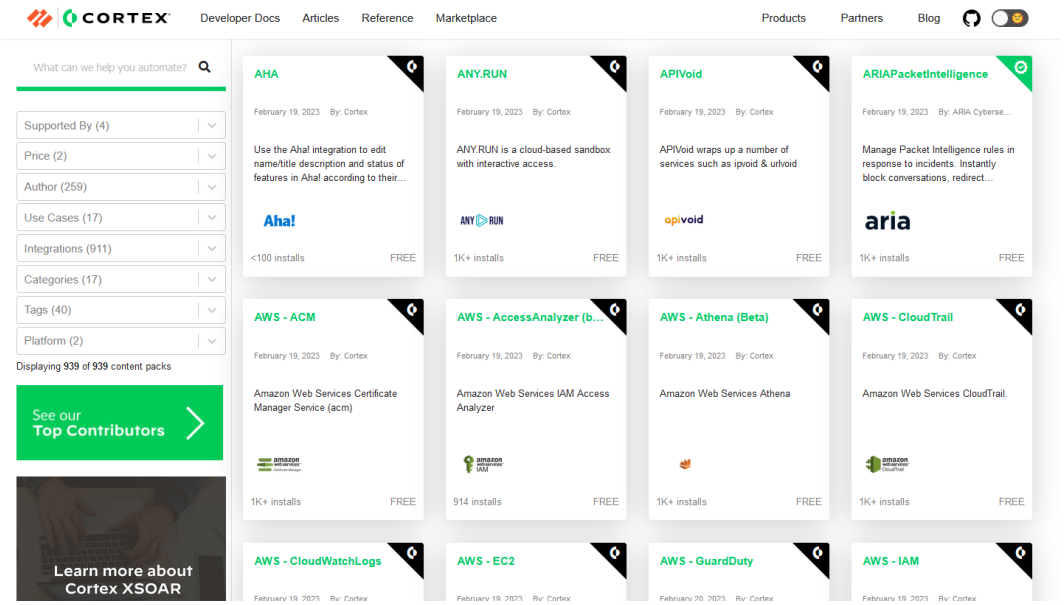
Περιέχει επίσης πολύ λεπτομερείς dashboard και οθόνη αναφορών που βοηθά να γίνεται κατανοητή η πραγματική κατάσταση του οργανισμού.



Εικόνα 16. Cortex XSOAR Dashboard.

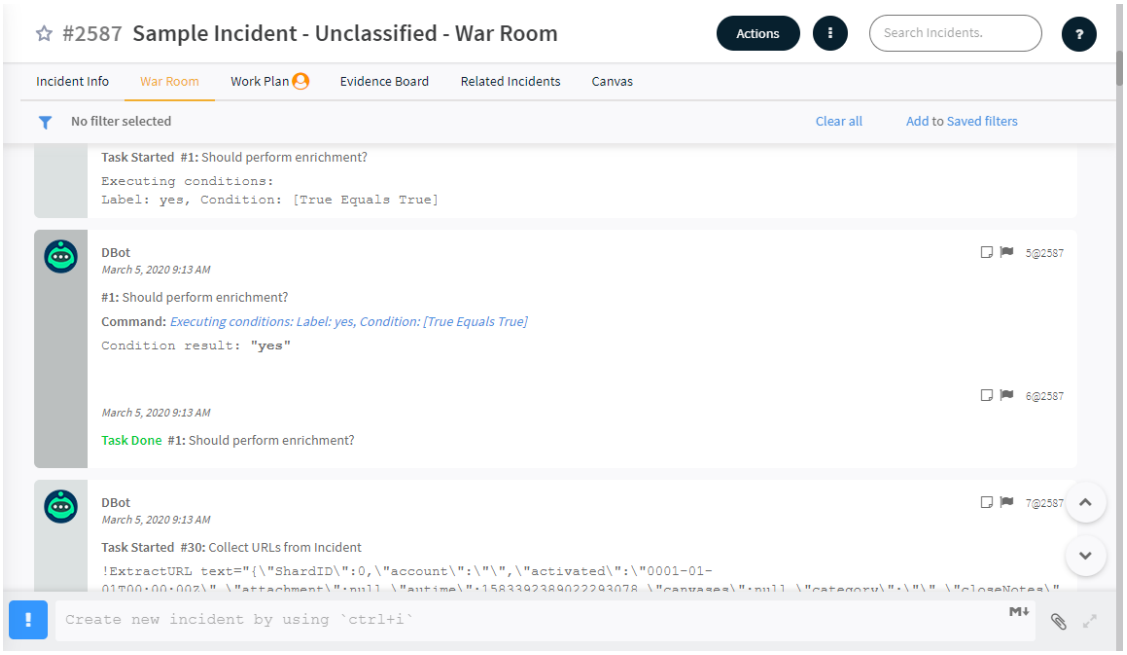
Ορισμένα μέρη του λογισμικού, για να είναι λειτουργικά, απαιτούνε την αγορά ανεξάρτητων λειτουργικών μονάδων, όπως η threat intelligence.

Διαθέτει ένα εύχρηστο Marketplace στην εφαρμογή που επιτρέπει στους χρήστες να προσθέτουν νέες ενσωματώσεις και λειτουργίες που αναπτύχθηκαν από την Palo Alto, τους προμηθευτές, τα μέλη της κοινότητας κλπ, καθιστώντας το ικανό να αλληλεπιδρά με σχεδόν οτιδήποτε χρειάζεται.



Εικόνα 17. Cortex XSOAR Marketplace

Στην war room του Cortex μπορούμε να δούμε εργασίες που έχουν ανατεθεί και εργασίες που έχουν ήδη εκπληρωθεί, ώστε να υπάρχει μια συνολική εικόνα για την υπόθεση.



Εικόνα 18. Cortex XSOAR War room.

Στους χρήστες της πλατφόρμας Cortex παρέχεται υποστήριξη από την Palo Alto, σύμφωνα με δύο πλάνα, ένα Standard και ένα Premium. Οι παρεχόμενες υπηρεσίες για κάθε πλάνο φαίνονται στην παρακάτω εικόνα 19.

	Summary Value	Standard Self-Help	Premium Optimized Experience
Onboarding Assistance	Customer journey kickoff	●	●
	Onboarding assistance		●
	Initial service configuration		●
	Use case assistance		●
Technical Support	Access to support community	●	●
	Access to Support Portal	●	●
	Telephone support		24/7
	Response time (S1)		< 1 hour
	Slack DFIR private channel		●
Education Training	Access to online documentation	●	●
	Access to online training	●	●
	Custom workshop		●
Optimized Experience	Annual health check	●	●
	Customized success plans		●
	Periodic operation reviews		●
	Executive business reviews		●
	Prioritized integration development		●

Εικόνα 19. Cortex XSOAR υποστήριξη πελατών.

Τα κυριότερα πλεονεκτήματα και μειονεκτήματα του Cortex XSOAR συνοψίζονται στον παρακάτω πίνακα.

Μειονεκτήματα	Πλεονεκτήματα
Περιορισμένος αριθμός χρηστών	Εξαιρετικές ενσωματώσεις και Marketplace
Συμπεριλαμβάνει μόνο έναν οργανισμό	Μεγάλη ποικιλία σε playbooks και API
Πολλές πρόσθετες λειτουργίες απαιτούν πληρωμή	Εύχρηστο playbook builder
Περιορισμένη υποστήριξη στην standard έκδοση	Ενσωματωμένο war room
	Εύχρηστο dashboard, playbook view και incidents view

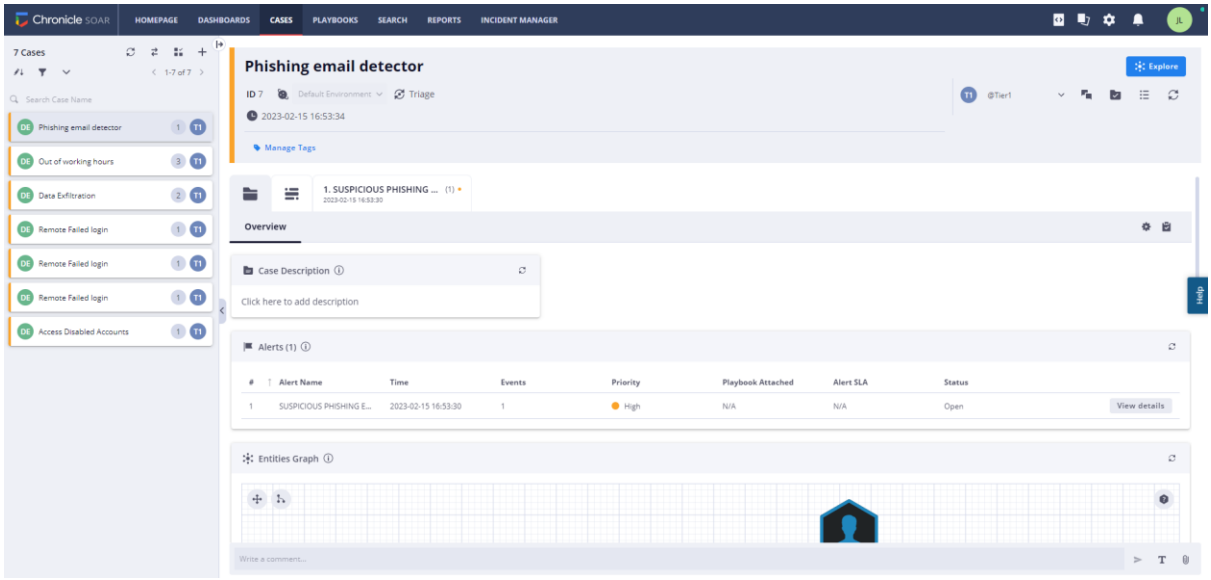
5-2-3. Chronicle SOAR[31]

Το Chronicle SOAR είναι η μετεξέλιξη του Siemplify, το οποίο εξαγοράστηκε από την Google το 2022. Επιτρέπει τη σύγχρονη, γρήγορη και αποτελεσματική απόκριση σε απειλές στον κυβερνοχώρο συνδυάζοντας την αυτοματοποίηση μέσω των playbooks, τη διαχείριση υποθέσεων και την ενοποίηση threat intelligence.

Το Chronicle SOAR αποτελεί μέρος της ολοκληρωμένης λύσης ασφαλείας της Google Chronicle Security Operations, η οποία είναι μια σουίτα που περιλαμβάνει SIEM, SOAR και Threat Intelligence. Παρέχεται κυρίως ως υπηρεσία Cloud-native, ενώ διατίθεται και on-premises με αρκετά αυξημένο κόστος. Για παράδειγμα, σύμφωνα με την AWS marketplace, μια βασική άδεια που δίνει πρόσβαση σε 2 χρήστες, 7 Playbooks, 5 συνδέσεις και 100 ημερήσιες ειδοποιήσεις θα κόστιζε 30.000$ ετησίως. Διατίθεται επίσης και σε δωρεάν έκδοση, με προεγκατεστημένα cases και αρκετές ενσωματώσεις.

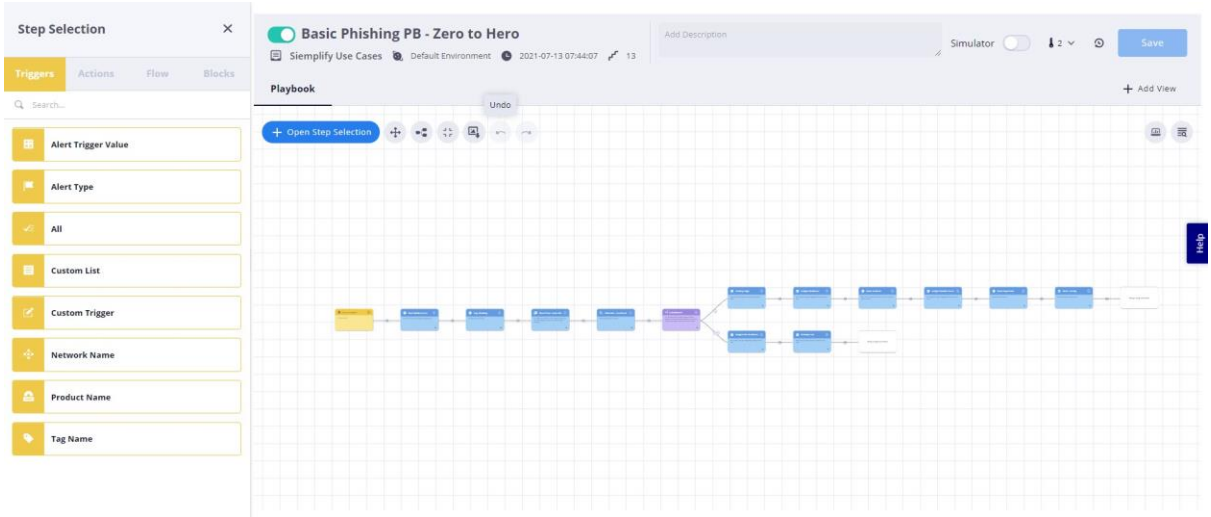
Στην πλατφόρμα, παρέχεται δυνατότητα διαχείρισης ανά συμβάν, μέσω της καρτέλας case management, από την οποία μπορεί να γίνει λήψη των δεδομένων, ομαδοποίηση, ιεράρχηση προτεραιοτήτων, εκχώρηση και διερεύνηση ειδοποιήσεων ασφαλείας από όλα τα εργαλεία ανίχνευσης. Η καρτέλα Cases παρέχει στους αναλυτές έναν τρόπο να διερευνήσουν τις εισερχόμενες ειδοποιήσεις ασφαλείας και να προστατέψουν τα workstations. Τα cases δημιουργούνται από ειδοποιήσεις από την πλατφόρμα SIEM. Επιπλέον, οι αναλυτές μπορούν να δημιουργήσουν μη αυτόματα και προσομοιωμένα cases και να λάβουν συγκεκριμένα δεδομένα. Η καρτέλα Cases εμφανίζει πληροφορίες σχετικές με το συμβάν. Οι εμφανιζόμενες πληροφορίες βασίζονται σε γραφικά στοιχεία που μπορούν να διαμορφωθούν από τον Administrator.

[31] SecOps Community Chronicle SOAR, https://chronicle.security/soar-free-edition/ , Accessed on: Feb 24, 2023.



Εικόνα 20. Cases Overview στο Chronicle SOAR.

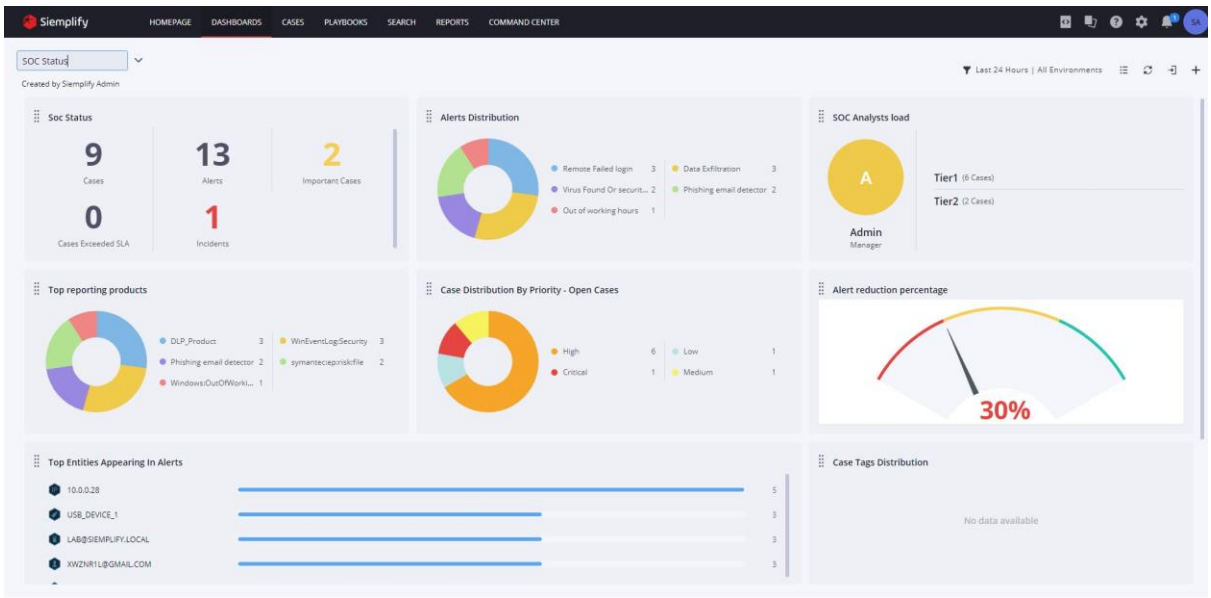
Με το Chronicle SOAR, μπορεί κανείς να δημιουργήσει εύκολα ή να χρησιμοποιήσει τα έτοιμα playbooks που αυτοματοποιούν επαναλαμβανόμενες εργασίες και τις διαδικασίες απόκρισης. Ένα playbook χτίζεται με triggers και ενέργειες/ροές. Μόλις ενεργοποιηθεί το συγκεκριμένο trigger, το playbook κινείται κατά μήκος των ενεργειών προς μια τελική ανάλυση. Η ροή του ελέγχου εκτελείται από τα αριστερά προς τα δεξιά ξεκινώντας με ένα καθορισμένο trigger (κίτρινο πλαίσιο) ως πρώτο στοιχείο, το οποίο είναι υποχρεωτικό. Στη συνέχεια, μετακινείται στο δεύτερο στοιχείο που μπορεί να είναι ένα σύνολο καθορισμένων ενεργειών που πρέπει να εκτελέσει το playbook (μπλε πλαίσιο). Το τελευταίο στοιχείο περιλαμβάνει τον προσδιορισμό της ροής του playbook με μια συνθήκη "If then… or else" (μωβ κουτί). Ένα παράδειγμα ενός playbook που αφορά τον εντοπισμό Phishing emails φαίνεται στην παρακάτω εικόνα.



Εικόνα 21. Playbook στο Chronicle SOAR.

Ο αναλυτής έχει την επιλογή να δοκιμάσει νέα playbooks στην πλατφόρμα μέσα σε έναν προσομοιωτή. Αυτό παρέχει δοκιμές alerts και cases, από τις οποίες ο χρήστης μπορεί να δοκιμάσει τη λειτουργικότητα του αυτοματισμού του. Όταν το playbook περάσει τη φάση του προσομοιωτή, στη συνέχεια τοποθετείται στο περιβάλλον παραγωγής.

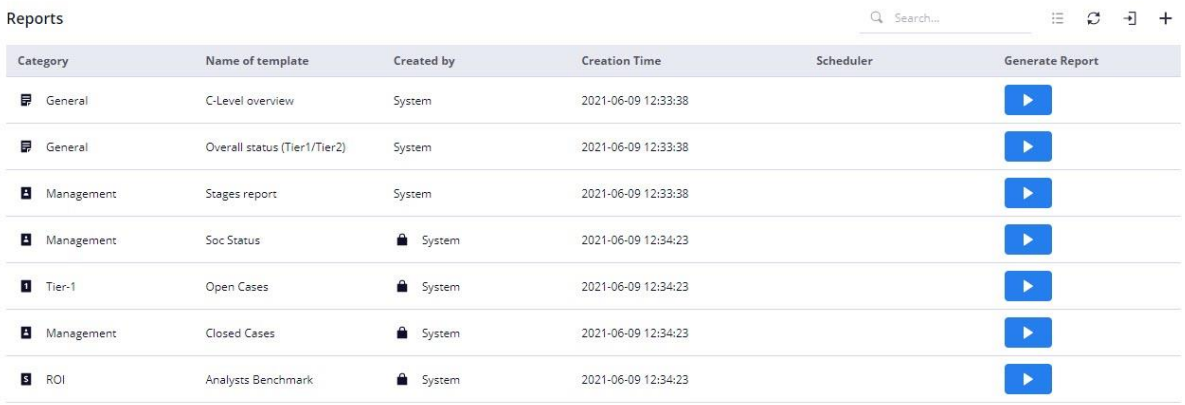
Η σελίδα Dashboards στην πλατφόρμα αποτελεί ένα ολοκληρωμένο και φιλικό προς τον χρήστη περιβάλλον το οποίο δίνει τη δυνατότητα στους αναλυτές να διαχειρίζονται πίνακες εργαλείων, δίνοντάς τους μια επισκόπηση των καθορισμένων δεδομένων σε διάφορες προβολές με τη μορφή γραφικών στοιχείων. Ένας πίνακας εργαλείων περιέχει έως και 12 γραφικά στοιχεία, τα οποία μπορούν να εμφανίζουν δεδομένα σε διάφορες μορφές, για οποιοδήποτε καθορισμένο περιβάλλον SOC.



Εικόνα 22. Dashboard του Chronicle SOAR.

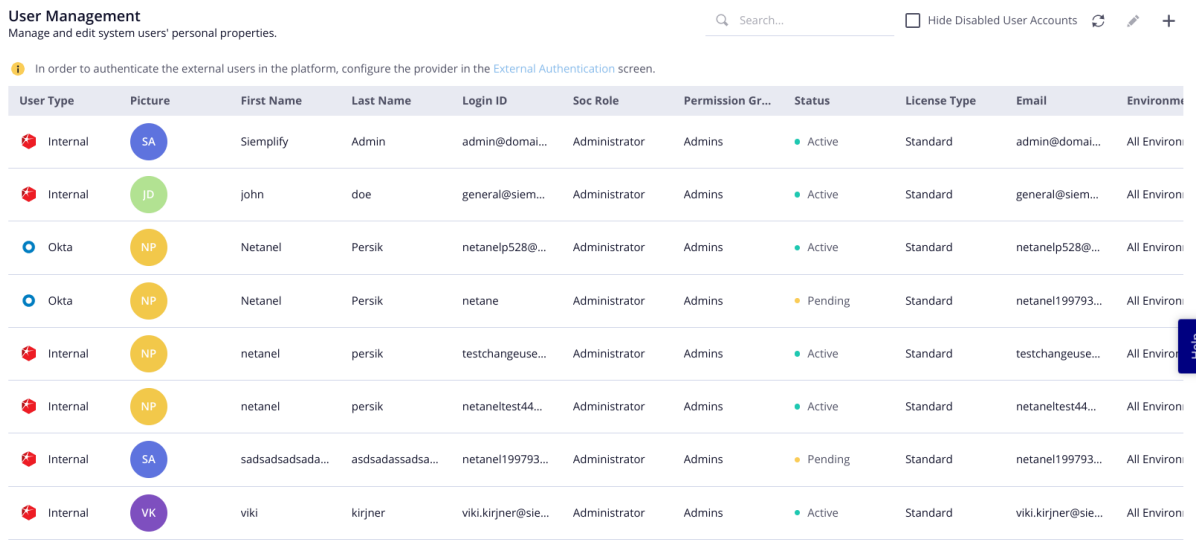
Το Chronicle SOAR παρέχει στους αναλυτές τέσσερις προκαθορισμένες αναφορές και την επιλογή δημιουργίας νέων. Μπορεί να γίνει εξαγωγή και να εισαχθούν Αναφορές σε άλλες πλατφόρμες. Οι προκαθορισμένες αναφορές που περιλαμβάνονται είναι:

- Management – SOC status
- Management – Closed Cases
- Tier 1 – Open Cases
- ROI – Analysts Benchmark



Εικόνα 23. Αυτόματες αναφορές από το Chronnicle SOAR.

Υπάρχουν διάφοροι τύποι χρηστών στην πλατφόρμα Chronicle SOAR και ο collaborator user είναι ένα υβρίδιο μεταξύ ενός βασικού χρήστη και ενός χρήστη view-only. Επίσης, πέρα από το Default περιβάλλον, μπορεί να γίνει προσθήκη κι άλλων. Αυτό είναι χρήσιμο για SOC που παρέχουν υπηρεσίες σε πολλά διαφορετικά δίκτυα, πελάτες ή επιχειρηματικές μονάδες εντός του οργανισμού.

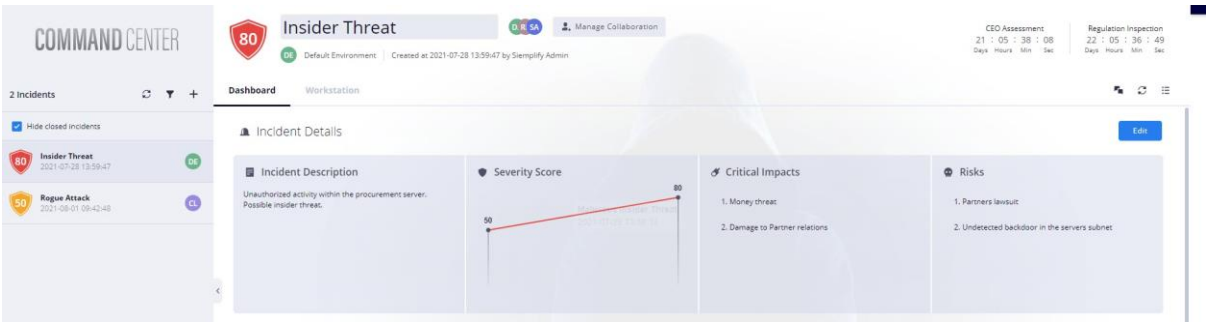


Εικόνα 24. User management στο Chronicle SOAR.

Παρέχεται επιπλέον ένα Command Center, το οποίο επιτρέπει την πρακτική διαχείριση περιστατικών και την συνεργασία από όλα τα αρμόδια τμήματα. Υπάρχουν δύο βασικοί τομείς του Command Center:

- **Workstations**, όπου όλοι οι ενεργοί collaborators χρήστες μπορούν να προσθέσουν updates, εργασίες, αποφάσεις, αξιολογήσεις της κατάστασης και άλλα

- **Dashboard** που περιλαμβάνει όλες τις σχετικές πληροφορίες συμβάντος.



Εικόνα 25. Command Center του Chronicle SOAR.

Για το Chronicle SOAR παρέχεται τεχνική υποστήριξη από την Google μέσω του Chronicle Support portal.

Τα κυριότερα πλεονεκτήματα και μειονεκτήματα του Chronicle SOAR συνοψίζονται στον παρακάτω πίνακα.

Μειονεκτήματα	Πλεονεκτήματα
Νεότερο προϊόν	Συμβατό με προϊόντα Google Security
Μικρή κοινότητα και λίγοι χρήστες	Εύχρηστο περιβάλλον και αναλυτικό documentation για την χρήση του.
Στην δωρεάν έκδοση υπάρχουν περιορισμοί στον αριθμό χρηστών, στο multi tenancy περιβάλλον και στον αριθμό χρήσης cases και playbooks.	Ενσωματωμένο Command Center
	Παρέχει έτοιμα playbooks καθώς και δυνατότητα ανάπτυξης νέων
	Υπάρχει Marketplace που διαθέτει Integratons, Power-ups και Analytics.

5-2-4. Shuffle[32]

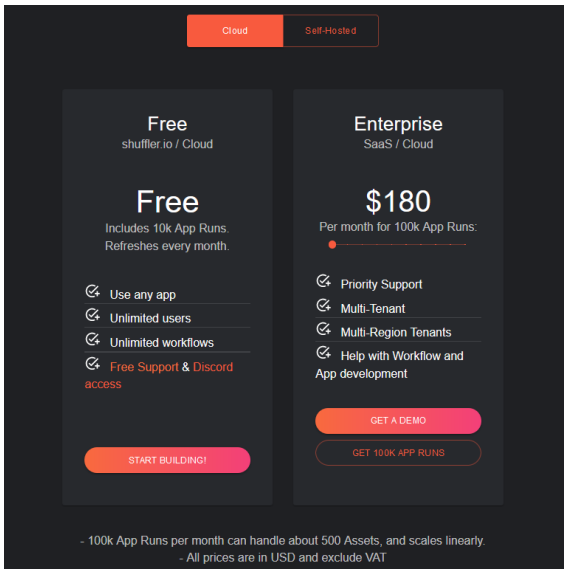
Το Shuffle ξεκίνησε ως project στα μέσα του 2019. Οι διαθέσιμες λύσεις αυτοματισμού στον κλάδο της ασφάλειας προσπαθούν να κάνουν τα πάντα ταυτόχρονα σε μια ενιαία πλατφόρμα, ενώ στόχος του Shuffle είναι να δημιουργήσει την καλύτερη λύση για να ενοποιήσει όλα τα υπάρχοντα εργαλεία.

Η πλατφόρμα Shuffle SOAR προσφέρει ένα ευρύ φάσμα λειτουργιών για να βοηθήσει τους οργανισμούς να αυτοματοποιήσουν τις διαδικασίες ασφαλείας τους, όπως αυτοματοποίηση incident response, συγκέντρωση πληροφοριών απειλών, αυτοματοποιημένη ανίχνευση και αποκατάσταση απειλών, αναλύσεις και αναφορές ασφαλείας. Περιλαμβάνει

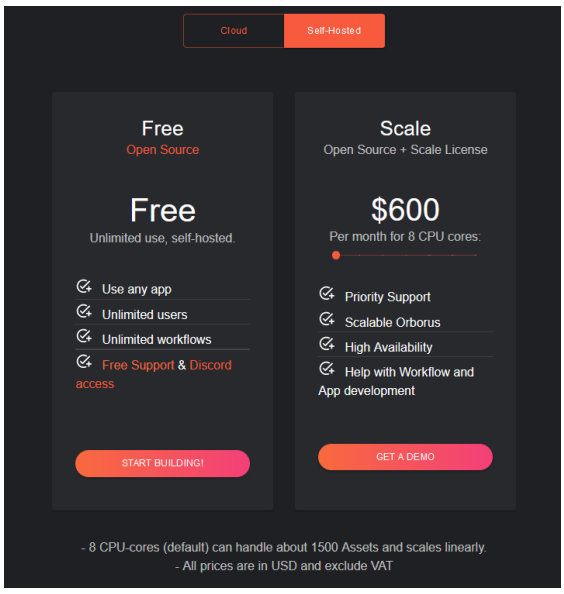
[32] Shuffle, https://shuffler.io/ , Accessed on: Feb 24, 2023.

επίσης ενοποιήσεις με διάφορα εργαλεία και υπηρεσίες ασφαλείας, όπως SIEM, threat intelligence feeds και εργαλεία endpoint protection, ενώ είναι αρκετά εύχρηστο.

Εκτός από τη δωρεάν έκδοση, υπάρχουν και εκδόσεις του Shuffle επί πληρωμή που προσφέρουν επιπλέον δυνατότητες και με τα έσοδα από αυτές χρηματοδοτείται η ανάπτυξη του προϊόντος. Η ανάπτυξη αφορά κυρίως self-hosted πλατφόρμα αλλά παρέχεται επίσης και στο cloud. Το κόστος των διαφορετικών εκδόσεων ποικίλει αναλόγως της επιλογής που αρμόζει στην κάθε ανάγκη, και πολλαπλασιάζεται αναλόγως των Apps runs. Ενδεικτικά το κόστος φαίνεται στις εικόνες 26 και 27.

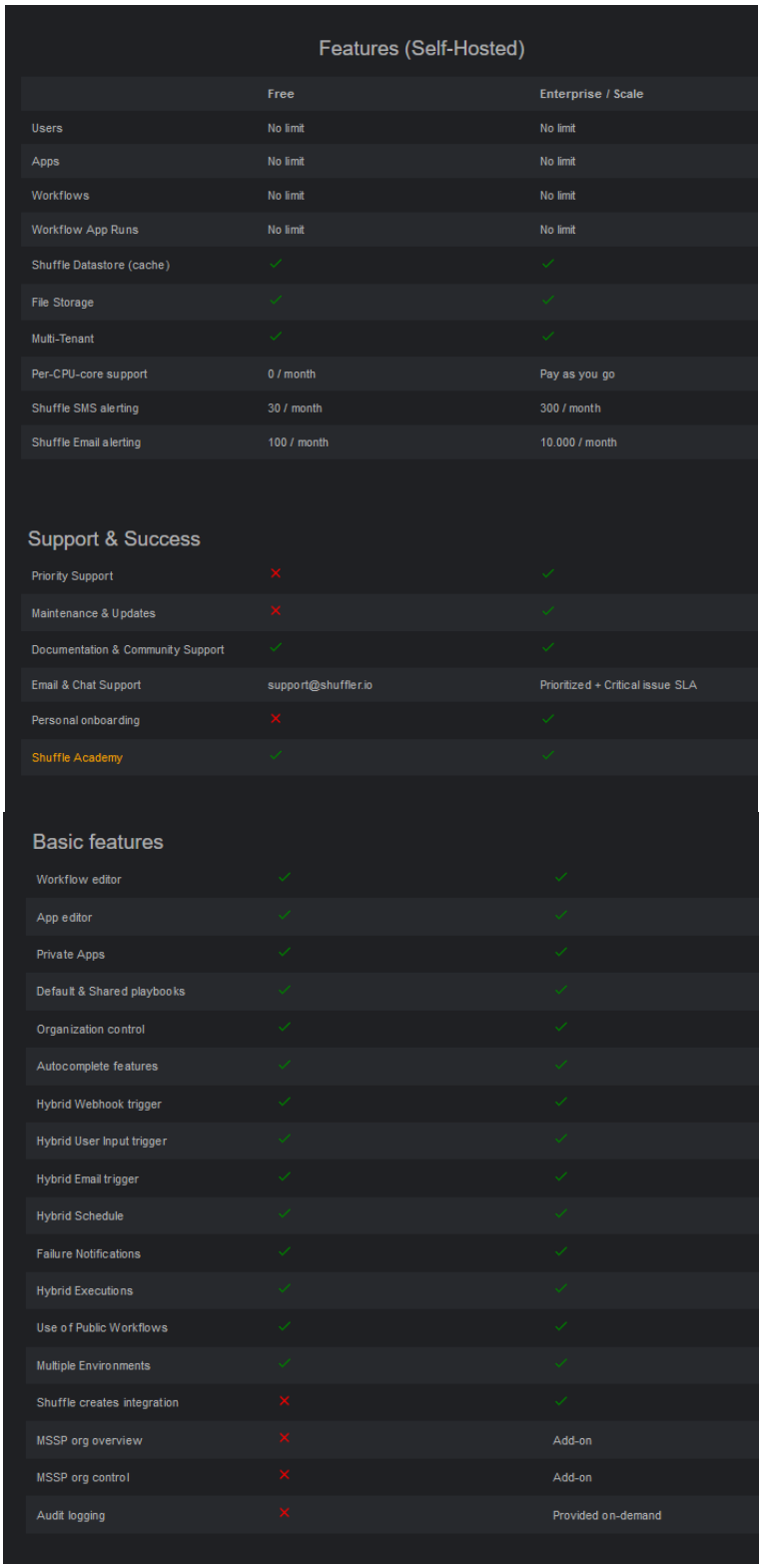


Εικόνα 26. Κόστος Shuffle στο cloud.



Εικόνα 27. Κόστος Shuffle self-hosted.

Τα χαρακτηριστικά κάθε έκδοσης φαίνονται στην παρακάτω εικόνα 28.



Features (Self-Hosted)

	Free	Enterprise / Scale
Users	No limit	No limit
Apps	No limit	No limit
Workflows	No limit	No limit
Workflow App Runs	No limit	No limit
Shuffle Datastore (cache)	✓	✓
File Storage	✓	✓
Multi-Tenant	✓	✓
Per-CPU-core support	0 / month	Pay as you go
Shuffle SMS alerting	30 / month	300 / month
Shuffle Email alerting	100 / month	10.000 / month

Support & Success

Priority Support	✗	✓
Maintenance & Updates	✗	✓
Documentation & Community Support	✓	✓
Email & Chat Support	support@shuffler.io	Prioritized + Critical issue SLA
Personal onboarding	✗	✓
Shuffle Academy	✓	✓

Basic features

Workflow editor	✓	✓
App editor	✓	✓
Private Apps	✓	✓
Default & Shared playbooks	✓	✓
Organization control	✓	✓
Autocomplete features	✓	✓
Hybrid Webhook trigger	✓	✓
Hybrid User Input trigger	✓	✓
Hybrid Email trigger	✓	✓
Hybrid Schedule	✓	✓
Failure Notifications	✓	✓
Hybrid Executions	✓	✓
Use of Public Workflows	✓	✓
Multiple Environments	✓	✓
Shuffle creates integration	✗	✓
MSSP org overview	✗	Add-on
MSSP org control	✗	Add-on
Audit logging	✗	Provided on-demand

Εικόνα 28. Βασικά χαρακτηριστικά free και enterprise edition του Shuffle.

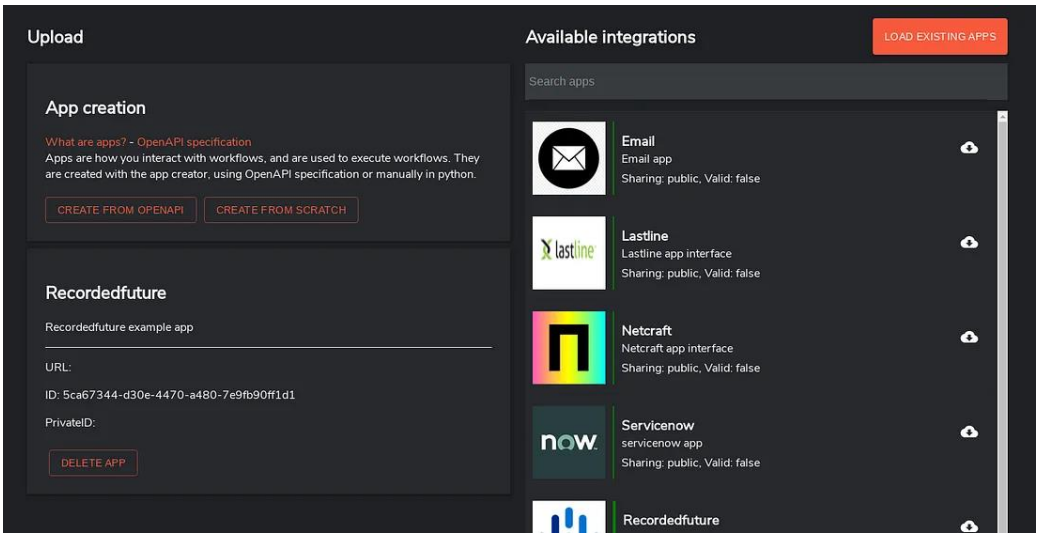
Εικόνα 29. Πρόσθετα χαρακτηριστικά free και enterprise edition του Shuffle.

Ένα βασικό μειονέκτημα είναι ότι δεν παρέχεται προς το παρόν Dashboard και reporting με την δωρεάν έκδοση, ενώ αυτό έχει προβλεφθεί να παρέχεται σε μελλοντική έκδοση.

Ωστόσο, παρέχονται χωρίς περιορισμό πληθώρα Use cases, Apps και Workflows που επιτρέπουν την διασύνδεση με άλλα εργαλεία, ενώ επίσης υπάρχει και ένας workflow editor και openAPI creator όπου ο χρήστης μπορεί να δημιουργήσει πολύ εύκολα δικά του workflows και APIs.

Εικόνα 30. Workflows στο Shuffle.

Το Shuffle διαθέτει κεντρικό αποθετήριο για αποθήκευση όλων των δεδομένων και των αρχείων (Shuffle Datastore και File Storage). Επίσης υπάρχει η δυνατότητα για multi tenant περιβάλλον στην δωρεάν μάλιστα έκδοση.

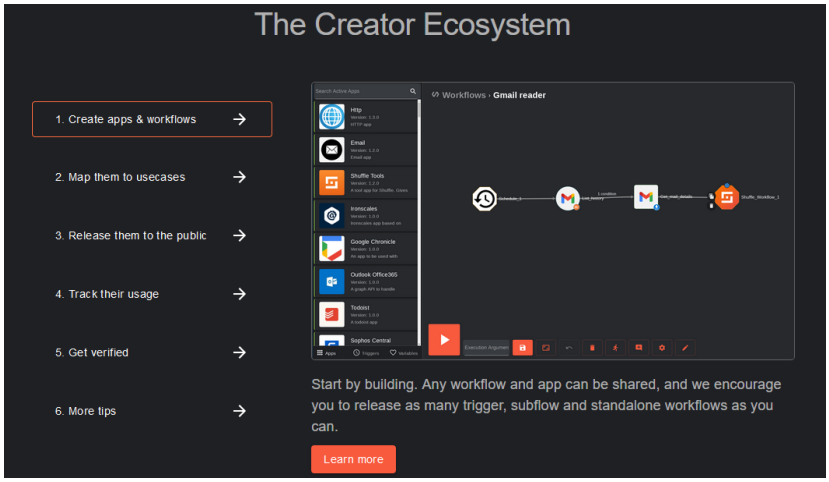


Εικόνα 31. App creation στο Shuffle.

Στην μελλοντική έκδοση Enterprise θα παρέχεται σύνδεση με το MITRE ATT&CK καθώς και SIEM, Reporting και Dashboards.

Στους χρήστες της Enterprise έκδοσης παρέχεται πλήρης υποστήριξη μέσω SLA (service-level agreement) ενώ στην δωρεάν έκδοση παρέχεται υποστήριξη είτε από τον δημιουργό μέσω email ή μέσω ιστοσελίδας (https://github.com/frikky/Shuffle/issues/new, https://shuffler.io/contact) ή από την κοινότητα που διατηρεί κανάλια στο Discord και στο Twitter.

Υπάρχει επίσης η δυνατότητα να συμμετέχει κάποιος ως creator συνεισφέροντας στην ανάπτυξη της πλατφόρμας και δημιουργώντας apps, workflows ή usecases.



Εικόνα 32. Creator Ecosystem στο Shuffle.

Τα κυριότερα πλεονεκτήματα και μειονεκτήματα της πλατφόρμας Shuffle φαίνονται στον παρακάτω πίνακα.

Μειονεκτήματα	Πλεονεκτήματα
Δεν διαθέτει προς το παρόν Dashboard και Reporting, ενώ αναμένεται να διατεθεί σε μελλοντική έκδοση.	Υλοποίηση είτε στο Cloud ή Self-hosted.
	Διαθέτει Use cases, Apps και Workflows χωρίς περιορισμό και στην δωρεάν έκδοση.
	Δυνατότητα δημιουργίας από τον χρήστη Use cases, Apps και Workflows.
	Υποστήριξη από την κοινότητα και τον δημιουργό.
	Χαμηλό κόστος για την Enterprise έκδοση.
	Αρκετά εύχρηστο.
	Δυνατότητα ενοποίησης με SIEM, threat intelligence feeds και άλλα εργαλεία.

5-3. Σύγκριση – πρόταση

Κατά τη σύγκριση συστημάτων SOAR ανοιχτού κώδικα, είναι σημαντικό να λαμβάνονται υπόψη οι συγκεκριμένες ανάγκες του οργανισμού, όπως ο αριθμός των εργαλείων ασφαλείας που θα πρέπει να ενοποιηθούν, το επίπεδο προσαρμογής που απαιτείται και το επίπεδο υποστήριξης που απαιτείται. Αξίζει επίσης να σημειωθεί ότι ορισμένα από αυτά τα SOAR ανοιχτού κώδικα έχουν μια μεγάλη κοινότητα προγραμματιστών και χρηστών που μπορούν να παρέχουν υποστήριξη, documentation και σεμινάρια που μπορεί να είναι επωφελή για έναν οργανισμό.

Όλα τα συστήματα SOAR ανοιχτού κώδικα που είδαμε παραπάνω είναι εξαιρετικά προσαρμόσιμα και μπορούν να ενοποιηθούν με ένα ευρύ φάσμα εργαλείων και πλατφορμών ασφαλείας. Μπορούν επίσης να επεκταθούν και να προσαρμοστούν ανάλογα οι λειτουργίες τους και μπορεί να είναι μια καλή επιλογή για οργανισμούς με περιορισμένους προϋπολογισμούς.

Οι πλατφόρμες SOAR που είδαμε παραπάνω πληρούν ως επί το πλείστων τα ποιοτικά χαρακτηριστικά που θέσαμε στην αρχή του κεφαλαίου, η κάθε μια με τα δικά της πλεονεκτήματα και μειονεκτήματα. Διαθέτουν δωρεάν και επί πληρωμή εκδόσεις, υποστήριξη αναλόγως των αναγκών κάθε εταιρείας, διαθέτουν Dashboard, πληθώρα ενσωματώσεων, playbooks και workflows και άλλα πολλά που διαφοροποιούνται από πλατφόρμα σε πλατφόρμα ως προς τον τρόπο που παρέχονται και κοστολούνται. Ο κάθε οργανισμός μπορεί να επιλέξει την πλατφόρμα που ταιριάζει περισσότερο στις ανάγκες του.

Το Shuffle, παρόλο που δεν διαθέτει προς το παρόν Dashboard και Reporting, ως open source πλατφόρμα βρίσκεται συνεχώς υπό ανάπτυξη και σε επόμενη έκδοση αναμένεται να παρέχει περισσότερες λειτουργίες. Ωστόσο, είναι αρκετά εύκολο στη χρήση και διαθέτει αρκετές ενσωματώσεις, use cases, apps και workflows χωρίς περιορισμό στην δωρεάν έκδοση, ενώ είναι δυνατή επίσης η δημιουργία από τον χρήστη νέων με πολύ εύκολο τρόπο. Ακόμα και η enterprise έκδοση είναι αρκετά πιο οικονομική λύση σε σχέση με τις παροχές από άλλες πλατφόρμες και μπορεί να αποτελέσει λύση για αρκετούς οργανισμούς.

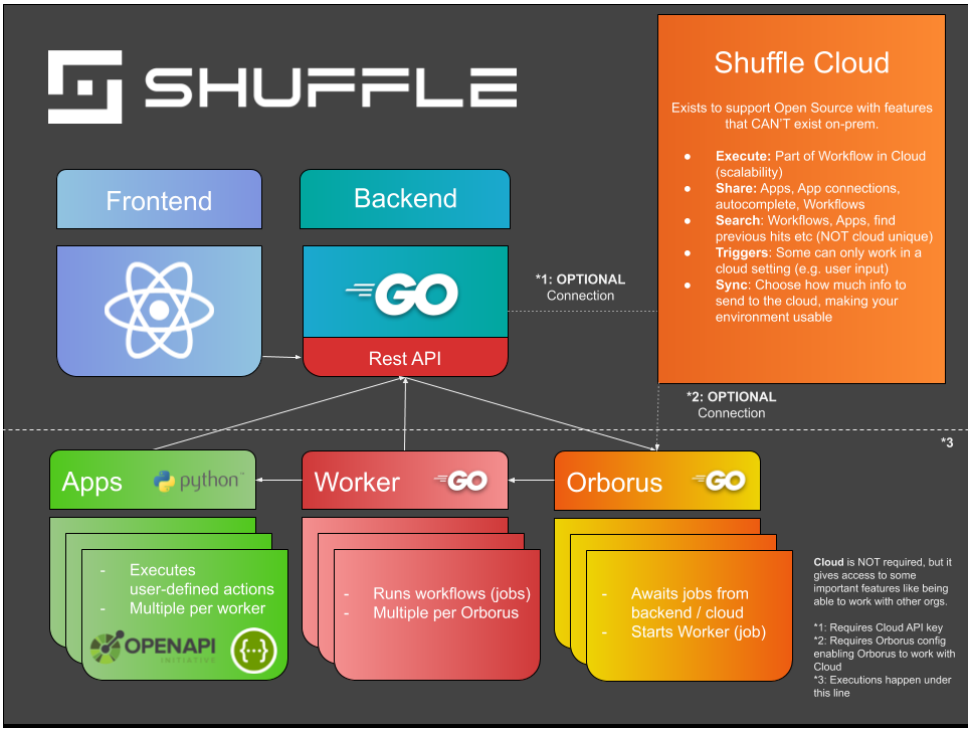
Στο επόμενο κεφάλαιο θα δούμε πιο αναλυτικά την υλοποίηση της πλατφόρμας Shuffle και θα πραγματοποιήσουμε ορισμένα use cases.

6. Shuffle

6-1. Εισαγωγή

Το Shuffle είναι μια πλατφόρμα SOAR ανοιχτού κώδικα, που μπορεί να αναπτυχθεί είτε σε Cloud μέσω του Google Cloud Functions ή On-premises, που προσφέρεται μέσω του Github χωρίς περιορισμό. Στόχος του είναι να προσφέρει όλες τις απαραίτητες δυνατότητες για τη μεταφορά δεδομένων σε μια επιχείρηση με εφαρμογές plug-and-play, καθιστώντας την αυτοματοποίηση προσιτή σε όλους. Δεν είναι αναγκαία η ύπαρξη ενός προγραμματιστή δίνοντας τη δυνατότητα σε όλους να μπορούν να αναπτύσσουν νέα, περίπλοκα (ή απλά) workflows σε λίγα λεπτά.

Η πλατφόρμα χωρίζεται σε δύο κύρια μέρη: Server και Workers. Ο Server λειτουργεί ως ο κεντρικός υπολογιστής των πάντων, από τη δραστηριότητα των API έως την επικύρωση των Workflow, ενώ οι Workers είναι μια άλλη αυτόνομη μονάδα, που λειτουργεί ως μικροϋπηρεσία.



Εικόνα 33. Αρχιτεκτονική Shuffle.

Τα θεμελιώδη δομικά στοιχεία του Shuffle είναι όλα σχεδιασμένα ώστε να είναι εικόνες Docker, που σημαίνει ότι μπορούν να εκτελούνται χωριστά σε διαφορετικά

περιβάλλοντα. Η παρακάτω λίστα περιέχει όλα τα απαραίτητα μέρη για την εκτέλεση ενός Workflow.[33]

Type	Technology	Note
Frontend	ReactJS	Cytoscape graphs & Material design
Backend	GolangRes	API that connects all the different parts
Database	Opensearch	A scalable, NoSQL database used as document store of everything
Orborus	Golang	Runs workers in a specific environment to connect locations
Worker	Golang	Deploys Apps to run Actions defined in a workflow
app sdk	Python	Used by Apps to talk to the backend

Για να γίνει χρήση του Shuffle, πρέπει να υπάρχουν έτοιμες ενσωματώσεις. Το Shuffle χρησιμοποιεί το OpenAPI και το πρότυπο Web API και δίνει πρόσβαση σε ένα πρόγραμμα builder για τη δημιουργία εφαρμογών. Στον ιστότοπο https://api.apis.guru/ υπάρχουν περισσότερες από 11.000 εφαρμογές του OpenAPI, κάτι το οποίο σημαίνει ότι μέσα σε λίγα λεπτά μπορεί κάποιος να δημιουργήσει στο Shuffle την ενοποίηση που επιθυμεί.

Τα Workflows είναι το μέρος του Shuffle όπου όλα ενώνονται. Χρησιμοποιώντας Apps, Triggers και Variables, το Shuffle δίνει πρόσβαση σε όλα τα εργαλεία που χρειάζονται για να επικοινωνούν οι διάφορες πλατφόρμες μεταξύ τους. Μια App έχει πολλαπλά Actions, οι οποίες με τη σειρά τους έχουν πολλαπλά Arguments. Τα Workflows είναι γραμμένα σε γλώσσα JSON.

Η πρόσβαση στα δεδομένα γίνεται ανά οργανισμό και ανά χρήστη. Αυτό σημαίνει ότι πρέπει να είναι κάποιος μέλος του οργανισμού από τον οποίο ζητάει δεδομένα. Ο διαχειριστής, έχει πρόσβαση σε όλες τις πληροφορίες ενός οργανισμού, ενώ οι χρήστες έχουν πρόσβαση μόνο στους δικούς τους πόρους και στις εφαρμογές που είναι ενεργοποιημένες. Οι κωδικοί των χρηστών κρυπτογραφούνται με AES-256. Η αυθεντικοποίηση των Apps και τα αρχεία κρυπτογραφούνται επίσης.

Υπάρχουν αρκετά βίντεο και οδηγίες για την εκμάθηση χρήσης του Shuffle τα οποία μπορεί να μελετήσει κανείς και βρίσκονται κυρίως στους ιστότοπους https://shuffler.io/docs[34] και https://medium.com/@Frikkylikeme[35].

[33] Shuffle Architecture, https://shuffler.io/docs/architecture , Accessed on: March 13, 2023.
[34] Shuffle documentation, https://shuffler.io/docs , Accessed on: March 13, 2023.
[35] Frikke, Blog for Shuffle https://medium.com/@Frikkylikeme , Accessed on: March 13, 2023.

6-2. Εγκατάσταση και έλεγχος του Shuffle

Η εγκατάσταση του Shuffle είναι προς το παρόν διαθέσιμη μόνο σε docker και ξεκινά χρησιμοποιώντας το docker-compose με τα στοιχεία διαμόρφωσης που βρίσκονται σε ένα αρχείο .env. Επομένως για την εγκατάσταση του Shuffle απαιτείται πρώτα να έχει γίνει εγκατάσταση των Docker και Docker-compose.

Η εγκατάσταση του Shuffle θα γίνει σε ένα VM Ubuntu 22.04 με IP 192.168.1.34.

Γίνεται λήψη του Shuffle από το Github με την εντολή

$ git clone https://github.com/frikky/Shuffle

```
nikos@nikos-virtual-machine:~$ sudo git clone https://github.com/frikky/Shuffle
Cloning into 'Shuffle'...
remote: Enumerating objects: 13285, done.
remote: Counting objects: 100% (311/311), done.
remote: Compressing objects: 100% (132/132), done.
remote: Total 13285 (delta 205), reused 277 (delta 179), pack-reused 12974
Receiving objects: 100% (13285/13285), 54.75 MiB | 1.12 MiB/s, done.
Resolving deltas: 100% (10159/10159), done.
nikos@nikos-virtual-machine:~$
```

Εικόνα 34. Λήψη του Shuffle από github.

Στην συνέχεια θα πρέπει να δημιουργήσουμε τις προαπαιτήσεις για την Opensearch database, μεταβαίνοντας στον φάκελο /Shuffle, δημιουργώντας το directory shuffle-database και τροποποιώντας το ownership σε guid:uid 1000:1000.

```
nikos@nikos-virtual-machine:~/Shuffle$ sudo mkdir shuffle-database
nikos@nikos-virtual-machine:~/Shuffle$ ls -la
total 96
drwxr-xr-x  9 root  root   4096 Μαρ  14 00:24 .
drwxr-x--- 16 nikos nikos  4096 Μαρ  14 00:20 ..
drwxr-xr-x  7 root  root   4096 Μαρ  14 00:21 backend
-rw-r--r--  1 root  root   3414 Μαρ  14 00:21 docker-compose.yml
-rw-r--r--  1 root  root   2706 Μαρ  14 00:21 .env
drwxr-xr-x  6 root  root   4096 Μαρ  14 00:21 frontend
drwxr-xr-x  5 root  root   4096 Μαρ  14 00:21 functions
drwxr-xr-x  8 root  root   4096 Μαρ  14 00:21 .git
drwxr-xr-x  4 root  root   4096 Μαρ  14 00:21 .github
-rw-r--r--  1 root  root    457 Μαρ  14 00:21 .gitignore
-rw-r--r--  1 root  root  34523 Μαρ  14 00:21 LICENSE
-rw-r--r--  1 root  root   5907 Μαρ  14 00:21 README.md
-rw-r--r--  1 root  root    934 Μαρ  14 00:21 SECURITY.md
drwxr-xr-x  2 root  root   4096 Μαρ  14 00:21 shuffle-apps
drwxr-xr-x  2 root  root   4096 Μαρ  14 00:24 shuffle-database
nikos@nikos-virtual-machine:~/Shuffle$ sudo chown -R 1000:1000 shuffle-database/
nikos@nikos-virtual-machine:~/Shuffle$
```

Εικόνα 35. Fix prerequisities for Opensearch database.

Εκτελούμε το docker-compose:

```
nikos@nikos-virtual-machine:~/Shuffle$ sudo docker-compose up -d
Creating network "shuffle_shuffle" with driver "bridge"
Pulling backend (ghcr.io/shuffle/shuffle-backend:latest)...
latest: Pulling from shuffle/shuffle-backend
c158987b0551: Pull complete
2bea3a8c2c53: Pull complete
bcdac01d8b80: Pull complete
4027ff5c317e: Pull complete
c61b452742c4: Pull complete
6530e6e102e5: Pull complete
15c78737a312: Pull complete
Digest: sha256:7acf157623c32e02635ce72565e56a9d6268b60c773da5fb496cb4660597220d
```

Εικόνα 36. Run docker-compose.

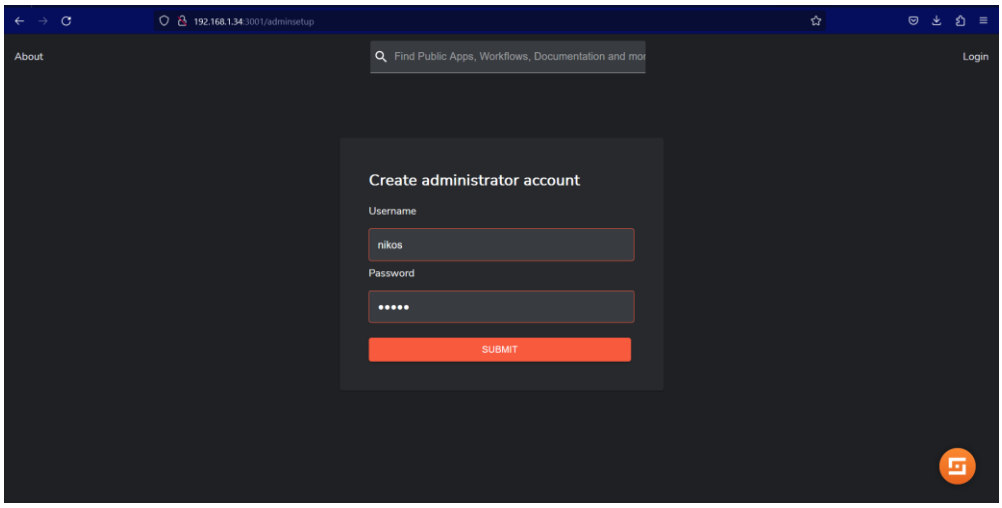
Τέλος, όπως προτείνεται από το Elasticsearch, για την καλή λειτουργία της opensearch database, θα πρέπει να αυξήσουμε το όριο των mmapfs counts ώστε να αποφύγουμε σφάλματα μνήμης[36]. Εκτελούμε την εντολή:

$ sudo sysctl -w vm.max_map_count=262144

```
Status: Downloaded newer image for opensearchproject/opensearch:2.4.0
Creating shuffle-opensearch ... done
Creating shuffle-backend    ... done
Creating shuffle-orborus    ... done
Creating shuffle-frontend   ... done
nikos@nikos-virtual-machine:~/Shuffle$ sudo sysctl -w vm.max_map_count=262144
vm.max_map_count = 262144
nikos@nikos-virtual-machine:~/Shuffle$
```

Εικόνα 37. Αύξηση vm max map counts.

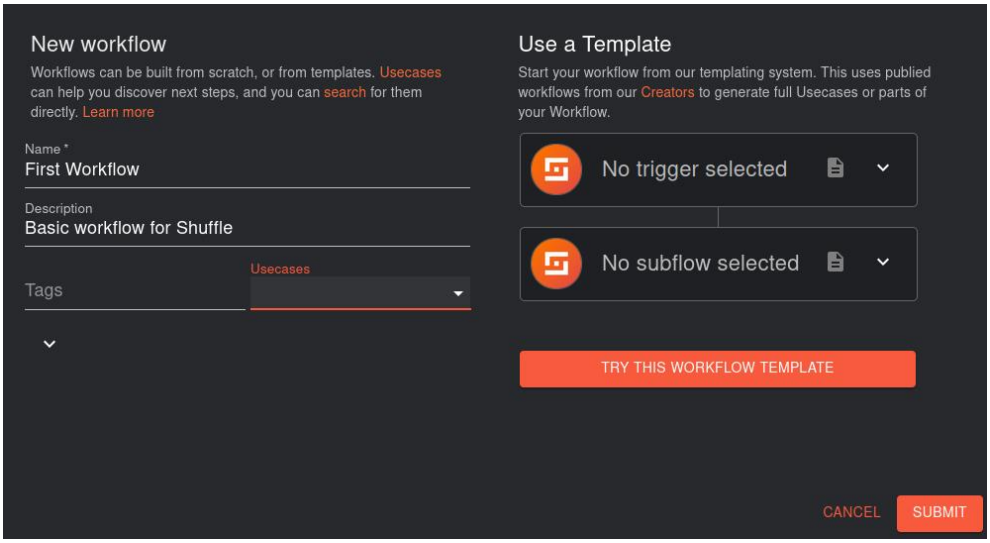
Για να μπούμε στο περιβάλλον του Shuffle, ανοίγουμε τον Browser και πληκτρολογούμε την IP του host όπου έχουμε εγκαταστήσει το Shuffle και την θύρα 3001 για http ή 3443 για https. Μόλις γίνει η πρώτη είσοδος στην εφαρμογή, μας ζητείται η δημιουργία λογαριασμού administrator.



Εικόνα 38. Είσοδος στο shuffle και δημιουργία λογαριασμού admin.

[36] Virtual memory, https://www.elastic.co/guide/en/elasticsearch/reference/current/vm-max-map-count.html , Accessed on: March 13, 2023.

Για να ελέγξουμε την ομαλή λειτουργία του Shuffle, θα δημιουργήσουμε ένα απλό Workflow. Στην κεντρική σελίδα Workflows, επιλέγουμε “New Workflow” και στην συνέχεια δίνουμε ένα όνομα και περιγραφή για το Workflow που θα δημιουργήσουμε και πατάμε Submit.

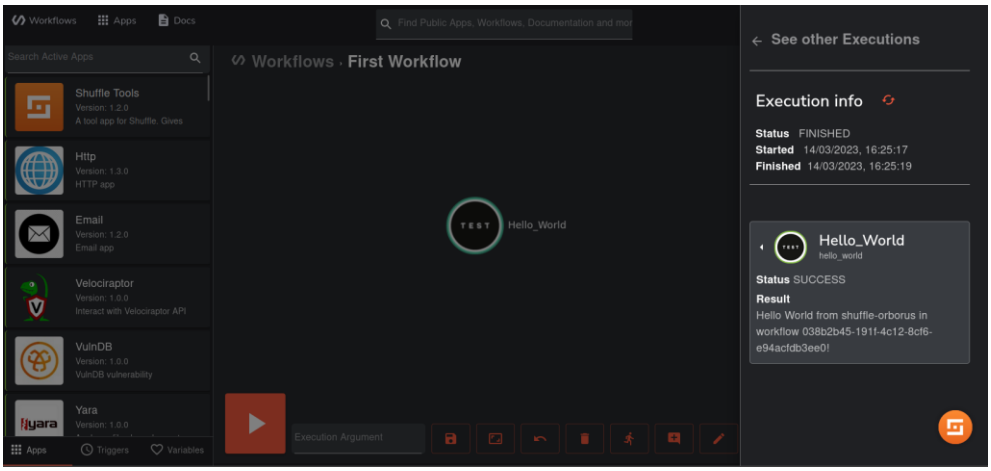


Εικόνα 39. Δημιουργία νέου Workflow.

Μετά το submit, βρισκόμαστε στην προβολή Workflow. Αυτή είναι μια κενή προβολή με μια δέσμη εφαρμογών στην αριστερή πλευρά. Θα δημιουργήσουμε τους εξής κόμβους (nodes):

- Ένας κόμβος "hello world". Αυτός θα είναι ο αρχικός μας κόμβος, δηλαδή η πρώτη ενέργεια που θα εκτελεστεί.
- Ένας κόμβος που επαναλαμβάνει δεδομένα από τον κόμβο “hello world”. Αυτό για να δείξουμε τα βασικά της μετάδοσης δεδομένων μεταξύ κόμβων.
- Ένας κόμβος που κάνει ένα http GET request με βάση το όρισμα εκτέλεσης, προσπαθώντας να αναλύσει την τιμή JSON "url".
- Ένας κόμβος που επιχειρεί να διαβάσει τα δεδομένα JSON από τον τρίτο κόμβο και να εκτυπώσει την IP που βρίσκει.
- Ένας scheduler. Αυτό θα κάνει το workflow να εκτελείται κάθε X δευτερόλεπτα με τα δεδομένα JSON {“url”: “https://ipv4.jsonip.com”}.

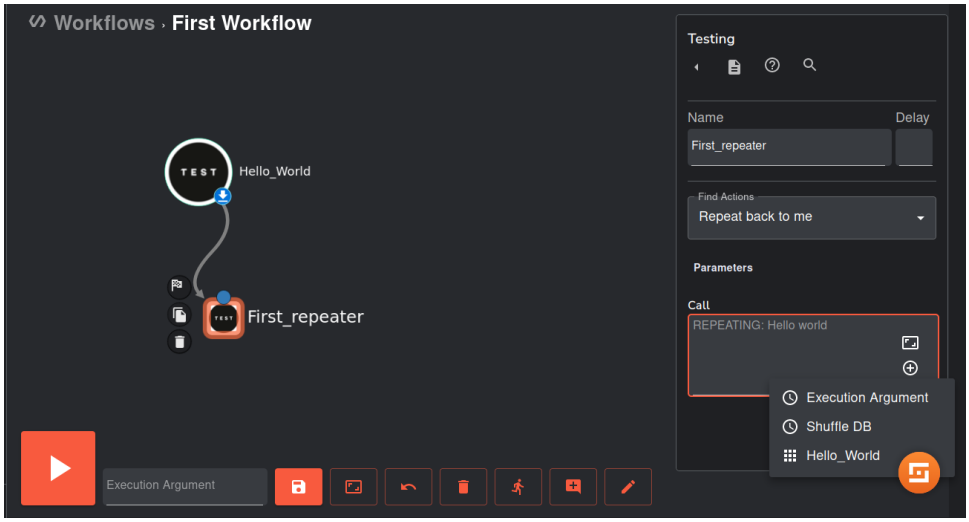
Από το μενού των App αριστερά, επιλέγουμε το Test App, το οποίο έχει ήδη ρυθμιστεί ως Action να εκτυπώνει το Hello World. Ονομάζουμε το workflow “Hello_world”, το αποθηκεύουμε και το εκτελούμε με το κουμπί “Test execution”. Στην παρακάτω εικόνα φαίνεται το επιτυχημένο αποτέλεσμα της εκτέλεσης.



Εικόνα 40. Εκτελώντας το πρώτο Workflow.

Στην συνέχεια προσθέτουμε άλλον ένα κόμβο ως Repeater node. Ο σκοπός του κόμβου Repeater είναι να δείξει πώς λειτουργεί η αλλαγή ενέργειας και η μετάδοση δεδομένων. Όταν σύρουμε τον δεύτερο κόμβο στο Workflow συνδέονται αυτόματα. Η διαφορά μεταξύ αυτών των κόμβων είναι ότι το μενού "Action" έχει αλλάξει από "Hello world" σε "Repeat back to me". Αυτή η συνάρτηση είναι χρήσιμη για τον εντοπισμό σφαλμάτων του αποτελέσματος που δίνει ένας κόμβος.

Ακολούθως, πρέπει να επιλέξουμε ποια δεδομένα θα επαναλάβουμε. Το "Repeat back to me" λαμβάνει μία μόνο παράμετρο, το "call", που είναι η τιμή που πρέπει να επαναληφθεί. Μπορούμε απλώς να γράψουμε κάτι στο πεδίο (π.χ. hello), ή μπορούμε να χρησιμοποιήσουμε δεδομένα από προηγούμενο κόμβο ή μεταβλητή. Κάνοντας κλικ στο εικονίδιο "+" μέσα στο πεδίο, θα εμφανίσει ένα αναπτυσσόμενο μενού. Αυτό το αναπτυσσόμενο μενού περιέχει όλες τις μεταβλητές στις οποίες έχουμε πρόσβαση, με βάση το τι είναι οι προηγούμενοι κόμβοι. Στην περίπτωσή μας, θέλουμε να επιλέξουμε το "Hello_world_node".

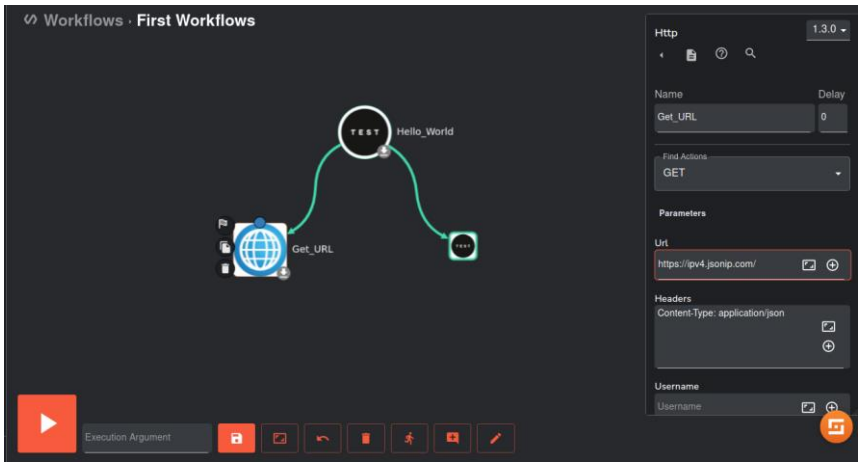


Εικόνα 41. Repeater node με επιλογή του προηγούμενου argument.

Για την συνέχεια θέλουμε να λάβουμε την δημόσια IP μας, δηλαδή θα πρέπει να την πάρουμε από εξωτερική πηγή. Αυτό μπορούμε να το κάνουμε από την υπηρεσία https://ipv4.jsonip.com/, η οποία επιστρέφει την IP με τη μορφή JSON.[37]

Για να υποβάλουμε ένα αίτημα GET, θα δοκιμάσουμε την εφαρμογή HTTP. Αυτή η εφαρμογή έχει σχεδιαστεί για να δοκιμάζει συνδέσεις με διαφορετικές υπηρεσίες και μπορεί να συνδυάσει όλες τις υπηρεσίες web μαζί. Υποστηρίζει όλες τις λειτουργίες του HTTP — GET, POST, PUT, DELETE.. — μαζί με τη δυνατότητα απευθείας εκτέλεσης curl.

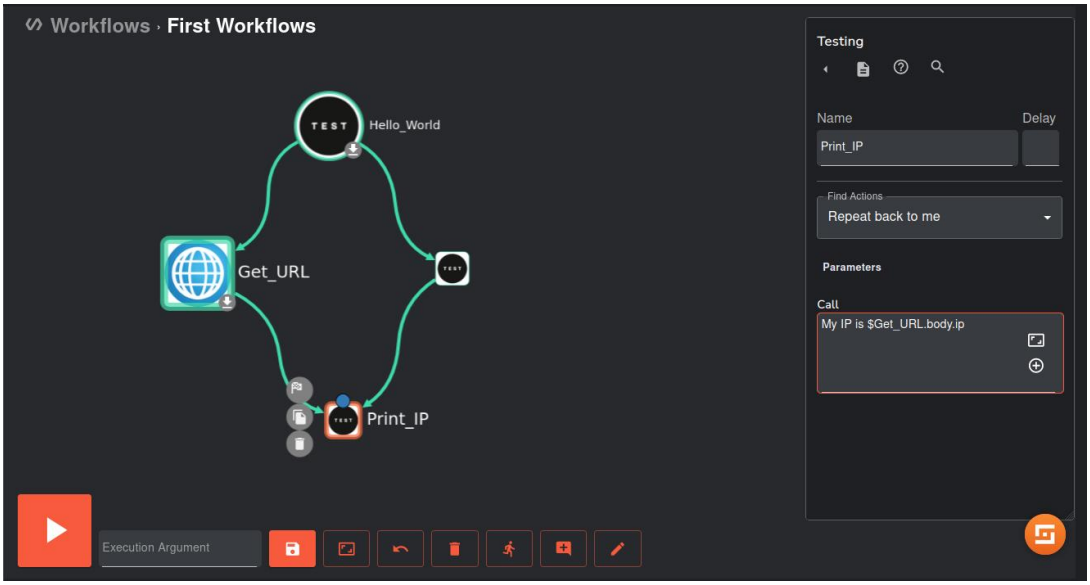
Εισάγουμε την εφαρμογή HTTP, την ονομάζουμε “Get URL” και την συνδέουμε με τον πρώτο κόμβο. Ο πρώτος κόμβος συνδέεται τόσο με τον “First_Repetear” όσο και με τον “Get URL”. Από το μενού “Actions” επιλέγουμε "GET" και εισάγουμε το URL για την λήψη της IP μας σε μορφή JSON.



Εικόνα 42. GET request.

[37] JSON IP, https://ipv4.jsonip.com/, Accessed on: March 13, 2023.

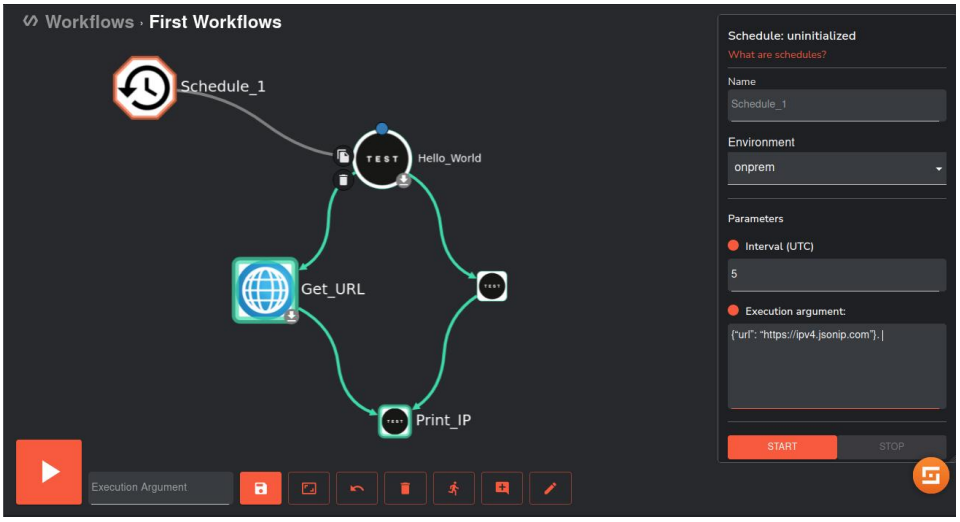
Θα χρησιμοποιήσουμε άλλο ένα Test app για να εμφανίσουμε την IP μας. Αυτή τη φορά όμως, θέλουμε να χρησιμοποιήσουμε κείμενο μαζί με τη μεταβλητή μας. Για να μπορέσουμε να χρησιμοποιήσετε δεδομένα από προηγούμενο κόμβο ξεκινάμε με $ και μετά το όνομα κόμβου: $Get_URL. Για να εμφανίσουμε την "ip" από τα δεδομένα JSON: $Get URL.body.ip. Όλα μαζί: “My IP is $Get_URL.body.ip.



Εικόνα 43. Εμφανίζοντας την IP από το GET request.

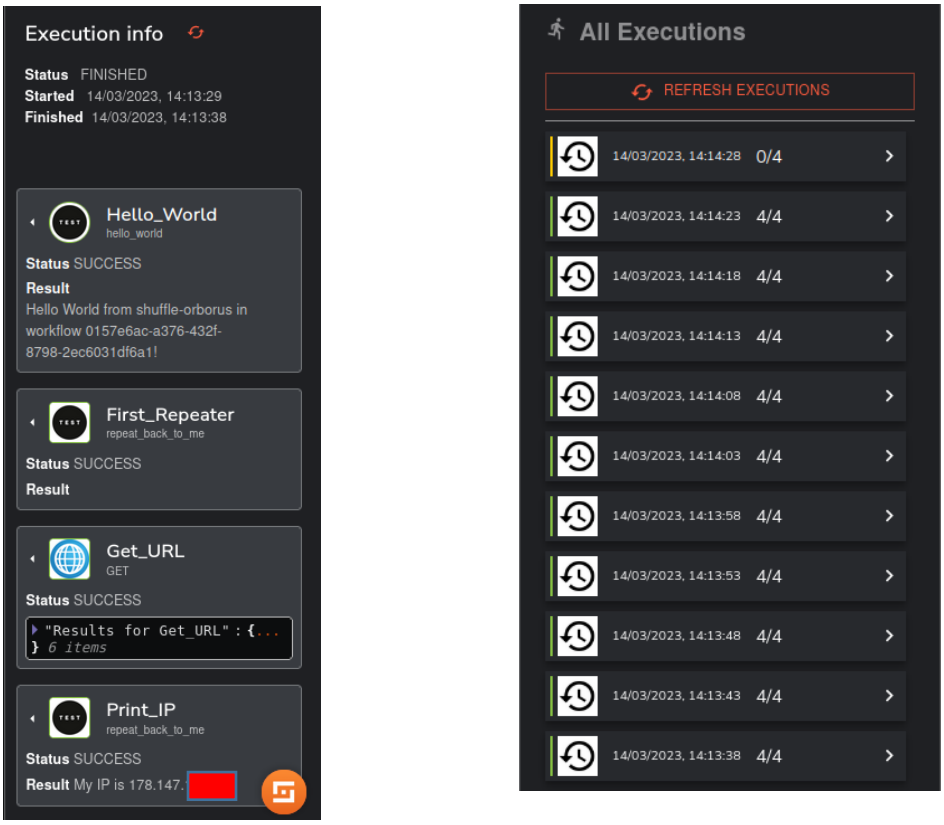
Άλλο ένα χαρακτηριστικό που είναι απαραίτητο για τον αυτοματισμό εργασιών είναι ο προγραμματισμός (scheduling). Για να προσθέσουμε έναν Schedule πηγαίνουμε στην καρτέλα “Triggers”, επιλέγουμε τον Schedule, τον σύρουμε στο Workflow που έχουμε φτιάξει και θα συνδεθεί αυτόματα στον αρχικό κόμβο, καθώς από εκεί θα πρέπει να ξεκινήσει η εκτέλεση. Με κλικ στον κόμβο , βλέπουμε ότι χρειάζεται δύο παραμέτρους: ένα διάστημα σε δευτερόλεπτα (χρόνος μεταξύ των εκτελέσεων) και το όρισμα εκτέλεσης.

Δίπλα από το κουμπί “Test execution” υπάρχει το πεδίο “Execution Argument”. Οτιδήποτε τοποθετείται σε αυτό το πεδίο γίνεται μια τιμή διαθέσιμη σε όλους τους κόμβους του Workflow μέσω της μεταβλητής $exec. Στην περίπτωσή μας, αποφασίσαμε προηγουμένως ότι θέλουμε να παρέχουμε μια διεύθυνση URL σε αυτό το πεδίο ως εξής: {“url”: “https://ipv4.jsonip.com”}. Αυτή η διεύθυνση URL χρησιμοποιείται στη συνέχεια στον κόμβο "Get_URL" για να ορίσουμε ποια διεύθυνση URL θέλουμε να λάβουμε. Για να υλοποιήσουμε το χρονοδιάγραμμα κάθε 5 δευτερόλεπτα ορίζουμε interval 5 και πατάμε START.



Εικόνα 44. Schedule workflow.

Αφού εκτελέσουμε το workflow, βλέπουμε ότι εκτελείται επιτυχώς κάθε 5 δευτερόλεπτα και παίρνουμε απάντηση την IP μας.



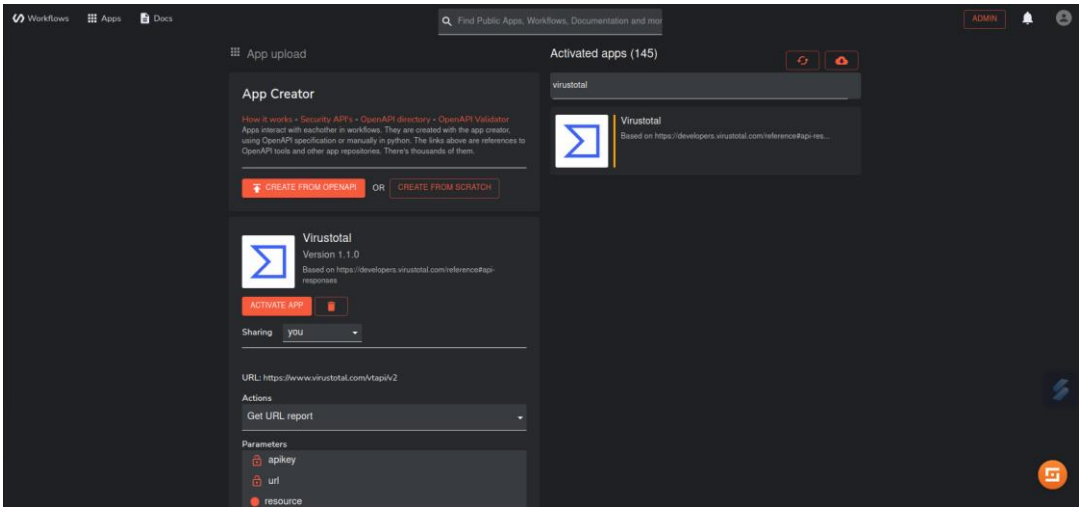
Εικόνα 45. Επιτυχής εκτέλεση workflow με χρονοδιάγραμμα.

6-3. Ενοποίηση του Shuffle με Virustotal και TheHive.

Σε αυτή την ενότητα θα δούμε τη διαδικασία δημιουργίας μιας εφαρμογής για το Shuffle και την ενσωμάτωσής της. Η ιδέα είναι να συνεχιστεί το Workflow που δημιουργήθηκε στην προηγούμενη ενότητα και να χτιστεί πάνω σε αυτό η λειτουργία του Virustotal και του TheHive. Καθώς το Virustotal δεν αποτελεί μέρος του Shuffle θα πρέπει να ξεκινήσουμε δημιουργώντας την ίδια την εφαρμογή. Αυτά είναι τα βήματα που θα ακολουθήσουμε:

- Ενεργοποίηση της εφαρμογής Virustotal με τη δυνατότητα λήψης της IP.
- Προσθήκη της ενέργειας Virustotal “Get IP report” στο Workflow.
- Ρύθμιση του TheHive.
- Δημιουργία alert στο TheHive με το ιστορικό της IP μας από το Virustotal.

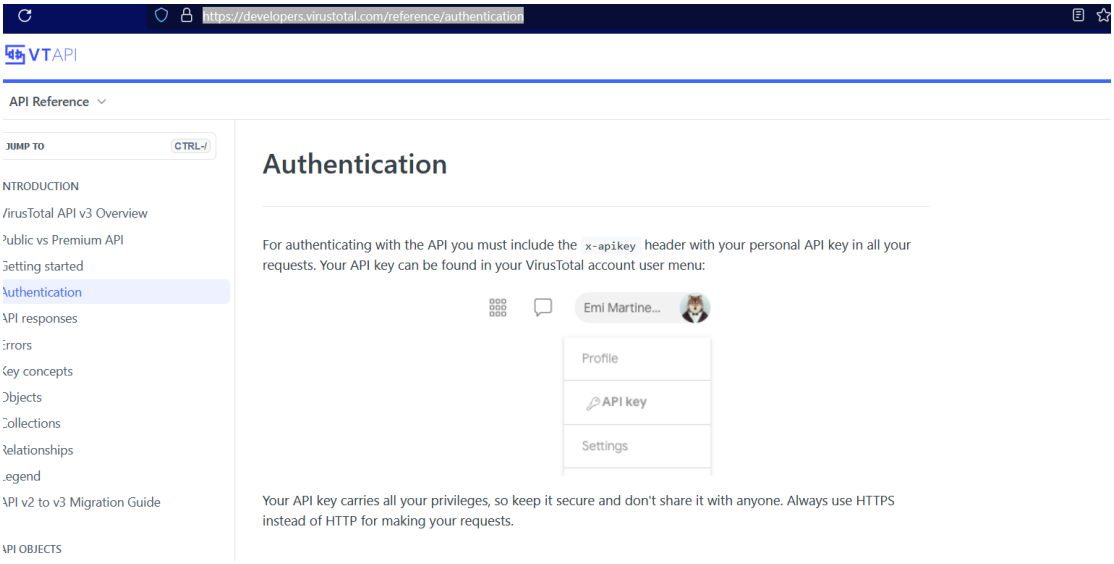
Εισερχόμαστε στην εφαρμογή και στην καρτέλα Apps όπου μας παρουσιάζεται η δυνατότητα δημιουργίας, επεξεργασίας, διαγραφής, αναζήτησης, λήψης και οτιδήποτε άλλο σχετίζεται με εφαρμογές. Αυτό το μέρος έχει πρόσβαση σε όλα όσα χρειαζόμαστε, συμπεριλαμβανομένης της δυνατότητας λήψης εφαρμογών από ένα αποθετήριο github, δημόσιο ή ιδιωτικό, δημιουργία εφαρμογής από το OpenAPI ή δημιουργία της από την αρχή. Στην περίπτωσή μας, θα κάνουμε αναζήτηση του Virustotal και θα πατήσουμε “ACTIVATE APP”.



Εικόνα 46. Ενεργοποίηση Virustotal App.

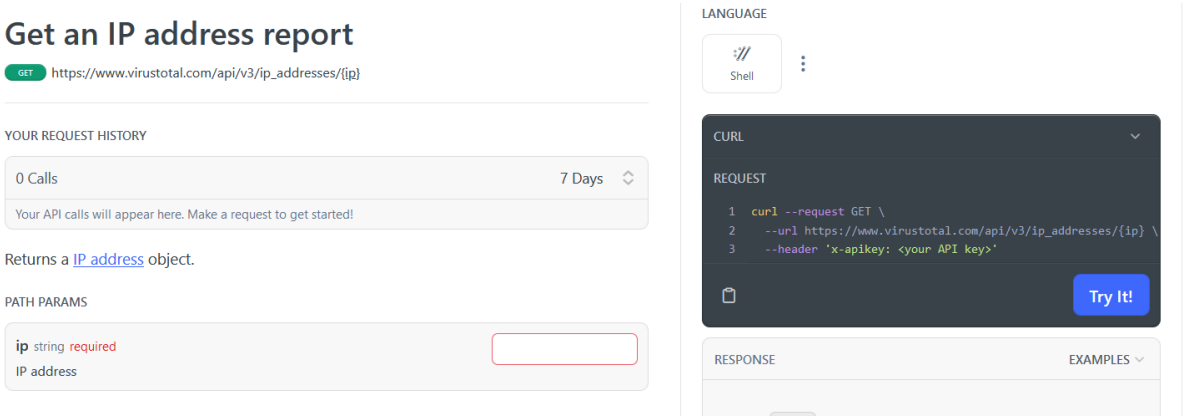
Οι παράμετροι που θα πρέπει να εισάγουμε εδώ είναι το Authentication και το Url που θα χρησιμοποιήσουμε για το Get IP report. Στην ιστοσελίδα του Virustotal, αναφέρεται ότι

πρέπει να χρησιμοποιήσουμε ένα προσαρμοσμένο x-apikey header, που σημαίνει ότι πρέπει να χρησιμοποιήσουμε ένα API key. [38]



Εικόνα 47. Virustotal authentication.

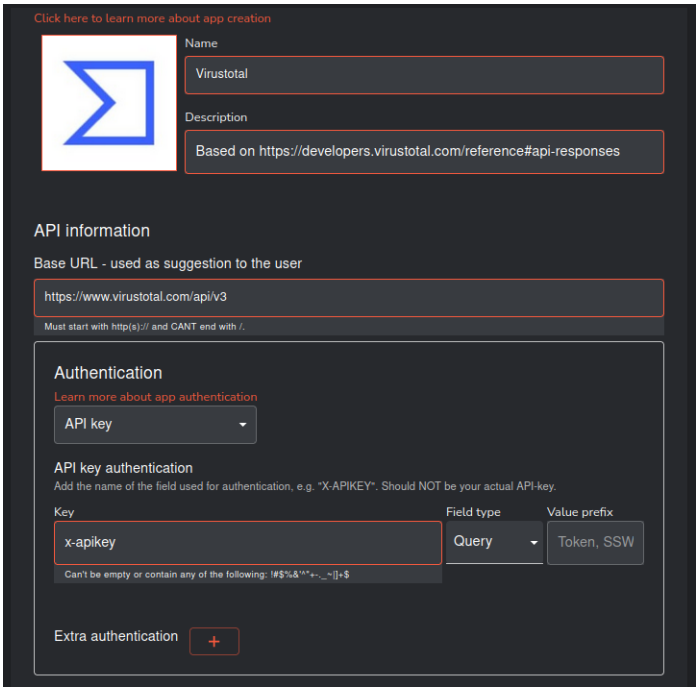
Στη συνέχεια, πρέπει να βρούμε τη διεύθυνση URL. Στην ιστοσελίδα του Virustotal βρίσκουμε πληροφορίες για το Get IP address report.[39]



Εικόνα 48. Virustotal Get IP address report.

Επιστρέφοντας στο Shuffle, έχουμε τώρα τις απαραίτητες πληροφορίες για τη δημιουργία μιας εφαρμογής για το Virustotal (BASE URL & Authentication scheme).

[38] Virustotal Authentication, https://developers.virustotal.com/reference/authentication, Accessed on: March 15, 2023.
[39] Virustotal Get an IP address report, https://developers.virustotal.com/reference/ip-info, Accessed on: March 15, 2023.

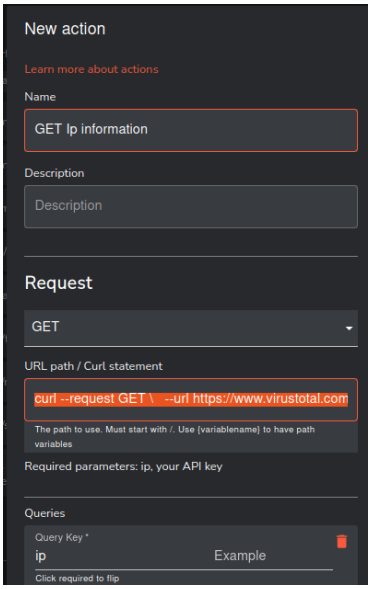


Εικόνα 49. Virustotal API στο Shuffle.

Στην συνέχεια θα δημιουργήσουμε ένα Action για την εφαρμογή πατώντας “New Action”. Στην καρτέλα “New Action” το επόμενο βήμα είναι να συμπληρώσουμε συγκεκριμένες πληροφορίες για την ενέργεια "Get IP Report". Συμπληρώνουμε ένα όνομα και προαιρετικά μια περιγραφή, και στην συνέχεια αντιγράφουμε τα ακόλουθα, που βρήκαμε στον ιστότοπο του Virustotal:

```
curl --request GET \
  --url https://www.virustotal.com/api/v3/ip_addresses/{ip} \
  --header 'x-apikey: <your API key>'
```

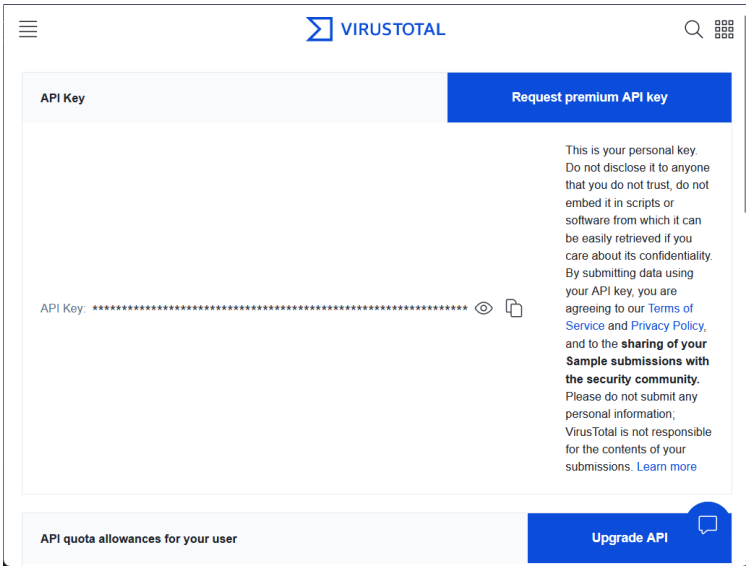
Η εντολή χρησιμοποιεί curl — ένα ευρέως χρησιμοποιούμενο εργαλείο γραμμής εντολών για την υποβολή αιτημάτων δικτύου (π.χ. HTTP). Το Shuffle υποστηρίζει την ανάλυση CURL, που σημαίνει ότι μπορούμε να χρησιμοποιήσουμε αυτήν την εντολή απευθείας για να εκτελεστεί το Action που επιθυμούμε.



Εικόνα 50. New Action Get IP information

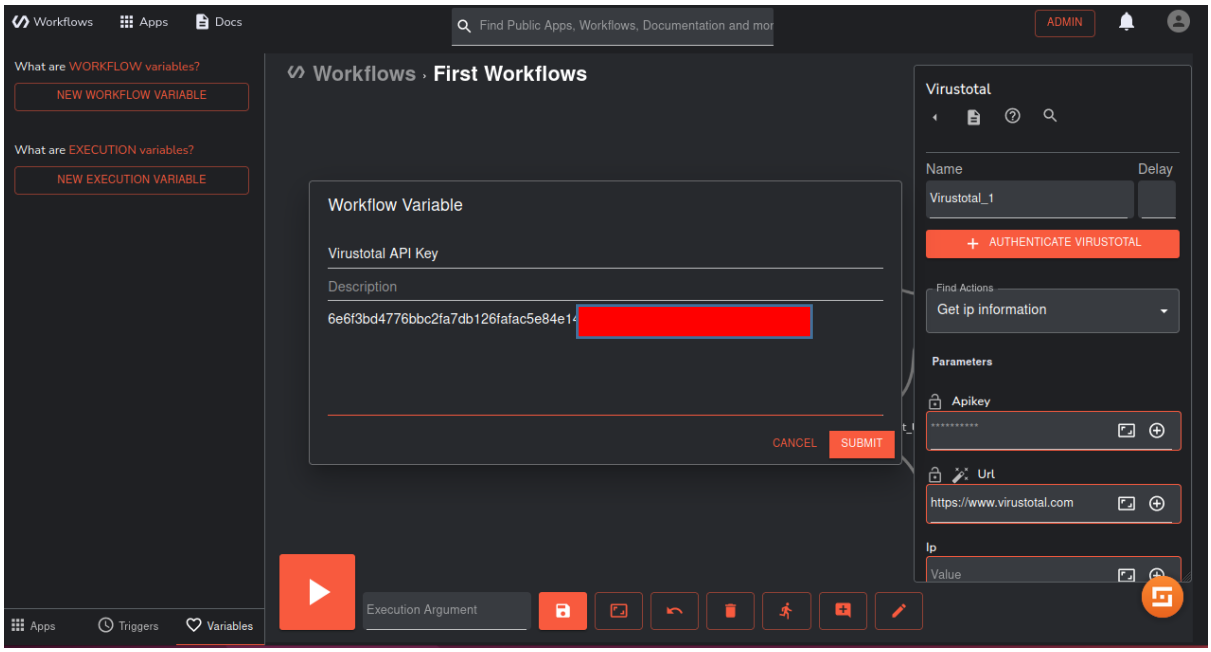
Κάνοντας κλικ στο κουμπί αποθήκευσης, το Shuffle θα δημιουργήσει τρία πράγματα: Ένα OpenAPI specification, ένα APP SDK σε κώδικα Python και μια ολοκληρωμένη Docker image.

Αφού ολοκληρωθεί η διαδικασία δημιουργίας του App, θα πρέπει τώρα να δοκιμάσουμε την εφαρμογή μας. Ξεκινάμε σύροντας την εφαρμογή Virustotal στην προβολή του Workflow που έχουμε δημιουργήσει, την επιλέγουμε και συμπληρώνουμε τα ορίσματα "apikey" και "ip". Για να βρούμε το API key για το Virustotal, θα πρέπει να έχουμε εγγραφεί στην ιστοσελίδα, να συνδεθούμε και να επιλέξουμε "API key" επάνω δεξιά.

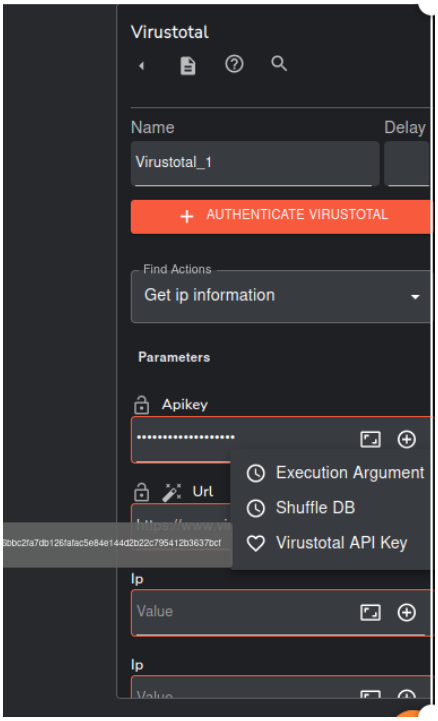


Εικόνα 51. API Key από την ιστοσελίδα του Virustotal.

Την τιμή του API Key, μπορούμε να την αποθηκεύσουμε ως μεταβλητή (Workflow Variables) από την καρτέλα Variables, επιλέγοντας “New workflow variable” και στην συνέχεια να την προσθέσουμε στο πεδίο “Apikey” από το αναδυόμενο μενού.

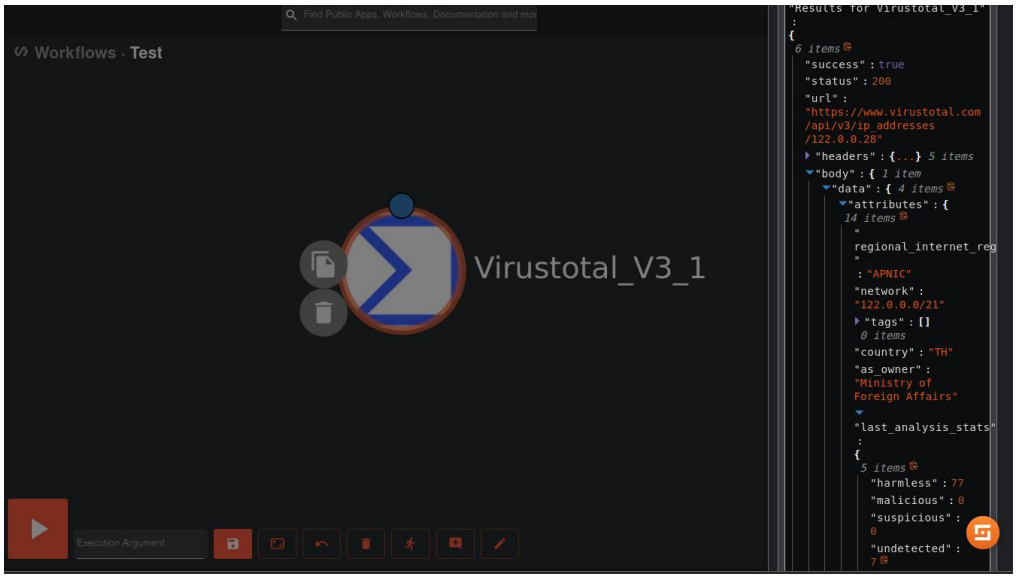


Εικόνα 52. Αποθήκευση API Key ως Workflow Variable.



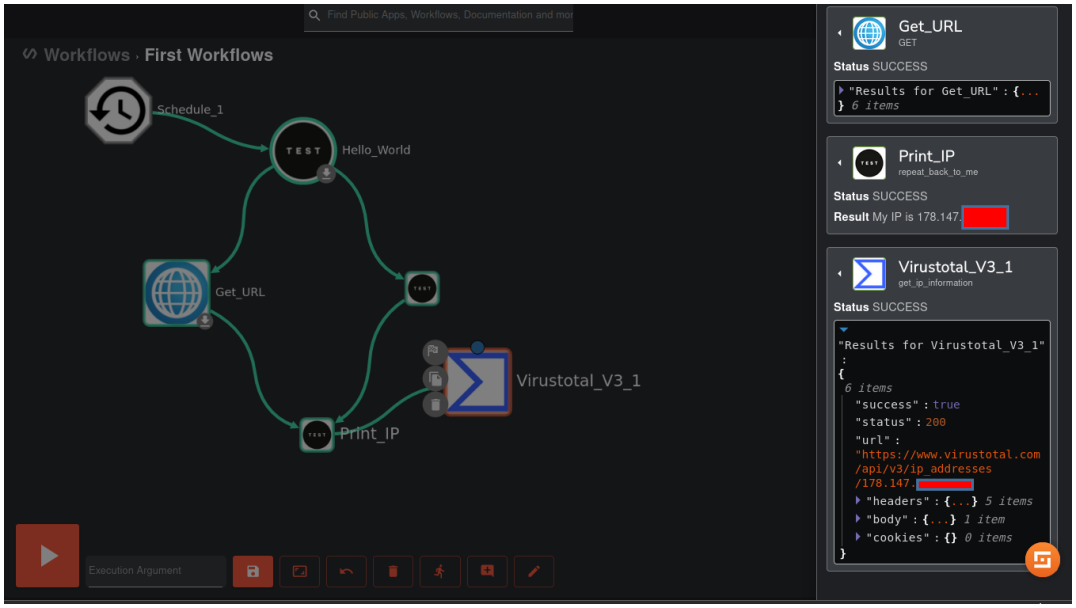
Εικόνα 53. Ρύθμιση παραμέτρων του Virustotal App.

Εκτελούμε το Workflow για κάποια IP – στην προκειμένη περίπτωση ελέγξαμε την IP 122.0.0.28 – και βλέπουμε ότι εκτελέστηκε επιτυχώς, λαμβάνοντας τα αποτελέσματα που χαρακτηρίζουν την IP harmless από 77 security vendors.



Εικόνα 54. Test Virustotal V3 App.

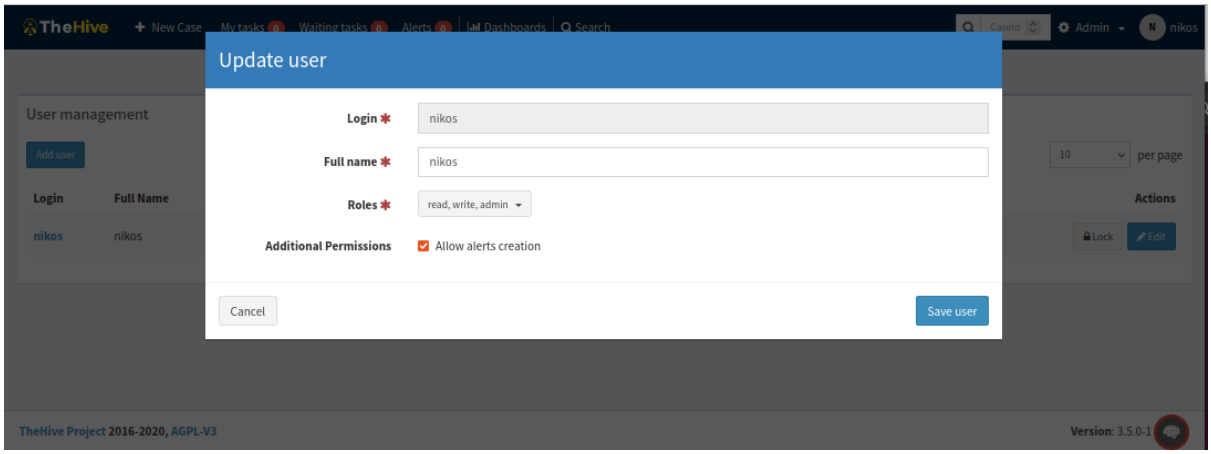
Αφού επετεύχθη η δοκιμή της εφαρμογής που δημιουργήσαμε, θα την προσθέσουμε τώρα στο Workflow "First Workflows" που έχουμε δημιουργήσει. Προσθέτουμε τον κόμβο του Virustotal, και τον συνδέουμε στον τελευταίο κόμβο "Print_IP" Ο στόχος εδώ είναι να χρησιμοποιήσουμε τη δική μας IP, που περνά από τον κόμβο "Get_URL" και να την αναζητήσουμε στο Virustotal. Αυτό το κάνουμε γράφοντας $Get URL.body.ip, καθώς τα δεδομένα που επιστρέφονται από τον κόμβο "Get_URL" έχουν τη μορφή {"body.ip": "your_ip"}. Το Workflow λειτούργησε με επιτυχία και όπως βλέπουμε πήραμε τα αποτελέσματα για την IP μας από το Virustotal.



Εικόνα 55. Επιτυχής εκτέλεση Workflow και λήψη αποτελεσμάτων της IP μας από το Virustotal.

Έχοντας δημιουργήσει μια εφαρμογή για να ανακτούμε δεδομένα από το Virustotal, είμαστε πλέον έτοιμοι να χρησιμοποιήσουμε τα δεδομένα αυτά στο TheHive.

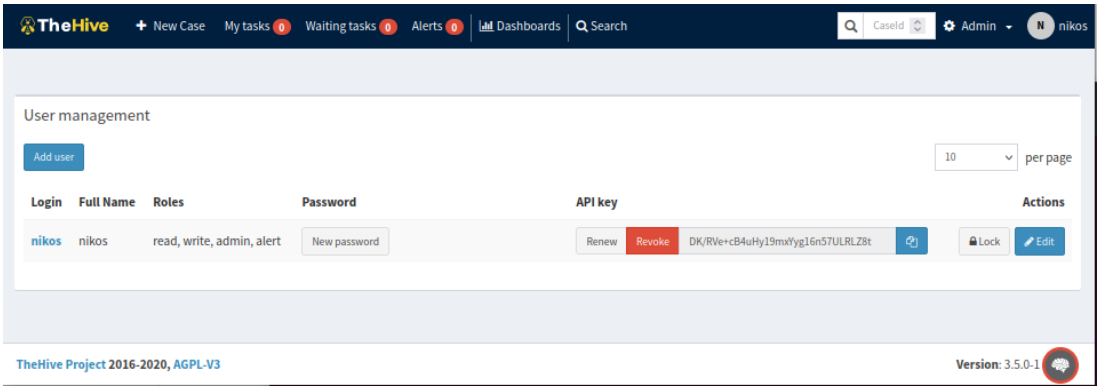
Έχουμε εγκαταστήσει το TheHive project[40] και συνδεόμαστε στην πλατφόρμα στην θύρα 9000. Έχουμε δημιουργήσει έναν χρήστη administrator τον οποίο θα επεξεργαστούμε ώστε να του δώσουμε δικαιώματα να δημιουργεί Alerts.



Εικόνα 56. TheHive user allow alert creation.

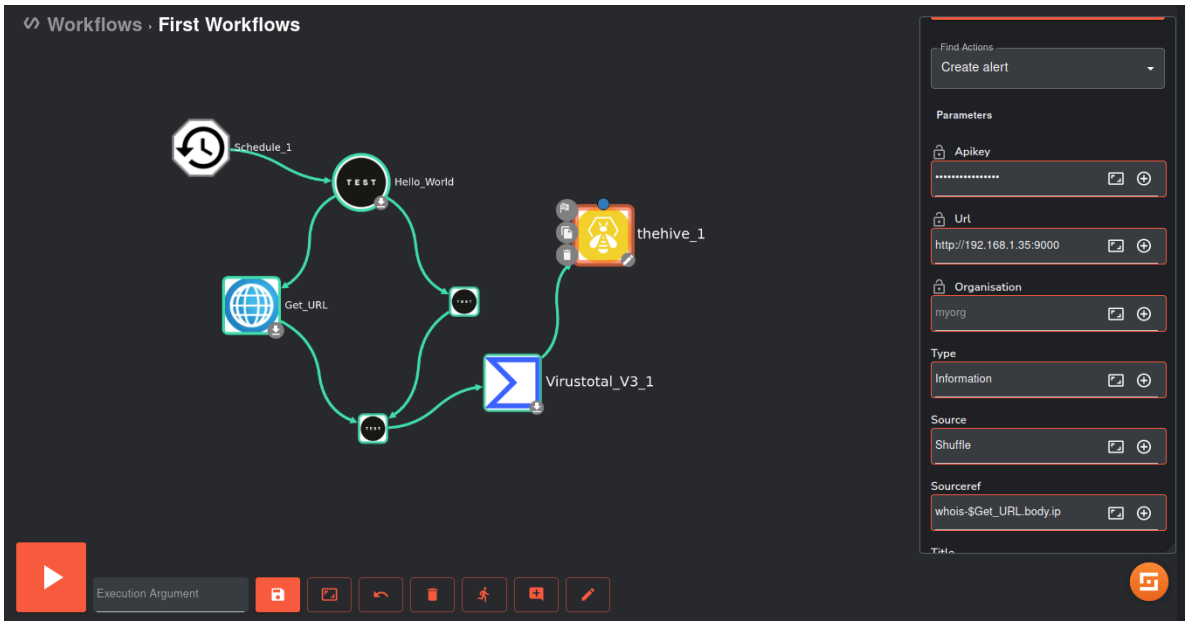
Στην συνέχεια δημιουργούμε ένα API Key για τον χρήστη και το αποθηκεύουμε στο Shuffle ως Workflow variable.

[40] Installation guide, https://docs.thehive-project.org/thehive/legacy/thehive3/installation/install-guide/#elasticsearch-installation, Accessed on: March 20, 2023.



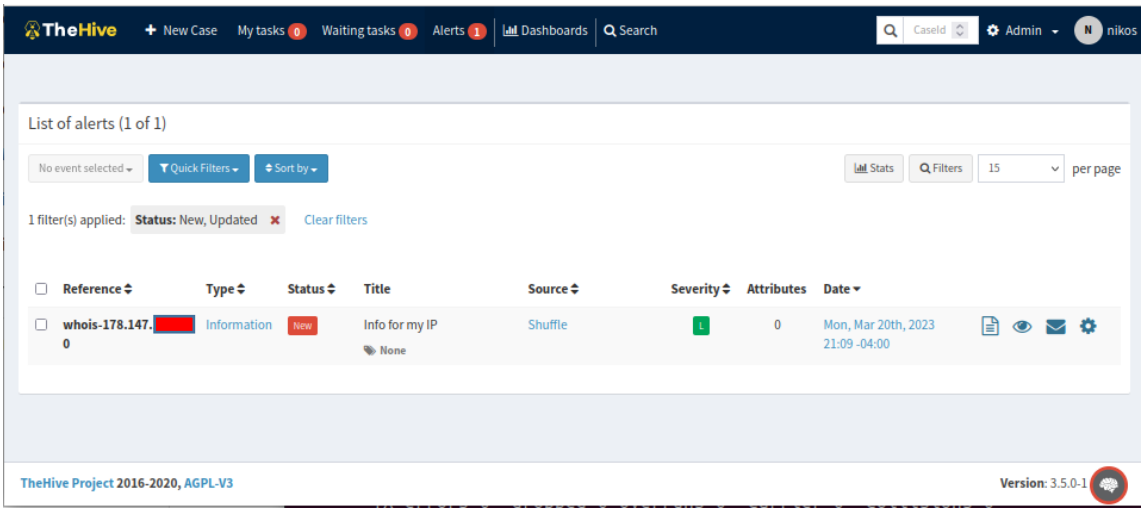
Εικόνα 57. API Key του χρήστη.

Με το API key για το TheHive, μπορούμε πλέον να δημιουργήσουμε μια ειδοποίηση. Καθώς το Shuffle έχει ήδη μια εφαρμογή για το TheHive, το μόνο που λείπει είναι να προσθέσουμε την ενέργεια "Create alert" στο Workflow. Εισάγουμε το App του TheHive στο Workflow, το συνδέουμε στον κόμβο Virustotal και συμπληρώνουμε τις απαιτούμενες παραμέτρους που θα εμφανιστούν στο Alert.



Εικόνα 58. Ολοκλήρωση Workflow με την ενοποίηση του TheHive.

Η εκτέλεση του Workflow οδηγεί σε μια νέα ειδοποίηση όπως φαίνεται παρακάτω. Για να βεβαιωθούμε ότι δημιουργεί μια νέα ειδοποίηση κάθε φορά που αλλάζει η εξωτερική μας IP, μπορούμε να ενεργοποιήσουμε ξανά τον Scheduler.



Εικόνα 59. Επιτυχής λήψη alert στο TheHive.

6-4. Extensions και usecases του Shuffle

Είδαμε στις προηγούμενες ενότητες, μέσα από απλές υλοποιήσεις, την ευκολία με την οποία είναι δυνατή η δημιουργία workflows μέσα από το Shuffle και η ενοποίηση με άλλες εφαρμογές και πλατφόρμες ασφαλείας. Ο Workflow designer είναι το μέρος του Shuffle που τα κάνει όλα να ενοποιηθούν μεταξύ τους. Μαζί με τον App creator και τις προεπιλεγμένες εφαρμογές (HTTP & Shuffle Toolbox), δίνει πρόσβαση σε απεριόριστες δυνατότητες αυτοματισμού, διασφαλίζοντας ότι ο καθένας μπορεί να μάθει να αυτοματοποιεί οτιδήποτε με λίγες μόνο ώρες εξάσκησης. Το Shuffle διατίθεται με μεγάλο αριθμό εφαρμογών και workflows, καθιστώντας το εύκολο τόσο στην έναρξη χρήσης όσο και στην επέκταση.

Άλλη μια κατηγορία εφαρμογών είναι οι επεκτάσεις (extensions), οι οποίες ουσιαστικά είναι ενσωματώσεις που συνεπάγονται την σύνδεση υπηρεσιών τρίτων με εισερχόμενα webhooks ως triggers σε ένα workflow. Με αυτό τον τρόπο δεδομένα από third-party API μπορούν να εισάγονται στο Shuffle.

Μερικές από τις επεκτάσεις που υπάρχουν στο Shuffle είναι:

- Single SignOn SSO: Επιτρέπει να γίνεται σύνδεση στο Shuffle από άλλες πηγές, πλήρως ελεγχόμενες από το εξωτερικό περιβάλλον.
- Wazuh: Το Wazuh είναι μια πλατφόρμα SIEM. Έχει αναπτυχθεί μια απλή προώθηση ειδοποιήσεων (alert) από το Wazuh στο Shuffle.
- TheHive: Μία από τις βασικές δυνατότητές του είναι τα webhook, τα οποία μπορούν να στέλνουν ενημερώσεις σε πραγματικό χρόνο σε ένα σύστημα

τρίτου μέρους κάθε φορά που αλλάζει οτιδήποτε εντός του TheHive (π.χ. μια νέα ειδοποίηση).

- MISP Malware Information Sharing Platform, είναι μια από τις καλύτερες εναλλακτικές λύσεις ανοιχτού κώδικα για το Threat Intelligence. Διατίθεται τρόπος χειρισμού δεδομένων σε πραγματικό χρόνο, όπως ενημερώσεις συμβάντων, ενημερώσεις ενδείξεων, επεξεργασία IDS flags, κ.λπ.

Υπάρχουν ακόμα επεκτάσεις για ELK, QRadar, Cortex, Splunk κλπ.

Τέλος, διατίθενται κάποια έτοιμα usecases για να βοηθήσουν τους χρήστες του Shuffle είτε να τα χρησιμοποιήσουν ως έχουν είτε να τα προσαρμόσουν στο σύστημά τους. Τα usecases αυτά χωρίζονται σε τέσσερις κατηγορίες: Collect, Enrich, Detect, Respond και Verify.

Εικόνα 60. Shuffle usecases.

Ενδεικτικά στην παρακάτω εικόνα βλέπουμε το usecase Email Management από την κατηγορία Collect. Σύμφωνα με το Workflow αυτό, γίνεται ανάγνωση κάθε email που λαμβάνεται στον IMAP Server και τρέχει δύο υπο-εργασίες, μια ελέγχοντας την IP του αποστολέα και η δεύτερη ελέγχοντας το domain από το Virustotal.

Εικόνα 61. Email reader IMAP.

7. Συμπεράσματα

Ο στόχος αυτής της διπλωματικής εργασίας ήταν η έρευνα και η κατανόηση της τεχνολογίας SOAR και της χρήσης των πλατφορμών SOAR στην ασφάλεια στον κυβερνοχώρο. Αφού έγινε αρχικά επεξήγηση της λειτουργίας ενός SOC καθώς και των κυριότερων εργαλείων ασφάλειας που χρησιμοποιούνται, στην συνέχεια περιεγράφηκε η τεχνολογία SOAR και δόθηκαν απαντήσεις στα ερωτήματα ποιες είναι οι χρήσεις αυτής της τεχνολογίας και τι προβλήματα επιλύει. Στην συνέχεια έγινε παρουσίαση και σύγκριση τεσσάρων από των πιο γνωστών πλατφορμών SOAR και τέλος έγινε περιγραφή της εγκατάστασης και της λειτουργίας της πλατφόρμας SOAR ανοικτού κώδικα Shuffle, η οποία όπως είδαμε προσφέρει ευκολία στον χειρισμό και ενσωμάτωση με αρκετές εφαρμογές.

Οι ειδικοί σε θέματα ασφάλειας συνήθως κατακλύζονται από το έργο της παρακολούθησης και του χειρισμού μιας ολοένα και πιο τεράστιας δεξαμενής ειδοποιήσεων ασφαλείας που δημιουργούνται από μια ποικιλία εργαλείων ασφαλείας. Ως εκ τούτου, ενδέχεται να αποτύχουν να ενεργήσουν έγκαιρα για την αντιμετώπιση συμβάντων ασφαλείας λόγω της μη αυτόματης και επαναλαμβανόμενης εργασίας λήψης και συνδυασμού πληροφοριών προειδοποίησης ασφαλείας από εργαλεία ασφαλείας πολλών προμηθευτών. Η ενορχήστρωση ασφαλείας στοχεύει στην υποστήριξη του προσωπικού ασφαλείας για την αποτελεσματική και αποδοτική παρακολούθηση και αντιμετώπιση περιστατικών ασφαλείας, επιτρέποντας τον συντονισμό και τη συνεργασία μεταξύ των ετερογενών ανεξάρτητων εργαλείων ασφαλείας. Η ενσωμάτωση και η ενορχήστρωση διαφόρων εργαλείων ασφαλείας σε έναν οργανισμό χρειάζεται μια ολοκληρωμένη λύση μιας πλατφόρμας SOAR. Πρόσφατα, κάθε είδους οργανισμοί έχουν αρχίσει να ενδιαφέρονται να υιοθετήσουν την τεχνολογία SOAR.

Ο αυτοματισμός ασφάλειας στον κυβερνοχώρο μειώνει τον φόρτο εργασίας του προσωπικού ασφαλείας, επομένως ο όγκος των ωρών που δαπανάται σε εργασίες ρουτίνας μπορεί να χρησιμοποιηθεί σε πιο παραγωγικές εργασίες, όπως η αξιολόγηση και η βελτίωση του τρέχοντος επιπέδου ασφαλείας του οργανισμού. Η χρήση των πλατφορμών SOAR επιτρέπει συνεπείς, ακριβείς και αποτελεσματικές απαντήσεις στις διάφορες απειλές ασφαλείας με ενορχήστρωση και αυτοματοποίηση.

Από την ανάλυση κατέστη σαφές ότι η πλατφόρμα δεν αναπτύχθηκε για να λειτουργεί ως μεμονωμένη λύση. Η αρχιτεκτονική του αποτελείται από πολλαπλά επίπεδα, αρκετά διακριτά, με χαρακτηριστικά σε κάθε επίπεδο που μπορούν να χρησιμοποιηθούν από τους

αναλυτές ή τους ερευνητές προκειμένου να μετριάσουν και να αντιμετωπίσουν υπάρχουσες ή πιθανές απειλές.

Όσον αφορά τις παρεχόμενες πηγές δεδομένων, το λογισμικό χρησιμοποιεί ενσωματώσεις που λειτουργούν ως σύνδεσμοι σε λογισμικό τρίτων. Αυτό παρέχει υποστήριξη στον αναλυτή, ο οποίος έπρεπε να αναπτύξει και να εκτελέσει πολλαπλές επαναλαμβανόμενες εργασίες, προκειμένου να ενσωματώσει διαφορετικό λογισμικό τρίτων στα παραδοσιακά SOCs. Αυτές οι συνδέσεις είναι στις περισσότερες περιπτώσεις εξαιρετικά προσαρμόσιμες και ο αναλυτής με λίγες μόνο γραμμές κώδικα, ή σε ορισμένες περιπτώσεις καθόλου κώδικα, μπορεί να ενσωματώσει πηγές από threat intelligence, network monitoring, διαχείριση συμβάντων, endpoint protection και άλλες λύσεις.

Ένα άλλο στοιχείο της τεχνολογίας SOAR, που παρέχει υποστήριξη στους χρήστες, είναι αυτό της οπτικοποίησης δεδομένων. Ένα σημαντικό πρόβλημα για τα σύγχρονα SOCs είναι ότι διαφορετικά λογισμικά τρίτων απαιτούν συνήθως διαφορετικές οθόνες, προκειμένου να διεξάγουν ανάλυση στα δεδομένα τους. Με την πλατφόρμα SOAR ο αναλυτής ενσωματώνει όλα τα δεδομένα τρίτων σε μία οθόνη.

Τέλος, ξίσου σημαντικό είναι το συστατικό του αυτοματισμού. Αυτό υποστηρίζει τους αναλυτές μειώνοντας δραστικά τους χρόνους απόκρισης, επιτρέποντάς τους να εμπλακούν και να παράγουν πιο ποιοτικά αποτελέσματα σχετικά με την ανάλυση και τις έρευνές τους. Η ικανότητα αυτοματισμού χρησιμοποιείται με την εφαρμογή playbooks ή workflows που περιέχουν όλα τα βήματα και τις ενέργειες που ακολουθούνται για την αντιμετώπιση μιας απειλής ασφαλείας. Σχεδιάζονται ως διαγράμματα ροής και υποστηρίζουν τους αναλυτές με αυτοματοποιημένες λύσεις.

Αυτά τα χαρακτηριστικά παρουσιάστηκαν μέσα από την λειτουργία της πλατφόρμας Shuffle στο προηγούμενο κεφάλαιο. Επίσης, παρουσιάστηκαν τα κυριότερα χαρακτηριστικά τεσσάρων γνωστών πλατφορμών SOAR στο κεφάλαιο 5, η κάθε μια με τα δικά της πλεονεκτήματα και μειονεκτήματα, που όμως όλες διατηρούν αυτά τα βασικά χαρακτηριστικά. Η έννοια των πολλαπλών ενσωματώσεων έκανε τις πλατφόρμες συμβατές με μια πληθώρα λογισμικού τρίτων, κάτι που οι αναλυτές βρίσκουν δύσκολο και χρονοβόρο μέσω της επανάληψης των ενεργειών που απαιτούνται. Το έργο τους μπορεί επίσης να υποστηριχθεί από τις πλατφόρμες SOAR, ώστε να προσαρμόζεται σε κάθε ανάγκη SOC.

Με περισσότερες τεχνολογικές εξελίξεις και έρευνα στην τεχνολογία SOAR, η τεχνολογία θα υιοθετηθεί περαιτέρω από τους οργανισμούς, οδηγώντας σε έναν πιο ασφαλή κυβερνοχώρο. Περαιτέρω θέματα έρευνας θα μπορούσαν να είναι η χρήση της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (ML) σε λογισμικά ασφάλειας.

Βιβλιογραφία

[1] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques, Journal of Network and Computer Applications", vol. 60, pp. 19-31, 2016.

[2] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," Journal of Network and Computer Applications, vol. 101, pp. 18-54, 2018.

[3] B. Schneier, "Security Orchestration for an Uncertain World", 2017, https://securityintelligence.com/security-orchestration-for-an-uncertain-world/

[4] Aher, B., "Importance of a Security Operations Center", 2018, https://dzone.com/articles/importance-of-security-operations-center

[5] Zimmerman C. "Ten Strategies of a World-Class Cybersecurity Operations Center." McLean, USA: MITRE Corporation, 2014. p. 8-9.: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.545&rep=rep1&type=pdf

[6] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul, "Security Operations Center: A Systematic Study and Open Challenges", p.7-9, 2020.

[7] C. Olt, "Establishing security operation centers for connected cars," ATZelectronics worldwide, vol. 14, no. 5, pp. 40–43, May 2019.

[8] Petters J. "IDS vs. IPS: What is the Difference?" , 2020. https://www.varonis.com/blog/ids-vs-ips/

[9] Nilă C, Apostol I, Patriciu V. "Machine learning approach to quick incident response." In: 2020, 13th International Conference on Communications, 2020. p. 291-292. https://doi.org/10.1109/COMM48946.2020.9141989

[10] Miller L. “Next-Generation Firewalls For Dummies.” New Jersey: John Wiley & Sons; 2019. p. 3-5.
https://incom.co.uk/wp-content/uploads/2020/10/Next-Generation-Firewalls-For-Dummies.pdf

[11] Hutchins, E.M., Cloppert, M.J., Amin, R.M. “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead. Issues” Inf. Warf. Secur. Res. 2011.

[12] Gartner Research. “Definition: Threat Intelligence”. Stamford, USA: Gartner Research, 2013
https://www.gartner.com/en/documents/2487216/definition-threat-intelligence

[13] Palo Alto Networks. “What is a Threat Intelligence Platform.” Santa Clara, USA: Palo Alto Networks, 2021
https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform

[14] “Securing What’s Now and What’s Next: 20 Cybersecurity Considerations for 2020,” Cisco, 2020
https://ebooks.cisco.com/story/2020-ciso-benchmark/page/4/13

[15] Gartner, “Security Orchestration, Automation and Response (SOAR)”, 2017
https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

[16] Jon Oltsik, “The evolution of security operations, automation and orchestration”, CSO, 2018,
https://www.csoonline.com/article/3270957/the-evolution-of-security-operations-automation-and-orchestration.html

[17] Jon Oltsik, “The rise of analyst-centric security operations technologies”, CSO, 2018
https://www.csoonline.com/article/3276463/the-rise-of-analyst-centric-security-operations-technologies.html

[18] Verizon “2016 Data Breach Investigations Report”, 2016
http://www.verizonenterprise.com/verizon-insights-lab/dbir/

[19] BakerHosteller, “Be Compromise Ready: Go Back to the Basics - 2017 Data Security Incident Response Report”, 2017,
https://www.bakerlaw.com/events/webinar-be-compromise-ready-go-back-to-the-basics

[20] Sharon Shea, “SOAR (security orchestration, automation and response)”, 2021
https://www.techtarget.com/searchsecurity/definition/SOAR

[21] J. Trull, “Top 5 best practices to automate security operations”, 2017,
https://cloudblogs.microsoft.com/microsoftsecure/2017/08/03/top-5-best-practices-to-automate-security-operations/

[22] ForeScout, “ForeScout Agentless Visibility and Control, White Paper”,
https://www.forescout.com/wp-content/uploads/2018/08/Agentless-Visibility-and-Control-ForeScout-White-Paper.pdf

[23] C. Islam, M.A. Babar, S. Nepal, “A Multi-Vocal Review of Security Orchestration”, 2017
https://arxiv.org/abs/2002.09190

[24] E. Feitosa, E. Souto, and D. H. Sadok, “An orchestration approach for unwanted Internet traffic identification, Computer Networks”, vol. 56, no. 12, pp. 2805-2831, 2012.

[25] SWIMLANE, “Security Orchestration | What is Security Orchestration?”
https://swimlane.com/solutions/security-automation-and-orchestration/security-orchestration/

[26] Dan Kaplan, “9 security orchestration and automation benefits: How SOAR helps improve incident response”, 2021
https://chronicle.security/blog/posts/security-orchestration-automation-response-benefits/

[27] Ina Nikolova, “What Are the Main Differences Between SIEM and SOAR?”, 2022,
https://www.linkedin.com/pulse/what-main-differences-between-siem-soar-ina-nikolova-ph-d-?trk=pulse-article_more-articles_related-content-card

[28] Crystal Bedell, “Definitive guide to SOAR. How to stop threats faster with security orchestration, automation and response”, 2019, p. 51-56. https://gallery.logrhythm.com/white-papers-and-e-books/definitive-guide-to-soar.pdf

[29] TheHive, https://thehive-project.org/

[30] Cortex XSOAR, https://www.paloaltonetworks.com/cortex/cortex-xsoar

[31] SecOps Community Chronicle SOAR, https://chronicle.security/soar-free-edition/

[32] Shuffle, https://shuffler.io/

[33] Shuffle Architecture, https://shuffler.io/docs/architecture

[34] Shuffle documentation, https://shuffler.io/docs

[35] Frikke, Blog for Shuffle https://medium.com/@Frikkylikeme

[36] Virtual memory, https://www.elastic.co/guide/en/elasticsearch/reference/current/vm-max-map-count.html

[37] JSON IP, https://ipv4.jsonip.com/

[38] Virustotal Authentication, https://developers.virustotal.com/reference/authentication

[39] Virustotal Get an IP address report, https://developers.virustotal.com/reference/ip-info

[40] Installation guide, https://docs.thehive-project.org/thehive/legacy/thehive3/installation/install-guide/#elasticsearch-installation