ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Μελέτη Τεχνολογιών Ασφάλειας EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform) και Antivirus. A Study of EDR (Endpoint Detection & Response), EPP (Endpoint Protection Platform) and Antivirus Technologies.
Ονοματεπώνυμο Φοιτητή	Ματάκιας Εμμανουήλ
Πατρώνυμο	Βασίλειος
Αριθμός Μητρώου	ΜΠΚΕΔ21031
Επιβλέπων	Κοτζανικολάου Παναγιώτης

Ημερομηνία Παράδωσης **Φεβρουάριος 2024**

Τριμελής Εξεταστική Επιτροπή

Κοτζανικολάου Παναγιώτης	Δουληγέρης Χρήστος	Ψαράκης Μιχαήλ
Αναπληρωτής Καθηγητής	Καθηγητής	Αναπληρωτής Καθηγητής

Ευχαριστίες

Η εργασία αυτή έγινε στα πλαίσια της διπλωματικής μου εργασίας στο πανεπιστήμιο Πειραιώς. Στο σημείο αυτό, θα ήθελα να ευχαριστήσω τους ανθρώπους που με βοήθησαν να φέρω εις πέρας τη διπλωματική μου εργασία.

- τον καθηγητή του Μεταπτυχιακού προγράμματος 'Κυβερνοασφάλεια και Επιστήμη Δεδομένων' Π. Κοτζανικολάου για την επίβλεψη του, στην συγγραφή αυτής της διπλωματικής εργασίας καθώς και
- τον καθηγητή Παπαγεωργίου Σπυρίδωνα, που αφιέρωσε χρόνο για τη γενική εποπτεία του θέματος, όσο και για την πολύτιμη βοήθεια και τη συμπαράσταση που μου πρόσφερε, για την πραγματοποίηση της εργασίας αυτής.

Περίληψη

Τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (EDR) παρέχουν ορατότητα σε εξελιγμένες εισβολές ταιριάζοντας τα συμβάντα του συστήματος με γνωστές αντίθετες συμπεριφορές. Ωστόσο, οι τρέχουσες λύσεις υποφέρουν από τρεις προκλήσεις:

- Τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (EDR) δημιουργούν μεγάλο όγκο ψευδών συναγερμών, δημιουργώντας συσσωρευμένες εργασίες έρευνας για τους αναλυτές.
- Ο προσδιορισμός της ειλικρίνειας αυτών των ειδοποιήσεων απειλής απαιτεί κουραστική χειρωνακτική εργασία, λόγω του συντριπτικού αριθμού κορμών συστήματος χαμηλού επιπέδου, δημιουργώντας ένα πρόβλημα "βελόνας στ'άχυρα".
- Εξαιτίας του τεράστιου φόρτου πόρων της διατήρησης αρχείων καταγραφής, στην πράξη τα αρχεία καταγραφής του συστήματος που περιγράφουν μακροχρόνιες εκστρατείες επιθέσεων, συχνά διαγράφονται πριν από την έναρξη μιας έρευνας.

Σκοπός αυτής της διατριβής είναι να αναλύσει τα οφέλη που προκύπτουν, από τα διάφορα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (EDR). Εισάγουμε την έννοια της πλατφόρμας προστασίας τελικών σημείων (EPP), η οποία είναι μια ολοκληρωμένη λύση ασφαλείας που αναπτύσσεται σε συσκευές τελικού σημείου, για προστασία από απειλές. Θα γίνει μια αναφορά στα προγράμματα προστασίας από ιούς, τα Anti-Virus (AV) και στα προγράμματα προστασίας από ιούς επόμενης γενιάς (NGAV). Θα γίνει μια αναφορά ως προς τις απειλές που διατρέχει ένα τελικό σημείο και τι ζημιά μπορεί να κάνουν αυτές στο τελικό σημείο. Θα εστιάσουμε σε μερικά εμπορικά συστήματα ανίχνευσης και απόκρισης τελικού σημείου (EDR), και θα εστιάσουμε σε τι προσφέρουν στο τελικό μας σημείο. Τέτοιες λύσεις είναι το McAfee MVision EDR, το CrowdStrike Falcon Insight και το Microsoft Defender ATP. Θα εξετάσουμε μερικά από τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (EDR), ανοιχτού κώδικα. Τέτοια συστήματα είναι το Wazuh, το OpenEDR και το Bluespawn. Θα τα εγκαταστήσουμε σε ορισμένα τελικά σημεία και θα εξετάσουμε το πως συμπεριφέρονται κατά τη διάρκεια μιας εισβολής σε κάποιο από τα συστήματα μας. Η εισβολή θα γίνει με το Caldera. Τέλος θα εξηγήσουμε την αναγκαιότητα των συστημάτων ανίχνευσης και απόκρισης τελικού σημείου, για την ασφάλεια των τελικών σημείων και των δεδομένων.

Abstract

Endpoint Detection and Response (**EDR**) tools provide visibility into advanced intrusions by correlating system events with known malicious behaviors. However, current solutions face three challenges:

- EDR tools generate a high volume of false alarms, leading to accumulated research tasks for analysts.
- Verifying the legitimacy of these threat alerts requires labor-intensive work due to the overwhelming number of low-level system logs, creating a "needle in a haystack" problem.
- Due to the massive resource load of maintaining log files, system logs describing long-term attack campaigns are often deleted before an investigation begins.

The goal of this thesis is to analyze the benefits and characteristics of various EDR tools. We introduce the concept of Endpoint Protection Platforms (EPP), which is a comprehensive security solution developed on endpoint devices to protect against threats. We will discuss Anti-Virus programs (AV), next-generation Anti-Virus programs (NGAV), threats to endpoints, and the damage these threats can cause. We will focus on some commercial Endpoint Detection and Response (EDR) systems, such as McAfee MVision EDR, CrowdStrike Falcon Insight, and Microsoft Defender ATP. Additionally, we will examine some open-source EDR systems like Wazuh, OpenEDR, and Bluespawn. These will be installed on specific endpoints, and their behavior during an intrusion, simulated using Caldera, will be analyzed. Finally, we will analyze why Endpoint Detection and Response systems are essential for the proper security of the endpoints and of the relevant data processed by the endpoints.

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1ο – Εισαγωγή στα συστήματα ασφαλείας από διάφορες επιθέσεις δικτύων

1.1 Εισαγωγή

Οι σημερινές εισβολές στα υπολογιστικά συστήματα είναι εξαιρετικά λεπτές και πολύπλοκες. Παράδειγμα τέτοιων επιθέσεων είναι οι Advanced Persistent Threats (APT), στις οποίες οι εισβολείς παραμονεύουν στο εταιρικό δίκτυο για μεγάλο χρονικά διάστημα ,με σκοπό να επεκτείνουν την εμβέλεια τους πριν ξεκινήσουν μια καταστροφική επίθεση στα υπολογιστικά συστήματα, που ανήκουν στο δίκτυο αυτό. (1) (2) (3) Αποφεύγοντας ενέργειες που θα προκαλούσαν αμέσως υποψίες, ο χρόνος παραμονής για τέτοιους επιτιθέμενους μπορεί να κυμαίνεται από εβδομάδες έως μήνες. (4) Αυτό συνέβη σε πολλές παραβιάσεις δεδομένων, όπως το Target, το Equifax και το Office of Personnel Management.

Υπάρχουν αρκετοί τρόποι για να καταλάβουμε διάφορες εισβολές στο δίκτυο μας. Μερικές από αυτές τις λύσεις είναι τα προγράμματα προστασίας από ιούς (**Anti-Virus** ή **AV**), που είναι ένα είδος λογισμικού με τη δυνατότητα της πρόληψης, σάρωσης, ανίχνευσης, εντοπισμού, αλλά και αφαίρεσης κακόβουλων λογισμικών από έναν υπολογιστή. (5) (6) Τα συστήματα ανίχνευσης εισβολέων (Intrusion Detection Systems ή IDS) είναι μια συσκευή ή εφαρμογή λογισμικού, που παρακολουθεί ένα δίκτυο ή διάφορα συστήματα, με σκοπό να βρει κακόβουλη δραστηριότητα ή παραβιάσεις πολιτικής. (7) Όμως υπάρχουν και πολλές άλλες λύσεις. Η εταιρική λύση που χρησιμοποιούμε, με σκοπό την καταπολέμηση των Advanced Persistent Threats (**APT**) είναι γνωστή ως συστήματα Ανίχνευσης και Απόκρισης Τελικού Σημείου (**EDR**). Τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), παρακολουθούν συνεχώς τις δραστηριότητες στους τελικούς κεντρικούς υπολογιστές και προβάλλουν ειδοποιήσεις για απειλές, εάν τυχόν παρατηρηθούν δυνητικά κακόβουλες συμπεριφορές.

1.2 Διαθέσιμα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου

Σε αντίθεση με τις τεχνικές σάρωσης υπογραφών ή ανίχνευσης ανωμαλιών, τα εργαλεία ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), κυνηγούν διάφορες απειλές, αντιστοιχίζοντας τα συμβάντα του συστήματος με μια βάση δεδομένων αντίπαλων Τακτικών, Τεχνικών και Διαδικασιών (**TTPs**). (8) Αυτές οι διαδικασίες είναι χειροκίνητοι κανόνες ειδικών, που περιγράφουν επίθεση χαμηλού επιπέδου σε μοτίβα. Η βάση δεδομένων αντίπαλων Τακτικών, Τεχνικών και Διαδικασιών (TTPs) είναι μοτίβα σε ιεραρχική μορφή, με τακτικές που περιγράφουν, το "γιατί" ένας εισβολέας εκτελεί μια δεδομένη ενέργεια, ενώ οι τεχνικές και οι διαδικασίες περιγράφουν "πώς" εκτελείται αυτή η ενέργεια. (9)

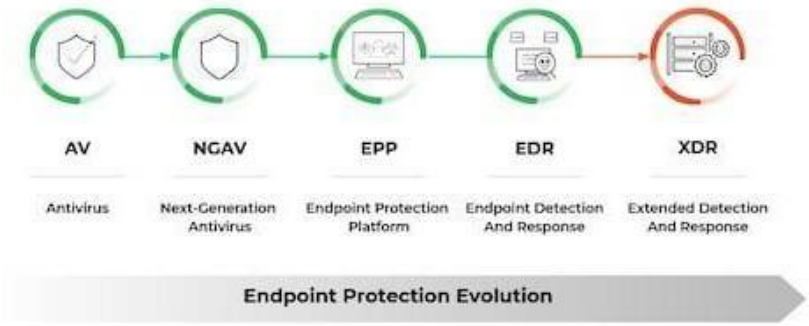
Σύμφωνα με μια πρόσφατη έρευνα, το 61% των οργανισμών αναπτύσσουν δικά τους εργαλεία ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), κυρίως για να παρέχουν πλήρη ορατότητα στις ενέργειες και τις τεχνικές των εισβολέων και να διευκολύνουν τη διερεύνηση απειλών. Το **ATT&CK** της **MITRE** (10) είναι μια δημόσια διαθέσιμη βάση δεδομένων Τακτικών, Τεχνικών και Διαδικασιών (TTP), την οποία επιμελούνται ειδικοί του τομέα, με βάση την

ανάλυση των επιθέσεων Advanced Persistent Threats (APT), πραγματικού κόσμου .Είναι μια από τις πιο ευρέως χρησιμοποιούμενες συλλογές Τακτικών, Τεχνικών και Διαδικασιών (TTP). Στην πραγματικότητα, και τα 10 κορυφαία εργαλεία ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), που ερευνήθηκαν από την Gartner αξιοποιούν τη βάση δεδομένων του **ATT&CK** της **MITRE** για τον εντοπισμό συμπεριφοράς αντιπάλου.

1.3 Άλλοι τρόποι προστασίας τελικών σημείων

Εκτός από τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), έχουμεαναπτύξει και διάφορες πλατφόρμες για την προστασία τελικών σημείων, όπως η πλατφόρμα προστασίας τελικών σημείων (**EPP**), (12) καθώς και τα Anti-Virus και νέας γενιάς **Anti-Virus** (**AV** και **NGAV**). Ο όγκος και η πολυπλοκότητα των κυβερνοεπιθέσεων ολοένα και αυξάνονται στη σημερινή εποχή, με αποτέλεσμα τα συστήματα και τα δεδομένα τεχνολογίας πληροφοριών να βρίσκονται υπό συνεχή απειλή επίθεσης. Οι κυβερνοεπιθέσεις (11) έχουν γίνει ολοένα καιπιο πολυεπίπεδες, χρησιμοποιώντας πολλαπλές, συντονισμένες τεχνικές με σκοπό, οι εισβολείς, να μπαίνουν στα συστήματα πληροφορικής ενός οργανισμού. Τα τελικά σημεία είναι συχνά η πόρτα από την οποία οι εισβολείς αποκτούν αρχική πρόσβαση. Η πλατφόρμα προστασίας τελικού σημείου (EPP) είναι μια ολοκληρωμένη λύση ασφαλείας, που αναπτύσσεταισε συσκευές τελικού σημείου για προστασία από απειλές. Μια πλατφόρμα προστασίας τελικού σημείου (EPP) είναι μια συλλογή τεχνολογιών ασφάλειας τερματικού σημείου, όπως προηγμένα προγράμματα προστασίας από κακόβουλα λογισμικά (Anti-Virus), ανίχνευση και απόκριση τελικού σημείου (**EDR**), κρυπτογράφηση δεδομένων και πρόληψη απώλειας δεδομένων. (13) (14) (15) Αυτές οι τεχνολογίες συνήθως συνεργάζονται με μια συσκευή τερματικού σημείου, με σκοπό τον εντοπισμό, την πρόληψη και την απαλοιφή απειλών ασφαλείας, όπως επιθέσεις κακόβουλου λογισμικού που βασίζονται σε αρχεία και γενικώς κακόβουλη δραστηριότητα. Μια πλατφόρμα προστασίας τελικού σημείου παρέχει ένα πλαίσιο για κοινή χρήση δεδομένων μεταξύ τεχνολογιών προστασίας τελικού σημείου. Αυτό παρέχει μια πιο αποτελεσματική προσέγγιση από μια συλλογή προϊόντων ασφαλείας που δεν έχουν την ικανότητα επικοινωνίας μεταξύ τους.

Όσον αφορά τα προγράμματα προστασίας από κακόβουλα λογισμικά (**Anti-Virus** ή **AV**), το λέει και το όνομα τους, προσπαθούν να προστατέψουν το τελικό μας σημείο από διάφορα κακόβουλα λογισμικά. Το **Anti-Virus** (ή **AV** για συντομογραφία), γνωστό και ως Anti-Malware, είναι ένα είδος λογισμικού με τη δυνατότητα της πρόληψης, σάρωσης, ανίχνευσης, εντοπισμού, αλλά και αφαίρεσης κακόβουλων λογισμικών από έναν υπολογιστή. Τα αποτελέσματα ενός τέτοιου λογισμικού μπορεί να είναι η επιβράδυνση ή ακόμα και η καταστροφή του συστήματος, ή μπορεί να διαγράψει τελείως αρχεία από έναν υπολογιστή. Ο σκοπός ενός κακόβουλου λογισμικού σήμερα είναι συνήθως η απόκτηση προσωπικών και οικονομικών πληροφοριών. Το Anti-Virus αναπτύχθηκε αρχικά για τον εντοπισμό και την αφαίρεση ιών από τους υπολογιστές, εξ ου και το όνομα του. Άρα καταλαβαίνουμε πόσο σημαντικό είναι αυτά τα τρία παραπάνω εργαλεία ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), εργαλεία πλατφόρμας προστασίας τελικών σημείων (**EPP**) και προγράμματα προστασίας από κακόβουλα λογισμικά (**Anti-Virus** ή **AV**), να συνεργάζονται μεταξύ τους για τη προστασία των τελικών σημείων.



Σχήμα 1.1 Αναβάθμιση συστημάτων ασφαλείας με την πάροδο του χρόνου.

1.4 Σκοπός της Διατριβής

Η παρούσα διατριβή αποτελείται από δύο μέρη το θεωρητικό μέρος και το πρακτικό μέρος. Στο θεωρητικό, προσπαθούμε να αναλύσουμε τα συστήματα ασφαλείας που μπορούμε να χρησιμοποιήσουμε σε έναν ηλεκτρονικό υπολογιστή, και τι προστασία παρέχουν απέναντι σε διάφορες επιθέσεις. Αυτά τα συστήματα ασφαλείας είναι τα Endpoint Detection & Response (EDR), Endpoint Protection Platform (EPP) και Anti-Virus (AV). Αυτά τα συστήματα ασφαλείας πολλές φορές αλληλοσυμπληρώνονται και με σκοπό να αποτρέπουν ή να δυσκολεύουν την εκτέλεση του κακόβουλου λογισμικού σε έναν ηλεκτρονικό υπολογιστή.

Στο πρακτικό κομμάτι θα στήσουμε έναν Domain Controller με δύο χρήστες που έχουν εγκατεστημένα EDR. Θα κάνουμε επιθέσεις από έναν τρίτο χρήστη και θα καταγράψουμε τη συμπεριφορά των συστημάτων αυτών.

1.5 Δομή της Διατριβής

Στο κεφάλαιο 2 αναπτύσσουμε τη θεωρία για τα συστήματα ασφαλείας Anti-Virus.Αναφέρουμε τον τρόπο λειτουργίας και τις μεθόδους που χρησιμοποιούν για να αναγνωρίσουν ένα κακόβουλο λογισμικό και πόσο αποτελεσματικά το κάνουν.

Στο κεφάλαιο 3 αναλύουμε την θεωρία στα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), τους τρόπους ανίχνευσης κακόβουλων περιστατικών, τις διαφορές που έχουν με τα συστήματα Anti-Virus. Τέλος κάνουμε μια αναφορά στη χρήση τεχνητής νοημοσύνης πάνω στα EDR.

Στο κεφάλαιο 4 θα κάνουμε μια εισαγωγή στις πλατφόρμες προστασίας τελικού σημείου, στον τρόπο λειτουργίας και στις παροχές που έχουν.

Στο 5ο κεφάλαιο αναλύουμε τον τρόπο λειτουργίας ενός Domain Controller, τη δομή του και τη σχέση του με το Active Directory. Τέλος αναλύουμε τη δομή και το τρόπο λειτουργίας ενός Active Directory.

Στο κεφάλαιο 6 θα ξεκινήσουμε το πειραματικό μέρος. Αναφέρουμε τι θα χρειαστούμε και τον τρόπο με τον οποίο θα στήσουμε το δικό μας το δικό μας εργαστήρι. Θα κάνουμε μια εισαγωγή σε open source EDR που θα χρησιμοποιήσουμε. Θα ξεκινήσουμε identity theft attack και θα καταγράψουμε τα αποτελέσματα των EDR.

Στο κεφάλαιο 7 αναφέρουμε τα συμπεράσματα μας καθώς και μελλοντική έρευνα.

Τέλος στη βιβλιογραφία αναφέρονται όλες οι πηγές που χρησιμοποιήθηκαν με σκοπό τη συγγραφή αυτής της διατριβής.

Κεφάλαιο 2ο – Συστήματα ασφαλείας Anti-Virus (AV)

2.1 Εισαγωγή στα κακόβουλα λογισμικά και Anti-Virus (AV)

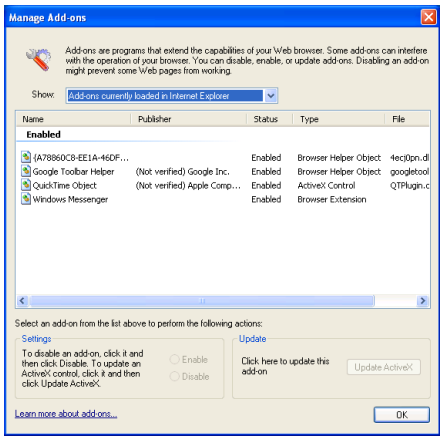
Το **Anti-Virus** (ή **AV** για συντομογραφία), γνωστό και ως **Anti-Malware**, είναι ένα είδος λογισμικού με τη δυνατότητα της πρόληψης, σάρωσης, ανίχνευσης, εντοπισμού, αλλά και αφαίρεσης κακόβουλων λογισμικών από έναν υπολογιστή. Όμως, τι εννοούμε με τον όρο κακόβουλο λογισμικό;

Κακόβουλο λογισμικό είναι ένας όρος, που αναφέρεται σε μια μεγάλη ποικιλία προγραμμάτων που έχουν σχεδιαστεί με σκοπό να βλάψουν ή να κάνουν άλλες ανεπιθύμητες ενέργειες σε έναν υπολογιστή, διακομιστή ή ακόμα και ένα δίκτυο υπολογιστών. Τέτοια μπορεί να είναι ιοί, λογισμικό κατασκοπείας και Trojan. Τα αποτελέσματα ενός τέτοιου λογισμικού μπορεί να είναι η επιβράδυνση ή ακόμα και η καταστροφή του συστήματος, ή μπορεί να διαγράψει τελείως αρχεία από έναν υπολογιστή.

Ο σκοπός ενός κακόβουλου λογισμικού σήμερα είναι συνήθως η απόκτηση προσωπικών και οικονομικών πληροφοριών. Το Anti-Virus αναπτύχθηκε αρχικά για τον εντοπισμό και την αφαίρεση ιών από τους υπολογιστές, εξ ου και το όνομα. Ωστόσο, με τον πολλαπλασιασμό άλλων κακόβουλων λογισμικών, το **AV** άρχισε να προστατεύει τους υπολογιστές και από άλλες διαφορετικές απειλές. Συγκεκριμένα, ο χρήστης είναι προστατευμένος από:

- **Malicious browser helper objects (BHO)**

Τα **BHO** είναι μια λειτουργική μονάδα DLL που έχει σχεδιαστεί για να παρέχει πρόσθετη λειτουργικότητα για το Internet Explorer. (16) (17)



Σχήμα 2.1 Επεκτασιμότητα του Internet Explorer με το BHO

Κάθε φορά που ξεκινά το Internet Explorer, ελέγχει τη registry για το κλειδί HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser

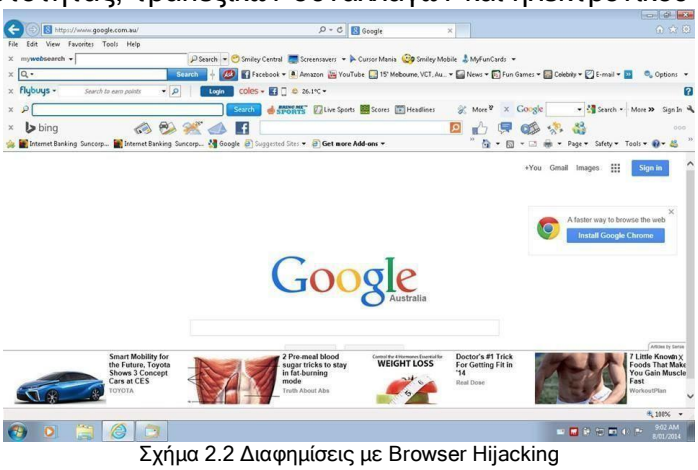
Helper Objects. Εάν ο Internet Explorer βρει αυτό το κλειδί, τότε αναζητά ένα κλειδί CLSID που υπάρχει σε αυτό το μονοπάτι.

Τα κλειδιά CLSID λένε στο browser ποια BHO να φορτώσει. Εάν το κακόβουλο BHO ξεκινήσει και υλοποιήσει τη διεπαφή IObjectWithSite, μπορεί να ελέγχει και να λαμβάνει συμβάντα από τον Internet Explorer.

- **Browser hijacking**

Το **browser hijacking** (18) είναι μια μορφή ανεπιθύμητου λογισμικού, που τροποποιεί τις ρυθμίσεις του browser χωρίς την άδεια του χρήστη, με σκοπό να εισάγει ανεπιθύμητες διαφημίσεις. Ένας browser hijacker μπορεί να αντικαταστήσει την αρχική σελίδα, σελίδα σφάλματος ή μηχανή αναζήτησης με τη δική του. Αυτά χρησιμοποιούνται γενικά για την επιβολή επισκέψεων σε έναν συγκεκριμένο ιστότοπο, αυξάνοντας τα διαφημιστικά του έσοδα.

Σε ορισμένες περιπτώσεις υπάρχει και κάποιο λογισμικό υποκλοπής spyware, όπως είναι ένα λογισμικό καταγραφής πληκτρολογίου για τη συλλογή προσωπικών πληροφοριών, όπως στοιχεία ελέγχου ταυτότητας, τραπεζικών συναλλαγών και ηλεκτρονικού ταχυδρομείου.



Σχήμα 2.2 Διαφημίσεις με Browser Hijacking

- **Ransomware**

Το **Ransomware** είναι ένας τύπος κακόβουλου λογισμικού, που απειλεί να δημοσιεύσει τα προσωπικά δεδομένα του θύματος ή να τον αποκλείσει οριστικά από την πρόσβαση σε αυτά, εκτός εάν υπάρχει οικονομική λύση. (19) (20) Ενώ κάποιο απλό ransomware μπορεί να κλειδώσει το σύστημα χωρίς να καταστρέψει κανένα αρχείο, το πιο προηγμένο κακόβουλο λογισμικό χρησιμοποιεί μια τεχνική που ονομάζεται εκβιασμός crypto viral. Κρυπτογραφεί τα αρχεία του θύματος, καθιστώντας τα απρόσιτα από αυτόν και απαιτεί πληρωμή λύτρων για την αποκρυπτογράφηση τους.

Σχήμα 2.3 Ransomware οδηγεί σε κρυπτογράφηση δεδομένων

- **Keyloggers**

Η καταγραφή πληκτρολογίου είναι η ενέργεια καταγραφής των πλήκτρων που χτυπήθηκαν σε ένα πληκτρολόγιο. Συνήθως τα προγράμματα αυτά εκτελούνται κρυφά, έτσι ώστε το θύμα να μην γνωρίζει ότι παρακολουθείται. Ένα καταγραφικό πλήκτρων μπορεί να είναι ,είτε λογισμικό, είτε υλικό. (21) (22) Τα προγράμματα αυτά είναι νόμιμα και χρησιμοποιούνται για να επιτρέπουν στους εργοδότες να επιβλέπουν τη χρήση των υπολογιστών τους. Τα **keylogger** χρησιμοποιούνται συχνά για την κλοπή κωδικών πρόσβασης και άλλων εμπιστευτικών πληροφοριών.

- **Backdoors**

Το **backdoor** είναι μια τυπικά κρυφή μέθοδος παράκαμψης του κανονικού ελέγχου ταυτότητας ή κρυπτογράφησης σε έναν υπολογιστή. (23) (24) Οι backdoor χρησιμοποιούνται για την εξασφάλιση απομακρυσμένης πρόσβασης σε έναν υπολογιστή ή για την απόκτηση πρόσβασης σε κρυπτογραφικά συστήματα. Από εκεί μπορεί να χρησιμοποιηθεί με σκοπό την απόκτηση πρόσβασης σε προνομιακές πληροφορίες, όπως κωδικοί πρόσβασης, κατεστραμμένα ή διαγραφή δεδομένων σε σκληρούς δίσκους ή μεταφορά πληροφοριών.

- **Rootkits**

Το **rootkit** είναι μια συλλογή λογισμικών υπολογιστή, που έχει σχεδιαστεί για να επιτρέπει την πρόσβαση ενός κακόβουλου χρήστη σε έναν υπολογιστή. (25) Η εγκατάσταση του Rootkit μπορεί να είναι αυτοματοποιημένη ή ένας εισβολέας μπορεί να το εγκαταστήσει, αφού αποκτήσει αυξημένα δικαιώματα. Μόλις εγκατασταθεί, καθίσταται δυνατή η απόκρυψη της εισβολής καθώς και η διατήρηση προνομιακής πρόσβασης. Ο πλήρης έλεγχος ενός συστήματος σημαίνει ότι το υπάρχον λογισμικό μπορεί να τροποποιηθεί.

- **Trojan horse**

Trojan είναι κάθε κακόβουλο λογισμικό που παραπλανά τους χρήστες σχετικά με την πραγματική του πρόθεση. Μόλις εγκατασταθούν, εκτελούν μια σειρά από κακόβουλες ενέργειες. Κάποια από αυτά τείνουν να επικοινωνούν με έναν ή περισσότερους διακομιστές στο Διαδίκτυο και περιμένουν οδηγίες. (26) Δεδομένου ότι, τα μεμονωμένα trojan συνήθως χρησιμοποιούν ένα συγκεκριμένο σύνολο θυρών για αυτήν την επικοινωνία, μπορεί να είναι σχετικά απλό να τα εντοπίσουμε.

- **Worms**

Το **worm** υπολογιστή είναι ένα αυτόνομο πρόγραμμα υπολογιστή κακόβουλου λογισμικού, που αναπαράγεται για να εξαπλωθεί σε άλλους υπολογιστές. Συχνά χρησιμοποιεί ένα δίκτυο υπολογιστών για να εξαπλωθεί, βασιζόμενο σε αστοχίες ασφαλείας στο θύμα για να έχει πρόσβαση σε αυτό.

Το θύμα θα χρησιμοποιηθεί ως κεντρικός υπολογιστής με σκοπό να σαρώσει και να μολύνει άλλους υπολογιστές. Μόλις το worm μολύνει και άλλα θύματα θα συνεχίσει τη διαδικασία, μέχρι να μολυνθούν όλοι οι υπολογιστές του δικτύου. (26)

Τα **worms** χρησιμοποιούν αναδρομικές μεθόδους για να αντιγράψουν τον εαυτό τους και να διανεμηθούν βάσει του νόμου της εκθετικής ανάπτυξης, ελέγχοντας και μολύνοντας έτσι όλο και περισσότερους υπολογιστές σε σύντομο χρονικό διάστημα. Τα **worms** σχεδόν πάντα προκαλούν τουλάχιστον κάποια βλάβη στο δίκτυο, έστω και μόνο με την κατανάλωση εύρους ζώνης, ενώ οι ιοί σχεδόν πάντα καταστρέφουν ή τροποποιούν αρχεία σε έναν στοχευμένο υπολογιστή.

- **Spywares**

Το **Spyware** είναι ένας τύπος κακόβουλου λογισμικού, που προσκολλάται και κρύβεται στο λειτουργικό σύστημα ενός υπολογιστή χωρίς την άδειά του θύματος, με σκοπό τη συλλογή πληροφοριών σχετικά με ένα άτομο ή έναν οργανισμό και την αποστολή τους σε άλλο σύστημα με τρόπο που βλάπτει τον χρήστη. (27)

Μπορεί να χρησιμοποιηθεί για την κατασκοπεία της διαδικτυακής δραστηριότητας και μπορεί να δημιουργήσει ανεπιθύμητες διαφημίσεις ή να κάνει το browser να εμφανίζει συγκεκριμένους ιστότοπους ή αποτελέσματα αναζήτησης.

- **Phishing**

Οι επιθέσεις ηλεκτρονικού ψαρέματος χρησιμοποιούν email ή δόλιες ιστοσελίδες για να προσπαθήσουν να εξαπατήσουν διάφορους χρήστες, ώστε κάποιος κακόβουλος χρήστης να κλέψει προσωπικές ή οικονομικές πληροφορίες, με σκοπό να θέσει σε κίνδυνο έναν λογαριασμό ή να κλέψει χρήματα παριστάνοντας ένα αξιόπιστο σύστημα. (28)

Μπορεί να ισχυριστούν ότι υπάρχει πρόβλημα με τα στοιχεία πληρωμής ή ότι έχουν παρατηρήσει δραστηριότητα σε έναν λογαριασμό και να ζητήσει ο κακόβουλος χρήστης να εισέλθει το θύμα σε έναν σύνδεσμο, για να δώσει προσωπικά του στοιχεία.

- **Άλλες μικρότερες επιθέσεις**

Ορισμένα **AV** εκτός από την προστασία των αρχείων από όλες αυτές τις επιθέσεις που αναφέρθηκαν παραπάνω, προσφέρουν και παραπάνω προστασία, όπως τείχη προστασίας (firewall) και αποκλεισμό ιστότοπων. Τα **AV** έχουν σχεδιαστεί, ώστε να αξιολογούν δεδομένα όπως ιστοσελίδες, αρχεία, λογισμικό και εφαρμογές,αλλά και για να βοηθήσουν στην εύρεση και την εξάλειψη κακόβουλου λογισμικού, όσο το δυνατόν γρηγορότερα.

2.2 Τρόπος λειτουργίας των Anti-Virus

Ένα μεγάλο ερώτημα είναι πως ακριβώς λειτουργεί ένα **AV**. Πολλοί χρήστες δεν ενδιαφέρονται για αυτή την πληροφορία, απλά ενδιαφέρονται να είναι προστατευμένοι. (5) (29) (30)

Το λογισμικό προστασίας από ιούς αρχίζει τη λειτουργία του σαρρώνοντας τα

προγράμματα και τα αρχεία του υπολογιστή στο οποίο είναι εγκατεστημένο, σε μια βάση δεδομένων γνωστών τύπων κακόβουλων λογισμικών και ελέγχει αν τα αρχεία και τα προγράμματα δεν είναι κακόβουλα.

Δεδομένου ότι καθημερινά δημιουργούνται νέα κακόβουλα λογισμικά και μολύνουν νέα συστήματα, το **AV** σαρώνει επίσης τους υπολογιστές για την πιθανότητα νέων ή άγνωστων απειλών κακόβουλου λογισμικού.Τα **AV** χρησιμοποιούν τρεις διαφορετικούς τρόπους ανίχνευσης:

1. Ειδική ανίχνευση:

Αναζητά σε όλα τα σημεία του υπολογιστή διάφορα γνωστά κακόβουλα λογισμικά. (30) (5)

2. Γενική ανίχνευση:

Αναζητά γνωστά διάφορα τμήματα ή διάφορους τύπους κακόβουλου λογισμικού και μοτίβα διαδικασιών κακόβουλων λογισμικών που σχετίζονται με μια κοινή βάση κώδικα. (30) (5)

3. Ευρετική ανίχνευση:

Σαρώνει όλο τον υπολογιστή για διάφορα άγνωστα κακόβουλα λογισμικά, εντοπίζοντας γνωστές ύποπτες δομές αρχείων.
Όταν το AV εντοπίσει ένα αρχείο που περιέχει έναν ιό, τότε η κίνηση που θα κάνει είναι να το απομονώσει και συνεχώς να ενημερώνει το χρήστη πως πρέπει να γίνει διαγραφή του ιού, καθιστώντας το απρόσιτο για το χρήστη και αφαιρώντας τον κίνδυνο για τη συσκευή. (30) (5)

2.2.1 Μέθοδοι αναγνώρισης που χρησιμοποιεί το Anti-Virus

Ένα από τα λίγα σταθερά θεωρητικά αποτελέσματα στη μελέτη των ιών υπολογιστών είναι η απόδειξη του Frederick B. Cohen το 1987, ότι δεν υπάρχει αλγόριθμος που να μπορεί να ανιχνεύσει τέλεια όλους τους πιθανούς ιούς. Ωστόσο, χρησιμοποιώντας διαφορετικά επίπεδα άμυνας, μπορεί να επιτευχθεί ένα ικανοποιητικό αποτέλεσμα ανίχνευσης.Υπάρχουν διάφορες μέθοδοι που μπορούν να χρησιμοποιήσουν τα Anti-Virus για τον εντοπισμό ενός κακόβουλου λογισμικού:

- **Ανίχνευση Sandbox**

Υπάρχει μια συγκεκριμένη τεχνική ανίχνευσης που βασίζεται στη συμπεριφορά ενός κακόβουλου λογισμικού, η οποία, αντί να ανιχνεύει το δακτυλικό αποτύπωμα συμπεριφοράς κατά το χρόνο εκτέλεσης, εκτελεί τα προγράμματα σε ένα εικονικό περιβάλλον, καταγράφοντας ποιες ενέργειες εκτελεί το πρόγραμμα. (30)

Έτσι ανάλογα με το αποτέλεσμα και με τις ενέργειες που έχουν καταγραφεί, το **AV** μπορεί να καθορίσει εάν το πρόγραμμα είναι κακόβουλο ή όχι. Εάν δεν είναι, τότε το πρόγραμμα αυτό εκτελείται σε πραγματικό περιβάλλον.

Αν και αυτή η τεχνική έχει αποδειχθεί αρκετά αποτελεσματική, δεδομένης της βαρύτητας και της βραδύτητάς της, χρησιμοποιείται σπάνια σε λύσεις προστασίας από ιούς τελικού χρήστη.

- **Τεχνικές εξόρυξης δεδομένων**

Οι τεχνικές αυτές, είναι από τις πιο πρόσφατες προσεγγίσεις που εφαρμόζονται στον εντοπισμό κακόβουλου λογισμικού. Οι αλγόριθμοι εξόρυξης δεδομένων και οι αλγόριθμοι μηχανικής μάθησης χρησιμοποιούνται για να προσπαθήσουν, να ταξινομήσουν τη συμπεριφορά ενός αρχείου (είτε ως κακόβουλο είτε ως καλόηθες) δεδομένης μιας σειράς χαρακτηριστικών του αρχείου, που εξάγονται από το ίδιο. (30)

- **Ανιχνευση με βάση τις υπογραφές**

Το παραδοσιακό λογισμικό Anti-Virus βασίζεται σε μεγάλο βαθμό στις υπογραφές για τον εντοπισμό κακόβουλου λογισμικού. Ουσιαστικά, όταν ένα δείγμα κακόβουλου λογισμικού φτάνει στα χέρια μιας εταιρείας προστασίας από ιούς, αναλύεται από διάφορους ερευνητές κακόβουλου λογισμικού ή από συστήματα δυναμικής ανάλυσης. (30)

Αν διαπιστωθεί, ότι πρόκειται για ένα κακόβουλο λογισμικό, τότε εξάγεται η κατάλληλη υπογραφή του αρχείου και προστίθεται στη βάση δεδομένων υπογραφών του λογισμικού αυτού. Παρόλο που η προσέγγιση αυτή, μπορεί να πιάσει αποτελεσματικά ένα κακόβουλο λογισμικό, οι δημιουργοί του κακόβουλου λογισμικού προσπαθούν να παρακάμψουν τα Anti-Virus, γράφοντας "ολιγόμορφους", "πολυμορφικούς" και "μεταμορφικούς" ιούς, που έχουν σκοπό να τροποποιούνται με κρυπτογράφηση διαφόρων τμημάτων του εαυτού τους, με αποτέλεσμα να μην ταιριάζουν με τις υπογραφές κακόβουλων λογισμικών, που έχουν καταγραφεί στη βάση δεδομένων.Πολλά κακόβουλα λογισμικά και ιοί ξεκινούν ως μια απλή και ενιαία μόλυνση και, είτε από διάφορες μεταλλάξεις, είτε από διάφορες βελτιώσεις που έγιναν από άλλους εισβολείς, μπορούν να εξελιχθούν σε τελείως διαφορετικά στελέχη, που ονομάζονται παραλλαγές.

2.2.2 Ομαδική ανίχνευση που χρησιμοποιεί το Anti-Virus

Όπως καταλαβαίνουμε η γενική ανίχνευση δεν αρκεί, καθώς αναφέρεται μόνο στον εντοπισμό και την αφαίρεση ιών που έχουν έναν μόνο ορισμό. Για παράδειγμα, το trojan Vundo έχει πολλά και διαφορετικά στελέχη, σύμφωνα με ορισμένα Anti-Virus.

Η εταιρεία Symantec ταξινομεί τα διάφορα στελέχη της οικογένειας Vundo σε δύο ξεχωριστές κατηγορίες, Trojan.Vundo και Trojan.Vundo.B. Αν και μπορούμε πολύ εύκολα να τακτοποιήσουμε ένα συγκεκριμένο κακόβουλο λογισμικό, έχουμε την δυνατότητα να ταυτοποιήσουμε πολύ πιο γρήγορα μια οικογένεια κακόβουλων λογισμικών, μέσω μιας γενικής υπογραφής ή μέσω μιας ανακριβούς αντιστοίχισης με μια υπάρχουσα υπογραφή στη βάση δεδομένων.

Οι ερευνητές κακόβουλων λογισμικών έχουν καταφέρει, να ανακαλύψουν κοινές περιοχές που όλα τα κακόβουλα λογισμικά μιας οικογένειας μοιράζονται μοναδικά.Με αυτόν τον τρόπο, έχουν τη δυνατότητα να δημιουργήσουν μια ενιαία γενική υπογραφή για όλη την οικογένεια.

Αυτές οι υπογραφές περιέχουν συχνά μη συνεχόμενο κώδικα, χρησιμοποιώντας άσχετους χαρακτήρες. Αυτοί οι άσχετοι χαρακτήρες επιτρέπουν στο σαρωτή να ανιχνεύει κακόβουλα λογισμικά ακόμα κι αν είναι γεμάτα με επιπλέον κώδικα που δεν βγάζει κανένα νόημα. Μια ανίχνευση που χρησιμοποιεί αυτή τη τεχνική λέγεται "ευρετική ανίχνευση".

2.3 Ιστορικά δεδομένα

Το πρόβλημα των υπολογιστών από κακόβουλα λογισμικά εμφανίζεται από πολύ νωρίς, συγκεκριμένα από τη δεκαετία του 1950. Έτσι εμφανίζεται και η ανάγκη δημιουργίας προγραμμάτων προστασίας από ιούς και γενικά από κακόβουλα λογισμικά.

1949-1980

Οι ρίζες του κακόβουλου λογισμικού χρονολογούνται από το 1949, όταν ο Ούγγρος επιστήμονας John von Neumann δημοσίευσε τη «Θεωρία των αυτοαναπαραγωγικών αυτομάτων». Το πρώτο γνωστό κακόβουλο λογισμικό εμφανίστηκε το 1971 και ονομάστηκε «Creeper virus». Αυτός το κακόβουλο λογισμικό μόλυνε τους μεγάλους υπολογιστές PDP-10 της Digital Equipment Corporation (DEC), που έτρεχαν το λειτουργικό σύστημα TENEX.

Ο ιός Creeper διαγράφηκε από ένα πρόγραμμα, που δημιουργήθηκε από τον Ray Tomlinson γνωστό ως "The Reaper". Μερικοί χρήστες θεωρούν το "The Reaper" ως το πρώτο Anti-Virus που γράφτηκε ποτέ. Το Reaper ήταν στην πραγματικότητα και αυτός ένας ιός που σχεδιάστηκε ειδικά, για να αφαιρεί τον ιό Creeper.

1980-1990

Τον ιό Creeper διαδέχτηκαν άλλοι πολλοί ιοί. Το πρώτο γνωστό κακόβουλο λογισμικό που εμφανίστηκε,μετά τον Creeper, ήταν το "Elk Cloner". Αυτό το κακόβουλο λογισμικό εμφανίστηκε το 1981,που μόλυνε τους υπολογιστές Apple II. Το 1983, ο όρος "ιός υπολογιστών" επινοήθηκε από τον Fred Cohen σε ένα από τα πρώτα δημοσιευμένα άρθρα σε πανεπιστημιακό περιοδικό, σχετικά με τους ιούς υπολογιστών.

Ο Cohen χρησιμοποίησε τον όρο "ιός υπολογιστή" για να περιγράψει προγράμματα, που επηρεάζουν άλλα προγράμματα υπολογιστή τροποποιώντας τα με τέτοιο τρόπο, ώστε να περιλαμβάνουν ένα εξελιγμένο αντίγραφο του εαυτού τους. Ένας πιο πρόσφατος ορισμός του κακόβουλου λογισμικού έχει δοθεί από τον Ούγγρο ερευνητή ασφαλείας Péter Szőr, ο οποίος το περιγράφει ως έναν κώδικα που αναπαράγει αναδρομικά ένα εξελιγμένο αντίγραφο του εαυτού του. Μια από τις πρώτες πραγματικές ευρέως διαδεδομένες μολύνσεις, ήταν ο "Brain" το 1986, ο οποίος ήταν συμβατός με τους υπολογιστές της IBM.

Από εκείνη τη χρονολογία έχει παρατηρηθεί, ότι ο αριθμός των κακόβουλων λογισμικών έχει αυξηθεί εκθετικά. Οι περισσότεροι από τους ιούς υπολογιστών που δημιουργήθηκαν στις αρχές και στα μέσα της δεκαετίας του 1980 περιορίζονταν στην αντιγραφή του εαυτού τους και δεν έκαναν κάτι σπουδαίο.

Αυτό άλλαξε, όταν όλο και περισσότεροι προγραμματιστές εξοικειώθηκαν με τον προγραμματισμό ιών υπολογιστών και δημιούργησαν ιούς ικανούς να χειραγωγήσουν υπολογιστές ή ακόμα και να καταστρέψουν δεδομένα σε υπολογιστές που έχουν μολυνθεί. Πριν γίνει το Διαδίκτυο ευρέως γνωστό, οι ιοί υπολογιστών μεταδίδονταν συνήθως από μολυσμένες δισκέτες. Τα Anti-Virus ενημερωνόταν σχετικά σπάνια.

Οι έλεγχοι για την ύπαρξη ιών γίνονταν στα εκτελέσιμα αρχεία και στους τομείς εκκίνησης των δισκέτων και των σκληρών δίσκων. Καθώς όμως, η χρήση του Διαδικτύου έγινε ευρέως γνωστή, οι ιοί άρχισαν να εξαπλώνονται διαδικτυακά.Μια από τις πρώτες αφαιρέσεις ενός ιού υπολογιστών που ήταν τεκμηριωμένη δημόσια πραγματοποιήθηκε από τον Bernd Fix το 1987, που αφαίρεσε τον Vienna Virus. (5)

Το 1987, ο Andreas Lüning και ο Kai Figge, ιδρυτές της G Data Software το 1985, κυκλοφόρησαν το πρώτο τους Anti-Virus, συμβατό με την πλατφόρμα Atari ST.Την ίδια χρονιά κυκλοφόρησε το Ultimate Virus Killer (UVK) από την ίδια εταιρεία, συμβατό πάλι με το AtariST και το AtariFalcon. (5)

Το 1987, στις Ηνωμένες Πολιτείες, ο John McAfee ίδρυσε την εταιρεία McAfee και, στο τέλος εκείνου του έτους, κυκλοφόρησε την πρώτη έκδοση του VirusScan. Επίσης το 1987 στην

Τσεχοσλοβακία, οι Peter Paško, Rudolf Hrubý και Miroslav Trnka δημιούργησαν την πρώτη έκδοση του **Anti-Virus** NOD. Το 1987-1988, κυκλοφόρησαν τα δύο πρώτα ευρετικά **Anti-Virus**. (5)

Το Flushot Plus δημιουργήθηκε από τον Ross Greenberg και το Anti4us από τον Erwin Lanting. Ωστόσο, η ευρετική μέθοδος που χρησιμοποιήθηκε από τα πρώτα **AV** ήταν τελείως διαφορετική από αυτή σήμερα. Οι πρώιμες ευρετικές μηχανές βασίζονταν στη διαίρεση του binary σε διαφορετικά τμήματα: δεδομένα και κώδικας.

Οι αρχικοί ιοί αναδιοργάνωναν τη διάταξη των τμημάτων με σκοπό να μεταβούν στο τέλος του αρχείου, όπου βρισκόταν ο πραγματικός κακόβουλος κώδικας. Αργότερα προστέθηκαν άλλα είδη πιο προηγμένων ευρετικών μεθόδων, όπως ύποπτα ονόματα ενοτήτων, λανθασμένο μέγεθος κεφαλίδας, κανονικές εκφράσεις και μερική αντιστοίχιση μοτίβων στη μνήμη.

Στη Γερμανία, ο Tjark Auerbach ίδρυσε την Avira το 1988 και κυκλοφόρησε την πρώτη έκδοση του AntiVir. Επίσης εκείνη την χρονολογία ο Frans Veldman κυκλοφόρησε την πρώτη έκδοση του ThunderByte Antivirus, επίσης γνωστή ως TBAV.

Στην Τσεχοσλοβακία, ο Pavel Baudiš και ο Eduard Kučera ξεκίνησαν το Avast και κυκλοφόρησαν την πρώτη του έκδοση. Τον Ιούνιο του 1988, στη Νότια Κορέα, ο Ahn Cheol-Soo κυκλοφόρησε το πρώτο του λογισμικό προστασίας από ιούς, με το όνομα V1.

Τέλος, το φθινόπωρο του 1988, στο Ηνωμένο Βασίλειο, ο Alan Solomon ίδρυσε την εταιρεία S&S International και δημιούργησε το Dr. Solomon's Anti-Virus Toolkit.

1990-2000

Το 1990, στην Ισπανία, ο Mikel Urizarbarrena ίδρυσε την Panda Security. Στην Ουγγαρία, ο ερευνητής ασφάλειας Péter Szőr κυκλοφόρησε την πρώτη έκδοση του antivirus Pasteur.

Στην Ιταλία, ο Gianfranco Tonello δημιούργησε την πρώτη έκδοση του VirIT eXplorer antivirus και στη συνέχεια ίδρυσε την TG Soft ένα χρόνο αργότερα. Το 1990 ιδρύθηκε ο Οργανισμός Έρευνας για την Καταπολέμηση των ιών υπολογιστών CARO και το 1991 κυκλοφόρησε το "Virus Naming Scheme", που αρχικά γράφτηκε από τους Friðrik Skúlason και Vesselin Bontchev.Το 1991, στις Ηνωμένες Πολιτείες, η Symantec κυκλοφόρησε την πρώτη έκδοση του Norton AntiVirus.

Την ίδια χρονιά, στην Τσεχία, ο Jan Gritzbach και ο Tomáš Hofer ίδρυσαν την AVG Technologies και κυκλοφόρησαν την πρώτη έκδοση του Anti-Virus Guard (AVG) μόλις το 1992.

Από την άλλη πλευρά, στη Φινλανδία, η F-Secure κυκλοφόρησε την πρώτη έκδοση του προϊόντος προστασίας από ιούς. Το 1992, στη Ρωσία, ο Igor Danilov κυκλοφόρησε την πρώτη έκδοση του SpiderWeb, η οποία αργότερα ονομάστηκε Dr. Web.Το 1994, το AV-TEST ανέφερε ότι υπήρχαν 28.613 μοναδικά δείγματα κακόβουλου λογισμικού, με βάση τον αλγόριθμο κατακερματισμού MD5, στη βάση δεδομένων τους, ενώ το 1999 υπήρχαν 98.428 μοναδικά δείγματα.Με τον καιρό ιδρύθηκαν και άλλες εταιρείες.

Το 1996, στη Ρουμανία, ιδρύθηκε η Bitdefender και κυκλοφόρησε την πρώτη έκδοση του Anti-Virus eXpert (AVX). Το 1997, στη Ρωσία, ο Eugene Kaspersky και η Natalya Kaspersky συνίδρυσαν την εταιρεία ασφαλείας Kaspersky Lab.

2000-2005

Το 2000, ο Rainer Link και ο Howard Fuhs ξεκίνησαν την πρώτη μηχανή προστασίας από ιούς ανοιχτού κώδικα, που ονομάζεται OpenAntivirus Project.Το 2001, ο Tomasz Kojm κυκλοφόρησε την πρώτη έκδοση του ClamAV, της πρώτης μηχανής προστασίας από ιούς ανοιχτού κώδικα που διατέθηκε στο εμπόριο.

Το 2002, στο Ηνωμένο Βασίλειο, ο Morten Lund και ο Theis Søndergaard συνίδρυσαν την εταιρία προστασίας από ιούς BullGuard.Το 2005, το AV-TEST ανέφερε ότι υπήρχαν 333.425 μοναδικά δείγματα κακόβουλου λογισμικού (με βάση το MD5) στη βάση δεδομένων τους.

2005-2014

Το 2007, το AV-TEST ανέφερε έναν αριθμό 5.490.960 νέων μοναδικών δειγμάτων κακόβουλου λογισμικού μόνο για εκείνο το έτος. Το 2012 και το 2013, οι εταιρείες προστασίας από ιούς ανέφεραν, ότι νέα δείγματα κακόβουλου λογισμικού κυμαίνονταν από 300.000 έως πάνω από 500.000 την ημέρα.

Με τα χρόνια έχει καταστεί απαραίτητο για το λογισμικό προστασίας από ιούς, να χρησιμοποιεί πολλές διαφορετικές στρατηγικές π.χ. συγκεκριμένη προστασία email και δικτύου ή μονάδες χαμηλού επιπέδου και αλγόριθμους ανίχνευσης, καθώς και να ελέγχει μια αυξανόμενη ποικιλία αρχείων, αντί για απλά εκτελέσιμα.

Οι ισχυρές μακροεντολές που χρησιμοποιούνται σε εφαρμογές επεξεργασίας κειμένου, όπως το Microsoft Word, παρουσίαζαν κίνδυνο. Τα προγράμματα εγγραφής ιών θα μπορούσαν να χρησιμοποιήσουν τις μακροεντολές για να γράψουν ιούς που είναι ενσωματωμένοι σε έγγραφα.

Αυτό σήμαινε, ότι οι υπολογιστές θα μπορούσαν πλέον να κινδυνεύουν από μόλυνση ανοίγοντας έγγραφα με κρυφές προσαρτημένες μακροεντολές. Αργότερα προγράμματα ηλεκτρονικού ταχυδρομείου, ιδιαίτερα το Outlook Express και το Outlook της Microsoft, ήταν ευάλωτα σε ιούς, που ήταν ενσωματωμένοι στο ίδιο το σώμα του email.

Ο υπολογιστής ενός χρήστη θα μπορούσε να μολυνθεί με το άνοιγμα ή την προεπισκόπηση ενός μηνύματος. Το 2005, η F-Secure ήταν η πρώτη εταιρεία ασφαλείας που ανέπτυξε μια τεχνολογία Anti-Rootkit, που ονομάζεται BlackLight. Επειδή οι περισσότεροι χρήστες είναι συνήθως συνδεδεμένοι στο Διαδίκτυο σε συνεχή βάση, ο Jon Oberheide πρότεινε για πρώτη φορά ένα σχέδιο προστασίας από ιούς, που βασίζεται στο Cloud το 2008.

Τον Φεβρουάριο του 2008 η McAfee Labs πρόσθεσε την πρώτη λειτουργία κατά του κακόβουλου λογισμικού, που βασίζεται σε cloud στο VirusScan με το όνομα Artemis. Δοκιμάστηκε από την AV-Comparatives τον Φεβρουάριο του 2008 και αποκαλύφθηκε επίσημα τον Αύγουστο του 2008 στο McAfee VirusScan.

2014-σήμερα

Μετά την έκδοση του 2013 της έκθεσης APT 1 από τη Mandiant, ο κλάδος έχει δει μια στροφή προς προσεγγίσεις χωρίς υπογραφή. Μια μέθοδος που είναι ικανή να ανιχνεύει και να μετριάζει τις επιθέσεις zero-day.

Έχουν εμφανιστεί πολυάριθμες προσεγγίσεις για την αντιμετώπιση αυτών των νέων μορφών απειλών, συμπεριλαμβανομένης της ανίχνευσης συμπεριφοράς με τη βοήθεια της τεχνητής νοημοσύνης, της μηχανικής μάθησης και των αρχείων που βασίζεται σε τεχνικές Cloud.

Μια μέθοδος από το Bromium περιλαμβάνει την τεχνική της micro-virtualization,με σκοπό την προστασία των υπολογιστών από κακόβουλη εκτέλεση κώδικα που ξεκινά από τον τελικό χρήστη. Μια άλλη προσέγγιση από τις Sentinel One και Carbon Black εστιάζει στην ανίχνευση συμπεριφοράς δημιουργώντας ένα πλήρες πλαίσιο γύρω από κάθε διαδρομή εκτέλεσης διεργασιών σε πραγματικό χρόνο, ενώ η εταιρεία Cylance αξιοποιεί ένα μοντέλο τεχνητής νοημοσύνης, που βασίζεται στη μηχανική μάθηση.

Αυτές οι προσεγγίσεις ορίζονται από τα μέσα ενημέρωσης και τις εταιρείες αναλυτών ως «επόμενης γενιάς» antivirus και συναντούν την ταχεία υιοθέτηση στην αγορά, ως πιστοποιημένες τεχνολογίες προστασίας από ιούς. (5)

2.4 Αποτελεσματικότητα Anti-Virus

Μελέτες τον Δεκέμβριο του 2007 έδειξαν, ότι η αποτελεσματικότητα του λογισμικού προστασίας από ιούς είχε μειωθεί το προηγούμενο έτος, ιδιαίτερα έναντι άγνωστων ή επιθέσεων zero-day. Το περιοδικό υπολογιστών c't βρήκε ότι τα ποσοστά ανίχνευσης για αυτές τις απειλές είχαν μειωθεί από 40-50% το 2006 και σε 20-30% το 2007. Εκείνη την εποχή, η μόνη εξαίρεση ήταν το antivirus NOD32, το οποίο διαχειριζόταν ποσοστό ανίχνευσης 68%. Σύμφωνα με τον ιστότοπο του ZeuS tracker, το μέσο ποσοστό ανίχνευσης για όλες τις παραλλαγές του γνωστού trojan ZeuS είναι μόλις 40%.

Το πρόβλημα μεγεθύνεται από την αλλαγή της πρόθεσης των δημιουργών ιών. Στα πρώτα βήματα των ιών, οι ιοί ήταν αρκετά προφανείς. Εκείνη την εποχή, οι ιοί γράφονταν από ερασιτέχνες και παρουσίαζαν καταστροφική συμπεριφορά ή ορισμένα αναδυόμενα παράθυρα. Οι σύγχρονοι ιοί, όμως γράφονται από επαγγελματίες, που χρηματοδοτούνται από εγκληματικές οργανώσεις.

Οι δοκιμές των Anti-Virus σε όλους τους κύριους σαρωτές ιών δείχνουν λεπτομερώς, ότι κανένα δεν παρέχει 100% ανίχνευση ιών. Τα καλύτερα παρείχαν έως και 99,9% ανίχνευση σε προσομοιωμένες καταστάσεις πραγματικού κόσμου, ενώ τα χαμηλότερα παρείχαν 91,1% σε δοκιμές που διεξήχθησαν τον Αύγουστο του 2013. Πολλοί σαρωτές ιών παράγουν επίσης ψευδώς θετικά αποτελέσματα, εντοπίζοντας καλοήθη αρχεία ως κακόβουλο λογισμικό. (30)

2.5 Κακόβουλα λογισμικά νέας τεχνολογίας

Τα Anti-Virus, όπως είναι φυσιολογικό δεν είναι πάντα αποτελεσματικά απέναντι σε νέα κακόβουλα λογισμικά.Αυτό συμβαίνει κυρίως, επειδή οι σχεδιαστές κακόβουλων λογισμικών δοκιμάζουν τα νέα δημιουργήματα τους στα σημαντικότερα Anti-Virus,με σκοπό να βεβαιωθούν ότι δεν εντοπίζονται από αυτά πριν μολύνουν υπολογιστές. Ορισμένα νέα κακόβουλα λογισμικά, ιδιαίτερα ransomware, χρησιμοποιούν πολυμορφικό κώδικα, με σκοπό να αποφύγουν τον εντοπισμό από Anti-Virus.

Αυτός ο τύπος κακόβουλου λογισμικού, ransomware, προέρχεται από διάφορους ιστότοπους που χρησιμοποιούν πολυμορφισμό.Αυτό σημαίνει ότι τυχαιοποιούν το αρχείο που στέλνουν και λαμβάνεται από γνωστά Anti-Virus. Σε αυτές τις περιπτώσεις το Anti-Virus που εκτελείται δεν εντοπίζει τίποτα. Στην πραγματικότητα είναι πολύ δύσκολο να ξεφορτωθείς το

ransomware και ποτέ δεν είναι σίγουρο ότι το κακόβουλο λογισμικό έχει φύγει πραγματικά από τον υπολογιστή. Συνήθως αυτού του τύπου το κακόβουλο λογισμικό , χρησιμοποιεί τη Μονάδα Επεξεργασίας Γραφικών (GPU) για να αποφύγει τον εντοπισμό από λογισμικά προστασίας. Η πιθανή επιτυχία αυτού περιλαμβάνει την παράκαμψη της Κεντρικής Μονάδας Επεξεργασίας(CPU), προκειμένου να καταστήσει πολύ πιο δύσκολο για τους ερευνητές ασφάλειας να αναλύσουν την εσωτερική λειτουργία του κακόβουλου λογισμικού.

Καθώς το **Internet of Things (IoT)** αναπτύσσεται και αναπτύσσεται ολοένα και περισσότερο η τεχνολογία, αυξάνεται ο κίνδυνος του εγκλήματος στον κυβερνοχώρο, ακόμα και για τα κινητά τηλέφωνα και άλλες συσκευές που συνδέονται στο Διαδίκτυο από νέα κακόβουλα λογισμικά . Συνεπώς πρέπει να βρούμε λύσεις και για τις IOT συσκευές και όχι μόνο για τον προσωπικό υπολογιστή. (30)

2.6 Μειονεκτήματα των Anti-Virus

Ένα λογισμικό προστασίας από ιούς εκτός από την προστασία που παρέχει σε υπολογιστικό σύστημα, μπορεί να το επηρεάσει με άσχημο τρόπο. Μπορεί να ρίξει κατακόρυφα

την απόδοση ενός υπολογιστή. Επιπλέον, αρκετοί χρήστες μπορεί να παρασύρονται σε μια ψευδή αίσθηση ασφάλειας όταν χρησιμοποιούν τον υπολογιστή με εγκατεστημένο Anti-Virus, θεωρώντας τους υπολογιστές τους άτρωτους, όμως μπορεί το Anti-Virus να παίρνει λανθασμένες αποφάσεις.

Μια λανθασμένη απόφαση μπορεί να οδηγήσει σε παραβίαση ασφάλειας. Εάν το λογισμικό προστασίας από ιούς χρησιμοποιεί ευρετική ανίχνευση, πρέπει να ρυθμιστεί με ακρίβεια για να ελαχιστοποιηθεί η εσφαλμένη αναγνώριση του αβλαβούς λογισμικού ως κακόβουλου (ψευδώς θετικό).Το ίδιο το λογισμικό προστασίας από ιούς εκτελείται συνήθως στο πολύ αξιόπιστο επίπεδο πυρήνα του λειτουργικού συστήματος, για να του επιτρέψει την πρόσβαση σε όλες τις πιθανές κακόβουλες διεργασίες και αρχεία, δημιουργώντας πιθανή την περίπτωση μιας πιθανής επίθεσης.

Η Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (NSA) και οι υπηρεσίες πληροφοριών του Κυβερνητικού Γραφείου Επικοινωνιών του Ηνωμένου Βασιλείου (GCHQ), αντίστοιχα, εκμεταλλεύονται λογισμικό προστασίας από ιούς για να κατασκοπεύουν χρήστες. Το λογισμικό προστασίας από ιούς έχει εξαιρετικά προνομιακή και αξιόπιστη πρόσβαση στο υποκείμενο λειτουργικό σύστημα, γεγονός που το καθιστά πολύ πιο ελκυστικό στόχο για απομακρυσμένες επιθέσεις.

2.7 Cloud Anti-Virus

Το λογισμικό προστασίας από ιούς Cloud είναι μια τεχνολογία που χρησιμοποιεί ένα ελαφρύ λογισμικό στον προστατευόμενο υπολογιστή, ενώ γίνονται αρκετές αναλύσεις δεδομένων των υπολογιστών στην υποδομή του παρόχου. Μια προσέγγιση για την εφαρμογή προστασίας από ιούς cloud περιλαμβάνει τη σάρωση ύποπτων αρχείων χρησιμοποιώντας πολλαπλά λογισμικά προστασίας από ιούς. Αυτή η προσέγγιση προτάθηκε από μια πρώιμη εφαρμογή της προστασίας με τη βοήθεια του Cloud από ιούς που ονομάζεται CloudAV.

Το CloudAV σχεδιάστηκε για να στέλνει προγράμματα ή έγγραφα σε ένα Cloud δικτύου, όπου χρησιμοποιούνται ταυτόχρονα πολλαπλά προγράμματα προστασίας από ιούς και ανίχνευσης συμπεριφοράς, προκειμένου να βελτιωθούν τα ποσοστά ανίχνευσης. Η παράλληλη σάρωση αρχείων με χρήση δυνητικά ασυμβίβαστων σαρωτών προστασίας από ιούς επιτυγχάνεται, με τη δημιουργία μιας εικονικής μηχανής ανά μηχανή ανίχνευσης και συνεπώς

την εξάλειψη πιθανών προβλημάτων.

Το CloudAV μπορεί επίσης να εκτελέσει "αναδρομική ανίχνευση", σύμφωνα με την οποία η μηχανή ανίχνευσης Cloud σαρώνει ξανά όλα τα αρχεία στο ιστορικό πρόσβασης και στα αρχεία του εκάστοτε υπολογιστή όταν εντοπίζεται μια νέα απειλή, βελτιώνοντας έτσι την ταχύτητα ανίχνευσης νέας απειλής.

Τέλος, το CloudAV είναι μια λύση για αποτελεσματική σάρωση ιών σε συσκευές που δεν διαθέτουν την υπολογιστική ισχύ για να εκτελέσουν οι ίδιες τις σαρώσεις. Μερικά παραδείγματα προϊόντων προστασίας από ιούς cloud είναι το Panda Cloud Antivirus και το Immunet. Η Comodo Group έχει δημιουργήσει επίσης antivirus που βασίζεται σε cloud.

Κεφάλαιο 3ο - Συστήματα ανίχνευσης και απόκρισης τελικού σημείου (EDR)

3.1 Εισαγωγή στα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (EDR)

Το **Endpoint Detection and Response (EDR)**, που αναφέρεται ως ανίχνευση τελικού σημείου και απόκριση απειλών (**EDTR**), είναι ένα σύστημα συλλογής και ανάλυσης πληροφοριών σε συστήματα τελικού σημείου, με στόχο την εύρεση παραβιάσεων ασφαλείας παρακολουθώντας τις συσκευές τελικού χρήστη. (31) (32) Εκτός από τον εντοπισμό, έχει ως στόχο τη γρήγορη απόκριση σε αποκαλυφθείσες ή πιθανές απειλές στον κυβερνοχώρο, όπως για παράδειγμα είναι το ransomware και malware. Χρησιμοποιεί διάφορες τεχνικές ανάλυσης δεδομένων για τον εντοπισμό ύποπτης συμπεριφοράς συστήματος, παρέχει πληροφορίες σχετικά με τα συμφραζόμενα, αποκλείει κάθε κακόβουλη δραστηριότητα και παρέχει προτάσεις για την αποκατάσταση των επηρεαζόμενων συστημάτων. (33)

Ο όρος ανίχνευση και απόκριση τελικού σημείου περιγράφει μόνο τις συνολικές δυνατότητες ενός συνόλου εργαλείων. Επομένως, οι λεπτομέρειες και οι δυνατότητες ενός συστήματος **EDR** μπορεί να εμφανίζουν μεγάλες διαφορές, ανάλογα με την εφαρμογή. Μια υλοποίηση **EDR** μπορεί να είναι:

- Ένα ειδικό εργαλείο που έχει κατασκευαστεί για το σκοπό ασφάλειας.
- Ένα μικρό μέρος ενός μεγαλύτερου εργαλείου παρακολούθησης ασφάλειας.
- Μια χαλαρή συλλογή εργαλείων, που χρησιμοποιούνται μαζί για να ασφαλίσουν υπολογιστικά συστήματα.

Καθώς οι επιτιθέμενοι αναπτύσσουν συνεχώς τις μεθόδους και τις δυνατότητές τους ως προς τη μόλυνση των υπολογιστικών συστημάτων,τα παραδοσιακά συστήματα προστασίας ενδέχεται να μην είναι αρκετά. Το **EDR** συνδυάζει δεδομένα και ανάλυση συμπεριφοράς, γεγονός που τα καθιστά αποτελεσματικά έναντι αναδυόμενων απειλών και ενεργών επιθέσεων, όπως:

1. Νέο κακόβουλο λογισμικό που δεν υπάρχει σε κάποια βάση δεδομένων.
2. Αναδυόμενες αλυσίδες εκμετάλλευσης.
3. Ransomware.
4. Προηγμένες επίμονες απειλές (**APT**).

Τα δεδομένα που συλλέγονται από εργαλεία ανίχνευσης και απόκρισης τελικού σημείου μπορούν να παρέχουν εντοπισμό κάποιας επίθεσης, αλλά και αποκατάσταση των υπολογιστικών συστημάτων που έχουν γίνει θύματα από επιθέσεις zero-day, που χρησιμοποιούνται πολύ συχνά σήμερα. Ο κλάδος της ασφάλειας πληροφορικής θεωρεί τα

εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), εργαλεία προηγμένης προστασίας από διάφορες απειλές στα υπολογιστικά συστήματα.

Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) είναι μοναδικό επειδή οι αλγόριθμοι του έχουν την ικανότητα όχι μόνο να ανιχνεύουν και να καταπολεμούν απειλές, αλλά και να εξορθολογίζουν τον τρόπο διαχείρισης των ειδοποιήσεων και των δεδομένων επιθέσεων.

Η χρήση της ανάλυσης συμπεριφοράς για την κατανόηση της δραστηριότητας των χρηστών σε πραγματικό χρόνο, επιτρέπει τον άμεσο εντοπισμό πιθανών απειλών, χωρίς παρεμβολές στα τελικά σημεία. Ενισχύει την εγκληματολογική έρευνα, ενοποιώντας τα διάφορα δεδομένα επιθέσεων σε δεδομένα που μπορούν να αναλυθούν, συνεργαζόμενοι πάντα με το πρόγραμμα προστασίας από ιούς και άλλα εργαλεία για την παροχή ενός ασφαλούς δικτύου.

3.1.1 Ιστορικά δεδομένα

Το 2013, ο Anton Chuvakin της Gartner επινόησε τον όρο "ανίχνευση και απόκριση απειλής τελικού σημείου" για εργαλεία, που επικεντρώνονται κυρίως στον εντοπισμό και τη διερεύνηση ύποπτων δραστηριοτήτων (και ιχνών τέτοιων) άλλων προβλημάτων σε κεντρικούς υπολογιστές και τελικά σημεία". Τώρα, είναι κοινώς γνωστό ως "ανίχνευση και απόκριση τελικούσημείου".

Σύμφωνα με την έκθεση Endpoint Detection and Response - Global Market Outlook (2017-2026), η υιοθέτηση λύσεων **EDR** που βασίζονται σε cloud και εσωτερικής εγκατάστασης, θα αυξάνεται 26% ετησίως και θα αποτιμάται στα 7273,26 εκατομμύρια δολάρια έως το 2026.

Σύμφωνα με την έκθεση Artificial Intelligence (AI) in Cyber Security Market της Zion Market Research, ο ρόλος της μηχανικής μάθησης και της τεχνητής νοημοσύνης θα δημιουργήσει μια αγορά κυβερνοασφάλειας 30,9 δισεκατομμυρίων δολαρίων έως το 2025.

Το 2020, ο πηγαίος κώδικας για ένα ευρέως χρησιμοποιούμενο εργαλείο ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), έγινε διαθέσιμος από την Comodo Cybersecurity ως OpenEDR. Η άδεια Commons Clause που εφάρμοσαν, την καθιστά διαθέσιμη δωρεάν και πιο αξιόπιστη, αλλά ρητά δεν ισχυρίζεται ότι πληροί τις απαιτήσεις εμπορικής επαναχρησιμοποίησης του ανοιχτού κώδικα.

3.2 Δυνατότητες των συστημάτων ανίχνευσης και απόκρισης τελικών σημείων (EDR)

Τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), όπως καταλαβαίνουμε από το όνομα, ασχολούνται κυρίως με τα υπολογιστικά συστήματα που ανήκουν σε κάποιο τελικό σημείο. Τι εννοούμε όμως με τον όρο τελικό σημείο; Αυτά τα συστήματα μπορεί να είναι οποιοδήποτε σύστημα υπολογιστή σε ένα δίκτυο. Τέτοια συστήματα μπορεί να είναι διάφοροι σταθμοί εργασίας τελικού χρήστη ή συστήματα διακομιστών. Τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείο είναι ικανά να προστατεύσουν τα περισσότερα λειτουργικά συστήματα που υπάρχουν στην αγορά (δηλαδή Windows, macOS, Linux, BSD, κ.λπ.), αλλά δυστυχώς, δεν έχουν τη δυνατότητα να κάνουν παρακολούθηση δικτύου. (33)

3.2.1 Λειτουργία των συστημάτων ανίχνευσης και απόκρισης τελικών σημείων (EDR)

Όμως πως λειτουργεί πραγματικά ένα σύστημα ανίχνευσης και απόκρισης τελικού χρήστη; Τα συστήματα ασφαλείας **EDR** έχουν τη δυνατότητα να καταγράφουν όλες τις δραστηριότητες και τα συμβάντα που λαμβάνουν χώρα στα συστήματα τελικών σημείων.Τα συστήματα **EDR**

παρέχουν στα συστήματα που το έχουν εγκατεστημένο την ορατότητα που χρειάζονται με σκοπό να αποκαλύπτονται διάφορα περιστατικά που συμβαίνουν σε πραγματικό χρόνο.Αυτά τα περιστατικά σε διαφορετική περίπτωση, δηλαδή χωρίς την απαιτούμενη ορατότητα, θα παρέμεναν αόρατα και οι χρήστες των διάφορων συστημάτων πολύ πιθανόν να μην καταλάβαιναν ότι υπάρχει κάποιο περιστατικό ασφάλειας. Βλέπουμε ότι μια λύση **EDR** παρέχει συνεχόμενη και ολοκληρωμένη ορατότητα του τι συμβαίνει στα τελικά σημεία κάθε στιγμή, σε πραγματικό χρόνο.

Ένα εργαλείο **EDR** θα πρέπει να προσφέρει προηγμένες δυνατότητες ανίχνευσης, διερεύνησης και απόκρισης απειλών συμπεριλαμβανομένης της αναζήτησης δεδομένων συμβάντων και της διαλογής ειδοποιήσεων διερεύνησης, επικύρωσης ύποπτης δραστηριότητας, κυνηγιού απειλών και εντοπισμού και περιορισμού κακόβουλης δραστηριότητας. Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) είναι ένα αναπόσπαστο μέρος μιας που έχει ως σκοπό την ολοκληρωμένη ασφάλεια πληροφοριών.

Σε αντίθεση με τα λογισμικά προστασίας από ιούς τα λεγόμενα Anti-Virus, τα **EDR** δεν είναι ένα λογισμικό το οποίο θα μας προστατέψει από όλα αυτά τα κακόβουλα λογισμικά που υπάρχουν και μολύνουν τους υπολογιστές. Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου έχουν ορισμένες δυνατότητες για να προστατέψουν τους υπολογιστές από διάφορα κακόβουλα λογισμικά και γενικά από ιούς.Εκτός από αυτό έχουν τη δυνατότητα να χρησιμοποιούν δεδομένα από κάποιο προϊόν προστασίας από ιούς.

3.2.2 Τρόπος ανίχνευσης

Πολλές φορές μπερδεύουμε τα λογισμικά προστασίας από ιούς (Anti-Virus) με τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**). Η διαφορά τους είναι, ότι τα λογισμικά προστασίας από ιούς (Anti-Virus) είναι κυρίως υπεύθυνα για την προστασία υπολογιστών από γνωστά κακόβουλα λογισμικά, που πιθανόν να έχουν μολύνει κάποιο σύστημα, ενώ από την άλλη ένα καλά εκτελεσμένο σύστημα ανίχνευσης και απόκρισης τελικού χρήστη (**EDR**) έχει τη δυνατότητα να εντοπίζει νέες ευπάθειες του συστήματος καθώς αυτές εκτελούνται.

Με αυτό τον τρόπο ένα σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) έχει τη δυνατότητα να εντοπίζει κακόβουλη δραστηριότητα από έναν εισβολέα κατά τη διάρκεια ενός ενεργού περιστατικού. Αυτό επιτρέπει στα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), να ανιχνεύει επιθέσεις κακόβουλου λογισμικού χωρίς να υπάρχουν αρχεία καταγραφής.Αυτή τη δυνατότητα δεν την διαθέτουν τα παραδοσιακά προγράμματα προστασίας από ιούς και έτσι κάποια επίθεση δεν θα μπορούν να τη σταματήσουν. Ωστόσο, πολλά συστήματα **EDR** αποτελούν μέρος των συστημάτων προστασίας από ιούς επόμενης γενιάς.Ο ρόλος ενός συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) εμπίπτει γενικά σε δύο κατηγορίες:

1. Συλλογή και ανάλυση πληροφοριών.

Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) εκτελούνται μέσω διάφορων αισθητήρων, οι οποίοι είναι εγκατεστημένοι στα τελικά σημεία που μπορεί να είναι κάποιος προσωπικός υπολογιστής ή κάποιος διακομιστής. Όλα αυτά τα δεδομένα συγκεντρώνονται σε κάποιο σημείο,με σκοπό να δημιουργήσουν μια πλήρη εικόνα της δραστηριότητας του τελικού σημείου, ανεξάρτητα από τη τοποθεσία που βρίσκεται η συσκευή.Έτσι με αυτό τον τρόπο τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), έχουν την ικανότητα να εντοπίσουν ύποπτη δραστηριότητα στο τελικό σημείο. Χρησιμοποιεί αρκετές πηγές δεδομένων για να συλλέξει από ένα τελικό σημείο.Αυτές οι πηγές

μπορεί να είναι:

- Παρακολούθηση επιδόσεων τελικού σημείου.
- Λεπτομέρειες διάφορων αρχείων που βρίσκονται στο τελικό σημείο.
- Διεργασίες που είναι ενεργές εκείνη τη στιγμή στο τελικό σημείο.
- Δεδομένα διαμόρφωσης ή άλλες πληροφορίες στο τελικό σημείο.

2. Εντοπισμός και εξουδετέρωση απειλών.

Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείο (**EDR**) έχουν τη δυνατότητα να προστατεύουν τα τελικά σημεία από κακόβουλα λογισμικά, κακόβουλα σενάρια ή κλεμμένα διαπιστευτήρια χρήστη. Έχει σχεδιαστεί, για να έχει τη δυνατότητα να παρακολουθεί τους τρόπους, τις τεχνικές και τις διαδικασίες που χρησιμοποιεί ένας εισβολέας και τις τακτικές που ακόλουθει αυτός ο εισβολέας.

Φυσικά τα συστήματα αυτά έχουν και άλλες δυνατότητες. Τα συστήματα αυτά έχουν τη δυνατότητα να καταλαβαίνουν με ποιον τρόπο εισβάλει κάποιος στο τελικό σημείο, αλλά εντοπίζει επίσης τη διαδρομή της δραστηριότητάς τους. Ο χρήστης μπορεί να πάρει πληροφορίες, όπως για παράδειγμα, πώς ο εισβολέας έμαθε για το δίκτυο και πώς έγινε η επίθεση. Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) έχουν την ικανότητα να προστατεύουν το τελικό σημείο από επιθέσεις όπως:

- Κακόβουλο λογισμικό (crimeware, ransomware, κ.λπ.)
- Επιθέσεις χωρίς αρχεία.
- Κακή χρήση νόμιμων εφαρμογών.
- Ύποπτη δραστηριότητα και συμπεριφορά χρήστη

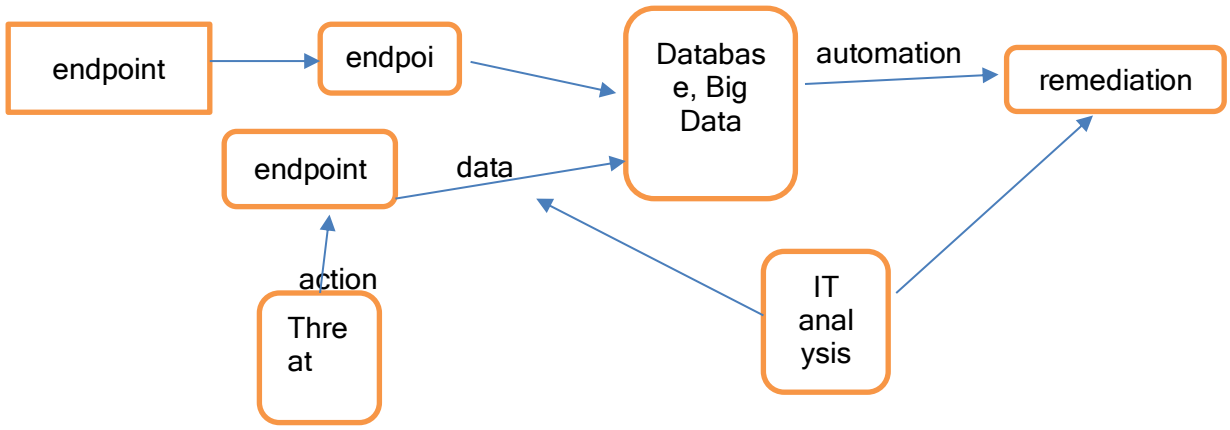
Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) είναι ικανά να οργανώνουν και να αναλύουν τα δεδομένα που συλλέγονται.Ένα τελικό σημείο, δηλαδή κάποια συσκευή πελάτη, έχει τη δυνατότητα να εκτελεί τμήματα του συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) αυτού, αλλά στην πραγματικότητα όλες αυτές οι λειτουργίες εκτελούνται από ένα κεντρικό σύστημα, που μπορεί να είναι μια συσκευή υλικού, ένας εικονικός διακομιστής ή κάποια υπηρεσία cloud. (31) (32) (33)

Τα απλά και παραδοσιακά συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) δεν έχουν αρκετές δυνατότητες ως προς την ασφάλεια των τελικών σημείων. Έχουν τη δυνατότητα μόνο της συλλογής δεδομένων και της εμφάνισης αυτών των δεδομένων.Μπορούν επίσης να συγκεντρώνουν τα δεδομένα και να δείχνουν τάσεις. Οι χειριστές μπορεί να δυσκολεύονται να παρακολουθούν και να λαμβάνουν αποφάσεις βάσει αυτού του τύπου δεδομένων. Τα προηγμένα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) έχουν τη δυνατότητα να περιλαμβάνουν μηχανική μάθηση ή τεχνητή νοημοσύνη, με σκοπό την αυτόματη αναγνώριση και ειδοποίηση για νέες και αναδυόμενες απειλές. Μπορούν επίσης να χρησιμοποιήσουν συγκεντρωτικές πληροφορίες από τον προμηθευτή του προϊόντος, για την καλύτερη επισήμανση απειλών. (34) (35)

Ορισμένα συστήματα επιτρέπουν την αντιστοίχιση της παρατηρούμενης ύποπτης συμπεριφοράς στο πλαίσιο **MITRE ATT&CK** με σκοπό να διευκολυνθεί η ανίχνευση διαφόρων προτύπων.Οι δυνατότητες αντιμετώπισης απειλών του συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), βοηθούν τον χειριστή να καταλάβει τι γίνεται και να λάβει ορισμένα διορθωτικά μέτρα.Μέσω των αποτελεσμάτων των συστημάτων ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), ο χρήστης έχει την ικανότητα να διαγνώσει ζητήματα που υπάρχουν στο

τελικό σημείο και να πραγματοποιήσει εγκληματολογική ανάλυση, η οποία μπορεί να επιτρέψει την παρακολούθηση ζητημάτων και μπορεί να βοηθήσει στην ανάδειξη παρόμοιας δραστηριότητας ή να βοηθήσει σε μια έρευνα.

Οι εγκληματολογικές αναλύσεις βοηθούν στον καθορισμό χρονοδιαγραμμάτων και στον εντοπισμό των επηρεαζόμενων συστημάτων μετά την παραβίαση.Έτσι με αυτό τον τρόπο, μπορεί να είναι σε θέση τα **EDR**, να συλλέξουν διάφορα τεχνουργήματα ή να διερευνήσουν τη ζωντανή μνήμη ενός συστήματος σε ύποπτα τελικά σημεία. Ο συνδυασμός παλιών και νέων δεδομένων κατάστασης μπορεί να συμβάλλει στην παροχή μιας πληρέστερης εικόνας κατά τη διάρκεια ενός περιστατικού. (35) (33)



Σχήμα 3.1 Πως λειτουργεί ένα EDR

Ορισμένα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) έχουν τη δυνατότητα να εκτελούν αυτοματοποιημένες δραστηριότητες αποκατάστασης.Τέτοιες μπορεί να είναι η αποσύνδεση ή διακοπή διακυβευμένων διαδικασιών, ειδοποίηση του χρήστη ή της ομάδας ασφάλειας πληροφοριών. Έχουν επίσης τη δυνατότητα να είναι σε θέση να απομονώνουν ή να απενεργοποιούν ενεργά ύποπτα τελικά σημεία ή λογαριασμούς. Ένα καλό σύστημα απόκρισης συμβάντων θα βοηθήσει επίσης στο συντονισμό των ομάδων κατά τη διάρκεια ενός ενεργού συμβάντος, συμβάλλοντας στη μείωση των επιπτώσεών του.

3.2.3 Προκλήσεις των εργαλείων EDR

Άρα όπως καταλαβαίνουμε, τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), είναι ζωτικής σημασίας για την ασφάλεια των υπολογιστών και ειδικότερα των επιχειρήσεων,όμως τρεις προκλήσεις υπονομεύουν τη χρησιμότητά τους στην πράξη.

Η πρώτη πρόκληση είναι,ότι οι βάσεις δεδομένων Τακτικών, Τεχνικών και Διαδικασιών (TTP), είναι βελτιστοποιημένες για ανάκληση και όχι για ακρίβεια. Δηλαδή, οι επιμελητές των βάσεων δεδομένων Τακτικών, Τεχνικών και Διαδικασιών (TTP), προσπαθούν να περιγράψουν όλες τις διαδικασίες που έχουν οποιαδήποτε πιθανότητα να σχετίζονται με επιθέσεις, ακόμα κι αν οι ίδιες διαδικασίες χρησιμοποιούνται ευρέως για αβλαβείς σκοπούς.

Ένα προφανές παράδειγμα αυτού του προβλήματος μπορεί να βρεθεί στην Τεχνική "Διαγραφή αρχείου" στο **ATT&CK** της **MITRE**, ενώ η διαγραφή αρχείου μπορεί να υποδηλώνει την παρουσία τακτικών αποφυγής επιθέσεων Advanced Persistent Threats (APT),που είναι επίσης απαραίτητο μέρος των δραστηριοτήτων των μη κακόβουλων χρηστών. Με αυτόν τον τρόπο, τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) είναι επιρρεπή σε μεγάλους όγκους ψευδών συναγερμών. Στην πραγματικότητα, τα εργαλεία ανίχνευσης και

απόκρισης τελικού σημείου (**EDR**), είναι ένας από τους βασικούς δράστες του προβλήματος «κόπωσης συναγερμού απειλών», που μαστίζει αυτή τη στιγμή τον κλάδο.

Μια πρόσφατη μελέτη διαπίστωσε, ότι η μεγαλύτερη πρόκληση για το 35% των ομάδων ασφαλείας είναι να συμβαδίζουν, με τον τεράστιο όγκο των ειδοποιήσεων. Κατά συνέπεια, οι πραγματικές επιθέσεις που εντοπίζονται από τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), κινδυνεύουν να χαθούν στο μεγάλο όγκο των ψευδών ειδοποιήσεων.

Η δεύτερη πρόκληση προέρχεται, από την αμφίβολη φύση των ειδοποιήσεων απειλών που δημιουργούνται από τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**). Μετά τη λήψη μιας ειδοποίησης, η πρώτη δουλειά ενός αναλυτή στον κυβερνοχώρο είναι να προσδιορίσει την ακρίβεια της ειδοποίησης. Οι αναλυτές στον κυβερνοχώρο, εξετάζουν το πλαίσιο γύρω από την προειδοποίηση που ενεργοποιήθηκε, μπαίνοντας στα αρχεία καταγραφής του συστήματος,όπου το εργαλείο ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) αποθηκεύει την ειδοποίηση.

Τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), συλλέγουν μια ποικιλία χρήσιμων πληροφοριών με βάση τα συμβάντα, όπως οι διεργασίες που εκτελούνται στον υπολογιστή και οι συνδέσεις δικτύου. Το δύσκολο έργο του αναλυτή του κυβερνοχώρου είναι να συνενώσει με μη αυτόματο τρόπο την αλυσίδα των συμβάντων του συστήματος. Εάν η ειδοποίηση κριθεί πραγματικά ύποπτη, ο αναλυτής στον κυβερνοχώρο επιχειρεί , να ανακτήσει και να συσχετίσει διάφορα στάδια της επίθεσης μέσω περαιτέρω εξέτασης τεράστιων αρχείων καταγραφής συστήματος.

Τα προϊόντα Security Indicator & Event Management (SIEM) είναι συχνά η διεπαφή μέσω της οποίας, εκτελείται αυτή η εργασία (π.χ. Splunk), επιτρέποντας στους αναλυτές να γράφουν μεγάλα ad-hoc ερωτήματα, με σκοπό να ενταχθούν σε στάδια επίθεσης, υπό την προϋπόθεση, ότι έχουν την εμπειρία και την εξειδίκευση να το πράξουν.

Η μακροπρόθεσμη διατήρηση αρχείων καταγραφής είναι η τρίτη πρόκληση για τα υπάρχοντα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**). Εξακολουθεί να είναι συνηθισμένο για τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), να διαγράφουν αρχεία καταγραφής συστήματος αμέσως μετά τη σύλληψή τους. Τα αρχεία καταγραφής αποθηκεύονται συνήθως σε μια μικρή ουρά (First In First Out ή FIFO), που αποθηκεύει προσωρινά δεδομένα ελέγχου για λίγες μόνο ημέρες, έτσι ώστε τα συμβάντα του συστήματος να μην είναι συνήθως διαθέσιμα κατά τη διερεύνηση μιας επίθεσης μεγάλης διάρκειας.

Ακόμη χειρότερα, εάν ένας οργανισμός δεν στελεχώσει μια ομάδα,που να καλύπτει και να ελέγχει την ασφάλεια και τα δεδομένα ελέγχου για ειδοποιήσεις που πυροδοτούνται για παράδειγμα το Σαββατοκύριακο, είναι πιθανόν τα συμβάντα του συστήματος να καταστραφούν μέχρι τη Δευτέρα.

Αυτό δείχνει, ότι παρά τις προόδους στην αποτελεσματικότητα της ανάλυσης αιτιών, η μακροπρόθεσμη διατήρηση του αρχείου καταγραφής του συστήματος δεν κλιμακώνεται στις μεγάλες επιχειρήσεις. Αυτό σημαίνει ότι τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), όχι μόνο δεν μπορούν να αποκομίσουν τα οφέλη της αιτιολογικής ανάλυσης κατά τη διερεύνηση απειλών, αλλά ότι τα τρέχοντα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), δεν διαθέτουν το απαραίτητο πλαίσιο για την κατανόηση των αλληλεξαρτήσεων μεταξύ των σχετικών ειδοποιήσεων των απειλών.

3.2.3.1 Προσπάθεια για διευκόλυνση των προκλήσεων στα εργαλεία EDR

Για να διευκολυνθεί η επικύρωση και η διερεύνηση των προειδοποιήσεων που προέρχονται από τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), πρέπει να διερευνήσουμε την προέλευση αυτών των δεδομένων. Η ανάλυση της προέλευσης των δεδομένων μπορεί να εφαρμοστεί σε αρχεία καταγραφής συστήματος για την ανάλυση συμβάντων κεντρικού υπολογιστή σε γραφήματα προέλευσης, που περιγράφουν το σύνολο της εκτέλεσης του συστήματος και διευκολύνουν την αιτιολογική ανάλυση των δραστηριοτήτων τουσυστήματος.

Τα τελευταία χρόνια, έχουν γίνει σημαντικές εξελίξεις που βελτιώνουν την πιστότητα και την αποτελεσματικότητα της αιτιολογικής ανάλυσης.Τα πρόσφατα αποτελέσματα δείχνουν ότι η αιτιολογική ανάλυση, μπορεί ακόμη και να αξιοποιηθεί για τη βελτίωση της διαλογής συναγερμών, με σκοπό την ανίχνευση εισβολών και για την εξαγωγή συσχετίσεων συναγερμών. Ακόμα καλύτερα, οι περισσότερες μηχανές αιτιολογικής ανάλυσης βασίζονται σε πλαίσια ελέγχου εμπορευμάτων (π.χ. Windows ETW), τα οποία αναλύουν την ίδια ροή πληροφοριών, που χρησιμοποιείται ήδη από τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**). (36)

Με βάση την προέλευση των δεδομένων, εισάγουμε μια νέα έννοια, με το όνομα Tactical Provenance, η οποία μπορεί να αιτιολογήσει τις αιτιώδεις εξαρτήσεις μεταξύ των ειδοποιήσεων απειλής, που δημιουργούνται από τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**). Αυτές οι αιτιακές εξαρτήσεις κωδικοποιούνται στη συνέχεια, σε ένα γράφημα τακτικής προέλευσης (**TPG**). Το βασικό πλεονέκτημα του γραφήματος τακτικής προέλευσης (**TPG**) είναι, ότι ένα γράφημα τακτικής προέλευσης (**TPG**), είναι πιο συνοπτικό από ένα κλασικό γράφημα προέλευσης ολόκληρου του συστήματος, επειδή αφαιρεί τα γεγονότα του συστήματος χαμηλού επιπέδου για τους αναλυτές του κυβερνοχώρου. Επιπλέον, τα γραφήματα τακτικής προέλευσης (**TPG**) παρέχουν οπτικοποιήσεις υψηλότερου επιπέδου επιθέσεων APT πολλαπλών σταδίων στους αναλυτές, οι οποίες βοηθούν στην επιτάχυνση της διαδικασίας έρευνας.

Για να αξιοποιήσουμε καλύτερα τον περιορισμένο διαθέσιμο χώρο στους κεντρικούς υπολογιστές για μακροπρόθεσμη αποθήκευση αρχείων καταγραφής, παρουσιάζουμε μια νέα τεχνική μείωσης αρχείων καταγραφής ,που αντί να αποθηκεύει όλα τα συμβάντα του συστήματος που υπάρχουν στα αρχεία καταγραφής, διατηρεί ένα ελάχιστα επαρκές σκελετο γράφημα. Αυτό το σκελετο γράφημα διατηρεί ακριβώς αρκετό πλαίσιο (συμβάντα συστήματος), για να εντοπίζει όχι μόνο αιτιώδεις συνδέσμους μεταξύ των υπαρχουσών ειδοποιήσεων,αλλά και τυχόν ειδοποιήσεις που ενδέχεται να ενεργοποιηθούν στο μέλλον. Παρόλο που τα γραφήματα σκελετού μειώνουν την πιστότητα των αρχείων καταγραφής συστήματος, εξακολουθούν να διατηρούν όλες τις απαραίτητες πληροφορίες για τη δημιουργία TPG με σκοπό την εκχώρηση βαθμολογίας απειλών, την αξιολόγηση κινδύνου και την οπτικοποίηση επίθεσης υψηλού επιπέδου.

3.3 Χρήση τεχνητής νοημοσύνης στα συστήματα EDR

Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου με τη βοήθεια της τεχνητής νοημοσύνης, έχει τη δυνατότητα να αποκαλύπτει αυτόματα τους Stealth Attackers, δηλαδή τους εισβολείς οι οποίοι δεν αφήνουν κάποιο ίχνος.

Η τεχνολογία των συστημάτων ανίχνευσης και απόκρισης τελικού σημείου (**EDR**),έχει ολοκληρωμένη ορατότητα σε όλα τα τελικά σημεία που είναι εγκατεστημένο και έχει τη δυνατότητα να εφαρμόζει αναλυτικά στοιχεία συμπεριφοράς. Αυτά τα στοιχεία αναλύουν δισεκατομμύρια συμβάντα σε πραγματικό χρόνο με σκοπό να ανιχνεύουν αυτόματα ίχνη ύποπτης συμπεριφοράς.Η κατανόηση μεμονωμένων συμβάντων ως μέρος μιας ευρύτερης ακολουθίας επιτρέπει στο εργαλείο **EDR** να εφαρμόζει λογική ασφαλείας που προέρχεται από κάποιον κεντρικό υπολογιστή.

Εάν μια ακολουθία συμβάντων ταιριάζει με ένα γνωστό **IOA**, το εργαλείο ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), θα αναγνωρίσει αυτή τη δραστηριότητα ως κακόβουλη και θα στείλει αυτόματα μια ειδοποίηση ανίχνευσης. Έχει την ικανότητα να ενσωματώνεται με τη νοημοσύνη των επιθέσεων και γενικά των απειλών ενός τελικού σημείου.

Η ενσωμάτωση με τη νοημοσύνη απειλών στον κυβερνοχώρο παρέχει ταχύτερη ανίχνευση των δραστηριοτήτων και των τακτικών, τεχνικών και διαδικασιών (TTP) που θεωρούνται ως κακόβουλες. Αυτό παρέχει πληροφορίες στους χρήστες που αφορούν την απόδοση των τελικών σημείων. Έτσι με αυτόν τον τρόπο,τα συστήματα **EDR** παρέχουν διάφορες λεπτομέρειες για τον αντίπαλο και οποιαδήποτε άλλη πληροφορία είναι αναγκαία για την κατανόηση της επίθεσης. (37) (35)

3.3.1 Η τεχνητή νοημοσύνη επιταχύνει τις έρευνες και την αποτελεσματική αποκατάσταση

Η ανίχνευση και η απόκριση τελικού σημείου (**EDR**) με τη βοήθεια τεχνητής νοημοσύνηςέχει τη δυνατότητα να επιταχύνει σε μεγάλο βαθμό την έρευνα και ειδικά την αποκατάσταση, επειδή οι πληροφορίες που συλλέγονται από τα τελικά σημεία, αποθηκεύονται σε ένα Cloud.

Το μοντέλο παρακολουθεί όλες τις σχέσεις και τις επαφές μεταξύ κάθε συμβάντος τελικού σημείου χρησιμοποιώντας μια τεράστια, ισχυρή βάση δεδομένων γραφημάτων, η οποία παρέχει διάφορες λεπτομέρειες και ένα πλαίσιο σε μικρό χρονικό διάστημα και σε κλίμακα, τόσο για ιστορικά δεδομένα, όσο και για δεδομένα σε πραγματικό χρόνο. Αυτό επιτρέπει στις ομάδες ασφαλείας να διερευνούν γρήγορα τα περιστατικά.

Αυτή η ταχύτητα και το επίπεδο ορατότητας, σε συνδυασμό με την ολοκληρωμένη, ενσωματωμένη ευφυΐα παρέχει τις πληροφορίες που απαιτούνται για την πλήρη κατανόηση των δεδομένων. Αυτό επιτρέπει στις ομάδες ασφαλείας να παρακολουθούν αποτελεσματικά ακόμη και τις πιο εξελιγμένες επιθέσεις και να αποκαλύπτουν έγκαιρα περιστατικά, καθώς και να τα αξιολογούν, να τα επικυρώνουν και να τα ιεραρχούν, οδηγώντας σε ταχύτερη και ακριβέστερη αποκατάσταση.

Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) με τη βοήθεια της τεχνητής νοημοσύνης έχει την ικανότητα να απομονώσει το τελικό σημείο. Επιτρέπει στους οργανισμούς να αναλάβουν γρήγορη και στιγμιαία δράση, απομονώνοντας δυνητικά παραβιασμένους κεντρικούς υπολογιστές από όλη τη δραστηριότητα του δικτύου.

Όταν ένα τελικό σημείο βρίσκεται υπό περιορισμό, εξακολουθεί να μπορεί να στέλνει και να λαμβάνει πληροφορίες από το Cloud, αλλά θα παραμείνει περιορισμένο ακόμη και αν διακοπεί η σύνδεση με το Cloud και θα παραμείνει σε αυτήν την κατάσταση περιορισμού κατά τις επανεκκινήσεις.

Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) με τη βοήθεια της τεχνητής νοημοσύνης περιλαμβάνει την απόκριση σε πραγματικό χρόνο, η οποία παρέχει βελτιωμένη ορατότητα που επιτρέπει στις ομάδες ασφαλείας να κατανοούν αμέσως τις απειλές που αντιμετωπίζουν και να τις αποκαθιστούν άμεσα, ενώ δημιουργεί μηδενικό αντίκτυπο στην απόδοση. (37) (35)

3.3.2 Managed Threat Hunting for Proactive Defense

Χρησιμοποιώντας το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), οι κυνηγοί απειλών εργάζονται προληπτικά με σκοπό να κυνηγήσουν, να διερευνήσουν και να εντοπίσουν τη δραστηριότητα απειλών στο περιβάλλον τους. Όταν βρίσκουν μια απειλή στο σύστημα,

εργάζονται μαζί με την ομάδα με σκοπό να αξιολογήσουν, να διερευνήσουν και να αποκαταστήσουν το περιστατικό, προτού προλάβει να γίνει μια πλήρης παραβίαση.

Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) λειτουργεί σαν ένα DVR στο τελικό σημείο, καταγράφοντας τη σχετική δραστηριότητα για τη σύλληψη περιστατικών για τα οποία δεν πάρθηκαν μέτρα, με σκοπό να γίνει πρόληψη. Οι πελάτες έχουν πλήρη ορατότητα σε όλα όσα συμβαίνουν στα τελικά σημεία τους από την άποψη της ασφάλειας, καθώς το **EDR** είναι ικανό να παρακολουθεί εκατοντάδες διαφορετικά συμβάντα που σχετίζονται με την ασφάλεια.

Τέτοια μπορεί να αναφέρονται σε δημιουργία ύποπτων διεργασιών στο τελικό σημείο, φόρτωση προγραμμάτων οδήγησης για το υλικό του τελικού σημείου, διάφορες τροποποιήσεις registry, πρόσβαση στο σκληρό δίσκο, πρόσβαση στη μνήμη ή κάποιες συνδέσεις δικτύου.Αυτό παρέχει στις ομάδες ασφαλείας τις χρήσιμες πληροφορίες που χρειάζονται, όπως:

- Τοπικές και εξωτερικές διευθύνσεις στις οποίες είναι συνδεδεμένος ο κεντρικός υπολογιστής.
- ‘Ολους τους λογαριασμούς χρηστών που έχουν συνδεθεί στο σύστημα, τόσο τοπικά όσο και απομακρυσμένα.
- Μια περίληψη των αλλαγών στα κλειδιά ASP, τα εκτελέσιμα αρχεία και τη χρήση του διαχειριστικού εργαλείου.
- Εκτελέσεις διαδικασιών.
- Συνοπτική και λεπτομερής δραστηριότητα δικτύου σε επίπεδο διεργασίας, συμπεριλαμβανομένων των αιτημάτων DNS, των συνδέσεων και των ανοιχτών θυρών.
- Δημιουργία αρχείου αρχειοθέτησης, συμπεριλαμβανομένων των συμπιεσμένων αρχείων RAR και ZIPS.
- Χρήση αφαιρούμενων μέσων.

Αυτή η πλήρης επίβλεψη της δραστηριότητας τελικού σημείου που μας προσφέρει το σύστημα **EDR** και σχετίζεται με την ασφάλεια, επιτρέπει στις ομάδες ασφαλείας να παρακολουθούν τις δραστηριότητες ενός εισβολέα σε πραγματικό χρόνο. Έτσι μπορούμε να καταλάβουμε ποιες εντολές εκτελεί ένας εισβολέας και ποιες τεχνικές εισχώρησης χρησιμοποιούν, ακόμη και όταν προσπαθούν να παραβιάσουν ή να μετακινηθούν σε ένα περιβάλλον.

3.3.3 Επιπλέον πλεονεκτήματα των συστημάτων EDR

Η καινοτόμος και αποτελεσματική φύση του συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) από μόνη της αποδεικνύει την αξία του, αλλά υπάρχουν πρόσθετα πλεονεκτήματα που είναι ακόμη πιο σημαντικά από την τεχνολογία. Συγκεκριμένα το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**):

- Είναι οικονομικά πιο αποδοτικό. Αντί να υπάρχει μια εσωτερική ομάδα ασφαλείας 24 ώρες για 7 ημέρες ή να αφήσουμε τα τελικά σημεία ανοιχτά σε επιθέσεις μεγάλης κλίμακας, το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) επιτρέπει να επενδύσουμε στην ασφάλεια της εταιρείας και των δεδομένων με τρόπο ρεαλιστικό για μια ομάδα μικρού έως μεσαίου μεγέθους.
- Κερδίζει αρκετό χρόνο. Επειδή υπάρχουν λιγότερες ειδοποιήσεις για ανάλυση με το **MalOpsTM** και λιγότερα ψευδώς θετικά, τα συστήματα **EDR** επιτρέπουν στους αναλυτές να αφιερώνουν περισσότερο χρόνο στη διερεύνηση νόμιμων απειλών.
- Έχει αυξημένη αποτελεσματικότητα της ομάδας. Αντί να αναλύει τις ειδοποιήσεις και να τις συγκρίνει με άλλα σημεία δεδομένων, τα συστήματα **EDR** συσχετίζουν τα σημεία

δεδομένων σε μια ενιαία ιστορία, εξοικονομώντας στους αναλυτές τεράστιες δαπάνες και χρόνο. Αυτό επιτρέπει στην ομάδα να επεξεργάζεται πιο αποτελεσματικά δεδομένα και να προστατεύει την εταιρεία. (34) (33)

3.4 Διάφορα εμπορικά εργαλεία EDR

Αρκετοί δημοφιλείς προμηθευτές προσφέρουν δυνατότητες εργαλείων **EDR**, είτε ως αυτόνομα προϊόντα είτε ως μέρος ενός πακέτου υπηρεσιών. Ένα σύστημα που είναι ικανό να συλλέγει πληροφορίες από πολλές πηγές, όπως τελικά σημεία, τείχη προστασίας, σαρώσεις δικτύου και αρχεία καταγραφής Διαδικτύου, ονομάζεται διαχείριση πληροφοριών ασφαλείας καισυμβάντων (**SIEM**). Ωστόσο, οι προμηθευτές ασφαλείας μπορούν να προσφέρουν ένα σύστημαανίχνευσης και απόκρισης τελικού σημείου (**EDR**) ως μέρος ενός πακέτου **SIEM**. Έτσι μπορεί να γίνει χρήση του συστήματος **EDR** από ένα κέντρο επιχειρήσεων ασφαλείας (**SOC**) για τη διερεύνηση και την απόκριση για τυχόν απειλές.

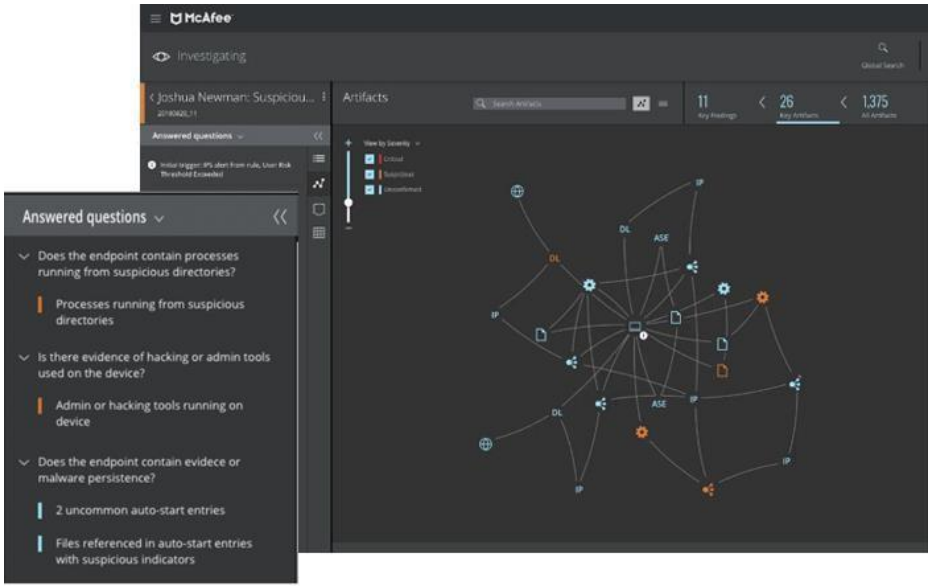
Πολλά συστήματα ανίχνευσης και απόκρισης τελικού σημείου που υπάρχουν στο εμπόριο είναι:

- Το McAfee MVision **EDR** είναι ένα εργαλείο ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) βασισμένο στο Cloud με δυνατότητες διερεύνησης καθοδηγούμενων από τεχνητή νοημοσύνη.

Το **MVISION EDR** μειώνει τον μέσο χρόνο για τον εντοπισμό και την απόκριση σε απειλές, επιτρέποντας σε όλους τους αναλυτές να κατανοούν τις ειδοποιήσεις, να ερευνούν πλήρως τα συμβάντα και να ανταποκρίνονται πιο γρήγορα.

Τα προηγμένα αναλυτικά στοιχεία διευρύνουν την ανίχνευση και δίνουν νόημα στις ειδοποιήσεις. Οι έρευνες και ο αυτοματισμός που καθοδηγούνται από την τεχνητή νοημοσύνη (AI) εξοπλίζουν ακόμη και αρχάριους αναλυτές, για το πώς να αναλύουν σε υψηλότερο επίπεδο και να ελευθερώνουν τους ανώτερους αναλυτές, να εφαρμόσουν τις δεξιότητές τους στο κυνήγι και να επιταχύνουν τον χρόνο απόκρισης.

Σχήμα 3.2 Front-end MVISION (55)



Σχήμα 3.3 Γράφημα επιθέσεων (55)

- Το CrowdStrike Falcon Insight προσφέρει υψηλή ορατότητα και ανάλυση δεδομένων τελικού σημείου, με συλλογή πληροφοριών με σκοπό να βοηθήσει στον εντοπισμό και τον μετριασμό των επιθέσεων.

Είναι από τα πιο αποτελεσματικά συστήματα κυβερνοασφάλειας διότι έχει:

- Επιφανειακά αξιόπιστες πληροφορίες συνδυάζοντας δεδομένα και προηγουμένως αποθηκευμένα σε μια ενιαία πηγή ασφαλείας και ένα κεντρικό αποθετήριο για τηλεμετρία μεταξύ τομέων
- Συλλογή, συγκέντρωση και ομαλοποίηση δεδομένων απειλών με ευκολία:

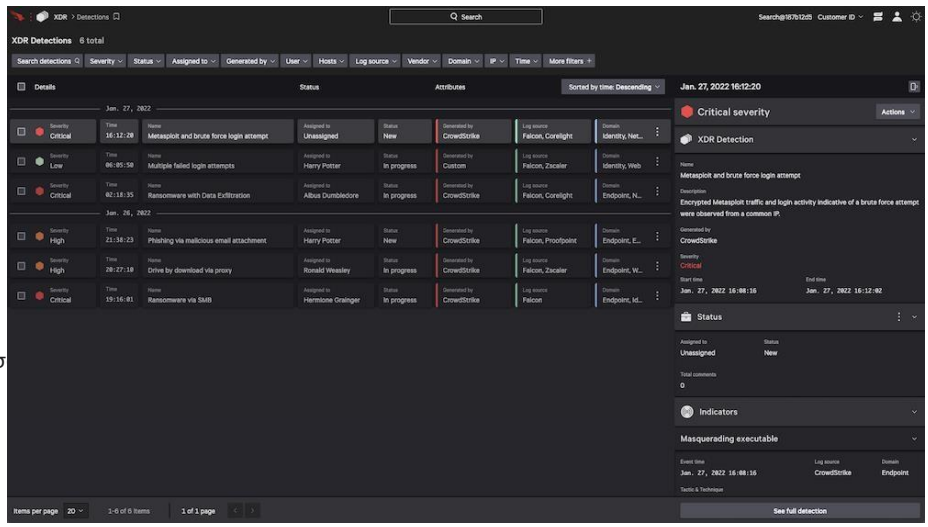
Οι ενσωματώσεις XDR με σκοπό και ένα κοινό σχήμα δεδομένων συνδυάζονται για τη διοχέτευση δεδομένων ασφάλειας μεταξύ τομέων σε μαζική κλίμακα, διασφαλίζοντας ότι οι ομάδες ασφαλείας έχουν την ορατότητα που χρειάζονται στο περιβάλλον τους.

- Βαθιά, εγγενής τηλεμετρία:

Τομείς πλατφόρμας CrowdStrike Falcon®: **EDR**, cloud, ταυτότητα, κινητά και πολλά άλλα.

- Ανάλυση από προμηθευτές:

Ενσωματώσεις τρίτων σε βασικούς τομείς ασφαλείας από συνεργάτες της CrowdXDR Alliance και κορυφαίους προμηθευτές του κλάδου.



Σχήμα 3.4 Crowdstrike Falcon XDR Front-end (56)

- Επιφανειακές επιθέσεις που χάνονται από προσεγγίσεις αποσιωπημένες:

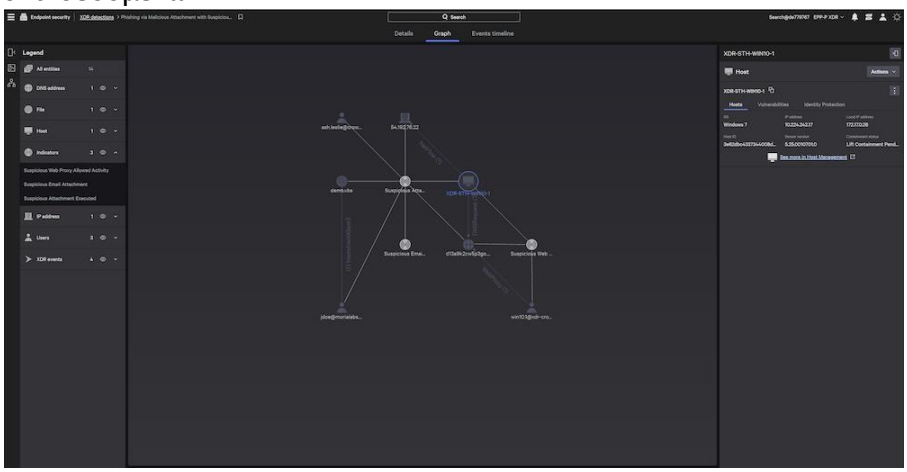
Εντοπισμός κρυφών επιθέσεων μεταξύ τομέων,όταν η τεχνητή νοημοσύνη απειλών στον κόσμο και τα προηγμένα αναλυτικά στοιχεία λειτουργούν στο ποικίλο περιβάλλον. Οι δυνατότητες εντοπισμού και προσαρμοσμένης ανίχνευσης δίνουν τη δυνατότητα και την ευελιξία που χρειάζεται ένας χρήστης.

- Διερεύνηση των απειλών μεταξύ τομέων όπως ποτέ πριν:

Οι ανιχνεύσεις που δημιουργούνται από το CrowdStrike όσο και οι προσαρμοσμένες ανιχνεύσεις από έναν εξερευνητή γραφημάτων, προβάλλουν ολόκληρη τη διαδρομή επίθεσης μεταξύ τομέων και το πλούσιο πλαίσιο, για γρήγορη κατανόηση και σίγουρη απόκριση.

- Βελτίωση της διαλογής και της διερεύνησης:

Οι ειδοποιήσεις προτεραιότητας, το πλούσιο πλαίσιο και οι λεπτομερείς πληροφορίες ανίχνευσης που έχουν αντιστοιχιστεί στο πλαίσιο **MITRE ATT&CK** βοηθούν τους αναλυτές να κατανοούν γρήγορα και να ενεργούν έναντι των απειλών. Η διαισθητική κονσόλα Falcon επιτρέπει τη γρήγορη προσαρμογή των προβολών, το φιλτράρισμα και την εύκολη περιστροφή για τα διάφορα σύνολα δεδομένων.



Σχήμα 3.5 Crowdstrike Falcon XDR Γράφημα επιθέσεων (56)

- Το **VMware Carbon Black Cloud Endpoint** είναι ένα προϊόν προστασίας από ιούς επόμενης γενιάς στηριζόμενο στο Cloud με αναλύσεις συμπεριφοράς Cloud **EDR**.
- Το **Broadcom EDR** μπορεί να χρησιμοποιηθεί με τη σουίτα Symantec Endpoint Protection (**SEP**) ή ως διαλυτό μέσο.
- Το εργαλείο FireEye Endpoint Security προσφέρει δυνατότητες **EDR** και μπορεί να εκτελέσει αυτοματοποιημένη απόκριση και διαχείριση χρησιμοποιώντας ανάλυση συμπεριφοράς και δείκτες συμβιβασμού.
- Το Microsoft Defender ATP μπορεί να εντοπίσει, να αναγνωρίσει και να διώξει τις προχωρημένες επιθέσεις από το τελικό σημείο.

Με λίγα λόγια, το Microsoft Defender ATP εντοπίζει αυτόματα και αποκαθιστά προηγμένες επιθέσεις στα τελικά σημεία. Διερευνά το εύρος και τον πιθανό αντίκτυπο κάθε απειλής, παρέχοντας αναφορές για τις διάφορες απειλές στα μηχανήματα του οργανισμού, επιτρέποντάς το μετριασμό και τη γρήγορη και εύκολη αφαίρεση των απειλών χρησιμοποιώντας προηγμένα εργαλεία και αυτοματισμό.

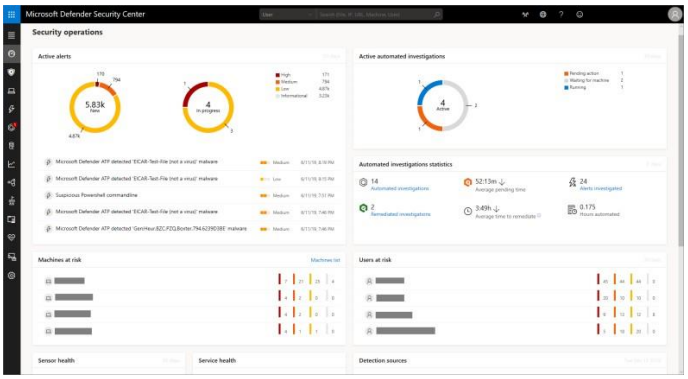
Το Microsoft Defender ATP δεν έχει agent και δεν απαιτεί ανάπτυξη ή υποδομή καθώς φιλοξενείται στο cloud. Η τεχνολογία του χρησιμοποιεί αισθητήρες συμπεριφοράς τελικού σημείου που βρίσκονται στο λειτουργικό σύστημα κάθε συσκευής.

Αυτοί οι αισθητήρες στα Windows συλλέγουν συνεχώς δεδομένα και τα τροφοδοτούν στην παρουσία cloud του Microsoft Defender του οργανισμού. Στη συνέχεια, το Microsoft Defender ATP αναλύει τη συμπεριφορά του κώδικα που εκτελείται στους υπολογιστές του οργανισμού και προσδιορίζει, εάν κάτι φαίνεται ότι μπορεί να αποτελεί απειλή.Καθώς οι οργανισμοί αντιμετωπίζουν απειλές, αυτές οι πληροφορίες ανατροφοδοτούνται στο cloud της Microsoft, το οποίο μαθαίνει ποια από αυτά τα πρότυπα συμπεριφοράς υποδηλώνουν απειλή.

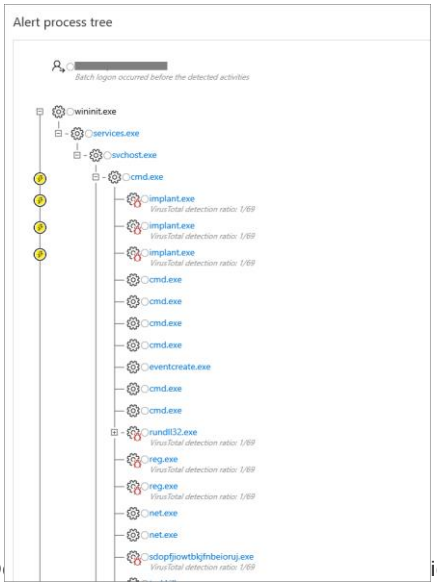
Όταν έχει εντοπιστεί μια απειλή στην παρουσία του Microsoft Defender ATP του οργανισμού, θα σαρώσει τις συσκευές του οργανισμού για την απειλή και θα ενημερώσει:

- Πως ξεκίνησε η απειλή.
- Ποια είναι η απειλή.
- Τι είναι πιθανό να κάνει η απειλή στον υπολογιστή.

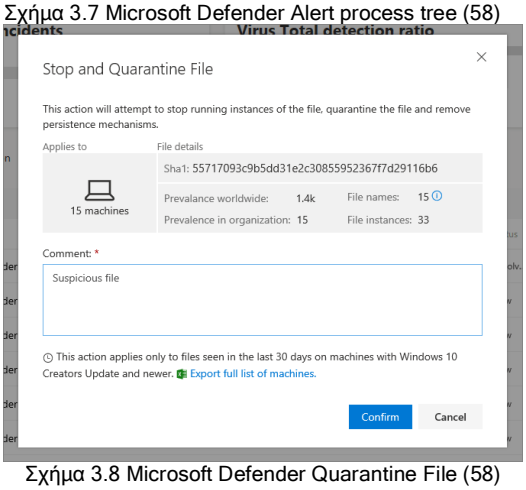
Στη συνέχεια, ο χρήστης έχει τη δυνατότητα να προβεί σε διάφορες ενέργειες για την αποκατάσταση της απειλής και την κατάργηση του προβλήματος, καθώς και την αυτοματοποιημένη αποκατάσταση, που εκτελείται από το Microsoft Defender ATP σε ορισμένες περιπτώσεις.



Σχήμα 3.6 Microsoft Defender Front-end



Σχήμα 3.7 Microsoft Defender Alert process tree (58)



Σχήμα 3.8 Microsoft Defender Quarantine File (58)

Εκτός από τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), που υπάρχουν στο εμπόριο, υπάρχουν και πολλά εργαλεία ανοιχτού κώδικα.Ενδέχεται όμως, να απαιτούν εκτεταμένες ρυθμίσεις παραμέτρων στο τελικό σημείο ή επιπλέον συστήματα για να είναι πλήρως εξοπλισμένα. Αυτά τα εργαλεία περιλαμβάνουν:

- **OSSEC**
- **Wazuh**
- **TheHive Cortex**
- **OpenEDR**
- **Bluespawn**

Τα εργαλεία ανίχνευσης και απόκρισης τελικών σημείων (**EDR**) επιτρέπουν στους οργανισμούς να παρακολουθούν συνεχώς τα τελικά σημεία και τους διακομιστές με σκοπό να εντοπίζουν δυνητικά κακόβουλες συμπεριφορές. Τα αποτελεσματικά εργαλεία **EDR** μπορούν να ανιχνεύσουν και να ανταποκριθούν σε αυτά τα συμβάντα για να μετριάσουν τη ζημιά στο τελικό σημείο και στο ευρύτερο δίκτυο.

3.5 Διαφορές EDR με Anti-Virus και SIEM

Μια κοινή ερώτηση που κάνουν οι χρήστες είναι σχετικά με τη διαφορά μεταξύ του **EDR** και ενός παραδοσιακού **Anti-Virus** (**AV**) ή επόμενης γενιάς Anti-Virus (**NGAV**). Στο μυαλό τους,δεν χρειάζονται και τις δύο τεχνολογίες. Αλλά αυτό δεν ισχύει.

Η πραγματικότητα είναι ότι και οι δύο τεχνολογίες εξυπηρετούν διαφορετικούς σκοπούς για την προστασία ενός δικτύου υπολογιστών. Τα **Anti-Virus** (**AV**) και τα Next Generation Anti-Virus (**NGAV**) επικεντρώνονται στην πρόληψη, αλλά έχουν μηδενική ορατότητα για το τι συνέβη κατά τη διάρκεια μιας επίθεσης. Έχουν σχεδιαστεί για να συλλαμβάνουν ένα κακόβουλο λογισμικό προτού εισέλθει σε ένα δίκτυο υπολογιστών. Ακόμα και όταν συλλαμβάνουν κάποιο κακόβουλο λογισμικό, δεν έχουν σχεδιαστεί για να δείχνουν από πού προήλθε ακριβώς αυτό το κακόβουλο λογισμικό και τον τρόπο με τον οποίο εξαπλώθηκε στο σύστημα.

Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), αναφέρει ακριβώς όλη την ιστορία του κακόβουλου λογισμικού και βοηθά το χρήστη να παρακολουθεί τον τρόπο με τον οποίο το εκτελέσιμο απέκτησε πρόσβαση στο σύστημα και επιχείρησε να τρέξει. Τα συστήματα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), όχι μόνο παρέχουν ορατότητα όταν κάποια επίθεση διακόπτεται από ένα Anti-Virus, αλλά όταν ο έλεγχος αποτυγχάνει με ένα καλό **NGAV**, πιθανότατα αντιμετωπίζεται μια σοβαρή επίθεση, όπως κακόβουλο λογισμικό

χωρίς αρχεία, εκμεταλλεύσεις zero-day ή προηγμένες επίμονες απειλές (APT).

Αυτοί οι τύποι επιθέσεων δεν αφήνουν υπογραφές, γεγονός που καθιστά πιο δύσκολο να αποφευχθούν και σχεδόν αδύνατο να εντοπιστούν χωρίς κάποια υπηρεσία, όπως το **EDR**. Αυτό θα προειδοποιήσει για απόπειρες επιθέσεων και θα παρέχει πληροφορίες,όταν οι εισβολείς έχουν ξεπεράσει όλες τις άμυνές και βρίσκονται αυτήν τη στιγμή στο δίκτυό υπολογιστών.

Μια άλλη κοινή ερώτηση είναι η διαφορά μεταξύ του συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) και της Διαχείρισης πληροφοριών και συμβάντων ασφαλείας (**SIEM**).

Το **SIEM** είναι μια τεχνολογία που συλλέγει αρχεία καταγραφής από τείχη προστασίας, διακομιστές και συσκευές δικτύου. Συγκεντρώνει όλα τα αρχεία καταγραφής του δικτύου με σκοπό να βοηθήσει στην παρακολούθηση της συμπεριφοράς, αναγνωρίζει απειλές και τις διερευνεί. Ωστόσο, πρέπει να οριστούν κανόνες και ερωτήματα με σκοπό να ενημερώνουν τη **SIEM** τι να αναζητήσει και ποιες συμπεριφορές να παρακολουθεί.

Το **SIEM** είναι μια εξαιρετική υπηρεσία για μια ολοκληρωμένη εικόνα των δραστηριοτήτων που λαμβάνουν χώρα στο δίκτυό. Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), ενοποιεί και αναλύει τα δεδομένα τελικού σημείου, εξοπλίζοντας τους αναλυτές, αντί να τους απαιτεί να αναλύσουν εκατοντάδες χιλιάδες αρχεία καταγραφής ή συμβάντα.

Τελικά, οι δύο τεχνολογίες εξυπηρετούν διαφορετικούς σκοπούς και μπορούν να αλληλοσυμπληρώνονται σε ένα ασφαλές περιβάλλον δικτύου, αλλά ο κύριος σκοπός του συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) είναι ο εξορθολογισμός, ο αποτελεσματικός εντοπισμός και η απόκριση σε απειλές. (38)

3.6 Σημαντικότητα των συστημάτων EDR

Όλοι οι οργανισμοί και γενικά όλοι οι χρήστες θα πρέπει να γνωρίζουν, ότι οι αντίπαλοι κάποια στιγμή θα επινοήσουν τελικά έναν τρόπο να ξεπεράσουν τις άμυνές, ανεξάρτητα από τοπόσο προχωρημένες είναι και πόσο προστατευμένοι είναι οι υπολογιστές των χρηστών.

Οι λόγοι για τους οποίους τα συστήματα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), θα πρέπει να αποτελεί μέρος της στρατηγικής ασφάλειας του τελικού σημείου σας είναι:

- Η πρόληψη από μόνη της δεν μπορεί να εξασφαλίσει τέλεια προστασία. Όταν η πρόληψη αποτυγχάνει, ο οργανισμός μπορεί να μείνει στο σκοτάδι από την τρέχουσα λύση ασφάλειας τελικού σημείου. Οι εισβολείς εκμεταλλεύονται αυτήν την κατάσταση για να παραμείνουν και να πλοηγηθούν μέσα στο δίκτυό υπολογιστών.
- Οι αντίπαλοι μπορεί να βρίσκονται μέσα στο δίκτυό για αρκετό καιρό και να επιστρέφουν κατά βούληση. Λόγω της σιωπηρής αποτυχίας, οι επιτιθέμενοι είναι ελεύθεροι να κυκλοφορούν στο περιβάλλον, δημιουργώντας συχνά backdoor που τους επιτρέπουν να επιστρέψουν κατά βούληση. Στις περισσότερες περιπτώσεις, ο οργανισμός μαθαίνει για την παραβίαση από τρίτους, όπως οι αρχές επιβολής του νόμου ή οι δικοί του πελάτες ή προμηθευτές.
- Οι οργανισμοί συνήθως δεν διαθέτουν την απαιτούμενη ορατότητα για την αποτελεσματική παρακολούθηση των τελικών σημείων. Όταν τελικά ανακαλυφθεί μια παραβίαση, ο οργανισμός-θύμα μπορεί να αφιερώσει μήνες προσπαθώντας να

αποκαταστήσει το συμβάν, επειδή δεν έχει την απαιτούμενη ορατότητα για να δει και να κατανοήσει ακριβώς τι συνέβη, με ποιον τρόπο συνέβη και πως να το διορθώσει, μόνο για να δει τον εισβολέα να επιστρέφει στο δίκτυο υπολογιστών.

- Απαιτείται πρόσβαση σε αξιόπιστες πληροφορίες για την καταγραφή ενός περιστατικού και για καταπολέμηση του. Οι οργανισμοί μπορεί όχι μόνο να μην έχουν την απαιτούμενη ορατότητα για να κατανοήσουν τι συμβαίνει στα τελικά σημεία τους, αλλά μπορεί να μην είναι σε θέση να καταγράψουν ό,τι σχετίζεται με την ασφάλεια, να το αποθηκεύσουν και στη συνέχεια να ανακαλέσουν τις πληροφορίες αρκετά γρήγορα όταν χρειάζεται.
- Η κατοχή των δεδομένων είναι μόνο μέρος της λύσης. Ακόμη και όταν τα δεδομένα είναι διαθέσιμα, οι ομάδες ασφαλείας χρειάζονται τους πόρους που απαιτούνται για την ανάλυση και την πλήρη αξιοποίησή τους. Αυτός είναι ο λόγος για τον οποίο πολλές ομάδες ασφαλείας διαπιστώνουν ότι αμέσως μετά την ανάπτυξη ενός προϊόντος συλλογής συμβάντων, όπως ένα SIEM, συχνά αντιμετωπίζουν ένα περίπλοκο πρόβλημα δεδομένων. Οι προκλήσεις γύρω από το να γνωρίζουμε τι πρέπει να αναζητήσουμε, την ταχύτητα και την επεκτασιμότητα αρχίζουν να εμφανίζονται και άλλα προβλήματα,προτού ακόμη μπορέσουν να αντιμετωπιστούν οι κύριοι στόχοι τους.
- Η αποκατάσταση μπορεί να είναι παρατεταμένη και δαπανηρή. Χωρίς τις δυνατότητες που αναφέρονται παραπάνω, οι οργανισμοί μπορούν να περάσουν εβδομάδες προσπαθώντας να διακρίνουν ποιες ενέργειες πρέπει να λάβουν.Συχνά η μόνη λύση είναι να επαναλάβουν την εικόνα των συστημάτων, κάτι που μπορεί να διαταράξει τις επιχειρηματικές διαδικασίες, να υποβαθμίσει την παραγωγικότητα και τελικά να προκαλέσει σοβαρή οικονομική ζημία.

3.7 Το μέλλον των συστημάτων EDR

Οι νέες δυνατότητες των συστημάτων ανίχνευσης και απόκρισης τελικών σημείων (**EDR**)έχουν ως αποτέλεσμα να βελτιώνουν τη νοημοσύνη των απειλών. Νέες δυνατότητες και υπηρεσίες διευρύνουν την ικανότητα των λύσεων των συστημάτων ανίχνευσης και απόκρισης τελικών σημείων (**EDR**) ,να εντοπίζουν και να διερευνούν νέες απειλές. Για παράδειγμα, οι υπηρεσίες πληροφοριών απειλών τρίτων, όπως το Trellix Global Threat Intelligence, αυξάνουν την αποτελεσματικότητα των λύσεων ασφάλειας τελικού σημείου.

Οι υπηρεσίες πληροφοριών απειλών παρέχουν σε έναν οργανισμό μια παγκόσμια δεξαμενή πληροφοριών σχετικά με τις τρέχουσες απειλές και τα χαρακτηριστικά τους. Αυτή η συλλογική νοημοσύνη βοηθά στην αύξηση της ικανότητας ενός συστήματος ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), να εντοπίζει εκμεταλλεύσεις, ειδικά επιθέσεις πολλαπλών επιπέδων και zero day attacks.

Πολλοί προμηθευτές ασφάλειας **EDR** προσφέρουν συνδρομές πληροφοριών απειλών ως μέρος της λύσης ασφάλειας τελικού σημείου τους.Επιπλέον, νέες ερευνητικές δυνατότητες σε ορισμένες λύσεις **EDR** μπορούν να αξιοποιήσουν την τεχνητή νοημοσύνη και τη μηχανική μάθηση, για να αυτοματοποιήσουν τα βήματα σε μια διαδικασία διερεύνησης.

Αυτές οι νέες δυνατότητες μπορούν να μάθουν τις βασικές συμπεριφορές ενός οργανισμού και να χρησιμοποιήσουν αυτές τις πληροφορίες, μαζί με μια ποικιλία άλλων πηγών πληροφοριών απειλών, για να ερμηνεύσουν τα ευρήματα.

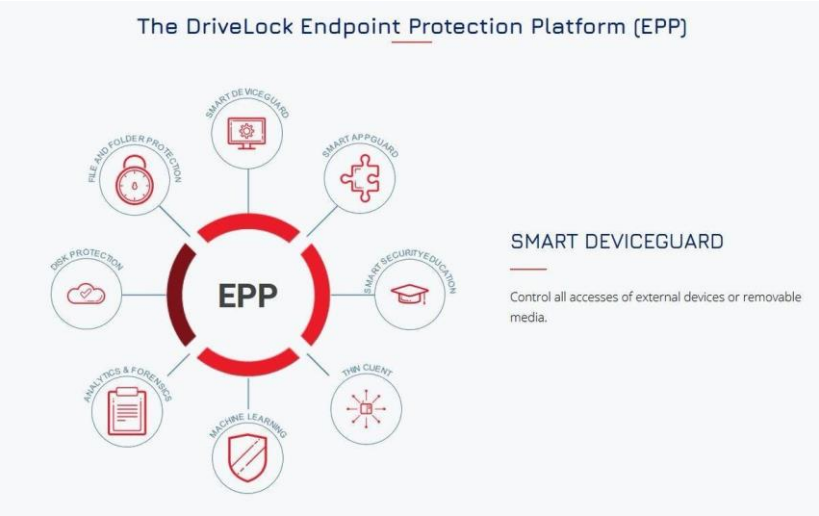
Ένας άλλος τύπος πληροφοριακών απειλών είναι το έργο Adversarial Tactics, Techniques, and Common Knowledge (**ATT&CK**) που βρίσκεται σε εξέλιξη στο **MITRE**, μια μη κερδοσκοπική ερευνητική ομάδα που συνεργάζεται με την κυβέρνηση των ΗΠΑ.

Το **ATT&CK** είναι μια βάση γνώσεων και ένα πλαίσιο που βασίζεται στη μελέτη εκατομμυρίων κυβερνοεπιθέσεων στον πραγματικό κόσμο. Το **ATT&CK** κατηγοριοποιεί τις κυβερνοαπειλές βάσει διαφόρων παραγόντων, όπως οι τακτικές που χρησιμοποιούνται για τη διείσδυση σε ένα σύστημα πληροφορικής, ο τύπος των τρωτών σημείων του συστήματος που εκμεταλλεύονται, τα εργαλεία κακόβουλου λογισμικού που χρησιμοποιούνται και οι εγκληματικές ομάδες που σχετίζονται με την επίθεση.

Το επίκεντρο της εργασίας είναι στον εντοπισμό προτύπων και χαρακτηριστικών που παραμένουν αμετάβλητα ανεξάρτητα από μικρές αλλαγές σε ένα κενό ασφαλείας. Λεπτομέρειες όπως οι διευθύνσεις IP, τα κλειδιά μητρώου και οι αριθμοί τομέα μπορούν να αλλάζουν συχνά. Αλλά οι μέθοδοι και οι τεχνικές ενός επιτιθέμενου συνήθως παραμένουν οι ίδιες.

Ένα σύστημα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), μπορεί να χρησιμοποιήσει αυτές τις κοινές συμπεριφορές, για να εντοπίσει απειλές που μπορεί να έχουν τροποποιηθεί με άλλους τρόπους.Καθώς οι επαγγελματίες ασφάλειας πληροφορικής αντιμετωπίζουν ολοένα και πιο περίπλοκες κυβερνοαπειλές και μεγαλύτερη ποικιλία στον αριθμό και τους τύπους των τελικών σημείων που έχουν πρόσβαση στο δίκτυο, χρειάζονται περισσότερη βοήθεια από την αυτοματοποιημένη ανάλυση και απόκριση που παρέχουν οι λύσεις εντοπισμού και απόκρισης τελικών σημείων.

Κεφάλαιο 4ο – Πλατφόρμες προστασίας τελικού σημείου (EPP)



Σχήμα 4.1 EPP-Συλλογη συστημάτων ασφαλείας (59)

4.1 Εισαγωγή στις πλατφόρμες προστασίας τελικού σημείου (EPP)

Στη σημερινή εποχή ο όγκος και η πολυπλοκότητα των κυβερνοεπιθέσεων ολοένα και αυξάνονται , με αποτέλεσμα τα συστήματα και τα δεδομένα τεχνολογίας πληροφοριών να βρίσκονται υπό συνεχή απειλή επίθεσης.

Οι κυβερνοεπιθέσεις έχουν γίνει ολοένα και πιο πολυεπίπεδες, χρησιμοποιώντας πολλαπλές, συντονισμένες τεχνικές με σκοπό, οι εισβολείς, να μπαίνουν στα συστήματα πληροφορικής ενός οργανισμού. Τα τελικά σημεία είναι συχνά η πόρτα από την οποία οι εισβολείς αποκτούν αρχική πρόσβαση.Η πλατφόρμα προστασίας τελικού σημείου (**EPP**) είναι μια ολοκληρωμένη λύση ασφαλείας, που αναπτύσσεται σε συσκευές τελικού σημείου για προστασία από απειλές. Όμως τι είναι ακριβώς μια πλατφόρμα προστασίας τελικού σημείου (EPP);

Μια πλατφόρμα προστασίας τελικού σημείου (**EPP**) είναι μια συλλογή τεχνολογιών ασφάλειας τερματικού σημείου, όπως προηγμένα προγράμματα προστασίας από κακόβουλα λογισμικά (**Anti-Virus**), ανίχνευση και απόκριση τελικού σημείου (**EDR**), κρυπτογράφηση δεδομένων και πρόληψη απώλειας δεδομένων.Αυτές οι τεχνολογίες συνήθως συνεργάζονται με μια συσκευή τερματικού σημείου,με σκοπό τον εντοπισμό, την πρόληψη και την απαλοιφή απειλών ασφαλείας, όπως επιθέσεις κακόβουλου λογισμικού που βασίζονται σε αρχεία και γενικώς κακόβουλη δραστηριότητα. (39) (40)

Μια πλατφόρμα προστασίας τελικού σημείου παρέχει ένα πλαίσιο για κοινή χρήση δεδομένων μεταξύ τεχνολογιών προστασίας τελικού σημείου. Αυτό παρέχει μια πιο αποτελεσματική προσέγγιση από μια συλλογή προϊόντων ασφαλείας που δεν έχουν την ικανότητα επικοινωνίας μεταξύ τους. Οι λύσεις που προσφέρουν οι πλατφόρμες προστασίας τελικού σημείου (**EPP**), μπορούν επίσης να βοηθήσουν τις ομάδες ασφαλείας, να διερευνήσουν και να ανταποκριθούν σε περιστατικά ασφαλείας καθώς συμβαίνουν αυτά σε πραγματικό χρόνο.

Οι πλατφόρμες προστασίας τελικών σημείων (**EPP**), έχουν επίσης τη δυνατότητα να παρέχουν έρευνα και αποκατάσταση σε περίπτωση δυναμικών συμβάντων ασφαλείας. Οι προηγμένες λύσεις των πλατφορμών προστασίας τελικών σημείων (**EPP**), χρησιμοποιούν πολλαπλές τεχνικές ανίχνευσης και διαχειρίζονται κυρίως Cloud δεδομένα, καθώς υποβοηθούνται από τέτοια δεδομένα με σκοπό να γίνεται προηγμένη παρακολούθηση συστημάτων τελικών σημείων, αλλά και απομακρυσμένη αποκατάσταση.

4.2 Τρόποι λειτουργίας και στρατηγικές των πλατφορμών προστασίας τελικού σημείου (EPP)

Μία από τις μεγαλύτερες απειλές για τα τελικά σημεία ενός οργανισμού, μιας επιχείρησης και γενικά ενός προσωπικού υπολογιστή είναι το κακόβουλο λογισμικό. Ο σκοπός του κακόβουλου λογισμικού είναι να μολύνει συνήθως μια συσκευή, που μπορεί να είναι ένας υπολογιστής και πολλά άλλα, παρασύροντας ένα χρήστη να κάνει κλικ σε έναν κακόβουλο σύνδεσμο που θα δει στο 'Ιντερνετ ή θα του το έχουν στείλει σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου, με σκοπό να το κατεβάσει και να εκτελέσει ένα μολυσμένο αρχείο ή να επισκεφτείέναν κακόβουλο ιστότοπο. Το κακόβουλο λογισμικό από τη στιγμή που θα εισέλθει στο περιβάλλον του χρήστη, έχει σκοπό να μολύνει όσο το δυνατόν περισσότερες διαδικασίες του συστήματος και σημεία δεδομένων.

Οι λύσεις προστασίας πλατφόρμας τελικού σημείου (EPP), έχουν την ικανότητα να

εμποδίσουν την είσοδο κακόβουλου λογισμικού στο περιβάλλον του ηλεκτρονικού υπολογιστή και να προστατεύσουν τα τελικά σημεία. Οι λύσεις της πλατφόρμας προστασίας τελικού σημείου αποκλείουν γνωστές απειλές για τα τελικά σημεία και μπορούν επίσης να εντοπίσουν άγνωστες απειλές ή απειλές zero-day.

Οι λύσεις προστασίας πλατφόρμας τελικών σημείων (EPP) για να μπορέσουν να προστατέψουν τα τελικά σημεία, χρησιμοποιούν διάφορες στρατηγικές για τον εντοπισμό, την πρόληψη και τον αποκλεισμό απειλών.

- Μια στρατηγική που χρησιμοποιούν τα συστήματα προστασίας πλατφόρμας τελικών σημείων (EPP), είναι η ανάλυση συμπεριφοράς των τελικών σημείων.

Αυτή η ανάλυση συνήθως περιλαμβάνει τη δημιουργία ενός βασικού γραφήματος που απεικονίζει τη συμπεριφορά για το κάθε τελικό σημείο, με σκοπό τον εντοπισμό ύποπτης ή ασυνήθιστης δραστηριότητας, ακόμα κι αν δεν ταιριάζει με μια γνωστή υπογραφή απειλής.

- Μια διαφορετική στρατηγική που ακολουθούν τα συστήματα προστασίας πλατφόρμας τελικών σημείων (EPP), είναι η ευφυΐα των απειλών των τελικών σημείων.

Το σύστημα προστασίας πλατφορμας τελικών σημείων(EPP), έχει τη δυνατότητα να ενσωματωθεί με διάφορες ροές που περιέχουν δεδομένα σχετικά με τις απειλές, τις τακτικές, τις τεχνικές και τις διαδικασίες αυτών των απειλών και να τις χρησιμοποιήσει για τον εντοπισμό απειλών.

- Μια διαφορετική στρατηγική που ακολουθούν τα συστήματα προστασίας πλατφόρμας τελικών σημείων με σκοπό την καταγραφή άγνωστων απειλών, είναι το sandboxing.

Οι περισσότερες λύσεις συστημάτων προστασίας πλατφόρμας τελικών σημείων (EPP), συνήθως διαθέτουν ένα sandbox ασφαλείας, που μπορεί να βάλει σε καραντίνα ορισμένα αρχεία που έχουν ύποπτη συμπεριφορά από κάποιο περιβάλλον, με σκοπό να το καταστήσουν ασφαλές.

Στο περιβάλλον sandbox, που υπάρχει σε ένα σύστημα προστασίας πλατφόρμας τελικών σημείων (**EPP**), υπάρχει η πιθανότητα κάποιο ύποπτο αρχείο να "εκραγεί" με ασφάλεια και να παρακολουθεί τη δραστηριότητά του χωρίς να θέτει σε κίνδυνο το υπόλοιπο σύστημα.Μια προηγμένη λύση προστασίας πλατφόρμας τελικών σημείων (EPP), χρησιμοποιεί τεχνολογίες πολλαπλών τελικών σημείων ανίχνευσης, συνδυάζοντας ανάλυση συμπεριφοράς και ευφυΐα απειλών.

Μπορεί να αναγνωρίσει άγνωστες απειλές και απειλές zero-day, καθώς και γνωστές υπογραφές επίθεσης. Τα σύγχρονα συστήματα προστασίας πλατφόρμας τελικών σημείων (**EPP**), αναπτύσσονται σε τελικά σημεία μέσω λογισμικού, αλλά η διαχείριση γίνεται στο Cloud και παρέχουν μια κεντρική κονσόλα που βασίζεται στον ιστό.

Οι λύσεις προστασίας τελικού σημείου αποτρέπουν τις παραβιάσεις συλλέγοντας μεγάλα τμήματα δεδομένων από τα τελικά σημεία και εφαρμόζουν τα καλύτερα εργαλεία, όπως τεχνητή νοημοσύνη (AI), ανάλυση συμπεριφοράς, νοημοσύνη απειλών και κυνηγοί ανθρώπινων απειλών.

Οι αποτελεσματικές λύσεις πρέπει να αξιοποιήσουν αυτά τα τεράστια δεδομένα, για να προβλέπουν συνεχώς πού θα εμφανιστεί η επόμενη προηγμένη απειλή.Η προστασία τελικού

σημείου παρέχει ουσιαστική ασφάλεια για πολλούς τύπους τερματικών σημείων, από έξυπνα τηλέφωνα έως εκτυπωτές.

Μια πλατφόρμα προστασίας τελικού σημείου (EPP), όπως είπαμε παραπάνω, είναι μια ολοκληρωμένη συλλογή τεχνολογιών προστασίας τελικού σημείου όπως Anti-Virus, κρυπτογράφηση δεδομένων, πρόληψη εισβολής και πρόληψη απώλειας δεδομένων που εντοπίζει και σταματά μια ποικιλία απειλών στο τελικό σημείο. (41) (42)

4.3 Τεχνικές που χρησιμοποιούν οι εισβολείς με σκοπό την αποφυγή πλατφόρμας προστασίας τελικού σημείου

Το βασικό κίνητρο πίσω από την ανάπτυξη πλατφόρμας προστασίας τελικού σημείου (EPP), ήταν το γεγονός ότι οι εισβολείς και γενικά οι κακόβουλοι χρήστες είχαν τη δυνατότητα να αποφεύγουν σχετικά εύκολα τις παραδοσιακές λύσεις ασφάλειας. Ουσιαστικά, οι εισβολείς έχουν προχωρήσει πέρα από τις δυνατότητες της παραδοσιακής ασφάλειας τελικού σημείου και είναι πλέον σε θέση να παραμείνουν απαρατήρητοι σε δίκτυα για μεγάλες χρονικές περιόδους, πράγμα καταστροφικό.

Υπάρχουν πέντε διαφορετικοί τρόποι που χρησιμοποιούν οι εισβολείς και έχουν τη δυνατότητα να παρακάμπτουν την παραδοσιακή ασφάλεια τελικού σημείου.

- Fileless Ransomware

Σε αυτές τις τεχνικές δεν υπάρχει κάποιο αρχείο με σκοπό να γίνει ο εντοπισμός και στη συνέχεια ο αποκλεισμός του. Οι τεχνικές χωρίς αρχεία για την παράδοση ransomware δεν διαταράσσονται σε μεγάλο βαθμό από την παραδοσιακή ασφάλεια τελικού σημείου.

Σύμφωνα με μια έκθεση κυβερνοασφάλειας από το SecureWorld, οι επιθέσεις χωρίς αρχεία αυξήθηκαν κατά 18% το πρώτο εξάμηνο του 2019 σε σύγκριση με το δεύτερο εξάμηνο του 2018. Μόνο με μια πλατφόρμα προστασίας τελικού σημείου (EPP), ο χρήστης τελικού σημείου έχει τη δυνατότητα να παρακολουθεί διάφορες συμπεριφορές με σκοπό να βρεθούν διάφορα μοτίβα που ειδοποιούν το χρήστη για τις τεχνικές επίθεσης χωρίς αρχεία.

- Διαθέσιμες νέες τεχνικές επίθεσης

Οι προηγμένες τεχνικές επίθεσης έχουν κλαπεί ή αναπτυχθεί από εγκληματίες του κυβερνοχώρου και διατίθενται προς πώληση ή απλώς υπάρχουν ως script ανοιχτού κώδικα στο διαδίκτυο και στο σκοτεινό ιστό (Dark Web). Η χρήση αυτών των σεναρίων και τακτικών επιτρέπει στη δραστηριότητα των επιτιθέμενων να φαίνεται φυσιολογική και να παραμένει κρυφή μέσα σε ένα δίκτυο.

- Ξεπερασμένα τελικά σημεία

Οι τεχνικές που χρησιμοποιούν οι εισβολείς, αλλά και ο αριθμός των διάφορων απειλών εξελίσσεται γρήγορα. Αυτό σημαίνει ότι οι προμηθευτές ασφαλείας είναι υποχρεωμένοι να αναπτύσσουν ενημερώσεις κώδικα και γενικά ενημερώσεις όσο το δυνατόν γρηγορότερα για να προσπαθήσουν να συμβαδίσουν με τις αναδυόμενες απειλές. Οι πράκτορες τελικού σημείου συχνά αποτυγχάνουν, αφήνοντας μεμονωμένα τελικά σημεία ανασφαλή.

Μια αναφορά Global Endpoint Security Trends για το 2019 έδειξε ότι το 35% των παραβιάσεων τελικού σημείου προκαλούνται από υπάρχοντα τρωτά σημεία. Δεδομένου ότι οι πλατφόρμες προστασίας τελικών σημείων βασίζονται συνήθως σε cloud, μπορούν να

παραμένουν συνεχώς ενημερωμένες , για να διατηρούν τα τελικά σημεία προστατευμένα από τις πιο πρόσφατες απειλές.

- Πολλαπλές πηγές δεδομένων

Οι παραδοσιακές λύσεις ασφάλειας τελικού σημείου εκτελούνται σε σχετική απομόνωση από την υπόλοιπη στοίβα ασφαλείας. Αυτό σημαίνει ότι απαιτεί πολλαπλά συστήματα για την προβολή της δραστηριότητας σε ένα μόνο τελικό σημείο και τον εντοπισμό τυχόν ύποπτης δραστηριότητας σε όλο το δίκτυο κατά τη διάρκεια μιας έρευνας.

Οι πλατφόρμες προστασίας τελικού σημείου (EPP), παρέχουν μια ενιαία πηγή αλήθειας, συνδυάζοντας δεδομένα από όλες τις λύσεις ασφαλείας σε όλη την πλατφόρμα για να παρέχουν εύκολη πρόσβαση σε δεδομένα και διερεύνηση ειδοποιήσεων.

- Φιλτραρισμένα δεδομένα τελικού σημείου

Πολλές λύσεις ασφάλειας τελικού σημείου φιλτράρουν δεδομένα τελικού σημείου που θεωρούνται άσχετα με μια απειλή σύμφωνα με γνωστά πρότυπα συμπεριφοράς και IOC. Τώρα που οι εισβολείς έχουν πιο προηγμένες τεχνικές, βασίζονται στο φιλτράρισμα δεδομένων τελικού σημείου για να φιλτράρουν τη δραστηριότητά τους. Όταν γίνεται συνεχώς καταγραφή δεδομένων δραστηριότητας τελικού σημείου, οι χρήστες έχουν τη δυνατότητα να εντοπίσουν αυτές τις νέες τεχνικές και να προβλέψουν νέες απειλές.

4.4 Παροχές των συστημάτων προστασίας πλατφόρμας τελικού σημείου (EPP)

Οι λύσεις των συστημάτων προστασίας πλατφόρμας τελικών σημείων (**EPP**), χρησιμοποιούν ένα ευρύ φάσμα δυνατοτήτων ασφάλειας, αλλά σε βασικό επίπεδο περιλαμβάνουν:

- Πρόληψη κακόβουλου λογισμικού που βασίζεται σε αρχεία.
- Ανίχνευση ύποπτης δραστηριότητας με τη χρήση τεχνικών που κυμαίνονται από δείκτες συμβιβασμού (IOC) έως και ανάλυση συμπεριφοράς.
- Εργαλεία διερεύνησης και αποκατάστασης για τη διαχείριση δυναμικών συμβάντων και ειδοποιήσεων.

Ωστόσο, κάθε πλατφόρμα μπορεί να διαφέρει σε πολλά χαρακτηριστικά από άλλες πλατφόρμες. Αυτό συμβαίνει, διότι ορισμένα χαρακτηριστικά είναι κατάλληλα για ορισμένες περιπτώσεις χρήσης.Οι πλατφόρμες προστασίας τελικού σημείου (EPP), είναι η τελευταία εξέλιξη της ασφάλειας ενός τελικού σημείου. Αναπτύχθηκαν με σκοπό να εντοπίζουν επιτιθέμενους που μπορούν να παρακάμψουν την παραδοσιακή ασφάλεια του τελικού σημείου, καθώς και για να βοηθήσουν στην ενοποίηση περίπλοκων στοίβων ασφαλείας.

Με την ενοποίηση αυτή βελτιώνεται και η κοινή χρήση δεδομένων, η οποία βελτιώνει τα διαθέσιμα αναλυτικά στοιχεία για τον εντοπισμό ύποπτης συμπεριφοράς. Επίσης, απλοποιεί σημαντικά τις λειτουργίες ασφαλείας.

Ένα άλλο σημαντικό πλεονέκτημα των πλατφορμών προστασίας τελικού σημείου (**EPP**) είναι η μετάβαση στο Cloud. Τα συστήματα EPP χρησιμοποιούν δεδομένα στο cloud και έχουν τη δυνατότητα να χρησιμοποιούν έναν μόνο, ελαφρύ παράγοντα για την παρακολούθηση όλων των τελικών σημείων ενός οργανισμού ή γενικά τα τελικά σημεία που πρέπει να ασφαλιστούν. Επιπλέον, τα δεδομένα που μπορούν να συλλεχθούν και να χρησιμοποιηθούν υπερβαίνουν κατά πολύ τα τελικά σημεία μιας μεμονωμένης εταιρείας.

Τα παγκόσμια κοινά δεδομένα που απεικονίζουν τις τακτικές επιτιθέμενων μπορούν να απορροφηθούν για να βελτιωθεί ο εντοπισμός των συμπεριφορών του

επιτιθέμενου.Μελετώντας τις «Κρίσιμες Δυνατότητες για Πλατφόρμες Προστασίας Τελικών Σημείων», η Gartner προαναγγέλλει τη σημασία του συστήματος προστασίας πλατφόρμας τελικού σημείου (**EPP**), που βασίζεται σε σύννεφο δηλώνοντας ότι, «Οι λύσεις **EPP** που βασίζονται στο cloud παρέχουν ταχύτερο χρόνο στην αξία, χαμηλότερο κόστος διαχείρισης και πιο ευέλικτες βελτιώσεις προϊόντων από τις παραδοσιακές επί τόπου αναπτύξεις».

Στο τελευταίο Magic Quadrant for Endpoint Protection Platforms της Gartner, η Gartner βλέπει τα συστήματα προστασίας πλατφόρμας τελικού σημείου (**EPP**), να εξελίσσονται ραγδαία έτσι ώστε να παρέχουν «αυτοματοποιημένη, ενορχηστρωμένη διερεύνηση συμβάντων και απόκριση παραβίασης». Πέρα από τα παραπάνω, οι πλατφόρμες προστασίας τελικού σημείου (**EPP**), που βασίζονται κυρίως σε Cloud, έχουν τη δυνατότητα να καθιστούν την ανάλυση συμπεριφοράς των δραστηριοτήτων ενός τελικού σημείου σε πραγματικό χρόνο.

Το πιο προηγμένο σύστημα προστασίας πλατφόρμας τελικού σημείου (**EPP**), έχει τη δυνατότητα να χρησιμοποιεί επεξεργασία ροής συμβάντων.Η επεξεργασία ροής συμβάντων είναι η ίδια τεχνολογία που χρησιμοποιείται στον εντοπισμό απάτης με πιστωτικές κάρτες.Αυτή η τεχνολογία χρησιμοποιείται με σκοπό να μεταμορφώσει την ασφάλεια του τελικού σημείου. Αυτό επιτρέπει τον εντοπισμό συμπεριφορών που επιδεικνύουν οι επιτιθέμενοι. Οι επιτιθέμενοι προσπαθουν σκόπιμα να συμπεριφερθούν φυσιολογικά,με σκοπό να κρύψουν τις τακτικές που ακολουθούν.

Ορισμένα συστήματα προστασίας πλατφόρμας τελικού σημείου (**EPP**), έχουν διάφορα χαρακτηριστικά που φαίνονται πολύ χρήσιμα ειδικά για τα τελικά σημεία ενός οργανισμού ή μιας επιχείρησης. Αυτά είναι:

- Προσεγγίσεις ανίχνευσης και αποκατάστασης πολλαπλών απειλών.

Μια πλατφόρμα προστασίας τελικού σημείου (**EPP**), μπορεί να παρέχει πολλαπλές λειτουργίες ανίχνευσης και αποκατάστασης απειλών ενσωματωμένες σε μία πλατφόρμα. Οι κοινές δυνατότητες της πλατφόρμας προστασίας τελικού σημείου (**EPP**), περιλαμβάνουν την ασφάλεια του προγράμματος περιήγησης ιστού, τη σάρωση υπογραφής κακόβουλου λογισμικού, τον αποκλεισμό διανυσμάτων επίθεσης για την αποτροπή κακόβουλου λογισμικού χωρίς αρχεία, την αποκατάσταση επαναφοράς και την αναγνώριση κλοπής διαπιστευτηρίων.

Κάθε προμηθευτής πλατφόρμας προστασίας τελικού σημείου (**EPP**), προσφέρει μια μοναδική συλλογή δυνατοτήτων, χρησιμοποιώντας διαφορετικές τεχνικές ανίχνευσης και αποκατάστασης. Ωστόσο, οι περισσότεροι προμηθευτές χρησιμοποιούν συστήματα ανίχνευσης και απόκρισης (**EDR**), και πρόληψη απώλειας δεδομένων (**DLP**). Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), είναι υπεύθυνο να παρακολουθεί τα συμβάντα του τελικού σημείου και να αποθηκεύει αυτά τα δεδομένα για μεταγενέστερη ανάλυση, ενώ το σύστημα πρόληψης απώλειας δεδομένων (**DLP**), είναι υπεύθυνο να εμποδίζει συνέχεια τους τελικούς χρήστες να μοιράζονται ευαίσθητες πληροφορίες εξωτερικά.

- Πλαίσιο Ένταξης.

Τα συστήματα προστασίας πλατφόρμας τελικών σημείων (**EPP**), βασίζονται συνήθως σε πλαίσια που υποστηρίζουν την ανταλλαγή πληροφοριών μεταξύ εργαλείων ασφαλείας, συμπεριλαμβανομένων τρίτων που είναι ήδη εγκατεστημένα στη στοίβα. Τα κοινά προϊόντα τρίτων κατασκευαστών ασφαλείας περιλαμβάνουν τα συστήματα πρόληψης απώλειας δεδομένων (**DLP**), συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) και συστήματα πρόληψης εισβολής (**IPS**).

Μια ανοιχτή αρχιτεκτονική του συστήματος προστασίας πλατφόρμας τελικού σημείου (**EPP**), έχει ως σκοπό την επίτευξη ορατότητας σε όλες τις συσκευές τελικού σημείου, καθώς και τα εργαλεία ασφάλειας τελικού σημείου σε ολόκληρο τον οργανισμό, επιτρέποντας στην ομάδα ασφάλειας να έχουν την ικανότητα να παρακολουθούν τα πάντα χρησιμοποιώντας έναν πίνακα ελέγχου ή ένα τερματικό σημείο, κονσόλα. Η ρύθμιση αυτής της συλλογικής ανταλλαγής πληροφοριών μεταξύ πολλών προϊόντων διευκολύνει τον γρήγορο εντοπισμό και την αποκατάσταση των τελικών σημείων από τις διάφορες απειλές.

- Κεντρική Διοίκηση.

Μια πλατφόρμα προστασίας τελικού σημείου (**EPP**), πρέπει να παρέχει μια κεντρική κονσόλα για να βοηθήσει τους τελικούς χρήστες στη διαχείριση όλων τελικών σημείων και λειτουργιών ασφαλείας τους.

Ο συγκεντρωτισμός αυτός παρέχει την διευκόλυνση στους τελικούς χρήστες ώστε να έχουν την απαιτούμενη ορατότητα σε απειλές ασφαλείας καθώς και σε ζητήματα συμμόρφωσης.Επίσης βοηθά στην απαλλαγή των ομάδων πληροφορικής από το βάρος της μετακίνησης μεταξύ οθονών για τη μη αυτόματη ανάλυση πληροφοριών απειλών.

Το ιδανικό γραφικό περιβάλλον της πλατφόρμας προστασίας τελικού σημείου (**EPP**) παρέχει ένα φιλικό προς τον χρήστη και διαμορφώσιμο πίνακα εργαλείων που περιλαμβάνει ειδοποιήσεις, βασικούς δείκτες απόδοσης (KPI) και την τρέχουσα κατάσταση ασφαλείας. Θα πρέπει να επιτρέπει στους χρήστες να διερευνούν εύκολα κάθε τελικό σημείο και κάθε απειλή.

- Πρόληψη απώλειας δεδομένων (**DLP**), που εμποδίζει τους τελικούς χρήστες να μοιράζονται ευαίσθητο περιεχόμενο εκτός του οργανισμού.
- Δεδομένα απειλών σε πραγματικό χρόνο.

Μια πλατφόρμα προστασίας τελικού σημείου (**EPP**), απαιτεί συνεχή πρόσβαση σε δεδομένα απειλών σε πραγματικό χρόνο, τόσο στον οργανισμό όσο και παγκοσμίως, για τον εντοπισμό και τον αποκλεισμό επιθέσεων zero-day. Ο προμηθευτής του **EPP** θα πρέπει να παρέχει πρόσβαση σε μια παγκόσμια βάση δεδομένων συνεχιζόμενης δραστηριότητας απειλών.

Οι κυβερνοεπιθέσεις, οι παραβιάσεις δεδομένων, οι εσωτερικές διαρροές δεδομένων και άλλοι τύποι παραβιάσεων ασφάλειας είναι κοινά στους περισσότερους οργανισμούς. Ωστόσο, οι πελάτες και οι συνεργάτες αναμένουν από τους οργανισμούς να προστατεύουν αξιόπιστα τα ευαίσθητα δεδομένα τους.

Μια παραβίαση δεδομένων μπορεί να έχει σημαντικό αρνητικό αντίκτυπο στην επιχείρηση.Οι πλατφόρμες προστασίας τελικών σημείων (**EPP**), βοηθούν στην προστασία των οργανισμών από επιθέσεις σε ευάλωτα τελικά σημεία. Μια πλατφόρμα προστασίας τελικών σημείων (**EPP**), επιτρέπει επίσης σε διαφορετικές τεχνολογίες ασφαλείας να ανταλλάσσουν πληροφορίες σχετικά με συμβάντα ασφαλείας, επιτρέποντας βαθύτερη ανάλυση και καλύτερη κατανόηση του τρόπου βελτίωσης της ασφάλειας τελικού σημείου του οργανισμού. Μια

πλατφόρμα προστασίας τελικού σημείου παρέχει ένα ενοποιημένο πλαίσιο και διεπαφή για ορατότητα και έλεγχο.

4.4.1 Διάφορα κρίσιμα στοιχεία που πρέπει να παρατηρήσει ένας οργανισμός σχετικά με το σύστημα EPP

Τα συστήματα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), είναι ένα από τα θεμελιώδη

στοιχεία μιας πλατφόρμας προστασίας τελικών σημείων (EPP). Ωστόσο, υπάρχουν πολλά άλλα στοιχεία, που οι οργανισμοί πρέπει να ενσωματώσουν στη στρατηγική τους στον κυβερνοχώρο, για να εξασφαλίσουν προστασία από προηγμένες απειλές και ταχέως εξελισσόμενα συστήματα από αντιπάλους οργανισμούς. Αυτά τα στοιχεία περιλαμβάνουν:

- Πρόληψη με σκοπό την αποφυγή όσο το δυνατόν περισσότερων κακόβουλων στοιχείων.
- Ανίχνευση με σκοπό την εύρεση και τέλος αφαίρεση επιτιθέμενων.
- Διαχειρισμός του κυνηγιού απειλών με σκοπό την ανύψωση και την ανίχνευση πέρα από την αυτοματοποίηση.
- Ενσωμάτωση πληροφοριών των διάφορων απειλών με σκοπό την κατανόηση και την πρόβλεψη των επιτιθέμενων και των τεχνικών τους.
- Διαχείριση ευπάθειας και υγιεινή πληροφορικής με σκοπό την προετοιμασία και την ενίσχυση του περιβάλλοντος του οργανισμού έναντι απειλών και επιθέσεων.

Με βάση τα παραπάνω, μια πλατφόρμα προστασίας τελικών σημείων (**EPP**), θα πρέπει να προσφέρει ένα ευρύ φάσμα δυνατοτήτων κυβερνοασφάλειας πέρα από την πρόληψη. Στην πραγματικότητα, όταν αναφερόμαστε στον όρο πρόληψη, συνήθως αναφερόμαστε μόνο στο στοιχείο του προγράμματος προστασίας από ιούς και γενικά από κακόβουλα λογισμικά επόμενη γενιάς (**NGAV**) μιας πλατφόρμας προστασίας τελικών σημείων (**EPP**). Ομοίως, το σύστημα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), πληροί μόνο τη δυνατότητα ανίχνευσης εντός της πλήρους σειράς υπηρεσιών της πλατφόρμας προστασίας τελικών σημείων (**EPP**). (42) (40)

4.5 Διαφορές παραδοσιακών πλατφορμών προστασίας τελικού σημείου (EPP) με EPP που στηρίζονται στο cloud

Παραδοσιακά, οι οργανισμοί χρησιμοποιούσαν μια λύση ασφάλειας τελικού σημείου που λειτουργούσε μέσω μιας εσωτερικής προσέγγισης hub-and-spoke, στο κέντρο της οποίας ήταν το κέντρο δεδομένων. Τα τελικά σημεία προστατεύονταν μέσω πρακτόρων οι οποίοι διαχειρίζονται από την κεντρική κονσόλα.

Αυτό δημιούργησε ένα θέμα ασφαλείας, επειδή τα τελικά σημεία εκτός της περιμέτρου του δικτύου δεν ήταν διαχειρίσιμα.Αυτό το μοντέλο δεν είναι πλέον αποτελεσματικό, καθώς οι νέες τάσεις όπως η ξαφνική άνοδος της εργασίας από το σπίτι και η παγκοσμιοποίηση του εργατικού δυναμικού έχουν ωθήσει πολλές επιχειρήσεις να αναζητήσουν πιο αποτελεσματικές λύσεις. Ορισμένοι έχουν μετασκευάσει τις παλαιού τύπου λύσεις τους, για να δημιουργήσουν μια υβριδική προσέγγιση, ενώ άλλοι έχουν αναζητήσει λύσεις στο Cloud.

Τα εργαλεία ασφάλειας τελικού σημείου στο Cloud ελέγχονται μέσω ενός κεντρικού γραφικού περιβάλλοντος στο Cloud και συνδέονται με συσκευές μέσω πρακτόρων που τοποθετούνται στα ίδια τα τελικά σημεία. Αυτοί οι πράκτορες μπορούν να λειτουργούν

ανεξάρτητα, όταν η συσκευή τελικού σημείου είναι εκτός σύνδεσης. Τα στοιχεία ελέγχου και οι πολιτικές του Cloud μεγιστοποιούν την απόδοση ασφάλειας, επεκτείνουν την πρόσβαση διαχειριστή και εξαλείφουν οποιαδήποτε θέματα ασφαλείας και αν υπήρξαν.

4.5.1 Διαφορές πλατφόρμας προστασίας τελικού σημείου (EPP) με συστήματα ανίχνευσης και απόκρισης τελικού σημείου (EDR)

Το σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) είναι μόνο ένα στοιχείο μιας πλατφόρμας προστασίας τελικού σημείου. Από την άλλη πλευρά, μια πλατφόρμα προστασίας τελικού σημείου αποτελείται από πολλές τεχνολογίες κυβερνοασφάλειας,

συμπεριλαμβανομένων των προγραμμάτων προστασίας από ιούς (Anti-Virus) επόμενης γενιάς, πληροφοριών απειλών, διαχείρισης ευπάθειας και συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**).

Μία πλήρως εξοπλισμένη πλατφόρμα προστασίας τελικού σημείου (**EPP**), ενσωματώνει μια λύση συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), με σκοπό να προσφέρει δυνατότητες ανίχνευσης. Τα συστήματα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**),δίνουν τη δυνατότητα σε μια πλατφόρμα προστασίας τελικού σημείου (**EPP**), να μετριάσει και να εξουδετερώσει μια παραβίαση που έχει αποκαλυφθεί.

Αυτό θα μπορούσε να σημαίνει περιορισμό των εκτεθειμένων τελικών σημείων για να σταματήσει η παραβίαση στα ίχνη της, επιτρέποντας την αποκατάσταση πριν από την εμφάνιση ζημιάς.Η ανίχνευση και η απόκριση τελικού σημείου (**EDR**) είναι μια τεχνολογία ασφαλείας που παρακολουθεί συνεχώς συσκευές τελικού σημείου και φόρτους εργασίας και παρέχει ορατότητα στη δραστηριότητα σε πραγματικό χρόνο στα τελικά σημεία. Αυτό επιτρέπει στις ομάδες κυβερνοασφάλειας να εντοπίζουν γρήγορα και αποτελεσματικά και να ανταποκρίνονται σε απειλές στον κυβερνοχώρο, όπως ransomware, κακόβουλο λογισμικό και παραβίαση τελικού σημείου.

Τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου(**EDR**) θεωρούνται ως ένα δίχτυ ασφαλείας, που συλλαμβάνει απειλές που δεν μπορούσαν να εντοπιστούν ή να αποκλειστούν από άλλες άμυνες στο τελικό σημείο.

Τα εργαλεία ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) παρέχουν προηγμένες δυνατότητες ανίχνευσης απειλών τελικού σημείου, συμπεριλαμβανομένης και της ανακάλυψης δεδομένων συμβάντων, της ταξινόμησης ειδοποιήσεων, της αναζήτησης απειλών, της ανίχνευσης κακόβουλης συμπεριφοράς και του περιορισμού απειλών. Επιτρέπουν στις ομάδες ασφαλείας όχι μόνο να εντοπίζουν και να διερευνούν επιθέσεις, αλλά και να λαμβάνουν μέτρα εξ αποστάσεως για τον περιορισμό και την εξάλειψη της απειλής.

Η σχέση μεταξύ της πλατφόρμας προστασίας τελικού σημείου (**EPP**) και του συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), είναι ότι οι πλατφόρμες προστασίας τελικού σημείου (**EPP**) ενδέχεται να περιέχουν μια λύση ή κάποια δυνατότητα συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**). Αυτό επιτρέπει στην πλατφόρμα προστασίας τελικού σημείου (**EPP**), όχι μόνο να εντοπίζει ανώμαλα συμβάντα, αλλά και να υποστηρίζει τις ομάδες ασφαλείας στη διερεύνηση, τον μετριασμό και την εξάλειψη των παραβιάσεων στα αρχικά στάδια, προτού προκαλέσουν ζημιά στα τελικά σημεία.

EPP	EDR
Antivirus/Malware	Behaviour Detection
Device Control	Threat Hunting
Web Filtering	Machine Learning
Data Leakage Prevention	IOC
Firewall	Remediation
Encryption	Forensics
	Root Cause Analysis

Σχήμα 4.1 Διαφορές EPP-EDR

Συνήθως οι οργανισμοί δεν επιλέγουν, για τα τελικά σημεία, μόνο πλατφόρμα προστασίας τελικού σημείου (**EPP**) ή συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**),αλλά η επιλογή που κάνουν είναι:

- Χρησιμοποιεί μια βασική λύση της πλατφόρμας προστασίας τελικού σημείου (**EPP**), που έχει μόνο προληπτικά μέτρα και δεν υποστηρίζει συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**).
- Χρησιμοποιεί μια προηγμένη λύση της πλατφόρμας προστασίας τελικού σημείου (**EPP**) που περιλαμβάνει συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**).Συνήθως με επιπλέον κόστος.

Με βάση τους παραπάνω ορισμούς, μπορούμε να καταλάβουμε ότι η ανίχνευση και η απόκριση τελικού σημείου (**EDR**), είναι μόνο ένα στοιχείο μιας πλατφόρμας προστασίας τελικού σημείου (**EPP**). Επιπλέον, μία πλατφόρμα προστασίας τελικού σημείου (**EPP**), αποτελείται από πολλές πρόσθετες τεχνολογίες κυβερνοασφάλειας πέρα από την ανίχνευση, συμπεριλαμβανομένων των προγραμμάτων προστασίας από ιούς και γενικά από κακόβουλα λογισμικά (Anti-Virus) και προγράμματα προστασίας επόμενης γενιάς (**NGAV**), του κυνηγιού απειλών, της ευφυΐας απειλών και της διαχείρισης ευπάθειας.

Μία προηγμένη ή πλήρως εξοπλισμένη πλατφόρμα προστασίας τελικών σημείων (**EPP**) ενσωματώνει μια λύση συστήματος ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), με σκοπό να προσφέρει ισχυρές δυνατότητες ανίχνευσης και απόκρισης.

Αυτή η ένωση των συστημάτων **EDR** και **EPP**, σε ένα ενιαίο σύστημα ασφάλειας επιτρέπει σε μια πλατφόρμα προστασίας τελικού σημείου (**EPP**), όχι μόνο να εντοπίζει ένα ανώμαλο συμβάν, αλλά και να διερευνά και να μετριάζει μια παραβίαση που αποκαλύπτεται. Αυτό θα μπορούσε να σημαίνει περιορισμό των εκτεθειμένων τελικών σημείων για να σταματήσει η παραβίαση στα ίχνη της, επιτρέποντας την αποκατάσταση πριν από την εμφάνιση ζημιάς.

Έτσι βλέπουμε ότι είναι πάρα πολύ σημαντικο για έναν οργανισμό ή και γενικά για οποιοδήποτε τελικό σημείο, να έχει μία συλλογή από συστήματα ασφαλείας. Τέτοια συστήματα είναι τα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), η πλατφόρμα προστασίας τελικού σημείου (**EPP**) και τέλος τα προγράμματα προστασίας από ιούς και γενικά από κακόβουλα λογισμικά (**Anti-Virus**) και φυσικά προγράμματα προστασίας από ιούς και γενικά κακόβουλα λογισμικά επόμενη γενιάς (**NGAV**).

4.5.2 Διάφορες παρανοήσεις που γίνονται μεταξύ πλατφόρμας προστασίας τελικού σημείου (EPP) και συστημάτων ανίχνευσης και απόκρισης τελικού σημείου (EDR)

Τώρα που εξετάσαμε τα βασικά στοιχεία της πλατφόρμας προστασίας τελικών σημείων (**EPP**) και του συστήματος ανίχνευσης και απόκρισης τελικών σημείων (**EDR**) και διερευνήσαμε τη σχέση που έχουν μεταξύ τους, πρέπει να ξεκαθαρίσουμε μερικές από τις πιο κοινές παρανοήσεις σχετικά με αυτές τις δύο δυνατότητες ασφάλειας.

1. Οι οργανισμοί πρέπει να επιλέξουν ένα σύστημα ασφάλειας μεταξύ της πλατφόρμας προστασίας τελικών σημείων (**EPP**) και του συστήματος ανίχνευσης και απόκρισης τελικών σημείων (**EDR**).

Οι οργανισμοί δεν χρειάζεται να κάνουν μια δυαδική επιλογή μεταξύ της πλατφόρμας προστασίας τελικών σημείων (**EPP**) ή του συστήματος ανίχνευσης και απόκρισης τελικών σημείων (**EDR**). Στην πραγματικότητα, αυτές είναι δύο ξεχωριστές δυνατότητες που έχουν

περιορισμένη αξία από μόνες τους.

Μπορείτε να σκεφτείτε την πλατφόρμα προστασίας τελικών σημείων (**EPP**) ως ένα αυτοκίνητο και το σύστημα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**) ως ένα κινητήρα. Έτσι καταλαβαίνουμε ότι το ένα είναι σχεδόν άχρηστο χωρίς το άλλο και πρέπει να συνεργάζονται για να έχουμε το καλύτερο δυνατό αποτέλεσμα.

2. Η πλατφόρμα προστασίας τελικών σημείων (**EPP**) είναι μια παθητική μορφή πρόληψης απειλών.

Το **EPP** σημαίνει πλατφόρμα προστασίας τελικού σημείου και όχι παθητική πρόληψη. Ενώ η πρόληψη είναι μια σημαντική ικανότητα εντός της πλατφόρμας προστασίας τελικών σημείων (**EPP**), είναι μόνο μια μορφή προστασίας που παρέχεται από την πλατφόρμα.

Εκτός από την πρόληψη, μια αληθινή πλατφόρμα προστασίας τελικών σημείων (**EPP**) θα περιλαμβάνει επίσης ανίχνευση, κυνήγι απειλών, ευφυΐα απειλών και διαχείριση ευπάθειας.

3. Αρκεί ένα αυτόνομο σύστημα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**).

Ένα σύστημα ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), βοηθά τις ομάδες ασφαλείας να κατανοήσουν τι ακριβώς συμβαίνει σε όλο το δίκτυο σε επίπεδο τελικού σημείου, το οποίο με τη σειρά του μπορεί να βοηθήσει να εντοπιστούν οι απειλές, που έχει ένα σύστημα και να αποκατασταθούν τα συστήματα που έχουν υποστεί επιθέσεις.

Ωστόσο, για την άμυνα ενάντια στις περισσότερες σύγχρονες επιθέσεις στον κυβερνοχώρο, είναι απαραίτητο να χρησιμοποιηθεί μια πολύ ευρύτερη και πιο ολοκληρωμένη σειρά δυνατοτήτων για την καλύτερη δυνατή προστασία του οργανισμού, συμπεριλαμβανομένων εκείνων που τροφοδοτούνται τόσο από ανθρώπινη νοημοσύνη όσο και από συμπληρωματικές τεχνολογίες. (43)

4.5.3 Διαφορές πλατφόρμας προστασίας τελικού σημείου (EPP) με άλλα συστήματα ασφάλειας

Υπάρχουν πολλές κατηγορίες προϊόντων ασφάλειας τελικού σημείου. Μερικά κοινά προϊόντα συνήθως περιλαμβάνουν Anti-Malware, ασφάλεια προγράμματος περιήγησης ιστού, ασφάλεια φορητών συσκευών, ασφάλεια ενσωματωμένης συσκευής και ανίχνευση καιαπόκριση τελικού σημείου (**EDR**).

Αυτά τα διαφορετικά προϊόντα βοηθούν στην προστασία μιας ποικιλίας τελικών σημείων, συμπεριλαμβανομένων διακομιστών, επιτραπέζιων υπολογιστών, φορητών υπολογιστών, smartphone και ενσωματωμένων συσκευών όπως εκτυπωτές και δρομολογητές.

Η πρόκληση των μεμονωμένων προϊόντων ασφαλείας τελικού σημείου είναι η δυσκολία της αποτελεσματικής διαχείρισης όλων. Τα τμήματα πληροφορικής συχνά παρακολουθούν λύσεις πολλαπλών τελικών σημείων. Αυτές οι μεμονωμένες εφαρμογές έχουν όλες διαφορετικές διεπαφές, απαιτώντας από τους υπαλλήλους να αλλάζουν μεταξύ οθονών, μειώνοντας την αποτελεσματικότητα.

Τα προϊόντα Siled point ενδέχεται επίσης να μην μπορούν να ανταλλάσσουν δεδομένα, γεγονός που σπαταλά την ευκαιρία για βαθύτερη ανάλυση θεμάτων ασφάλειας. Αυτό σημαίνει, ότι τα προϊόντα είναι λιγότερο αποτελεσματικά.

Μια πιο ολοκληρωμένη και κεντρική προσέγγιση για την ασφάλεια τελικού σημείου είναι μια πλατφόρμα προστασίας τελικού σημείου (**EPP**). Ένα **EPP** παρέχει πολλαπλές τεχνολογίες

ασφάλειας τελικών σημείων και δυνατότητες αποκατάστασης σε ένα μέρος.

Κεφάλαιο 5ο - Domain Controller (DC) ένας ελεγκτής δικτύου

5.1 Εισαγωγή στους Domain Controllers (DC) και οι κύριες λειτουργίες τους

Ένας **Domain Controller(DC)** είναι ένας τύπος **server,** που επεξεργάζεται αιτήματα γιαέλεγχο ταυτότητας από χρήστες εντός ενός **Domain** υπολογιστή. (44) (45) Οι **Domain Controllers (DC)** χρησιμοποιούνται πιο συχνά σε τομείς της υπηρεσίας καταλόγου **Active Directory (AD)** των Windows, αλλά χρησιμοποιούνται επίσης και με άλλους τύπους συστημάτων διαχείρισης ταυτότητας. Οι **Domain Controllers (DC)** αντιγράφουν πληροφορίες υπηρεσίας καταλόγου **Active Directory (AD)** για τους τομείς τους, συμπεριλαμβανομένων των χρηστών, των διαπιστευτηρίων ελέγχου ταυτότητας και των πολιτικών ασφάλειας της επιχείρησης.

Η βασική λειτουργία των **Domain Controllers (DC)**, είναι να περιορίζουν την πρόσβαση σε πόρους **Domain** επαληθεύοντας την ταυτότητα χρήστη μέσω διαπιστευτηρίων σύνδεσης και αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση σε αυτούς τους πόρους. Οι **Domain Controllers (DC)** εφαρμόζουν πολιτικές ασφαλείας σε αιτήματα πρόσβασης σε πόρους **Domain**. Για παράδειγμα, σε έναν **Domain Active Directory (AD)** των Windows, ο **Domain Controller (DC)** αντλεί πληροφορίες ελέγχου ταυτότητας για λογαριασμούς χρηστών από το **Active Directory (AD)**.

Ένας **Domain Controller (DC)** μπορεί να λειτουργήσει ως ένα ενιαίο σύστημα, αλλά συνήθως υλοποιείται σε συμπλέγματα για βελτιωμένη αξιοπιστία και διαθεσιμότητα. Για **Domain Controller (DC)** που εκτελούνται στα **Active Directories (AD)**των Windows, κάθε σύμπλεγμα περιλαμβάνει το**Primary Domain Controller (PDC)** και έναν ή περισσότερους **Backup Domain Controllers (BDC)**. Σε περιβάλλοντα όπως Unix και Linux, οι **Backup Domain Controllers (BDC)** αντιγράφουν βάσεις δεδομένων ελέγχου ταυτότητας από τον **Primary Domain Controller (PDC)**.

5.1.1 Εισαγωγή στα Active Directories (AD) και στις κύριες λειτουργίες τους

Το **Active Directory (AD)** είναι μια βάση δεδομένων και ένα σύνολο υπηρεσιών, που συνδέει τους χρήστες με τους πόρους δικτύου που χρειάζονται για να ολοκληρώσουν την εργασία τους.Η βάση δεδομένων (ή ο κατάλογος) περιέχει σημαντικές πληροφορίες σχετικά με το περιβάλλον, συμπεριλαμβανομένων των χρηστών και των υπολογιστών που υπάρχουν και ποιος επιτρέπεται να κάνει τι. (46) (47)

Για παράδειγμα, η βάση δεδομένων μπορεί να περιλαμβάνει 100 λογαριασμούς χρηστών με λεπτομέρειες όπως τον τίτλο εργασίας, τον αριθμό τηλεφώνου και τον κωδικό πρόσβασης κάθε ατόμου. Θα καταγράψει επίσης τις άδειες τους.Οι υπηρεσίες ελέγχουν μεγάλο μέρος της δραστηριότητας που διεξάγεται στο περιβάλλον πληροφορικής. Συγκεκριμένα διασφαλίζουν, ότι κάθε άτομο είναι αυτό που ισχυρίζεται ότι είναι (έλεγχος ταυτότητας), συνήθως ελέγχοντας το αναγνωριστικό χρήστη και τον κωδικό πρόσβασης που εισάγει και του επιτρέπουν να έχει πρόσβαση μόνο στα δεδομένα που επιτρέπεται να χρησιμοποιεί (εξουσιοδότηση).

5.1.1.1 Εισαγωγή στο Active Directory (AD) και στα πλεονεκτήματα του

Η υπηρεσία καταλόγου **Active Directory (AD)** απλοποιεί τη ζωή για τους διαχειριστές και τους τελικούς χρήστες, ενώ ενισχύει την ασφάλεια για τους οργανισμούς. Οι διαχειριστές απολαμβάνουν κεντρική διαχείριση χρηστών και δικαιωμάτων, καθώς και κεντρικό έλεγχο των διαμορφώσεων του υπολογιστή και των χρηστών μέσω της δυνατότητας πολιτικής ομάδας **AD**.

Οι χρήστες μπορούν να πραγματοποιήσουν έλεγχο ταυτότητας μια φορά και στη συνέχεια να έχουν πρόσβαση σε οποιουσδήποτε πόρους στο **Domain** για τον οποίο είναι εξουσιοδοτημένοι (με απλή σύνδεση). Επιπλέον, τα αρχεία αποθηκεύονται σε ένα κεντρικό αποθετήριο, όπου μπορούν να κοινοποιηθούν με άλλους χρήστες για διευκόλυνση της συνεργασίας και να δημιουργηθούν κατάλληλα αντίγραφα ασφαλείας από ομάδες **IT** για να διασφαλιστεί η επιχειρηματική συνέχεια.

5.1.1.2 Πως λειτουργεί ένας Active Directory (AD)

Η κύρια υπηρεσία των **Active Directory (AD)** είναι οι υπηρεσίες **Domain Active Directory Domain Services (ADDS)**, η οποία αποτελεί μέρος του λειτουργικού συστήματος Windows Server. Οι διακομιστές που εκτελούν το **Active Directory Domain Service (AD DS)** ονομάζονται **Domain Controllers (DC)**. Οι οργανισμοί έχουν συνήθως πολλαπλούς **Domain Controllers (DC)** και ο καθένας έχει ένα αντίγραφο του καταλόγου για ολόκληρο το **Domain**. Οι αλλαγές που πραγματοποιούνται στον κατάλογο ενός **Domain Controller (DC)**, όπως η ενημέρωση κωδικού πρόσβασης ή η διαγραφή ενός λογαριασμού χρήστη αντιγράφονται και στα άλλα **Domain Controllers (DC)**, ώστε να παραμένουν όλα ενημερωμένα. (46) (47)

Ένας διακομιστής Global Catalog είναι ένας **Domain Controller (DC)** που αποθηκεύει ένα πλήρες αντίγραφο όλων των αντικειμένων στον κατάλογο του **Domain** του και ένα μερικό αντίγραφο όλων των αντικειμένων όλων των άλλων τομέων στο σύμπλεγμα δομών. Αυτό επιτρέπει στους χρήστες και τις εφαρμογές να βρίσκουν αντικείμενα σε οποιοδήποτε **Domain** του δάσους τους. Επιτραπέζιοι υπολογιστές, φορητοί υπολογιστές και άλλες συσκευές με Windows (και όχι Windows Server) μπορούν να αποτελούν μέρος ενός περιβάλλοντος **Active Directory (AD)**, αλλά δεν εκτελούν το **Active Directory Domain Service (ADDS)**.

Το **Active Directory Domain Service (ADDS)** βασίζεται σε πολλά καθιερωμένα πρωτόκολλα και πρότυπα, συμπεριλαμβανομένων των **LDAP** (Lightweight Directory Access Protocol), **Kerberos** και **DNS** (Domain Name System).

5.1.1.3 Η δομή ενός Active Directory (AD)

Το **Active Directory (AD)** έχει τρεις κύριες βαθμίδες: περιοχές, δέντρα και δάση. Ένα **Domain** είναι μια ομάδα σχετικών χρηστών, υπολογιστών και άλλων αντικειμένων του **Active Directory (AD)**. Πολλοί τομείς μπορούν να συνδυαστούν σε ένα δέντρο και πολλά δέντρα μπορούν να ομαδοποιηθούν σε ένα δάσος. Ένα **Domain** είναι ένα όριο διαχείρισης.

Τα αντικείμενα για έναν δεδομένο **Domain** αποθηκεύονται σε μια ενιαία βάση δεδομένων και μπορούν να διαχειρίζονται σαν ολότητα. Ένα δάσος είναι ένα όριο ασφαλείας. Τα αντικείμενα σε διαφορετικά δάση δεν μπορούν να αλληλεπιδράσουν μεταξύ τους, εκτός εάν οι διαχειριστές κάθε δάσους δημιουργήσουν μια εμπιστοσύνη μεταξύ τους. Για παράδειγμα, εάν υπάρχουν πολλές μη συνδεδεμένες επιχειρηματικές μονάδες, πιθανότατα πρέπει να δημιουργηθούν πολλά δάση. (46) (47)

5.1.2 Ρύθμιση ενός Domain Controller (DC) σε Active Directory (AD)

Ο **Domain Controller (DC)** είναι μια λειτουργία της υπηρεσίας καταλόγου **Active Directory**

(AD) της Microsoft και οι **Domain Controllers (DC)** είναι διακομιστές που μπορούν να χρησιμοποιήσουν την υπηρεσία καταλόγου **Active Directory (AD)** για να ανταποκρίνονται σε αιτήματα ελέγχου ταυτότητας.

Δεν πρέπει οι οργανισμοί να στηρίζονται σε έναν μόνο **Domain Controller (DC)**, ακόμα και όταν πρόκειται για μικρούς οργανισμούς. Οι βέλτιστες πρακτικές απαιτούν έναν κύριο **Domain Controller (DC)** και τουλάχιστον έναν εφεδρικό **Domain Controller (DC)** για την αποφυγή διακοπής λειτουργίας λόγω μη διαθεσιμότητας του συστήματος.

Μια άλλη καλύτερη πρακτική είναι η ανάπτυξη κάθε **Domain Controller (DC)** σε έναν αυτόνομο φυσικό διακομιστή. Αυτό περιλαμβάνει **Virtual Domain Controllers (VDC)**, οι οποίοι θα πρέπει να εκτελούνται σε virtual machines (VM) που εκτελούνται σε διαφορετικούς φυσικούς κεντρικούς υπολογιστές. Οι **Domain Controllers (DC)** μπορούν να αναπτυχθούν σε φυσικούς διακομιστές, που εκτελούνται ως VMsor ως μέρος μιας υπηρεσίας καταλόγου cloud. Τα βήματα για τη ρύθμιση ενός **AD Domain Controller (DC)**περιλαμβάνουν:

- **Domain Assessment**. Το πρώτο βήμα για τη ρύθμιση ενός **Domain Controller (DC)** είναι να αξιολογηθεί το **Domain** στον οποίο θα ρυθμιστεί ο **Controller**. Αυτή η αξιολόγηση περιλαμβάνει τον προσδιορισμό των τύπων **Domain Controllers (DC)** που χρειάζονται, πού θα βρίσκονται και πώς θα συνδιάζεται η λειτουργία τους με τα υπάρχοντα συστήματα στο **Domain**.
- **Νέα ανάπτυξη ή προσθήκη**. Είτε σχεδιαστεί μια νέα ανάπτυξη **AD Domain Controllers (DC),** είτε προστεθεί ένας νέος **Controller** για ένα υπάρχον **Domain**, πρέπει να καθοριστεί η θέση του **Domain Controller (DC)** και οι πόροι που απαιτούνται για την εκτέλεση του κεντρικού **Domain Controller (DC)** και τυχόν **Domain Controller (DC)** σε εικονικό περιβάλλον.
- **Ασφάλεια βάσει σχεδίου**. Είναι επιτακτική ανάγκη να προστατευτεί ένας **Domain Controller (DC)** από εσωτερικές ή εξωτερικές επιθέσεις. Επίσης, πρέπει να σχεδιαστεί η αρχιτεκτονική του **Domain Controller (DC)**, ώστε να είναι ασφαλής από διακοπές της υπηρεσίας λόγω απώλειας συνδεσιμότητας, απώλειας ισχύος ή αστοχιών συστήματος.

Οι προδιαγραφές για τη ρύθμιση των **AD Domain Controller (DC)** ποικίλλουν ανάλογα με την έκδοση του Windows Server που χρησιμοποιείται στο **Domain**.

5.2 Σημαντικότητα των Domain Controllers (DC) στα σύγχρονα συστήματα

Οι **Domain Controllers (DC)**ελέγχουν όλη την πρόσβαση στον **Domain**, αποκλείοντας τη μη εξουσιοδοτημένη πρόσβαση σε δίκτυα **Domain**, ενώ επιτρέπουν στους χρήστες πρόσβαση σε όλες τις εξουσιοδοτημένες υπηρεσίες καταλόγου.Ο **Domain Controller (DC)** ελέγχει όλη την πρόσβαση στο δίκτυο, επομένως είναι σημαντικό να προστατεύεται με πρόσθετους μηχανισμούς ασφαλείας όπως:

- Τείχη προστασίας (Firewalls): Το τείχος προστασίας είναι μια συσκευή ασφαλείας δικτύου, που αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο.
- Ασφαλή και απομονωμένα δίκτυα.
- Πρωτόκολλα ασφαλείας και κρυπτογράφηση για την προστασία των αποθηκευμένων δεδομένων.
- Περιορισμένη χρήση μη ασφαλών πρωτοκόλλων, όπως πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (**Remote Desktop Protocol RDP**), σε controllers. Το **Remote Desktop Protocol (RDP)** είναι ένα ασφαλές πρωτόκολλο επικοινωνίας δικτύου.
- Ανάπτυξη σε μια φυσικά περιορισμένη τοποθεσία για ασφάλεια.
- Ταχεία διαχείριση ενημερώσεων κώδικα και διαμόρφωσης.

- Αποκλεισμός της πρόσβασης στο Διαδίκτυο για Domain Controller (DC).

Οι **Domain Controllers (DC)** ελέγχουν όλη την πρόσβαση σε υπολογιστικούς πόρους σε έναν οργανισμό, επομένως πρέπει να είναι σχεδιασμένοι για να αντιστέκονται σε επιθέσεις και να συνεχίζουν να λειτουργούν υπό αντίξοες συνθήκες.

5.3 Διάφορες επιλογές υλοποίησης του Domain Controller (DC) στα σύγχρονα συστήματα

Οι ακόλουθες επιλογές είναι διαθέσιμες κατά τη ρύθμιση ενός **Domain Controller (DC)** με **Active Directory (AD)**:

- **Domain Name System (DNS) server:**

Το **Domain Name System (DNS)** είναι ο τηλεφωνικός κατάλογος του Διαδικτύου. Όταν οι χρήστες πληκτρολογούν ονόματα **Domain** όπως «google.com» ή «nytimes.com» σε προγράμματα περιήγησης ιστού, το **DNS** είναι υπεύθυνο για την εύρεση της σωστής διεύθυνσης **IP** για αυτούς τους ιστότοπους. Στη συνέχεια, τα προγράμματα περιήγησης χρησιμοποιούν αυτές τις διευθύνσεις για να επικοινωνούν με διακομιστές προέλευσης ή διακομιστές CDN edge για πρόσβαση σε πληροφορίες ιστότοπου.

Όλα αυτά συμβαίνουν χάρη στους **DNS servers,** δηλαδή μηχανήματα αφιερωμένα στην απάντηση ερωτημάτων **DNS**. Η λειτουργία του **Domain Name System (DNS)** είναι:

Σε ένα τυπικό ερώτημα DNS χωρίς καμία προσωρινή αποθήκευση, υπάρχουν τέσσερις **servers** που συνεργάζονται για να παραδώσουν μια διεύθυνση **IP** στον πελάτη: αναδρομικοί επιλύτες, διακομιστές ονομάτων ρίζας, διακομιστές ονομάτων TLD και έγκυροι διακομιστές ονομάτων.

Ο αναδρομέας **DNS** (αναφέρεται επίσης ως ο αναλυτής **DNS**) είναι ένας **server** που λαμβάνει το ερώτημα από τον πελάτη **DNS** και στη συνέχεια αλληλεπιδρά με άλλους **servers DNS** για να εντοπίσει τη σωστή **IP**. Μόλις ο επιλύτης λάβει το αίτημα από τον πελάτη, το πρόγραμμα επίλυσης στη συνέχεια συμπεριφέρεται ως πελάτης ο ίδιος, ερωτώντας τους άλλους τρεις τύπους **DNS servers** αναζητώντας τη σωστή **IP**.

1. Πρώτα ο επιλύτης υποβάλλει ερώτημα στον **server** ονομάτων ρίζας. Ο ριζικός **server** είναι το πρώτο βήμα για τη μετάφραση ονομάτων **Domain** αναγνώσιμων από τον άνθρωπο σε διευθύνσεις **IP**. Στη συνέχεια, ο ριζικός **server** αποκρίνεται στον επιλύτη με τη διεύθυνση ενός **DNS server** ανώτατου επιπέδου (**TLD**) (όπως .com ή .net) που αποθηκεύει τις πληροφορίες για τα **Domain** του.
2. Στη συνέχεια, ο αναλυτής θέτει ερωτήματα στον **server TLD**. Ο **server TLD** αποκρίνεται με τη διεύθυνση **IP** του έγκυρου **server** ονομάτων του **Domain**. Στη συνέχεια, ο αναδρομέας ρωτά τον έγκυρο **server** ονομάτων, ο οποίος θα απαντήσει με τη διεύθυνση **IP** του **server** προέλευσης.
3. Το πρόγραμμα επίλυσης θα μεταβιβάσει τελικά τη διεύθυνση **IP** του **server** προέλευσης στον πελάτη. Χρησιμοποιώντας αυτήν τη διεύθυνση **IP**, ο πελάτης μπορεί στη συνέχεια να ξεκινήσει ένα ερώτημα απευθείας στον **server** προέλευσης και ο **server** προέλευσης θα απαντήσει στέλνοντας δεδομένα ιστότοπου,που μπορούν να ερμηνευτούν και να εμφανιστούν από το πρόγραμμα περιήγησης ιστού.

Ο **Domain Controller (DC)** μπορεί να ρυθμιστεί ώστε να λειτουργεί ως διακομιστής **DNS**.

- **Δυνατότητες καθολικού καταλόγου**: Ο **Domain Controller (DC)** μπορεί να ρυθμιστεί

ώστε να χρησιμοποιεί τον καθολικό κατάλογο, ο οποίος επιτρέπει στον **Controller** να επιστρέφει πληροφορίες **Active Directory (AD)** για οποιοδήποτε αντικείμενο στον οργανισμό, ανεξάρτητα από το αν το αντικείμενο βρίσκεται στον ίδιο **Domain** με το **Domain Controller (DC)**. Αυτό είναι χρήσιμο για μεγάλες επιχειρήσεις με πολλά **AD Domain**.

- **Domain Controller (DC) μόνο για ανάγνωση (RODC)**: Οι **Domain Controllers (DC)**που χρησιμοποιούνται σε υποκαταστήματα ή σε άλλες περιπτώσεις όπου η συνδεσιμότητα δικτύου είναι περιορισμένη, μπορούν να διαμορφωθούν ως μόνο για ανάγνωση.
- **Directory Services Restore Mode (DSRM)**: Το **Directory Services Restore Mode (DSRM)** παρέχει την επιλογή να γίνει έκτακτη συντήρηση, συμπεριλαμβανομένης της επαναφοράς αντιγράφων ασφαλείας, στον **Domain Controller (DC)**. Ένας κωδικός πρόσβασης **Directory Services Restore Mode (DSRM)** πρέπει να διαμορφωθεί εκ των προτέρων.

5.4 Πλεονεκτήματα και περιορισμοί των Domain Controllers (DC)

Τα οφέλη του **Domain Controller (DC)** περιλαμβάνουν:

- Η κεντρική διαχείριση των **Domain Controllers (DC)** επιτρέπει στους οργανισμούς να ελέγχουν την ταυτότητα όλων των αιτημάτων υπηρεσιών καταλόγου, χρησιμοποιώντας έναν κεντρικό **Domain Controller (DC)**.
- Οι διανεμημένοι και αναπαραγόμενοι **Domain Controllers (DC)** επιβάλλουν πολιτικές ασφαλείας και αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση σε εταιρικά δίκτυα και WAN.
- Η πρόσβαση σε διακομιστές αρχείων και άλλους πόρους δικτύου μέσω των **Domain Controllers (DC)** παρέχει απρόσκοπτη ενοποίηση με υπηρεσίες καταλόγου όπως το **Active Directory (AD)** της **Microsoft**.
- Η υποστήριξη για ασφαλή πρωτόκολλα ελέγχου ταυτότητας και μεταφοράς σε **Domain Controllers (DC)** βελτιώνει την ασφάλεια της διαδικασίας ελέγχου ταυτότητας.

Ορισμένοι περιορισμοί του **Domain Controller (DC)** περιλαμβάνουν:

- Ένα μόνο σημείο αποτυχίας για τον έλεγχο τομέα δικτύου.
- Επειδή ελέγχουν την πρόσβαση σε ολόκληρο το δίκτυο, οι **Domain Controllers (DC)** είναι στόχος κυβερνοεπιθέσεων. Η επιτυχής παραβίαση ενός **Domain Controller (DC)** θα μπορούσε, να δώσει στον εισβολέα πρόσβαση σε όλους τους πόρους δικτύου τομέα καθώς και σε διαπιστευτήρια ελέγχου ταυτότητας για όλους τους χρήστες στο **Domain**.
- Τα δίκτυα που χρησιμοποιούν οι **Domain Controllers (DC)** για έλεγχο ταυτότητας και ασφάλεια πρόσβασης εξαρτώνται από αυτά. Για να μειωθεί ο κίνδυνος διακοπής λειτουργίας, οι **Domain Controllers (DC)** μπορούν να αναπτυχθούν σε διάφορες ομάδες.
- Οι **Domain Controllers (DC)** απαιτούν πρόσθετη υποδομή και μηχανισμούς ασφαλείας.

Πλεονεκτήματα	Μειωνεκτήματα
Κεντρική διαχείριση για έλεγχο πρόσβασης	Μεμονωμένο σημείο αποτυχίας για τον έλεγχο δικτύου
Κατανομή και αναπαραγωγή	Στόχος για κυβερνοεπιθέσεις
Ελέγχει την πρόσβαση σε πόρους δικτύων και σε server αρχείων	Η διακοπή λειτουργίας μπορεί να προκαλέσει καταστροφικές αποτυχίες πρόσβασης

Υποστηρίζει ασφαλή έλεγχο ταυτότητας και εξουσιοδότηση	Απαιτεί πρόσθετουςς υπολογιστικούς πόρους

Σχήμα 5.1 Πλεονεκτήματα και Μειονεκτήματα ενός Domain Controller

Οι **Domain Controllers (DC)** είναι θεμελιώδη στοιχεία για την εξασφάλιση μη εξουσιοδοτημένης πρόσβασης στα **Domain** ενός οργανισμού.

Κεφάλαιο 6ο – Πειραματικό μέρος

Αφού καλύψαμε το θεωρητικό υπόβαθρο που είναι απαραίτητο και κατανοήσαμε διάφορες σημαντικές έννοιες, όπως τι είναι ένα σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**), Anti-Virus (**AV**), πλατφόρμα προστασίας τελικού σημείου (**EPP**) και **Domain Controller (DC)**, ας περάσουμε στην πράξη να δούμε πως πραγματικά δουλεύουν και να κατανοήσουμε καλύτερα πόσο σημαντικά είναι για την ιδιωτικότητα των χρηστών.

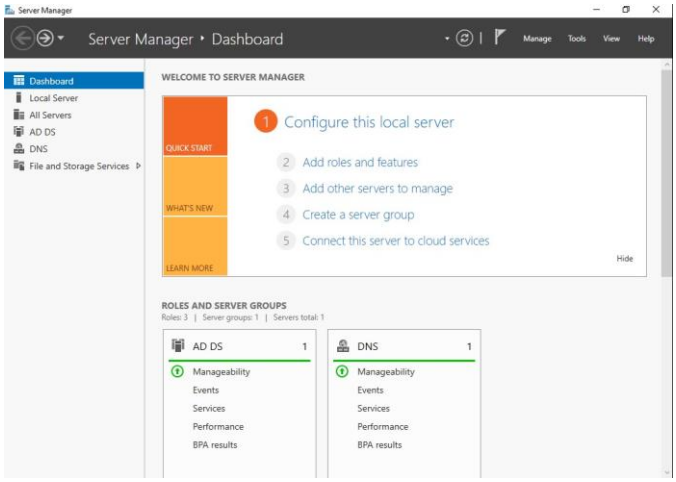
6.1 Τι θα χρειαστούμε για το πειραματικό μέρος μας

Θα χρειαστούμε να στήσουμε ένα τοπικό δίκτυο, στο οποίο θα υπάρχουν δυο τελικά σημεία με λειτουργικά συστήματα Windows 10 και Windows 11 αντίστοιχα. Σε αυτά τα λειτουργικά συστήματα θα εγκαταστήσουμε κάποια συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) ανοιχτού κώδικα. Θα εγκαταστήσουμε τα ανοιχτού κώδικα συστήματα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) **Wazuh**, **Bluespawn** και **OpenEDR**.

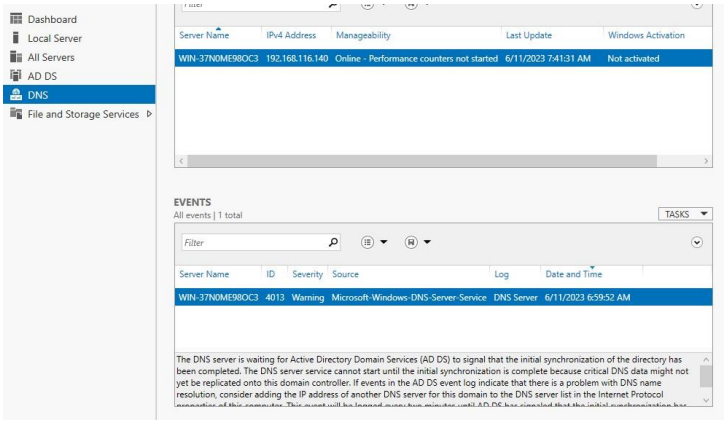
Τέλος στο τοπικό δίκτυο μας θα χρειαστούμε έναν **Domain Controller (DC)**, το οποίο θα έχει το ρόλο του **Administrator** στα τελικά σημεία μας. Για να είμαστε σωστοί πρέπει στον **Domain Controller (DC)** να ρυθμίσουμε τον ενεργό κατάλογο μας ή αλλιώς **Active Directory (AD)**, που έχει όλα τα στοιχεία για τα τελικά σημεία που βρίσκονται στο τοπικό δίκτυο, καθώς και τον DNS server για να μπορέσουν τα τελικά σημεία να έχουν πρόσβαση στο διαδίκτυο.

6.1.1 Windows Server 2016

Για το πειραματικό μέρος αυτής της διπλωματικής πρέπει να χρησιμοποιήσουμε ένα λειτουργικό σύστημα, το οποίο θα χρησιμοποιήσουμε για **Domain Controller (DC)**. Το λειτουργικό σύστημα που θα χρησιμοποιήσουμε είναι το λειτουργικό **Windows Server 2016** που έχει όλες τις δυνατότητες για να γίνει Domain Controller (DC). (48) (49)



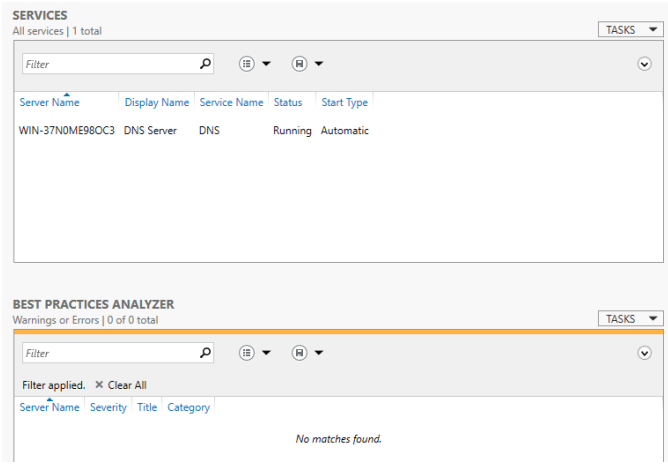
Σχήμα 6.1 Windows Server 2016



Σχήμα 6.2 Configure DNS Server

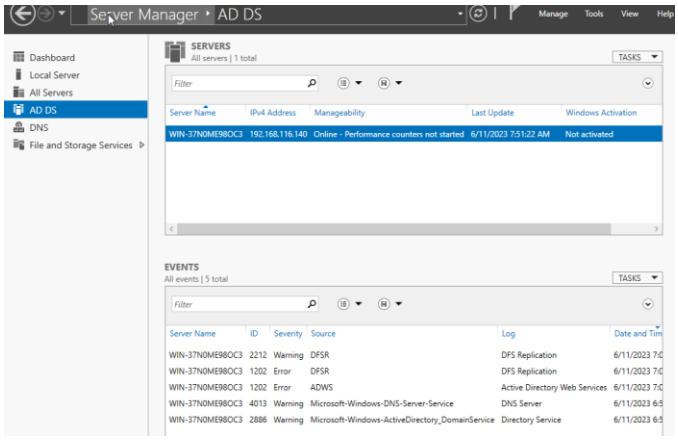
Με το που ανοίξουμε το λειτουργικό σύστημα μας εμφανίζεται το **Dashboard** με όλους τους **servers** που θα χρειαστούμε. Στη συνέχεια θα ρυθμίσουμε το **Active Directory (AD)**, τον **Domain Name System (DNS) server** και τους χρήστες που θα υπάρχουν στον **Domain Controller (DC)**.

Εδώ παρατηρούμε τον **Domain Name System (DNS) server** (50) που μόλις ρυθμίσαμε και βλέπουμε το όνομα του καθώς και την **IP** του. Πιο κάτω μπορούμε να δούμε και τα **Events**. Αν συνεχίσουμε λίγο πιο κάτω θα δούμε και τα **Services** που τρέχουν στον **server**.



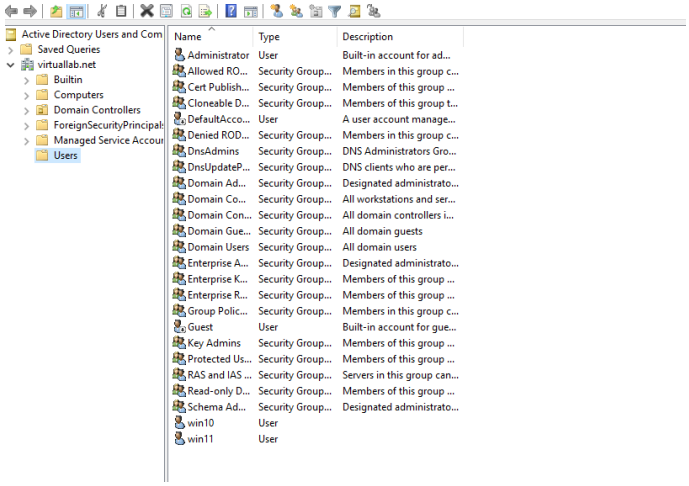
Σχήμα 6.3 Λεπτομέρειες του DNS Server

Έχουμε ρυθμίσει και τον **Active Directory (AD)**. Όπως είδαμε και στον **Domain Name System (DNS) server** βλέπουμε και εδώ το όνομα καθώς και την **IP** του. Πιο κάτω βλέπουμε και τα **Events** όπως και τα **Services**.



Σχήμα 6.4 Configure Active Directory

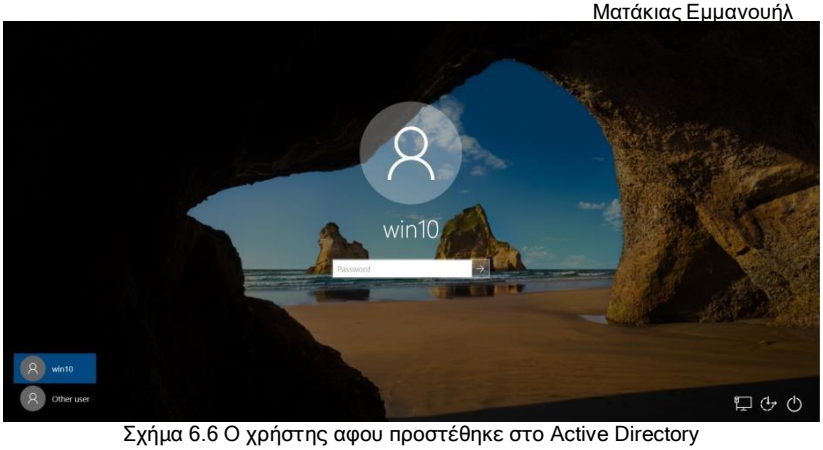
Για την υλοποίηση αυτής της διπλωματικής θα χρειαστεί να προσθέσουμε δυο χρήστες, όσα δηλαδή είναι και τα τελικά μας σημεία που θα χρησιμοποιήσουμε στα πλαίσια αυτής της διπλωματικής.Εκτός από τον χρήστη **Administrator** θα υπάρχει και ένας χρήστης που είναι



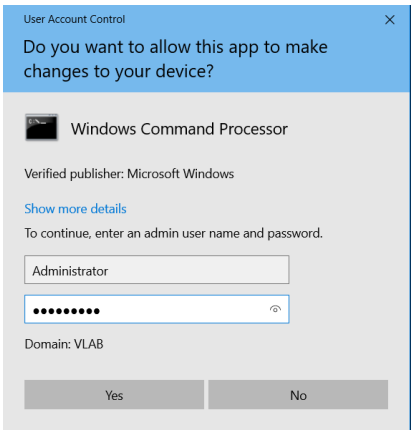
υπολογιστής που έχει **Windows 10** (έχει όνομα win10)και ένας υπολογιστής που έχει **Windows 11** (έχει όνομα win11).

Σχήμα 6.5 Πρόσθεση χρηστών σε Active Directory

Κάθε χρήστης έχει το όνομα του και έναν κωδικό που ρυθμίσαμε παραπάνω. Κάθε φορά που θέλουμε να κάνουμε κάτι σε αυτούς τους χρήστες θα μας ζητήσει τα **credentials** του χρήστη **Administrator**. Ως παράδειγμα θα δείξουμε τον χρήστη **win10**.



Σχήμα 6.6 Ο χρήστης αφου προστέθηκε στο Active Directory



Σχήμα 6.7 Κάθε κίνηση ζητάει credentials του Administrator

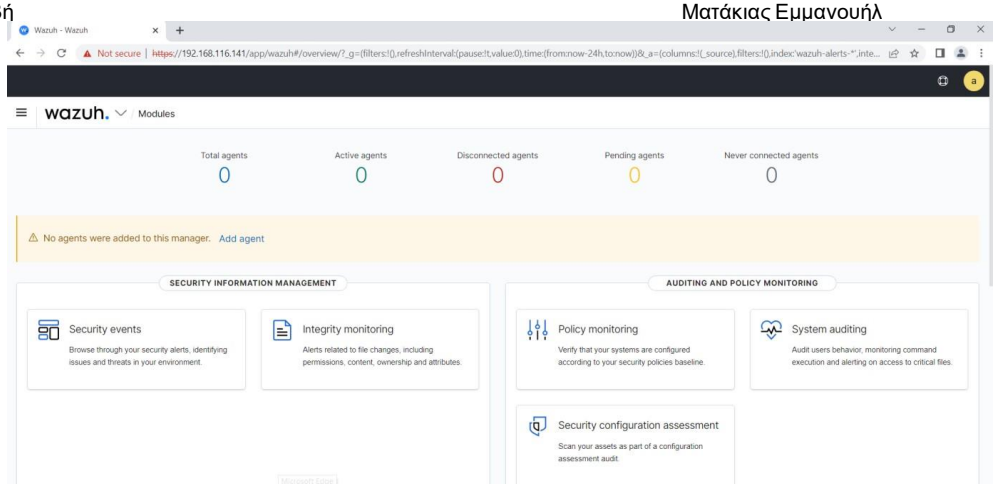
6.2 Εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (EDR), Wazuh

6.2.1 Τι είναι το εργαλείο Wazuh

Το εργαλείο **Wazuh** είναι μια δωρεάν πλατφόρμα ανοιχτού κώδικα που έχει ως σκοπό την ανίχνευση και απόκριση σε τελικά σημεία. Είναι ένα σύστημα ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) και χρησιμοποιείται με σκοπό την πρόληψη, τον εντοπισμό και την απόκριση απειλών σε ένα υπολογιστικό σύστημα.

Προστατεύει την εργασία που γίνεται σε περιβάλλοντα εσωτερικής εγκατάστασης, σε εικονικά μηχανήματα, κοντέινερ και περιβάλλοντα που βασίζονται σε υπηρεσίες Cloud. Η λύση **Wazuh** αποτελείται από έναν παράγοντα ασφάλειας τελικού σημείου, που αναπτύσσεται στα συστήματα παρακολούθησης, και έναν διακομιστή διαχείρισης, ο οποίος συλλέγει και αναλύει δεδομένα που συλλέγονται από τους agents. (51) (52)

Επιπλέον, το Wazuh έχει ενσωματωθεί πλήρως με το Elastic Stack, παρέχοντας μια μηχανή αναζήτησης και ένα εργαλείο οπτικοποίησης δεδομένων που επιτρέπει στους χρήστες να πλοηγούνται στις ειδοποιήσεις ασφαλείας τους.



Σχήμα 6.8 Front-end του Wazuh

Το **Wazuh** έχει μια κεντρική αρχιτεκτονική πολλαπλών πλατφορμών που επιτρέπει την εύκολη παρακολούθηση και διαχείριση πολλαπλών συστημάτων ταυτόχρονα. Παρέχει μια λύση ασφαλείας ικανή να παρακολουθεί υποδομές, να ανιχνεύει απειλές, απόπειρες εισβολής, ανωμαλίες συστήματος, κακώς διαμορφωμένες εφαρμογές και μη εξουσιοδοτημένες ενέργειες χρήστη. Παρέχει επίσης ένα πλαίσιο για την αντιμετώπιση περιστατικών και τη συμμόρφωση με τους κανονισμούς.

Το εργαλείο **Wazuh** ιδρύθηκε το 2015 από τον Santiago Basset ως fork του OSSEC. Έχει έδρα στο Silicon Valley της Καλιφόρνια, αν και έχει παγκόσμια παρουσία με μια ομάδα παραπάνω από 100 άτομα και διανέμεται στις Ηνωμένες Πολιτείες, την Ισπανία και την Αργεντινή.

6.2.2 Software Components

Το εργαλείο **Wazuh** αποτελείται από τρία κύρια στοιχεία: τον **agent** που εγκαθίσταται στο τελικό σημείο, τον **διακομιστή** που γίνεται η ανάλυση των δεδομένων και τον **manager**, ο οποίος βλέπει όλα τα δεδομένα μέσω της οπτικοποίησης.

- **Wazuh agent**

Έχει σχεδιαστεί για να εκτελεί μια σειρά εργασιών στο τελικό σημείο, με στόχο τον εντοπισμό απειλών και, όταν είναι απαραίτητο, να ενεργοποιεί αυτόματες αποκρίσεις.

Μπορεί να τρέξει σε πολλές διαφορετικές πλατφόρμες, συμπεριλαμβανομένων των Windows, Linux, Mac OS X, AIX, Solaris και HP-UX. Οι **Wazuh agent** μπορούν να ρυθμιστούν και να διαχειρίζονται από τον διακομιστή **Wazuh**.

- **Wazuh server**

Ο **διακομιστής** είναι υπεύθυνος για την ανάλυση των δεδομένων που λαμβάνονται από τους **agents** που είναι εγκατεστημένοι στα τελικά σημεία, την επεξεργασία συμβάντων μέσω αποκωδικοποιητών και κανόνων και τη χρήση πληροφοριών απειλών για την αναζήτηση γνωστών IOC (Indicators Of Compromise).

Ένας μεμονωμένος διακομιστής **Wazuh** μπορεί να αναλύσει δεδομένα από εκατοντάδες ή χιλιάδες **agents** και να κλιμακωθεί οριζόντια όταν ρυθμιστεί σε λειτουργία συμπλέγματος.

- **Wazuh manager**

Οι ειδοποιήσεις που δημιουργούνται από το **Wazuh agent** αποστέλλονται στο **manager**, όπου τοποθετούνται σ'ένα ευρετήριο και αποθηκεύονται. Ο Wazuh manager παρέχει μια ισχυρή διεπαφή χρήστη για οπτικοποίηση και ανάλυση δεδομένων, η οποία μπορεί επίσης να χρησιμοποιηθεί για τη διαχείριση και την παρακολούθηση της διαμόρφωσης και της κατάστασης των **agents**.

6.2.3 Δυνατότητες του εργαλείου Wazuh

Μια σύντομη παρουσίαση ορισμένων από τις πιο κοινές περιπτώσεις χρήσης της λύσης του εργαλείου ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) Wazuh.

- Ανίχνευση εισβολής

Οι **Wazuh agents** σαρώνουν τα συστήματα που παρακολουθούν αναζητώντας κακόβουλο λογισμικό, rootkits και ύποπτες ανωμαλίες. Μπορούν να ανιχνεύσουν κρυφά αρχεία, διεργασίες με απόκρυψη ή μη καταχωρημένους ακροατές δικτύου, καθώς και ασυνέπειες στις αποκρίσεις κλήσεων συστήματος.

Εκτός από τις δυνατότητες του **agent**, ο **διακομιστής** χρησιμοποιεί μια προσέγγιση που βασίζεται στην υπογραφή για την ανίχνευση εισβολής, χρησιμοποιώντας τη μηχανή κανονικής έκφρασης για να αναλύσει συλλεγμένα δεδομένα καταγραφής και να αναζητήσει δείκτες συμβιβασμού.

- Ανάλυση δεδομένων καταγραφής

Οι **Wazuh agents** έχουν την δυνατότητα να διαβάζουν τα αρχεία καταγραφής του λειτουργικού συστήματος και των εφαρμογών και να τα προωθούν με ασφάλεια σε έναν κεντρικό διαχειριστή για ανάλυση. Έτσι τα αποτελέσματα τα αποθηκεύει βάσει κανόνων. Όταν δεν έχει αναπτυχθεί κανένας παράγοντας, ο **διακομιστής** μπορεί επίσης να λαμβάνει δεδομένα μέσω συστήματος καταγραφής από συσκευές ή εφαρμογές δικτύου.

Οι κανόνες του εργαλείου ανίχνευσης και απόκρισης τελικού σημείου (**EDR**) **Wazuh**, βοηθούν την έγκυρη ενημέρωση για σφάλματα εφαρμογής ή συστήματος, εσφαλμένες ρυθμίσεις παραμέτρων, απόπειρες και επιτυχείς κακόβουλες δραστηριότητες, παραβιάσεις πολιτικής και μια ποικιλία άλλων ζητημάτων ασφάλειας και λειτουργίας.

- Παρακολούθηση ακεραιότητας αρχείων

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**) **Wazuh** έχει τη δυνατότητα να παρακολουθεί το σύστημα αρχείων, εντοπίζοντας αλλαγές στο περιεχόμενο, τα δικαιώματα, την ιδιοκτησία και τα χαρακτηριστικά των αρχείων που πρέπει να παρακολουθεί ο χρήστης του υπολογιστικού συστήματος.

Επιπλέον, προσδιορίζει εγγενώς τους χρήστες και τις εφαρμογές που χρησιμοποιούνται για τη δημιουργία ή την τροποποίηση αρχείων. Οι δυνατότητες παρακολούθησης ακεραιότητας αρχείων μπορούν να χρησιμοποιηθούν σε συνδυασμό με τη νοημοσύνη απειλών, για τον εντοπισμό απειλών ή κεντρικών υπολογιστών που έχουν παραβιαστεί. Επιπλέον, πολλά πρότυπα συμμόρφωσης με τους κανονισμούς, όπως το PCI DSS, το απαιτούν.

- Ανίχνευση ευπάθειας

Οι **Wazuh agents** έχουν τη δυνατότητα να αντλούν δεδομένα αποθέματος λογισμικού και να στέλνουν αυτές τις πληροφορίες στον **διακομιστή**, όπου σχετίζονται με βάσεις δεδομένων CVE (Common Vulnerabilities and Exposure) που ενημερώνονται συνεχώς,

προκειμένου να εντοπίσουν γνωστά ευάλωτα λογισμικά.

Η αυτοματοποιημένη αξιολόγηση ευπάθειας βοηθά το χρήστη να βρει τα αδύνατα σημεία στα κρίσιμα στοιχεία του υπολογιστικού συστήματος και ο χρήστης να προβεί σε διορθωτικές ενέργειες προτού οι εισβολείς τα εκμεταλλευτούν με σκοπό να υπονομεύσουν την τυχόν επιχείρησή ή να κλέψουν εμπιστευτικά δεδομένα.

- **Αξιολόγηση διαμόρφωσης**

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** έχει τη δυνατότητα να παρακολουθεί τις ρυθμίσεις διαμόρφωσης του συστήματος και των εφαρμογών, με σκοπό να διασφαλίσει ότι συμμορφώνονται με τις πολιτικές ασφαλείας, τα πρότυπα και τους οδηγούς συμμόρφωσης.

Οι **agents** εκτελούν περιοδικές σαρώσεις για να ανιχνεύσουν εφαρμογές που είναι γνωστό ότι είναι ευάλωτες, δεν έχουν επιδιορθωθεί ή δεν έχουν ρυθμιστεί με ασφάλεια.

Επιπλέον, οι έλεγχοι διαμόρφωσης μπορούν να προσαρμοστούν, προσαρμόζοντάς τους έτσι ώστε να ευθυγραμμίζονται σωστά με τον οργανισμό ή την επιχείρηση. Οι ειδοποιήσεις περιλαμβάνουν συστάσεις για καλύτερη διαμόρφωση, αναφορές και χαρτογράφηση με κανονιστική συμμόρφωση.

- **Απόκριση περιστατικού**

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** παρέχει εκ των υστέρων ενεργές αποκρίσεις για να εκτελέσει διάφορα αντίμετρα για την αντιμετώπιση ενεργών απειλών, όπως τον αποκλεισμό πρόσβασης σε ένα σύστημα από την πηγή απειλής όταν πληρούνται ορισμένα κριτήρια.

Επιπλέον, το εργαλείο ανίχνευσης και απόκρισης (**EDR**), **Wazuh** μπορεί να χρησιμοποιηθεί για την απομακρυσμένη εκτέλεση εντολών ή ερωτημάτων συστήματος, εντοπίζοντας δείκτες συμβιβασμού (**IOC**) και βοηθώντας στην εκτέλεση άλλων εργασιών ζωντανής εγκληματολογίας ή απόκρισης συμβάντων.

- **Κανονιστική Συμμόρφωση**

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** παρέχει μερικούς από τους απαραίτητους ελέγχους ασφαλείας για να γίνει συμβατός με τα πρότυπα και τους κανονισμούς της βιομηχανίας. Αυτά τα χαρακτηριστικά, σε συνδυασμό με την επεκτασιμότητα και την υποστήριξη πολλαπλών πλατφορμών βοηθούν τους οργανισμούς να ανταποκριθούν στις απαιτήσεις τεχνικής συμμόρφωσης.

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** χρησιμοποιείται ευρέως από εταιρείες διεκπεραίωσης πληρωμών και χρηματοπιστωτικά ιδρύματα για την κάλυψη των απαιτήσεων PCI DSS (Payment Card Industry Data Security Standard). Η διεπαφή χρήστη ιστού του παρέχει αναφορές και πίνακες εργαλείων που μπορούν να βοηθήσουν με αυτόν και άλλους κανονισμούς (π.χ. GPG13 ή GDPR).

- **Ασφάλεια στο cloud**

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** βοηθά στην παρακολούθηση της υποδομής σε υπηρεσίες cloud σε επίπεδο API, χρησιμοποιώντας μονάδες ενσωμάτωσης που είναι σε θέση να αντλούν δεδομένα ασφαλείας από γνωστούς παρόχους

cloud, όπως το Amazon AWS, το Azure ή το Google Cloud.

Επιπλέον, το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** παρέχει κανόνες για την αξιολόγηση της διαμόρφωσης του περιβάλλοντος cloud, εντοπίζοντας εύκολα τις αδυναμίες. Επιπλέον, οι **agents** χρησιμοποιούνται συνήθως για την παρακολούθηση περιβαλλόντων cloud σε επίπεδο παρουσίας.

- Ασφάλεια κοντέινερ

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** παρέχει ορατότητα ασφάλειας στους κεντρικούς υπολογιστές και τα κοντέινερ του **Docker**, παρακολουθώντας τη συμπεριφορά τους και εντοπίζοντας απειλές, τρωτά σημεία και ανωμαλίες.

Ο **Wazuh agent** έχει εγγενή ενοποίηση με τη μηχανή **Docker,** που επιτρέπει στους χρήστες να παρακολουθούν εικόνες, τόμους, ρυθμίσεις δικτύου και κοντέινερ που τρέχουν.

Το εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh** συλλέγει και αναλύει συνεχώς λεπτομερείς πληροφορίες χρόνου εκτέλεσης. Για παράδειγμα, ειδοποίηση για κοντέινερ που εκτελούνται σε προνομιακή λειτουργία, ευάλωτες εφαρμογές, κέλυφος που εκτελείται σε κοντέινερ, αλλαγές σε μόνιμους τόμους ή εικόνες και άλλες πιθανές απειλές.

Το εργαλείο **Wazuh** εκτός από τις ειδοποιήσεις που μας παρέχει, είναι ικανό για την προστασία από διάφορες απειλές. Τέτοιες είναι:

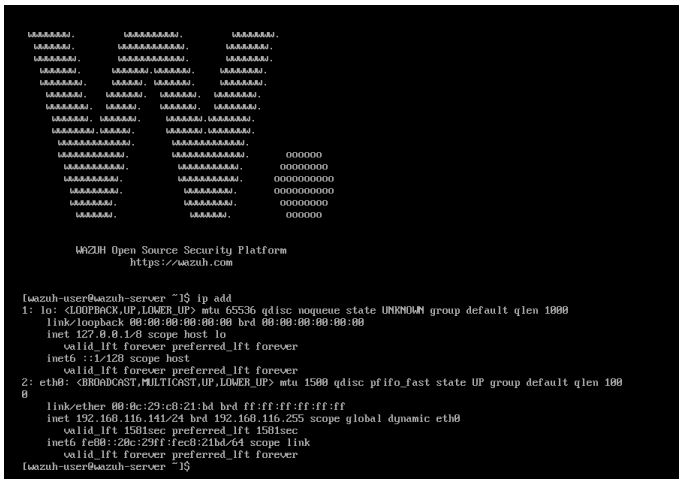
- Το **Wazuh** έρχεται με τη μονάδα **MITRE ATT&CK** που αντιστοιχίζει τα ανιχνευμένα συμβάντα στις διαφορετικές τακτικές και τεχνικές του αντιπάλου για πληροφορίες σχετικά με τα συμφραζόμενα. Επίσης, απορροφά δεδομένα πληροφοριών απειλών τρίτων για να επεκτείνει τις δυνατότητές του για κυνήγι απειλών και επιτρέπει τη δημιουργία προσαρμοσμένων ερωτημάτων με σκοπό το φιλτράρισμα συμβάντων και τη βοήθεια στη διερεύνηση συμβάντων.
- Οι δυνατότητες ανάλυσης συμπεριφοράς Wazuh περιλαμβάνουν τη χρήση προηγμένων αναλυτικών στοιχείων για τον εντοπισμό αποκλίσεων από την κανονική συμπεριφορά, που μπορεί να υποδηλώνουν πιθανές απειλές για την ασφάλεια. Αυτές οι δυνατότητες περιλαμβάνουν την παρακολούθηση της ακεραιότητας του αρχείου, την κίνηση δικτύου, τη συμπεριφορά των χρηστών και ανωμαλίες στις μετρήσεις απόδοσης του συστήματος.
- Το Wazuh ανταποκρίνεται αυτόματα σε απειλές για να μετριάσει τις πιθανές επιπτώσεις στην υποδομή. Είναι δυνατή η χρησιμοποίηση των ενσωματωμένων ενεργειών απόκρισης ή να δημιουργηθούν προσαρμοσμένες ενέργειες σύμφωνα με το σχέδιο απόκρισης συμβάντων.
- Το Wazuh είναι ενσωματωμένο με υπηρεσίες cloud για συλλογή και ανάλυση τηλεμετρίας. Προστατεύει εγγενή και υβριδικά περιβάλλοντα cloud, συμπεριλαμβανομένης της υποδομής κοντέινερ, εντοπίζοντας και ανταποκρινόμενη σε τρέχουσες και αναδυόμενες απειλές.
- Το Wazuh ενσωματώνει τροφοδοσίες ευφυΐας απειλών για τον εντοπισμό και την απόκριση σε γνωστές απειλές. Ενσωματώνεται με πηγές πληροφοριών απειλών, συμπεριλαμβανομένων πληροφοριών ανοικτού κώδικα (OSINT), εμπορικών ροών και δεδομένων που συνεισφέρουν οι χρήστες για να παρέχει ενημερωμένες πληροφορίες για πιθανές απειλές.

6.2.4 Configuration

Στα πλαίσια αυτής της διπλωματικής θα εγκαταστήσουμε το σύστημα ανίχνευσης και απόκρισης (**EDR**), **Wazuh** στο χρήστη **win10** με το λειτουργικό σύστημα **Windows 10**.

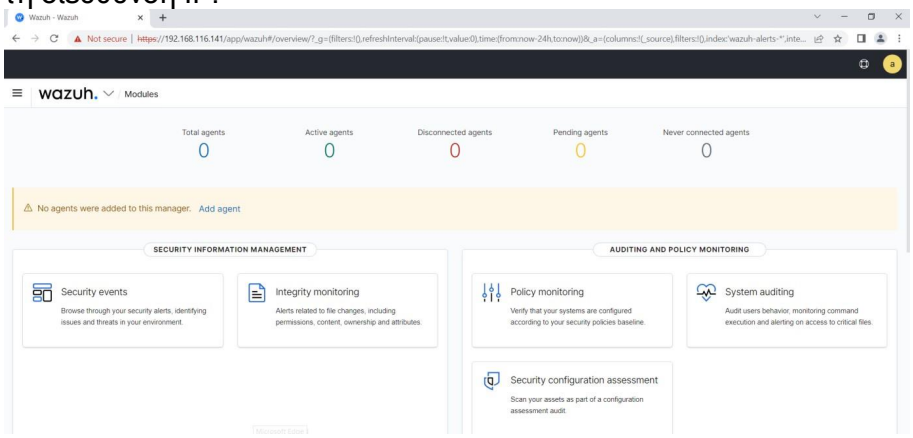
Για να κάνουμε σωστή εγκατάσταση και σωστό configuration στο τελικό μας σημείο θα χρησιμοποιήσουμε ένα virtual machine που υπάρχει. Αυτό το virtual machine είναι ο διακομιστής του συστήματος ανίχνευσης και απόκρισης τελικών σημείων (**EDR**), **Wazuh**.

Για να το κάνουμε αυτό πρέπει να έχουμε εγκατεστημένο από πριν το VMware ή το VirtualBox. Αφού γίνει αυτό ξεκινάμε το virtual machine και θα προσπαθήσουμε να βρούμε τη διεύθυνση IP.



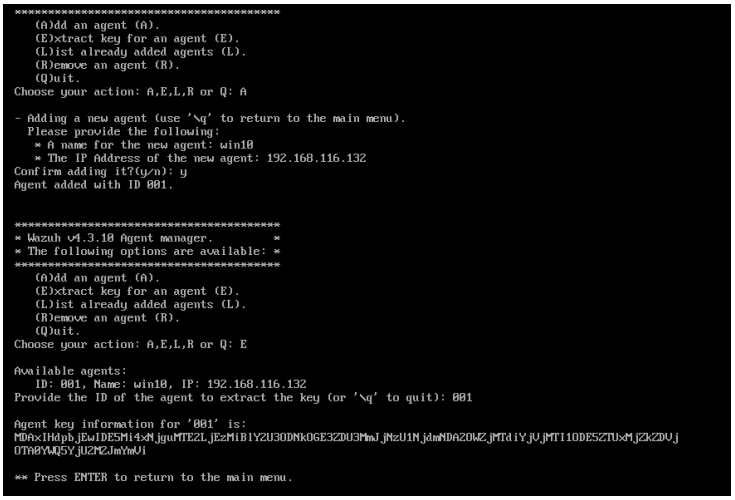
Σχήμα 6.9 Wazuh Server

Αφού βρούμε τη διεύθυνση IP, θα ανοίξουμε το browser του διαχειριστή του οργανισμούκαι θα πληκτρολογήσουμε τη διεύθυνση IP.



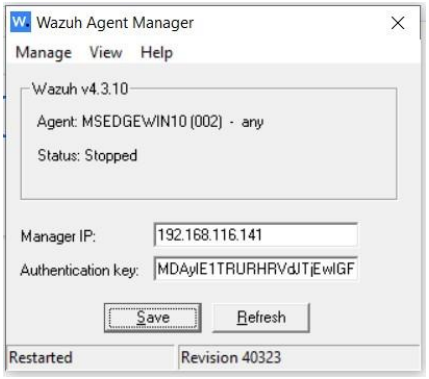
Σχήμα 6.10 Configure Wazuh from browser

Τώρα θα πρέπει να προσθέσουμε τους agents για να κάνουμε διαχείριση των διαφόρων τελικών σημείων. Θα πάμε στο virtual machine και θα προσθέσουμε τα στοιχεία του τελικού σημείου.



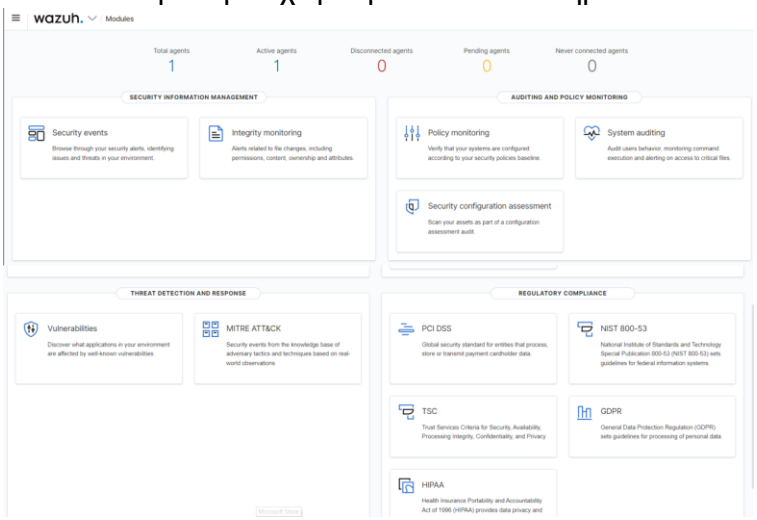
Σχήμα 6.11 Προσθέτουμε τον agent

Στην συνέχεια θα πάμε στο τελικό σημείο και θα εγκαταστήσουμε το Wazuh agent. Αφού το κάνουμε αυτό θα εμφανιστεί ένα παράθυρο που θα πρέπει να βάλουμε τη διεύθυνση IP και το κλειδί που μας έδωσε ο διακομιστής



Σχήμα 6.12 Agent Manager

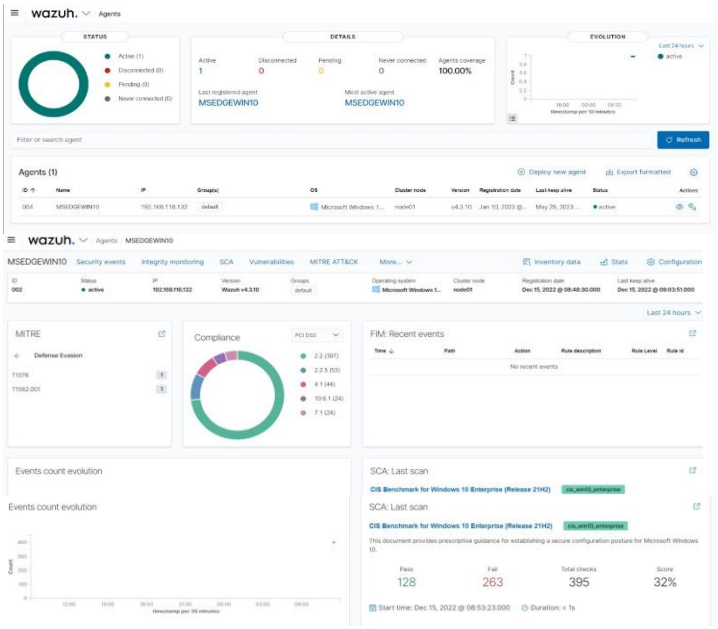
Αφού γίνει αυτό ο καινούριος agent θα προστεθεί στο manager και θα μπορέσουμε να τον δούμε στο browser και να κάνουμε τη διαχείριση του τελικού σημείου.



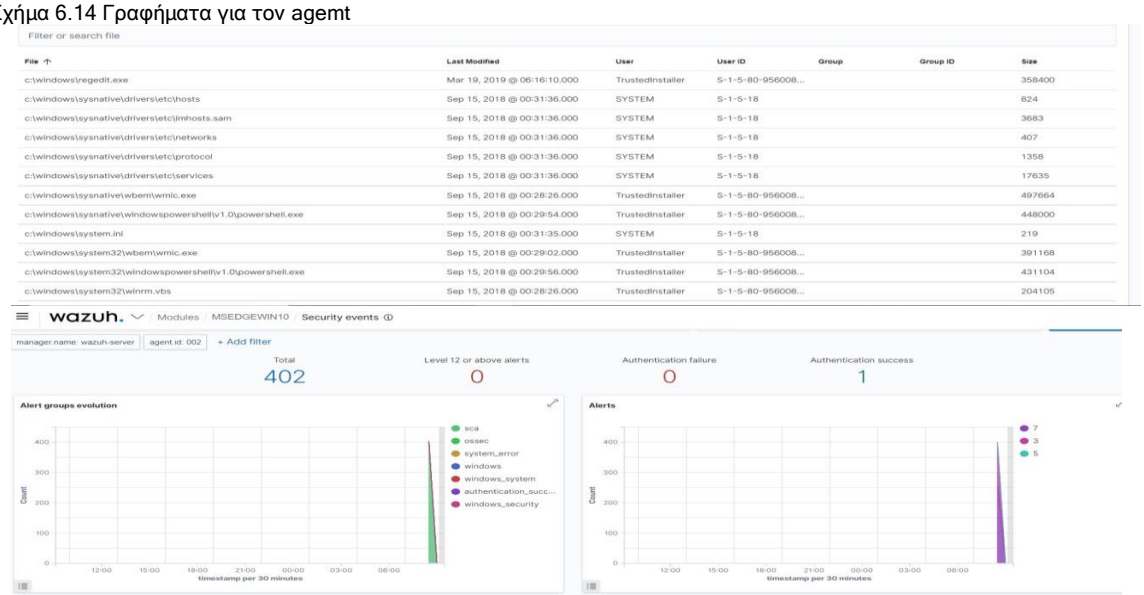
Σχήμα 6.13 Total agents

Αν πάμε στη καρτέλα active θα δούμε το τελικό σημείο που έχουμε εγκαταστήσει και όλες τις πληροφορίες που υπάρχουν για αυτό το υπολογιστικό σύστημα, όπως το id, το όνομα, το λειτουργικό σύστημα και την έκδοση του, τα συμβάντα του υπολογιστή, τα PCI, τα alerts και πληροφορίες για αυτά τα alerts.

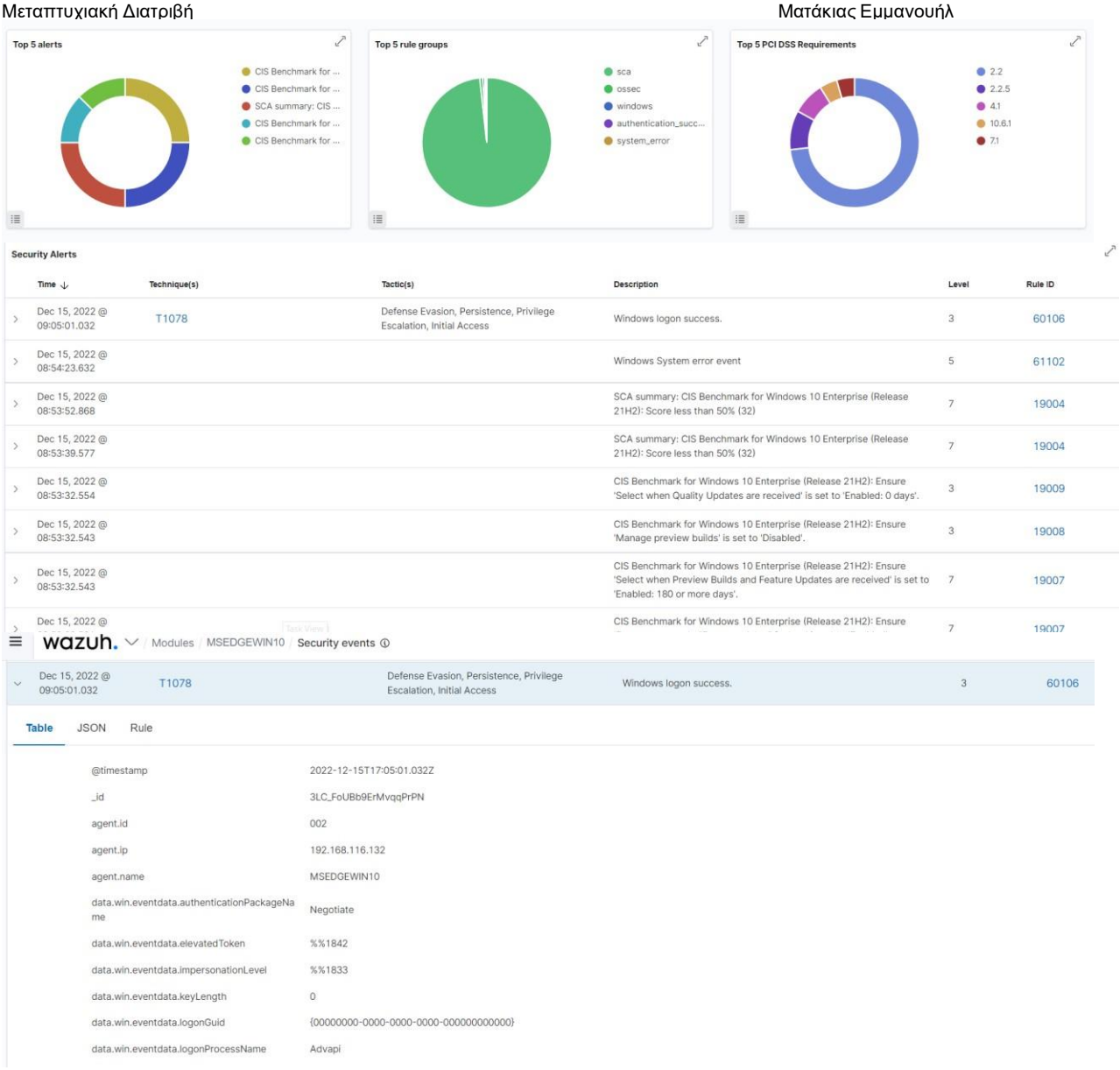
Μπορούμε να δούμε επίσης τα αρχεία του υπολογιστικού συστήματος, καθώς ο διακομιστής τα αναλύει σε περίπτωση ύπαρξης ύποπτου αρχείου. Επιπλέον μας δείχνει και διάφορα γραφήματα για αυτές τις πληροφορίες.



Σχήμα 6.14 Γραφήματα για τον agemt

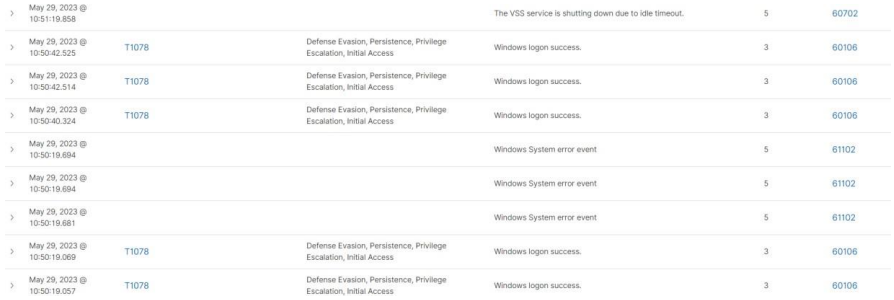


Όπως βλέπουμε τον counter Total μπορούμε να δούμε όλα τα συμβάντα που υπάρχουν.



Σχήμα 6.15 Λεπτομέρειες επίθεσηςς

Μπορούμε να πάρουμε πληροφορίες για το κάθε ένα security alert ξεχωριστά και να καταλάβει ο διαχειριστής τι συμβαίνει στο σύστημα, καθώς φαίνεται και η ημερομηνία που έγιναν όλα αυτά τα συμβάντα. Δυστυχώς το **Wazuh** και γενικά τα συστήματα **EDR** μετά από λίγο χρονικό διάστημα διαγράφει τα συμβάντα. Ας δούμε μετά από διάστημα 3 μηνών αν θυμάται τίποτα από τις προηγούμενες επιθέσεις. Επίσης κάνουμε καινούριες επιθέσεις και θα δούμε τα αποτελέσματα.



Σχήμα 6.16 Παραδείγματα επιθέσεων

Από ότι βλέπουμε από τις ημερομηνίες καταλαβαίνουμε ότι έχει κρατήσει στη μνήμη μόνο τα καινούρια και τα παλιά έχουν διαγραφεί.Να σημειωθεί ότι χρησιμοποιήσαμε την πλατφόρμα επίθεσης **CALDERA**,με σκοπό να κάνουμε επιθέσεις στο λειτουργικό σύστημα που έχει εγκατεστημένο το **EDR Wazuh**. Τα **alerts** που πήραμε είναι αποτελέσματα των επιθέσεων από το **CALDERA**.

6.3 Εργαλείο ανίχνευσης και απόκρισης τελικών σημείων (EDR), BLUESPAWN

6.3.1 Τι είναι το εργαλείο BLUESPAWN

Το **BLUESPAWN** είναι ένα ενεργό εργαλείο ανίχνευσης και απόκρισης άμυνας και τελικού σημείου, που σημαίνει ότι μπορεί να χρησιμοποιηθεί από τους χρήστες για τον γρήγορο εντοπισμό, αναγνώριση και εξάλειψη κακόβουλης δραστηριότητας και κακόβουλου λογισμικού σε ένα δίκτυο. (53)

Το εργαλείο **BLUESPAWN** βοηθά τους χρήστες και γενικά την blue team, να παρακολουθούν τα συστήματα σε πραγματικό χρόνο ενάντια σε ενεργούς εισβολείς, εντοπίζοντας ανώμαλη δραστηριότητα σε αυτά τα συστήματα.

6.3.1.1 Τι περιλαμβάνει το εργαλείο BLUESPAWN

Το BLUESPAWN είναι ένα εργαλείο ανοιχτού κώδικα και περιλαμβάνει τα εξής:

- Γρήγορο εντοπισμό κακόβουλης δραστηριότητας.
- Μεγάλη κάλυψη ως προς την ανίχνευση κακόβουλης δραστηριότητας.
- Καλύτερη κατανόηση της επιφάνειας επίθεσης των Windows με σκοπό την καλύτερη δυνατή υπεράσπιση.
- Περισσότερο λογισμικό ανοιχτού κώδικα Blue Team: Ενώ υπάρχουν πολλά εργαλεία ανοιχτού κώδικα Red Team εκεί έξω, η συντριπτική πλειονότητα μερικών από τα καλύτερα εργαλεία της Blue Team είναι κλειστού κώδικα (π.χ. **AV**, **EDR**, SysInternals, κ.λπ.). Δεν χρειάζεται να βασιζόμαστε στην ασφάλεια μέσω της αφάνειας για την αποτροπή κακόβουλών παραγόντων.
- Επίδειξη των χαρακτηριστικών των API λειτουργικών συστημάτων: Για να το δημιουργήσουμε, εξετάσαμε έναν τόνο Τεκμηρίωσης της Microsoft, Απαντήσεις StackOverflow και πολλά άλλα. Ας ελπίσουμε ότι άλλοι μπορεί να βρουν κάποιο σημείο από τον κώδικα χρήσιμο.

6.3.2 Γραμμές εντολών

Στα πλαίσια αυτής της διπλωματικής θα εγκαταστήσουμε το εργαλείο **BLUESPAWN** στοχρήστη **win11** με το λειτουργικό **Windows 11**. Το εργαλείο **BLUESPAWN** αποτελείται από 3 κύριες λειτουργίες όπως αναφέρονται παρακάτω.

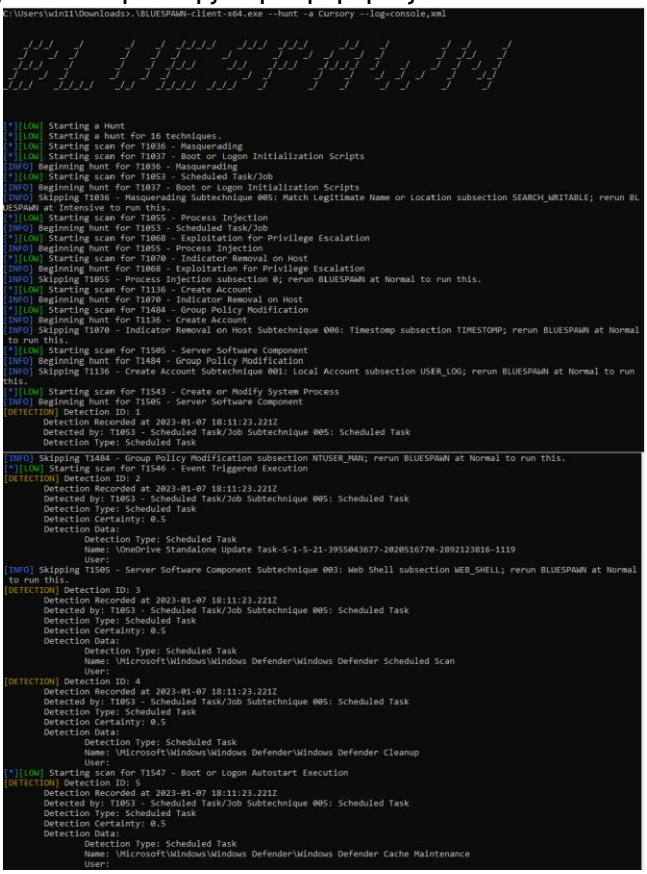
Σχήμα 6.17 Πληροφορίες για το Bluespawn

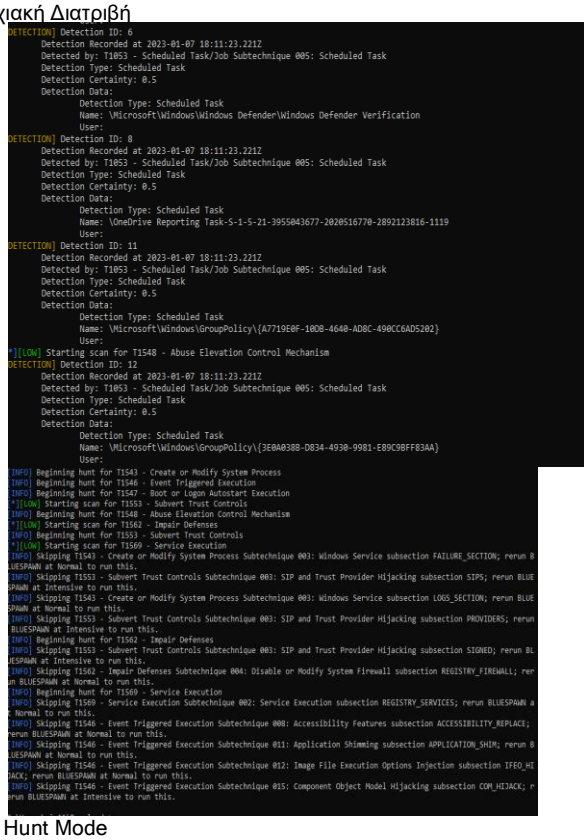
```
log options:
 -o, --output arg  Specify the output folder for any logs written to a file
                   (default: .)

mitigate options:
      --mode [=arg(=audit)]     Selects whether to audit or enforce each
                                mitigations. Options are audit and enforce.
                                Ignored if --gen-config is specified (default:
                                audit)
      --config-json arg         Specify a file containing a JSON
                                configuration for which mitigations and policies should
                                run
      --enforcement-level [=arg(=moderate)]
                                Specify the enforcement level for
                                mitigations. This is used to select which policies should
                                be run. Available levels are none, low,
                                moderate, high, and all (default: moderate)
      --add-mitigations arg     Specify additional JSON files containing
                                mitigations.
      --gen-config arg          Generate a default JSON configuration file
                                (./bluespawn-mitigation-config.json) with the
                                specified level of detail. Options are global,
                                mitigations, and mitigation-policies. Will not
                                run any mitigations if this is specified
                                (default: mitigations)

scan options:
      --scan-folder [=arg(=)]   Specify a folder to scan
      --scan-file [=arg(=)]     Specify a file to scan
      --scan-process [=arg(=)]  Specify a process to scan by PID


C:\Users\win11\Downloads>
```

Αρκετές από αυτές τις ενότητες έχουν υποενότητες (οι οποίες ενδέχεται να μην έχουν δημιουργηθεί ακόμα στη βάση κωδικών) όπως αναφέρονται παρακάτω και όλες βρίσκονται σε διάφορα στάδια σχεδιασμού, έρευνας και ανάπτυξης. Επιπλέον, υποστηρίζονται από μια σειρά από άλλες ενότητες.

Αυτές είναι όλες οι επιλογές που έχει το εργαλείο από αυτά έχουμε:

- Hunt: Αναζήτηση αποδείξεων κακόβουλης συμπεριφοράς.



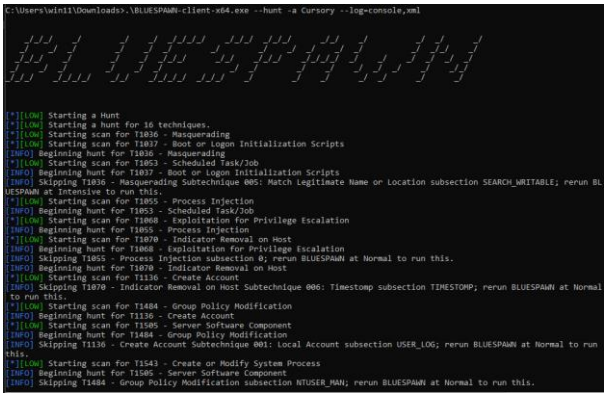


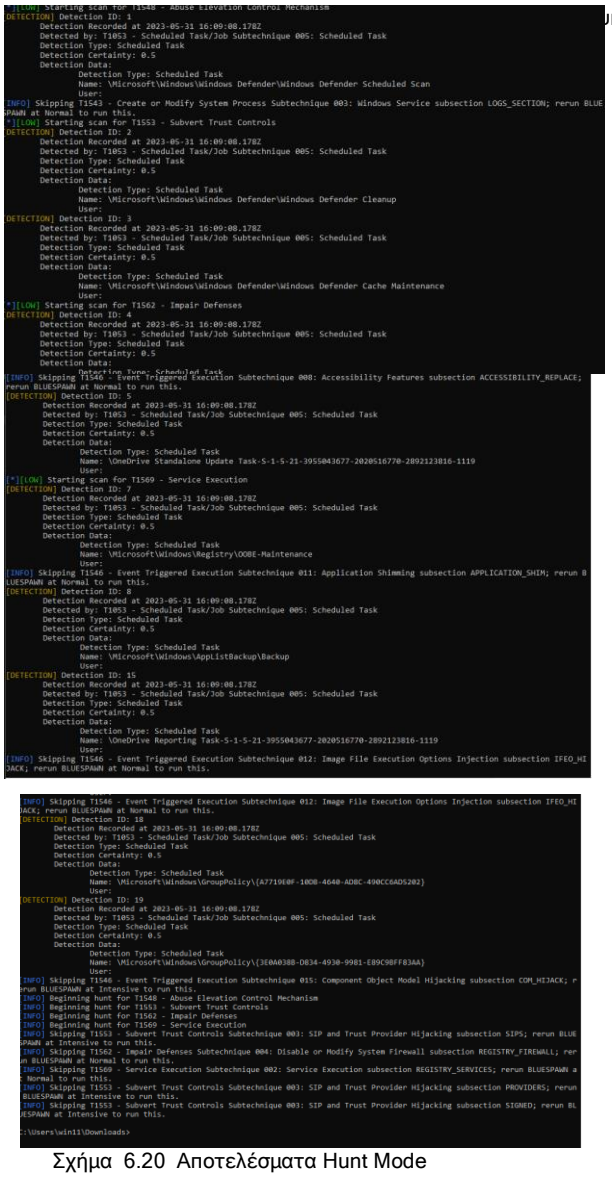
Σχήμα 6.18 Hunt Mode

Για να καταλάβουμε πως λειτουργεί αυτή η λειτουργία θα δοκιμάσουμε να τρέξουμε επίθεση από το **Caldera** ,να την αφήσουμε να τελειώσει, για να αναζητήσουμε στη συνέχεια κακόβουλα αρχεία.

Σχήμα 6.19 Επιθέσεις με το Caldera

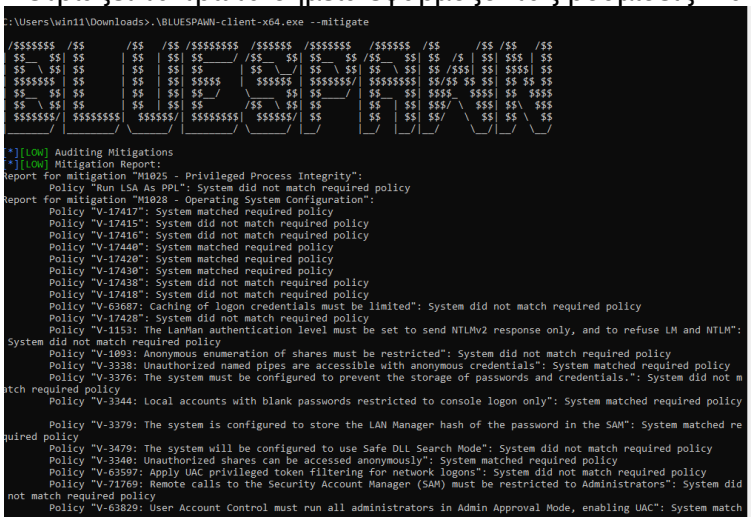
Τώρα θα αρχίσουμε το **Hunt mode** από το **Bluespawn** και θα περιμένουμε αποτελέσματα αναζήτησης κακόβουλων αρχείων.



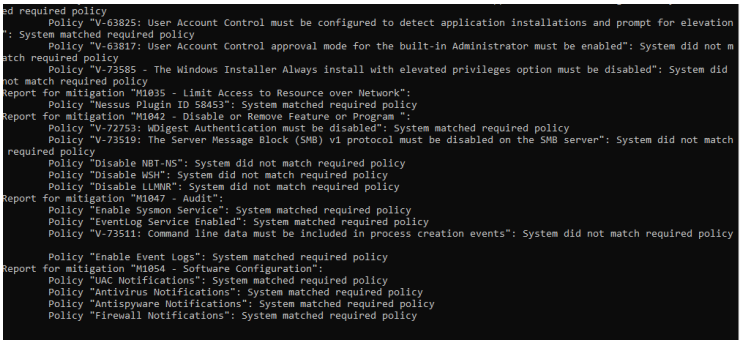


Σχήμα 6.20 Αποτελέσματα Hunt Mode

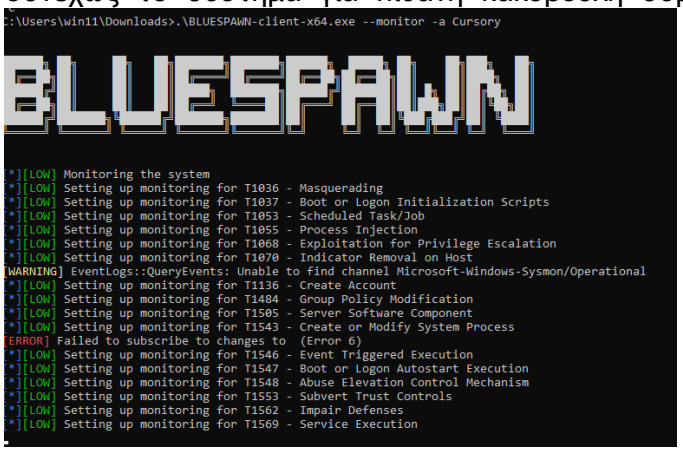
- Mitigate: Μετριάζει τα τρωτά σημεία εφαρμόζοντας ρυθμίσεις ασφαλείας.



Σχήμα 6.21 Mitigate Mode



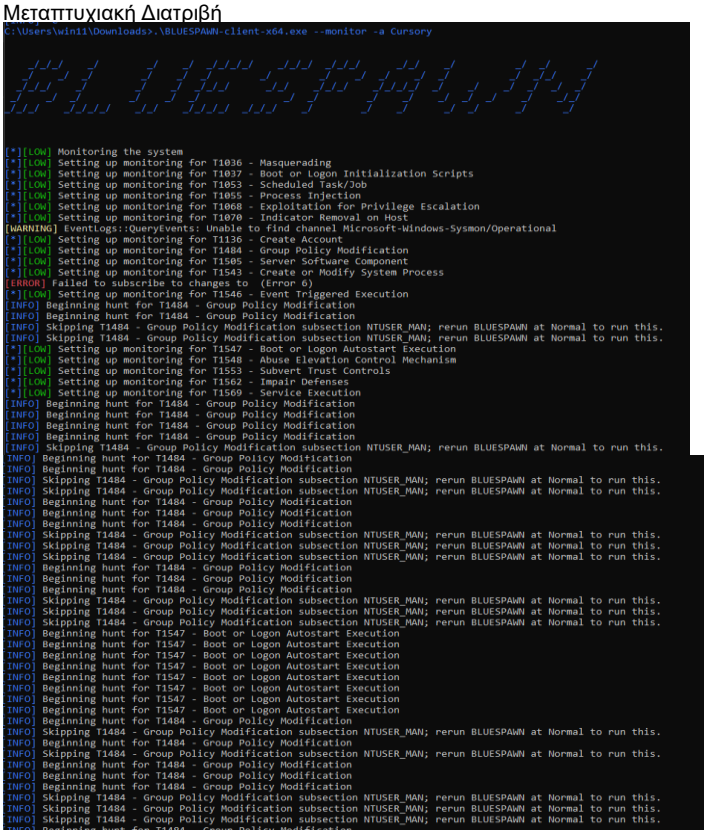
- Monitor: Παρακολουθεί συνεχώς το σύστημα για πιθανή κακόβουλη συμπεριφορά.



Σχήμα 6.22 Monitor Mode

Για να εξετάσουμε λίγο πως δουλεύει θα κάνουμε επιθέσεις με το **Caldera,** ενώ έχουμε ανοιχτό το monitor και θα βρούμε όλα τα αποτελέσματα που θα έρθουν στο **EDR**. Θα ξεκινήσουμε ένα **Thief Operation** από το **Caldera**:

Και περιμένουμε.



Σχήμα 6.23 Αποτελέσματα μετά από επίθεση

Βλέπουμε ότι μας ήρθε κάτι στο **EDR** και έτσι μπορούμε να κάνουμε διάφορες λειτουργίες για να αποτρέψουμε την επίθεση και να προστατέψουμε τον υπολογιστή μας.

- Scan: Χρησιμοποιείται για την αξιολόγηση αντικειμένων που προσδιορίζονται από κυνήγια και για τη λήψη απόφασης, εάν πρόκειται για ύποπτο και κακόβουλο λογισμικό ή όχι.
- User: Περιέχει κύριο πρόγραμμα, IOBase και άλλες παρόμοιες λειτουργίες.
- Util: Περιέχει μια συλλογή ενοτήτων που υποστηρίζουν βασικές λειτουργίες όπως:

1. Configuration
2. Event Logs
3. File System
4. Log
5. PEs
6. Processes

6.4 Πλατφόρμα επιθέσεων CALDERA

6.4.1 Τι είναι το CALDERA

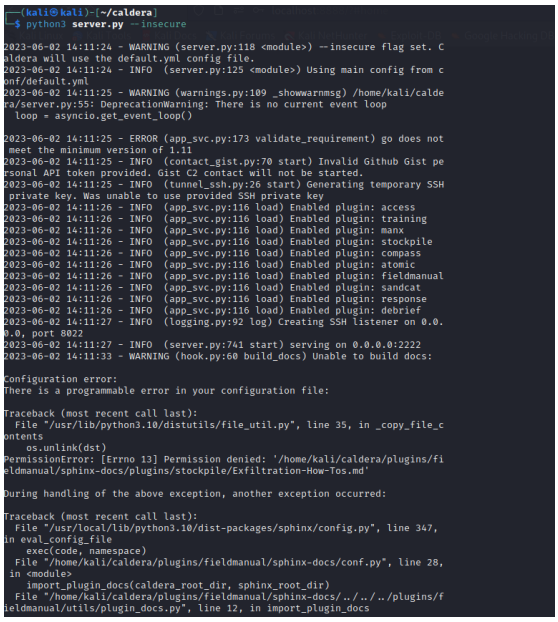
Το εργαλείο **CALDERA** είναι ένα πλαίσιο ασφάλειας στον κυβερνοχώρο, που έχει σχεδιαστεί για να εκτελεί εύκολα αυτόνομες ασκήσεις παραβίασης και προσομοίωσης. Μπορεί επίσης να χρησιμοποιηθεί για την εκτέλεση χειροκίνητων δεσμεύσεων της **red team** ή αυτοματοποιημένης απόκρισης περιστατικών.

Το εργαλείο **CALDERA** βασίζεται στο πλαίσιο **MITRE ATT&CK™** και είναι ένα ενεργό ερευνητικό έργο στη **MITRE**.

Το πλαίσιο **CALDERA** αποτελείται από δύο στοιχεία:

1. **The core system**: Αυτός είναι ο κώδικας πλαισίου, που περιλαμβάνει έναν ασύγχρονο διακομιστή εντολών και ελέγχου (C2) με REST API και διεπαφή ιστού.
2. **Plugins**: Αυτά είναι ξεχωριστά αποθετήρια που κρέμονται από το βασικό πλαίσιο, παρέχοντας πρόσθετη λειτουργικότητα. Παραδείγματα περιλαμβάνουν πράκτορες, διεπαφές GUI, συλλογές **TTP** και άλλα. (54)

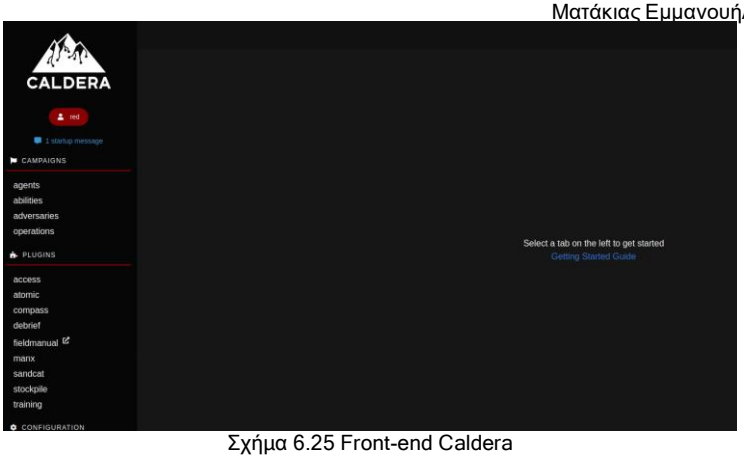
Για να ξεκινήσουμε το πλαίσιο **CALDERA** πρέπει πρώτα να εγκαταστήσουμε το service και στη συνέχεια να ξεκινήσουμε το server.



Σχήμα 6.24 Εγκατάσταση του Caldera σε Kali Linux

Το πλαίσιο **CALDERA** είναι web-based και μπορούμε να εισέλθουμε από τον browser γράφοντας για url το localhost και την πόρτα, που στη συγκεκριμένη περίπτωση είναι η 8888.

Τα credentials είναι:
Username:red
Password:admin

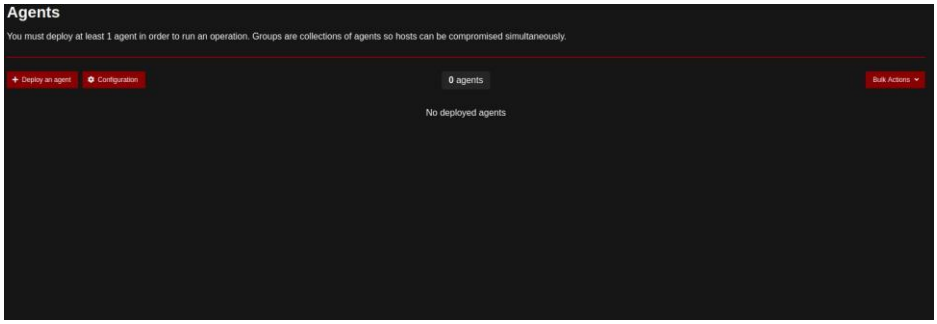


Σχήμα 6.25 Front-end Caldera

6.4.2 Software Components

Το εργαλείο **CALDERA** αποτελείται από διάφορα στοιχεία, που αναφέρονται σε υπολογιστές που επιθυμούμε να κάνουμε άσκηση παραβίασης και τακτικές για την άσκηση παραβίασης.

- **Agents**: Οι **Agents** είναι προγράμματα λογισμικού που συνδέονται ξανά στο CALDERA σε συγκεκριμένα χρονικά διαστήματα για να λάβουν οδηγίες. Οι **Agents** επικοινωνούν με τον διακομιστή **CALDERA** μέσω μιας μεθόδου επαφής, η οποία ορίστηκε αρχικά κατά την εγκατάσταση του **Agent**.



Σχήμα 6.26 Front-end Agents

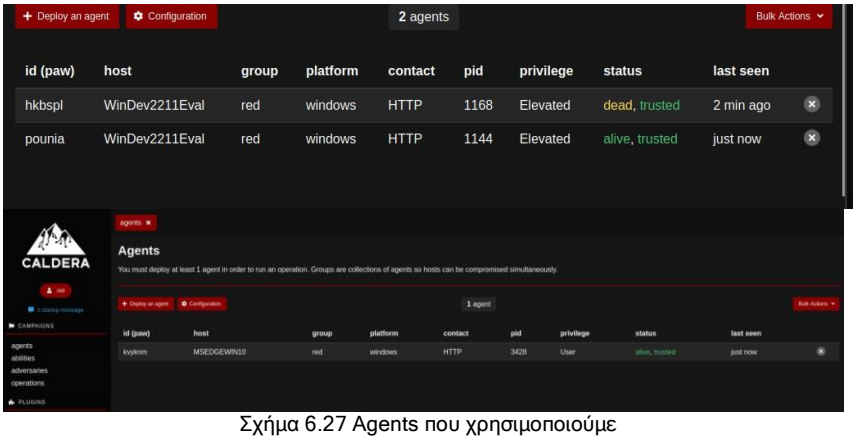
Οι εγκατεστημένοι **Agents** εμφανίζονται στη διεπαφή χρήστη στο παράθυρο διαλόγου Agents. Το **CALDERA** περιλαμβάνει μια σειρά από προγράμματα πρακτόρων, το καθένα προσθέτοντας μοναδική λειτουργικότητα. Μερικά παραδείγματα παρατίθενται παρακάτω:

1. **Sandcat**: Ένας πράκτορας GoLang που μπορεί να επικοινωνεί μέσω διαφόρων καναλιών C2, όπως HTTP, Github GIST ή DNS tunneling.
2. **Manx**: Ένας πράκτορας GoLang που επικοινωνεί μέσω της επαφής TCP και λειτουργεί ως αντίστροφο κέλυφος
3. **Ragdoll**: Ένας πράκτορας Python που επικοινωνεί μέσω της επαφής HTML

Οι **Agents** μπορούν να τοποθετηθούν σε μια ομάδα, είτε κατά την εγκατάσταση μέσω σημαιών γραμμής εντολών, είτε με επεξεργασία του πράκτορα στη διεπαφή χρήστη. Αυτές οι ομάδες χρησιμοποιούνται κατά την εκτέλεση μιας λειτουργίας, για τον προσδιορισμό σε ποιους πράκτορες θα εκτελεστούν οι ικανότητες.Η ομάδα καθορίζει εάν ένας πράκτορας είναι «κόκκινος πράκτορας» ή «μπλε πράκτορας».

Οποιοσδήποτε πράκτορας ξεκινά στην ομάδα "μπλε" θα είναι προσβάσιμος από τον μπλε πίνακα εργαλείων. Όλοι οι άλλοι πράκτορες θα είναι προσβάσιμοι από τον κόκκινο πίνακα ελέγχου

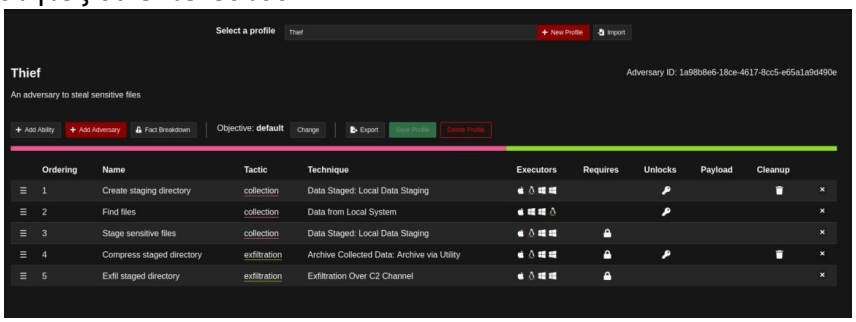
.



Σχήμα 6.27 Agents που χρησιμοποιούμε

- **Abilities and Adversaries: Ability** είναι μια συγκεκριμένη εφαρμογή τακτικής ATT&CK που μπορεί να εκτελεστεί σε εκτελούμενους **Agents**. Τα **Abilities** θα περιλαμβάνουν τις εντολές προς εκτέλεση, τις πλατφόρμες στις οποίες μπορούν να εκτελεστούν οι εντολές (π.χ. Windows / PowerShell), ωφέλιμα φορτία που θα συμπεριληφθούν και μια αναφορά σε μια ενότητα για την ανάλυση της εξόδου στον διακομιστή **CALDERA**.

Adversary: Τα προφίλ **Adversary** είναι ομάδες ικανοτήτων, που αντιπροσωπεύουν τις τακτικές, τις τεχνικές και τις διαδικασίες (TTP) που είναι διαθέσιμες σε έναν παράγοντα απειλής. Τα προφίλ αντιπάλου χρησιμοποιούνται κατά την εκτέλεση μιας λειτουργίας, για να προσδιοριστεί ποιες ικανότητες θα εκτελεστούν.



Σχήμα 6.28 Δοκιμή επίθεσης Thief

Σε αυτή την περίπτωση θα χρησιμοποιήσουμε το προφίλ **Thief Adversary** για να συλλέξουμε τα στοιχεία του χρήστη που θέλουμε να επιτεθούμε.

- **Operations:** Τα **Operations** εκτελούν διάφορα **Abilities** σε ομάδες **Agents**. Τα προφίλ **Adversaries** χρησιμοποιούνται για να καθοριστεί ποια **Abilities** θα εκτελεστούν και οι ομάδες **Agents** χρησιμοποιούνται, για να καθοριστεί σε ποιους **Agents** θα εκτελεστούν τα **Abilities**.

Σχήμα 6.29 Τα στάδια μιας επίθεσης

Η σειρά με την οποία εκτελούνται τα **Abilities** καθορίζεται από τον προγραμματιστή. Μερικά παραδείγματα σχεδιαστών που περιλαμβάνονται από προεπιλογή στο **CALDERA**, παρατίθενται παρακάτω:

1. **Atomic**: Εκτελούμε **Abilities** στο προφίλ του **Adversary**, σύμφωνα με την ατομική σειρά του **Adversary**.
2. **Batch**: Εκτελούμε όλα τα **Abilities** στο προφίλ **Adversary** ταυτόχρονα.
3. **Buckets**: Εκτελούμε **Abilities** στο προφίλ του **Adversary** ομαδοποιημένες κατά τακτική ATT&CK.

Όταν κάποιο **Ability** εκτελείται σε ένα **Operation**, δημιουργείται ένας σύνδεσμος για κάθε **Agent** εάν:

- Όλα τα στοιχεία σύνδεσης και οι απαιτήσεις γεγονότων έχουν εκπληρωθεί.
- Ο **Agent** έχει έναν εκτελεστή, στον οποίο το **Ability** έχει ρυθμιστεί να εκτελείται.
- Ο **Agent** δεν έχει ακόμη εκτελέσει το **Ability** ή το **Ability** έχει επισημανθεί ως επαναλαμβανόμενη διαδικασία.

Ένα γεγονός είναι μια αναγνωρίσιμη πληροφορία για έναν δεδομένο υπολογιστή. Τα ονόματα γεγονότων αναφέρονται σε αρχεία **Abilities** και θα αντικατασταθούν με τις τιμές γεγονότων, όταν δημιουργηθεί ένας σύνδεσμος από το **Ability**.

Οι εντολές σύνδεσης μπορεί να είναι ασαφείς, ανάλογα με τις μυστικές ρυθμίσεις της λειτουργίας.Οι δημιουργημένοι σύνδεσμοι προστίθενται στην αλυσίδα **Operations**. Η αλυσίδα περιέχει όλους τους συνδέσμους που δημιουργήθηκαν για το **Operation**.

Όταν ένα **Agent** κάνει check in, θα συλλέξει τις οδηγίες του. Στη συνέχεια εκτελούνται οι οδηγίες, ανάλογα με τον εκτελεστή που χρησιμοποιείται, και τα αποτελέσματα αποστέλλονται πίσω στον διακομιστή **CALDERA**.

Στη συνέχεια, λαμβάνονται τα αποτελέσματα, το **CALDERA** θα χρησιμοποιήσει έναν αναλυτή για να προσθέσει τυχόν συλλεχθέντα στοιχεία στη λειτουργία. Οι αναλυτές αναλύουν το αποτέλεσμα ενός **Ability** εξαγωγής πιθανών γεγονότων.

Εάν επιτρέπονται πιθανά γεγονότα μέσω των κανόνων γεγονότων, το γεγονός προστίθεται στη λειτουργία, για χρήση σε μελλοντικούς συνδέσμους.

- **Plugins:** Το **CALDERA** όπως είπαμε παραπάνω, είναι ένα πλαίσιο που επεκτείνεται από διάφορα **Plugins**. Αυτά τα **Plugins** παρέχουν στο **CALDERA** κατά κάποιο τρόπο, επιπλέον λειτουργικότητα.Πολλά **Plugins** περιλαμβάνονται από προεπιλογή στο **CALDERA**. Μερικά αξιοσημείωτα παραδείγματα είναι παρακάτω, αν και μια πιο πλήρης και λεπτομερής λίστα μπορεί να βρεθεί στη σελίδα της Βιβλιοθήκης προσθηκών:

1. **Sandcat**: Ο **Agent** Sandcat είναι ο συνιστώμενος **Agent** για νέους χρήστες.
2. **Stockpile**: Αυτό το **Plugin** κατέχει την πλειονότητα των **Abilities** ανοιχτού κώδικα, των **Adversaries**, των σχεδιαστών και των παραγόντων που δημιουργήθηκαν από την ομάδα **CALDERA**.
3. **Training**: Το **Plugin Training** καθοδηγεί τους χρήστες στις περισσότερες λειτουργίες του **CALDERA** και συνιστάται για νέους χρήστες.

Κεφάλαιο 7ο – Συμπεράσματα Διατριβής

7.1 Συμπεράσματα μελέτης

Το Endpoint Detection and Response (EDR) είναι ένα κρίσιμο στοιχείο στη σύγχρονη στρατηγική κυβερνοασφάλειας, παρέχοντας στις οργανώσεις τα μέσα για τον εντοπισμό, την αντίδραση και τη μείωση προηγμένων απειλών που στοχεύουν σε τελικά σημεία. Καταλήγοντας, μπορούν να επισημανθούν αρκετά βασικά σημεία σχετικά με το EDR:

- **Εντοπισμός Προηγμένων Απειλών:** Οι λύσεις EDR διαδραματίζουν κρίσιμο ρόλο στον εντοπισμό προηγμένων και εξελισσόμενων κυβερνοαπειλών που ενδέχεται να παρακάμψουν τα παραδοσιακά μέτρα ασφαλείας.
- **Παρακολούθηση και Ορατότητα σε Πραγματικό Χρόνο:** Τα εργαλεία EDR παρέχουν

πραγματική παρακολούθηση και ορατότητα στις δραστηριότητες των τελικών σημείων, παρέχοντας στις ομάδες ασφαλείας εισαγωγές σχετικά με πιθανές περιπτώσεις ασφάλειας.

- **Αντίδραση και Έρευνα Συμβάντων:**Το EDR διευκολύνει την άμεση αντίδραση συμβάντων παρέχοντας λεπτομερείς πληροφορίες σχετικά με τη φύση των περιστατικών ασφάλειας, επιτρέποντας στις ομάδες ασφαλείας να ερευνήσουν και να αντιμετωπίσουν αποτελεσματικά τις απειλές.

- **Συμπεριφορική Ανάλυση:** Το EDR εκμεταλλεύεται τη συμπεριφορική ανάλυση για τον εντοπισμό ανωμαλιών στα πρότυπα δραστηριοτήτων, επιτρέποντας τον πρόωρο εντοπισμό κακόβουλης συμπεριφοράς και επιθέσεων zero-day.

- **Ενσωμάτωση Πληροφοριών για Απειλές:** Η ενσωμάτωση με πληροφορίες απειλών ενισχύει τη δυνατότητα των λύσεων EDR να αναγνωρίζουν και να ανταποκρίνονται σε γνωστές και νεότερες απειλές.

- **Αυτοματοποιημένη Αντίδραση και Αντιμετώπιση:** Πολλές λύσεις EDR ενσωματώνουν δυνατότητες αυτοματοποιημένης αντίδρασης για να περιορίσουν και να αντιμετωπίσουν γρήγορα τις απειλές, μειώνοντας το πιθανό αντίκτυπο των περιστατικών ασφάλειας.

- **Υγιεινή Ασφαλείας:** Το EDR υπογραμμίζει τη σημασία της διατήρησης καλής υγιεινής ασφαλείας των τελικών σημείων, εξασφαλίζοντας ότι τα τελικά σημεία είναι σωστά ρυθμισμένα, ενημερωμένα και επιδιορθωμένα για να ελαχιστοποιηθούν οι ευπάθειες.

- **Ανάλυση Συμπεριφοράς Χρήστη και Οντότητας (UEBA):** Οι λύσεις EDR συχνά ενσωματώνουν την ανάλυση συμπεριφοράς χρήστη και οντότητας (UEBA) για τον εντοπισμό προτύπων συμπεριφοράς χρήστη, βοηθώντας στον εντοπισμό εσωτερικών απειλών και μη εξουσιοδοτημένης πρόσβασης.
- **Ενσωμάτωση με το Ασφαλειολογικό Οικοσύστημα:** Η επιτυχής υλοποίηση του EDR περιλαμβάνει απροβλημάτιστη ενσωμάτωση με άλλα εργαλεία και πλατφόρμες ασφαλείας για τη δημιουργία ενός συνεκτικού και ολοκληρωμένου οικοσυστήματος κυβερνοασφάλειας.

- **Συνεχής Παρακολούθηση και Βελτίωση:** Το EDR είναι ένας εξελισσόμενος τομέας, και οι οργανώσεις πρέπει να παρακολουθούν και να βελτιώνουν διαρκώς τις στρατηγικές τους για να προσαρμόζονται σε νέες και αναδυόμενες απειλές.

Συνοψίζοντας, το EDR αποτελεί θεμελιώδες συστατικό μιας σύγχρονης στρατηγικής κυβερνοασφάλειας, επιτρέποντας στις οργανώσεις να αντιμετωπίζουν αποτελεσματικά τις απειλές και να ανταποκρίνονται σε περιστατικά ασφάλειας των τελικών σημείων.

7.2 Μελλοντική έρευνα

Τα συστήματα ανίχνευσης και αντίδρασης τελικών σημείων (EDR) αποτελούν κρίσιμα στοιχεία στην κυβερνοασφάλεια, παρέχοντας στις οργανώσεις τη δυνατότητα ανίχνευσης και αντίδρασης σε προηγμένες απειλές που στοχεύουν τελικά σημεία, όπως υπολογιστές, διακομιστές και κινητές συσκευές. Δεδομένου ότι η τεχνολογία εξελίσσεται με γοργούς ρυθμούς, κάποιες πιθανές κατευθύνσεις για το μέλλον των συστημάτων EDR είναι:

- **Ενσωμάτωση της Τεχνητής Νοημοσύνης και της Μηχανικής Μάθησης:** Συνεχής ενσωμάτωση της τεχνητής νοημοσύνης (ΤΝ) και της μηχανικής μάθησης (ΜΜ) στα συστήματα EDR για την ενίσχυση των δυνατοτήτων ανίχνευσης απειλών. Αυτό περιλαμβάνει την αξιοποίηση προβλεπτικής ανάλυσης και ανάλυσης συμπεριφοράς για τον εντοπισμό ανωμαλιών που μπορεί να υποδεικνύουν μια πιθανή απειλή.

- **Αυξημένος αυτοματισμός:** Αυξημένος αυτοματισμός των ενεργειών αντίδρασης για τον άμεσο περιορισμό και την αντιμετώπιση των απειλών. Ο αυτοματισμός βοηθά τις οργανώσεις να αντιδρούν σε περιστατικά πιο γρήγορα, μειώνοντας τον χρόνο που απαιτείται για τον περιορισμό των επιπτώσεων μιας κυβερνοαπειλής.

- **Συστήματα EDR φιλικά προς τον Χώρο του Νέφους:** Συστήματα EDR σχεδιασμένα ειδικά για περιβάλλοντα νέφους για την αντιμετώπιση της μετάβασης προς υποδομές βασισμένες στο νέφος. Καθώς οι οργανώσεις συνεχίζουν να μετακινούνται προς το νέφος, οι λύσεις EDR πρέπει να προσαρμοστούν για την προστασία των άκρων σε αυτά τα δυναμικά και κατανεμημένα περιβάλλοντα.

- **Ενσωμάτωση με την Προέκταση της Ανίχνευσης και της Αντίδρασης (XDR):** Ενσωμάτωση με πλατφόρμες Προέκτασης Ανίχνευσης και Αντίδρασης (XDR) για την παροχή μιας πιο ολιστικής και διασυνοριακής αντίληψης των περιστατικών ασφαλείας. Οι λύσεις XDR συνήθως επεκτείνονται πέρα από τα άκρα για να περιλαμβάνουν ασφάλεια δικτύου, ηλεκτρονικού ταχυδρομείου και νέφους.

- **Πλαίσιο Ασφαλείας Μηδενικής Εμπιστοσύνης:** Συμμόρφωση με το πλαίσιο ασφαλείας Μηδενικής Εμπιστοσύνης, όπου τα συστήματα EDR διαδραματίζουν κρίσιμο ρόλο στο συνεχή έλεγχο της ασφάλειας των άκρων και στη διασφάλιση ότι μόνο εξουσιοδοτημένα πρόσωπα έχουν πρόσβαση σε ευαίσθητους πόρους.
- **Κοινοποίηση Πληροφοριών Απειλής:** Βελτιωμένη συνεργασία και κοινοποίηση πληροφοριών μεταξύ των λύσεων EDR για την ενίσχυση της πληροφορίας απειλής. Αυτό μπορεί να περιλαμβάνει την κοινοποίηση ενδείξεων παραβίασης (IoCs) και άλλων σχετικών δεδομένων απειλής για την ενίσχυση της συνολικής θέσης ασφαλείας.

- **Ενσωμάτωση Ανάλυσης Συμπεριφοράς Χρηστών και Οντοτήτων (UEBA):** Ενσωμάτωση Ανάλυσης Συμπεριφοράς Χρηστών και Οντοτήτων (UEBA) για την ανάλυση και τον εντοπισμό ανωμαλιών στα πρότυπα συμπεριφοράς που μπορεί να υποδεικνύουν εσωτερικές απειλές ή παραβιάσεις λογαριασμών χρηστών.

- **Σκέψεις για Απορρήτου και Συμμόρφωση:** Ενισχυμένα χαρακτηριστικά απορρήτου και σκέψεις για συμμόρφωση για τον αντιμετωπισμό των εξελισσόμενων κανονιστικών απαιτήσεων. Καθώς οι νόμοι περί προστασίας δεδομένων γίνονται πιο αυστηροί, οι λύσεις EDR μπορεί να χρειαστεί να ενσωματώσουν χαρακτηριστικά που εξασφαλίζουν τη συμμόρφωση με τους κανονισμούς περί προστασίας της ιδιωτικότητας.

- **Δυνατότητες "Threat Haunting":** Βελτιωμένες δυνατότητες αναζήτησης απειλών (threat haunting) για ενδυνάμωση των ομάδων ασφαλείας να αναζητούν ενεργά και να εντοπίζουν πιθανές απειλές, αντί να βασίζονται αποκλειστικά σε αυτόματη ανίχνευση.

Είναι σημαντικό να σημειωθεί ότι το τοπίο της κυβερνοασφάλειας είναι δυναμικό, και η εξέλιξη των συστημάτων EDR θα επηρεαστεί πιθανώς από νέες τεχνολογίες, τοπία απειλών και

την εξελισσόμενη φύση των κυβερνοαπειλών. Για τις πιο ενημερωμένες πληροφορίες, συνιστάται η συμβουλή των πιο πρόσφατων αναφορών της βιομηχανίας, των ενημερώσεων των προμηθευτών και των ειδήσεων κυβερνοασφάλειας.

Βιβλιογραφία

1. (11 August 2019). *What Is an Advanced Persistent Threat (APT)?* Cisco.

2. (2013). *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Cole., Eric.

3. (11 August 2019). *Cyber Threats to the Financial Services and Insurance Industries.* FireEye.

4. (26 May 2023). *Intelligence, Microsoft Threat, Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.* Microsoft Security Blog.

5. (April 11, 2011.). *What is antivirus software?* Microsoft.

6. (May 17, 2009). *The Evolution of Viruses and Worms.* Thomas Chen, Jean-Marc Robert.

7. (2017). *What is an Intrusion Detection System (IDS)?* Check Point Software.

8. (2019-09-29). *EDR Security and Protection for the Enterprise.* Cynet.

9. (1993). *TTP - A time-triggered protocol for fault-tolerant real-time systems.* Kopetz, Herman; Grunsteidl, Gunter.

10. (2022-04-18). *What is the MITRE ATT&CK Framework?* Rapid7.

11. (7 July 2017). *What makes a cyberattack? Experts lobby to restrict the term.* Satter, Raphael.

12. (August 21, 2015.). *What is endpoint security and how does it work?*

13. (July 22, 2015). *Endpoint security management overview.*

14. (October 7, 2015). *Endpoint security & network protection.*

15. (October 7, 2015). *Endpoint security and compliance management design guide.*

16. (2021-12-05). *Browser Hijack Objects (BHOs).* Malwarebytes Labs.

17. (1999). *Programming Microsoft Internet Explorer.* Roberts Scott.

18. (7 February 2015). *Browser Hijacking Fix & Browser Hijacking Removal.* Microsoft.

19. (28 July 2016). *Petya Ransomware Master File Table Encryption.* Mimoso, Michael.

20. (10 March 2012). *Ransomware: Fake Federal German Police (BKA) notice.* SecureList (Kaspersky Lab).

21. (2013-09-11). *Keylogger.* Oxford dictionaries.

22. (n.d.). *What is a Keylogger?* PC Tools.

23. (5 April 2018). *How a Crypto 'Backdoor' Pitted the Tech World Against the NSA.* Zetter, Kim .

24. (2015-03-14.). *Static Detection of Application Backdoors.* Chris Wysopal, Chris Eng.

25. (2021-11-13). *What is Rootkit – Definition and Explanation.* www.kaspersky.com.

26. (March 29, 2020). *Difference between viruses, worms, and trojan.* Symantec Security Center. Broadcom Inc.

27. (May 10, 2011). *The Spyware Inferno.* Wienbar, Sharon.

28. (2011-01-31). *The Phishing Guide: Understanding and Preventing Phishing Attacks.* Ollmann, Gunter.

29. (December 1, 2006). *Learning to Detect and Classify Malicious Executables in the Wild.* Kolter, J. Zico; Maloof, Marcus A.

30. (August 26, 2014). *A Brief History of Antivirus Software.* techlineinfo.com.

31. (2019-09-29). *EDR Security and Protection for the Enterprise.* Cynet.

32. (2019-09-29). *What is Endpoint Detection and Response (EDR)? - Definition from Techopedia.* Techopedia.com.

33. (2021-09-03). *Endpoint Detection and Response (EDR) - What is EDR and why is it important? - Definition from Cyberpedia.* Palo Alto Networks.

34. (2019-09-29). *What is endpoint detection and response (EDR)? A definition by WhatIs.com.* SearchSecurity.

35. (2019-10-10). *Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: Zion Market Research.* Zion Market.

36. (n.d.). *Symantec Endpoint Detection & response Data Sheet.* Broadcom.

37. (2019-10-10). *10 Ways AI And Machine Learning Are Improving Endpoint Security.* Business 2 Community.

38. (27-9-2020). *Check Point Research.*

39. (13 September 2016). *Symantec Rolls Out New Cloud-Based Endpoint Protection Solution For SMBs.* Kuranda, Sarah.

40. (18 April 2017). *Released versions of Symantec Endpoint Protection.* Enterprise Technical Support.

41. (28 October 2016). *How intrusion prevention works.* Enterprise Technical Support.

42. (19 October 2016). *The Forrester Wave: Endpoint Security Suites.* Sherman, Chris; McClean, Christopher; Schiano, Salvatore; Dostie, Peggy.

43. (28 October 2016). *About the Symantec Endpoint Protection firewall.* Enterprise Technical Support.

44. (2016-11-16). *What is a Domain Controller? - Definition from Techopedia.* Techopedia.com.

45. (13 February 2011). *Domain Controller Roles.* Microsoft Tech .

46. (21 January 2005). *Directory data store.* Microsoft Corporation.

47. (5 February 2014). *Active Directory Backup and Restore.* TechNet Microsoft.

48. (April 4, 2015). *TechNet: What's New in Storage Services in Windows Server Technical.*

49. (April 10, 2015). *Microsoft to release next generation of Windows Server in 2016.* Network World. IDG.

50. (April 4, 2015). *TechNet: What's New in DNS Client in Windows Server Technical Preview (Updated: 1 October 2014).*

51. (10 May 2021). *Wazuh : Security Information and Event Management (SIEM) for Small and Medium-Sized Enterprises.* Arora, Varul .

52. (10 May 2021). *OSSEC Wazuh, un monitor de seguridad para redes de ordenadores.* RedesZone.

53. (n.d.). *bluespawn.* ION28/github.

54. (n.d.). *CALDERA.* mitre/github.

55. (n.d.). https://cybersecurity-excellence-awards.com/candidates/mcafee-mvision-edr/

56. (n.d.). https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/