ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΣΥΣΤΗΜΑΤΑ ΠΡΟΣΔΙΟΡΙΣΜΟΥ ΚΑΙ ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗΣ ΑΠΟΚΡΙΣΗΣ ΣΕ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ (XDR): ΜΕΛΕΤΗ ΕΦΑΡΜΟΣΙΜΟΤΗΤΑΣ ΤΟΥ OPENC2 ΣΕ XDR»

Του φοιτητή
Τσιλιγκαρίδη Χρήστου
Αρ. Μητρώου: 185299

Επιβλέπων
Ηλιούδης Χρήστος
Καθηγητής

Ημερομηνία Ιανουάριος 2023

Τίτλος Π.Ε Σύστηματα προσδιορισμού και αυτοματοποιημένης απόκρισης σε κυβερνοεπιθέσεις: μελέτη εφαρμοσιμότητας του OpenC2 σε XDR

Κωδικός Π.Ε. 23133

Ονοματεπώνυμο φοιτητή Τσιλιγκαρίδης Χρήστος

Ονοματεπώνυμο εισηγητή Ηλιούδης Χρήστος

Ημερομηνία ανάληψης Π.Ε. 10/03/2023

Ημερομηνία περάτωσης Π.Ε 24/01/2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Πρόλογος

Ένας από τους βασικούς λόγους επιλογής αυτής της πτυχιακής εργασίας είναι το ενδιαφέρον μου για την ασφάλεια πληροφορικών συστημάτων και η εργασιακή μου εμπειρία στον χώρο ως Αναλυτής Κυβερνοασφάλειας. Βλέποντας πως οι κακόβουλοι χρήστες μέρα με την μέρα αυξάνουν την πολυπλοκότητα και την αυτοματοποίηση των επιθέσεων τους και ότι οι παραδοσιακοί τρόποι ανίχνευσης και αντιμετώπισης τέτοιων επιθέσεων πλέον δεν έχουν την απαιτούμενη αποτελεσματικότητα, αποφάσισα να μελετήσω τις παθογένειες και τους περιορισμούς των υπάρχων λύσεων στην κυβερνοασφάλεια και με ποιους τρόπους θα μπορούσαν τα σύγχρονα Κέντρα Κυβερνοασφάλειας (SOC) να αντιμετωπίσουν αυτές τις απειλές και να αυξήσουν την αποτελεσματικότητά τους μέσω πιο προηγμένων και αυτοματοποιημένων λύσεων ασφαλείας όπως για παράδειγμα η χρήση XDR αρχιτεκτονικής. Τέλος, μελετώντας όλες τις νέες και παλιές λύσεις κυβερνοασφάλειας θα εμπλουτιστούν οι γνώσεις μου πάνω σε αυτές.

Περίληψη

Καθώς η συχνότητα και η πολυπλοκότητα των επιθέσεων στον κυβερνοχώρο συνεχίζουν να αυξάνονται, οι οργανισμοί αντιμετωπίζουν πρωτοφανείς προκλήσεις στην προσπάθειά τους για να διασφαλίσουν ότι τα πληροφοριακά και υπολογιστικά συστήματά τους θα παραμείνουν αλώβητα. Στην παρούσα Διπλωματική Εργασία θα γίνει μια ολοκληρωμένη διερεύνηση και ανάλυση της αρχιτεκτονικής που χρησιμοποιείται σε XDR (Extended Detection and Response) συστήματα. Έπειτα θα γίνει μια αναφορά και σύγκριση μεταξύ του παραδοσιακού τρόπου εντοπισμού και απόκρισης σε επιθέσεις και στους νέους τρόπους εντοπισμού και απόκρισης. Επιπλέον θα αναλυθεί εις βάθος το OpenC2 (Open Command and Control) πρωτόκολλο και το OVAL (Open Vulnerability and Assessment Language) προτύπου και το πως μπορούν να χρησιμοποιηθούν στην XDR αρχιτεκτονική. Και τέλος θα γίνει μια μελέτη εφαρμοσιμότητας του OpenC2 σε XDR αρχιτεκτονική στο πλαίσιο μια έξυπνης πόλης και σε ένα σενάριο κυβερνοεπίθεσης σε πληροφοριακά συστήματα της πόλης.

«Systems for identification and automated response to cyber-attacks: an applicability study of OpenC2 in XDR»

Christos Tsiligkaridis

Abstract

As the frequency and sophistication of cyber attacks continue to increase, organisations face unprecedented challenges in their efforts to ensure that their information and computing systems remain intact. The following dissertation will provide a comprehensive exploration and analysis of the architecture used in XDR (Extended Detection and Response) systems. Then a review and comparison will be made between the traditional way of detecting and responding to attacks and the new ways of detecting and responding. In addition, the OpenC2 (Open Command and Control) protocol and the OVAL (Open Vulnerability and Assessment Language) standard will be analyzed in depth and how they can be used in the XDR architecture. And finally a study will be done on the applicability of OpenC2 in XDR architecture in the context of a smart city and in a cyber attack scenario on city information systems.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή κ. Ηλιούδη για τις κατευθυντήριες γραμμές που βοήθησαν προς την ολοκλήρωση της πτυχιακής. Επίσης θα ήθελα να ευχαριστήσω όλους τους φίλους μου που με στήριξαν καθ' όλη την διάρκεια της εκπόνησης της πτυχιακής εργασίας.

Περιεχόμενα

Κατάλογος Σχημάτων

Συντομογραφίες

ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία
APT	Advanced Persistent Threat
SIEM	Security Information and Event Management
CTI	Cyber Threat Intelligence – Cyber Threat Information
OpenC2	Open Command and Control
OVAL	Open Vulnerability and Assessment Language
IAM	Identity and Access Management
VPN	Virtual Private Networks
AD	Active Directory
LDAP	Lightweight Directory Access Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
NAT	Network Address Translation
ERP	Enterprise Resource Planner
CRM	Custom Relationship Management
DLP	Data Loss Prevention
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
NAC	Network Access Controls
HIPS	Host Intrusion Prevention System
IP	Internet Protocol
TTPs	Tactics, Techniques and Procedures
NTA	Network Traffic Analysis
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DOS	Denial of Service
XML	Extended Markup Language

NSA	National Security Agency
PICERL	Preparation; Identification; Containment; Eradication; Recovery; Lessons Learned
XDR	Extended Detection and Response
SOAR	Security orchestration, automation and response
TIP	Threat Intelligence Platform
OASIS	Organization for the Advancement of Structured Information Standards
SOC	Security Operation Center

Κεφάλαιο 1ο: Εισαγωγή

1.1 Το πρόβλημα

Η διαρκής και ανελλιπώς εξέλιξη των απειλών και των επιθέσεων στον κυβερνοχώρο έχει δημιουργήσει σοβαρές προκλήσεις για τους οργανισμούς παγκοσμίως. Η αυξανόμενη πολυπλοκότητα αυτών των απειλών μπορεί να αποδοθεί σε διάφορους παράγοντες, συμπεριλαμβανομένης της ταχείας εξέλιξης της τεχνολογίας, της ευρείας υιοθέτησης συνδεδεμένων συσκευών και της ολοένα και μεγαλύτερης και αναπτυσσόμενης οικονομίας γύρω από το κυβερνοέγκλημα. Ως αποτέλεσμα, οι εγκληματίες του κυβερνοχώρου αναπτύσσουν πιο προηγμένες τακτικές και εργαλεία για να πετύχουν τους σκοπούς τους. Κάποιοι από τους σκοπούς τους μπορεί να είναι η αποκόμιση μεγάλων χρηματικών ποσών από ιδιώτες και οργανισμούς, η παράλυση κάποιον ή όλων των κρίσιμων υποδομών μιας χώρας, η κλοπή πνευματικής περιουσίας.

Ένα παράδειγμα της αυξημένης πολυπλοκότητας είναι η Προηγμένη Επίμονη Επίθεση (Advance Persistent Threat, APT). Συνήθως σε τέτοιες επιθέσεις τα άτομα που παίρνουν μέρος έχουν υψηλή εξειδίκευση στον τομέα της κυβερνοασφάλειας, των δικτύων υπολογιστών, των λειτουργικών συστημάτων και καλή γνώση προγραμματισμού. Συχνά αυτά τα άτομα υποστηρίζονται από κράτη για να εξαπολύσουν τις επιθέσεις τους σε άλλα κράτη ή μεγάλες εταιρείες που δραστηριοποιούνται σε άλλα κράτη. Αξιοσημείωτες APT επιθέσεις είναι η επίθεση με κωδική ονομασία "Επιχείρηση Ολυμπιακοί Αγώνες" ενάντια του πυρηνικού προγράμματος του Ιράν με την χρήση του computer worm ονόματι "Stuxnet"[1], όπου ξεκίνησε το 2005-2006 και ανακαλύφθηκε το 2010, η επίθεση στο Ουκρανικό δίκτυο ηλεκτρικής ενέργειας (Δεκέμβριος του 2015) με την χρήση του κακόβουλου λογισμικού "BlackEnergy 3"[2], όπως και η τεράστιας σε έκταση κυβερνοεπίθεση λυτρισμικού (ransomware) "Wannacry"[3] η οποία ξέσπασε τον Μάιο του 2017, προσβάλλοντας πάνω από 300,000 ηλεκτρονικούς υπολογιστές ανά τον κόσμο.

Για να αντιμετωπιστούν όλοι αυτοί οι κίνδυνοι και επιθέσεις στον χώρο της κυβερνοασφάλειας, ακαδημαϊκά ιδρύματα, ερευνητές και εταιρείες κυβερνοασφάλειας έχουν αναπτύξει μια πληθώρα από λύσεις. Οι "παραδοσιακές λύσεις κυβερνοασφαλείας" αποτελούσαν και αποτελούν τα κύρια εργαλεία που έχουν στην διάθεσή τους οι οργανισμοί έτσι ώστε να προστατευθούν από τις απειλές και τις επιθέσεις στον κυβερνοχώρο. Αυτές οι λύσεις συνήθως περιλαμβάνουν πλατφόρμες προστασίας τερματικών κόμβων (Endpoint Protection), τείχη προστασίας (Firewalls), συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) και συστήματα ανίχνευσης και πρόληψης εισβολών[4]. Οι παραδοσιακές αυτές λύσεις αν και έχουν ένα καλό ποσοστό αποτελεσματικότητας έναντι ορισμένων απειλών, αντιμετωπίζουν περιορισμούς και δυσκολίες στην αντιμετώπιση των πολύπλοκων και συνεχώς εξελισσόμενων απειλών και επιθέσεων στον κυβερνοχώρο. Οι κύριοι περιορισμοί που αντιμετωπίζουν είναι η ανίχνευση απειλών βάση προϋπάρχοντος μοτίβου απειλής, μεγάλο ποσοστό "ψευδών θετικών" (false positives) περιστατικών ασφαλείας, ανεπαρκείς ορατότητα και επίβλεψη στο τοπίο των απειλών σε ένα δίκτυο, η ανεπαρκείς εστίαση στην συμπεριφορά των χρηστών και σε συμπεριφορικά μοντέλα και φτωχή η ενοποίηση, αλληλοσυσχέτιση και συνεργασία μεταξύ όλων των παραδοσιακών λύσεων που υπάρχουν στο εκάστοτε δίκτυο.

1.2 Περιοχή Έρευνας

Τα τελευταία χρόνια τα πληροφοριακά συστήματα οργανισμών, εταιρειών, επιχειρήσεων, κρατών, ακαδημαϊκών ιδρυμάτων και ερευνητικών κέντρων δέχονται όλο ένα και περισσότερες

κυβερνοεπιθέσεις, οι οποίες τείνουν να είναι πιο πολύπλοκες και πιο αθόρυβες. Η συγκεκριμένη πτυχιακή εργασία θα επικεντρωθεί στην ανάλυση της αρχιτεκτονικής σε συστήματα προσδιορισμού και αυτοματοποιημένης απόκρισης σε περιστατικά ασφαλείας, στην ανάλυση της παραδοσιακής προσέγγισης για τον εντοπισμό απειλών και επιθέσεων και της παραδοσιακής απόκρισης σε αυτά και σε νέα πρωτόκολλα και πρότυπα που μπορούν να βοηθήσουν στην γρηγορότερη απόκριση σε κυβερνοεπιθέσεις. Η συνεχείς αλλαγές στις τακτικές και στα μοτίβα των επιθέσεων δεν αφήνουν χώρο για εφησυχασμό στην έρευνα γύρω από την κυβερνοασφάλεια και η ανάπτυξη και η εφαρμογή αποτελεσματικών τρόπων, μεθόδων, πρακτικών και τεχνολογιών για την προστασία πληροφοριακών συστημάτων είναι πιο επιτακτική από ποτέ άλλοτε.

1.3 Στόχοι

Η παρούσα πτυχιακή εργασία στοχεύει στην ενδελεχή μελέτη της αρχιτεκτονικής που διέπει τα XDR συστήματα και το πως η φιλοσοφία του XDR μπορεί να βελτιώσει την έγκυρη αναγνώριση των απειλών-επιθέσεων στο δίκτυο και την γρήγορη απόκριση σε περιστατικά ασφαλείας. Έπειτα, στην ανάδειξη των όποιων αδυναμιών των ήδη υπάρχων λύσεων κυβερνοασφάλειας στις όλο ένα και πιο πολύπλοκες και εξελισσόμενες απειλές-επιθέσεις στον κυβερνοχώρο και πως η ολιστικπροσέγγιση που προσφέρει η XDR αρχιτεκτονική μπορεί να εμπλουτίσει σε μεγάλο βαθμό την ασφάλεια ενός δικτύου και συνάμα ενός οργανισμού. Επιπλέον, πως χρησιμεύει το πρωτόκολλο OpenC2 και το πρότυπο OVAL στις λύσεις κυβερνοασφάλειας και ιδιαίτερα στην XDR αρχιτεκτονική. Τέλος, μια μελέτη εφαρμοσιμότητας του OpenC2 στην XDR αρχιτεκτονική και θα ακολουθήσει μια ολοκληρωμένη ανάλυση σεναρίου, η οποία θα καταδεικνύει την χρήση του OpenC2 για την αντιμετώπιση ενός περιστατικού ασφαλείας σε μια πολύπλοκη υποδομή μιας έξυπνης πόλης.

1.4 Επιτεύγματα

Η παρούσα πτυχιακή εργασία συνεισφέρει στην κατανόηση της αρχιτεκτονικής XDR μέσω της διεξοδικής ανάλυσης των στοιχείων και των τεχνολογιών που την απαρτίζουν. Κάνει σαφής τους προβληματισμούς και τα προβλήματα γύρω από τους παραδοσιακούς τρόπους ανίχνευσης και απόκρισης σε περιστατικά ασφαλείας και αναδεικνύει νέους τρόπους οι οποίοι βοηθούν στην αποτελεσματικότερη ανίχνευση, απόκριση και διαχείριση περιστατικών ασφαλείας. Επιπλέον αναλύει εις βάθος το πρωτόκολλο OpenC2 και το πρότυπο OVAL με τέτοιον τρόπο που αναδεικνύονται οι δυνατότητες που έχουν όταν χρησιμοποιούνται. Και τέλος μέσω της μελέτης περίπτωσης γίνονται σαφείς οι ανάγκες για την χρησιμοποίηση συστημάτων όπως το XDR και δίνεται ένα πλαίσιο κάτω από το οποίο δίνατε να λειτουργήσει το OpenC2 πρωτόκολλο.

1.5 Διάρθρωση πτυχιακής

Η δομή της παρούσας πτυχιακής εργασίας έχει ως εξής. Στο πρώτο κεφάλαιο το οποίο είναι εισαγωγικό, εξηγείτε το πρόβλημα πάνω στο οποίο εξετάζονται λύσεις και περιγράφονται οι στόχοι που θέτονται για την πορεία της πτυχιακής εργασίας. Στο δεύτερο κεφάλαιο γίνεται ανάλυση της XDR (eXtended Detection and Response) αρχιτεκτονικής σε βάθος, αναλύοντας τις πηγές δεδομένων και το πως γίνεται η συλλογή από αυτές, η ανάλυση των δεδομένων έτσι ώστε να γίνει ο εντοπισμός κάποιας πιθανής επίθεσης, η αυτοματοποιημένες ενέργειες που γίνονται σε περίπτωση περιστατικού ασφαλείας, ο ρόλος των Πληροφοριών για Κυβερνοαπειλές (Cyber Threat Intelligence – CTI) σε μια XDR αρχιτεκτονική, το πως γίνεται η ενσωμάτωση (integration) από ήδη υπάρχοντα συστήματα και λύσεις ασφαλείας και τέλος πως η οπτικοποίηση και η απεικόνιση των περιστατικών ασφαλείας βοηθάει του αναλυτές. Στο τρίτο κεφάλαιο γίνεται η ανάλυση του παραδοσιακού τρόπου εντοπισμού

και απόκρισης σε συμβάντα όταν αυτό γίνεται χωρίς την ενσωμάτωση του XDR και έπειτα πως οι νέες τεχνολογίες μπορούν να εμπλουτίσουν σημαντικά το πεδίο του γρήγορου εντοπισμού και απόκρισης. Στο τέταρτο κεφάλαιο γίνεται η ανάλυση του OpenC2 (Open Command and Control) πρωτοκόλλου και του OVAL (Open Vulnerability and Assessment Language) προτύπου. Στο πέμπτο κεφάλαιο πραγματοποιείτε μια μελέτη εφαρμοσιμότητας για την χρησιμοποίηση του OpenC2 πρωτοκόλλου στην αρχιτεκτονική του XDR. Τέλος, στο έκτο κεφάλαιο ακολουθούν τα συμπεράσματα και οι προτεινόμενες μελλοντικές επεκτάσεις της πτυχιακής εργασίας.

Κεφάλαιο 2ο: Σύστημα προσδιορισμού και αυτόματης απόκρισης σε κυβερνοεπιθέσεις – XDR (eXtended Detection and Response)

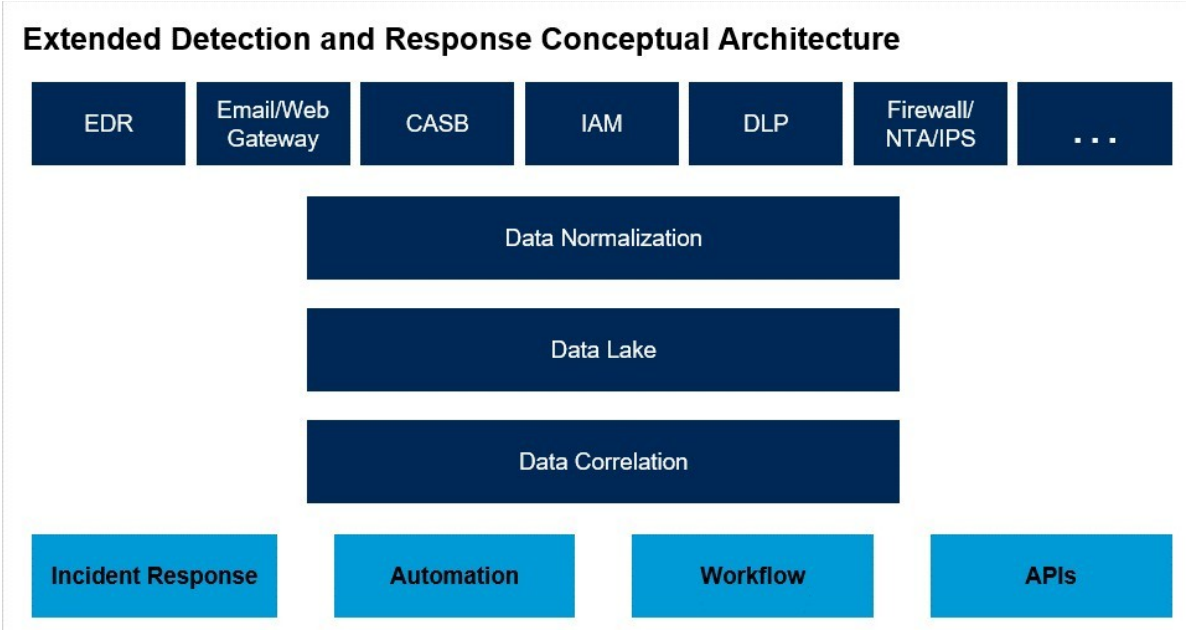
2.1 Εισαγωγή στο XDR και στην αρχιτεκτονική του

Ο όρος Εκτεταμένη Ανίχνευση και Απόκριση (XDR – eXtended Detection and Response) πρωτοεμφανίζεστε το 2018 από τον επικεφαλή τεχνολογίας, Νιρ Ζούκ (Nir Zuk), της εταιρείας Palo Alto Networks κατά την διάρκεια της ομιλίας του στο συνέδριο "Ignite". Κατά την διάρκεια της παρουσίασης γίνεται αναφορά ότι το γράμμα "X" στο ακρωνύμιο "XDR" σημαίνει "τα πάντα/οτιδήποτε", δηλαδή ανίχνευση και απόκριση σε όλα τα σημεία του δικτύου[5]. Από εκεί και πέρα πολλές συζητήσεις έχουν υπάρξει από επαγγελματίες στον χώρο της κυβερνοασφάλειας ως προς τον ορισμό του όρου "XDR". Για κάποιους είναι η συλλογή και συγκέντρωση δεδομένων από τα ήδη υπάρχοντα προϊόντα ασφαλείας που έχουν αναπτυχθεί στο δίκτυο, ο εμπλουτισμός τους με δεδομένα από ροές Πληροφοριών για Κυβερνοαπειλές (CTI feeds), η ανάλυση τους με την δυνατότητα μηχανικής μάθησης και χρήση τεχνητής νοημοσύνης και τελικός η δυνατότητα αυτοματοποιημένης απόκρισης σε περιστατικά ασφαλείας. Για άλλους είναι μια ευρύτερη προσέγγιση για αποδοτικότερη συλλογή δεδομένων, έρευνα, απόκριση σε περιστατικά ασφαλείας και κυνήγι απειλών. Σαφής ορισμός και επεξήγηση του όρου "XDR" δεν υπάρχει και έτσι για την συγκεκριμένη πτυχιακή εργασία θα ορίσουμε τον όρο "XDR" όπως τον ορίζει η εταιρεία Forrester Research, "XDR είναι η εξέλιξη του EDR, που βελτιστοποιεί την ανίχνευση, τη διερεύνηση, την απόκριση και το κυνήγι απειλών σε πραγματικό χρόνο. Το XDR ενοποιεί την ανίχνευση περιστατικών ασφαλείας από τερματικούς κόμβους μέσω της τηλεμετρίας από εργαλεία ασφάλειας και επιχειρηματικά εργαλεία, όπως ηλεκτρονικό ταχυδρομείο, διαχείριση ταυτότητας και πρόσβασης (Identity and Access Management – IAM), δίκτυο, νέφος και άλλα. Πρόκειται για μια εγγενής πλατφόρμα νέφους χρησιμοποιώντας υποδομές μεγάλων δεδομένων (Big Data) για να παρέχει στις ομάδες κυβερνοασφάλειας μεγαλύτερες δυνατότητες ευελιξίας, επεκτασιμότητας, ανίχνευσης και δυνατότητες αυτοματισμού."[6].

Επίσης η αρχιτεκτονική που χρησιμοποιούν διάφορες εταιρείες που αναπτύσσουν συστήματα προσδιορισμού και αυτόματης απόκρισης σε κυβερνοεπιθέσεις (XDR) μπορεί να διαφέρει ανάλογα την εταιρεία αλλά στο γενικό πλαίσιο η αρχιτεκτονική των XDR συστημάτων δομείτε από τα παρακάτω στοιχεία/συστατικά:

- Συλλογή δεδομένων: Η συλλογή δεδομένων από πληθώρα πηγών μέσα από το δίκτυο του οργανισμού.
- Επεξεργασία δεδομένων: Περιλαμβάνεται η κανονικοποίηση, ο καθαρισμός και ο εμπλουτισμός των δεδομένων με στόχο να καταστούν έτοιμα για ανάλυση.
- Ανάλυση δεδομένων: Η ανάλυση των δεδομένων για τον εντοπισμό κακόβουλης συμπεριφοράς μέσω τεχνικών που συμπεριλαμβάνουν τεχνική νοημοσύνη, μηχανική μάθηση και κανόνες.
- Απόκριση σε περιστατικό ασφαλείας: Εφόσον μια κακόβουλη συμπεριφορά έχει ανιχνευτεί και υπάρχει περιστατικό ασφαλείας, έπεται και η απόκριση σε αυτό.

- Ροές Πληροφοριών για Κυβερνοεπιθέσεις: Εκμετάλλευση των Πληροφοριών για Κυβερνοεπιθέσεις έτσι ώστε να καταστεί ο εντοπισμός και η απόκριση σε κυρβενοεπιθέσεις πιο αποτελεσματικός
- Ενσωμάτωση: Η ενσωμάτωση επιτρέπει στα XDR συστήματα να αξιοποιούν δεδομένα από διάφορες λύσεις ασφαλείας έτσι ώστε να παρέχουν μια πιο ολοκληρωμένη εικόνα για την κατάσταση ασφαλείας ενός οργανισμού.
- Οπτικοποίηση: Η οπτικοποίηση μέσω διαδραστικών πινάκων ελέγχου για τον γρήγορο εντοπισμό και την γρήγορη διερεύνηση πιθανών περιστατικών ασφαλείας από τους αναλυτές κυβερνοασφάλειας.



Σχήμα 2.1.1: Αφαιρετικός σχεδιασμός της αρχιτεκτονικής XDR [52]

2.2 Πηγές δεδομένων και συλλογή από αυτές

Όπως κάθε σύστημα που χρησιμοποιεί αρχεία καταγραφής (logs) από άλλα συστήματα ασφαλείας, έτσι και οι XDR λύσεις χρειάζονται αρχεία καταγραφής από διάφορα συστήματα που έχουν αναπτυχθεί στο δίκτυο. Μερικές από τις πηγές δεδομένων που μπορεί να αντλήσει δεδομένα είναι:

- Ηλεκτρονικό ταχυδρομείο
- Πηγές αυθεντικοποίησης (π.χ VPN, AD, LDAP)
- Διακομιστές ιστού (π.χ IIS, Apache, Tomcat)
- Δικτυακές συσκευές (π.χ Router, Switch)
- Δικτυακές υπηρεσίες (π.χ DHCP, NAT, DNS)
- Εφαρμογές επιχειρήσεων (π.χ ERP, CRM)
- Έλεγχοι ασφαλείας (π.χ Firewall, DLP, NAC, IPS, IDS)
- Ασφάλεια τερματικών κόμβων (π.χ Antivirus, HIPS, EDR)

Οι παραπάνω πηγές δεδομένων για το XDR είναι μέρος της πολυεπίπεδης λογικής που εφαρμόζει το μοντέλο "Άμυνα εις βάθος"[72]. Το μοντέλο "Άμυνα εις βάθος" είναι μια στρατηγική κυβερνοασφάλειας που περιλαμβάνει την ανάπτυξη πολλαπλών επιπέδων ελέγχων ασφαλείας με σκοπό την προστασία των πληροφοριακών συστημάτων ενός οργανισμού. Τα XDR συστήματα διαδραματίζουν σημαντικό ρόλο σε αυτό το μοντέλο, διότι συγκεντρώνουν και συσχετίζουν δεδομένα από όλα τα επίπεδα του μοντέλου για να παρέχουν μια ολοκληρωμένη και ολιστική εικόνα σε όλα τα σημεία/επίπεδα του δικτύου ενός οργανισμού.

Σχήμα 2.2.1: Μοντέλο "Άμυνα εις βάθος" [53]

2.3 Επεξεργασία δεδομένων

Σε αυτή την ενότητα θα αναλυθούν οι τρόποι με τους οποίους γίνεται η επεξεργασία των δεδομένων από τα XDR συστήματα, έτσι ώστε τα δεδομένα να έρθουν στην κατάλληλη μορφή για ανάλυση από τους κατάλληλους μηχανισμούς.

2.3.1 Κανονικοποίηση δεδομένων

Η κανονικοποίηση των δεδομένων σε όσα συστήματα παίρνουν δεδομένα από πολλαπλά και διαφορετικά συστήματα είναι κάτι το απαραίτητο.[7][8] Η κανονικοποίηση διευκολύνει σε μεγάλο βαθμό τη σύγκριση και την ανάλυση δεδομένων από διαφορετικές πήγες που παραδίδουν δεδομένα σε διαφορετική μορφή. Αυτό επιτυγχάνετε μέσω της μετατροπής των συλλεχθέντων δεδομένων σε μια κοινή μορφή, μορφή που θα καταλαβαίνει το σύστημα που πρόκειται να τα αναλύσει, έτσι ώστε να

εντοπίσει μοτίβα επιθέσεων και να ανιχνεύσει ανωμαλίες σε διάφορα συμβάντα κυβερνοασφάλειας. [7]

Η κανονικοποίηση των δεδομένων είναι ζωτικής σημασίας για τα συστήματα ανίχνευσης και απόκρισης σε κυβερνοεπιθέσεις, κυρίως για την διασφάλιση της συγκρισιμότητας των δεδομένων από διαφορετικές πηγές, προκειμένου να αναλύουν και να επεξεργάζονται δεδομένα με συνεκτικό τρόπο. Τα δεδομένα από διαφορετικές πηγές, όπως αρχεία καταγραφής, η κίνηση του δικτύου και συμβάντα τερματικών κόμβων, μπορούν να διαφέρουν ως προς τη δομή, τη μορφή και την ποιότητά τους.[7] Έτσι, μέσω της κανονικοποίησης των δεδομένων, οι διαφορές αυτές μπορούν να αμβλυνθούν σε μεγάλο βαθμό, επιτρέποντας στα συστήματα ανίχνευσης και απόκρισης να συγκρίνουν και να αναλύουν αποτελεσματικότερα τα δεδομένα που δέχονται.

Επιπλέον, η κανονικοποίηση των δεδομένων διαδραματίζει επίσης σημαντικό ρόλο στην βελτίωση της ποιότητας των δεδομένων με την τυποποίηση της αναπαράστασης των δεδομένων, την μείωση των διπλοεγγραφών, δηλαδή την μείωση των ίδιων δεδομένων που αναπαριστούνται με διαφορετική μορφή, και την εξάλειψη στις όποιες ασυμφωνίες υπάρχουν μεταξύ των δεδομένων. Η διαδικασία αυτή διασφαλίζει ότι τα δεδομένα θα είναι ακριβή, αξιόπιστα και συνεπή, γεγονός που ενισχύει τις δυνατότητες ανίχνευσης και απόκρισης στα συστήματα ασφαλείας. Ακόμα, η κανονικοποίηση συμβάλει στον εξορθολογισμό την επεξεργασίας των δεδομένων, επιτρέποντας στα συστήματα κυβερνοασφάλειας να επεξεργάζονται τα δεδομένα πιο αποτελεσματικά. Η διαδικασία αυτή μειώνει σημαντικά την πολυπλοκότητα της ανάλυσης δεδομένων και μπορεί να συμβάλει στην βελτίωση της απόδοσης και χρήση των υπολογιστικών πόρων στα συστήματα κυβερνοασφάλειας.[8]

Οι **τρόποι** με τους οποίους μπορεί να γίνει κανονικοποίηση των δεδομένων είναι διάφοροι και μπορούν να διαφέρουν ανάλογα με το σύστημα που θα τα δεχτεί ή το σύστημα που θα τα παράξει. Κάποιο κύριοι τρόποι είναι το φιλτράρισμα, η ανάλυση (parsing) και ο εμπλουτισμός των ακατέργαστων δεδομένων. Αυτοί οι τρόποι διασφαλίζουν ότι τα δεδομένα θα μετατραπούν σε μια τυποποιημένη και σωστά δομημένη μορφή που μπορεί να αναλυθεί και να επεξεργαστεί αποτελεσματικά.

Ανάλυση(parsing). Η ανάλυση περιλαμβάνει την εξαγωγή πληροφοριών από τα ακατέργαστα δεδομένα και την μετατροπή τους σε μια δομημένη μορφή. Οι αναλυτές (parsers) έχουν σχεδιαστεί με τέτοιο τρόπο για να κατανοούν συγκεκριμένες μορφές δεδομένων και να εξάγουν στοιχεία κλειδιά από τα δεδομένα. Για παράδειγμα, οι αναλυτές (parsers) αρχείων καταγραφής μπορούν να εξάγουν πεδία όπως, χρονοσφραγίδες, τύπους συμβάντων, αναγνωριστικά χρηστών όπως ψευδώνυμο και διευθύνσεις IP αποστολέα και προορισμού. Οι τεχνικές ανάλυσης μπορεί να ποικίλλουν ανάλογα με την πηγή δεδομένων, για παράδειγμα:

- Κανονικές εκφράσεις: Οι κανονικές εκφράσεις χρησιμοποιούνται για την εξαγωγή πληροφοριών από μη δομημένα δεδομένα με την χρήση ειδικά διαμορφωμένων μοτίβων. Όταν το εκάστοτε μοτίβο που έχουμε δημιουργήσει βρεθεί μέσα στα δεδομένα, εξάγετε η πληροφορία που ταιριάξει με το μοτίβο.
- Ανάλυση (parsing) βάση την γραμματική: Αυτοί οι αναλυτές (parsers) χρησιμοποιούν γραμματικούς κανόνες για τον εντοπισμό και την εξαγωγή συγκεκριμένων στοιχείων από μη δομημένες μορφές δεδομένων.[13] Αυτοί οι αναλυτές μπορούν να χειριστούν και εμφωλευμένες δομές δεδομένων και έτσι μπορούν να παρέχουν μια πιο αποτελεσματική ανάλυση σε σχέση με τις κανονικές εκφράσεις.

- Εξατομικευμένοι αναλυτές (parsers): Οι εξατομικευμένοι αναλυτές προσαρμόζονται σε συγκεκριμένες μορφές και δομές δεδομένων, παρέχοντας μια βελτιστοποιημένη λύση ανάλυσης για τυχόν υπάρχουσες μοναδικές πηγές δεδομένων. Αυτοί οι αναλυτές συνήθως σχεδιάζονται και υλοποιούνται από οργανισμούς ή από τους ίδιους τους δημιουργούς των μοναδικών πηγών με σκοπό να αντιμετωπίσουν τις συγκεκριμένες απαιτήσεις που δημιουργούνται για την ανάλυση των δεδομένων.

Ένας άλλος τρόπος είναι το **φιλτράρισμα**. Το φιλτράρισμα είναι η τεχνική αφαίρεσης άσχετων ή περιττών δεδομένων, η οποία συμβάλει αισθητά στη μείωση του όγκου των προς ανάλυση δεδομένων και βελτιώνει την αποδοτικότητα του συστήματος. Οι τεχνικές φιλτραρίσματος μπορεί να περιλαμβάνουν την αφαίρεση των διπλοεγγραφών, την χρήση λευκών ή μαύρων λιστών, τον αποκλεισμό συγκεκριμένων τύπων δεδομένων και τον αποκλεισμό συγκεκριμένων τύπων συμβάντων τα οποία δεν σχετίζονται με την κυβερνοασφάλεια. Το φιλτράρισμα μπορεί να γίνει με διάφορους τρόπους, όπως:

- Φιλτράρισμα βάσει κανόνων: Το φιλτράρισμα βάσει κανόνων περιέχει τον ορισμό συγκεκριμένων συνθηκών που πρέπει να πληρούνται για να αποκλειστούν ή να συμπεριληφθούν τα δεδομένα στην ανάλυση. Οι συνθήκες αυτές μπορεί να βασίζονται για παράδειγμα σε χαρακτηριστικά όπως διεύθυνση IP προορισμού και αποστολέα ή το security event ID. Αυτή η τεχνική δίνει στους οργανισμούς το πλεονέκτημα να επιλέξουν τα δεδομένα που είναι σημαντικά για τις ανάγκες ασφαλείας τους.
- Φιλτράρισμα με την βοήθεια μηχανικής μάθησης: Η χρήση αλγορίθμων μηχανικής μάθησης μπορούν να χρησιμοποιηθούν για τον εντοπισμό μοτίβων στα δεδομένα και έτσι να γίνει αυτόματη η διαδικασία του φιλτραρίσματος άσχετων ή περιττών πληροφοριών. Αυτοί οι αλγόριθμοι έχουν την δυνατότητα να μαθαίνουν από ιστορικά δεδομένα και προηγούμενες παρατηρήσεις στο δίκτυο και έτσι μπορούν να προσαρμόζουν τα κριτήρια φιλτραρίσματός τους βάσης των αλλαγών που παρατηρούν.

Έχοντας κατά νου όσα αναφέρθηκαν παραπάνω για την κανονικοποίηση δεδομένων και την πληθώρα ελέγχων ασφαλείας που τροφοδοτούν με δεδομένα, καταλαβαίνουμε τις διάφορες προκλήσεις που μπορούν να προκύψουν. Μερικές απ’ αυτές είναι:

- Η πολυπλοκότητα των πηγών δεδομένων: Με τον όλο ένα και αυξανόμενο αριθμό πηγών δεδομένων στα σύγχρονα συστήματα κυβερνοασφάλειας, η ανάλυση και η κανονικοποίηση των δεδομένων γίνεται όλο και πιο πολύπλοκη. Κάθε πηγή δεδομένων μπορεί να έχει τη δική της μοναδική μορφή, δομή και σημασιολογία, γεγονός που κάνει πιο επιτακτική την ανάπτυξη και συντήρηση εξατομικευμένων αναλυτών (custom parsers) και κανόνων κανονικοποίησης.
- Η ποιότητα των δεδομένων: Η ποιότητα των ακατέργαστων δεδομένων μπορεί να επηρεάσει σημαντικά την διαδικασία κανονικοποίησης των δεδομένων. Ατελή, ανακριβής ή ασυνεπής δεδομένα μπορεί να οδηγήσουν σε εσφαλμένη ανάλυση και να εμποδίσουν τα συστήματα ασφαλείας να ανιχνεύσουν και να ανταποκριθούν σε απειλές ή επιθέσεις αποτελεσματικά.
- Επιδόσεις και επεκτασιμότητα: Οι σημερινοί οργανισμοί συλλέγουν ολοένα και περισσότερα και πιο πολύπλοκα δεδομένα. Έτσι, η απόδοση και η επεκτασιμότητα των διαδικασιών που σχετίζονται με την κανονικοποίηση καθίστανται καίριας σημασίας. Οι απαραίτητες τεχνικές κανονικοποίησης πρέπει να είναι αποτελεσματικές για να διασφαλίζετε ότι τα συστήματα που επεξεργάζονται και αναλύουν τα δεδομένα, θα κάνουν εγκαίρως τις απαραίτητες ενέργειες

χωρίς μεγάλους χρόνους καθυστέρησης και χωρίς να υπερφορτώνουν τους διαθέσιμους πόρους του συστήματος.

Τέλος, η κανονικοποίηση των δεδομένων στα XDR συστήματα είναι πολλή σημαντική για την σωστή ανάλυση τους από τις μηχανές ανάλυσης και την εύρυθμη λειτουργία της XDR αρχιτεκτονικής. Αναλύοντας τα επιμέρους στάδια της επεξεργασίας των δεδομένων όπως η κανονικοιποίηση, ο συσχετισμός των δεδομένων και ο εμπλουτισμός των δεδομένων μπορούμε να καταλάβουμε τον κρίσιμο ρόλο που διαδραματίζουν για τον σωστό εντοπισμό απειλών και επιθέσεων στο δίκτυο ενός οργανισμού.

2.3.2 Συσχέτιση δεδομένων

Η συσχέτιση δεδομένων διαδραματίζει κρίσιμο ρόλο στην ανάλυση περιστατικών ασφαλείας στις λύσεις κυβερνοασφάλειας. Η συσχέτιση δεδομένων περιλαμβάνει τον εντοπισμό μοτίβων και σχέσεων μεταξύ διαφορετικών δεδομένων, επιτρέποντας στα συστήματα κυβερνοασφάλειας να αποκτούν μια ολοκληρωμένη εικόνα των πιθανών απειλών μέσα στο δίκτυο. Η συσχέτιση δεδομένων είναι ιδιαίτερα σημαντική στα συστήματα XDR, όπου τα δεδομένα από πολλαπλές και διάφορες πηγές πρέπει να αναλυθούν με συνεκτικό τρόπο έτσι ώστε η διερεύνηση, ο εντοπισμός και η αντιμετώπιση απειλών να γίνουν γρηγορότερα και αποτελεσματικότερα.

Η συσχέτιση δεδομένων μπορεί να βοηθήσει στην ενίσχυση των δυνατοτήτων για την ανίχνευση απειλών στα συστήματα κυβερνοασφάλειας. Με τον κατάλληλο συσχετισμό δεδομένων τα συστήματα ασφαλείας θα έχουν την δυνατότητα να ανιχνεύσουν σύνθετες και πολύπλοκες απειλές που μπορεί να μην είναι διακριτές κατά την ανάλυση μεμονωμένων δεδομένων. Έτσι, ο οργανισμός θα είναι σε θέση να κατανοήσει το τοπίο απειλών σε βάθος κάτι που οδηγεί στην ακριβέστερη και αποτελεσματικότερη ανίχνευση απειλών. Επίσης, η αποτελεσματική συσχέτιση δεδομένων μπορεί να συμβάλει στην μείωση των ψευδών θετικών και ψευδών αρνητικών αποτελεσμάτων στα συστήματα κυβερνοασφάλειας.[9][10] Με τον έγκαιρο εντοπισμό μοτίβων μεταξύ διαφορετικών δεδομένων, οι τεχνικές συσχέτισης μπορούν να φιλτράρουν άσχετα συμβάντα ή συμβάντα που δεν είναι κακόβουλα, μειώνοντας έτσι τα ψευδώς θετικά περιστατικά κυβερνοασφάλειας.

Οι τρόποι και οι τεχνικές συσχέτισης δεδομένων μπορούν σε γενικές γραμμές να κατηγοριοποιηθούν σε:

- Συσχέτιση βάσει κανόνων
- Συσχέτιση μέσω στατιστικών μεθόδων
- Συσχέτιση βάσει μηχανικής μάθησης

Αυτές οι τεχνικές αποσκοπούν στον εντοπισμό μοτίβων και σχέσεων μεταξύ διαφορετικών δεδομένων με στόχο την ενίσχυση των δυνατοτήτων ανάλυσης, ανίχνευσης και απόκρισης σε απειλές από τα συστήματα κυβερνοασφάλειας.

Η **συσχέτιση βάσει κανόνων** μπορεί να περιλαμβάνει τη χρήση προκαθορισμένων κανόνων ή συνθηκών με σκοπό τον εντοπισμό σχέσεων μεταξύ συμβάντων ασφαλείας.[10] Αυτό μπορεί να γίνει με απλές αντιστοιχίσεις μέσω της σύγκρισης στοιχείων βάση συγκεκριμένων χαρακτηριστικών, όπως για παράδειγμα τις διευθύνσεις IP προορισμού και αποστολέα. Επίσης μπορεί να γίνει συσχέτιση βάση την συχνότητα ή τον όγκο εμφάνισης κάποιον στοιχείων. Για παράδειγμα, ένας κανόνας που θα μας ειδοποιεί όταν οι αποτυχημένες προσπάθειες σύνδεσης στο εταιρικό δίκτυο από έναν χρήστη

εντός ενός χρονικού πλαισίου υπερβούν ένα συγκεκριμένο αριθμό που έχουμε θέσει εμείς ως ανώτατο όριο.

Η **τεχνικές μέσω στατιστικών μεθόδων** αξιοποιούν μαθηματικές και στατιστικές μεθόδους για τον εντοπισμό μοτίβων και σχέσεων στα δεδομένα.[11] Αυτές οι τεχνικές μπορούν να προσφέρουν μια προσέγγιση βασισμένη στα δεδομένα και πιο αντικειμενική σε σύγκριση με τις μεθόδους που βασίζονται σε κανόνες όπως αναφέραμε παραπάνω. Ένα παράδειγμα είναι η ανίχνευση ανωμαλιών στο δίκτυο. Για τον εντοπισμό ασυνήθιστων μοτίβων και σχέσεων στα δεδομένα μπορούν να επιστρατευθούν τεχνικές όπως η ομαδοποίηση ή η ανάλυση ακραίων τιμών. Αυτές οι τεχνικές μπορούν να βοηθήσουν στην ανακάλυψη απειλών που δεν έχουν ανιχνευθεί κατά τον παρελθόν ή συμβάντων που αποκλίνουν σημαντικά από τον κανόνα μια επίθεσης, κάτι τέτοιο συμβαίνει και με τις ολοένα και πιο περίπλοκες και πολυσύνθετες κυβερνοεπιθέσεις.

Επίσης, οι **τεχνικές συσχέτισης που βασίζονται στην μηχανική μάθηση** αξιοποιούν προηγμένους αλγορίθμους για τον αυτόματο εντοπισμό μοτίβων και σχέσεων μεταξύ των δεδομένων.[12] Αυτές οι τεχνικές μπορούν να προσαρμόζονται στις αλλαγές των δεδομένων με μεγάλο βαθμό επιτυχίας, επιτρέποντάς τους να βελτιώνουν τα μοντέλα συσχέτισής τους και συνάμα να βελτιώνουν τις δυνατότητές τους στην ανίχνευση απειλών με την πάροδο του χρόνου. Για παράδειγμα, οι αλγόριθμοι εποπτευόμενης μάθηση, όπως τα δέντρα αποφάσεων, οι μηχανές διανυσμάτων ή τα νευρωνικά δίκτυα μπορούν να εκπαιδευτούν σε ήδη κατηγοριοποιημένα δεδομένα για τον εντοπισμό μοτίβων ή σχέσεων μεταξύ των δεδομένων. Έπειτα αυτά τα μοντέλα εφόσον έχουν περάσει την φάση της μάθησης, μπορούν να χρησιμοποιηθούν για να κατηγοριοποιήσουν νέα δεδομένα που δεν έχουν πρότερα κατηγοριοποιηθεί.

Τέλος, όπως καταλαβαίνουμε η συσχέτιση δεδομένων είναι ένα πολύ σημαντικό κομμάτι της επεξεργασίας των δεδομένων στα συστήματα ασφαλείας και δει στα συστήματα XDR. Καθώς οι επιτιθέμενοι προσαρμόζουν και αλλάζουν συνεχώς τις τακτικές, τις τεχνικές και τις διαδικασίες τους (TTPs)[73], τα μοντέλα συσχέτισης πρέπει να μπορούν να ακολουθούν με επιτυχία αυτές τις αλλαγές κρατώντας σε υψηλό επίπεδο την αποτελεσματικότητά τους ως προς τον εντοπισμό και την ανίχνευση αυτών των απειλών. Η επεξεργασία των δεδομένων είναι άρρηκτα συνδεδεμένη με την ασφάλεια των οργανισμών. Δεδομένα που έχουν υποστεί σωστή επεξεργασία θα βοηθήσουν στην γρηγορότερη και αποτελεσματικότερη ανάλυση δεδομένων και έπειτα στην έγκυρη ανίχνευση απειλών έτσι ώστε οι οργανισμοί να χτίσουν μια δυνατότερη άμυνα απέναντι σε όλο και πιο εξελιγμένες απειλές και επιθέσεις.

2.4 Ανάλυση δεδομένων / Ανίχνευση απειλών

Καθώς συνεχίζουμε το ταξίδι μας στην αρχιτεκτονική που διέπει τα XDR συστήματα, επόμενος μας σταθμός είναι η ανάλυση δεδομένων και ανίχνευση απειλών (Analytics and Detection). Όσο οι επιθέσεις και οι απειλές γίνονται πιο περίπλοκες και περνούν απαρατήρητες από τα συστήματα ασφαλείας, τόσο η ανάγκη για προηγμένες μεθόδους και μηχανισμούς ανίχνευσης απειλών θα γίνεται πιο επιτακτική. Ο ρόλος την ανάλυσης (Analytics) είναι ύψιστης σημασίας για την διάκριση ανωμαλιών, τον έγκυρο εντοπισμό πιθανών απειλών και επιθέσεων και εν τέλει στην κατανόηση της φύσης αυτών των απειλών. Αυτό μας οδηγεί στην ανίχνευση απειλών. Η ανίχνευση απειλών σε ένα XDR πλαίσιο, δύναται να χαρακτηριστεί η μίξη από κλασικές μεθόδους ανίχνευσης απειλών (π.χ βάσει υπογραφών, ευρετική ανάλυση) και πιο προηγμένων μεθόδων (π.χ ανίχνευση ανωμαλιών με χρήση τεχνητής νοημοσύνης και μηχανικής μάθησης καθολικά). Σύμφωνα με έκθεση της IBM, οι οργανισμοί που έχουν αναπτύξει XDR ανιχνεύουν την παραβίαση έναν μήνα νωρίτερα, κατά μέσο

όρο, σε σχέση με τους οργανισμούς που δεν διαθέτουν XDR. Συγκεκριμένα 275 μέρες για την ανίχνευση παραβίασης όσων χρησιμοποιούν XDR και 304 μέρες για την ανίχνευση παραβίασης όσων δεν χρησιμοποιούν XDR.[14]

2.4.1 Ανίχνευση βάσει υπογραφών (Signature-Based Detection)

Ακόμα και στον κόσμο του XDR, παλιές, χιλιοδουλεμένες και έμπιστες τεχνικές ανίχνευσης απειλών συνεχίζουν να υπάρχουν και στην περίπτωση αυτή μιλάμε για την ανίχνευση βάσει υπογραφών. Η ανίχνευση βάσει υπογραφών είναι μια τεχνική που εντοπίζει κακόβουλο λογισμικό μέσω της σύγκρισης κάποιον χαρακτηριστικών ενός αρχείου ή ακόμα και της δραστηριότητας του δικτύου, με μια βάση δεδομένων γνωστών μοτίβων που έχουν σχέσει με κακόβουλες ενέργειες. Αυτά τα μοτίβα ή αλλιώς "υπογραφές", είναι μοναδικά χαρακτηριστικά που σχετίζονται με συγκεκριμένους τύπους κακόβουλων λογισμικών (π.χ keylogger)[15].

Όταν ένα αρχείο εισέρχεται στο δίκτυο, το σύστημα ανίχνευσης βάσει υπογραφών σαρώνει το εισερχόμενο αρχείο συγκρίνοντάς το με τις υπογραφές που έχει στην βάση δεδομένων του. Αν υπάρξει κάποια αντιστοίχιση, το σύστημα στιγματίζει το αρχείο ως κακόβουλο και αντιδράει σε αυτό ειδοποιώντας τον χρήστη για την ύπαρξη κακόβουλου λογισμικού[16].

Η βάση δεδομένων υπογραφών είναι το βασικό συστατικό του συστήματος. Αυτή η βάση δεδομένων είναι μια ολοκληρωμένη και καλά δομημένη συλλογή υπογραφών κακόβουλου λογισμικού, η οποία ενημερώνετε συνεχώς από πωλητές προϊόντων κυβερνοασφάλειας (π.χ Kaspersky, ESET, κλπ).

Η διαδικασία της δημιουργίας μια υπογραφής είναι δύσκολη και επιχειρείται από έμπειρους αναλυτές και ερευνητές κακόβουλων λογισμικών (malware analysts) οι οποίοι έχουν την γνώση να αποδομήσουν ένα κακόβουλο λογισμικό και να βγάλουν συμπεράσματα για το πως λειτουργεί. Έτσι, μετά την αναγνώριση των μοναδικών χαρακτηριστικών ή μοτίβων του εκάστοτε κακόβουλου λογισμικού, συγκεντρώνουν τα ευρήματά τους σε μια υπογραφή. Έπειτα αυτή η νέα υπογραφή που δημιούργησαν θα προστεθεί στον μακρύ κατάλογο της βάσης δεδομένων με τις γνωστές υπογραφές, έτσι ώστε να μπορέσει να ανιχνευθεί και σε άλλα συστήματα[17].

2.4.2 Ανίχνευση μέσω Ευρετικής Ανάλυσης (Heuristic Analysis)

Ακόμη μία μέθοδος που χρησιμοποιούταν πριν την έλευση του XDR και ενσωματώνεται και αυτή στο οπλοστάσιο της XDR αρχιτεκτονικής για τον εντοπισμό απειλών είναι η ανίχνευση μέσω ευρετικής ανάλυσης. Σε σχέση με την ανίχνευση βάσει υπογραφών η οποία μπορεί και αναγνωρίζει γνωστές απειλές, η ευρετική ανάλυση έχει την δυνατότητα να ανιχνεύσει και άγνωστες απειλές[18]. Έτσι η ευρετική ανάλυση έρχεται να συμπληρώσει σε ένα βαθμό τα κενά που αφήνει η ανίχνευση βάσει υπογραφών.

Τώρα ως προς την λειτουργία της ευρετικής ανάλυσης, ο θεμέλιος λίθος αυτής της τεχνικής είναι η ανάπτυξη ευρετικών αλγορίθμων, δηλαδή, ένα σύνολο από κανόνες γνωστών συμπεριφορών κακόβουλων λογισμικών. Για παράδειγμα ως προς την συμπεριφορά τους, διαφορετικά συμπεριφέρεται ένας πληροφοριοκλέφτης (infostealer malware) και αλλιώς ένα λυτρισμικό (ransomware). Αυτοί οι κανόνες μπορεί να ελέγχουν απλές ενέργειες όπως η εγγραφή σε ένα αρχείο συστήματος ή αλλαγές σε αρχεία , έως και πιο σύνθετες συμπεριφορές όπως η εκτέλεση κώδικα με τέτοιον τρόπο που να υποδηλώνει κακόβουλη ενέργεια. Στη συνέχεια οι συμπεριφορές που παρατηρήθηκαν συγκρίνονται με τον σύνολο των ευρετικών κανόνων. Εάν υπάρξει ταύτιση, το σύστημα θα στιγματίσει το αρχείο ή την κίνηση του δικτύου ως πιθανή κακόβουλη ενέργεια. Έπειτα

μπορεί να ειδοποιήσει τον χρήστη και ανάλογα με το πόσο σίγουρο είναι το σύστημα για το συμπέρασμα που έβγαλε, μπορεί ακόμη και να θέσει σε καραντίνα το πιθανός κακόβουλο αρχείο.

Η ευρετική ανάλυση είναι μια μέθοδος που μπορεί να αντιμετωπίσει τους πολυμορφικούς ιούς υπολογιστών, οι οποίοι έχουν την δυνατότητα να αλλάζουν και να προσαρμόζουν τον κώδικα τους συνεχώς για να περάσουν απαρατήρητοι από τους αμυντικούς ελέγχους του συστήματος[19]. Πρέπει όμως να επισημανθεί ότι η ευρετική ανάλυση μπορεί να επιφέρει μεγάλο αριθμό από ψευδώς θετικά αποτελέσματα/συναγερμούς, καθώς τα νόμιμα και μη κακόβουλα λογισμικά σε ένα σύστημα μπορεί να παρουσιάζουν συμπεριφορές οι οποίες ταιριάζουν με τους ευρετικούς κανόνες.

2.4.3 Ανίχνευση βάσει ανωμαλιών (Anomaly-Based Detection)

Η ανίχνευση βάσει ανωμαλιών είναι μια μέθοδος που χρησιμοποιείται στην κυβερνοασφάλεια για τον εντοπισμό ασυνήθιστης ή αποκλίνουσας από τα κανονικά πλαίσια συμπεριφοράς, κάτι που μπορεί να υποδεικνύει μια πιθανή απειλή ή επίθεση[20]. Η αρχή που διέπει τον συγκεκριμένο τύπο ανίχνευσης απειλών είναι πως οι κακόβουλες ενέργειες θα διαφέρουν από την φύση τους από της κανονικές και νόμιμες ενέργειες, ξεχωρίζοντας τες έτσι ως ανωμαλίες. Με αυτόν τον τρόπο το σύστημα μπορεί να ανιχνεύσει νέες απειλές.

Για να μπορέσει να λειτουργήσει αποτελεσματικά η ανίχνευση βάσει ανωμαλιών θα πρέπει να ορίσουμε μία "στάνταρ κατάσταση", η οποία θα ορίζει τι θεωρείται φυσιολογική συμπεριφορά για το σύστημά μας. Αυτή η "στάνταρ κατάσταση" συνήθως χτίζεται μετά την ευρεία ανάλυση των ιστορικών δεδομένων του συστήματος, κάτι που μπορεί να συμπεριλαμβάνει τις δραστηριότητες των χρηστών, το μοτίβο της κίνησης του δικτύου και άλλων στοιχείων[21].

Στη συνέχεια και αφού έχει δημιουργηθεί η "στάνταρ κατάσταση", το σύστημα ανίχνευσης παρακολουθεί συνεχώς τη συμπεριφορά του συστήματος. Η τρέχουσα συμπεριφορά του συστήματος θα συγκρίνετε με την "στάνταρ κατάσταση" και σε περίπτωση που εντοπιστεί σοβαρή απόκλιση, αυτή η απόκλιση θα χαρακτηριστεί ως ανωμαλία του συστήματος. Εδώ πρέπει να επισημανθεί ότι η ανωμαλία δεν σημαίνει αυτόματα και ύπαρξη απειλής. Η εκάστοτε ανωμαλία του συστήματος θα πρέπει να διερευνηθεί διεξοδικά από τους αναλυτές ασφαλείας και έπειτα την ανάλυση θα υπάρξει το πόρισμα για τον εάν υπάρχει κάποια υπαρκτή απειλή στο σύστημα. Παρ' όλα αυτά το σύστημα μπορεί να έχει ρυθμιστεί να λαμβάνει και αυτό κάποιες πρώτες ενέργειες, όπως για παράδειγμα ο αποκλεισμός μιας ύποπτης διεύθυνσης IP.

Η ανίχνευση βάσει ανωμαλιών έχει την δυνατότητα να ανιχνεύει νέες και άγνωστες απειλές καθώς δεν βασίζεται σε κάτι προκαθορισμένο. Αυτό την καθιστά έναν από τους πιο δυνατούς μηχανισμούς στην ανίχνευση απειλών μηδενικής ημέρας (Zero day exploit or zero day vulnerability). Ευπάθειες μηδενικής ημέρας είναι ένας τύπος ευπάθειας που τον εκμεταλλεύονται για πρώτοι φορά οι επιτιθέμενοι, κάτι που σημαίνει πως δεν έχει ανιχνευθεί ποτέ στο παρελθόν από κάποιο σύστημα ασφαλείας[22]. Τέλος, μία από τις πολλές προκλήσεις που αντιμετωπίζει αυτή η μέθοδος ανίχνευσης απειλών είναι ότι οι επιτιθέμενοι ίσως μπορέσουν να καμουφλάρουν τις πράξεις τους και οι ενέργειες τους να χαρακτηρίζονται ως κανονική συμπεριφορά και όχι σαν ανωμαλία στο σύστημα και έτσι να πετύχουν την αποφυγή ανίχνευσης από το σύστημα.

2.4.4 Η μηχανική μάθηση στην ανίχνευση απειλών

Η μηχανική μάθηση σαν πεδίο είναι ένα παρακλάδι της τεχνητής νοημοσύνης που επιτρέπει στους υπολογιστές να μαθαίνουν από τα δεδομένα. Οι αλγόριθμοι μηχανικής μάθησης έχουν την δυνατότητα να εξάγουν μοτίβα από τα δεδομένα με τα οποία τροφοδοτούνται, επιτρέποντάς τους να

κάνουν προβλέψεις ή να λαμβάνουν αποφάσεις χωρίς να έχουν προσχεδιαστεί για αυτές τις ενέργειες. Αυτή η δυνατότητα που έχουν ως προς την προσαρμοστική μάθηση, καθιστά την μηχανική μάθηση ένα ισχυρό εργαλείο στα χέρια του κόσμου της κυβερνοασφάλειας και ιδίως στην περίπτωση μας, δηλαδή στην ανίχνευση απειλών στο πλαίσιο του XDR. Η ενσωμάτωση της μηχανικής μάθησης στο XDR πλαίσιο ήταν κάτι το αναπόφευκτο λαμβάνοντας υπόψη τον τεράστιο όγκο δεδομένων που καλείτε να αναλύσει. Έτσι, η μηχανική μάθηση ενισχύει τις δυνατότητες του XDR επιτρέποντας στο σύστημα να μαθαίνει από ιστορικά δεδομένα, να ανιχνεύει σύνθετα μοτίβα, να ανιχνεύει ανωμαλίες και να λαμβάνει τεκμηριωμένες αποφάσεις και όλα αυτά σε πραγματικό χρόνο και με ελάχιστη ανθρώπινη παρέμβαση καθ' όλη την διάρκεια[23].

Ως προς την ανίχνευση απειλών οι αλγόριθμοι μηχανικής μάθησης είναι σε θέση να εκπαιδευτούν για να μάθουν την "κανονική" συμπεριφορά ενός συστήματος και οποιαδήποτε απόκλιση από την κανονική συμπεριφορά να εκφραστεί ως ανωμαλία, η οποία δυνητικά μπορεί να σηματοδοτήσει την ύπαρξη μιας απειλής[23]. Επίσης μπορεί να προβλέψει την πιθανότητα μελλοντικών απειλών που μπορούν να υπάρξουν αναλύοντας παλιά περιστατικά ασφαλείας και παλιές παραβιάσεις. Έτσι, αυτού του είδους η προληπτική προσέγγιση επιτρέπει στους οργανισμούς να αναπτύξουν προληπτικά μέτρα προστασίας. Επιπλέον, η αλγόριθμοι μηχανικής μάθησης μπορούν να ταξινομούν δεδομένα βάσει μοτίβων πάνω στα οποία έχουν εκπαιδευτεί, έτσι ώστε να διακρίνουν μια έννομη και καλοήθη ενέργεια σε σχέση με μια δυνητικά κακόβουλη ενέργεια.

Ας έχουμε υπόψιν ότι διαφορετικοί τύποι αλγορίθμων μηχανικής μάθησης έχουν διαφορετικά πλεονεκτήματα και μειονεκτήματα όταν εφαρμόζονται στην κυβερνοασφάλειας και δει στην ανίχνευση απειλών. Για παράδειγμα, οι αλγόριθμοι εποπτευόμενης μάθησης, όπως οι μηχανές διανυσμάτων ή τα νευρωνικά δίκτυα μπορούν να αποτελέσουν ισχυρά εργαλεία για την ανίχνευση γνωστών απειλών, όταν υπάρχει πληθώρα κατάλληλων δεδομένων για να εκπαιδεύσουν τέτοιους αλγορίθμους[24]. Έπειτα, οι αλγόριθμοι μάθησης χωρίς επίβλεψη (Unsupervised) όπως οι αλγόριθμοι ομαδοποίησης ή οι αυτοκωδικοποιητές, μπορούν να είναι χρήσιμοι για την ανίχνευση νεο-εμφανισθέντων και άγνωστων απειλών με τον εντοπισμό ανωμαλιών στα δεδομένα. Τέλος, οι αλγόριθμοι ενισχυτικής μάθησης μπορούν να φανούν χρήσιμοι ως προς την δυναμική προσαρμογή στις εξελισσόμενες απειλές ενός ενεργού πληροφοριακού περιβάλλοντος[24].

2.4.5 Η τεχνητή νοημοσύνη στην ανίχνευση απειλών

Όπως είδαμε παραπάνω η μηχανική μάθηση, είναι ένα υποσύνολο της τεχνητής νοημοσύνης που περιλαμβάνει αλγορίθμους που μαθαίνουν και βελτιώνονται από την εμπειρία, επιτρέποντας στα συστήματα να αναλύουν και να ερμηνεύουν αυτόματα πολύπλοκα μοτίβα μέσα σε μεγάλα σύνολα δεδομένων. Απ' την άλλη μεριά η τεχνητή νοημοσύνη είναι μια ευρύτερη έννοια που αναφέρεται σε συστήματα ή μηχανές που μιμούνται την ανθρώπινη νοημοσύνη, μαθαίνουν από την εμπειρία σε βάθος χρόνου, προσαρμόζονται σε νέα δεδομένα και εκτελούν εργασίες που μοιάζουν με τις ανθρώπινες. Η τεχνητή νοημοσύνη εμπλουτίζει τις δυνατότητες του XDR σχεδιασμού προσδίδοντας νοημοσύνη στη διαδικασία ανίχνευσης και αντιμετώπισης απειλών. Υπερβαίνει την απλή μάθηση και πρόβλεψη, καθώς μπορεί να κατανοήσει, να αιτιολογήσει και να δράσει βάσει των δεδομένων.

Η τεχνητή νοημοσύνη μπορεί να εφαρμοστεί με διάφορους τρόπους. Εδώ θα αναφερθούμε σε δύο τεχνολογίες/μεθόδους. Στην Επεξεργασία Φυσικής Γλώσσας και στην Ανάλυση Πλαισίου/Περιεχομένου, που διαδραματίζουν σημαντικό ρόλο στην σύγχρονη ανίχνευση απειλών.

Η Επεξεργασία Φυσικής Γλώσσας είναι ένα υποπεδίο της τεχνητής νοημοσύνης που επιτρέπει στους υπολογιστές να κατανοούν, να ερμηνεύουν και να αναπαράγουν την ανθρώπινη γλώσσα με

ουσιαστικό τρόπο. Στην περίπτωση της κυβερνοασφάλειας και της ανίχνευσης απειλών μπορεί να εφαρμοστεί με διάφορους τρόπους. Εμείς θα δούμε πως μπορεί να εφαρμοστεί στην ανίχνευση Ηλεκτρονικού Ψαρέματος (phishing). Η Επεξεργασία Φυσικής Γλώσσας θα μπορέσει να αναλύσει τη γλώσσα που χρησιμοποιείται στα μηνύματα ηλεκτρονικού ταχυδρομείου, έτσι ώστε να εντοπίσει και να επισημάνει πιθανές απόπειρες Ηλεκτρονικού Ψαρέματος. Αυτό μπορεί να το πετύχει μέσω της ανίχνευσης αμυδρών ενδείξεων στο κείμενο που μπορεί να υποδηλώνουν κακόβουλη πρόθεση, όπως για παράδειγμα ο επείγων χαρακτήρας του μηνύματος, το αίτημα προς τον χρήστη για δημοσιοποίηση ευαίσθητων πληροφοριών ή ακόμα και στην ανίχνευση ύποπτων συνδέσμων[25].

Η Ανάλυση Πλαισίου περιλαμβάνει την κατανόηση του πλαισίου στο οποίο λαμβάνει χώρα ένα συγκεκριμένο γεγονός ή μια συγκεκριμένη συμπεριφορά. Στην κυβερνοασφάλεια, χρησιμοποιείται κυρίως για τη διάκριση μεταξύ καλοπροαίρετων και δυνητικά κακόβουλων δραστηριοτήτων. Για παράδειγμα στην Ανάλυση Συμπεριφοράς, η ανάλυση πλαισίου μπορεί να χρησιμοποιηθεί για την κατανόηση της συμπεριφοράς του χρήστη και κάτω από πιο ιδιαίτερο πλαίσιο συνέβη αυτή η συμπεριφορά. Για παράδειγμα, η πρόσβαση ενός συγκεκριμένου χρήστη σε ευαίσθητα δεδομένα κατά την διάρκεια των ωρών που εργάζεται είναι κάτι το φυσιολογικό. Ωστόσο, η ίδια ενέργεια πρόσβασης σε ευαίσθητα δεδομένα θα ήταν ύποπτη αν συνέβαινε αργά το βράδυ ή από μια τοποθεσία από την οποία δεν έχει συνδεθεί παλαιότερα ο χρήστης. Επίσης, με την κατανόηση του πλαισίου της κίνησης του δικτύου βοηθάει το σύστημα στον εντοπισμό πιθανών απειλών. Για παράδειγμα, μια ξαφνική αύξηση μεταφοράς δεδομένων σε μια ξένη χώρα θα μπορούσε να αποτελέσει μια ένδειξη για πιθανή απειλή μη εξουσιοδοτημένης μεταφοράς δεδομένων[26].

Καθώς ολοκληρώνεται το κεφάλαιο της ανίχνευσης απειλών, είναι σαφές ότι στο χώρο της ασφάλειας πληροφοριακών συστημάτων χρειάζεται μια πολύπλευρη προσέγγιση για τον εντοπισμό απειλών και επιθέσεων. Από τις πολυδουλεμένες παραδοσιακές μεθόδους, όπως η ανίχνευση μέσω υπογραφών και η ευρετική ανάλυση, έως την εφαρμογή πιο σύνθετων τεχνολογιών όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση. Κλείνοντας, είναι σημαντικό να αναγνωρίσουμε πως για να έχουμε μια δυνατή και αποτελεσματική ανίχνευση απειλών, πρέπει οι μέθοδοι που έχουμε στο οπλοστάσιό μας να χρησιμοποιούνται με τέτοιον τρόπο έτσι ώστε η μία τεχνολογία να βοηθάει ή ακόμα και να καλύπτει τα κενά μιας άλλης τεχνολογίας σε αυτό το πολυσύνθετο και δύσκολο παζλ της ανίχνευσης απειλών.

2.5 Απόκριση σε περιστατικά ασφαλείας

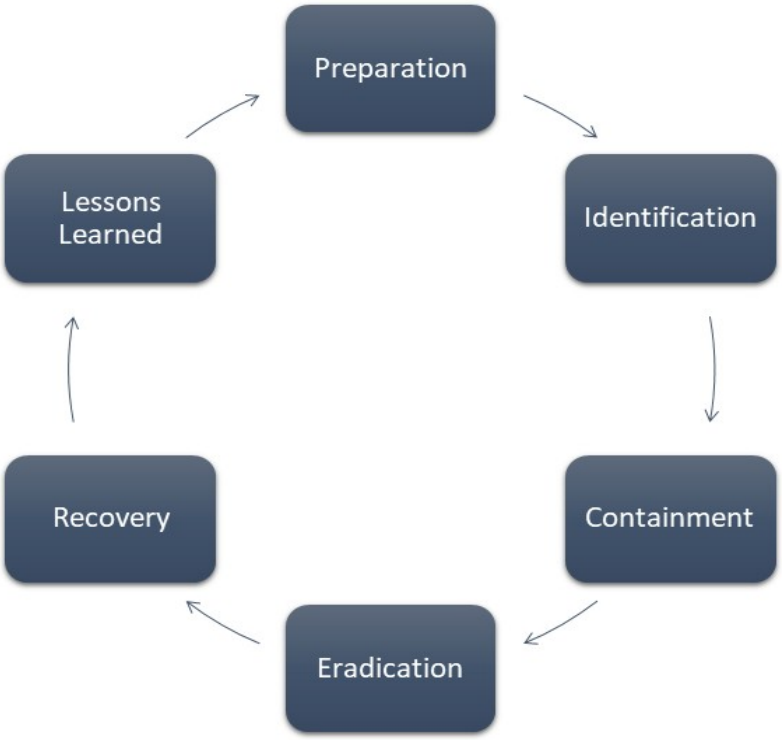
Η απόκριση σε περιστατικά ασφαλείας στα συστήματα XDR είναι μια εκτεταμένη διαδικασία που περιλαμβάνει πολλαπλά στάδια και συστατικά, από την ανίχνευση, τον περιορισμό, την εξάλειψη και την αποκατάσταση ως τις ενέργειες που πρέπει να γίνουν μετά το περιστατικό. Στην δική μας περίπτωση θα ακολουθηθεί το πλαίσιο PICERL (Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned), ένα πλαίσιο που χρησιμοποιείται για απόκριση σε περιστατικά ασφαλείας[27].

Η **φάσης της προετοιμασίας** αφορά την ετοιμότητα πριν από την εκδήλωση ενός συμβάντος. Αυτό περιλαμβάνει διάφορα βασικά στοιχεία σε τεχνικό και διοικητικό επίπεδο. Αρχικά, θα πρέπει να διευθετηθεί μια Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας (Incident Response Team) στην οποία θα λαμβάνουν μέρος συγκεκριμένα άτομα και θα έχουν συγκεκριμένους ρόλους. Έπειτα θα πρέπει να αναπτυχθεί ένα Σχέδιο Αντιμετώπισης Περιστατικών. Το σχέδιο αυτό θα πρέπει να περιγράφει αναλυτικά όλες τις ενέργειες που θα πρέπει να γίνουν σε ένα περιστατικό ασφαλείας και τον κατάλογο με τα κατάλληλα εργαλεία που θα χρησιμοποιηθούν. Επιπλέον, οι ασκήσεις

ετοιμότητας για ένα πιθανό περιστατικό κυβερνοασφάλειας είναι ένα σημαντικό κομμάτι στην φάση της προετοιμασίας.

Η **φάση της ανίχνευσης** του περιστατικού έχει αναλυθεί διεξοδικά στο αμέσως προηγούμενο κεφάλαιο (2.4).

Μόλις επαληθευτεί μια απειλή, η διαδικασία αντιμετώπισης περιστατικών περνάει στο **στάδιο του περιορισμού.** Τα συστήματα XDR μπορούν να εφαρμόζουν αυτόματα ενέργειες περιορισμού, όπως η απομόνωση ενός μολυσμένου τελικού κόμβου από το δίκτυο, ο αποκλεισμός διευθύνσεων IP ή η αλλαγή των ελέγχων πρόσβασης, για να αποτραπεί η περαιτέρω εξάπλωση της απειλής.
Το **στάδιο της εξάλειψης** περιλαμβάνει την απομάκρυνση της απειλής από το σύστημα. Αυτό μπορεί να περιλαμβάνει τη διαγραφή κακόβουλων αρχείων, την αντιστροφή των αλλαγών που έγιναν από το κακόβουλο λογισμικό ή την επιδιόρθωση ευπαθειών που αξιοποιήθηκαν από τους κακόβουλους χρήστες.
Η **φάση της αποκατάστασης** είναι η διαδικασία επαναφοράς των προσβεβλημένων συστημάτων σε κανονική λειτουργία. Στα συστήματα XDR, η διαδικασία αυτή μπορεί επίσης να αυτοματοποιηθεί σε κάποιο βαθμό, όπως με την επαναφορά των συστημάτων σε ασφαλή κατάσταση ή την επανεγκατάσταση του επηρεαζόμενου λογισμικού[28]. Τέλος, αφού αντιμετωπιστεί ένα περιστατικό ασφαλείας, είναι σημαντικό να διενεργηθεί μια ανασκόπηση μετά το περιστατικό. Αυτό περιλαμβάνει την ανάλυση του τι συνέβη, γιατί συνέβη και πώς αντέδρασε ο οργανισμός και οι μηχανισμοί που έχει αναπτύξει. Η ανάλυση αυτή βοηθά στον εντοπισμό τομέων για βελτίωση της διαδικασίας αντιμετώπισης περιστατικών ασφαλείας.



Σχήμα 2.5.1: Μοντέλο PICERL [54]

Εν κατακλείδι, η αποτελεσματική αντιμετώπιση περιστατικών σε συστήματα XDR απαιτεί την εις βάθος κατανόηση του συστήματος του οργανισμού, σαφές σχέδιο αντιμετώπισης περιστατικών, αποτελεσματική χρήση ειδοποιήσεων σε πραγματικό χρόνο, επαρκεί αυτοματοποίηση, τακτικές δοκιμές τον ελέγχων και των διαδικασιών, εκπαίδευση του προσωπικού και συνεχή βελτίωση. Ακολουθώντας αυτά τα βήματα, μπορεί να διασφαλιστεί σε μεγάλο βαθμό ότι ο οργανισμός είναι προετοιμασμένος για κάθε περιστατικό ασφαλείας.

2.6 Ροές Πληροφοριών για Κυβερνοεπιθέσεις (CTI feeds)

Συνεχίζοντας ως προς τον ρόλο που κατέχουν οι Ροές Πληροφοριών για Κυβερνοεπιθέσεις στην αρχιτεκτονική του XDR. Οι Ροές Πληροφοριών για Κυβερνοεπιθέσεις είναι δομημένες ροές δεδομένων που παρέχουν αξιοποιήσιμες πληροφορίες σχετικά με τις τρέχουσες και πιθανές απειλές στον κυβερνοχώρο. Αυτές οι ροές παρέχουν συνήθως δείκτες παραβίασης (IOCs), τακτικές, τεχνικές και διαδικασίες (TTPs), και άλλα σχετικά δεδομένα απειλών[29]. Έτσι αυτές οι πληροφορίες μπορούν να τροφοδοτηθούν σε XDR συστήματα και να βοηθήσουν στον εντοπισμό και εξακρίβωση απειλών γρήγορα και με ακρίβεια. Επίσης μπορούν να χρησιμοποιηθούν για την ιεράρχηση των απειλών, παρέχοντας ένα πλαίσιο για τις απειλές, το πιθανό αντίκτυπο που θα επιφέρουν στον οργανισμό και τον τρόπο δράσεις τους. Με αυτή την ιεράρχηση ο οργανισμός θα είναι σε θέση να καθορίσει ποιες απειλές θα πρέπει να αντιμετωπιστούν πρώτες. Επιπλέον, μπορούν να βοηθήσουν στο προληπτικό κυνήγι απειλών στο δίκτυο του εκάστοτε οργανισμού. Παρέχοντας πληροφορίες για τις τελευταίες τακτικές, τεχνικές και διαδικασίες που χρησιμοποιούν οι κυβερνοεγκληματίες μπορούν να βοηθήσουν

τους αναλυτές κυβερνοασφάλειας να εντοπίσουν κρυφές απειλές που ίσως να έχουν περάσει απαρατήρητες λόγω της έλλειψης πληροφοριών για αυτές.

Μερικές από τις πλατφόρμες ροών πληροφοριών για κυβερνοεπιθέσεις (TIP – Threat Intelligence Platform) είναι οι παρακάτω:

- MISP[77]: Μια δωρεάν πλατφόρμα ανοιχτού κώδικα για τον διαμοιρασμό πληροφοριών για κυβερνοεπιθέσεις
- Record Future[78]: Μια επί-πληρωμή πλατφόρμα για τον διαμοιρασμό πληροφοριών για κυβερνοεπιθέσεις. Θεωρείτε πρωτοπόρος στον κόσμο του CTI
- Anomali[79]: Μια επί-πληρωμή πλατφόρμα για τον διαμοιρασμό πληροφοριών για κυβερνοεπιθέσεις

Τέλος πρέπει να επισημανθεί ότι η επιλογή Ροών Πληροφοριών για Κυβερνοεπιθέσεις (CTI feeds), των κατηγοριών αυτών των ροών αλλά και της ποσότητας που θα εισέλθει στα XDR συστήματα, πρέπει να γίνει με προσεκτικό και τεκμηριωμένο τρόπο για να αποφευχθούν συμβάντα όπως η άσχετη χρήση πληροφοριών, πληροφοριών για απειλές που δεν σχετίζονται άμεσα με τον τομέα που δραστηριοποιείται ο οργανισμός. Για παράδειγμα μία φαρμακοβιομηχανία, θα πρέπει να λαμβάνει πληροφορίες για ομάδες επιτιθέμενων που επιχειρούν εναντίων φαρμακοβιομηχανιών και να μην λαμβάνει πληροφορίες από άλλους άσχετους τομείς.

2.7 Ενσωμάτωση (Integrations)

Η αρχιτεκτονική των XDR συστημάτων αντιπροσωπεύει μια αλλαγή προτύπου στην ασφάλεια στον κυβερνοχώρο. Ενσωματώνει πολλαπλά προϊόντα ασφαλείας σε ένα συντονισμένο σύστημα ασφαλείας, παρέχοντας ολιστική ορατότητα σε όλο το ψηφιακό τοπίο ενός οργανισμού. Τα στοιχεία που ενσωματώνονται στο XDR περιλαμβάνουν συνήθως στοιχεία ασφαλείας όπως η ανίχνευση και η απόκριση τελικών κόμβων (EDR), η ανάλυση κίνησης δικτύου (NTA), η διαχείριση πληροφοριών και συμβάντων ασφαλείας (SIEM), τα εργαλεία ασφαλείας νέφους και άλλα. Οι ενσωματώσεις μπορούν να αναλυθούν από διάφορες σκοπιές ως προς τις λειτουργικότητές τους[30].

Από την επιχειρησιακή σκοπιά , οι ενσωματώσεις εξορθολογίζουν την επιχειρησιακή λειτουργία των συστημάτων ασφαλείας εξαλείφοντας την ανάγκη για πολλαπλά αυτόνομα και ανεξάρτητα μεταξύ τους προϊόντα ασφαλείας και τις αντίστοιχες κονσόλες διαχείρισής τους. Η ενοποιημένη προσέγγιση που επιτυγχάνετε μέσω των ενσωματώσεων, μειώνει την πολυπλοκότητα της διαχείρισης μια πολυεπίπεδης υποδομής ασφαλείας, οδηγώντας σε μεγαλύτερη επιχειρησιακή ετοιμότητα και παράλληλα εξοικονομεί χρήματα για τον οργανισμό.

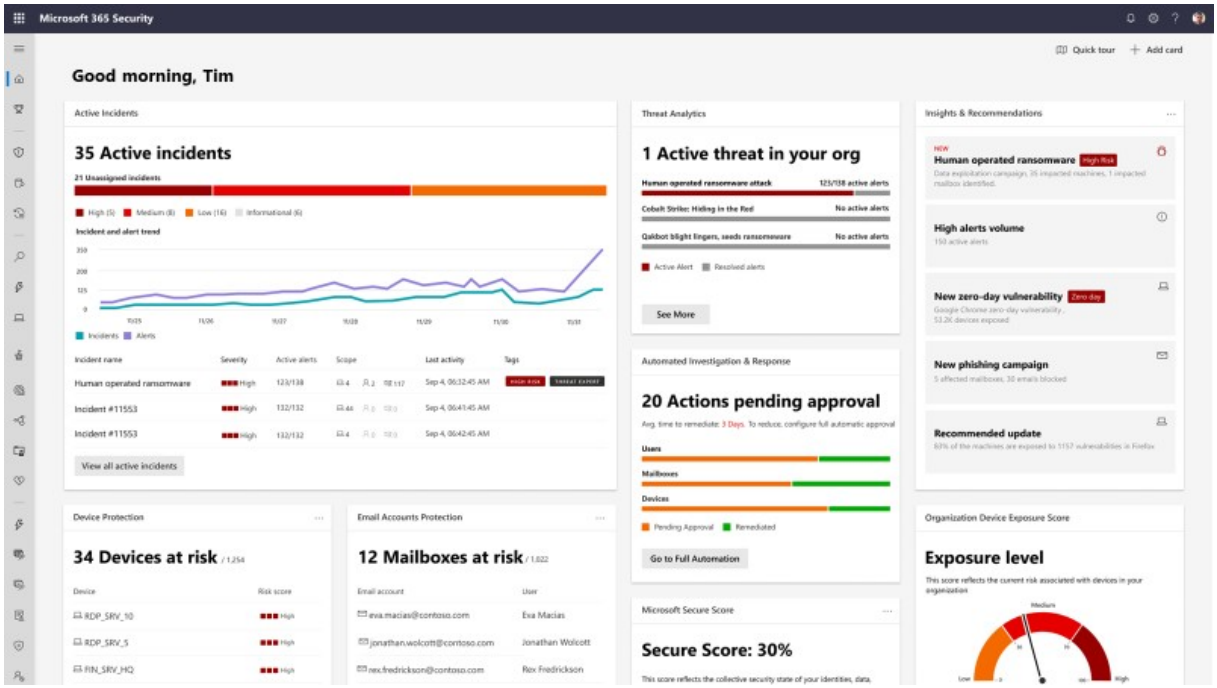
Από στρατηγική σκοπιά για τους οργανισμούς, οι ενσωματώσεις βοηθούν στην ανάπτυξη μιας προληπτικής στάσης ενάντια σε απειλές και επιθέσεις. Με συνεχή παρακολούθηση, ανίχνευση απειλών και αυτοματοποιημένη απόκριση σε περιστατικά ασφαλείας, οι οργανισμοί μπορούν να ευθυγραμμιστούν με τις συνεχώς μεταβαλλόμενες απειλές στον κυβερνοχώρο. Η ενισχυμένη ορατότητα σε όλο το πληροφοριακό σύστημα επιτρέπει στους οργανισμούς να εντοπίζουν και να αποκαθιστούν τα τρωτά σημεία, ενισχύοντας έτσι τη συνολική στάση ασφαλείας τους.

Είναι επίσης σημαντικό να σημειωθεί ότι η διενέργεια ενσωματώσεων και από τις δύο σκοπιές δεν είναι εύκολη διαδικασία. Από στρατηγική σκοπιά είναι μια διαδικασία αλλαγής της νοοτροπίας λειτουργίας στην οποία πρέπει να συμπλεύσουν αρμονικά όλοι οι εμπλεκόμενοι, από το διοικητικό συμβούλιο μέχρι τους αναλυτές και τους μηχανικούς. Από επιχειρησιακή σκοπιά, κατά την διάρκεια

των ενσωματώσεων πιθανός θα προκύψουν ασυμβατότητες υπαρχόντων προϊόντων ασφαλείας τα οποία να μην μπορούν να ενσωματωθούν εύκολα ή και καθόλου στην ολιστική αρχιτεκτονική του XDR. Σε αυτό το πρόβλημα, λύση μπορεί να δώσει το πρωτόκολλο OpenC2 το οποίο θα αναλύσουμε στο ομότιτλο κεφάλαιο παρακάτω.

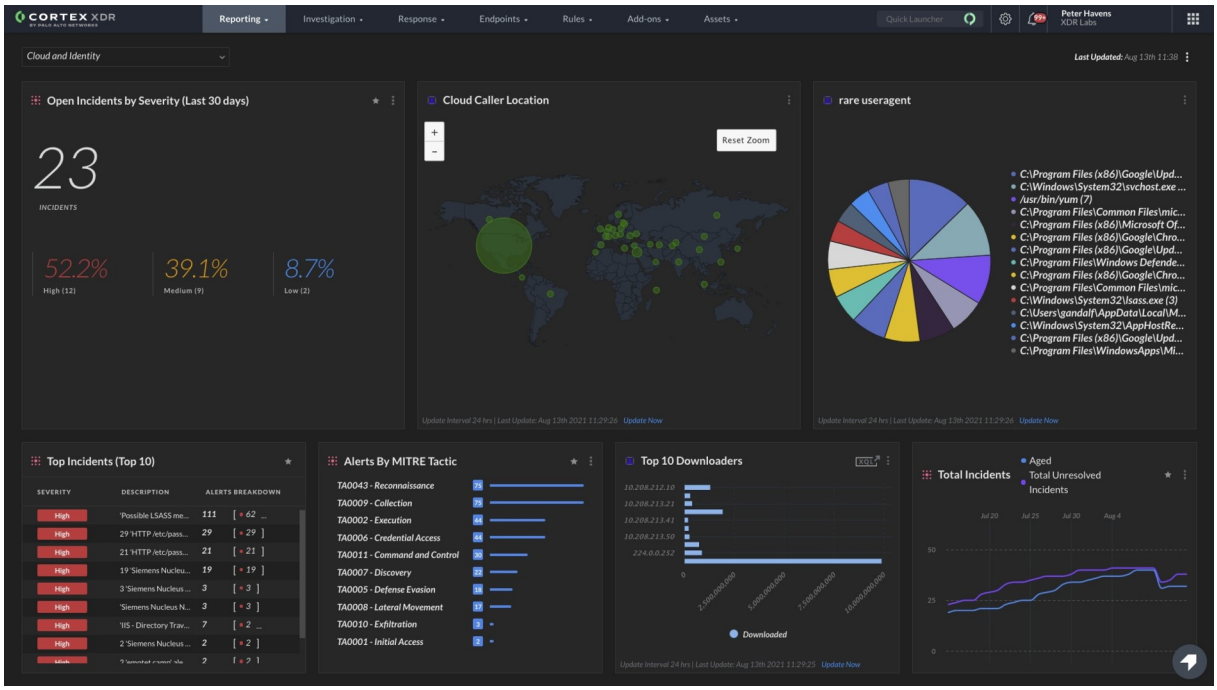
2.8 Οπτικοποίηση / Απεικόνιση

Στο τελευταίο υποκεφάλαιο θα εστιάσουμε στον ρόλο της οπτικοποίησης των δεδομένων και την χρήση των ταμπλό (Dashboards) στα συστήματα XDR και πως αυτά βοηθούν τους αναλυτές που χρησιμοποιούν ένα τέτοιο σύστημα να γίνουν πιο αποτελεσματικοί. Η οπτικοποίηση είναι ένα κρίσιμο στοιχείο στον κόσμο του XDR καθώς μπορεί να μεταφέρει στους αναλυτές όλα τα πολύπλοκα δεδομένα και τις σχέσεις μεταξύ αυτών, σε μια μορφή που θα είναι ευκολότερη η ανάγνωση τους, η ανάλυσή τους και η κατανόησή τους. Τα ταμπλό απ' την άλλη πλευρά, ενοποιούν αυτά τα οπτικά δεδομένα, παρουσιάζοντας οργανωμένα διαφόρων ειδών μετρήσεις, τάσεις και πληροφορίες για την κατάσταση ασφαλείας του συστήματος[31].



Σχήμα 2.8.1: Ταμπλό του XDR συστήματος της Microsoft [55]

Όπως έχουμε αναφέρει πρότερα, τα XDR συστήματα συλλέγουν τεράστιες ποσότητες δεδομένων από πάρα πολλές πηγές. Οι τεχνικές οπτικοποίησης που εφαρμόζονται απλοποιούν αυτά τα δεδομένα, προσφέροντας έτσι την δυνατότητα στους αναλυτές κυβερνοασφάλειας να ανιχνεύσουν μοτίβα και πιθανές ανωμαλίες στα δεδομένα αυτά. Έπειτα, τα ταμπλό συγκεντρώνουν αυτές τις απεικονίσεις για να παράσχουν μια ολοκληρωμένη εικόνα στους αναλυτές έτσι ώστε να τους διευκολύνουν ως προς τις λήψεις αποφάσεων σε περιστατικά ασφαλείας με ταχύτερη και καλύτερη πληροφόρηση. Τα ταμπλό πρέπει να σχεδιάζονται με γνώμονα την απλότητα και την ευχρηστία τους, διότι εάν είναι περίπλοκα μπορεί να εμποδίσουν τους αναλυτές, ενώ θα πρέπει να τους βοηθάνε, και να μειώσουν σε μεγάλο βαθμό τις επιχειρησιακές τους ικανότητες[31]. Επιπλέον, τα ταμπλό πρέπει να είναι σε θέση να λαμβάνουν πληροφορίες σε πραγματικό χρόνο και να ενημερώνουν συνεχώς τις διεπαφές χρήστη για να αποδίδουν στους αναλυτές τα πιο πρόσφατα δεδομένα. Έτσι η αναλυτές θα είναι σε θέση να αναλύσουν και να προσδιορίσουν ποια περιστατικά ασφαλείας επείγουν άμεσης επίλυσης λόγω της κρισιμότητάς τους και ποια μπορούν να παραμεληθούν για ένα μικρό και εύλογο χρονικό διάστημα.



Σχήμα 2.8.2: Ταμπλό του XDR συστήματος της Palo Alto Networks [56]

Συνοψίζοντας, η οπτικοποίηση και τα ταμπλό παίζουν σημαντικό ρόλο στην αποτελεσματική χρήση των συστημάτων XDR από τους χρήστες του. Παρουσιάζουν το αποσαφηνισμένο πεδίο απειλών σε πραγματικό χρόνο από τα συστήματα που λαμβάνουν πληροφορίες, ενισχύουν την ανίχνευση απειλών από τους αναλυτές και συμβάλλουν στην επιτυχή και γρήγορη αντιμετώπιση περιστατικών ασφαλείας, μετασχηματίζοντας πολύπλοκα δεδομένα σε αξιοποιήσιμες πληροφορίες.

Κεφάλαιο 3ο: Σύγκριση παραδοσιακού τρόπου εντοπισμού και απόκρισης σε περιστατικά ασφαλείας και νέων τρόπων εντοπισμού και απόκρισης

3.1 Ανάλυση παραδοσιακού τρόπου εντοπισμού και απόκρισης σε κυβερνοεπιθέσεις

Οι οργανισμοί από την αρχή της ύπαρξής τους, όταν ακόμα δεν υπήρχαν πληροφοριακά συστήματα, προσπαθούσαν να προστατεύσουν την πνευματική και φυσική ιδιοκτησία τους και τα δεδομένα τους. Αυτές οι πληροφορίες και τα δεδομένα, υπήρχαν μέσα σε κτιριακές υποδομές και για να διασφαλιστεί ότι δεν θα κλαπούν ή θα παραποιηθούν δημιουργήθηκαν οι κατάλληλοι μηχανισμοί ασφαλείας όπως θωρακισμένες πόρτες, φύλακες επί εικοσιτετραώρου βάσης και άλλα μέτρα για την προστασία των κτιρίων. Όμως καθώς αυτές οι πληροφορίες και δεδομένα άρχισαν να μεταφέρονται από το χαρτί σε υπολογιστικά συστήματα μέσω της ψηφιοποίησής του , οι ανάγκες για την προστασία τους άλλαξαν. Οι οργανισμοί πλέον καλούνται να προστατέψουν τα πληροφοριακά συστήματά τους, στα οποία κρατούνται κρίσιμα δεδομένα, από νέας απειλές και επιθέσεις που προέρχονται από τον πολυδιάστατο περιβάλλον του κυβερνοχώρου.

Μερικοί από τους παραδοσιακούς τρόπους για εντοπισμό απειλών είναι οι εξής: Λογισμικό προστασίας από ιούς (Antivirus Software), Συστήματα Ανίχνευσης Εισβολής (IDS), Συστήματα Αποτροπής Εισβολής (IPS), Τοίχοι Προστασίας (Firewalls) και Συστήματα Διαχείρισης Πληροφοριών και Περιστατικών Ασφαλείας (SIEM).

3.1.1 Αντιικό Λογισμικό (Antivirus Software)

Ξεκινώντας θα αναλυθεί η λειτουργία Αντιικών Λογισμικών (Antivirus Software). Τα αντιικά λογισμικά αποτελούν την πρώτη γραμμή άμυνας ενάντια στα κακόβουλα λογισμικά, όπως των ιών, των σκουλικιών, των δούρειων ίππων, των λυτρισμικών και άλλων. Ως προς τον τρόπο λειτουργίας τους, σαρώνουν αρχεία και καταλόγους του συστήματος και συγκρίνουν τα ευρήματά τους με μια βάση δεδομένων με γνωστά κακόβουλα λογισμικά που διαθέτουν. Ουσιαστικά αναζητούν μοτίβα με βάση τις υπογραφές ή τους ορισμούς γνωστών κακόβουλων λογισμικών. Αυτή η μέθοδος είναι άκρος αποτελεσματική έναντι γνωστών απειλών, αλλά αν χρειαστεί να αναγνωρίσει κακόβουλα λογισμικά για τα οποία δεν έχουν δημιουργηθεί ακόμα οι κατάλληλες υπογραφές, παρουσιάζει χαμηλή ως και μηδενική αποτελεσματικότητα.

Έτσι, πολλά αντιικά λογισμικά για να αυξήσουν την αποδοτικότητά τους στην ανίχνευση άγνωστων απειλών, ενσωματώνουν στο οπλοστάσιό τους, μεθόδους ανίχνευσης που βασίζονται σε ευρετικούς αλγόριθμους. Αυτή η προσέγγιση περιλαμβάνει την ανάλυση της συμπεριφοράς αρχείων και προγραμμάτων για τον εντοπισμό ύποπτων μοτίβων που μπορεί να υποδεικνύουν νέο ή τροποποιημένο κακόβουλο λογισμικό. Επίσης, τα λογισμικά αυτά μπορεί να περιλαμβάνουν και επιπρόσθετες λειτουργίες, όπως η σάρωση μηνυμάτων ηλεκτρονικού ταχυδρομείου, έλεγχο των διαδικτυακών ιστοσελίδων και αυτόματες ενημερώσεις της βάσης δεδομένων όπου κρατούνται όλες οι υπογραφές. Να αναφερθεί επιπλέον ότι ορισμένες λύσεις παρέχουν και προστασία σε πραγματικό χρόνο για το σύστημα, ελέγχοντας συνεχώς τα νέα αρχεία και λογισμικά που εισέρχονται στο σύστημα[32].

3.1.2 Συστήματα Ανίχνευσης Απειλών (Intrusion Detection Systems)

Τα συστήματα ανίχνευσης απειλών έχουν σχεδιαστεί για να παρακολουθούν την ροή του δικτύου και τις δραστηριότητες του συστήματος για τυχόν κακόβουλες δραστηριότητες. Ουσιαστικά λειτουργούν ως ένα σύστημα παρακολούθησης, εξετάζοντας συνεχώς τη συμπεριφορά του δικτύου για να αναγνωρίσουν οποιαδήποτε απόκλιση από τον συνηθησμένο τρόπο λειτουργίας του δικτύου ή τους προκαθορισμένους κανόνες. Γενικά η ανίχνευση απειλών αναφέρετε ως η πράξη της διεξοδικής εξέτασης των συμβάντων σε ένα υπολογιστικό σύστημα ή δίκτυο και της αξιολόγησής τους για ενδείξεις μη εξουσιοδοτημένης πρόσβασης σε αυτά. Αυτά τα συστήματα μπορούν να υφίστανται σε μορφή λογισμικού ή υλικού[33].

Ανάλογα με το εύρος ανίχνευσής τους, τα συστήματα ανίχνευσης εισβολών μπορούν να ταξινομηθούν σε IDS προσανατολισμένο στον υπολογιστή (Host-IDS), IDS προσανατολισμένο στο δίκτυο (Network-IDS) και υβριδικά IDS (Hybrid-IDS).

Τα IDS προσανατολισμένα στον υπολογιστή (HIDS) είναι συστήματα εγκατεστημένα σε τερματικά συστήματα (π.χ υπολογιστής) και ανιχνεύουν εισβολές σε επίπεδο υπολογιστή. Αυτά τα συστήματα συνήθως αναζητούν αλλαγές σε κρίσιμα αρχεία, ύποπτες κλήσεις συστήματος ή ασυνήθιστες διεργασίες. Επικεντρώνονται κυρίως στον εντοπισμό εσωτερικών απειλών ή απειλών που έχουν ήδη διεισδύσει στις άμυνες ενός δικτύου.

Τα IDS προσανατολισμένα στο δίκτυο (NIDS) είναι συστήματα που παρακολουθούν και αναλύουν την κίνηση του δικτύου για ενδείξεις εισβολής. Έχουν την δυνατότητα να αναλύσουν τόσο την εισερχόμενη κίνηση όσο και την εξερχόμενη, πράγμα που τα καθιστά ικανά να μπορούν να ανιχνεύσουν εξωτερικές επιθέσεις κατά του δικτύου, καθώς και απόπειρες μεταφοράς αρχείων από το εσωτερικό δίκτυο, σε κάποιο εξωτερικό ύποπτο δίκτυο.

Τα υβριδικά IDS όπως υποδηλώνει και το όνομα, συνδυάζουν χαρακτηριστικά και από τα Host-IDS και από τα Network-IDS. Έτσι, μπορούν να αναλύουν ταυτόχρονα τόσο την κυκλοφορία του δικτύου όσο και την συμπεριφορά του τερματικού συστήματος. Αυτό επιτρέπει στα υβριδικά συστήματα να παρέχουν πιο ολοκληρωμένη εικόνα για την ασφάλεια του δικτύου, και ενδεχομένως να ανιχνεύουν απειλές που μεμονωμένα τα Host-IDS και Network-IDS να μην μπορούσαν να ανιχνεύσουν λόγω της μονόπλευρης προσέγγισής τους[34].

3.1.3 Συστήματα Αποτροπής Εισβολών (Intrusion Prevention Systems)

Ένας σύστημα αποτροπής εισβολών είναι ένα μέσο ασφαλείας που παρακολουθεί συνεχώς ένα δίκτυο για πιθανή εισβολή ή κακόβουλη δραστηριότητα και εντοπίσει κάτι τέτοιο αναλαμβάνει δράση και ενεργεί κατάλληλα για την αποτροπή της. Κάποιες από τις ενέργειες αυτές μπορεί να είναι η έγκαιρη ειδοποίηση των υπεύθυνων για την ασφάλεια του δικτύου, η απόρριψη των πακέτων της κακόβουλης ενέργειας και ο αποκλεισμός της κυκλοφορίας από την διεύθυνση προέλευσης της απειλής ή της επίθεσης. Για να αναγνωρίσουν την απειλή τα συστήματα αυτά χρησιμοποιούν τεχνικές όπως η ανίχνευση μέσω υπογραφών, ανίχνευση βάσει ανωμαλιών και ακόμα με την χρήση προκαθορισμένων πολιτικών ασφαλείας που σε περίπτωση που παραβιαστούν, πυροδοτείτε και η αντίστοιχη ενέργεια που έχει προκαθοριστεί[35]. Υπάρχουν διάφοροι τύποι συστημάτων αποτροπής εισβολών, κάθε ένα με τα δικά του χαρακτηριστικά και είναι τα εξής:

- Network-IPS: Αυτού του είδους το IPS τοποθετείτε σε συγκεκριμένα σημεία στην τοπολογία ενός δικτύου για να παρακολουθεί όλη την κυκλοφορία του δικτύου και να ελέγχει για πιθανές παραβιάσεις[35].

- Host-IPS: Αυτού το είδους το IPS τοποθετείτε σε τερματικά συστήματα (π.χ υπολογιστές) και παρακολουθεί την δικτυακή ροή του τερματικού αλλά και τις αλλαγές και τις κλήσεις του λειτουργικού συστήματος και ελέγχει για πιθανές παραβιάσεις[35].
- Wireless-IPS: Αυτού το είδους το IPS είναι ένα σύστημα για τον έλεγχο του ασύρματου δικτύου ενός οργανισμού. Ως σκοπό έχει τον επιτήρηση του ραδιοφάσματος εντός του εναέριου χώρου του ασύρματου δικτύου και τον έλεγχο για πιθανές απειλές όπως την εισδοχή ενός μη πιστοποιημένου χρήστη στο ασύρματο δίκτυο, ανωμαλίες και παρεμβολές στο εύρος συχνοτήτων και άλλα[36].

Τα συστήματα αποτροπής εισβολών έχουν γίνει ένας σημαντικός πυλώνας στην σύγχρονη ασφάλεια των πληροφοριακών συστημάτων των οργανισμών. Η ικανότητά τους να ανιχνεύουν και να αποτρέπουν απειλές σε πραγματικό χρόνο, προσφέρει στους οργανισμούς έναν προληπτικό μηχανισμό άμυνας.

3.1.4 Τείχος Προστασίας (Firewall)

Το τείχος προστασίας, στην κύρια μορφή του, είναι ένας δικτυακός αμυντικός μηχανισμός ο οποίος ελέγχει την εισερχόμενη και εξερχόμενη κίνηση χρησιμοποιώντας ένα σύνολο κανόνων (firewall rules) για να εντοπίσει και να επιτρέψει την ασφαλή κίνηση ή σε άλλη περίπτωση να αποκλείσει κακόβουλη κίνηση και απειλές. Είναι συνεπώς ένα προστατευτικό φράγμα μεταξύ των συσκευών ενός έμπιστου εσωτερικού δικτύου και των μη αξιόπιστων δικτύων, για παράδειγμα το Διαδίκτυο (Internet). Αυτά τα συστήματα μπορούν να υφίστανται σε μορφή λογισμικού ή υλικού. Ένας τείχος προστασίας σε μορφή υλικού βρίσκεται μεταξύ του εξωτερικού δικτύου και του εσωτερικού δικτύου, παρέχοντας ένα είδος προστασίας από κακόβουλες ενέργειες και απειλές. Απ΄ την άλλη ένα τείχος προστασίας λογισμικού εγκαθιστάτε ανεξάρτητα σε διαφορετικές φυσικές συσκευές. Αυτού του είδους η προσέγγιση προσφέρει μεμονωμένο έλεγχο, επιτρέποντας την πρόσβαση σε κάποια λειτουργία ή εφαρμογή και παράλληλα μπορεί να αποκλείει ενέργειες που χαρακτηρίζονται ως απειλή κατά το δοκούν. Υπάρχουν διάφοροι τύποι Τείχους Προστασίας (Firewall) όπου ο καθένας χρησιμοποιείτε για διαφορετικά σενάρια. Μερικοί τύποι είναι:

- Τείχος προστασίας ενιαίας διαχείρισης απειλών (Unified Threat Management Firewall): Αυτού το είδους η προσέγγιση προσφέρει μια ενοποιημένη και ολοκληρωμένη λύση που μπορεί να περιλαμβάνει στοιχεία όπως αντιικό λογισμικό, IDS/IPS δυνατότητες, φιλτράρισμα περιεχομένου και την παραδοσιακή λειτουργία ενός τοίχους προστασίας. Η προσέγγιση αυτή χρησιμοποιείται κυρίως από μικρούς και μεσαίους οργανισμούς παρέχοντας πολλαπλά χαρακτηριστά ασφαλείας σε μία μόνο λύση/συσκευή. Κύριο πλεονέκτημα αυτής της επιλογής είναι η μείωση του κόστους εγκατάστασης, ανάπτυξης και συντήρησης του συγκεκριμένου ελέγχου ασφαλείας[37].
- Τείχος προστασίας με επιθεώρηση κατάστασης (Stateful Inspection Firewall): Αυτού του είδους η προσέγγιση σε αντίθεση με την απλή επιθεώρηση πακέτων, παρακολουθεί την κατάσταση των υφιστάμενων συνδέσεων δικτύου, ενώ παράλληλα εξετάζει την εισερχόμενη κυκλοφορία και τη σαρώνει για πιθανές απειλές και επιθέσεις. Η συγκεκριμένη τεχνική είναι προγραμματισμένη να διακρίνει τα νόμιμα πακέτα για διαφορετικούς τύπους συνδέσεων (TCP ή UDP ροές). Όταν ένα πακέτο φτάνει στο τείχος προστασίας, το τείχος προστασίας ελέγχει τη βάση δεδομένων του με τις ενεργές συνδέσεις. Εάν το πακέτο ταιριάζει με μια υπάρχουσα σύνδεση στον πίνακα, το τείχος προστασίας το αφήνει να περάσει χωρίς περαιτέρω ελέγχους. Εάν το πακέτο δεν ταιριάζει με κάποια υπάρχουσα σύνδεση, το τείχος προστασίας εφαρμόζει

το σύνολο κανόνων του στο πακέτο για να καθορίσει εάν θα το επιτρέψει να περάσει. Σε περίπτωση που το πακέτο ξεκινά μια νέα σύνδεση και οι κανόνες του τείχους προστασίας το επιτρέπουν, το τείχος προστασίας δημιουργεί μια νέα καταχώρηση στον πίνακα συνδέσεων. Αυτού του είδους τα τείχη προστασίας μπορούν να αμυνθούν διάφορους τύπους επιθέσεων άρνησης παροχής υπηρεσιών (Denial Of Service Attacks) και από διάφορους τύπους αναγνωριστικών περασμάτων όπως η σάρωση θυρών (Port Scanning)[38].

- Τείχος προστασίας μεσολαβητής (Proxy Firewall): Ένα τείχος προστασίας μεσολαβητής, είναι μια συσκευή ασφαλείας δικτύου που λειτουργεί ως ενδιάμεσος μεταξύ μια τελικής συσκευής (π.χ υπολογιστής) και του διαδικτύου. Έτσι αντί να έχουμε απευθείας σύνδεση μεταξύ τελικής συσκευής και διαδικτύου, ο μεσολαβητής παρεμβάλει μεταξύ των εισερχόμενων και εξερχόμενων πακέτων από το εσωτερικό δίκτυο προς το διαδίκτυο. Έπειτα επιθεωρεί τα περιεχόμενα του πακέτου, εξετάζοντας τα δεδομένα του επιπέδου εφαρμογής (Application Layer) και έτσι μπορεί να εντοπίζει κακόβουλα πακέτα που άλλοι τύποι τειχών προστασίας ενδέχεται να μην εντοπίσουν.

3.1.5 Συστήματα Διαχείρισης Πληροφοριών και Περιστατικών Ασφαλείας (SIEM)

Αρχικά ο όρος/τεχνολογία SIEM είναι ένας συνδυασμός SIM (Security Information Management) και SEM (Security Event Management) δυο προγενέστερων τεχνολογιών που ενώθηκαν για να δημιουργήσουν το SIEM (Security Information and Event Management)[47][48][49]. Μέχρι και το 2007 SIM και SEM λειτουργούσαν ξεχωριστά χωρίς να υπάρχει διαλειτουργικότητα μεταξύ τους. Την περίοδο 2005-2007 η ανάγκη στην αγορά για ένα ενιαίο σύστημα διαχείρισης πληροφοριών και περιστατικών που σχετίζονται με την κυβερνοασφάλεια έφερε στην επιφάνεια τα πρώτα SIEM προϊόντα Υπάρχουν αναφορές ότι και κατά την πενταετία 2000-2005 υπήρχαν συστήματα SIEM αλλά αυτά αναπτύσσονταν και έμεναν για εσωτερική χρήση και μόνον. Οργανισμοί που ανέπτυσσαν SIEM για ιδία χρήση φαίνεται να ήταν μεγάλες τράπεζες και κρατικές υπηρεσίες μεγάλων κρατών. Ένα SIEM είναι το κύριο στοιχείο ενός SOC (Security Operation Center) και παρέχει στους οργανισμούς δυνατότητες να συλλέξουν, να αποθηκεύσουν και να αναλύσουν δεδομένα σχετικά με την κυβερνοασφάλεια από την πληροφοριακή υποδομή τους. Συνήθως ένα σύστημα SIEM αποτελείται από τα παρακάτω συνιστώσες:

- Συλλογή Δεδομένων: Ως συλλογή δεδομένων σε ένα περιβάλλον SIEM χαρακτηρίζετε η συγκομιδή δεδομένων από πολλές και διάφορες πηγές από ένα ή πολλά πληροφοριακά συστήματα μέσα σε έναν οργανισμό. Η πηγές από τις οποίες μπορεί να συλλέξει σημαντικά δεδομένα μπορεί να είναι δικτυακές συσκευές (Μεταγωγείς, Δρομολογητές, Τείχη Προστασίας), προϊόντα ασφαλείας (IDS, IPS, EDR, AV) και από διακομιστές όπως διακομιστής ηλεκτρονικού ταχυδρομείου, διακομιστής διαδικτύου και διακομιστή βάσης δεδομένων. Επιπλέον, οι τρόποι με τους οποίους θα λάβει τα δεδομένα το SIEM ποικίλλουν. Ένας τρόπος είναι να αναπτυχθούν πράκτορες (agents) στις πηγές δεδομένων, έτσι οι πράκτορες θα συλλέγουν τοπικά στις πηγές τα δεδομένα και θα τα στέλνουν στον κεντρικό server του SIEM. Ένας άλλος τρόπος είναι χωρίς την ανάπτυξη πρακτόρων, έτσι οι πηγές θα στέλνουν δεδομένα μέσω διαφόρων δικτυακών πρωτοκόλλων όπως για παράδειγμα η χρήση API και του syslog πρωτοκόλλου.
- Κανονικοποίηση Δεδομένων: Η κανονικοποίηση των δεδομένων σε ένα περιβάλλον SIEM χρειάζεται γιατί τα δεδομένα που λαμβάνει το σύστημα διαφέρουν αρκετά ως προς την μορφή τους. Για παράδειγμα, το σύστημα θα δέχεται δεδομένα από Τείχη Προστασίας, από

συστήματα IDS/IPS, logs από τερματικά συστήματα κ.α. Όλα αυτά τα διαφορετικά δεδομένα θα πρέπει να έρθουν σε μια κοινή και συμβατή μορφή έτσι ώστε να γίνει ομαλότερη η αποθήκευση και η ανάλυσή τους σε μεταγενέστερο χρόνο.

- Αποθήκευση Δεδομένων: Μετά την κανονικοποίηση των δεδομένων τα δεδομένα αυτά θα πρέπει να αποθηκευτούν για πολλούς και διάφορους λόγους. Ο κυριότερος λόγος είναι η ανάλυση τους. Η μηχανές ανάλυσης θα πρέπει να έχουν πρόσβαση στα δεδομένα για να τα αναλύσουν είτε σε πραγματικό χρόνο είτε ετεροχρονισμένα. Επίσης η αποθήκευση δεδομένων συμβάλει στην διαδικασία της ανάπτυξης του χρονοδιαγράμματος ενός περιστατικού ασφαλείας και βοηθάνε πολύ την εγκληματολογική έρευνα. Τέλος τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν για την εκμάθηση μοντέλων μηχανικής μάθησης ως προς την ανίχνευση απειλών ή επιθέσεων.
- Alerting (Ειδοποιήσεις): Η διαδικασία της ειδοποίησης σε ένα περιβάλλον SIEM είναι πολύ σημαντική. Μετά την ανίχνευση ενός πιθανού περιστατικού ασφαλείας, μια ανωμαλίας ή ενός συμβάντος που χρειάζεται ανάλυσης από ειδικό αναλυτή, οι υπεύθυνοι κυβερνοασφάλειας θα πρέπει με κάποιον τρόπο να ενημερωθούν έγκαιρα. Ένα SIEM παρέχει τη δυνατότητα της έγκαιρης ειδοποίησης με πολλούς τρόπους. Για παράδειγμα μπορεί να στείλει e-mail, να στείλει sms, να εμφανίσει μια ειδοποίηση σε μια εφαρμογή διαχείρισης πιθανόν περιστατικών και άλλα. Με αυτόν τον τρόπο οι αρμόδιοι ενημερώνονται εγκαίρως για όποιες πιθανές απειλές υπάρχουν στο δίκτυο και στα πληροφοριακά τους συστήματα.
- Συσχέτιση δεδομένων/συμβάντων: Η διαδικασία της συσχέτισης είναι μια σημαντική διεργασία για ένα SIEM καθώς περιλαμβάνει την διαδικασία της ανάλυσης συμβάντων με σκοπό την αναγνώριση πιθανών απειλών ασφαλείας μέσω αναγνώρισης μοτίβων και συσχετίσεων. Ο κύριος σκοπός της συσχέτισης συμβάντων είναι η επεξεργασία ακατέργαστων δεδομένων και η εξαγωγή αξιοποιήσιμων πληροφοριών, συσχετίζοντας φαινομενικά άσχετα συμβάντα/δεδομένα και έτσι μπορεί να γίνει εντοπισμός περιστατικών ασφαλείας που διαφορετικά θα μπορούσαν να περάσουν απαρατήρητα από το σύστημα. Ο τρόπος με τον οποίο γίνεται η διαδικασία της συσχέτισης είναι μέσω κανόνων. Για να δημιουργηθούν αυτοί οι κανόνες, έμπειροι μηχανικοί ανίχνευσης (detection engineers) καταρτίζουν ένα σύνολο από κανόνες και τους θέτουν σε εφαρμογή. Επιπλέον οι δημιουργία κανόνων θα πρέπει να γίνεται με προσοχή έτσι ώστε να μην δημιουργούνται κανόνες οι οποίοι θα ανιχνεύουν "κακόβουλες ενέργειες" οι οποίες στην πραγματικότητα είναι νόμιμες και δεν είναι κακόβουλες.
- Οπτικοποίηση Δεδομένων: Η οπτικοποίηση δεδομένων αναφέρεται στην γραφική απεικόνιση των πληροφοριών που σχετίζονται με την ασφάλεια των συστημάτων. Τέτοιες πληροφορίες για παράδειγμα μπορεί να είναι ο αριθμός τον πακέτων που περνάνε από ένα firewall. Η απεικόνιση συχνά γίνεται μέσα από dashboards που περιλαμβάνουν γραφήματα, διαγράμματα, μπάρες και σχήματα. Μέσω των dashboards οι αναλυτές που θα παρακολουθούν το SIEM θα είναι σε θέση να κατανοήσουν σε τη κατάσταση βρίσκεται η υποδομή που παρακολουθούν σε πραγματικό χρόνο και έτσι να παίρνουν πιο σωστές και ολοκληρωμένες αποφάσεις.

3.1.6 Σενάριο εντοπισμού και απόκρισης σε κυβερνοεπίθεση βάση το παραδοσιακού τρόπου

Στο συγκεκριμένο υποκεφάλαιο θα αναλυθεί πως γίνεται ο εντοπισμός και η απόκριση σε ένα περιστατικό ασφαλείας βάση της παραδοσιακής μεθόδου στο πλαίσιο ενός Security Operation Center.

Αρχικά, ο αναλυτής αναμένει για τις ειδοποιήσεις που του έρχονται στην κονσόλα του SIEM. Από την στιγμή που θα έρθει μια ειδοποίηση, ξεκινάει μιας πρώτης τάξεως ανάλυση για να διαπιστωθεί ποιο σύστημα φαίνεται να επηρεάζεται και κατά πόσο είναι αληθινή η ειδοποίηση για το περιστατικό ασφαλείας που του έχει εμφανιστεί, καθώς υπάρχει περίπτωση να μην είναι ένα πραγματικό περιστατικό ασφαλείας. Όλη αυτή η διαδικασία της ανάλυσης παραδοσιακά γίνεται χειροκίνητα, δηλαδή ο αναλυτής θα πρέπει να αναλύσει όλα τα δεδομένα μόνος του, πηγαίνοντας από αρχεία καταγραφής σε αρχεία καταγραφής, συλλέγοντας πληροφορίες από διαφορετικά συστήματα καταγραφής, ώστε να είναι σε θέση να βγάλει ένα σωστό τελικό πόρισμα. Ο αναλυτής εκτός από τα εργαλεία που του διαθέτει το SOC σε τοπικό επίπεδο, έχει στην διάθεση του και πολλά online εργαλεία που τον βοηθάνε στην ανάλυση και στην τελική του ετυμηγορία. Κάποια από τα online εργαλεία είναι τα παρακάτω:

- VirusTotal[58]: Το VirusTotal είναι μια online πλατφόρμα στην οποία κάποιος μπορεί να υποβάλλει ένα αρχείο, ένα URL, μια IP ή ένα hash, και το VirusTotal θα κάνει μια ανάλυση και θα επιστρέψει ένα αποτέλεσμα, εάν δηλαδή κάτι είναι κακόβουλο.
- AbuseIPDB[59]: Το AbuseIPDB είναι μια online πλατφόρμα στην οποία γίνεται η συλλογή των IPs που αναφέρονται ως κακόβουλες ή που έχουν χρησιμοποιηθεί για παράνομες ενέργειες.
- Cisco Talos Reputation Lookup[60]: Το Cisco Talos Reputation Lookup είναι μια υπηρεσία που προσφέρεται online μέσω του Cisco Talos. Αυτή η υπηρεσία προσφέρει την δυνατότητα στον χρήστη να αναζητήσει ένα URL, ένα domain ή μια IP με σκοπό να μάθει ιστορικά δεδομένα για τις συγκεκριμένες οντότητες στο διαδίκτυο.
- urlscan.io[61]: Το urlscan.io είναι μια online πλατφόρμα στην οποία ο χρήστης υποβάλλει ένα URL και του επιστρέφετε μια μικρή έκθεση/αναφορά σχετικά με την συμπεριφορά της ιστοσελίδας και αν βρέθηκε κάτι κακόβουλο.
- AnyRun sandbox[62]: Το AnyRun είναι μια online πλατφόρμα για την ανάλυση κακόβουλου λογισμικού. Ο χρήστης ανεβάζει το αρχείο που θέλει να αναλυθεί και το AnyRun το αναλύει και επιστρέφει στον χρήστη τα χαρακτηριστικά τα οποία μπορούν να είναι κακόβουλα ή ύποπτα.
- AlienVault OTX[63]: Το AlienVault OTX είναι μια online πλατφόρμα για τον διαμοιρασμό πληροφοριών σχετικά με απειλές, για παράδειγμα IOCs, IP που έχουν χρησιμοποιηθεί σε malware campaings κ.α.
- Shodan[64]: Το Shodan είναι μια online πλατφόρμα που βοηθάει τους χρήστες να βρουν διάφορα χαρακτηριστικά από υπολογιστικά συστήματα που είναι με κάποιον τρόπο προσβάσιμα στο διαδίκτυο. Οι αναλυτές συνήθως το χρησιμοποιούν για να βρουν πληροφορίες σχετικά με διευθύνσεις IP που φέρονται να ανήκουν στην υποδομή ενός κακόβουλου χρήστη ή μιας κακόβουλης ομάδας.

- Censys[65]: Το Censys είναι μια online πλατφόρμα παρόμοια με το Shodan που αναφέρθηκε παραπάνω. Οι αναλυτές συνήθως χρησιμοποιούν πάνω από μια πλατφόρμα του ίδιου σκοπού, είτε για να διασταυρώσουν πληροφορίες είτε για την εξεύρεση νέων πληροφοριών.
- Cuckoo sandbox[66]: Το Cuckoo sandbox είναι μια online πλατφόρμα παρόμοια με το AnyRun που αναφέρθηκε παραπάνω. Η ιδιαιτερότητα του είναι πως είναι ανοιχτού κώδικα και ο καθένας μπορεί να δει τον πηγαίο κώδικα του Cuckoo και να τον αναλύσει.

Εάν ο αναλυτής, μετά την ανάλυση που έκανε, καταλήξει πως δεν είναι ένα πραγματικό περιστατικό ασφαλείας και είναι ένα False Positive Alert, τότε μαρκάρει την ειδοποίηση ως False Positive και γράφει ένα μικρό κείμενο για ποιον λόγω θεωρεί πως είναι False Positive. Στην περίπτωση που καταλήξει πως βρίσκετε αντιμέτωπος με ένα πραγματικό περιστατικό ασφαλείας περνάει στην φάση της απόκρισης στο περιστατικό. Ανάλογα με το περιστατικό ασφαλείας, ο αναλυτής θα ενεργήσει κατάλληλα. Για παράδειγμα, εάν το περιστατικό δεν είναι τόσο σοβαρό μπορεί να ενεργήσει και μόνος του. Στην περίπτωση που το περιστατικό είναι σοβαρό τότε θα πρέπει να ενημερώσει κάποιον ανώτερο ή την Ομάδα Απόκρισης Περιστατικών (Incident Response Team). Ο βασικός και παραδοσιακός τρόπος απόκρισης είναι και αυτός χειροκίνητος. Για παράδειγμα, στην περίπτωση που ένας Web Server έχει μολυνθεί από κακόβουλο λογισμικό και οι κακόβουλοι χρήστες έχουν πρόσβαση σε αυτόν, το incident response team αποφασίζει πως ο server πρέπει να απομονωθεί από το υπόλοιπο δίκτυο. Οι παραδοσιακοί τρόποι για να συμβεί αυτό είναι οι παρακάτω:

- 1η περίπτωση: Ο server έχει επάνω του EDR sensor. Με την ευκολία που παρέχει το EDR, το incident response team αναγνωρίζει τον server μέσω της EDR πλατφόρμας και τον απομονώνει από το υπόλοιπο δίκτυο μέσω των δυνατοτήτων που προσφέρει ο EDR sensor.
- 2η περίπτωση: Ο server δεν έχει EDR sensor και έτσι το incident response team λαμβάνει την απόφαση να επικοινωνήσει με τους τεχνικούς δικτύου για να απομονώσουν τον server με κάποια τεχνική όπως τμηματοποίηση δικτύου, απομόνωση υποδικτύου, λίστα ελέγχου πρόσβασης (Access Control List), κ.α.
- 3η περίπτωση: Ο server δεν είναι προσβάσιμος μέσω κάποιας τεχνικής απομακρυσμένης πρόσβασης (remote control) και είτε το incident response team είτε κάποιος τεχνικός δικτύου θα πρέπει να μεταβεί στον φυσικό χώρο που βρίσκετε ο server και να του αφαιρέσει το φυσικό μέσο (Ethernet cable) που δίνει πρόσβαση στο δίκτυο.

3.2 Νέοι τρόποι και λύσεις εντοπισμού και απόκρισης σε κυβερνοεπιθέσεις

Στο σύγχρονο τοπίο της διασυνδεδεμένης παγκόσμιας κοινωνίας μας, η εξάπλωση των επιθέσεων στον κυβερνοχώρο έχει φτάσει σε πρωτοφανή επίπεδα αποτελώντας σημαντική απειλή για τους οργανισμούς, για ολόκληρα έθνη και ακόμη και για τους ανθρώπους. Η διασφάλιση της προστασίας των ευαίσθητων δεδομένων αλλά και των δεδομένων εν γένει και η διατήρηση της ακεραιότητας των ψηφιακών και πληροφοριακών συστημάτων απαιτεί τη μέγιστη δυνατή εγρήγορση. Εντούτοις, είναι σημαντικό να αναγνωρίσουμε σε αυτό το σημείο ότι οι παραδοσιακές μεθοδολογίες που χρησιμοποιούνται παραδοσιακά για το κομβικό αυτό έργο, επιβαρύνονται από μείζονος σημασίας(αξιοσημείωτους) περιορισμούς. Στο υποκεφάλαιο αυτό θα διερευνηθούν κάποιοι επιπλέον νέοι τρόποι και τεχνολογίες που βοηθούν στον εντοπισμό απειλών και επιθέσεων. Θα αναλυθούν νέοι και καινοτόμοι τρόποι σαν μεμονωμένες λύσεις και τεχνολογίες, διότι έχει ήδη αναλυθεί μια δομή γύρω από νέους τρόπους και διαδικασίες στο κεφάλαιο 2 όπου αναλύεται η αρχιτεκτονική XDR. Νέοι τρόποι εντοπισμού και απόκρισης σε κυβερνοεπιθέσεις μπορούν να εφαρμοστούν και σε αρχιτεκτονικές εκτός XDR.

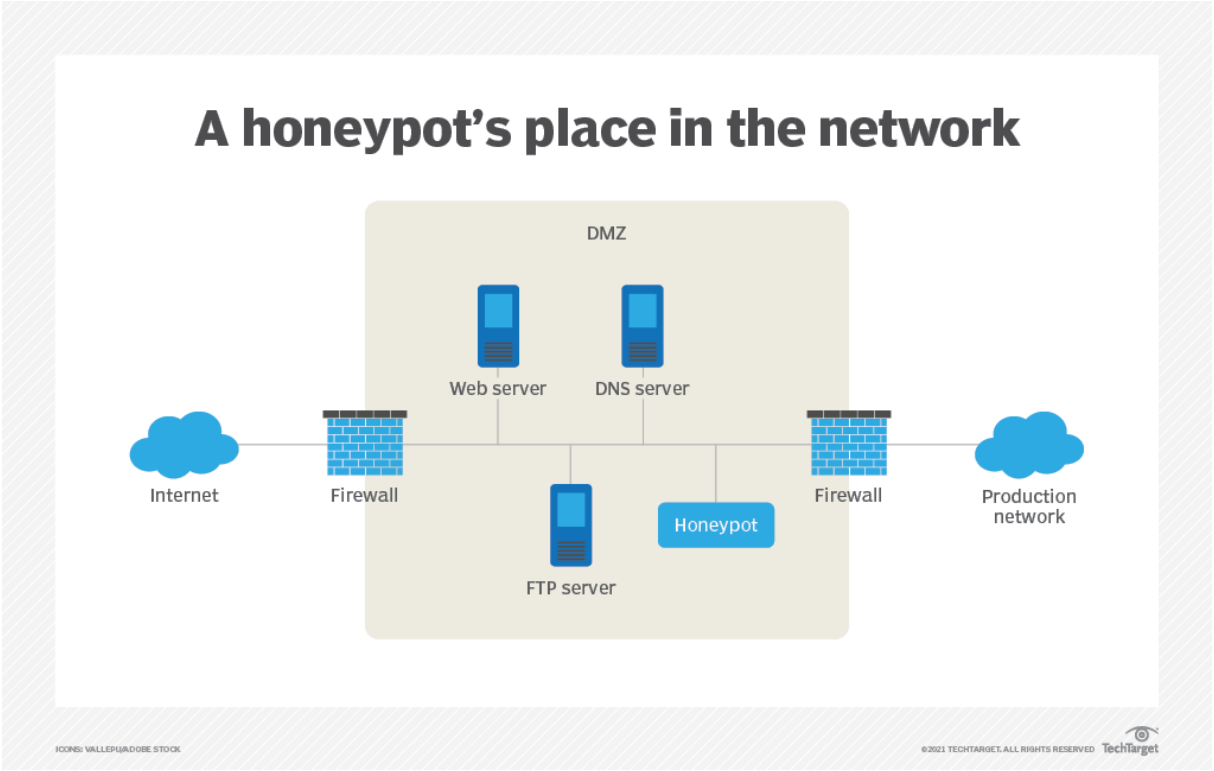
3.2.1 Honeypots

Τα honeypots είναι ένα μηχανισμός αντιπερισπασμού του επιτιθέμενου. Ένα honeypot δεν είναι ένα πραγματικό σύστημα αλλά ένα ψεύτικο σύστημα που μοιάζει με πραγματικό[74]. Ο σκοπός ενός honeypot είναι να αποπροσανατολίσει τον επιτιθέμενο από τον πραγματικό στόχο και να τον κάνει να χάσει χρόνο προσπαθώντας να επιτεθεί σε ένα σύστημα που δεν θα του παράσχει ούτε σημαντικές πληροφορίες αλλά ούτε και ένα σημείο για αναπήδηση σε ένα άλλο σημείου του δικτύου. Το honeypot μπορεί να τοποθετηθεί είτε στο εσωτερικό ενός δικτύου (π.χ DMZ ή σε περιοχή του δικτύου με αυξημένους δείκτες πιθανής εκδήλωσης επίθεση), είτε στο Διαδίκτυο. Η εκάστοτε τοποθέτηση εξυπηρετεί και διαφορετικούς σκοπούς και για αυτόν τον λόγο υπάρχουν οι δυο κύριες κατηγορίες:

- Honeypot για ερευνητικούς σκοπούς: Αυτά τα honeypot συνήθως τοποθετούνται στο Διαδίκτυο (Internet) για να προσελκύουν περισσότερους επιτιθέμενους. Ο σκοπός τους είναι καθαρά ερευνητικός. Έτσι, οι πληροφορίες που συλλέγονται είναι γύρω από τις συμπεριφορές του επιτιθέμενου στο σύστημα και τις τεχνικές που χρησιμοποίησε για να επιτεθεί στο σύστημα. Μετά την ανάλυση αυτών των πληροφοριών, οι ερευνητές ασφαλείας μπορούν να έχουν μια φρέσκια άποψη σχετικά με τις τεχνικές και τα συμπεριφορικά μοντέλα των επιθέσεων που γίνονται αυτή τη στιγμή στον κυβερνοχώρο.
- Honeypot για σκοπούς άμυνας και έγκυρης προειδοποίησης: Αυτά τα honeypot συνήθως τοποθετούνται σε πραγματικά πληροφοριακά συστήματα και δίκτυα. Ο σκοπός τους είναι η άμεση προειδοποίηση για μια υπάρχουσα ή επικείμενη επίθεση. Από την στιγμή που εμφανιστεί κάποια ειδοποίηση για παράξενη κίνηση στο honeypot θα πρέπει να ξεκινήσουν και οι κατάλληλες διαδικασίες του incident response. Οι αναλυτές θα πρέπει να αναλύσουν τα δεδομένα και να διαπιστώσουν αν πρόκειται για πραγματική παραβίαση του honeypot. Έπειτα, θα πρέπει να καταγράψουν τις κινήσεις του επιτιθέμενου μέσα στο honeypot, να αναγνωρίσουν συμπεριφορικά μοντέλα, τεχνικές και εργαλεία που χρησιμοποιεί ο επιτιθέμενος, με σκοπό να αναζητήσουν τα ίδια και στα συστήματα παραγωγής και στο δίκτυο παραγωγής.

Επίσης, ανάλογα με το πως αλληλεπιδρά ο επιτιθέμενος με το honeypot υπάρχουν και δύο παρακάτω τύποι:

- Honeypot χαμηλής αλληλεπίδρασης: Αυτό το είδος honeypot χρησιμοποιείται για να παρομοιάσει μια συγκεκριμένη υπηρεσία, για παράδειγμα ένα SSH Honeypot ή ένα RDP Honeypot. Αυτά τα honeypot δεν χρειάζονται πολλούς υπολογιστικούς πόρους και είναι εύκολα να εγκατασταθούν και να ρυθμιστούν.
- Honeypot υψηλής αλληλεπίδρασης: Αυτό το είδος honeypot χρησιμοποιείται για να παρομοιάσει ένα πραγματικό υπολογιστικό σύστημα ή ένα πραγματικό δίκτυο με υπηρεσίες. Σε αυτή την περίπτωση ο επιτιθέμενος θα πρέπει να σπαταλήσει περισσότερο χρόνο για να εξερευνήσει και να εκμεταλλευτεί όποιες ευπάθειες έχει το honeypot. Αυτά τα honeypot χρειάζονται πολλούς υπολογιστικούς πόρους, διότι προσομοιάζουν ένα πραγματικό πληροφοριακό σύστημα ή δίκτυο και η σωστή εγκατάσταση και ρύθμιση τους είναι δύσκολη και περίπλοκη.

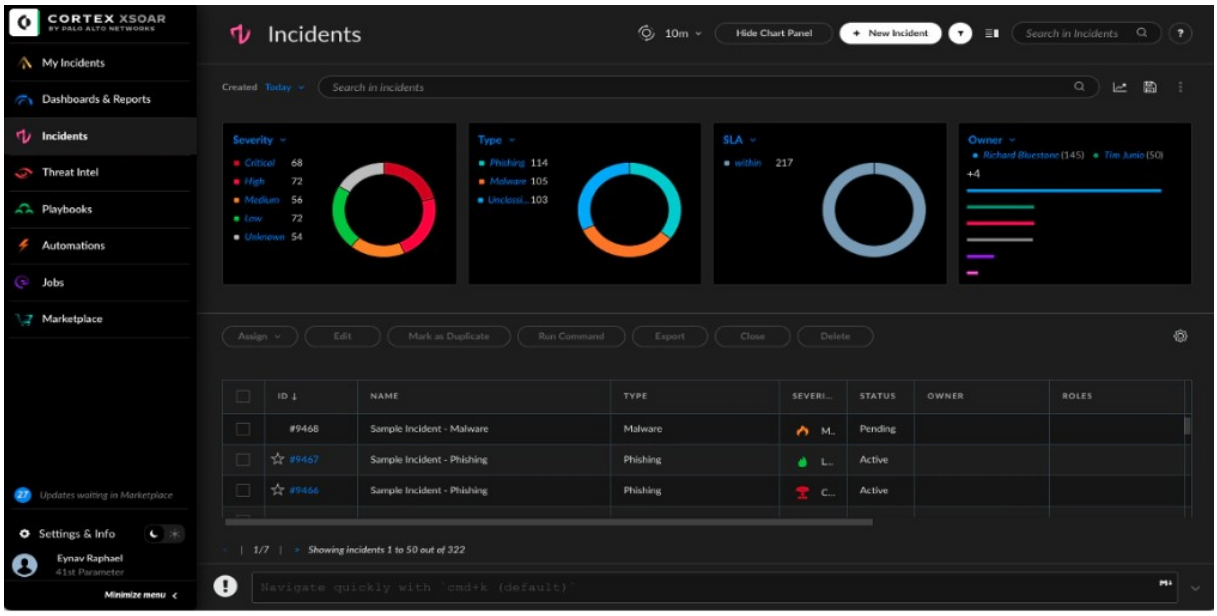


Σχήμα 3.2.1: Παράδειγμα θέσης τοποθέτησης ενός honeypot στο δίκτυο [75]

Τέλος, θα πρέπει να υπάρχει μεγάλη προσοχή όταν εγκαθιστάτε και ρυθμίζετε ένα honeypot γιατί η λανθασμένη ρύθμιση του μπορεί να θέσει σε κίνδυνο την υποδομή παραγωγής. Τελικός όμως τα θετικά που προκύπτουν από την χρήση των honeypots υπερτερούν των κινδύνων από την χρήση honeypots.

3.2.2 Security orchestration, automation, and response (SOAR)

Το SOAR μπορεί να χαρακτηριστεί ως μια πλατφόρμα η οποία ενσωματώνη μια πληθώρα από εργαλεία και τεχνολογίες κυβερνοασφάλειας που βοηθάνε σε τρεις τομής. Την ενορχήστρωση της κυβερνοασφάλειας, την αυτοματοποίηση ενεργειών ασφαλείας και την απόκριση σε περιστατικά ασφαλείας. Στον τομέα της ενορχήστρωσης γίνεται η διευθέτηση για το πως θα συνεργάζονται και θα επικοινωνούν τα διάφορα εργαλεία και τεχνολογίες κυβερνοασφάλειας που ενσωματώνονται στον SOAR κορμό. Έτσι, όταν προκύπτει ένα περιστατικό ασφαλείας το SOAR θα μπορεί να ξεκινάει αυτόματα μια σειρά από προεπιλεγμένες ενέργειες σε κάθε ένα από τα εργαλεία κυβερνοασφάλειας που έχει στην φαρέτρα του. Στον τομέα της αυτοματοποίησης ενεργειών ασφαλείας το SOAR είναι σε θέση να αυτοματοποιήσει μια σειρά από διεργασίες που μέχρι πρότινος έπρεπε να εκτελεστούν χειροκίνητα από κάποιον αναλυτή. Για παράδειγμα η συλλογή και η ανάλυση των δεδομένων, η συσχέτιση τους, η επαλήθευση περιστατικού ασφαλείας και τέλος οι ενέργειες για την αντιμετώπιση του περιστατικού ασφαλείας που εκδόθηκε. Στον τομέα της απόκρισης σε περιστατικά ασφαλείας διευκολύνει την τακτική διαχείριση των περιστατικών διαθέτοντας μια σειρά από διευκολύνσεις όπως για παράδειγμα εγχειρίδιο για την σωστή αντιμετώπιση κάθε είδους περιστατικού ασφαλείας. Επίσης μπορεί να διαθέτει στους αναλυτές μια ενοποιημένη πλατφόρμα για την προβολή των αυτοματοποιημένων ενεργειών που εκτελούνται αυτή τη στιγμή αλλά και ιστορικά δεδομένα και πληροφορίες για παρελθοντικές αυτοματοποιημένες ενέργειες.



Σχήμα 3.2.2: Απεικόνιση της SOAR πλατφόρμας της Palo Alto Networks [76]

Επιπλέον το SOAR μπορεί να ενσωματώσει Ροές Πληροφοριών για Κυβερνοεπιθέσεις (CTI feeds) με σκοπό την τροφοδότηση των εργαλείων και των αναλυτών με επικαιροποιημένα δεδομένα σχετικά με τις απειλές που υπάρχουν αυτή τη στιγμή στον κυβερνοχώρο. Τέλος η προσέγγιση που προσφέρει μια SOAR πλατφόρμα συνδυάζοντας ενορχήστρωση, αυτοματοποίηση και απόκριση, ενισχύει σημαντικά τις δυνατότητες για άμεση επίλυση περιστατικών ασφαλείας και δίνει αρκετά εργαλεία και δυνατότητες στους αναλυτές να επιλύουν σε πραγματικό χρόνο το οποιοδήποτε περιστατικό ασφαλείας προκύψει.

Κεφάλαιο 4ο: Ανάλυση του OpenC2 πρωτοκόλλου και του OVAL προτύπου

4.1 Ανάλυση του OpenC2 πρωτοκόλλου

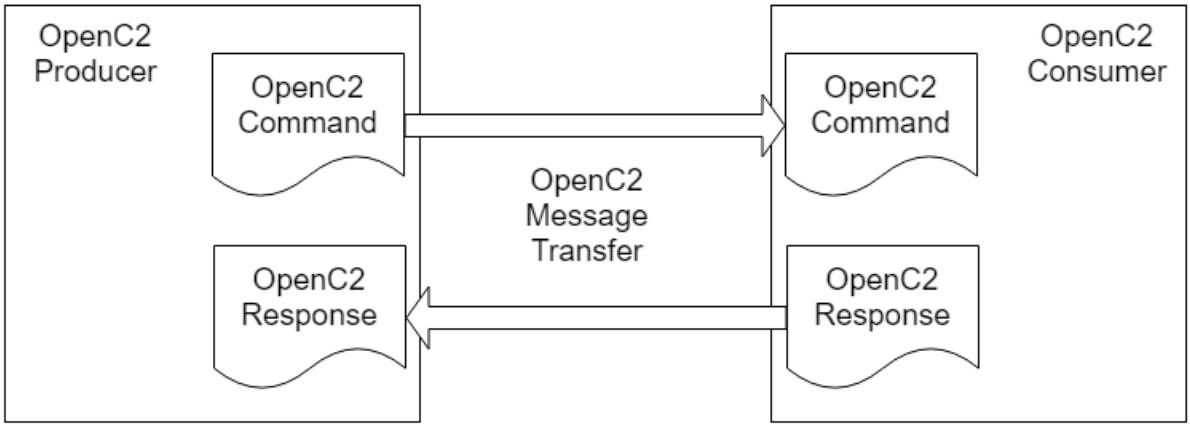
Αν μπορούσαμε με μια πρόταση να δώσουμε έναν ορισμό για το OpenC2 σε γενικό πλαίσιο η πρόταση είναι η εξής: "Το OpenC2 είναι μια τυποποιημένη γλώσσα για τη διεύθυνση και τον έλεγχο τεχνολογιών που παρέχουν ή υποστηρίζουν αμυντικές δυνατότητες στον κυβερνοχώρο"[40]. Στην ερώτηση "Ποια ανάγκη έρχεται να καλύψει το OpenC2;", η απάντηση έχει ως εξής: Το OpenC2 αναπτύχθηκε για να καλύψει την ανάγκη ύπαρξη μιας τυποποιημένης γλώσσας για την δημιουργία αμφίδρομης επικοινωνίας, δηλαδή command and control, μεταξύ διαφορετικών τεχνολογιών και συστημάτων ασφάλειας. Η βασική αδυναμία των συμβατικών/παραδοσιακών αμυντικών συστημάτων έγκειται στην αδυναμία τους να επικοινωνούν και να συνεργάζονται αποτελεσματικά μεταξύ διαφορετικών τεχνολογιών, πλατφορμών και μηχανημάτων. Αυτή την αδυναμία προσπαθεί να λύση το OpenC2, έτσι ώστε οι αρχιτεκτονικές που εφαρμόζονται αυτή τη στιγμή να μεταβούν από το απομονωμένο και με επίκεντρο το προϊόν πλαίσιο σε ένα πιο διαλειτουργικό και διασυνδεδεμένο πλαίσιο/πλάνο. Το OpenC2 είναι ένα βασικό στοιχείο για τον εξορθολογισμό των επικοινωνιών μεταξύ μηχανών, προσφέροντας μια γλώσσα με την οποία θα μπορούν να μιλούν όλα τα μηχανήματα μεταξύ τους, ανεξαρτήτως κατασκευαστή και αρχιτεκτονικής. Κύριος στόχος του είναι η ενορχήστρωση στοιχείων και συστημάτων κυβερνοάμυνας, υπερβαίνοντας τις όποιες ιδιαιτερότητες ή δυσκολίες από συγκεκριμένα προϊόντα ή τεχνολογίες ασφαλείας. Αυτή η προσέγγιση διασφαλίζει την προσαρμοστικότητα στις εξελισσόμενες απειλές, βοηθώντας τους οργανισμούς να παραμείνουν σε ένα καλό επίπεδο ωριμότητας έναντι των απειλών. Επίσης, η τυποποιημένη γλώσσα που προσφέρει το OpenC2 επιτρέπει τη σαφή και αδιαμφισβήτητη επικοινωνία μεταξύ μηχανών, μειώνοντας τον κίνδυνο παρερμηνειών και ενισχύοντας τη συνολική αποτελεσματικότητα των επιχειρήσεων κυβερνοάμυνας. Επιπλέον να αναφερθεί ότι το OpenC2 αναπτύσσεται από τον OASIS (Organization for the Advancement of Structured Information Standards). Ο OASIS είναι μια μη κερδοσκοπική κοινοπραξία που προωθεί την ανάπτυξη, τη σύγκλιση και την υιοθέτηση ανοικτών προτύπων για την κοινότητα της κυβερνοασφάλειας αλλά και της πληροφορικής στο σύνολο. Τέλος, στην ανάπτυξη του OpenC2 βοηθούν ανεξάρτητοι ερευνητές κυβερνοασφάλειας, μεγάλοι οργανισμοί και κυβερνητικοί φορείς όπως για παράδειγμα η NSA[39].

4.1.1 Η αρχιτεκτονική του OpenC2

Η αρχιτεκτονική του OpenC2 έχει σχεδιαστεί με τέτοιον τρόπο έτσι ώστε να μπορεί να υλοποιεί στην πράξη όσα υποστηρίζει ότι μπορεί να κάνει το OpenC2 σε θεωρητικό επίπεδο. Στην αρχιτεκτονική του OpenC2 μπορούμε να διακρίνουμε πολλά μέρη αλλά τα κυριότερα και σημαντικότερα είναι τα εξής τέσσερα[42][41]:

- OpenC2 παραγωγοί: Οι OpenC2 παραγωγοί έχουν ως κύριο ρόλο την δημιουργία OpenC2 εντολών. Είναι αυτοί που όταν εντοπιστεί μια επίθεση θα πρέπει εκδώσουν τις κατάλληλες εντολές. Οι εντολές αυτές είναι οδηγίες που καθορίζουν συγκεκριμένες ενέργειες που πρέπει να γίνουν από τους OpenC2 καταναλωτές ως απάντηση σε ένα συμβάν κυβερνοασφάλειας ή για προληπτικές ενέργειες και τροποποιήσεις στα υπάρχοντα μέτρα ασφαλείας ενός μηχανήματος.

- OpenC2 καταναλωτές: Οι OpenC2 καταναλωτές λαμβάνουν τις εντολές από τους OpenC2 παραγωγούς, τις ερμηνεύουν και τις εκτελούν.
- OpenC2 εντολή: Μια OpenC2 εντολή είναι ένα μήνυμα με συγκεκριμένη δομή που ορίζει μια ενέργεια που πρέπει να πραγματοποιηθεί από έναν OpenC2 καταναλωτή. Παρακάτω θα αναλυθεί λεπτομερώς η δομή ενός OpenC2 Command.
- OpenC2 απόκριση: Μια OpenC2 απόκριση είναι ένα μήνυμα που στέλνετε πίσω στον παραγωγό μιας OpenC2 εντολής, για να τον ενημερώσει αν ελήφθη η εντολή του και αν όλα πήγαν καλά με την ερμηνεία της και την εκτέλεσή της. Παρακάτω θα αναλυθεί λεπτομερώς η δομή ενός OpenC2 Response.



Σχήμα 4.1.1: Αφηρημένη απεικόνιση του κορμού της αρχιτεκτονικής που διέπει OpenC2 [42]

Επίσης, ως OpenC2 παραγωγοί μπορούν να χαρακτηριστούν τα εξής:

- Πλατφόρμες ενορχήστρωσης ασφαλείας (SOAR – Security Orchestration, automation and response)
- Συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM - Security Information and Event Management)
- Πλατφόρμες πληροφοριών για απειλές (TIP - Threat Intelligence Platforms)
- Προϊόντα ελέγχου πρόσβασης στο δίκτυο (NAC – Network Access Control)

Επιπλέον, ως OpenC2 καταναλωτές μπορούν να χαρακτηριστούν τα εξής:

- Τείχος προστασίας (Firewall)
- Συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS – Intrusion Detection and Prevention Systems)
- Ένας απλός τελικός κόμβος δικτύου (Π.χ IP camera, PC, Laptop, Printer)

Προχωρώντας συνεχίζουμε με την ανάλυση της δομής μιας OpenC2 εντολής. Όπως είδαμε και παραπάνω η εντολή δίνετε από ένα σύστημα (Producer) προς ένα άλλο ή άλλα συστήματα (Consumer(s)). Οι καταναλωτές θα πρέπει να ενεργήσουν βάση της εντολής που πήραν. Η εντολή περιγράφει μια ενέργεια που πρέπει να εκτελεστεί σε έναν στόχο και μπορεί να περιλαμβάνει πληροφορίες που προσδιορίζουν τον ενεργοποιητή ή τους ενεργοποιητές (Actuator(s)), που πρόκειται να εκτελέσουν την εντολή. Τα τέσσερα κύρια πεδία μιας OpenC2 εντολής είναι τα εξής[41]:

- Ενέργεια (Action): Με τον όρο “Ενέργεια”, περιγράφετε η ενέργεια που θα πρέπει να γίνει από το μηχάνημα που θα οριστεί στο πεδίο “Στόχος”. Είναι υποχρεωτικό πεδίο.
- Στόχος (Target): Με τον όρο “Στόχος”, περιγράφετε το μηχάνημα το οποίο θα δεχτεί την ενέργεια. Είναι υποχρεωτικό πεδίο.
- Παράμετροι (Arguments): Οι παράμετροι είναι συμπληρωματικοί και παρέχουν επιπλέον πληροφορίες για το πως θα πρέπει να εκτελεστεί η εντολή. Για παράδειγμα για πόσο χρονικό διάστημα θα εκτελεστεί. Είναι προαιρετικό πεδίο.
- Ενεργοποιητής (Actuator): Με τον όρο “Ενεργοποιητής”, περιγράφετε ο κατάλληλος μηχανισμός που είναι υπεύθυνος για να εκτελέσει την ενέργεια που έχει οριστεί στο πεδίο “Ενέργεια”. Είναι προαιρετικό πεδίο.

Μετά την δημιουργία και την αποστολή μια OpenC2 εντολής, ο OpenC2 παραγωγός περιμένει από το σύστημα που θα λάβει αυτή την εντολή να του επιστρέψει μια απάντηση, δηλαδή μια OpenC2 απόκριση. Μια OpenC2 απόκριση χαρακτηρίζεται το μήνυμα που στέλνει ένας παραλήπτης μιας εντολής πίσω στον αποστολέα της εντολής. Το ελάχιστο που πρέπει να περιέχει μια απόκριση για να θεωρηθεί έγκυρη, σε επίπεδο δομής του μηνύματος απόκρισης, από την πλευρά του παραλήπτη, είναι η πληροφορία σχετικά με το αποτέλεσμα της εκτέλεσης της εντολής. Για παράδειγμα αν η εντολή εκτελέστηκε επιτυχώς ή αν υπήρξε κάποιο πρόβλημα κατά την εκτέλεσή της. Αυτό του είδους η πληροφορία μπορεί να είναι ένας κωδικός κατάστασης (status code). Κάτι που συναντάμε και στο μήνυμα απάντησης ενός HTTP αιτήματος.

Συνεχίζοντας θα δούμε και θα αναλύσουμε διεξοδικά μια OpenC2 εντολή, έτσι ώστε να είμαστε εξοικειωμένοι με την μορφή της. Η εντολή είναι η εξής:

```
{
    "action": "deny",
    "target": {
        "ipv4_connection": {
            "protocol": "tcp",
            "src_addr": "1.2.3.4",
            "src_port": 10996,
            "dst_addr": "198.2.3.4",
            "dst_port": 80
        }
    },
    "args": {
        "start_time": 1534775460000,
        "duration": 500,
        "response_requested": "ack",
        "slpf": {
            "drop_process": "none"
        }
    },
    "actuator": {
        "slpf": {
            "asset_id": "30"
        }
    }
}
```

Σχήμα 4.1.2: Παράδειγμα OpenC2 εντολής

Από την παραπάνω OpenC2 εντολή είμαστε σε θέση να καταλάβουμε ότι η εντολή χρησιμοποιείτε για την ενέργεια της άρνησης μιας IPv4 σύνδεσης μεταξύ δυο μηχανημάτων. Ας εμβαθύνουμε περισσότερο όμως:

- "action": "deny" – Σαν ενέργεια ανατίθεται η λειτουργία της αποτροπής, με σκοπό να σταματήσει μια πράξη από την ολοκλήρωσή της.
- "target": { "ipv4_connection": - Σαν στόχος της ενέργειας deny τίθεται μια IPv4 σύνδεση με τα παρακάτω χαρακτηριστικά:
  - "protocol": "tcp" - Το πρωτόκολλο της σύνδεσης πρέπει να είναι TCP
  - "src_addr": "1.2.3.4" - Η IP διεύθυνση προέλευσης πρέπει να είναι η "1.2.3.4"
  - "src_port" : 10996 – Η πόρτα προέλευσης πρέπει να είναι η 10996
  - "dst_addr" : "192.2.3.4" – Η IP διεύθυνση προορισμού πρέπει να είναι η "192.2.3.4"
  - "dst_port" : 80 – Η πόρτα προορισμού πρέπει να είναι η 80 (Η 80 είναι η default port για το πρωτόκολλο HTTP)
- "args": - Εδώ περιγράφονται οι επιπλέον παράμετροι που συνήθως υπάρχουν για πολύ συγκεκριμένες λειτουργίες. Οι επιπλέον παράμετροι είναι:
  - "start_time": 1534775460000 – Η ακριβής ημερομηνία και ώρα που θα πρέπει να εκτελεστεί ο εντολή. Η μορφή της ακριβούς ημερομηνίας και ώρας είναι σε μορφή Epoch – Unix Time
  - "duration": 500 – Πόσα δευτερόλεπτα θα έχει ισχύς η εντολή
  - "response_requested": "ack" – Το είδος της απάντησης που περιμένει ο OpenC2 παραγωγός από τον OpenC2 καταναλωτή
  - "splf": { "drop_process" : "none"} – Είναι η οδηγία για το πως θα πρέπει να γίνει ο χειρισμός των πακέτων που θα μπλοκαριστούν
- "actuator": { "slpf": { "asset_id": "30" } } - Εδώ γίνεται ο ακριβής προσδιορισμός του ενεργοποιητή που θα εκτελέσει την ενέργεια της απόρριψης της IPv4 σύνδεσης

4.1.2 Τρόποι λειτουργίας των OpenC2 Παραγωγών, Καταναλωτών και Συσκευών

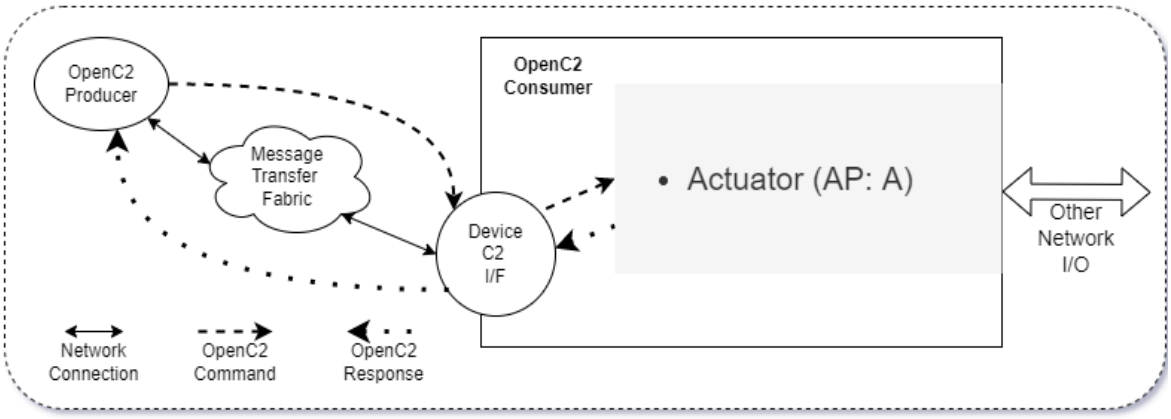
Σε αυτή την ενότητα θα μελετηθούν διάφοροι τρόποι με τους οποίους μπορούν να λειτουργούν οι OpenC2 Παραγωγοί, Καταναλωτές και Συσκευές. Παρακάτω εξετάζονται τέσσερις ενδεικτικοί σχεδιασμοί για μια συσκευή τύπου OpenC2 Καταναλωτής[42]:

1. Ο Καταναλωτής μπορεί να κάνει μόνο μία λειτουργία, έτσι ως αποτέλεσμα, υποστηρίζει μόνο ένα Προφίλ Ενεργοποιητή (Actuator Profile – AP). Ουσιαστικά είναι ο πιο απλός σχεδιασμός που μπορεί να έχει ένας OpenC2 καταναλωτής.
2. Ο Καταναλωτής υλοποιεί πολλαπλές λειτουργίες, έτσι ως αποτέλεσμα, υποστηρίζει πολλαπλά AP. Τα AP αυτά μπορεί να είναι διαφορετικά αλλά και ίδια και να υλοποιούν ίδιες ή διαφορετικές ενέργειες και διεργασίες.
3. Ο Καταναλωτής είναι ενός είδους διαχειριστής για μια σειρά από συσκευές. Με αυτό τον τρόπο λειτουργεί σαν ενδιάμεσος μεταξύ Παραγωγού και συσκευών που θα δεχτούν τις

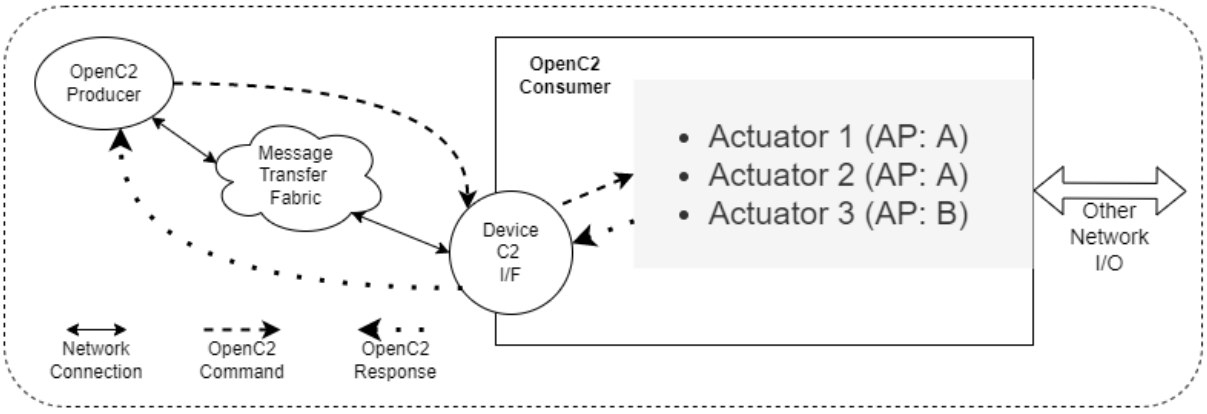
εντολές. Οι συσκευές που θα δεχτούν τις εντολές μπορεί να μην είναι όλες ίδιες και επίσης υπάρχει η περίπτωση να μην χρησιμοποιούν ή να καταλαβαίνουν το OpenC2 πρωτόκολλο.

4. Ο Καταναλωτής είναι ένας διαχειριστής για μια σειρά από συσκευές, όπου η διαχείριση αυτών των συσκευών γίνεται μέσω του OpenC2. Με αυτόν τον σχεδιασμό ο OpenC2 καταναλωτής μπορεί να έχει διττό ρόλο, του καταναλωτή αλλά και ενίοτε του παραγωγού.

Σε όλους τους παραπάνω σχεδιασμούς, ο όρος "συσκευή" αναφέρετε σε μια συσκευή που μπορεί να έχει φυσική ή εικονική υπόσταση σε οποιοδήποτε υπολογιστικό και πληροφοριακό περιβάλλον. Όταν αναφέρετε ο όρος "συσκευή" πρόκειται για μια συσκευή που λαμβάνει IP διεύθυνση και είναι προσβάσιμη στο δίκτυο για οποιαδήποτε ενέργεια. Αναλύοντας καλύτερα οι σχεδιασμοί 1 και 2, γίνεται αντιληπτό πως ο παραγωγός έχει άμεση και ρητή γνώση των Actuator Profiles (APs) που υπάρχουν στον καταναλωτή. Αυτή η γνώση επιτρέπει στον Παραγωγό να δίνει εντολές OpenC2 που επηρεάζουν άμεσα τη λειτουργία της συσκευής του Καταναλωτή. Ο σαφής δίαυλος επικοινωνίας επιτρέπει τον ακριβή έλεγχο και τον αποτελεσματικό συντονισμό μεταξύ του Παραγωγού και του Καταναλωτή, βελτιώνοντας τις λειτουργίες του συστήματος.



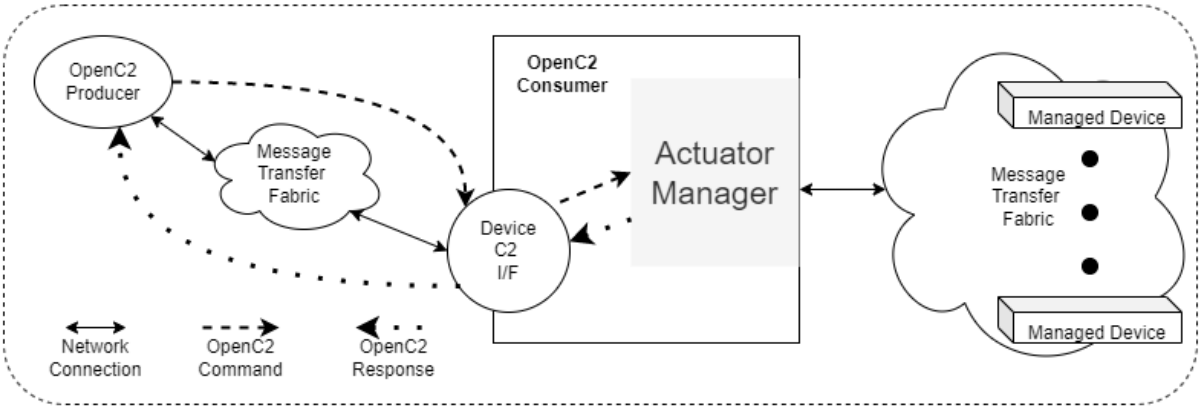
Σχήμα 4.1.3: Παράδειγμα 1ου σχεδιασμού [42]



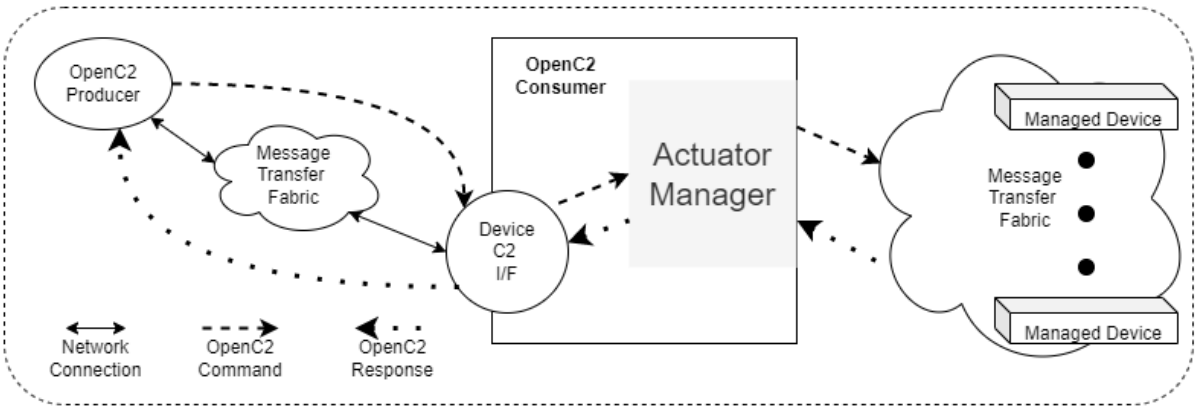
Σχήμα 4.1.4: Παράδειγμα 2ου σχεδιασμού [42]

Στους σχεδιασμούς 3 και 4, οι καταναλωτές υπάγονται σε μια αρχιτεκτονική τύπου "διαχειριστή". Ο παραγωγός έχει γνώση των δυνατοτήτων που υποστηρίζονται από τον διαχειριστή καταναλωτή, αλλά επηρεάζει μόνο έμμεσα τη λειτουργία των συσκευών στις οποίες θα στείλει τις OpenC2 εντολές. Στον σχεδιασμό 3 ο παραγωγός δεν γνωρίζει πως ο τρόπος επικοινωνίας μεταξύ του καταναλωτή και των συσκευών που διαχειρίζεται ο καταναλωτής, είναι εντολές και απαντήσεις OpenC2, ενώ στον

σχεδιασμό 4 ο τρόπος επικοινωνίας μεταξύ καταναλωτή και διαχειριζόμενων συσκευών βασίζεται ρητά στο OpenC2. Τέλος, μπορούν να υπάρξουν και σχεδιασμοί στους οποίους θα υπάρχει μια μίξη, δηλαδή ένα μέρος από τις διαχειριζόμενες συσκευές να μπορούν να κατανοούν το OpenC2 και κάποιες άλλες να μην έχουν την δυνατότητα ερμηνείας OpenC2 εντολών[42].



Σχήμα 4.1.5: Παράδειγμα 3ου σχεδιασμού [42]



Σχήμα 4.1.6: Παράδειγμα 4ου σχεδιασμού [42]

4.1.3 Η ασφάλεια του OpenC2 πρωτοκόλλου

Οι επιτιθέμενοι βλέπουν τα συστήματα κυβερνοάμυνας και κυβερνοασφάλειας ως πολύ κρίσιμους στόχους. Ο λόγος είναι απλός. Στην περίπτωση που μπορέσουν να επιτεθούν σε αυτά τα συστήματα και να τα θέσουν εκτός λειτουργίας, θα είναι σε θέση να εξαπολύουν τις επιθέσεις προς τα άλλα συστήματα που θέλουν να προσβάλουν χωρίς να τους εμποδίζει κανείς και χωρίς να φοβούνται αν γίνουν αντιληπτοί. Στην ακόμη χειρότερη περίπτωση, οι επιτιθέμενοι θα μπορούσαν να στρέψουν τα ίδια τα συστήματα ασφαλείας ενάντια της υποδομής που προστατεύουν. Η ασφάλεια στο πλαίσιο του OpenC2 κινείται σε δύο άξονες:

- Απειλές και επιθέσεις στα δίκτυα και συστήματα που δύναται να δράση το OpenC2
- Επιθέσεις που στοχεύουν το OpenC2 καθαυτό

Οι απειλές, οι επιθέσεις, τα τρωτά σημεία και οι επιπτώσεις σε μια υλοποίηση του OpenC2 θα πρέπει να αναλύονται με γνώμονα τους στόχους που θέλει να πετύχει ο επιτιθέμενος και στις επιπτώσεις που προκύπτουν. Οι απειλές μπορούν να χαρακτηριστούν στις τρεις παρακάτω κατηγορίες:

- Κακόβουλοι χρήστες (εξωτερικά και εσωτερικά του δικτύου): Χρήστες που έχουν ως στόχο την παράλυση του OpenC2 ως πρωτόκολλο επικοινωνίας
- Μη κακόβουλοι χρήστες: Λάθη χρηστών οι οποίοι δεν είχαν ως στόχο να βλάψουν και να προκαλέσουν κακό αλλά από το λάθος τους δημιουργούν σημαντικά κενά ασφαλείας και ασύμμετρες απειλές.
- Δομικές απειλές: Ως δομικές απειλές μπορούν να χαρακτηριστούν οι αστοχίες υλικού και τα σφάλματα λογισμικού, τα οποία μπορούν να επηρεάσουν την ακεραιότητα ή τη διαθεσιμότητα του OpenC2 πρωτοκόλλου

Επιπλέον, οι επιθέσεις μπορούν χαρακτηριστούν ως εξής:

- Παθητικές επιθέσεις: Ο επιτιθέμενος παρατηρεί την κυκλοφορία στο δίκτυο και έχει την δυνατότητα να διαβάζει τα μηνύματα που κυκλοφορούν στο δίκτυο. Για παράδειγμα, αν η OpenC2 κίνηση δεν είναι κρυπτογραφημένη, μπορεί να υποκλέψει την κίνηση και να εξάγει χρήσιμες πληροφορίες για την υποδομή του δικτύου που θα επιτεθεί αλλά και για τις επιθέσεις που πρόκειται να διαπράξει ή διαπράττει. Για παράδειγμα, θα μπορούσε καταλάβει αν οι επιθέσεις που εξαπολύει εκείνη τη στιγμή, έχουν γίνει αντιληπτές και επίσης θα μπορούσε και να χαρτογραφήσει μέχρι ενός συγκεκριμένου σημείου τις συσκευές που ελέγχονται μέσω OpenC2 εντολών.
- Ενεργητικές επιθέσεις (Εξωτερικά του δικτύου): Ένας επιτιθέμενος μπορεί να προσπαθήσει να τροποποιήσει την OpenC2 κυκλοφορία διαγράφοντας, καθυστερώντας ή επαναλαμβάνοντας τα OpenC2 μηνύματα. Επίσης μπορεί να προσπαθήσει να τροποποιήσει το περιεχόμενο ενός μηνύματος ή να παρουσιάσει τον εαυτό του σαν OpenC2 παραγωγό (Spoofing Attack)[67] και να στέλνει αυτός μηνύματα. Αν κάποιες από αυτές τις ενέργειες πετύχουν, ο επιτιθέμενος μπορεί να παρεμποδίσει το OpenC2 από το να στείλει τις κατάλληλες αμυντικές εντολές προς τα συστήματα που έχουν δεχτεί μια επίθεση και έτσι να το εκτροχιάσει των καθηκόντων του.
- Επιθέσεις εκ των έσω: Ένας εσωτερικός χρήστης, ιδίως ένας χρήστης με αναβαθμισμένα προνόμια, μπορεί να είναι σε θέση να εκτελέσει με μεγαλύτερο βαθμό επιτυχίας οποιαδήποτε από τις παθητικές και ενεργητικές επιθέσεις που έχουν ήδη αναφερθεί και επιπλέον μπορεί να ενεργήσει ως εξουσιοδοτημένος χρήστης για να εκτελέσει άλλες ενέργειες, για παράδειγμα να καλύψει τα ίχνη του. Αυτές οι ενέργειες θα μπορούσαν να περιλαμβάνουν λανθασμένη ρύθμιση συσκευών, αλλαγή κανόνων πολιτικής ασφαλείας, έκδοση κακόβουλων εντολών από εξουσιοδοτημένες πηγές, ακόμη και απενεργοποίηση συστημάτων.
- Supply Chain Attacks: Οι επιθέσεις στην εφοδιαστική αλυσίδα μπορούν να συμβούν σε πολλαπλά επίπεδα εντός του OpenC2 οικοσυστήματος. 3 σημαντικά επίπεδα με μεγάλο βαθμό επιτυχίας μια τέτοιας επίθεσης είναι: Η εισαγωγή κακόβουλου κώδικα σε υλοποιήσεις εργαλείων που υποστηρίζουν OpenC2, στην παραποίηση των καναλιών διανομής (π.χ αποθετήρια λογισμικού και διακομιστές ενημερώσεων) και της παραβίασης της διαλειτουργικότητας μεταξύ εργαλείων που χρησιμοποιούν το OpenC2 για επικοινωνία.

Τέλος, είναι χρήσιμο να αναφερθούμε στο μοντέλο CIA[69] και τις τρεις αρχές του (Confidentiality – Εμπιστευτικότητα, Integrity – Ακεραιότητα , Availability – Διαθεσιμότητα) και ειδικότερα πως αυτές οι αρχές εφαρμόζονται στο γενικό πλαίσιο του OpenC2:

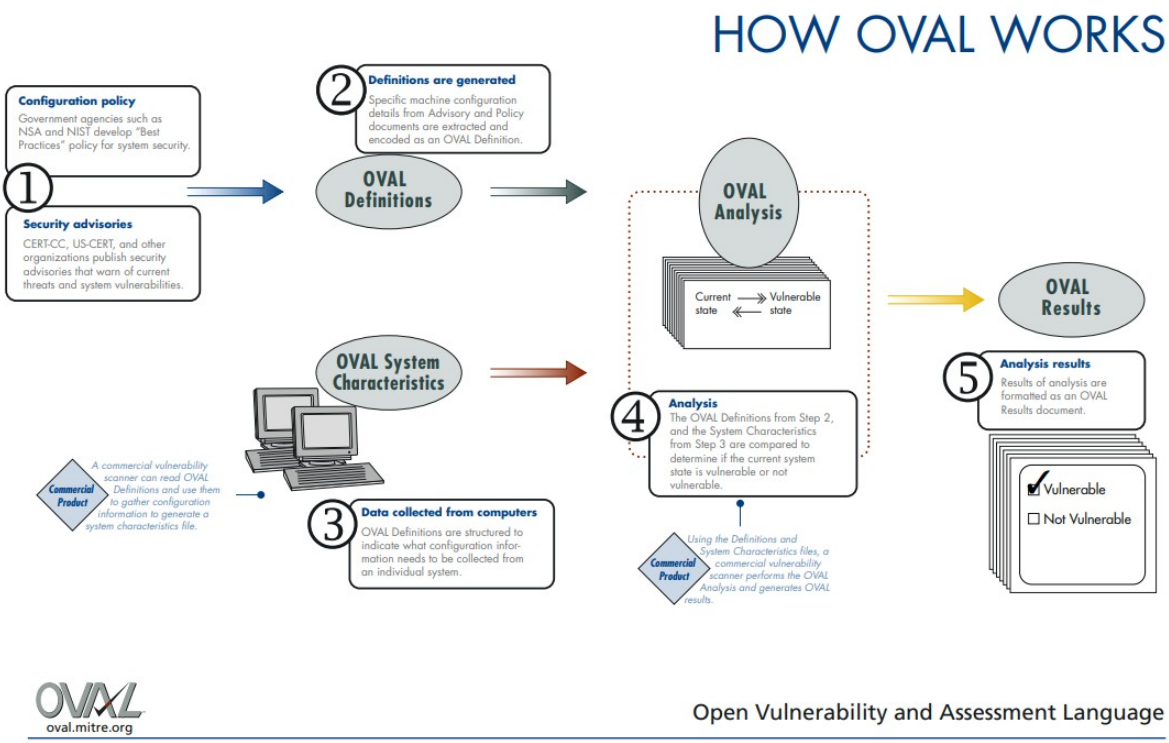
- Εμπιστευτικότητα στο OpenC2: Στο πλαίσιο του OpenC2 η εμπιστευτικότητα αναφέρεται στην προστασία των ευαίσθητων πληροφοριών που μεταφέρονται από το OpenC2. Περιλαμβάνει μηχανισμούς οι οποίοι δεν θα επιτρέπουν σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στα μηνύματα που μεταφέρονται μεταξύ OpenC2 καταναλωτή και παραγωγό. Η εμπιστευτικότητα μπορεί να διασφαλιστεί με την χρήση κρυπτογράφησης και ασφαλών πρωτοκόλλων επικοινωνίας.
- Ακεραιότητα στο OpenC2: Στο πλαίσιο του OpenC2 η ακεραιότητα εστιάζει στην διασφάλιση πως τα δεδομένα που μεταφέρονται θα παραμείνουν αναλλοίωτα καθώς μεταφέρονται μέσω των καναλιών μεταφοράς δεδομένων. Η ακεραιότητα μπορεί να διασφαλιστεί με την χρήση ψηφιακών υπογραφών και κρυπτογραφικών συναρτήσεων κατακερματισμού.
- Διαθεσιμότητα στο OpenC2: Στο πλαίσιο του OpenC2 η διαθεσιμότητα εστιάζει στην διασφάλιση πως η υποδομή του OpenC2 θα είναι σταθερά λειτουργική και δεν θα διαταράσσετε η λειτουργία της. Τρόποι με τους οποίους διασφαλίζετε η διαθεσιμότητα είναι οι λύσεις για προστασία από επιθέσεις άρνησης υπηρεσιών και η εξισορρόπηση φορτίου.

4.2 Ανάλυση του OVAL προτύπου

Το OVAL (Open Vulnerability and Assessment Language) είναι ένα πρότυπο που ως σκοπό έχει να παρέχει ένα τυποποιημένο και διαλειτουργικό πλαίσιο για την περιγραφή και αξιολόγηση των τρωτών σημείων ασφαλείας σε συστήματα υπολογιστών. Στόχος του είναι να καθιερώσει μια κοινή γλώσσα που να ενισχύει την συνοχή, να διευκολύνει τη διαλειτουργικότητα μεταξύ των εργαλείων ασφαλείας και να υποστηρίζει την αυτοματοποίηση των διαδικασιών αξιολόγησης και αποκατάστασης των ευπαθειών. Ο οργανισμός που ηγήθηκε της πρωτοβουλίας για την δημιουργία του OVAL προτύπου είναι ο οργανισμός MITRE[68] και το 2002 το OVAL έκανε την πρώτη του εμφάνιση. Αν και ο MITRE ήταν και είναι ο κύριος ηγέτης για το OVAL, ο χαρακτήρας του προτύπου είναι συνεργατικός. Έτσι πολλοί άνθρωποι από την ευρύτερη κοινότητα της κυβερνοασφάλειας συνεισφέρουν στην ανάπτυξη και συντήρηση του προτύπου.

Τα τρία κύρια στοιχεία που περιβάλουν την αρχιτεκτονική του OVAL προτύπου είναι τα εξής:

- OVAL γλώσσα
- OVAL αποθετήριο
- OVAL διερμηνέας (interpreter)



Σχήμα 4.2.1: Η λειτουργία του OVAL προτύπου [57]

4.2.1 Η OVAL γλώσσα

Η γλώσσα OVAL μπορεί να χαρακτηριστεί ως το πιο σημαντικό στοιχείο του OVAL προτύπου. Η γλώσσα OVAL ορίζει τρία κύρια βήματα για την δημιουργία μιας διαδικασίας αξιολόγησης. Τα βήματα είναι τα εξής:

- Συλλογή πληροφοριών σχετικά με το σύστημα που τίθεται προς δοκιμή.
- Ανάλυση του συστήματος και ο εντοπισμός της κατάστασης του συστήματος.
- Η σύνθεση τελικής αναφοράς με τα αποτελέσματα της ανάλυσης.

Το κάθε ένα από τα παραπάνω τρία βήματα για να υλοποιηθεί χρειάζεται την βοήθεια από τρία τυποποιημένα σχήματα (schemas). Για το κάθε ένα σχήμα παράγεται και το αντίστοιχο XML αρχείο στο οποίο περιγράφονται οι ενέργειες που πρέπει να πραγματοποιηθούν για την συλλογή των κατάλληλων δεδομένων. Τα τρία σχήματα που χρησιμοποιούνται είναι τα εξής:

1. Σχήμα Χαρακτηριστικών Συστήματος (Για συλλογή πληροφοριών σχετικά με το σύστημα)
2. Σχήμα Εξέτασης (Για ορισμό των δοκιμών(tests) που θα σκανάρουν στο σύστημα)
3. Σχήμα Αποτελεσμάτων (Για την σύνθεση της τελικής αναφοράς)

Το **Σχήμα Χαρακτηριστικών Συστήματος** χρησιμοποιεί την γλώσσα σήμανσης XML (eXtensible Markup Language)[70] για να περιγράψει και να κωδικοποιήσει τα δεδομένα που σχετίζονται με τις ρυθμίσεις του συστήματος, όπως ρυθμίσεις για τις εγκατεστημένες εφαρμογές στο σύστημα, τις παραμέτρους του λειτουργικού συστήματος και άλλων μεταβλητών που σχετίζονται με την ασφάλεια του συστήματος. Έτσι, δημιουργείτε ένα αρχείο XML με τα χαρακτηριστικά του συστήματος το οποίο μπορεί να αναφερθεί και ως μια βάση δεδομένων με τα χαρακτηριστικά του συστήματος. Επιπλέον, το συγκεκριμένο αρχείο XML μπορεί να συγκριθεί με "OVAL τεστ" που θα δούμε παρακάτω στο

Σχήμα Εξέτασης. Η σύγκριση αυτή γίνεται με σκοπό την ανάλυση του συστήματος για θέματα ευπαθειών, θέματα ρυθμίσεων (δηλαδή εαν υπάρχουν misconfigurations) και θέματα επιδιορθώσεων. Κατά βάση, αυτό που ορίζετε από το σχήμα είναι μια τυποποιημένη μορφή για την ανταλλαγή των χαρακτηριστικών των υπολογιστικών συστημάτων, η οποία μπορεί να συμβάλει στην εύκολη και γρήγορη ανταλλαγή δεδομένων μεταξύ των επαγγελματιών στον χώρο της κυβερνοασφάλειας και της ασφάλειας συστημάτων.

Το **Σχήμα Εξέτασης** με την σειρά του καθορίζει το παρακάτω σετ από τεστ:

- OVAL τεστ ευπαθειών: Με αυτό τον τρόπο καθορίζει ποιες θα πρέπει να είναι οι συνθήκες σε ένα υπολογιστικό σύστημα έτσι ώστε αυτό να χαρακτηριστεί ως ευπαθή σύστημα σε μια συγκεκριμένη ευπάθεια.
- OVAL τεστ επιδιόρθωσης: Με αυτόν τον τρόπο καθορίζει τις συνθήκες που πρέπει να υπάρχουν έτσι ώστε μια επιδιόρθωση να είναι κατάλληλη για το υπάρχον υπολογιστικό σύστημα.
- OVAL τεστ απογραφής: Με αυτόν τον τρόπο καθορίζει τις συνθήκες που πρέπει να υπάρχουν έτσι ώστε ένα λογισμικό να θεωρείτε εγκατεστημένο στο υπολογιστικό σύστημα.
- Oval τεστ συμμόρφωσης: Με αυτόν τον τρόπο καθορίζει τις συνθήκες που πρέπει να υπάρχουν έτσι ώστε ένα υπολογιστικό σύστημα να θεωρείτε ότι είναι συμμορφωμένο βάση μιας συγκεκριμένης πολιτικής που έχει οριστεί έναντι σε ευπάθειες.

Το Σχήμα Εξέτασης χρησιμοποιεί την XML για να κωδικοποιήσει τις πληροφορίες που σχετίζονται με την κατάσταση του συστήματος (για παράδειγμα αν το σύστημα είναι ευάλωτο σε μια επίθεση) επιτρέποντας την αυτοματοποίηση των δοκιμών (tests) σε ένα σύστημα. Τα τυποποιημένα σχήματα της γλώσσας OVAL επιτρέπουν επίσης τους επαγγελματίες της κυβερνοασφάλειας να συζητούν τις τεχνικές λεπτομέρειες για το κατά πόσον ένα σύστημα έχει ευπάθειες, με έναν πιο συνεκτικό και ακριβή τρόπο, αφήνοντας πολύ μικρό περιθώριο για παρερμηνείες. Τέλος, το σχήμα για τη συγγραφή OVAL Τεστ χωρίζεται σε δύο διακριτά τμήματα. Το "θεμελιώδες" σχήμα που καλύπτει τα βασικότερα στοιχεία της μορφής που θα έχουν οι δοκιμές (tests) και τα "ειδικά" σχήματα που προορίζονται για δοκιμές προσαρμοσμένες σε συγκεκριμένες εφαρμογές/λογισμικά ή λειτουργικά συστήματα. Για παράδειγμα, υπάρχουν διαφορετικά τεστ για πλατφόρμες που τρέχουν Unix και άλλα τεστ για πλατφόρμες που τρέχουν Windows.

Το **Σχήμα Αποτελεσμάτων** χρησιμοποιεί την XML για να κωδικοποιήσει τις πληροφορίες που σχετίζονται με τα αποτελέσματα της αξιολόγησης ενός υπολογιστικού συστήματος. Το δεδομένα που εμπεριέχονται στο XML αρχείο αποτελεσμάτων, δίνουν μια εικόνα για την τρέχουσα κατάσταση ενός συστήματος που συγκρίθηκε με ένα σύνολο από OVAL δοκιμές (τεστ). Το Σχήμα Αποτελεσμάτων μπορεί να εισαχθεί σε διάφορα λογισμικά και αυτά με την σειρά τους να ερμηνεύσουν τα δεδομένα και εν τέλει να κάνουν τις κατάλληλες ενέργειες για την άμβλυνση και τον μετριασμό των τρωτών σημείων ενός συστήματος. Για παράδειγμα, στην αναφορά που δημιουργήθηκε από το Σχήμα Αποτελεσμάτων αναφέρετε ο εντοπισμός μιας ευπάθειας σε έναν Apache Web Server. Στην ίδια αναφορά υπάρχει η δυνατότητα για αναφορά επιλύσεων της ευπάθειας. Η επίλυση για το συγκεκριμένο παράδειγμα μπορεί να είναι η λήψη "ενημέρωσης επιδιόρθωσης¨(security update/patch) εάν και εφόσον υπάρχει. Να αναφερθεί ότι και το Σχήμα Αποτελεσμάτων χωρίζεται σε δύο τμήματα, στο "θεμελιώδες" σχήμα και στα "ειδικά" σχήματα όπως είδαμε και παραπάνω στο Σχήμα Εξέτασης.

4.2.2 OVAL αποθετήριο

Το OVAL αποθετήριο είναι ένα κεντρικό σημείο στο οποίο συγκεντρώνονται όλες οι "OVAL εξετάσεις" και οι δοκιμές (tests). Τα τεστ/δοκιμές βρίσκονται στο αποθετήριο και είναι δωρεάν προς όλους. Επίσης για όσους ενδιαφέρονται να αναπτύξουν, να συντηρήσουν, να υποβάλουν και να συζητήσουν τεστ, υπάρχει το φόρουμ του αποθετηρίου το οποίο είναι ένας δημόσια προσβάσιμος χώρος συζητήσεων γύρω από τα OVAL τεστ. Τα μέλη της κοινότητας με την σειρά τους μπορούν να προτείνουν νέου τύπου "OVAL εξετάσεις" και τεστς υποβάλλοντάς τα στο φόρουμ για δημόσια διαβούλευση μεταξύ των μελών της κοινότητας. Μετά από ενδελεχή έλεγχο από συγκεκριμένη ομάδα που χειρίζεται την έγκριση των τεστ αλλά και από τα μέλη της κοινότητας, ένα υποβληθέν τεστ/ορισμός γίνεται δεκτό και προστίθεται στο αποθετήριο μαζί με όλους τους υπόλοιπα τεστ και είναι διαθέσιμο δημόσια για τον οποιοδήποτε θέλει να το χρησιμοποιήσει.

4.2.3 OVAL διερμηνέας

Ο OVAL διερμηνέας είναι ένα λογισμικό το οποίο έχει ως κύριο σκοπό, την εκτέλεση OVAL ορισμών στα εκάστοτε υπολογιστικά συστήματα. Τα σχήματα που είδαμε παραπάνω (Ορισμών, Αποτελεσμάτων, Χαρακτηριστικών Συστήματος) εφαρμόζονται και γίνονται λειτουργικά μέσω του διερμηνέα. Για παράδειγμα, ο διερμηνέας εκτελεί το Σχήμα Χαρακτηριστικών Συστήματος. Εφόσον έχει μαζέψει τις πληροφορίες για το υπολογιστικό σύστημα, περνάει στην φάση της αξιολόγησης τους συστήματος εκτελώντας το Σχήμα Ορισμών το οποίο αποφασίζει ποιες δοκιμές/τεστς είναι κατάλληλα να τρέξουν για την αξιολόγηση του συστήματος. Το αποτέλεσμα της αξιολόγησης τροφοδοτείτε στο Σχήμα Αποτελεσμάτων το οποίο παράγει μια αναφορά, η οποία θα αναφέρει λεπτομερώς την κατάσταση του συστήματος, για παράδειγμα αν το σύστημα πληροί τις καθορισμένες απαιτήσεις ασφαλείας, αν έχει ευπάθειες, ποιες είναι αυτές, τον βαθμό κρισιμότητας των ευπαθειών και αν υπάρχουν λανθασμένες ρυθμίσεις (misconfigurations).

Εν κατακλείδι, το OVAL αποτελεί ένα βασικό και κομβικό πρότυπο στον τομέας της ασφάλειας των υπολογιστικών συστημάτων. Με την χρήση μιας δομημένης γλώσσας βασισμένη στην XML, το OVAL προσφέρει ένα συμπαγές πλαίσιο για τον ορισμό και την αξιολόγηση υπολογιστικών συστημάτων έναντι ευπαθειών. Επίσης, πέρα από την πολλή καλή δόμηση του προτύπου στον τεχνικό τομέα, το OVAL ακμάζει και στηρίζεται χάρη στις προσπάθειες της κοινότητας της κυβερνοασφάλειας. Η τεχνογνωσία και το έργο που παρέχει η κοινότητα στο πρότυπο, εξασφαλίζει τη συνεχή ανάπτυξη του περιεχομένου αλλά και του προτύπου εν γένη. Στην ουσία, το OVAL μπορεί να χαρακτηριστεί ως ο ακρογωνιαίος λίθος για τυποποιημένες και αυτοματοποιημένες αξιολογήσεις ασφαλείας, προωθώντας την διαλειτουργικότητα, την αποτελεσματικότητα και την συλλογική προσπάθεια και προσέγγιση για την ενίσχυση της ανθεκτικότητας των υπολογιστικών συστημάτων έναντι σε ευπάθειες και απειλές.

4.3 Η χρησιμότητα τους στην XDR αρχιτεκτονική

Στον χώρο της κυβερνοασφάλειας η σύμπλευση του OpenC2 και του OVAL ξεχωρίζουν ως βασικοί πυλώνες για την ενίσχυση των συστημάτων XDR αλλά και της αρχιτεκτονικής βάσει την οποία συνθέτεται ένα XDR σύστημα. Το OpenC2 διαδραματίζει κρίσιμο ρόλο στην τυποποίηση της επικοινωνίας μεταξύ διαφορετικών εργαλείων ασφαλείας, στην προώθηση της διαλειτουργικότητας και στη δυνατότητα ενορχηστρωμένων αντιδράσεων έναντι απειλών. Η ευελιξία του, δίνει τη δυνατότητα στους ειδικούς στον τομέα της κυβερνοασφάλειας να δημιουργούν προσαρμοσμένες λύσεις ανάλογα του τοπίου των απειλών που έχουν να αντιμετωπίσουν, προωθώντας την

προσαρμοστικότητα απέναντι στις ολοένα εξελισσόμενες προκλήσεις και απειλές. Παράλληλα, το OVAL αντιμετωπίζει την κρίσιμη πτυχή της διαχείρισης των ευπαθειών στο πλαίσιο του XDR, παρέχοντας μια τυποποιημένη γλώσσα για την έκφραση και την αξιολόγηση των ευπαθειών. Επίσης, η OVAL υποστηρίζει αυτοματοποιημένες αξιολογήσεις ευπαθειών. Αυτό ευθυγραμμίζεται άψογα με τη γενική έμφαση στην αυτοματοποίηση σε περιβάλλοντα XDR, εξασφαλίζοντας μια συνεπή και αποτελεσματική προσέγγιση για τον εντοπισμό και την ιεράρχηση των ευπαθειών σε διαφορετικά συστήματα. Επιπλέον, η ενσωμάτωση του OVAL με εργαλεία σάρωσης ενισχύει τη συνολική αποτελεσματικότητα των πρακτικών διαχείρισης ευπαθειών. Η αυτοματοποιημένη αξιολόγηση των ευπαθειών, που υποστηρίζεται από το OVAL, επιτρέπει στους υπεύθυνους για την ανίχνευση ευπαθειών να εντοπίζουν άμεσα και να ιεραρχούν τις προσπάθειες αποκατάστασης, κάτι που είναι ζωτικής σημασίας για τη διατήρηση μιας ισχυρής δομής ασφαλείας. Συνοψίζοντας, η ενσωμάτωση του OpenC2 και του OVAL στις αρχιτεκτονικές XDR ενισχύει την τυποποιημένη επικοινωνία, προωθεί την προσαρμοστικότητα στην αντιμετώπιση απειλών και υποστηρίζει αυτοματοποιημένες αξιολογήσεις ευπάθειας. Αυτή η σύνθεση συμβάλλει σε ένα πιο ανθεκτικό, οχυρωμένο και αυτοματοποιημένο πλαίσιο άμυνας, κάτι που είναι ζωτικής σημασίας στο δυναμικά αναπτυσσόμενο τοπίο απειλών στον κυβερνοχώρο.

Κεφάλαιο 5ο: Μελέτη περίπτωσης

Σε αυτό το κεφάλαιο θα μελετήσουμε την εφαρμοσιμότητα του OpenC2 πρωτοκόλλου σε ένα XDR προϊόν και θα γίνει ένα παράδειγμα λειτουργίας του σε ένα σενάριο επίθεσης ενάντια στην υποδομή μιας έξυπνης πόλης. Αρχικά θα ορίσουμε το περιβάλλον και το πλαίσιο στο οποίο θα εφαρμοστεί το OpenC2, δηλαδή την πόλη μας και την υποδομή της έξυπνης πόλης.

5.1 Ορισμός περιβάλλοντος και σεναρίου

Το περιβάλλον που ορίζετε, είναι ο μητροπολιτική ενότητα της Θεσσαλονίκης. Στην μητροπολιτική Θεσσαλονίκη ανήκουν οκτώ (8) δήμοι[51].

ΣΗΜΕΙΩΣΗ: Παρακαλώ να έχετε υπόψιν σας πως τα παραδείγματα από εδώ και κάτω είναι φανταστικά και μέρος ενός σεναρίου.

Ως προς την υποδομή της πόλης αρχικά αναφέρετε ότι ο κάθε δήμος έχει τα δικά του συστήματα, υποδομή και πληροφοριακά συστήματα για να αναπτύσσει και να διαχειρίζεται τα στοιχεία που απαρτίζουν την έξυπνη πόλη. Τα στοιχεία και συστήματα του κάθε έξυπνου δήμου επικοινωνούν μερικός και έτσι η διαλειτουργικότητα υπάρχει για κάποια τμήματα, για παράδειγμα υπάρχει διαμοιρασμός πληροφοριών για την κατάσταση στους οδικούς άξονες. Ως προς την ασφάλεια των συστημάτων, των στοιχείων αλλά και εν γένη της έξυπνης πόλης που συνεπάγεται και στην ασφάλεια των πολιτών βρέθηκαν πολλά προβλήματα και προκλήσεις. Οι προκλήσεις για την ασφάλεια και την απόκριση σε περιστατικά ασφαλείας που προκύπτουν από αυτή την ασύνδετη αρχιτεκτονική είναι οι εξής:

1. Απουσία ενοποιημένων πολιτικών ασφαλείας: Η απουσία ενοποιημένων πολιτικών ασφαλείας μπορεί να οδηγήσει σε ασυνεπή εφαρμογή των μέτρων ασφαλείας. Η καθιέρωση και η επιβολή πολιτικών ασφαλείας σε ολόκληρη την πόλη γίνεται ακόμη πιο δύσκολη όταν κάθε δήμος έχει τους δικούς του κανόνες και πολιτικές ασφαλείας.
2. Κίνδυνοι ασφάλειας διαλειτουργικότητας: Τα προβλήματα διαλειτουργικότητας μεταξύ διαφορετικών συστημάτων μπορούν να δημιουργήσουν τρωτά σημεία ασφαλείας. Η ενσωμάτωση διαφορετικών τεχνολογιών χωρίς τυποποιημένη προσέγγιση ασφάλειας μπορεί να οδηγήσει σε μια ασθενή συνολική αρχιτεκτονική ασφάλειας. Επίσης, διαφορετικοί κατασκευαστές (vendors) ενδέχεται να χρησιμοποιούν ιδιόκτητα πρωτόκολλα και τεχνολογίες, γεγονός που οδηγεί σε προκλήσεις και κινδύνους διαλειτουργικότητας. Η εξασφάλιση απρόσκοπτης επικοινωνίας και ενσωμάτωσης μεταξύ συστημάτων από διαφορετικούς κατασκευαστές είναι πολύπλοκη και φέρει κινδύνους ασυμβατότητας.
3. Ασυμβατότητες και ασυνέπειες στις ενημερώσεις ασφαλείας: Η έγκυρες ενημερώσεις ασφαλείας σε όλα αυτά τα διαφορετικά συστήματα είναι δύσκολη και περίπλοκη. Τα διαφορετικά χρονοδιαγράμματα και πρακτικές για την εφαρμογή επιδιορθώσεων και ενημερώσεων μπορεί να έχουν ως αποτέλεσμα ορισμένα συστήματα να είναι πιο ευάλωτα σε γνωστές ευπάθειες ή ακόμα κάποια συστήματα να τεθούν εκτός λειτουργίας λόγω του μη ανεκτού ρίσκου.
4. Κατανομή πόρων για την κυβερνοασφάλεια: Η διάθεση πόρων για δράσεις κυβερνοασφάλειας μπορεί να διαφέρει μεταξύ των δήμων ανάλογα με το επίπεδο πληροφόρησης σχετικά με τις

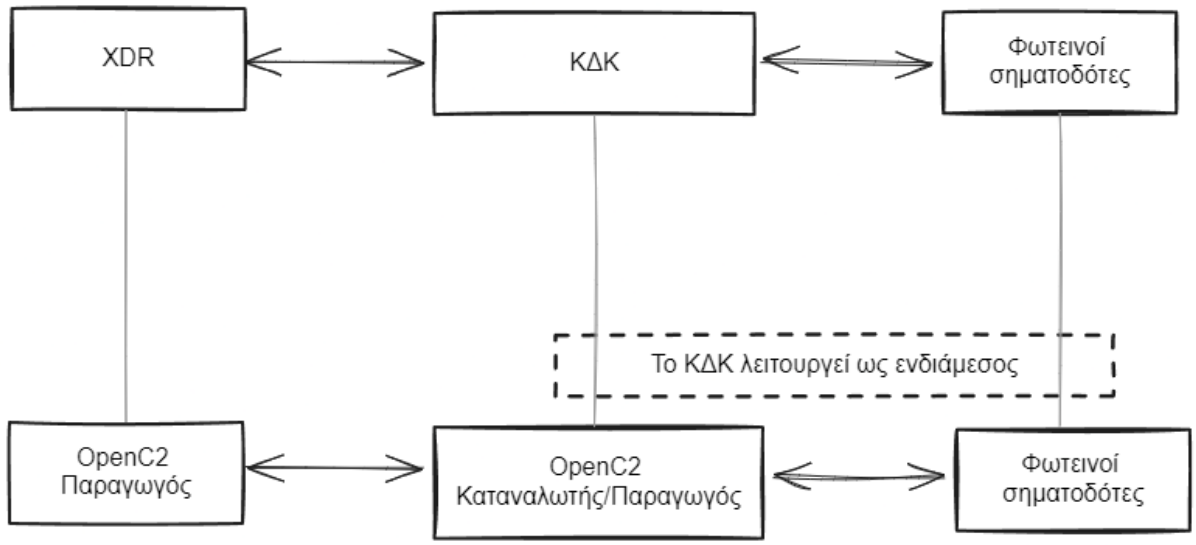
απειλές στον κυβερνοχώρο ή τους περιορισμούς του προϋπολογισμού. Η επίτευξη μιας ισορροπημένης και ολοκληρωμένης στρατηγικής κυβερνοασφάλειας σε ολόκληρη την πόλη είναι ζωτικής σημασίας.

5. Ανισότητες δεξιοτήτων στην κυβερνοασφάλεια του εκάστοτε δήμου: Επίσης υπάρχει μεγάλη πιθανότητα να υπάρχουν διαφορές στις δεξιότητες και την εμπειρία στον τομέα της ασφάλειας στον κυβερνοχώρο μεταξύ του προσωπικού που είναι υπεύθυνο για τη διαχείριση της ασφάλειας σε κάθε δήμο. Η αντιμετώπιση των διαφορετικών δεξιοτήτων και η εξασφάλιση ενός ομοιόμορφου επιπέδου εμπειρίας και εξειδίκευσης αποτελεί μια μεγάλη πρόκληση.
6. Δυσκολία συντονισμού στην ανταπόκριση σε περιστατικά ασφαλείας: Σε περίπτωση περιστατικού ασφαλείας, ο συντονισμός μιας αποτελεσματικής αντίδρασης σε πολλούς δήμους με διαφορετικά συστήματα και υποδομές είναι πολύπλοκο και χρονοβόρο. Η έλλειψη τυποποιημένων διαδικασιών αντιμετώπισης περιστατικών μπορεί να εμποδίσει τη γρήγορη επίλυση του περιστατικού ασφαλείας.
7. Έλλειψη κεντρικής εποπτείας: Η απουσία κεντρικής εποπτείας μπορεί να εμποδίσει την ικανότητα της πόλης, δηλαδή την Μητροπολιτική Ενότητα Θεσσαλονίκης, να έχει μια ολιστική εικόνα του τοπίου των απειλών και να αντιδράσει συντεταγμένα σε περίπτωση ευρείας επίθεσης.

Μετά από τους παραπάνω προβληματισμούς, όλοι οι δήμοι συμφωνούν να υλοποιήσουν μια λύση η οποία θα παρέχει κεντρική εποπτεία για όλα τα συστήματα της έξυπνης πόλης όλων των δήμων.

Σε αυτό το σενάριο, η Μητροπολιτική Ενότητα έχει κάνει ένα σημαντικό βήμα προς την ενίσχυση της ασφάλειας και της αποτελεσματικότητας της Μητροπολιτικής Ενότητας έναντι σε κυβερνοεπιθέσεις αναπτύσσοντας ένα ολοκληρωμένο σύστημα XDR. Το σύστημα αυτό δεν είναι μόνο υπεύθυνο για τη λειτουργία των έξυπνων φαναριών, αλλά ενσωματώνει επίσης προηγμένες τεχνολογίες ασφαλείας για όλη την υποδομή της έξυπνης πόλης με βάση την αρχιτεκτονική που περιγράφεται στο κεφάλαιο 2. Επιπλέον, πηγαίνει ένα βήμα παραπέρα ενσωματώνοντας το πρωτόκολλο OpenC2, προσθέτοντας ένα επίπεδο διαλειτουργικότητας στον τρόπο με τον οποίο γίνεται η απόκριση σε πιθανές επιθέσεις στην υποδομή. Η ενσωμάτωση του πρωτοκόλλου OpenC2 αποτελεί στρατηγική κίνηση, επιτρέποντας στο σύστημα XDR να ανταποκρίνεται στις επιθέσεις γρήγορα και αποτελεσματικά, εφόσον έχει ανιχνεύσει κάποιου είδους επίθεση στην υποδομή. Η διαλειτουργικότητα που προσφέρει το OpenC2 διασφαλίζει ότι τα διάφορα συστήματα ασφαλείας μπορούν να λειτουργούν παράλληλα, ενισχύοντας τη συνολική ανθεκτικότητα της υποδομής έναντι σε κυβερνοεπιθέσεις και δημιουργώντας έναν συμπαγή μηχανισμό άμυνας για την Μητροπολιτική Ενότητα.

Οι έξυπνοι φωτεινοί σηματοδότες (ΕΦΣ) από την μεριά τους δεν ενσωματώνουν το OpenC2 και δεν κατανοούν OpenC2 εντολές. Για αυτόν τον λόγω δημιουργήθηκε ένα ειδικό σύστημα το Κέντρο Διαχείρισης Κυκλοφορίας (ΚΔΚ). Το ΚΔΚ ενσωματώνει το πρωτόκολλο OpenC2 και έτσι στην προκειμένη περίπτωση, λειτουργεί ως ενδιάμεσος γεφυρώνοντας το χάσμα μεταξύ XDR και ΕΦΣ. Το ΚΔΚ διαχειρίζεται τους έξυπνους φωτεινούς σηματοδότες εντός της Μητροπολιτικής Ενότητας, λειτουργώντας ως ειδικό σύστημα για σκοπούς που σχετίζονται με την κυκλοφορία. Η ενσωμάτωση του πρωτοκόλλου OpenC2 στο ΚΔΚ του επιτρέπει να επικοινωνεί με την ευρύτερη



Σχήμα 5.1.1: Σχήμα προτεινόμενης αρχιτεκτονικής

Κατά τη διαδικασία ανάλυσης δεδομένων στο πλαίσιο του συστήματος XDR, οι φωτεινοί σηματοδότες διαδραματίζουν καθοριστικό ρόλο στη συλλογή και τη μετάδοση των σχετικών πληροφοριών. Η ροή δεδομένων είναι επιμελώς σχεδιασμένη ώστε να διασφαλίζεται η απρόσκοπτη ροή δεδομένων από το επιχειρησιακό επίπεδο στο σύστημα XDR για ολοκληρωμένη ανάλυση και ανίχνευση απειλών. Αρχικά να αναφέρουμε ότι οι έξυπνοι φωτεινοί σηματοδότες στη μητροπολιτική ενότητα συγκεντρώνουν σχετικά δεδομένα που σχετίζονται με τις συνθήκες κυκλοφορίας, την κατάσταση των σηματοδοτών, τις συνολικές συνθήκες λειτουργίας αλλά και την κατάσταση των φωτεινών σηματοδοτών σε επίπεδο ασφαλείας . Τα δεδομένα αυτά διαβιβάζονται στη συνέχεια στο Κέντρο Διαχείρισης Κυκλοφορίας , το οποίο χρησιμεύει ως κεντρικός κόμβος για τη διαχείριση και το συντονισμό της κυκλοφορίας εντός της πόλης. Το ΚΔΚ ενεργεί ως συγκεντρωτής πληροφοριών σε πραγματικό χρόνο από διάφορους φωτεινούς σηματοδότες που είναι διασκορπισμένοι σε όλη τη μητροπολιτική ενότητα.

Για την αποτελεσματική επικοινωνία και μεταφορά δεδομένων, το ΚΔΚ χρησιμοποιεί το πρωτόκολλο syslog για τη διαβίβαση των συλλεχθέντων δεδομένων στο σύστημα XDR. Το Syslog, ένα πρωτόκολλο για την αποστολή αρχείων καταγραφής (logs) και εξασφαλίζει μια αξιόπιστη και τυποποιημένη μέθοδο μετάδοσης πληροφοριών. Αυτή η επιλογή του πρωτοκόλλου ευθυγραμμίζεται με τους στόχους διαλειτουργικότητας της συνολικής αρχιτεκτονικής του συστήματος, επιτρέποντας την ομαλή επικοινωνία των διαφόρων στοιχείων.

Σχήμα 5.1.2: Διαδικασία μεταφοράς δεδομένων από τους έξυπνους κόμβους προς το XDR

Από εκεί και πέρα το XDR έχει τον ρόλο της ανάλυσης των δεδομένων που του έχουν παρασχεθεί. Στην περίπτωση που εντοπίσει κάποιου είδους επίθεση ή απειλή προς το σύστημα των έξυπνων φαναριών μπορεί να επέμβει με διάφορες τρόπους για να αποκατασταθεί η κανονική λειτουργία των συστημάτων ή να μειωθεί η πιθανότητα εξάπλωσης της επίθεσης και σε άλλα συστήματα. Για παράδειγμα το XDR (που στην περίπτωσή μας είναι ο OpenC2 παραγωγός) θα μπορούσε να εκδώσει κάποιες εντολές από τις παρακάτω εντολές:

- Πλήρης απομόνωση: Αποσύνδεση από το δίκτυο όλων των έξυπνων φωτεινών σηματοδοτών. Με αυτόν τον τρόπο περιορίζετε ο αντίκτυπος της κυβερνοεπίθεσης και εμποδίζει τον εισβολέα να συνεχίσει να χειρίζεται τους σηματοδότες κυκλοφορίας ή να συλλέγει δεδομένα από τις προσβεβλημένες συσκευές.
- Μερική απομόνωση: Τμηματοποίηση των επηρεαζόμενων από την επίθεση έξυπνων φωτεινών σηματοδοτών. Με αυτό τον τρόπο όποιοι φωτεινοί σηματοδότες δεν έχουν επηρεαστεί από την επίθεση μένουν κανονικά με την έξυπνη λειτουργία τους.
- Επαναφορά σε κατάσταση ασφαλής λειτουργίας: Η επαναφορά σε ασφαλή λειτουργία διασφαλίζει ότι το σύστημα φωτεινών σηματοδοτών λειτουργεί με βάση αξιόπιστες και επαληθευμένες ρυθμίσεις, ελαχιστοποιώντας τον κίνδυνο ανεπιθύμητων συνεπειών που μπορεί να προκλήθηκαν από την επίθεση.

Σχήμα 5.1.3: Διαδικασία μεταφοράς OpenC2 εντολών

5.2 Σημασιολογική περιγραφή έξυπνων φωτεινών σηματοδοτών

Σε αυτό το υποκεφάλαιο θα αναλυθεί πως μπορεί να γίνει η σημασιολογική περιγραφή έξυπνων σηματοδοτών. Η έξυπνη πόλη μας έχει πολλούς έξυπνους σηματοδότες οι οποίοι δεν είναι από τον ίδιο κατασκευαστή. Η κατασκευαστές των έξυπνων σηματοδοτών οφείλουν να παραδώσουν ένα αρχείο με πληροφορίες σχετικά με την καλή λειτουργία ή την ορθή λειτουργία των συστημάτων που έχουν αναπτύξει, στην προκειμένη περίπτωση αυτά τα συστήματα είναι οι έξυπνοι σηματοδότες. Αυτό το αρχείο θα περιγράφει σημασιολογικά τα χαρακτηριστικά που πρέπει να ελέγχονται και τις τιμές που πρέπει να έχουν αυτά τα χαρακτηριστικά. Αυτού του είδους η περιγραφή πρέπει να υπάρχει διότι η ορθή λειτουργία ενός συστήματος από έναν συγκεκριμένο κατασκευαστή μπορεί να διαφέρει από την ορθή λειτουργία ενός συστήματος από έναν διαφορετικό κατασκευαστή. Μερικά από τα χαρακτηριστικά που μπορεί να περιλαμβάνονται στο αρχείο ορθής λειτουργίας των έξυπνων φωτεινών σηματοδοτών είναι τα εξής:

- Οι χρόνοι των σημάτων: Σε αυτό το πεδίο θα περιγράφονται οι ορθοί χρόνοι των σημάτων (κόκκινο, πορτοκαλί, πράσινο). Για παράδειγμα, ο χρόνος του κόκκινου χρώματος στον σηματοδότη θα να είναι 30 δευτερόλεπτα, ο χρόνος του πορτοκαλί χρώματος στον σηματοδότη θα είναι 4 δευτερόλεπτα και ο χρόνος του πράσινου χρώματος στον σηματοδότη θα είναι 10 δευτερόλεπτα
- Οι φάσεις των σημάτων: Σε αυτό το πεδίο θα περιγράφεται η ορθή σειρά των φάσεων των σημάτων. Για παράδειγμα η ορθή σειρά των φάσεων θα πρέπει να είναι το μοτίβο Κόκκινο-Πράσινο-Πορτοκαλί-Κόκκινο και πάντα με τους κατάλληλους χρόνους

- Πιστοποιημένοι χρήστες: Σε αυτό το πεδίο θα περιγράφονται οι χρήστες και ίσως και συγκεκριμένες διευθύνσεις διαδικτύου (IP) που έχουν την δικαιοδοσία για απομακρυσμένη σύνδεση και επεξεργασία στις ρυθμίσεις στον εκάστοτε έξυπνο φωτεινό σηματοδότη
- Σφάλματα: Σε αυτό το πεδίο θα περιγράφονται τα όποια σφάλματα μπορεί να προκύψουν αλλά δεν επηρεάζουν άμεσα την λειτουργία και την ασφάλεια των σηματοδοτών
- Κατανάλωση ενέργειας: Σε αυτό το πεδίο θα περιγράφονται τα ανεκτά όρια στην κατανάλωση ενέργειας από τον εκάστοτε σηματοδότη
- Πρωτόκολλα επικοινωνίας: Σε αυτό το πεδίο θα περιγράφονται τα πρωτόκολλα επικοινωνίας που πρέπει να χρησιμοποιεί ο σηματοδότης. Για παράδειγμα αυτά τα πρωτόκολλα πρέπει να είναι HTTPS, OpenC2 και MTTQ[71]
- Χρονικό διάστημα αποστολής δεδομένων: Σε αυτό το πεδίο ορίζετε κάθε πότε θα πρέπει να στέλνει δεδομένα ο σηματοδότης στα συστήματα επίβλεψής του. Για παράδειγμα θα πρέπει να στέλνει δεδομένα για την κατάστασή του κάθε δέκα (10) δευτερόλεπτα
- Ανεκτός χρόνος μη παραλαβής δεδομένων: Σε αυτό το πεδίο ο κατασκευαστής ορίζει το ανεκτό χρονικό διάστημα μη παραλαβής δεδομένων από τον έξυπνο σηματοδότη. Για παράδειγμα αν ο σηματοδότης στέλνει δεδομένα κάθε δέκα (10) δευτερόλεπτα, ο ανεκτός χρόνος μη παραλαβής δεδομένων μπορεί να οριστεί στα εκατό (100) δευτερόλεπτα

Έτσι, με την ύπαρξη μιας βάσης που μπορεί να χαρακτηριστεί ως σωστής ή ορθής λειτουργίας του σηματοδότη, υπάρχει η δυνατότητα να δημιουργηθούν οι κατάλληλοι κανόνες εντοπισμού μεταβολών αυτών των χαρακτηριστικών με σκοπό τον έγκυρο εντοπισμό κάποιας δυσλειτουργίας ή κάποιας επίθεσης στον εκάστοτε σηματοδότη. Γι' αυτόν τον λόγο είναι σημαντικό ο κάθε κατασκευαστής να δημιουργεί ένα τέτοιου είδους έγγραφο.

Παρακάτω παρατίθενται παραδείγματα για το πως θα μπορούσαν να παρθούν τα παραπάνω χαρακτηριστικά με την χρήση OpenC2 commands και OVAL Definitions.

OpenC2 Command:

```
{
  "action": "query",
  "target": {
    "features": ["signal_times", "signal_phases", "errors", "energy_consumption", "communication_protocols", "data_transmission_interval", "tolerable_non_receipt_time"]
  },
  "actuator": {
    "endpoint": {
      "asset_id": "smart_traffic_light_E38"
    }
  }
}
```

OpenC2 Response:

```
{
 "status": "200",
 "results": {
  "signal_times": "30-15-4-30",
  "signal_phases": "Red-Green-Orange-Red",
  "errors": "Minor",
  "energy_consumption": "150W",
  "communication_protocols": ["HTTP", "MQTT", "OpenC2"],
  "data_transmission_interval": 60,
   "tolerable_non_receipt_time": 180
  }
}
```

Το παραπάνω OpenC2 command ζητάει από τον σηματοδότη με όνομα “smart_traffic_light_E38” όλα τα χαρακτηριστικά που έχει ορίσει ο κατασκευαστής και λαμβάνει μια απάντηση με τα χαρακτηριστικά που ζήτησε και τις τιμές τους. Συνεχίζοντας υπάρχει το παράδειγμα με την υλοποίηση ενός OVAL Definition.

OVAL Definition:

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-definitions-5 http://oval.mitre.org/language/version5.10/oval-definitions-schema.xsd"
  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
  xmlns:independent="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent">
  <!-- Στο "generator" γίνεται η περιγραφή του συστήματος που δημιουργεί το OVAl Definition-->
  <generator>
    <oval:product_name>Status Checker</oval:product_name>
    <oval:product_version>1.0</oval:product_version>
    <oval:schema_version>1.1.1</oval:schema_version>
    <oval:timestamp>2024-01-22T00:00:00</oval:timestamp>
  </generator>
  <!-- Στο "definiton γίνεται ο ορισμός της εξέτασης για την αξιολόγηση των φωτεινών σηματοδοτών"-->
  <definition id="oval:org.example:def:1" version="1" class="compliance">
    <metadata>
      <title>Check Smart Traffic Light Functionality</title>
      <description>This OVAL definition checks whether a specific smart traffic light is functioning
        correctly based on the vendor's specifications.</description>
    </metadata>
    <criteria>
      <criterion comment="Check traffic light functionality">
        <test check="all" check_existence="at_least_one_exists" version="1">
          <object object_ref="oval:org.example:obj:1" />
          <state state_ref="oval:org.example:ste:1" />
        </test>
      </criterion>
    </criteria>
  </definition>
  <!-- Στο "objects" περιγράφονται ποια συστήματα τίθενται προς αξιολόγηση-->
  <objects>
    <independent:entity_object id="oval:org.example:obj:1" version="1">
      <independent:object reference="smart_traffic_light_from_vendor_X" />
    </independent:entity_object>
  </objects>
```

Σχήμα 5.1.4: Πρώτο μέρος του OVAL Definition

```
<!-- Στο "states" περιγράφονται ποια χαρακτηριστικά του συστήματος πρέπει να ελεγχθούν -->
<states>
  <independent:component_state id="oval:org.example:ste:1" version="1">
    <independent:attribute attribute_name="signal_times">30-15-4-30</independent:attribute>
    <independent:attribute attribute_name="signal_phases">Red-Green-Orange-Red</independent:attribute>
    <independent:attribute attribute_name="errors">Minor</independent:attribute>
    <independent:attribute attribute_name="energy_consumption">100 W</independent:attribute>
    <independent:attribute attribute_name="communication_protocols">HTTP, MTTQ, OpenC2</independent:attribute>
    <independent:attribute attribute_name="data_transmission_interval">60</independent:attribute>
    <independent:attribute attribute_name="tolerable_non_receipt_time">180</independent:attribute>
  </independent:component_state>
</states>
</oval_definitions>
```

Σχήμα 5.1.5: Δεύτερο μέρος του OVAL Definition

Τέλος, για κάθε διαφορετικό κατασκευαστή φαναριού θα υπάρχει και το ανάλογο OVAL Definition και OpenC2 command.

5.3 Υποθετικό σενάριο επίθεσης

Σε ένα υποθετικό σενάριο, φανταστείτε μια περίπλοκη κυβερνοεπίθεση με στόχο την έξυπνη υποδομή της πόλης, η οποία επιχειρεί να θέσει σε κίνδυνο τη λειτουργία των έξυπνων φαναριών ή ακόμα και να τα θέσει εκτός λειτουργίας και να διαταράξει το σύστημα διαχείρισης της κυκλοφορίας. Οι επιτιθέμενοι έχουν την δυνατότητα να τροποποιήσουν ένα γνωστό κακόβουλου λογισμικό, και να το κάνουν ικανό να εκμεταλλευτεί ευπάθειες στο λογισμικό ελέγχου των φαναριών κυκλοφορίας αλλά και σε επίπεδο υλικού να τροποποιήσει τους προγραμματιζόμενους λογικούς ελεγκτές (PLCs) των φαναριών.

Καθώς οι επιτιθέμενοι διεισδύουν στο σύστημα και παίρνουν πρόσβαση στους φωτεινούς σηματοδότες, προσπαθούν να χειραγωγήσουν τους φωτεινούς σηματοδότες για να δημιουργήσουν χάος στους δρόμους της πόλης. Οι φωτεινοί σηματοδότες σε αυτό το σημείο συνεχίζουν να αποστέλλουν τα δεδομένα τους κανονικά στο ΚΔΚ, κάτι που σημαίνει πως οι επιτιθέμενοι δεν τα έχουν αποκόψει από την λειτουργία της αποστολής δεδομένων, το ΚΔΚ λαμβάνει κανονικά τα δεδομένα και τα αποστέλλει στο XDR σύστημα όπως έχουμε περιγράψει παραπάνω.

Μετά την λήψη των δεδομένων, το XDR σύστημα αναλύει τα δεδομένα και μέσω των τεχνικών και των κανόνων που έχουν δημιουργηθεί για ανίχνευση επιθέσεων, αντιλαμβάνεται την ύπαρξη απειλής ή επίθεσης. Για τον επιτυχημένο εντοπισμό της επίθεσης έπαιξε σημαντικό ρόλο και η σημασιολογική περιγραφή της ορθής λειτουργίας των έξυπνων φωτεινών σηματοδοτών. Έτσι μετά την αρχική επιβεβαίωση του περιστατικού ασφαλείας, το XDR σύστημα συνεχίζει την ανάλυση και την συσχέτιση δεδομένων από διάφορες πηγές για να προσδιορίσει την φύση και το εύρος της επίθεσης και πόσα και ποια συστήματα έχουν επηρεαστεί από την επίθεση. Εφόσον έχει καταστεί σαφές το εύρος τη επίθεσης και έχει εντοπίσει ποια συστήματα είναι παραβιασμένα, το XDR περνάει στην φάση της απόκρισης στο περιστατικό ασφαλείας εκδίδοντας OpenC2 εντολές προς το ΚΔΚ. Στην προκειμένη περίπτωση εκδίδει εντολές για να απομονωθούν οι παραβιασμένοι φωτεινοί σηματοδότες από το συνολικό δίκτυο, με σκοπό να σταματήσει η εξάπλωση της επίθεσης. Το ΚΔΚ από την πλευρά του θέτει σε λειτουργία τους κατάλληλους ενεργοποιητές (Actuators) οι οποίοι θα εκτελέσουν την ενέργεια της απομόνωσης και εν συνεχεία μεταφράζει τις OpenC2 εντολές που πήρε από το XDR σε ενέργειες που μπορούν να κατανοήσουν οι φωτεινοί σηματοδότες. Έπειτα, εφόσον το XDR λάβει τις κατάλληλες απαντήσεις από το ΚΔΚ πως οι εντολές που έδωσε έχουν εκτελεστεί στους φωτεινούς σηματοδότες, μπορεί να θεωρεί ότι το συμβάν έχει μετριαστεί σε σημείο που δεν απειλείτε περαιτέρω η υποδομή αλλά και οι άνθρωποι στους δρόμους.

Σε αυτό το σενάριο που αναπτύχθηκε, έγινε σαφές πως η δύναμη της αρχιτεκτονικής που εφαρμόζει η έξυπνη πόλη έγκειται στην ικανότητά της να ανιχνεύει, να αναλύει και να ανταποκρίνεται σε κυβερνοαπειλές σε πραγματικό χρόνο, αναδεικνύοντας τη σημασία μιας ενιαίας προσέγγισης της κυβερνοασφάλειας και την σημαντικότητα να μπορεί να επεμβαίνει σε τόσο κρίσιμα συστήματα σε τόσο γρήγορα χρόνο.

Κεφάλαιο 6ο: Συμπεράσματα – Μελλοντικές επεκτάσεις

6.1 Συμπεράσματα

Η παρούσα πτυχιακή εργασία αποτελεί ένα σημείο αναφοράς όσο αφορά την ανάλυση της βασικής αρχιτεκτονικής που διέπει τα συστήματα προσδιορισμού και αυτοματοποιημένης απόκρισης σε κυβερνοεπιθέσεις (XDR – Extended Detection and Response). Αρχικά έγινε η ανάλυση της αρχιτεκτονικής XDR παρουσιάζοντας τις δυνατότητές της να ενσωματώνει και να συσχετίζει δεδομένα σε πολλαπλά επίπεδα ασφαλείας, επιτρέποντας μια πιο ολοκληρωμένη και προληπτική στρατηγική άμυνας. Η ανάλυση έγινε στο επίπεδο που μπορούσε να καταστεί αυτό εφικτό, λόγω του ότι τα συστήματα XDR είναι μια νέα προσέγγιση ως προς τον εντοπισμό και απόκριση σε κυβερνοεπιθέσεις, η βιβλιογραφία και η διάθεση πληροφορίας από τις εταιρείες που αναπτύσσουν XDR συστήματα, είναι ελάχιστη κάτι που δυσκόλεψε την διαδικασία εύρεσης πηγών. Επιπλέον, αναλύθηκε ο παραδοσιακός τρόπος ανίχνευσης και απόκρισης σε κυβερνοεπιθέσεις και κατέστησαν σαφές οι περιορισμοί που υπάρχουν λόγω της πολυπλοκότητας και της έντασης των κυβερνοεπιθέσεων. Έπειτα, διερευνήθηκαν οι νέες προσεγγίσεις για τον εντοπισμό και την αντιμετώπιση απειλών στον κυβερνοχώρο, αναγνωρίζοντας τη σημασία της μηχανικής μάθησης, της τεχνητής νοημοσύνης και της ανάλυσης συμπεριφοράς για την ενίσχυση των δυνατοτήτων των λύσεων κυβερνοασφάλειας. Η υιοθέτηση αυτών των προηγμένων τεχνολογιών υπόσχεται τον εντοπισμό και την άμβλυνση των απειλών σε πραγματικό χρόνο, ελαχιστοποιώντας έτσι την έκθεση των οργανισμών σε σοβαρές απειλές και επιθέσεις. Επιπλέον, διεξήχθη λεπτομερής ανάλυση του πρωτοκόλλου OpenC2 και του προτύπου OVAL, αναδεικνύοντας τους ρόλους τους στην τυποποίηση, την ενίσχυση της επικοινωνίας, της ανταλλαγής πληροφοριών και της άμεσης απόκρισης σε ένα οικοσύστημα κυβερνοασφάλειας. Η διαλειτουργικότητα που παρέχει το OpenC2 διευκολύνει έναν πιο δυναμικό και ευέλικτο αμυντικό μηχανισμό, ενώ το OVAL τυποποιεί την αξιολόγηση των ευπαθειών και εξασφαλίζει μια ολοκληρωμένη προσέγγιση για την αξιολόγηση της ασφάλειας των συστημάτων. Καθώς οι οργανισμοί συνεχίζουν να αντιμετωπίζουν όλο ένα και πιο εξελιγμένες απειλές στον κυβερνοχώρο, οι αναφορές που έχουν γίνει στην παρούσα πτυχιακή εργασία εύχομαι να αναδεικνύουν την ανάγκη για μια ολιστική και πιο προσαρμοστική αρχιτεκτονική ασφάλειας. Τέλος είναι σημαντικό όλες οι αρχιτεκτονικές ασφαλείας και οι τρόποι που δομούνται τα Security Operation Centers (SOC) να τίθενται υπό αυστηρές κρητικές και αξιολογήσεις, με σκοπό να παραμένουν πάντα επίκαιρες στο συνεχές εξελισσόμενο και μεταβαλλόμενο περιβάλλον της κυβερνοασφάλειας.

6.2 Μελλοντικές επεκτάσεις

Καθώς το τοπίο της κυβερνοασφάλειας συνεχίζει να εξελίσσεται με πρωτοφανή ρυθμό, η παρούσα πτυχιακή εργασία παρείχε μια εκτεταμένη μελέτη της XDR αρχιτεκτονικής, των νέων προσεγγίσεων για την ανίχνευση και την αντιμετώπιση απειλών και την κριτική ανάλυση του πρωτοκόλλου OpenC2 και του προτύπου OVAL. Ωστόσο, η δυναμική φύση των απειλών στον κυβερνοχώρο και η ταχεία εξέλιξη της τεχνολογίας παρουσιάζουν μια σειρά από ευκαιρίες για μελλοντική έρευνα και ανάπτυξη.

Η παρούσα πτυχιακή θέτει τα θεωρητικά θεμέλια για την διεξαγωγή εμπειρικών μελετών και πραγματικών εφαρμογών για την αξιολόγηση της πρακτικής αποτελεσματικότητας των XDR συστημάτων σε μια σειρά από πληροφοριακά περιβάλλοντα όπως ένα παραδοσιακό IT περιβάλλον, ένα cloud περιβάλλον ή ένα IoT[81] περιβάλλον. Επιπλέον, υπάρχουν περιθώρια για διερεύνηση της

ενσωμάτωσης του XDR στο Zero Trust μοντέλο ασφάλειας και πως το XDR βοηθάει μια Zero Trust αρχιτεκτονική[82]. Μια τέτοια προσέγγιση μπορεί να προσφέρει μεγαλύτερη διαφάνεια και ορατότητα στην πληροφοριακή υποδομή, να μειώσει σημαντικά την πολυπλοκότητα γύρω από την ανάλυση των αναλυτών κυβερνοασφάλειας και του φόρτου εργασίας τους και να μειώσει το συνολικό κόστος των κεφαλαίων που προωθούνται για λύσεις κυβερνοασφάλειας από έναν οργανισμό[83].

Στο επίπεδο του OpenC2 μπορεί να διεξαχθεί μελέτη σχετικά με την πρακτική εφαρμογή του OpenC2 πρωτοκόλλου σε διάφορα IT περιβάλλοντα, όπως για παράδειγμα ένα IoT περιβάλλον, και το πως συμπεριφέρεται μέσα ένα ρεαλιστικό σενάριο εφαρμογής[84][85]. Επιπλέον, υπάρχει χώρος για μελέτη και σύγκριση των χρόνων απόκρισης και των πόρων που χρησιμοποιούνται σε ένα περιστατικό ασφαλείας όταν η απόκριση γίνεται με την χρήση του OpenC2 πρωτοκόλλου και όταν η απόκριση γίνεται με την χρήση και την βοήθεια άλλων τεχνολογιών και διαδικασιών.

Τέλος, μια περιοχή που είναι αρκετά σημαντική και χρήζει περαιτέρω μελέτης είναι η περιοχή γύρω από τα μοντέλα της μηχανικής μάθησης που χρησιμοποιούνται για την ανίχνευση απειλών. Σε αυτή την μελέτη θα μπορούσαν να αναλυθούν οι υπάρχοντες αλγόριθμοι μηχανική μάθησης γύρω από την ανίχνευση απειλών, η επιτυχία τους να ανιχνεύουν γνωστές απειλές αλλά και νεο-εμφανισθέντες απειλές και το πως θα μπορούσαν οι υπάρχοντες αλγόριθμοι να βελτιωθούν και να προσαρμοστούν κάτω από συγκεκριμένες συνθήκες και συγκεκριμένα πληροφοριακά περιβάλλοντα έτσι ώστε να παρουσιάζουν μεγαλύτερα ποσοστά επιτυχίας στην ανίχνευση απειλών.[80]

ΒΙΒΛΙΟΓΡΑΦΙΑ

Papers

[1] S. Al-Rabiaah, "The “Stuxnet” Virus of 2010 As an Example of A “APT” and Its “Recent” Variances," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 2018, pp. 1-5, doi: 10.1109/NCG.2018.8593143.

[2] M. Geiger, J. Bauer, M. Masuch and J. Franke, "An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems," 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 2020, pp. 1537-1543, doi: 10.1109/ETFA46521.2020.9212128.

[3] Q. Chen and R. A. Bridges, "Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 2017, pp. 454-460, doi: 10.1109/ICMLA.2017.0-119.

[4] M. A. Rassam, M. A. Maarof, and A. Zainal, “Big Data Analytics Adoption for Cyber-security: A Review of Current Solutions, Requirements, Challenges and Trends,” J. Inf. Assur. Secur., vol. 11, pp. 124–145, 2017.

[5] Palo Alto Networks Ignite, “Ignite USA '18 Keynote - Nir Zuk (featuring Keren Elazari),” Youtube, Jun 4, 2018 [Video file]. Available: https://www.youtube.com/watch?v=c71uPTimW_A. (accessed May 13, 2023).

[6] A. Mellen, “Introducing the forrester new tech: Extended detection and response (XDR) - a battle between precedent and Innovation,” *Forrester*, 02-Aug-2021. [Online]. Available: https://www.forrester.com/blogs/introducing-the-forrester-new-tech-extended-detection-and-response-xdr-a-battle-between-precedent-and-innovation/ (accessed May 13, 2023).

[7] K. Kent and M. Souppaya , “Guide to computer security log management - NIST,” *nist.gov*, Sep-2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf. (accessed May 13, 2023).

[8] D. Suprina, “The importance of data normalization in IPS,” *Help Net Security*, 07-Jan-2013. [Online]. Available: https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/. (accessed May 13, 2023).

[9] C. Abad, J. Taylor, C. Sengul, W. Yurcik, Y. Zhou and K. Rowe, "Log correlation for intrusion detection: a proof of concept," *19th Annual Computer Security Applications Conference, 2003. Proceedings.*, Las Vegas, NV, USA, 2003, pp. 255-264, doi: 10.1109/CSAC.2003.1254330.

[10] E. Pontes, A. E. Guelfi, S. T. Kofuji, A. A. A. Silva and A. E. Guelfi, "Applying multi-correlation for improving forecasting in cyber security," *2011 Sixth International Conference on Digital Information Management*, Melbourne, VIC, Australia, 2011, pp. 179-186, doi: 10.1109/ICDIM.2011.6093323.

[11] R. Trost, *Practical intrusion analysis: Prevention and detection for the twenty-first century*. Upper Saddle River (N.J.): Addison-Wesley, 2010.

[12] A. Hero, S. Kar, J. Moura, J. Neil, H. V. Poor, M. Turcotte, and B. Xi, “Statistics and data science for Cybersecurity,” *Issue 5.1, Winter 2023*, vol. 5, no. 1, 2023.

[13] R. M. van der Goot, “Normalization and parsing algorithms for uncertain input,” the University of Groningen research portal, https://research.rug.nl/en/publications/normalization-and-parsing-algorithms-for-uncertain-input (accessed May 13, 2023).

[14] IBM Corporation, “Cost of a Data Breach Report 2022,” IBM, Armonk, NY, USA, 2022. [Online]. Available: https://www.ibm.com/downloads/cas/3R8N1DZJ. (accessed May 13, 2023).

[15] R. Calderon, “The Benefits of Artificial Intelligence in Cybersecurity,” Econ. Crime Forensics Capstones. 36., 2019.

[16] “Cybersecurity spotlight – signature-based vs anomaly-based detection,” CIS, https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-signature-based-vs-anomaly-based-detection (accessed May 22, 2023).

[17] “How does detection work?,” Ebrary, https://ebrary.net/26722/computer_science/detection_work (accessed May 22, 2023).

[18] O. T. Suryati and A. Budiono, “Impact analysis of malware based on Call Network API with Heuristic Detection Method,” International Journal of Advances in Data and Information Systems, vol. 1, no. 1, pp. 1–8, 2020. doi:10.25008/ijadis.v1i1.176

[19] Kaspersky, “What is heuristic analysis?,” usa.kaspersky.com, https://usa.kaspersky.com/resource-center/definitions/heuristic-analysis (accessed May 22, 2023).

[20] M. Ahmed, A. Naser Mahmood, and J. Hu, “A survey of Network Anomaly Detection Techniques,” Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016. doi:10.1016/j.jnca.2015.11.016

[21] M. L. Proença, C. Coppelmans, M. Bottoli, and L. de Souza Mendes, “Baseline to help with network management,” e-Business and Telecommunication Networks, pp. 158–166, 2006. doi:10.1007/1-4020-4761-4_12

[22] A. AlEroud and G. Karabatis, "A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks," 2012 International Conference on Cyber Security, Alexandria, VA, USA, 2012, pp. 40-45, doi: 10.1109/CyberSecurity.2012.12.

[23] I. F. Kilincer, F. Ertam, and A. Sengur, “Machine learning methods for cyber security intrusion detection: Datasets and comparative study,” Computer Networks, vol. 188, p. 107840, 2021. doi:10.1016/j.comnet.2021.107840

[24] R. Prasad and V. Rohokale, “Artificial Intelligence and machine learning in cyber security,” Springer Series in Wireless Technology, pp. 231–247, 2019. doi:10.1007/978-3-030-31703-4_16

[25] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, “Phishing email detection using Natural Language Processing Techniques: A literature survey,” Procedia Computer Science, vol. 189, pp. 19–28, 2021. doi:10.1016/j.procs.2021.05.077

[26] “Building context-aware cybersecurity alerts,” Tata Consultancy Services, https://www.tcs.com/insights/topics/cybersecurity-topic/article/context-aware-cybersecurity (accessed Jun. 10, 2023).

[27] M. of C. Services, “Cyber security incident response process,” Province of British Columbia, https://alpha.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/cyber-security-incident-response-process (accessed Dec. 12, 2023).

[28] “Incident response sans: The 6 steps in depth,” Cynet, https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/ (accessed Dec. 12, 2023).

[29] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, *Guide to cyber threat information sharing*, 2016. doi:10.6028/nist.sp.800-150

[30] “What is XDR (extended detection and response)?,” IBM, https://www.ibm.com/topics/xdr (accessed Jun. Dec, 2023).

[31] M. Shealy, “How data visualization helps prevent cyber attacks,” Klipfolio, https://www.klipfolio.com/blog/how-data-visualization-prevents-cyber-attacks (accessed Dec. 12, 2023).

[32] “What is Antivirus,” Check Point Software, https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-antivirus/ (accessed Dec. 12, 2023).

[33] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: Techniques, datasets and challenges,” Cybersecurity, vol. 2, no. 1, 2019. doi:10.1186/s42400-019-0038-7

[34] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, “Intrusion detection system: A comprehensive review,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, 2013. doi:10.1016/j.jnca.2012.09.004

[35] Z. Wang and X. Li, “Intrusion Prevention System Design,” Lecture Notes in Electrical Engineering, pp. 375–382, 2013. doi:10.1007/978-1-4471-4847-0_47

[36] Yujia Zhang, Guanlin Chen, Wenyong Weng and Zebing Wang, "An overview of wireless intrusion prevention systems," 2010 Second International Conference on Communication Systems, Networks and Applications, Hong Kong, China, 2010, pp. 147-150, doi: 10.1109/ICCSNA.2010.5588671.

[37] “What is a Firewall?,” Cisco, https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (accessed Dec. 12, 2023).

[38] Kaspersky, “What is a Firewall? definition and explanation,” www.kaspersky.com, https://www.kaspersky.com/resource-center/definitions/firewall (accessed Dec. 12, 2023).

[39] S. Waterman, “NSA’s new Open language for cyber-defenses will aid interoperability,” CyberScoop, https://cyberscoop.com/openc2-nsa-open-source-cyber-defense/ (accessed Dec. 24, 2023).

[40] OpenC2, https://openc2.org/ (accessed Dec. 24, 2023).

[41] V. Mavroeidis and J. Brule, “A nonproprietary language for the command and control of cyber defenses – openc2,” Computers & Security, vol. 97, p. 101999, 2020. doi:10.1016/j.cose.2020.101999

[42] “Open Command and Control (OpenC2) Architecture,” Open Command and Control (OpenC2) Architecture Specification Version 1.0, https://docs.oasis-open.org/openc2/oc2arch/v1.0/oc2arch-v1.0.html (accessed Dec. 24, 2023).

[43] “Open Command and Control (OpenC2) Language,” Open Command and Control (OpenC2) Language Specification Version 1.0, https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs02/oc2ls-v1.0-cs02.html (accessed Dec. 24, 2023).

[44] “Open vulnerability and assessment language,” OVAL, https://oval.mitre.org/ (accessed Dec. 24, 2023).

[45] Lucideus, “Open vulnerability assessment language: An overview: Lucideus research,” Medium, https://medium.com/@lucideus/open-vulnerability-assessment-language-an-overview-lucideus-research-2dc8acbbdf19 (accessed Dec. 24, 2023).

[46] Introduction to oval - NIST Computer Security Resource Center, https://csrc.nist.gov/CSRC/media/Projects/Security-Content-Automation-Protocol/documents/docs/conference%20presentations/workshops/OVAL%20Tutorial%201%20-%20Overview.pdf (accessed Dec. 24, 2023).

[47] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, “Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures,” Sensors, vol. 21, no. 14, p. 4759, 2021. doi:10.3390/s21144759

[48] D. Swift, “A Practical Application of SIM/SEM/SIEM Automating Threat Identification,” SANS Institute, https://www.sans.org/white-papers/1781/ (accessed Jan. 4, 2024).

[49] K. -O. Detken, T. Rix, C. Kleiner, B. Hellmann and L. Renners, "SIEM approach for a higher level of IT security in enterprise networks," 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Warsaw, Poland, 2015, pp. 322-327, doi: 10.1109/IDAACS.2015.7340752.

[50] “What is Siem? how does it work?,” Fortinet, https://www.fortinet.com/resources/cyberglossary/what-is-siem (accessed Jan. 4, 2024).

[51] “Περιοχή παρέμβασης,” ΜΗΤΡΟΠΟΛΙΤΙΚΗ ΘΕΣΣΑΛΟΝΙΚΗ, https://thma.gov.gr/perioxi-paremvasis/ (accessed Jan. 5, 2024).

[52] S. Singh, “Modern Cyber Defense-part 7-extended detection & response (XDR),” Medium, https://sanjeev41924.medium.com/modern-cyber-defense-part-7-extended-detection-response-xdr-d76fd3b5fef5 (accessed Jan. 8, 2024).

[53] “Infographic: Defense-in-depth,” Colohouse, https://colohouse.com/infographic-defense-in-depth/ (accessed Jan. 8, 2024).

[54] “Incident response phases – identification,” Halkyn Security Blog, https://www.halkynconsulting.co.uk/a/2019/06/incident-response-identification/ (accessed Jan. 8, 2024).

[55] R. Lefferts, “Microsoft delivers unified SIEM and XDR to modernize security operations,” Microsoft Security Blog, https://www.microsoft.com/en-us/security/blog/2020/09/22/microsoft-unified-siem-xdr-modernize-security-operations/ (accessed Jan. 8, 2024).

[56] “The third generation of XDR has arrived!,” Palo Alto Networks Blog, https://www.paloaltonetworks.sg/blog/2021/08/third-generation-xdr-has-arrived/ (accessed Jan. 8, 2024).

[57] “Open vulnerability and assessment language,” OVAL Language Overview, https://oval.mitre.org/language/about/overview.html (accessed Jan. 8, 2024).

[58] “How it works,” VirusTotal, https://docs.virustotal.com/docs/how-it-works (accessed Jan. 12, 2024).

[59] “About abuseipdb,” AbuseIPDB, https://www.abuseipdb.com/about.html (accessed Jan. 12, 2024).

[60] Cisco Talos Intelligence Group - Comprehensive Threat Intelligence, https://www.talosintelligence.com/ (accessed Jan. 12, 2024).

[61] Urlscan.io, “Urlscan.io a sandbox for the web,” About, https://urlscan.io/about/ (accessed Jan. 12, 2024).

[62] ANY.RUN - Interactive Online Malware Sandbox, https://any.run/ (accessed Jan. 12, 2024).

[63] AlienVault Open Threat Exchange, https://otx.alienvault.com/ (accessed Jan. 12, 2024).

[64] Shodan, https://www.shodan.io/ (accessed Jan. 12, 2024).

[65] Censys, https://censys.com/ (accessed Jan. 12, 2024).

[66] N. Fox, “Cuckoo sandbox overview,” Varonis, https://www.varonis.com/blog/cuckoo-sandbox (accessed Jan. 12, 2024).

[67] “What is a spoofing attack? detection & prevention,” Rapid7, https://www.rapid7.com/fundamentals/spoofing-attacks/ (accessed Jan. 14, 2024).

[68] MITRE, https://www.mitre.org/ (accessed Jan. 14, 2024).

[69] [1] “What is the CIA triad and why is it important?,” Fortinet, https://www.fortinet.com/resources/cyberglossary/cia-triad (accessed Jan. 14, 2024).

[70] “What is XML?,” Amazon, https://aws.amazon.com/what-is/xml/ (accessed Jan. 14, 2024).

[71] “The standard for IOT messaging,” MQTT, https://mqtt.org/ (accessed Jan. 14, 2024).

[72] “What is defense in depth? defined and explained,” Fortinet, https://www.fortinet.com/resources/cyberglossary/defense-in-depth (accessed Jan. 15, 2024).

[73] “What are TTPS? tactics, Techniques & Procedures explained,” Splunk, https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html (accessed Jan. 15, 2024).

[74] “What is a honeypot?,” www.kaspersky.com, https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot (accessed Jan. 17, 2024).

[75] B. Lutkevich, C. Clark, and M. Cobb, What is a honeypot? how it protects against Cyber Attacks, https://www.techtarget.com/searchsecurity/definition/honey-pot (accessed Jan. 17, 2024).

[76] “XSOAR 8: Re-architected for performance, scalability, and Reliability,” Palo Alto Networks Blog, https://www.paloaltonetworks.com/blog/security-operations/xsoar-8-re-architected-for-performance-scalability-and-reliability/ (accessed Jan. 17, 2024).

[77] MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing, https://www.misp-project.org/ (accessed Jan. 18, 2024).

[78] Recorded Future: Securing Our World With Intelligence, https://www.recordedfuture.com/ (accessed Jan. 18, 2024).

[79] Security Operations Platform Powered by AI I Anomali, https://www.anomali.com/ (accessed Jan. 18, 2024).

[80] S. Dua and X. Du, Data Mining and Machine Learning in Cybersecurity. Boca Raton, FL: CRC Press, 2011.

[81] M. Repetto, A. Carrega, and R. Rapuzzi, “An architecture to manage security operations for Digital Service Chains,” Future Generation Computer Systems, vol. 115, pp. 251–266, 2021. doi:10.1016/j.future.2020.08.044

[82] M. Tsai, S. Lee, and S. W. Shieh, “Strategy for implementing of Zero trust architecture,” IEEE Transactions on Reliability, pp. 1–8, 2024. doi:10.1109/tr.2023.3345665

[83] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, “Theory and application of Zero trust security: A brief survey,” Entropy, vol. 25, no. 12, p. 1595, 2023. doi:10.3390/e25121595

[84] D. Sparrell, “Cyber-safety in healthcare IOT,” 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K), 2019. doi:10.23919/ituk48006.2019.8996148

[85] Demonstrating the use of openc2 and soar, https://static1.squarespace.com/static/5a94b67ff93fd440f0516297/t 5fcf6b001901dd4d2ed4a228/1607428864536/using+soar+with+openc2.pdf (accessed Jan. 18, 2024).