
# ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
**ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ**

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ


# Συγκριτική μελέτη SIEM εργαλείων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των


Καλπούζος Στέργιος
Κίγκας Νικόλαος


**Επιβλέπων :** Καμπουράκης Γεώργιος

**Μέλη εξεταστικής επιτροπής:**
- Μπαρμπάτσαλου Κωνσταντία
- Καρύδα Μαρία

Σάμος, Μάϊος 2023

# Πρόλογος και ευχαριστίες

Είμαστε στην ευχάριστη θέση να παρουσιάσουμε αυτή τη διπλωματική, η οποία αντιπροσωπεύει το αποκορύφωμα πολυετούς έρευνας, μάθησης και σκληρής δουλειάς. Η παρούσα διπλωματική εργασία είναι το αποτέλεσμα μιας συνεργασίας με πολλούς ανθρώπους που μας στήριξαν και μας ενθάρρυναν σε όλη τη διάρκεια της διαδικασίας. Είναι μεγάλο προνόμιο να μοιραζόμαστε την έρευνά μας με την ακαδημαϊκή κοινότητα και να συνεισφέρουμε στο σύνολο των γνώσεων στον τομέα μας.

Θα θέλαμε να εκφράσουμε τις ευχαριστίες μας στα πολλά άτομα που συνέβαλαν στην ολοκλήρωση αυτής της διπλωματικής εργασίας. Πρώτα και κύρια, θέλουμε να ευχαριστήσουμε τον επιβλέπων διδάσκων μας, κύριο Καμπουράκη Γεώργιο, για την καθοδήγηση, την υποστήριξή της και τα οξυδερκή σχόλιά του. Ευχαριστούμε επίσης τα μέλη της επιτροπής της διατριβής μας, κυρίες Μπαρμπάτσαλου Κωνσταντία και Καρύδα Μαρία, για την πολύτιμη συμβολή και την εποικοδομητική κριτική τους. Επιπρόσθετα, θα θέλαμε να ευχαριστήσουμε την οικογένεια και τους φίλους μας για την αμέριστη υποστήριξη και ενθάρρυνση σε όλη τη διάρκεια της ακαδημαϊκής μας πορείας.

Τέλος, θα θέλαμε να ευχαριστήσουμε την επιχείρηση στην οποία ανήκουμε, η οποία μας έδωσε τη δυνατότητα να πραγματοποιήσουμε αυτήν την έρευνα, την επωνυμία της οποίας δεν μπορούμε να αναφέρουμε για λόγους ασφαλείας. Χωρίς την υποστήριξη αυτών των ατόμων και οργανισμών, η παρούσα διατριβή δεν θα ήταν δυνατή.



Καλπούζος Στέργιος

Κίγκας Νικόλαος

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

# Πίνακας περιεχομένων

# Ακρωνύμια

| | |
|---|---|
| SIEM | Security Information and Event Management |
| SEM | Security Event Management |
| SIM | Security Information Management |
| SOC | Security Operations Center |
| OT | Operational Technology |
| UEBA | User Entity Behavior Analytics |
| EID | Event ID |
| EDR | Endpoint Detection and Response |
| SOAR | Security Orchestration, Automation and Response |
| NDR | Network Detection and Response |
| SaaS | Software as a Service |

# Περίληψη

Τα συστήματα Διαχείρισης Πληροφοριών και Συμβάντων Ασφάλειας (SIEM) έχουν γίνει σήμερα ένα κρίσιμο και ουσιαστικό στοιχείο σύνθετων δικτύων και επιχειρήσεων, αποτελώντας βασικό άξονα γύρω από τον οποίο περιστρέφονται οι λειτουργίες ασφάλειας ενός οργανισμού.

Αποτελεί γεγονός ζωτικής σημασίας η αξιολόγηση της ποιότητας μίας τέτοιας λύσης και η διασφάλιση ότι η διαχείρισή της, από την ομάδα SOC, θα επιφέρει την κάλυψη των απαιτήσεων ασφάλειας που έχει θέσει μια επιχείρηση ή ένας οργανισμός.

Δεδομένης της ύπαρξης ευρέως φάσματος SIEM λύσεων που είναι διαθέσιμες σήμερα στην αγορά καθώς και της ποικιλομορφίας των υπό προστασία αγαθών, το έργο των ατόμων που έχουν κληθεί να επιλέξουν το κατάλληλο SIEM προϊόν για τον οργανισμό στον οποίο ανήκουν, καθίσταται δυσχερές.

Κάθε πλατφόρμα SIEM φέρει πολλά πλεονεκτήματα και μειονεκτήματα. Πολλά εξ' αυτών είναι ευρέως και δημόσια γνωστά, ωστόσο υπάρχουν και κάποια τα οποία είναι εμφανή μόνο μέσα από την ουσιαστική διαχείριση και τριβή με τη εκάστοτε λύση.

Στην παρούσα εργασία επιχειρείται μια συγκριτική μελέτη δύο εκ των κορυφαίων SIEM εργαλείων από τη σκοπιά ενός αναλυτή ασφάλειας που τις διαχειρίζεται. Ως βασικό μέσο σύγκρισης θα δημιουργηθούν και θα χρησιμοποιηθούν κοινές περιπτώσεις χρήσης (use cases) κακόβουλων τακτικών και τεχνικών.

**Λέξεις Κλειδιά:** *διαχείριση πληροφοριών και συμβάντων ασφαλείας, παρακολούθηση ασφαλείας, διαχείριση αρχείων καταγραφής, ανίχνευση απειλών, κυβερνοασφάλεια, κέντρο λειτουργιών ασφαλείας, analytics ασφαλείας, σύγκριση προμηθευτών, συμβάντα ασφαλείας, αρχεία καταγραφής, περιπτώσεις χρήσης, κανόνες συσχέτισης, αδικήματα ασφαλείας, περιστατικά ασφαλείας, κακόβουλες τακτικές, κακόβουλες τεχνικές*

# Abstract

Security Information and Event Management (SIEM) systems have today become a critical and essential component of complex networks and enterprises, forming a key axis around which an organization's security operations revolve.

It is vital to assess the quality of such a solution and ensure that its management by the SOC team will meet the security requirements set by a business or organization.

Given the wide range of SIEM solutions available in the market today as well as the diversity of assets under protection, the task of individuals tasked with choosing the right SIEM product for their organization becomes difficult.

Each SIEM platform has many advantages and disadvantages. Many of these are widely and publicly known, however there are also some which are only apparent through the essential management and friction with each solution.

In this paper, a comparative study of two of the leading SIEM tools is attempted from the point of view of a security analyst who manages them. As a basic means of comparison, common use cases of malicious tactics and techniques will be created and used.

**Keywords:** *SIEM (Security Information and Event Management), security monitoring, log management, threat detection, cybersecurity, Security Operations Center (SOC), security analytics, vendor comparison, security events, logs, use cases, correlation rules, security offences, security incidents, malicious tactics, malicious techniques*

# 1

# *Εισαγωγή*

## *1.1 Εντοπισμός και διαχείριση περιστατικών ασφαλείας*

Οι εξελιγμένες κυβερνο-επιθέσεις έχουν γίνει ένας σημαντικός αντίπαλος στον διαρκώς εξελισσόμενο κυβερνο-χώρο. Οι μέρες στις οποίες βασιζόμασταν σε έλεγχο της περιμέτρου μιας οντότητας (εταιρείας ή οργανισμού) ή σε λύσεις προστασίας από ιούς έχουν πλέον παρέλθει. Αναγκαιότητα των ημερών που ζούμε αποτελεί η χρήση πολύ-επίπεδων αμυντικών τεχνολογιών.

Βασική προϋπόθεση για τον εντοπισμό μίας κυβερνο-επίθεσης από τους αναλυτές ασφάλειας είναι η ύπαρξη καταγεγραμμένων γεγονότων, τα οποία αρχικά θα πρέπει να συλλέξουν από κάθε επηρεασμένο πληροφοριακό σύστημα και έπειτα να πραγματοποιήσουν αναζήτηση και συσχέτιση επί αυτών. Ωστόσο, με την συνεχή ραγδαία εξέλιξη της τεχνολογίας, αυξάνεται ανάλογα και ο ρυθμός παραγωγής των γεγονότων με άμεση συνέπεια και στον τελικό όγκο των δεδομένων. Το γεγονός αυτό σε συνδυασμό με το πλήθος και την ποικιλομορφία των πληροφοριακών συστημάτων ενός οργανισμού, καθιστά αδύνατο τον έγκαιρο εντοπισμό μίας επίθεσης, καθώς έως ότου ο αναλυτής καταφέρει να συλλέξει τα απαιτούμενα γεγονότα από τα επιμέρους επηρεασμένα συστήματα, αυτά ενδέχεται να έχουν διαγραφεί προκειμένου να μην υπάρξει ολική κάλυψη του αποθηκευτικού χώρου και κατά συνέπεια διακοπή υπηρεσιών.

Τα παραπάνω οδήγησαν στην ανάγκη μίας λύσης κεντρικής συλλογής και αποθήκευσης γεγονότων, η οποία θα έδινε παράλληλα δυνατότητες γρήγορης αναζήτησης και συσχέτισης επί των γεγονότων με σκοπό τον έγκαιρο εντοπισμό μίας επίθεσης. Η λύση που καλύπτει τις παραπάνω απαιτήσεις είναι τα συστήματα Security Information and Event Management (SIEM).

Με τον όρο SIEM αναφερόμαστε σε μια λύση λογισμικού που συγκεντρώνει και αποθηκεύει δραστηριότητα από πολλές διαφορετικές πηγές (sources) με τελικό σκοπό την ανάδειξη περιστατικών ασφαλείας (offences ή incidents) μέσω κανόνων (rules) που συσχετίζουν τις δραστηριότητες αυτές.

Πηγές δραστηριοτήτων μπορούν να αποτελέσουν οι σταθμοί εργασίας τελικών χρηστών (endpoints), δικτυακές συσκευές (όπως routers, switches, firewalls), διακομιστές, domain controllers, βάσεις δεδομένων, λειτουργικά συστήματα, εφαρμογές, άλλες κεντρικές λύσεις ασφάλειας, υπηρεσίες cloud, συστήματα περιβάλλοντος βιομηχανικής πληροφορικής (OT) και πολλές άλλες που ενδέχεται να βρεθούν στην υποδομή ενός οργανισμού ή μιας επιχείρησης.

Η πιο συνηθισμένη μορφή δραστηριότητας είναι τα γεγονότα (events), τα οποία επί το πλείστων βρίσκονται αποθηκευμένα σε αρχεία καταγραφής (log files) ή βάσεις δεδομένων. Μία επιπλέον μορφή δραστηριότητας η οποία μπορεί να πλαισιώσει τα events και να εμπλουτίσει τις πληροφορίες ενός περιστατικού είναι οι δικτυακές ροές (flows).

Η κεντρική συλλογή, η μακροχρόνια αποθήκευση και η συσχέτιση σε πραγματικό χρόνο των ποικιλόμορφων γεγονότων και δικτυακών ροών από τις αναρίθμητες πηγές, αναμφίβολα καθιστούν την λύση SIEM αναπόσπαστο εργαλείο ενός Security Operation Center (SOC)[1], καθώς ενισχύονται οι βασικές ιδιότητες της ορατότητας (visibility) και της άμεσης απόκρισης (response) σε περιστατικά ασφάλειας.

Με το πέρασμα των χρόνων τα εργαλεία SIEM έχουν εξελιχθεί και έχουν γίνει κάτι περισσότερο από εργαλεία που απλώς συνδυάζουν τη διαχείριση πληροφοριών ασφάλειας (SIM) και τη διαχείριση συμβάντων ασφάλειας (SEM), αφού πλέον μπορούν και προσφέρουν προηγμένες αναλύσεις συμπεριφοράς χρηστών και οντοτήτων (UEBA) χάρη στη δύναμη της τεχνητής νοημοσύνης και του machine learning.

Τα συγκεκριμένα συστήματα καταφέρνουν να ανταποκριθούν έγκαιρα σε επίθεση με ακρίβεια που πλησιάζει το 90% και ταχύτητα συσχέτισης γεγονότων 60 δευτερολέπτων, έχοντας παράλληλα τη δυνατότητα παροχής λεπτομερών εκθέσεων συμμόρφωσης με νόμους και πλαίσια [1].

Στην αγορά υπάρχουν πολλές λύσεις SIEM, οι οποίες διαφέρουν ως προς την αρχιτεκτονική, τις απαιτήσεις λειτουργίας, τις υποστηριζόμενες πηγές γεγονότων, τις δυνατότητες και τους περιορισμούς σχετικά με τις βασικές τεχνικές απαιτήσεις (όπως επεξεργασία γεγονότων, δημιουργία κανόνων συσχέτισης, ανάδειξη περιστατικών και ειδοποίηση αναλυτών), τις επιπρόσθετες -των βασικών- δυνατοτήτες καθώς επίσης και του κόστους.

Το πεδίο εφαρμογής, το μέγεθος, τα πληροφοριακά αγαθά, το περιβάλλον και οι επιχειρησιακές λειτουργίες, το επίπεδο εξειδίκευσης αναλυτών ασφάλειας κάθε οργανισμού ή εταιρίας είναι μοναδικά, γεγονός που σε συνδυασμό με τις διαφοροποιήσεις που προαναφέραμε ως προς τις δυνατότητες των διαφόρων λύσεων, καθιστά δύσκολο έως ακατόρθωτο να γνωρίζει κάποιος κατά τη φάση της έρευνας αγοράς, τις δυσκολίες και τους περιορισμούς που ενδέχεται να συναντήσει κατά την υλοποίηση και παραγωγική λειτουργία της λύσης την οποία εξετάζει προς προμήθεια.

Κάποια ενδεικτικά συχνά προβλήματα που αντιμετωπίζουν οι οργανισμοί σχετικά με μία λύση SIEM είναι το υψηλό ποσοστό false-positive alerts, η αναποτελεσματική ιεράρχηση των περιστατικών ασφάλειας, η περιορισμένη πληροφορία στο περιεχόμενο των γεγονότων, η χειροκίνητη διαμόρφωση περίπλοκων κανόνων, με σκοπό τον έλεγχο στη συσχέτιση γεγονότων και την αναφορά (reporting) περιστατικών ασφάλειας, με ότι χρονικό κόστος αυτό συνεπάγεται, η περιορισμένη γνώση των αναλυτών SOC σε γλώσσες πρόσβασης και διαχείρισης βάσεων δεδομένων και κατά συνέπεια πινάκων με πεδία και εγγραφές, καθώς

[1] Με τον όρο Security Operations Center (SOC) αναφερόμαστε σε ομάδες από security analysts και experts που αφιερώνονται σε υψηλής ποιότητας λειτουργίες κυβερνοασφάλειας. Βασική επιδίωξη ενός Security Operations Center είναι η ανίχνευση και απόκριση σε οποιοδήποτε περιστατικό λάβει χώρα στα πληροφοριακά αγαθά που επιβλέπει.

και περιορισμούς της εκάστοτε λύσης σε τομείς όπως άνω φράγματα σε πλήθος κανόνων που σηματοδοτούν διαφορετικά περιστατικά ή μέγιστος αριθμός από περιστατικά που αναγνωρίζονται από το κάθε σύστημα.

## *1.2 Αντικείμενο διπλωματικής*

Το βασικό αντικείμενο της συγκεκριμένης εργασίας αποτελεί η συγκριτική μελέτη δύο εκ των κορυφαίων (Leaders κατά το Magic Quadrant for SIEM της Gartner για τον Ιούνιο του 2022) [2] λύσεων SIEM:

- IBM Qradar και
- Microsoft Sentinel.

Η σύγκριση έχει ως κύριο σκοπό να αναδείξει πλεονεκτήματα αλλά και περιορισμούς μεταξύ των λύσεων, αφενός ως προς τις βασικές τεχνικές λειτουργίες που καλείται ένας αναλυτής ασφάλειας να εκτελεί κατά τη διαχείριση ενός τέτοιου συστήματος και αφετέρου ως προς την κάλυψη βασικών τεχνικών απαιτήσεων που οφείλουν αυτού του είδους οι λύσεις να προσφέρουν.

Προκειμένου να αναδειχθούν παράμετροι προς σύγκριση αλλά και να έχουμε το κατά δύναμη αντικειμενικότερα ποιοτικά ή ποσοτικά κριτήρια σύγκρισης, κρίνεται απαραίτητη η προσομοίωση της διαχείρισης των δύο λύσεων από την οπτική ενός αναλυτή ασφάλειας.

Όπως αναφέρθηκε στην παράγραφο 1.1 οι επιπρόσθετες δυνατότητες και λειτουργίες που πλαισιώνουν τις βασικές, μίας λύσης SIEM, ποικίλουν μεταξύ των λύσεων. Το γεγονός αυτό επηρεάζει το πεδίο εφαρμογής και σύγκρισης της παρούσας εργασίας. Παράδειγμα βασικής διαφοράς των δύο εξεταζόμενων λύσεων είναι η επιπρόσθετη λύση SOAR (Security Orchestration, Automation and Response), η οποία μεταξύ άλλων, φέρει τη δυνατότητα αυτοματισμού ενεργειών που θα έκανε χειροκίνητα κάποιος αναλυτής, ως ενέργειες απόκρισης σε περιστατικά ασφάλειας. Στην λύση Microsoft Sentinel η λύση SOAR συμπεριλαμβάνεται out of the box, ενώ η IBM παρέχει την αντίστοιχη λύση ως SaaS υπηρεσία προς διασύνδεση με το QRadar ξεχωριστά και με επιπλέον κόστος.

Μία ακόμη βασική διαφορά που πρέπει να αναφερθεί είναι η ορατότητα, η ανάλυση και η αξιοποίηση δικτυακών ροών (network flows). Το Microsoft Sentinel στον συγκεκριμένο τομέα, σε αντίθεση με την πλειονότητα άλλων SIEM λύσεων, δεν διαθέτει τέτοιου είδους δυνατότητα και οι οργανισμοί καταφεύγουν στην προμήθεια λύσης Network Detection and Response (NDR) για την κάλυψη των σχετικών απαιτήσεων ασφάλειας. Στο IBM QRadar παρέχεται η δυνατότητα δημιουργίας περιστατικών με βάση είτε μόνο στην παρακολούθηση συγκεκριμένων δικτυακών ροών ενός δικτύου, είτε συνδυάζοντας αυτές με κοινά γεγονότα καταγραφής (events).

Κατά συνέπεια προκειμένου να μην οδηγηθούμε σε μια σύγκριση μεταξύ ανομοιογενών παραμέτρων, θα περιορίσουμε την προσομοίωση των λειτουργιών στις βασικές μίας λύσης SIEM, οι οποίες είναι η αναζήτηση επί γεγονότων καταγραφής, η δημιουργία κανόνων συσχέτισης γεγονότων για την ανάδειξη περιστατικών ασφαλείας και η προβολή των αντίστοιχων περιστατικών έπειτα της ικανοποίησης των κανόνων.

Απαραίτητο στοιχείο για την εκτέλεση των προαναφερόμενων λειτουργιών αποτελεί η ύπαρξη σεναρίων επίθεσης ή αλλιώς περιπτώσεων χρήσης (Use Cases) κακόβουλων τακτικών και τεχνικών. Για την επίτευξη του βασικού ζητούμενου της εργασίας κρίνεται σκόπιμο κάθε use case να εξεταστεί από κοινού και στις δύο λύσεις. Συνεπώς, ένα επιπλέον αντικείμενο της εργασίας αποτελεί η παρουσίαση και η

προσομοίωση κάποιων βασικών use cases που θα πρέπει να περιλαμβάνονται στο ευρετήριο ενός SOC καθώς και ο τρόπος εντοπισμού αυτών από τις δύο εξεταζόμενες λύσεις SIEM.

## *1.3 Δομή της διπλωματικής*

Στο Κεφάλαιο 2 παρουσιάζονται τα use cases αρχικά σε θεωρητικό επίπεδο με την περιγραφή τους και τα βασικά τους στοιχεία, έπειτα η υλοποίησή τους σε κάθε εξεταζόμενη λύση SIEM και τέλος η προσομοίωση αυτών. Στο Κεφάλαιο 3 αναπτύσσεται η σύγκριση των δύο εξεταζόμενων λύσεων, κατά την οποία αναφέρονται σημαντικές διαφορές που σημειώθηκαν στο πλαίσιο εργασιών του Κεφαλαίου 2.

# 2

# *Use Cases*

Για κάθε use case που θα παρουσιάσουμε θα αναφέρουμε τα ακόλουθα:

- **Objective**: τον στόχο που προσπαθεί να επιτύχει.
- **MITRE Tactics & Techniques**: τις τακτικές και τις τεχνικές - κατά την γνωσιακή βάση MITRE ATT&CK [3]- τις οποίες προσπαθούμε να εντοπίσουμε μέσω του use case.
- **LogSources**: τον τύπο των γεγονότων ο οποίος εμμέσως προσδιορίζει τα συστήματα πηγές από τα οποία έχουν παραληφθεί τα γεγονότα. Για το QRadar το πεδίο είναι το Log Source Type ενός Log Source ενώ για το Sentinel το Data Type ενός Data Connector.
- **Severity/Criticality**: ο βαθμός κρισιμότητας που θέτουμε στο περιστατικό το οποίο θα δημιουργηθεί. Δυστυχώς δεν υπάρχει προτυποποίηση επ' αυτού του πεδίου και κάθε σύστημα διαθέτει τη δικιά του κλίμακα. Συνεπώς προβήκαμε στην ακόλουθη αντιστοίχιση-παραδοχή, προκειμένου να έχουμε μία κατά δύναμη κοινή κατηγοριοποίηση.

| Sentinel (Criticality) | QRadar (Severity) |
|---|---|
| **Informational** | **0,1,2** |
| **Low** | **3,4,5** |
| **Medium** | **6,7,8** |
| **High** | **9,10** |

Έπειτα για κάθε λύση αναφέρουμε το rule το οποίο θα παράξει το offense/incident, τα ίδια τα offenses/incidents, τα events που ικανοποίησαν τα κριτήρια του rule και τέλος για όποια κρίνεται απαραίτητο, παρουσιάζουμε τις ενέργειες που ικανοποιούν τα κριτήρια ή αλλιώς την προσομοίωση της επίθεσης.

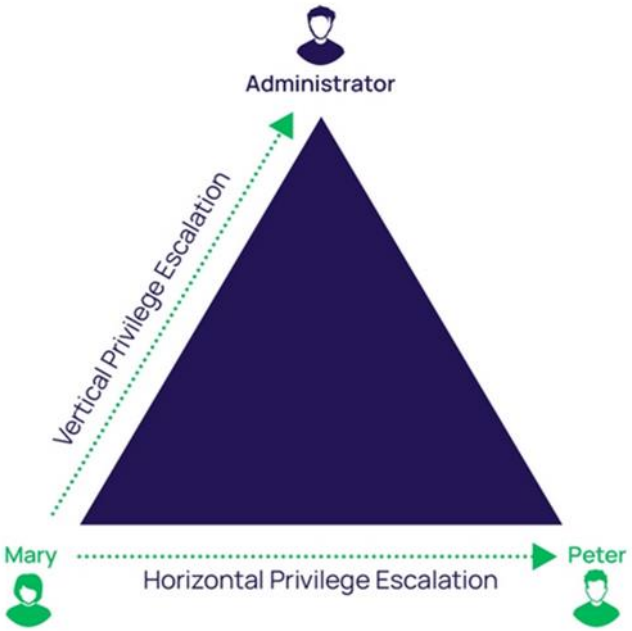
## *2.1 A member was added to a built in privileged domain security group.*

**Objective**: Ένα σύστημα Active Directory διαχειρίζεται, μεταξύ άλλων, από τους παρακάτω privileged ρόλους [4]:

- Domain Admins: αποτελεί ένα AD security group το οποίο πρώτο σκέφτονται όσοι συζητούν για διαχείριση ενός Active Directory συστήματος. Το συγκεκριμένο group έχει εξ' ορισμού πλήρη δικαιώματα διαχειριστή σε όλους τους servers, τα workstations, τους Domain Controllers και γενικά κάθε συσκευή που είναι joined στο domain. Σε κάθε υπολογιστή που συνδέεται στο AD προστίθεται το Domain Admins στο local Administrators group. Καθώς η εφαρμογή του least privilege επιφέρει πολυπλοκότητα στη διαχείριση, συχνά τα IT τμήματα εκμεταλλεύονται το εύρος εφαρμογής του δικαιώματος για να πραγματοποιήσουν μαζικές ενέργειες διαχείρισης των συστημάτων. Οι λογαριασμοί με τον ρόλο αυτό στην ουσία κρατούν τα «κλειδιά του βασιλείου», εφόσον έχουν τη δυνατότητα access σε κάθε σύστημα, σε κάθε file, σε κάθε subnet του ενδοδικτύου του οργανισμού.
- Enterprise Admins: είναι μια ομάδα στο forest root domain που έχει πλήρη δικαιώματα σε κάθε τομέα και δομή του AD.
- Administrators: αποτελούν διαχειριστές του AD domain, έχοντας default admin δικαιώματα καθώς και δυνατότητα παροχής των δικαιωμάτων αυτών σε Domain και Enterprise Admins.
- Schema Admins: group το οποίο έχει το δικαίωμα να τροποποιεί το σχήμα το Active Directory Forest schema.

Από τους παραπάνω ρόλους επιλέξαμε να ασχοληθούμε με τον εντοπισμό προσθήκης Active Directory User Account σε Domain Admins group (Event ID 4728 [5]), αφού με βάση το least privilege principle η απόδοση τόσο ισχυρών δικαιωμάτων στα πλαίσια ενός domain θα πρέπει να ελέγχεται συνεχώς και όταν πραγματοποιείται θα πρέπει να υπάρχει πλήρως αιτιολογημένο αίτημα αλλαγής (change request) σε κάποιο ticketing σύστημα το οποίο ιδανικά να αποτελεί πηγή της SIEM λύσης για πιο άμεσες ενέργειες επιβεβαίωσης false positive από τους αναλυτές.

Η τεχνική του privilege escalation είναι ευρέως γνωστή, αφού κακόβουλοι κάνοντας χρήση της αποκτούν υπό τον έλεγχό τους όλο το εσωτερικό δίκτυο μιας επιχείρησης ή ενός οργανισμού.



**MITRE Tactic**: Persistence, Privilege Escalation

**MITRE Technique**: T1098 - Account Manipulation, T1078 - Valid Accounts

**LogSources**: Microsoft Windows Security Events

**Severity/Criticality**: High (9)

### *2.1.1 QRadar*

#### *2.1.1.1* Rule

Rule Description

Apply A member was added to a built in privileged domain security group on events which are detected by the Local system
and when the event(s) were detected by one or more of Microsoft Windows Security Event Log
and when any of EventID (custom) match 4728
and when any of Group Name (custom) match Domain Admins

Rule Actions

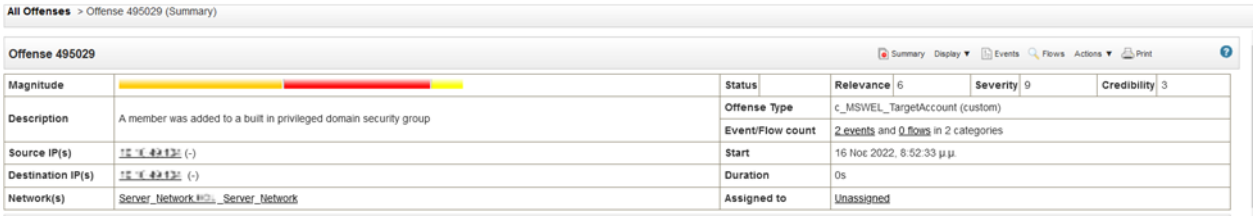
- Set Severity to 9
- Force the detected Event to create a NEW offense, select the offense using c_MSWEL_TargetAccount (custom)

Rule Responses

- Dispatch New Event
  - Event Name: A member was added to a built in privileged domain security group
  - Event Description: A member was added to a built in privileged domain security group
  - Severity: 9 Credibility: 0 Relevance: 0
  - High-Level Category: Risk
  - Low-Level Category: Compliance Violation
  - Force the dispatched event to create a NEW offense, select the offense using c_MSWEL_TargetAccount (custom)

This Rule will be: Enabled

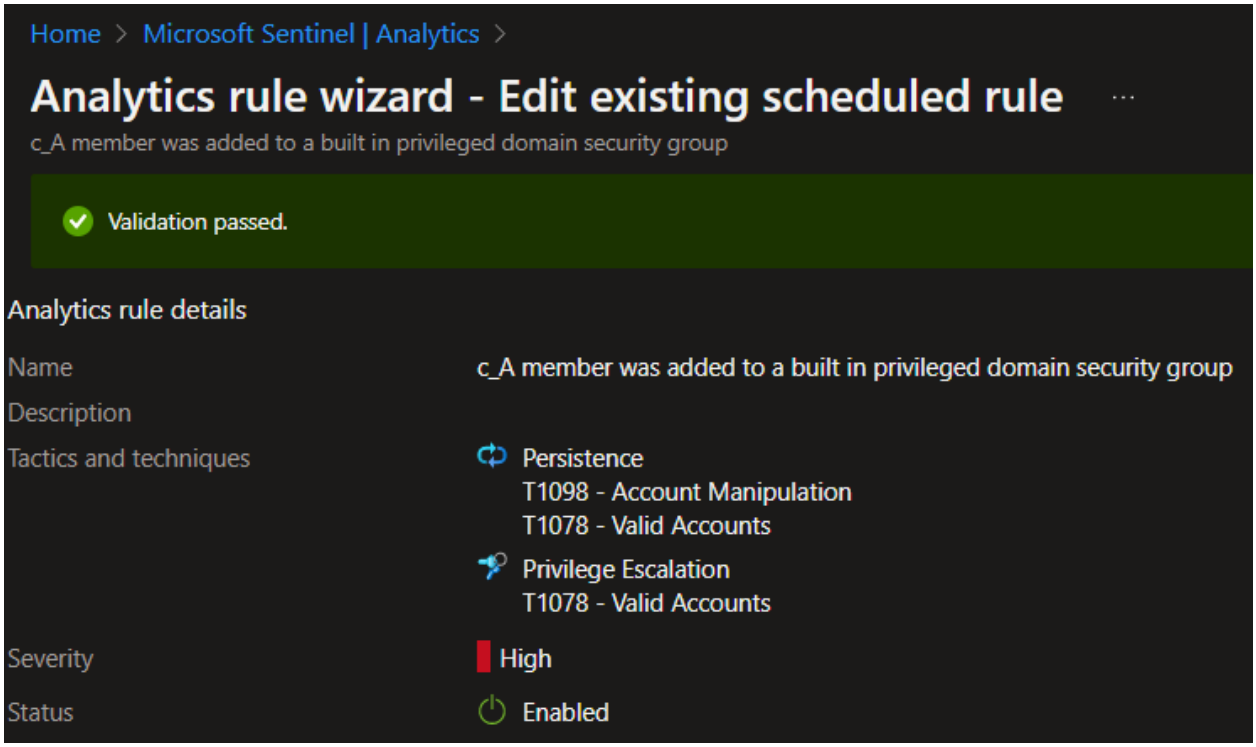
#### *2.1.1.2 Offense*




#### *2.1.1.3 Event*

### *2.1.2 Sentinel*

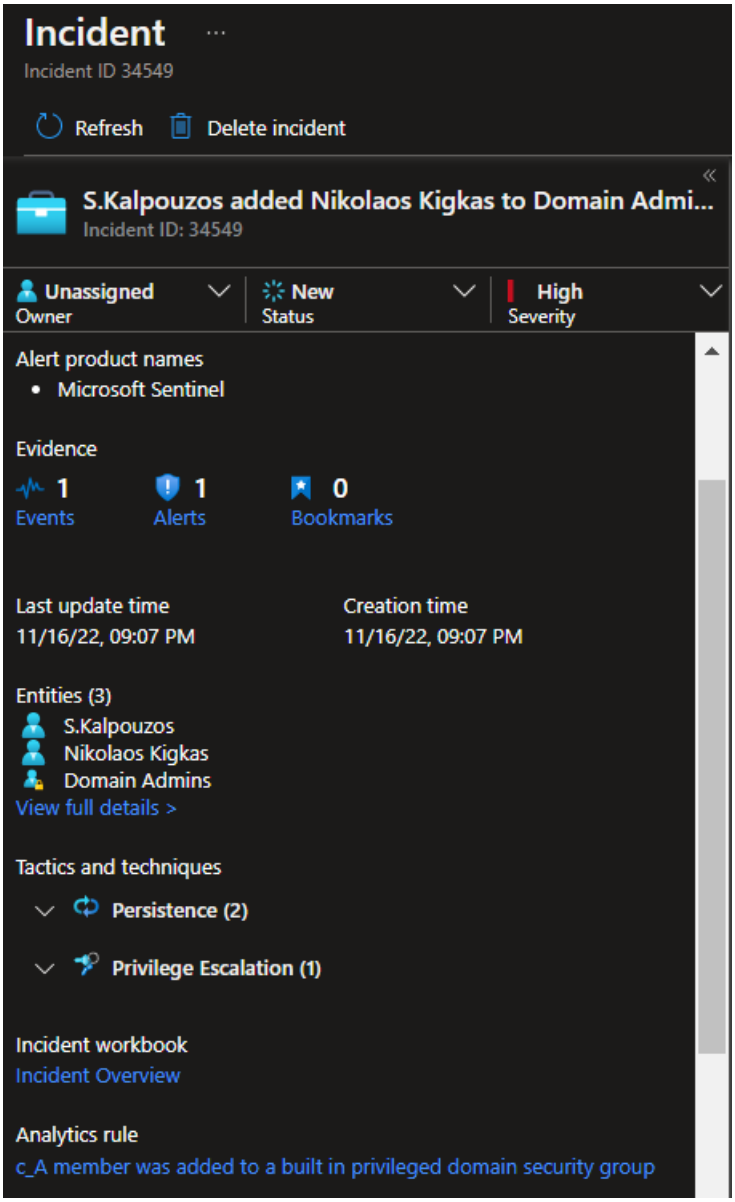
#### *2.1.2.1 Rule*



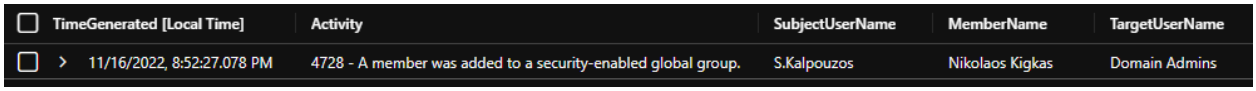

*Rule Query*

```
SecurityEvent
| where EventID == 4728
|  where TargetAccount in ('INTRANET\\Administrators', 'INTRANET\\Domain
Admins', 'INTRANET\\Enterprise Admins')
| extend MemberName = extract("(CN|cn)=([^,]*)",2,EventData)
| summarize by TimeGenerated, SubjectUserName, MemberName, TargetUserName
| sort by TimeGenerated desc
```

### *2.1.2.2 Incident*




### *2.1.2.3 Events*



| TimeGenerated [Local Time] | Activity | SubjectUserName | MemberName | TargetUserName |
|---|---|---|---|---|
| 11/16/2022, 8:52:27.078 PM | 4728 - A member was added to a security-enabled global group. | S.Kalpouzos | Nikolaos Kigkas | Domain Admins |

## *2.2 DOS Attack detected on published services*

**Objective** : Η αποστολή πολλών αιτημάτων σε πολύ σύντομο χρονικό διάστημα προς μία δημοσιευμένη στο Internet υπηρεσία, είναι από τις απλούστερες ενέργειες επίτευξης μίας επίθεσης τύπου άρνησης υπηρεσίας (Denial of Service). Ο σκοπός της επίθεσης είναι η κατανάλωση υπολογιστικών ή δικτυακών πόρων είτε της ίδιας της υπηρεσίας, είτε του τείχους προστασίας που βρίσκεται μπροστά από την υπηρεσία, με σκοπό να μην μπορούν να εξυπηρετηθούν θεμιτά αιτήματα. Η αμεσότητα πρόσβασης σε μία δημοσιευμένη στο Internet υπηρεσία, καθιστά την επίθεση αυτή μία από τις συχνότερες επιθέσεις και τις περισσότερες φορές πραγματοποιείται μόνο και μόνο για την επίτευξη της άρνησης. Ωστόσο δεν είναι λίγες οι φορές που έχει πραγματοποιηθεί στα πλαίσια μίας πιο εξειδικευμένης επίθεσης, προκειμένου οι οργανισμοί να επιστήσουν την προσοχή τους σε αυτή, ενώ οι επιτιθέμενοι παράλληλα πραγματοποιούν άλλες κακόβουλες ενέργειες.

Για να εντοπίσουμε μία τέτοια επίθεση, μία καλή ένδειξη αποτελεί η παρακολούθηση του ρυθμού αιτημάτων που καταφτάνουν στον web server, τα οποία φυσικά έχουν επιτραπεί από το αντίστοιχο firewall που τον προστατεύει. Τα αιτήματα είθισται να τα μετράμε ανά λεπτό, συνεπώς η μετρική μας θα είναι τα requests per minute (rpm). Το ποιό θα είναι το όριο που θα τεθεί στην μετρική, το οποίο θα υποδεικνύει μία DoS επίθεση, το καθορίζουν πρωτίστως η αντοχή των πόρων του εξυπηρετητή, καθώς και ο συνηθισμένος ρυθμός επισκεψιμότητας. Προκειμένου να αναπαράξουμε την συγκεκριμένη περίπτωση χρήσης χωρίς παράλληλα να υλοποιήσουμε μέχρι τέλους την επίθεση, θέσαμε το threshold της μετρικής στο σχετικά χαμηλό όριο των 500 rpm.

**MITRE Tactic**: Impact

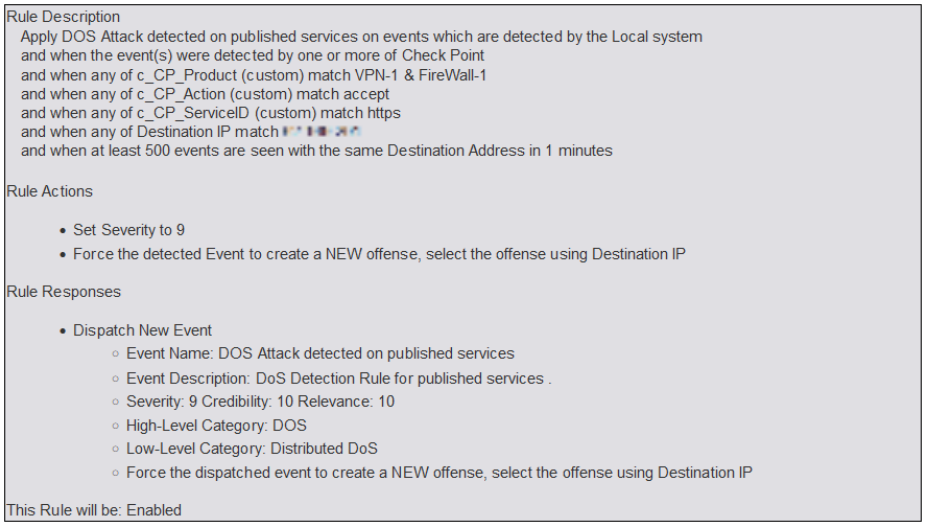
**MITRE Technique**: T1498 – Network Denial of Service

**LogSources**: CheckPoint Firewall

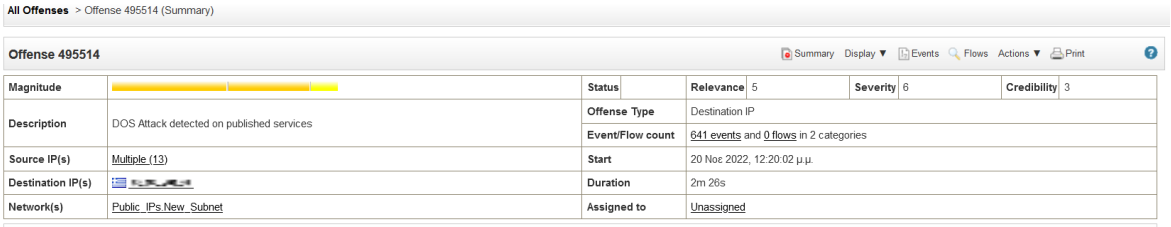
**Severity/Criticality**: High (9)

### *2.2.1 QRadar*

#### *2.2.1.1 Rule*



### *2.2.1.2 Offense*



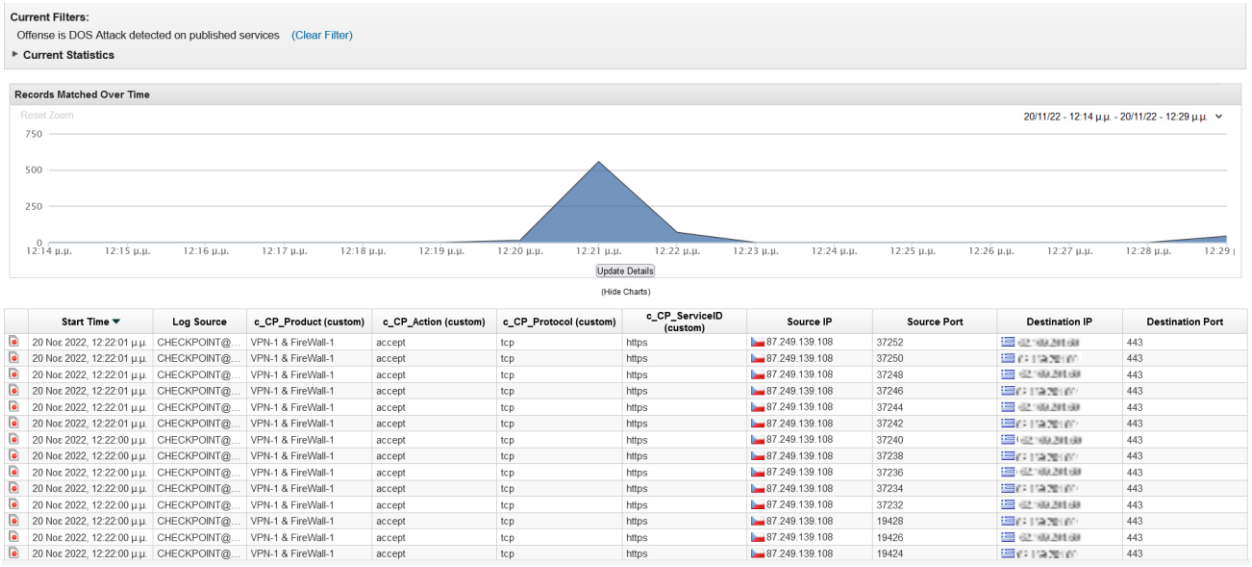
All Offenses > Offense 495514 (Summary)

**Offense 495514**

Summary | Display ▼ | Events | Flows | Actions ▼ | Print

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Magnitude** | | **Status** | | **Relevance** | 5 | **Severity** | 6 | **Credibility** | 3 |
| **Description** | DOS Attack detected on published services | **Offense Type** | Destination IP | | | | |
| | | **Event/Flow count** | 641 events and 0 flows in 2 categories | | | | |
| **Source IP(s)** | Multiple (13) | **Start** | 20 Νοε 2022, 12:20:02 μ.μ. | | | | |
| **Destination IP(s)** | [redacted] | **Duration** | 2m 26s | | | | |
| **Network(s)** | Public_IPs,New_Subnet | **Assigned to** | Unassigned | | | | |

### *2.2.1.3 Events*



**Current Filters:**

Offense is DOS Attack detected on published services (Clear Filter)

▸ **Current Statistics**

**Records Matched Over Time**

Reset Zoom 20/11/22 - 12:14 μ.μ. - 20/11/22 - 12:29 μ.μ.

750
500
250
0

12:14 μ.μ. 12:15 μ.μ. 12:16 μ.μ. 12:17 μ.μ. 12:18 μ.μ. 12:19 μ.μ. 12:20 μ.μ. 12:21 μ.μ. 12:22 μ.μ. 12:23 μ.μ. 12:24 μ.μ. 12:25 μ.μ. 12:26 μ.μ. 12:27 μ.μ. 12:28 μ.μ. 12:29 μ.μ.

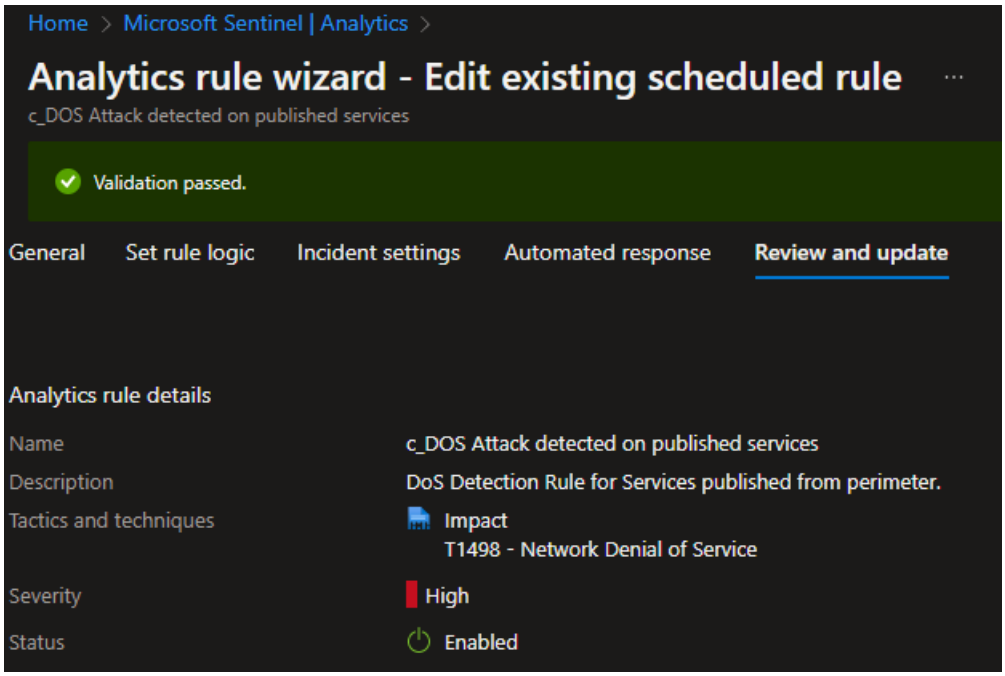
Update Details

(Hide Charts)

| Start Time | Log Source | c_CP_Product (custom) | c_CP_Action (custom) | c_CP_Protocol (custom) | c_CP_ServiceID (custom) | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|---|---|---|---|---|
| 20 Νοε 2022, 12:22:01 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37252 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:01 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37250 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:01 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37248 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:01 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37246 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:01 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37244 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:01 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37242 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37240 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37238 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37236 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37234 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 37232 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 19428 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 19426 | [redacted] | 443 |
| 20 Νοε 2022, 12:22:00 μ.μ. | CHECKPOINT@... | VPN-1 & FireWall-1 | accept | tcp | https | 87.249.139.108 | 19424 | [redacted] | 443 |

### *2.2.2 Sentinel*

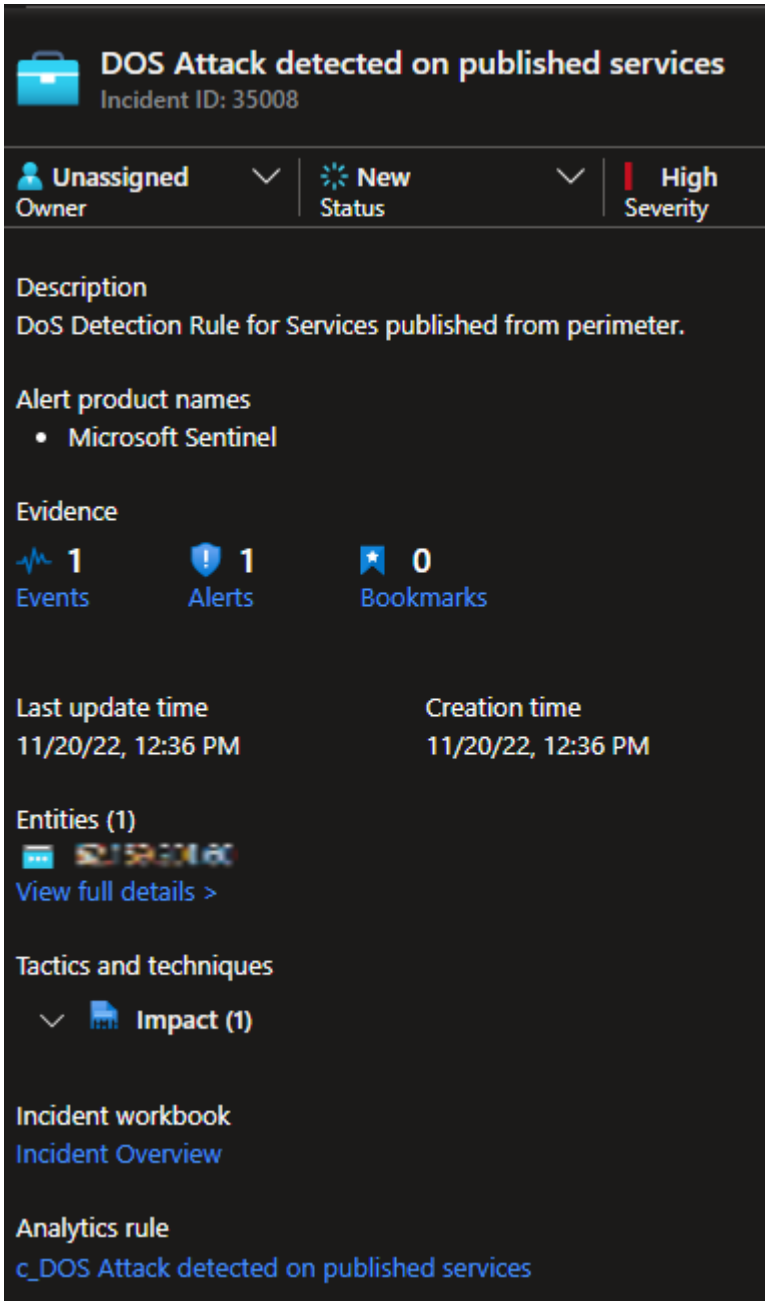
#### *2.2.2.1 Rule*




*Rule Query*

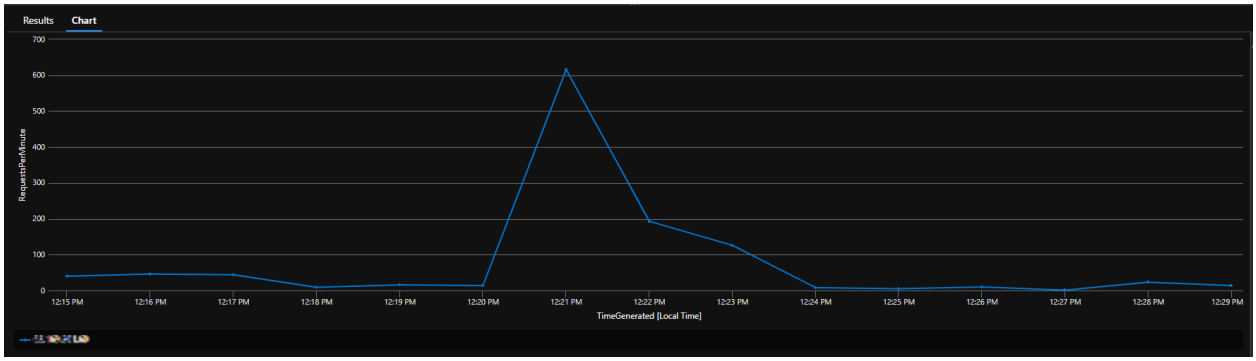
```
CommonSecurityLog
| where DeviceVendor == "Check Point"
| where DeviceProduct == "VPN-1 & FireWall-1"
| where DeviceAction == "Accept"
| where Activity == "https"
| where DestinationIP startswith "XXX.XXX.XXX."
| summarize RequestsPerMinute = count() by bin(TimeGenerated, 1min), DestinationIP
| where RequestsPerMinute >= 500
| sort by TimeGenerated desc
```

#### *2.2.2.2 Incident*



#### *2.2.2.3 Events*

| TimeGenerated [Local Time] | DestinationIP | RequestsPerMinute |
|---|---|---|
| 11/20/2022, 12:21:00.000 PM | [redacted] | 615 |




### *2.2.3 Επίθεση*

Προκειμένου να ενεργοποιήσουμε τους κανόνες, πραγματοποιήσαμε προσομοίωση μικρού μεγέθους DoS επίθεσης με χρήση σχετικού module του Metasploit.

```
msf6 auxiliary(dos/http/slowloris) > options

Module options (auxiliary/dos/http/slowloris):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   delay             15               yes       The delay between sending keep-alive headers
   rand_user_agent   true             yes       Randomizes user-agent with each request
   rhost             [redacted]       yes       The target address
   rport             443              yes       The target port
   sockets           300              yes       The number of sockets to use in the attack
   ssl               false            yes       Negotiate SSL/TLS for outgoing connections

msf6 auxiliary(dos/http/slowloris) > run

[*] Starting server...
[*] Attacking [redacted] with 300 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 300
[*] Sending keep-alive headers... Socket count: 300
[*] Sending keep-alive headers... Socket count: 300
[*] Sending keep-alive headers... Socket count: 300
[*] Sending keep-alive headers... Socket count: 300
[*] Sending keep-alive headers... Socket count: 300
^C[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(dos/http/slowloris) >
```

## *2.3 Detected audit policy disable*

**Objective**: Η απενεργοποίηση, η τροποποίηση ή ο αποκλεισμός security controls είναι μία από τις πιο συνηθισμένες συμπεριφορές των επιτιθέμενων. Το MITRE ATT&CK framework κατηγοριοποιεί το συγκεκριμένο τύπο κακόβουλων ενεργειών στην τεχνική " T1562 Impair Defenses". Κατά την τεχνική αυτή οι επιτιθέμενοι τροποποιούν κακόβουλα στοιχεία ενός περιβάλλοντος θύματος προκειμένου να εμποδίσουν ή να απενεργοποιήσουν αμυντικούς μηχανισμούς. Αυτό δεν περιλαμβάνει μόνο την παρεμπόδιση της προληπτικής άμυνας, όπως τα τείχη προστασίας και τα προγράμματα προστασίας από ιούς, αλλά και τις δυνατότητες ανίχνευσης που μπορούν να χρησιμοποιούν οι υπερασπιστές για να ελέγχουν τη δραστηριότητα και να εντοπίζουν κακόβουλη συμπεριφορά.

Οι επιτιθέμενοι θα μπορούσαν επίσης να στοχεύσουν μηχανισμούς συγκέντρωσης και ανάλυσης συμβάντων ή να διαταράξουν με άλλο τρόπο αυτές τις διαδικασίες αλλάζοντας στοιχεία του συστήματος.

Στο συγκεκριμένο σημείο θα ασχοληθούμε με την sub-technique T1562.002 του MITRE ATT&CK framework, που είναι η απενεργοποίηση του logging των Windows. Εξ' ορισμού η υπηρεσία καταγραφής συμβάντων (Event Logging) ξεκινάει με την έναρξη λειτουργίας του συστήματος, ενώ το ποια συμβάντα συστήματος καταγράφονται σε αυτή καθορίζεται από την audit policy που διατηρείται στην local security policy.

Οι τελευταίες εκδόσεις Windows περιλαμβάνουν ένα command-line εργαλείο γραμμής εντολών το AuditPol.exe που επιτρέπει τη διαχείριση και τον έλεγχο των audit policy υποκατηγοριών. Οι κακόβουλοι μπορούν να χρησιμοποιήσουν το σύνολο εντολών του AuditPol.exe, προκειμένου να απενεργοποιήσουν κάποιον έλεγχο ή να διαγράψουν μια συγκεκριμένη πολιτική ελέγχου. Για παράδειγμα με την εντολή auditpol /set/category:"Account Logon"/success:disable /failure:disable, καταργείται το auditing της κατηγορίας Account Logon.

Σκοπός κατά συνέπεια του συγκεκριμένου use case είναι ο εντοπισμός της ενέργειας αλλαγής μίας audit πολιτικής και πιο συγκεκριμένα η ενέργεια της απενεργοποίησή της. Ο εντοπισμός επιτυγχάνεται τόσο με το άμεσο γεγονός της αλλαγής (Event ID 4719 [6]) με συγκεκριμένους κωδικούς ενεργειών (%%8448 = Success removed και %%8450 = Failure removed), όσο και με το γεγονός της εκτέλεσης του προγράμματος auditpol με συγκεκριμένες παραμέτρους (set και disable) στην εντολή (Event ID 4688 [7]).

**MITRE Tactic**: Impair Defenses

**MITRE Technique**: T1562.002 – Disable Windows Event Logging

**LogSources**: Microsoft Windows Security Events

**Severity/Criticality**: Medium (7)

### *2.3.1 QRadar*

#### *2.3.1.1 Rules*

##### *2.3.1.1.1 Detected Audit Policy disable*

Rule Description
Apply Detected Audit Policy disable on events which are detected by the Local system
and when the event(s) were detected by one or more of Microsoft Windows Security Event Log
and when any of Log Source match winserver
and when any of EventID (custom) match 4719
and when any of c_MSWEL_Changes (custom) match %%84(48|50)

Rule Actions

- Set Severity to 7
- Force the detected Event to create a NEW offense, select the offense using Log Source

Rule Responses

- Dispatch New Event
  - Event Name: Detected Audit Policy disable
  - Event Description: Detect audit policy change where action is Success remove (%%8448) or Failure remove (%%8450).
  - Severity: 7 Credibility: 0 Relevance: 0
  - High-Level Category: Audit
  - Low-Level Category: Audit Logs Clearance Attempt
  - Force the dispatched event to create a NEW offense, select the offense using Log Source

This Rule will be: Enabled

##### *2.3.1.1.2 Detected Audit Policy disable using Auditpol*

Rule Description
Apply Detected Audit Policy disable using Auditpol on events which are detected by the Local system
and when the event(s) were detected by one or more of Microsoft Windows Security Event Log
and when any of Log Source match winserver
and when any of EventID (custom) match 4688
and when any of ProcessName (custom) match auditpol.exe
and when any of ProcessCmd (custom) match (?i)auditpol.*\set.*disable

Rule Actions

- Set Severity to 7
- Force the detected Event to create a NEW offense, select the offense using Log Source

Rule Responses

- Dispatch New Event
  - Event Name: Detected Audit Policy disable using Auditpol
  - Event Description: Detect use of audipol.exe with set and disable parameters.
  - Severity: 7 Credibility: 0 Relevance: 0
  - High-Level Category: Audit
  - Low-Level Category: Audit Logs Clearance Attempt
  - Force the dispatched event to create a NEW offense, select the offense using Log Source

This Rule will be: Enabled

### *2.3.1.2 Offense*

**Offense 496460** Summary Display ▼ Events Flows Actions ▼ Print

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Magnitude** | | **Status** | | **Relevance** 6 | **Severity** 7 | **Credibility** 3 | |
| **Description** | Detected Audit Policy disable using Auditpol | **Offense Type** | Log Source | | | | |
| | | **Event/Flow count** | 2 events and 0 flows in 1 categories | | | | |
| **Source IP(s)** | [redacted] | **Start** | 24 Νοε 2022, 9:15:02 μ.μ. | | | | |
| **Destination IP(s)** | [redacted] | **Duration** | 9s | | | | |
| **Network(s)** | Server_Network [redacted] Server_Network | **Assigned to** | Unassigned | | | | |

**List of Rules Contributing to Offense**

| | Rule Name | Events/Flows | First Event/Flow | Last Event/Flow |
|---|---|---|---|---|
| | Detected Audit Policy disable | 1 | 4m 40s | 4m 40s |
| | Detected Audit Policy disable using Auditpol | 1 | 4m 30s | 4m 30s |

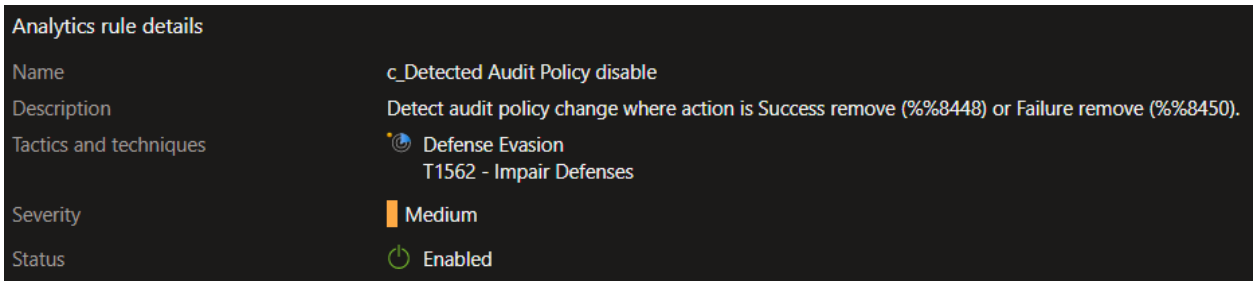
### *2.3.1.3 Events*

| Start Time | Log Source | EventID (custom) | Event Name | Username | c_MSWEL_CategoryId (custom) | c_MSWEL_SubcategoryGUID (custom) | c_MSWEL_Changes (custom) | ProcessName (custom) | ProcessCmd (custom) |
|---|---|---|---|---|---|---|---|---|---|
| 24 Νοε 2022, 9:15:02 μ.μ. | winserver | 4688 | Success Audit: A new process has been cre... | [redacted] | N/A | N/A | N/A | auditpol.exe | "C:\Windows\system32\auditpol.exe" /set "/subcategory:Process Creation" /success:disable /failure:disable |
| 24 Νοε 2022, 9:15:02 μ.μ. | winserver | 4719 | Success Audit: System audit policy was chan... | [redacted] | %%8276 | cce922b-69ae-11d9-bed3-505054503... | %%8448 | N/A | N/A |

### *2.3.2 Sentinel*

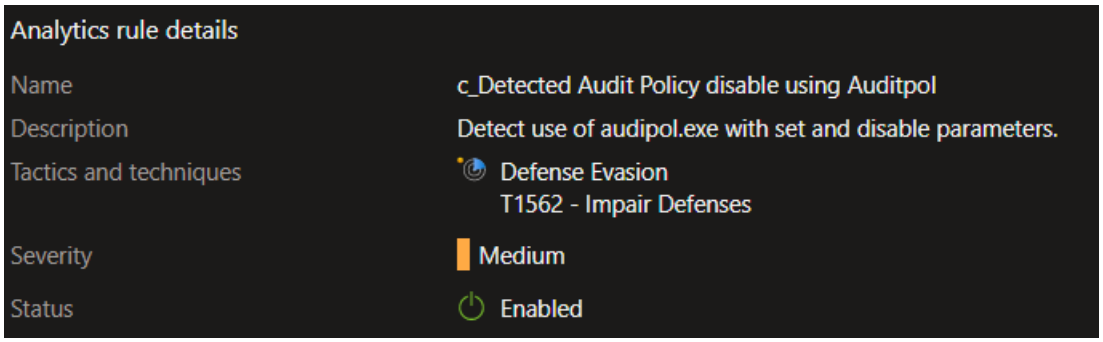
#### *2.3.2.1 Rules*

##### *2.3.2.1.1 Detected Audit Policy disable*



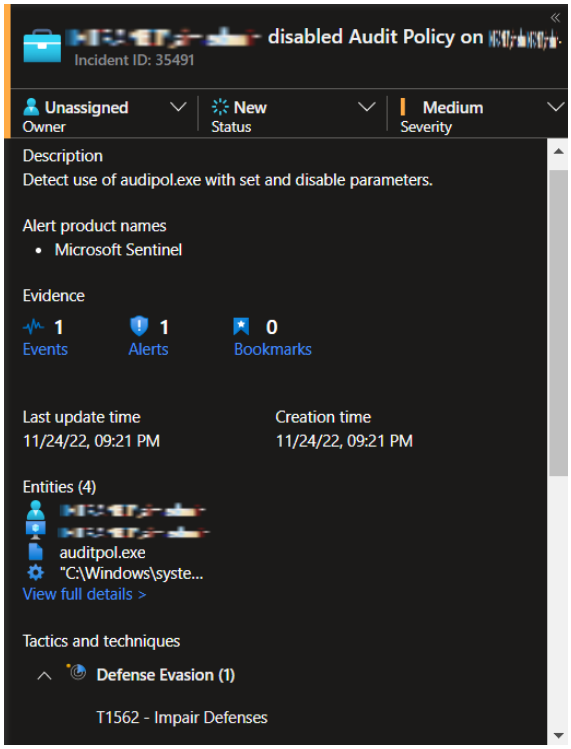

```
let Changes = datatable(ChangeCode:string, ChangeName:string) [
"%%8448","Success removed",
"%%8449","Success added",
…
];
let CategoryNames = datatable(CategoryName:string, CategoryCode:string) [
"System","%%8272",
"Logon/Logoff","%%8273",
…
];
let SubcategoryNames = datatable(SubcategoryName:string, SubcatGuid:string) [
"Security State Change","0CCE9210-69AE-11D9-BED3-505054503030",
"Security System Extension","0CCE9211-69AE-11D9-BED3-505054503030",
…
];
SecurityEvent
| where Computer startswith "winserver"
| where EventID == 4719 and AuditPolicyChanges matches regex "%%84(48|50)"
| extend SubcategoryGuidUpper = toupper(SubcategoryGuid)
| join kind = leftouter (SubcategoryNames) on $left.SubcategoryGuidUpper == $right.SubcatGuid
| join kind = leftouter (Changes) on $left.AuditPolicyChanges == $right.ChangeCode
| join kind = leftouter (CategoryNames) on $left.CategoryId == $right.CategoryCode
|   project   TimeGenerated,   Activity,   Computer,   Account,   CategoryId,   CategoryName,
SubcategoryGuidUpper, SubcategoryName, AuditPolicyChanges, ChangeName
| sort by TimeGenerated desc
```

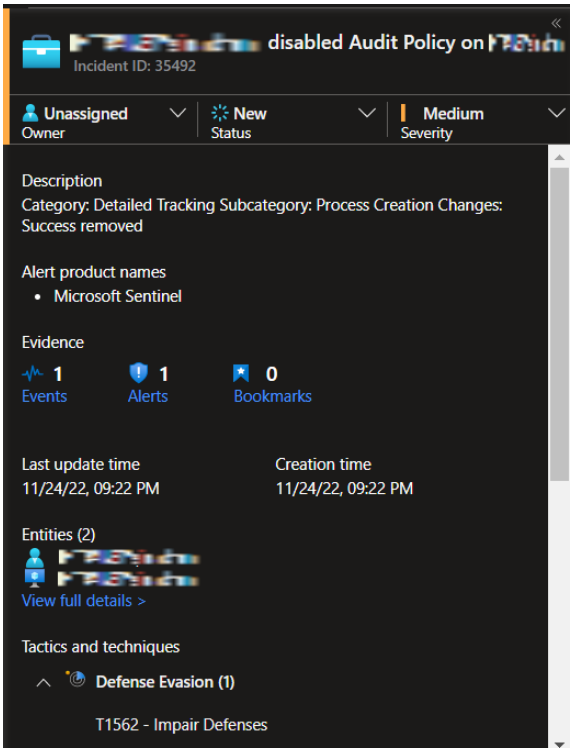
### *2.3.2.1.2 Detected Audit Policy disable using Auditpol*




```
SecurityEvent
| where Computer startswith "winserver"
| where EventID == 4688
    and Process == "auditpol.exe"
    and CommandLine matches regex "(?i)auditpol.*\\/set.*disable"
| project TimeGenerated, Activity, Computer, Account, Process, CommandLine
| sort by TimeGenerated desc
```

### *2.3.2.2 Incidents*



#### *2.3.2.3 Events*

| TimeGenerated [Local Time] | Activity | Computer | Account | Process | CommandLine |
|---|---|---|---|---|---|
| 11/24/2022, 9:14:59.040 PM | 4688 - A new process has been created. | [redacted] | [redacted] | auditpol.exe | "C:\Windows\system32\auditpol.exe" /set "/subcategory:Process Creation" /success:disable /failure:disable |

| | |
|---|---|
| TimeGenerated [UTC] | 2022-11-24T19:14:59.0650888Z |
| Activity | 4719 - System audit policy was changed. |
| Computer | [redacted] |
| Account | [redacted] |
| CategoryId | %%8276 |
| CategoryName | Detailed Tracking |
| SubcategoryGuidUpper | 0CCE922B-69AE-11D9-BED3-505054503030 |
| SubcategoryName | Process Creation |
| AuditPolicyChanges | %%8448 |
| ChangeName | Success removed |

### *2.3.3 Επίθεση*

```
PS C:\Windows\system32> auditpol /get /subcategory:"Process Creation"
System audit policy
Category/Subcategory                      Setting
Detailed Tracking
  Process Creation                        Success
PS C:\Windows\system32> auditpol /set /subcategory:"Process Creation" /success:disable /failure:disable
The command was successfully executed.
PS C:\Windows\system32> auditpol /get /subcategory:"Process Creation"
System audit policy
Category/Subcategory                      Setting
Detailed Tracking
  Process Creation                        No Auditing
PS C:\Windows\system32> _
```

## *2.4 Possible SSH Brute force attack detected*

**Objective**: Μια brute force επίθεση αποτελεί μια πολύ δημοφιλή «cracking» μέθοδο. Η συγκεκριμένου τύπου επίθεση αντιπροσωπεύει το 5% των επιβεβαιωμένων security breaches. Η επίθεση αυτή περιλαμβάνει το λεγόμενο «guessing» του ονόματος ενός χρήστη και του κωδικού πρόσβασής του. Είναι μια σχετικά απλή μέθοδος επίθεσης με αρκετά υψηλά ποσοστά επιτυχίας και κίνητρο την κλοπή πληροφοριών, τη μόλυνση sites με malware ή και τη διακοπή ενός service.

Ο πλέον συνηθισμένος τρόπος επίθεσης brute force είναι μέσω συγκεκριμένων scripts ή εργαλείων μέσω των οποίων δοκιμάζεται ένας μεγάλος αριθμός passwords μέχρι να βρεθεί αυτό που θα επιτρέψει στον επιτιθέμενο να αποκτήσει πρόσβαση στο σύστημα και κατ' επέκταση στην υπηρεσία.

Τα δημοφιλέστερα services τα οποία παρέχουν αυθεντικοποίηση και στοχοποιούνται από την εν λόγω επίθεση είναι:

- HTTP/HTTP Management Services (port 80/TCP και 443/TCP)
- SSH (port 22/TCP)
- RDP / Terminal Services (3389/TCP)
- FTP (21/TCP)
- Telnet (port 23/TCP)
- LDAP (port 389/TCP)
- MSSQL(port 3306/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)

Στο συγκεκριμένο use case επιλέξαμε να πραγματοποιήσουμε brute force επίθεση σε υπηρεσία SSH, την οποία εξυπηρετούσε ένας Ubuntu 20.04.5 server (θύμα), με τη βοήθεια σχετικού auxiliary scanner exploit script του Metasploit framework ενός Kali Linux μηχανήματος (επιτιθέμενος). Έχοντας γνώση πως ο χρήστης nksk είναι υπαρκτός, παραμετροποιήσαμε ανάλογα το exploit μαζί με το γνωστό built-in λεξικό του Kali "rockyou.txt" προκειμένου να στοχεύσουμε τον συγκεκριμένο λογαριασμό. Ωστόσο, η λογική του κανόνα δεν εξαρτάται από συγκεκριμένο χρήστη, αφού καταμετράμε ανά λεπτό τα γεγονότα αποτυχημένων προσπαθειών σύνδεσης SSH που παρέχονται από το syslog facility Auth ανεξαρτήτου χρήστη. Τελικώς, η ικανοποίηση του κανόνα και κατ΄ επέκταση η δημιουργία περιστατικού επέρχεται εφόσον σε διάρκεια ενός λεπτού παρατηρηθούν 5 από τα προαναφερόμενα γεγονότα.

**MITRE Tactic**: Credential Access

**MITRE Technique**: T1110.001 - Brute Force: Password Guessing

**LogSources**: Syslog (Auth Facility)

**Severity/Criticality**: Medium (6)

### *2.4.1 QRadar*

#### *2.4.1.1 Rule*

Rule Description

Apply Possible Brute force attack detected on events which are detected by the Local system
and when the event(s) were detected by one or more of ubuserver
and when the event QID is one of the following (44250069) User failed to login to SSH, incorrect password
and when at least 5 events are seen with the same QID in 1 minutes

Rule Actions

- Set Severity to 6
- Force the detected Event to create a NEW offense, select the offense using Log Source

Rule Responses

- Dispatch New Event
  - Event Name: Possible Brute force attack detected
  - Event Description: Detect multiple authentication attempts against a specific host in short period of time.
  - Severity: 6 Credibility: 0 Relevance: 0
  - High-Level Category: Access
  - Low-Level Category: Unauthorized Access Attempt
  - Force the dispatched event to create a NEW offense, select the offense using Log Source

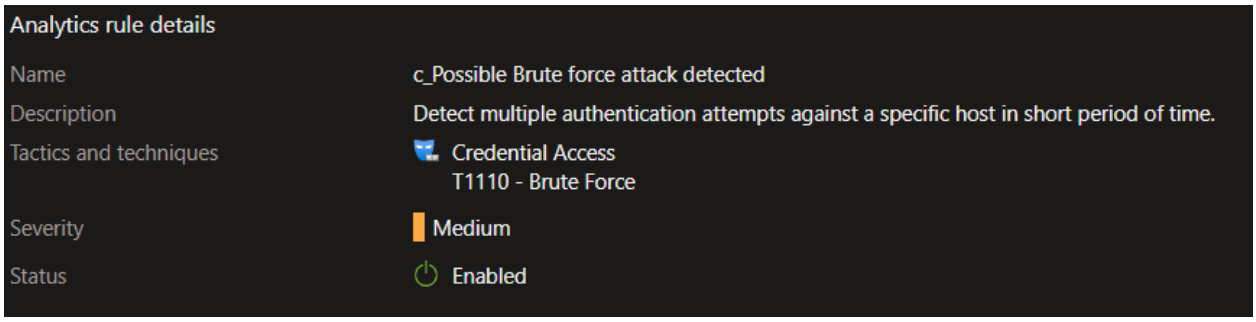
This Rule will be: Enabled

#### *2.4.1.2 Offense*


#### *2.4.1.3 Events*

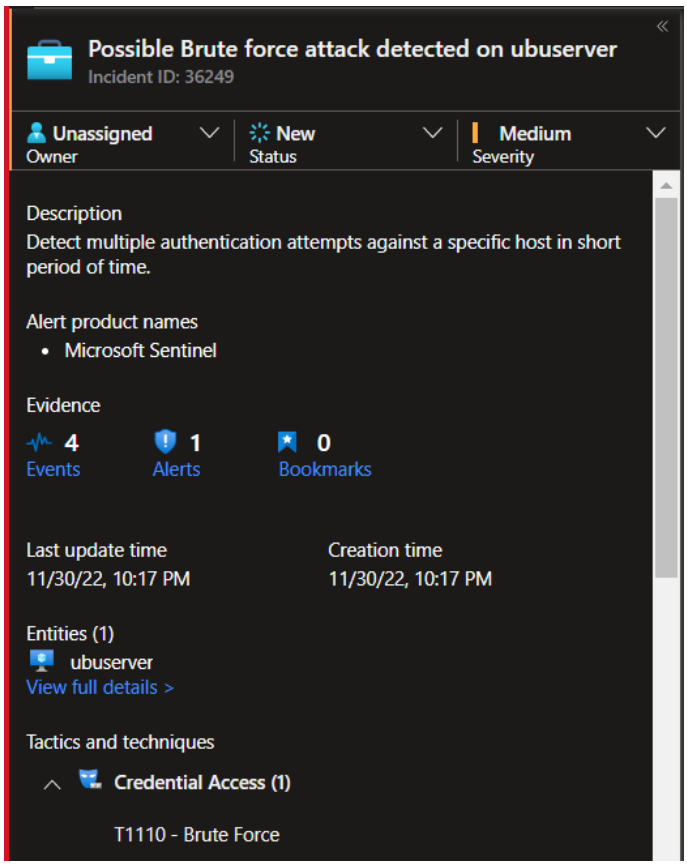
### *2.4.2 Sentinel*

#### *2.4.2.1 Rule*




```
Syslog
| where Computer == "ubuserver"
| where Facility == "auth"
| where ProcessName == "sshd"
| where SyslogMessage startswith "Failed password for"
| extend UserName = extract("for (invalid user |)(\\S*)",2,SyslogMessage)
| extend SourceIP = extract("from (\\S*)",1,SyslogMessage)
| extend SourcePort = extract("port (\\S*)",1,SyslogMessage)
| project TimeGenerated, HostName, SyslogMessage, UserName, SourceIP, SourcePort
| summarize AttemptsPerMinute = count() by bin(TimeGenerated, 1min), HostName
| where AttemptsPerMinute >= 5
| sort by TimeGenerated desc
```

#### *2.4.2.2 Incident*



### *2.4.2.3 Events*

| TimeGenerated [Local Time] | HostName | UserName | AttemptsPerMinute |
|---|---|---|---|
| 11/30/2022, 10:11:00.000 PM | ubuserver | nksk | 5 |
| 11/30/2022, 10:10:00.000 PM | ubuserver | nksk | 17 |
| 11/30/2022, 10:09:00.000 PM | ubuserver | nksk | 19 |
| 11/30/2022, 10:08:00.000 PM | ubuserver | nksk | 5 |

## *2.4.3 Επίθεση*

```
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                  Required  Description
   ----              ---------------                  --------  -----------
   BLANK_PASSWORDS   false                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                           no        A specific password to authenticate with
   PASS_FILE         /usr/share/wordlists/rockyou.txt no        File containing passwords, one per line
   RHOSTS                                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22                               yes       The target port
   STOP_ON_SUCCESS   false                            yes       Stop guessing when a credential works for a host
   THREADS           1                                yes       The number of concurrent threads (max one per host)
   USERNAME          nksk                             no        A specific username to authenticate as
   USERPASS_FILE                                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                            no        Try the username as the password for all users
   USER_FILE                                          no        File containing usernames, one per line
   VERBOSE           false                            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > run

[*]  :22 - Starting bruteforce
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

## *2.5 Detected use of Remote Administration tool*

**Objective**: Ένας επιτιθέμενος μπορεί να χρησιμοποιεί λογισμικά όπως Team Viewer, AnyDesk, Go2Assist, LogMein, AmmyAdmin, με τα οποία επιτυγχάνεται απομακρυσμένη σύνδεση και διαχείριση ενός συστήματος – μέλους του υπό επίθεση δικτύου.

Τέτοιου είδους λογισμικά, τα οποία συνήθως κατηγοριοποιούνται ως Remote Access ή Remote Administration (RA), θεωρούνται legitimate ως ένας εναλλακτικός και οικονομικός τρόπος δημιουργίας ενός remote desktop session και αφήνονται ελεύθερα σε επίπεδο Application Control από μηχανισμούς ασφάλειας ενός οργανισμού. Σε άλλες περιπτώσεις αποτελούν component ενός malware με στόχο τη δημιουργία μιας reverse σύνδεσης ή μιας επανασύνδεσης του επιτιθέμενου με το σύστημα- στόχο, στα πλαίσια διατήρησης της πρόσβασης (persistence).

Τον τελευταίο καιρό έχει παρατηρηθεί η ευρεία χρήση τέτοιου είδους λογισμικών στα πλαίσια επιθέσεων τύπου κοινωνικής μηχανικής και ιδιαιτέρως Voice Phishing (Vishing) attacks, κατά τις οποίες το θύμα με το πρόσχημα της τεχνικής υποστήριξης, πείθεται από τον επιτιθέμενο να εγκαταστήσει ένα από τα προαναφερόμενα λογισμικά επιτρέποντας με αυτόν τον τρόπο την απομακρυσμένη διαχείριση του υπολογιστή του. Με την απόκτηση της συγκεκριμένης μη εξουσιοδοτημένης πρόσβασης, η διεπαφή επίθεσης (Attack Surface) για τον επιτιθέμενο έχει διευρυνθεί σε μεγάλο βαθμό αφού πλέον είναι σε θέση να διεξάγει, ανάλογα με το κίνητρο-στόχο, ποικίλες επιθέσεις όπως να μολύνει το δίκτυο με κακόβουλο λογισμικό, να διεξάγει κατασκοπεία, δολιοφθορά, εξαγωγή εταιρικών και προσωπικών πληροφοριών.

Ο εντοπισμός αυτής της τεχνικής μπορεί να επιτευχθεί πρωτίστως χρησιμοποιώντας την κατηγοριοποίηση ενός Application Control μηχανισμού όπως Firewall ή EDR. Στην περίπτωσή μας, θα χρησιμοποιήσουμε τα γεγονότα συνδέσεων που προέρχονται από applications και περνούν από το Firewall περιμέτρου. Πιο συγκεκριμένα θα φιλτράρουμε τα γεγονότα αυτά με την τιμή “Remote Administration” για το σχετικό πεδίο στο οποίο ο μηχανισμός μας αναφέρει την κατηγορία του application (AppCategory).

Να τονιστεί σε αυτό το σημείο ότι ο έγκυρος εντοπισμός μας βασίζεται στην εγκυρότητα της γνωσιακής βάσης και της κατηγοριοποίησης του κατασκευαστή του εκάστοτε εργαλείου. Θα πρέπει να λάβουμε υπόψη μας πως κάποιο ήδη υπάρχων application με μικρή φήμη ή κάποιο εργαλείο που πρόκειται να υπάρξει στο μέλλον ενδέχεται να μην κατηγοριοποιηθεί σωστά ή να αργήσει σημαντικά η κατηγοριοποίησή του. Το παραπάνω γεγονός δεν θα είχε ως αποτέλεσμα μόνο τον μη εντοπισμό, αλλά σε περίπτωση που υπήρχε σχετική πολιτική αποκλεισμού στον εκάστοτε μηχανισμό, η σύνδεση θα ήταν επιτυχής.

Λόγω του παραπάνω, κρίνεται απαραίτητος ένας παράλληλος εντοπισμός για την ίδια περίπτωση χρήσης. Ένα παράδειγμα μπορεί να αποτελέσει η χρήση ενός inventory ή μίας λίστας από ονόματα σχετικών RA εκτελέσιμων και η αναζήτηση αυτών σε γεγονότα εκκίνησης διεργασιών (EID 4688 [7]).

**MITRE Tactic**: Command and Control

**MITRE Technique**: T1219 - Remote Access Software

**LogSources**: CheckPoint Firewall

**Severity/Criticality**: Medium (7)

### *2.5.1 QRadar*

#### *2.5.1.1 Rule*

Rule Description

Apply Detected use of Remote Administration tool on events which are detected by the Local system
and when the event(s) were detected by one or more of Check Point
and when any of c_CP_Product (custom) match Application Control
and when any of c_CP_AppCategory (custom) match Remote Administration

Rule Actions

- Set Severity to 7
- Force the detected Event to create a NEW offense, select the offense using c_CP_SrcMachineName (custom)

Rule Responses

- Dispatch New Event
  - Event Name: Detected use of Remote Administration tool
  - Event Description: Detect the use of Remote Administration tool from CheckPoint Application Control blade.
  - Severity: 7 Credibility: 0 Relevance: 0
  - High-Level Category: Control System
  - Low-Level Category: Remote Connection Event
  - Force the dispatched event to create a NEW offense, select the offense using c_CP_SrcMachineName (custom)

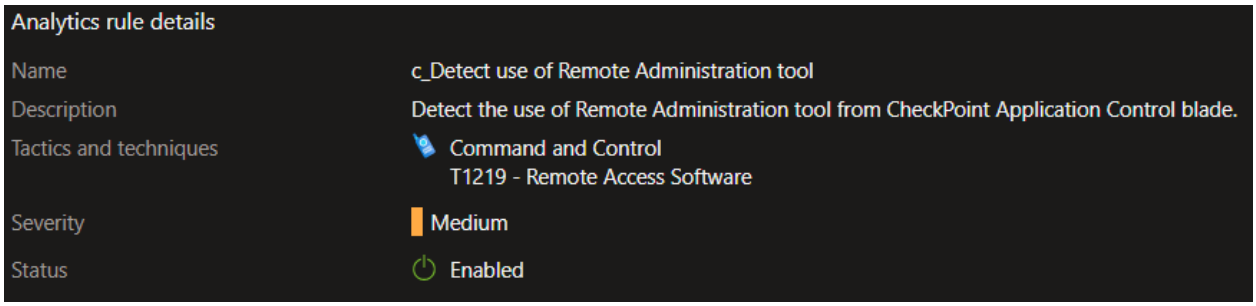
This Rule will be: Disabled

#### *2.5.1.2 Offense*


#### *2.5.1.3 Events*

### *2.5.2 Sentinel*

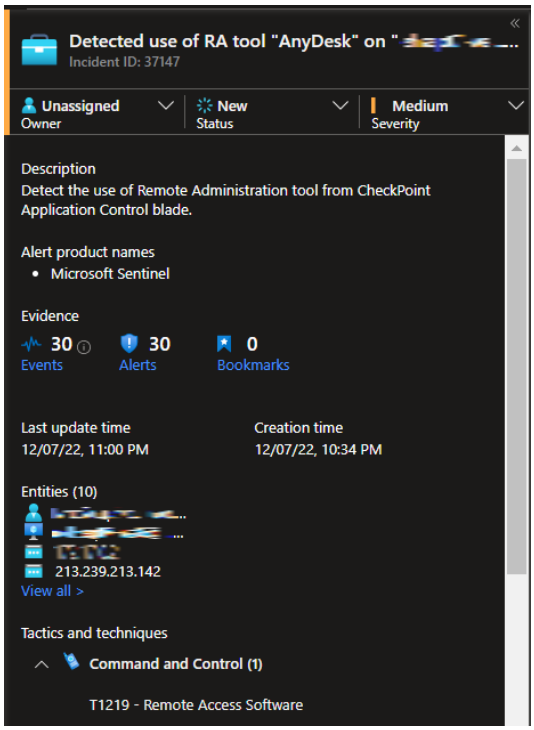
#### *2.5.2.1 Rule*




Rule Query:

```
CommonSecurityLog
| where DeviceVendor == "Check Point"
| where DeviceProduct == "Application Control"
| where AppCategory_CP_CF == "Remote Administration"
| project TimeGenerated, AppName, AppRisk, AppDesc_CP_CF, SourceUserName,
SourceHostName, SourceIP, DestinationIP, DestinationPort
| sort by TimeGenerated desc
```

#### *2.5.2.2 Incident*



### *2.5.2.3 Events*

| | |
|---|---|
| TimeGenerated [UTC] | 2022-12-07T20:34:34.985Z |
| AppName | AnyDesk |
| AppRisk | High |
| AppDesc_CP_CF | AnyDesk is a remote desktop application which allows users to control computers remotely over the internet. |
| SourceUserName | [redacted] |
| SourceHostName | [redacted] |
| SourceIP | [redacted] |
| DestinationIP | 195.181.174.174 |
| DestinationPort | 443 |

## *2.6 Detect process creation from removable media*

**Objective**: Είναι συχνή πρακτική των επιτιθέμενων να εγκαθιστούν κακόβουλο κώδικα σε εξωτερικές φυσικές συσκευές αποθήκευσης (USB), με σκοπό είτε την εξαγωγή δεδομένων είτε την μόλυνση των αγαθών του δικτύου. Σε ορισμένες περιπτώσεις, όπου ο επιτιθέμενος δεν έχει φυσική πρόσβαση στον σταθμό στόχο, μπορεί να εκμεταλλευτεί την περιέργεια ενός τελικού χρήστη για το τι μπορεί να περιέχει το USB drive που "τυχαία" βρήκε πεσμένο κάτω. Για έναν οργανισμό όπου δεν έχει καθολικά αποτρέψει την σύνδεση εξωτερικών μέσων αποθήκευσης ή που το έχει κάνει αλλά με κάποιος χρήστες ή σταθμούς σε εξαίρεση, κρίνονται απαραίτητοι οι δύο ακόλουθοι εντοπισμοί:

α) Παρακολούθηση για νέες αποδόσεις γραμμάτων σε μονάδες δίσκου ή σημεία προσάρτησης που εκχωρούνται σε μια συσκευή αποθήκευσης δεδομένων κατά τη σύνδεσή της.

β) Παρακολούθηση νέων εκτελούμενων διεργασιών έπειτα της σύνδεσης αφαιρούμενου μέσου.

Στα πλαίσια αυτής της περίπτωσης χρήσης έγινε προσπάθεια να συνδυαστούν οι δύο παραπάνω περιπτώσεις παρακολούθησης έτσι ώστε να δημιουργείται ένα περιστατικό όταν εκτελεστεί μία διεργασία της οποίας το αρχείο εκτέλεσης βρίσκεται σε οποιοδήποτε σημείο μέσα στην αφαιρούμενη μονάδα αποθήκευσης. Τα γεγονότα στα οποία βασίζεται αυτός ο εντοπισμός φυσικά προέρχονται από τον τελικό σταθμό του χρήστη και είναι τα Microsoft Windows Security Events 6416 [8] για την απόκτηση του drive letter που αποδόθηκε στο μέσο κατά τη σύνδεσή του και το 4688 [7] όπου με όρισμα το drive letter από το 6416 θα μας υποδείξει οποιαδήποτε δημιουργία διεργασίας της οποίας το αρχείο εκτέλεσης έχει πλήρη διαδρομή που ξεκινάει από το ορισμένο drive letter.

**MITRE Tactic**: Exfiltration

**MITRE Technique**: T1052 - Exfiltration Over Physical Medium

**LogSources**: Microsoft Windows Security Events (EIDs 4688 & 6416)

**Severity/Criticality**: Low (5)

### *2.6.1 QRadar*

#### *2.6.1.1 Rule*

Rule Description

Apply Detect process creation from removable media on events which are detected by the Local system
and when the event(s) were detected by one or more of Microsoft Windows Security Event Log
and when the event(s) were detected by one or more of winEndpoint
and when any of EventID (custom) match 6416|4688
and when at least 2 events are seen with the same Drive Name (custom) and different EventID (custom) in 10 minutes

Rule Actions

- Set Severity to 5
- Force the detected Event to create a NEW offense, select the offense using Computer (custom)

Rule Responses

- Dispatch New Event
  - Event Name: Detect process creation from removable media
  - Event Description: Monitor for newly executed processes when removable media is mounted.
  - Severity: 5 Credibility: 0 Relevance: 0
  - High-Level Category: System
  - Low-Level Category: Process Creation Success
  - Force the dispatched event to create a NEW offense, select the offense using Computer (custom)

This Rule will be: Enabled

#### *2.6.1.2 Offense*

**Offense 499825**

Summary Display ▼ Events Flows Actions ▼ Print

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Magnitude | [redacted] | Status | | Relevance | 1 | Severity | 5 | Credibility | 2 |
| Description | Detect process creation from removable media | Offense Type | Computer (custom) | | | | |
| | | Event/Flow count | 54 events and 0 flows in 2 categories | | | | |
| Source IP(s) | 192.168.56.1 | Start | 13 Δεκ 2022, 8:10:46 μ.μ. | | | | |
| Destination IP(s) | 192.168.56.1 | Duration | 10m 1s | | | | |
| Network(s) | other | Assigned to | Unassigned | | | | |

**List of Rules Contributing to Offense**

| Rule Name | Events/Flows | First Event/Flow | Last Event/Flow |
|---|---|---|---|
| Detect process creation from removable media | 54 | 12m 35s | 2m 34s |

#### *2.6.1.3 Events*

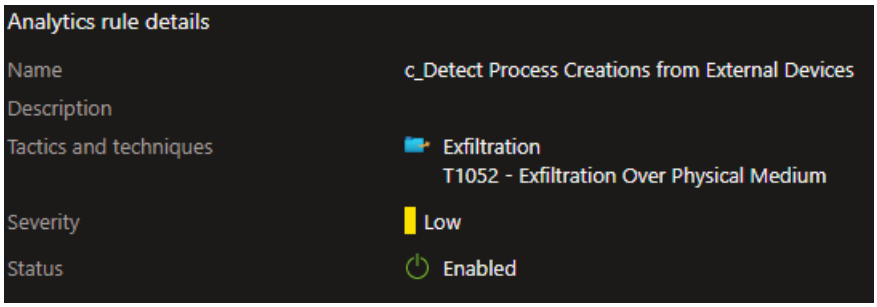
Current Filters:
Drive Name (custom) is D:\ (Clear Filter) Offense is Detect process creation from removable media (Clear Filter) Log Source is not Custom Rule Engine-171 [redacted] (Clear Filter)
▸ Current Statistics

(Show Charts)

| Start Time | Log Source | Username | EventID (custom) | Event Name | New Process ID (custom) | ProcessName (custom) | Process CommandLine (custom) | Creator Process ID (custom) | Creator Process Name (custom) | Drive Name (custom) | ClassName (custom) | Device ID (custom) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 Δεκ 2022, 8:20:47 μ.μ. | winEndpoint | N.Kigkas | 4688 | Success Audit: A new process has been created | 0x3ca4 | Setup.exe | "D:\Setup.exe" | 0x5ca8 | C:\Windows\explorer.exe | D:\ | N/A | N/A |
| 13 Δεκ 2022, 8:20:27 μ.μ. | winEndpoint | N/A | 6416 | A new external device was recognized by the System | N/A | N/A | N/A | N/A | N/A | D:\ | WPD | SWD\WPDBUSENUM_??_USBSTO... |

### *2.6.2 Sentinel*

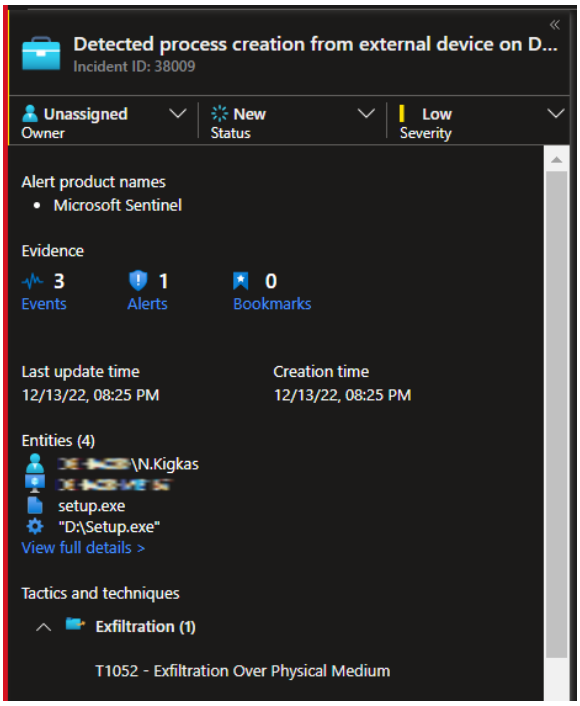
#### *2.6.2.1 Rule*




Rule Query:

```
SecurityEvent
| where Computer == "winEndpoint"
| where EventID == 6416
| where ClassName == "WPD"
| join kind = leftouter (
SecurityEvent
| where Computer == " winEndpoint"
| where EventID == 4688
| extend DriveOfProcess = extract('"(\\S*\\\\)',1,CommandLine)
) on $left.DeviceDescription == $right.DriveOfProcess
| project-rename DrivePlugTimestamp = TimeGenerated, CreateProcTimestamp = TimeGenerated1
| project CreateProcTimestamp, Account1, Activity1, Process1, CommandLine1, NewProcessId1,
NewProcessName1, ParentProcessName1, DrivePlugTimestamp, Computer, Activity, DeviceDescription,
DeviceId
| sort by CreateProcTimestamp desc
```

### *2.6.2.2 Incident*




### *2.6.2.3 Events*

| | |
|---|---|
| CreateProcTimestamp [UTC] | 2022-12-13T18:17:08.4644806Z |
| Account1 | \N.Kigkas |
| Activity1 | 4688 - A new process has been created. |
| Process1 | Setup.exe |
| CommandLine1 | "D:\Setup.exe" |
| NewProcessId1 | 0x6698 |
| NewProcessName1 | \Device\HarddiskVolume42\Setup.exe |
| ParentProcessName1 | C:\Windows\explorer.exe |
| DrivePlugTimestamp [UTC] | 2022-12-13T18:20:31.9718498Z |
| Computer | |
| Activity | 6416 - A new external device was recognized by the System |
| DeviceDescription | D:\ |
| DeviceId | SWD\WPDBUSENUM_??_USBSTOR#Disk&Ven_Dell&Prod_Recovery_ |

## *2.7 Detect child process from Office application*

**Objective**: Το Microsoft Office είναι μια αρκετά κοινή σουίτα εφαρμογών στους Windows σταθμούς εργασίας των τελικών χρηστών σε ένα εταιρικό δίκτυο και για αυτό οι επιτιθέμενοι συχνά την εκμεταλλεύονται στις επιθέσεις τους.

Η δημιουργία κακόβουλων θυγατρικών διεργασιών είναι μια κοινή στρατηγική κακόβουλου λογισμικού. Κακόβουλο λογισμικό που εκμεταλλεύεται το Office συχνά εκτελεί μακροεντολές VBA και περιέχει κώδικα για λήψη και προσπάθεια εκτέλεσης περισσότερων ωφέλιμων φορτίων, ενώ επίσης συχνή πρακτική είναι η διατήρηση (persistence) του κακόβουλου λογισμικού μέσω των Office εφαρμογών.

Για τον εντοπισμό της τεχνικής αρκεί να εντοπίσουμε τα γεγονότα δημιουργίας διεργασιών (EID 4688 [7] των οποίων οι διεργασίες Parent ή αλλιώς Creator θα είναι οποιαδήποτε εκ των winword, excel, powerpnt ή msaccess.

Ωστόσο, ενδέχεται επίσης ορισμένες νόμιμες επιχειρηματικές εφαρμογές να δημιουργήσουν θυγατρικές διαδικασίες για καλοήθεις σκοπούς. όπως η δημιουργία μιας γραμμής εντολών ή η χρήση του PowerShell για τη διαμόρφωση των ρυθμίσεων μητρώου.

**MITRE Tactic**: Persistence

**MITRE Technique**: T1137 - Office Application Startup

**LogSources**: Microsoft Windows Security Events (EIDs 4688)

**Severity/Criticality**: Medium (7)

### *2.7.1 QRadar*

#### *2.7.1.1 Rule*

Rule Description

Apply Detect child process from Office application on events which are detected by the Local system
and when the event(s) were detected by one or more of Microsoft Windows Security Event Log
and when any of EventID (custom) match 4688
and when any of Creator Process (custom) match (?i)WINWORD\.EXE|EXCEL\.EXE|POWERPNT\.EXE|MSACCESS\.EXE
and NOT when any of Process Name (custom) match (?i)WINWORD\.EXE|EXCEL\.EXE|POWERPNT
\.EXE|MSACCESS\.EXE

Rule Actions

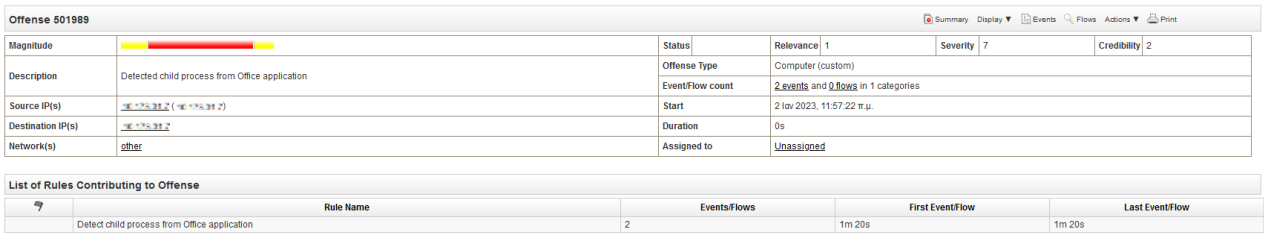
- Set Severity to 7
- Force the detected Event to create a NEW offense, select the offense using Computer (custom)

Rule Responses

- Dispatch New Event
  - Event Name: Detected child process from Office application
  - Event Description: Office apps include Word, Excel, PowerPoint and Access. Creating malicious child processes is a common malware strategy. Malware that abuses Office as a vector often runs VBA macros and exploit code to download and attempt to run more payloads. However, some legitimate line-of-business applications might also generate child processes for benign purposes; such as spawning a command prompt or using PowerShell to configure registry settings.
  - Severity: 5 Credibility: 0 Relevance: 0
  - High-Level Category: System
  - Low-Level Category: Process Creation Success
  - Force the dispatched event to create a NEW offense, select the offense using Computer (custom)

This Rule will be: Enabled

#### *2.7.1.2 Offense*



Offense 501989

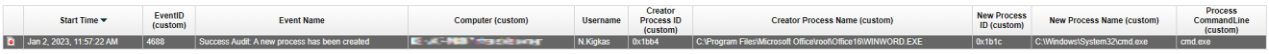
Summary Display ▼ Events Flows Actions ▼ Print

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Magnitude | | Status | | Relevance | 1 | Severity | 7 | Credibility | 2 |
| Description | Detected child process from Office application | Offense Type | Computer (custom) | | | | |
| | | Event/Flow count | 2 events and 0 flows in 1 categories | | | | |
| Source IP(s) | [redacted] | Start | 2 Ιαν 2023, 11:57:22 π.μ. | | | | |
| Destination IP(s) | [redacted] | Duration | 0s | | | | |
| Network(s) | other | Assigned to | Unassigned | | | | |

List of Rules Contributing to Offense

| Rule Name | Events/Flows | First Event/Flow | Last Event/Flow |
|---|---|---|---|
| Detect child process from Office application | 2 | 1m 20s | 1m 20s |

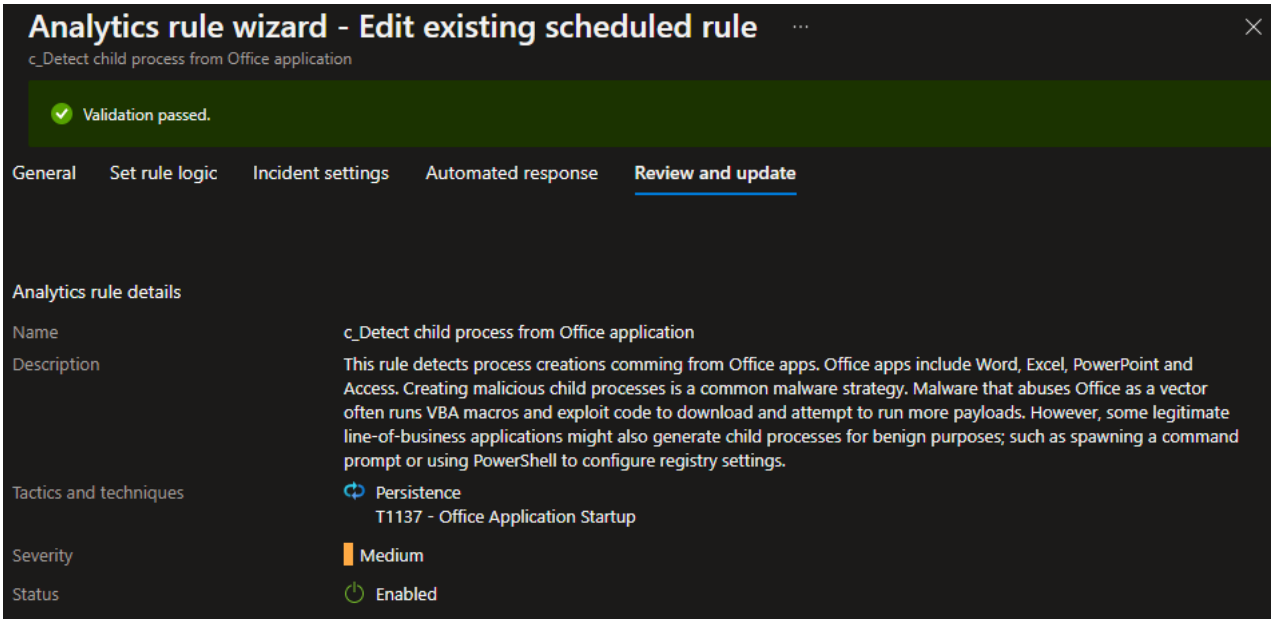
#### *2.7.1.3 Events*



| Start Time | EventID (custom) | Event Name | Computer (custom) | Username | Creator Process ID (custom) | Creator Process Name (custom) | New Process ID (custom) | New Process Name (custom) | Process CommandLine (custom) |
|---|---|---|---|---|---|---|---|---|---|
| Jan 2, 2023, 11:57:22 AM | 4688 | Success Audit: A new process has been created | [redacted] | N.Kigkas | 0x1bb4 | C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE | 0x1b1c | C:\Windows\System32\cmd.exe | cmd.exe |

### *2.7.2 Sentinel*

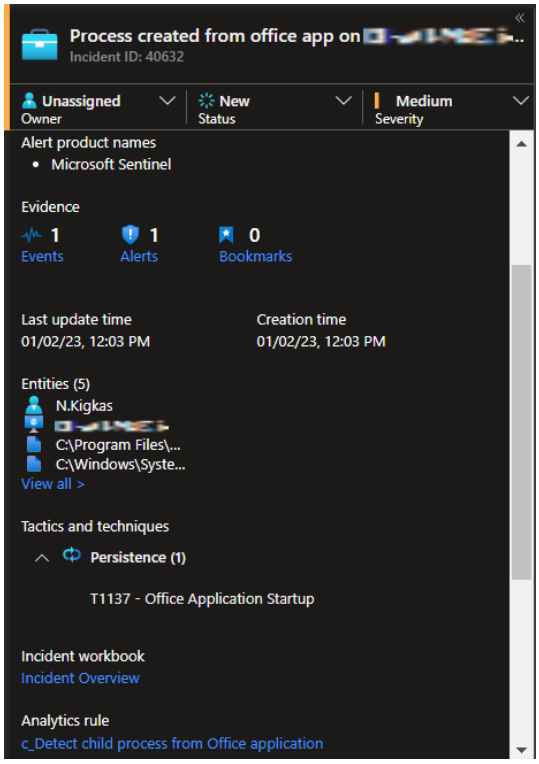
#### *2.7.2.1 Rule*




Rule Query:

```
SecurityEvent
| where EventID == 4688
| extend ParentProcess = extract(@'([^\\]*)$',1,ParentProcessName)
| where ParentProcess in~ ('WINWORD.EXE','EXCEL.EXE','POWERPNT.EXE','MSACCESS.EXE')
| where Process !in~ ('WINWORD.EXE','EXCEL.EXE','POWERPNT.EXE','MSACCESS.EXE')
| project TimeGenerated, Activity, Computer, SubjectUserName, ProcessId, ParentProcessName,
NewProcessId, NewProcessName, CommandLine
| sort by TimeGenerated desc
```

### *2.7.2.2 Incident*

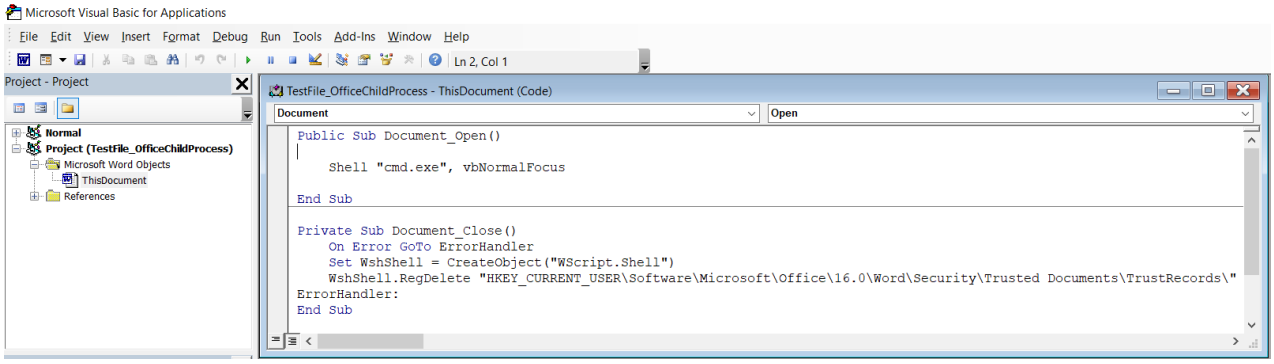


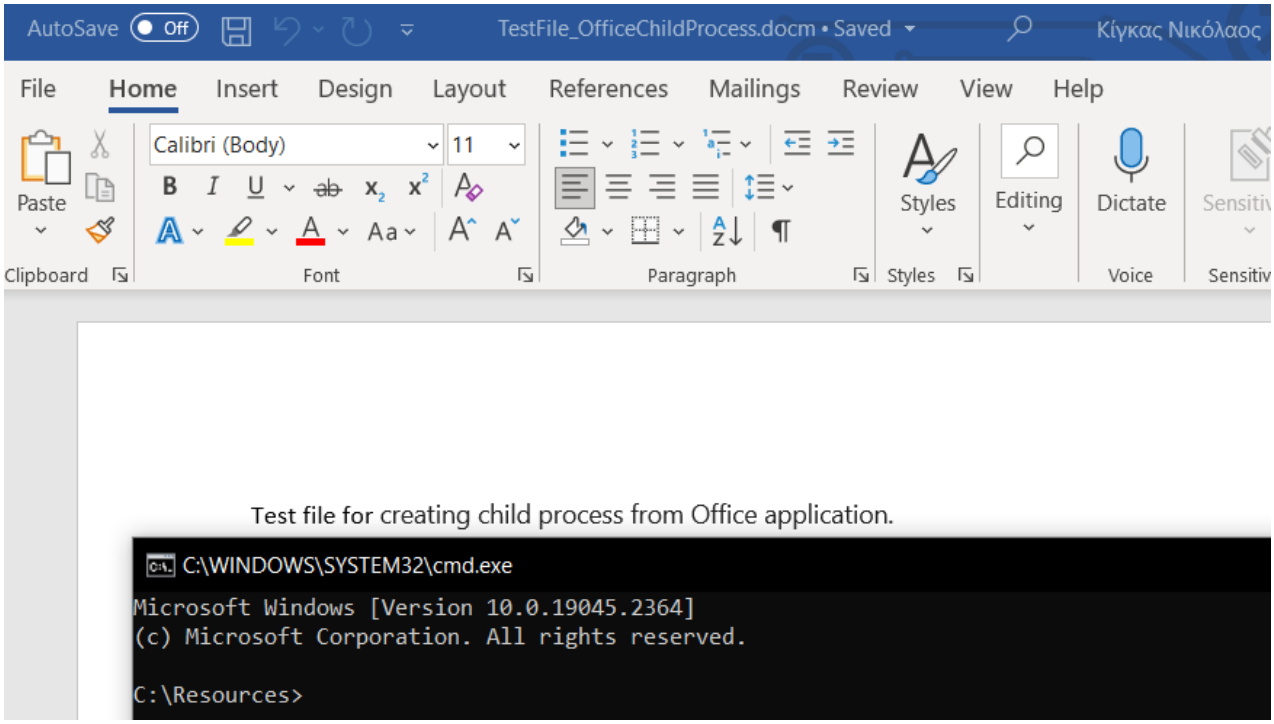

### *2.7.2.3 Events*

| | |
|---|---|
| TimeGenerated [UTC] | 2023-01-02T09:57:11.6042905Z |
| Activity | 4688 - A new process has been created. |
| Computer | |
| SubjectUserName | N.Kigkas |
| ProcessId | 0x1bb4 |
| ParentProcessName | C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE |
| NewProcessId | 0x1b1c |
| NewProcessName | C:\Windows\System32\cmd.exe |
| CommandLine | cmd.exe |

### *2.7.3 Επίθεση*

Για την προσομοίωση της τεχνικής αρκεί να δημιουργήσουμε ένα DOCM αρχείο το οποίο θα περιέχει Macro κώδικα ο οποίος απλώς θα εκτελεί τη διεργασία της γραμμής εντολών κατά το άνοιγμα του αρχείου.



# 3

# *Σύγκριση*

## *3.1 Συχνότητα εκτέλεσης κανόνων*

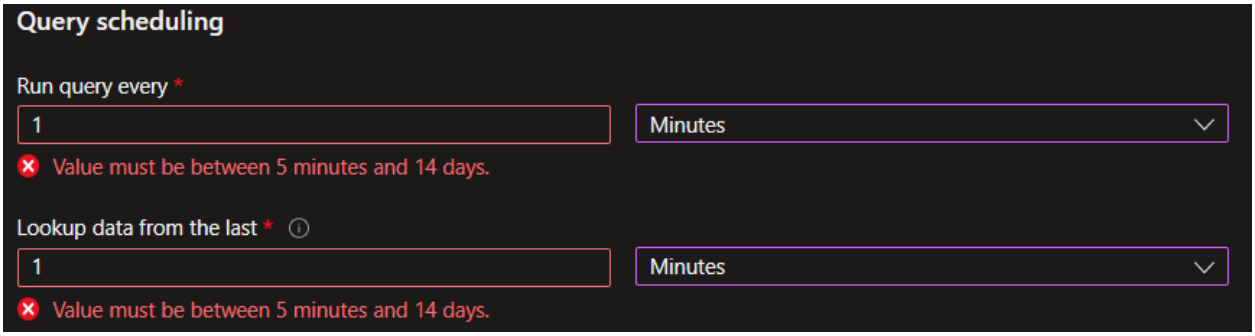
Όπως έχουμε αναφέρει ο έγκαιρος εντοπισμός κάποιου περιστατικού είναι από τα σημαντικότερα χαρακτηριστικά ενός SOC. Οφείλουμε λοιπόν να αναφέρουμε ένα γεγονός που επηρεάζει το παραπάνω χαρακτηριστικό και το γεγονός αυτό είναι η συχνότητα εκτέλεσης των κανόνων που παράγουν τα περιστατικά. Το προαναφερόμενο οφείλεται στον τρόπο λειτουργίας της κάθε λύσης και για τον λόγο αυτό πρέπει να αναφερθούμε σε κάποια βασικά στοιχεία και να περιγράψουμε συνοπτικά την ροή λειτουργίας της κάθε λύσης.

Το συστήματα του IBM QRadar διαχωρίζονται σε ρόλους. Οι ρόλοι που σχετίζονται με τα γεγονότα είναι οι Event Collector και Event Processor. Ο Event Collector αρχικά είναι υπεύθυνος για την συλλογή, κατηγοριοποίηση (low & high level categories) και κανονικοποίηση των γεγονότων και τέλος για την αποστολή των επεξεργασμένων γεγονότων στον ρόλο Event Processor. Στη συνέχεια το στοιχείο custom rule engine (CRE) το οποίο εκτελείται στα συστήματα με τον ρόλο Event Processor επεξεργάζεται τα γεγονότα και τα συγκρίνει με τους καθορισμένους κανόνες. Όταν οι συνθήκες ενός κανόνα ικανοποιηθούν ο Event Processor εκτελεί τις ενέργειες που έχουν τεθεί στον κανόνα ως response actions, όπως για παράδειγμα η δημιουργία ενός περιστατικού.

Τα αντίστοιχα βασικά στοιχεία του Microsoft Sentinel τα οποία χρήζουν αναφοράς είναι τα Tables που βρίσκονται στο Log Analytics Workspace και στα οποία αποθηκεύονται τα γεγονότα και οι Analytics κανόνες, οι οποίοι εκτελούν καθορισμένα KQL Queries επί των γεγονότων και τα επιστρεφόμενα ως αποτέλεσμα γεγονότα θα αποτελούν τα γεγονότα του περιστατικού. Ο κάθε κανόνας έχει την δική του ξεχωριστή συχνότητα και επόμενη στιγμή εκτέλεσης ανεξάρτητα από την λήψη των γεγονότων.

Από τις παραπάνω ροές συμπεραίνουμε πως στο QRadar ένα περιστατικό δημιουργείται σχεδόν σε πραγματικό χρόνο από την στιγμή της λήψης των απαραίτητων γεγονότων, αφού όλοι οι κανόνες ελέγχονται με τη λήψη κάθε γεγονότος. Η όποια καθυστέρηση θα οφείλεται καθαρά και μόνο στη διαθεσιμότητα δικτυακών και επεξεργαστικών πόρων.

Στο Sentinel από την άλλη μπορούμε να θεωρήσουμε ότι η συλλογή των γεγονότων γίνεται επίσης σε σχεδόν πραγματικό χρόνο, ωστόσο η διαφορά παρουσιάζεται με το γεγονός ότι ο κανόνας θα εκτελεστεί στην επόμενη προγραμματισμένη στιγμή, ανεξάρτητα με τα γεγονότα που έχουν ληφθεί έως τότε. Η διαφορά είναι εμφανέστερη με τον περιορισμό της συχνότητας εκτέλεσης του KQL Query / κανόνα να λαμβάνει ως ελάχιστη τιμή τα 5 λεπτά.




Η παραπάνω διαφορά μπορεί να μην είναι εμφανής εάν η τελική ενέργεια είναι απλώς η ανέγερση ενός περιστατικού ως ειδοποίηση. Εάν όμως έχουμε στη διάθεσή μας και θέλουμε να αξιοποιήσουμε τις δυνατότητες αυτόματων ενεργειών περιορισμού (automated response actions) μέσω κάποιου playbook, οι οποίες παρέχονται από κάποια SOAR λύση, καθυστέρηση ανταπόκρισης της τάξης των 5 λεπτών μπορεί να επιφέρει σημαντικές επιπτώσεις σε συγκεκριμένου τύπου περιστατικά, όπως για παράδειγμα Ransomware.

## *3.2 Ευκολία και ευελιξία δημιουργίας κανόνων συσχέτισης*

Αναφορικά με την ευκολία και την ευελιξία ως προς την ανάπτυξη κανόνων συσχέτισης οφείλουμε αρχικά να αναφέρουμε ότι είναι υποκειμενικά κριτήρια σύγκρισης καθώς αυτά καθορίζονται από την εμπειρία και την εξοικείωση που έχει ο κάθε αναλυτής με την κάθε λύση. Είναι ωστόσο προφανές πως τα χρόνια κτήσης και διαχείρισης μίας λύσης σε καμία περίπτωση δεν αρκούν ως παράμετροι για να προσδιοριστεί ο βαθμός εξειδίκευσης ενός αναλυτή. Δεδομένων των παραπάνω και με τον βαθμό εξειδίκευσης που διαθέτουμε θα αναφέρουμε κάποιες εμπειρικές παρατηρήσεις σχετικά με τις προαναφερόμενες μετρικές.

Στο IBM QRadar το χτίσιμο ενός κανόνα πραγματοποιείται μέσω ενός φιλικού προς τον χρήστη γραφικού περιβάλλοντος με προκαθορισμένες αλλά παραμετροποιήσιμες συνθήκες. Το γεγονός αυτό καθιστά εύκολη τη δημιουργία των κανόνων χωρίς να είναι απαραίτητη η γνώση και η χρήση κάποιας query language όπως Ariel Query Language (AQL). Ωστόσο, το ίδιο γεγονός επηρεάζει αντιστρόφως ανάλογα την ευελιξία συσχέτισης δεδομένων καθώς η χρήση προκαθορισμένων συνθηκών καθίσταται περιορισμός όταν πρέπει να συνδυαστούν γεγονότα από διαφορετικές πηγές και μάλιστα υπό συνθήκες με βάση είτε κάποιες τιμές πεδίων είτε του χρονικού παράγοντα. Χαρακτηριστικό παράδειγμα αποτέλεσε η περίπτωση “Detect process creation from removable media” [2.6.1.1] κατά την οποία έπρεπε να καθοριστεί η χρονική σειρά λήψης των γεγονότων και να ελεγχθεί η τιμή ενός πεδίου του δεύτερου χρονικά γεγονότος με όρισμα από το πρώτο. Είναι φυσικό να αυξάνεται η δυσκολία υλοποίησης ανάλογα με την πολυπλοκότητα της λογικής μίας περίπτωσης χρήσης, αλλά η δυσκολία αυτή αυξάνεται ακόμα περισσότερο με τον προαναφερόμενο περιορισμό.

Στο Microsoft Sentinel η δημιουργία ενός κανόνα πραγματοποιείται υποχρεωτικά με τη χρήση query language και συγκεκριμένα της Kusto Query Language (KQL). Το μειονέκτημα στο γεγονός αυτό είναι προφανές και είναι ότι ένας αναλυτής που διαθέτει την γενική γνώση για την υλοποίηση μίας περίπτωσης χρήσης, στο Sentinel δεν θα μπορέσει να την υλοποιήσει εάν δεν γνωρίζει την παραπάνω γλώσσα. Μπορεί να ακούγεται περιοριστικό το παραπάνω γεγονός, ωστόσο καθώς κάποιος εξοικειώνεται με την KQL, ανακαλύπτει συνεχώς νέες δυνατότητες αναφορικά με την συσχέτιση και τον εμπλουτισμό των δεδομένων. Γενικότερα μπορούμε να πούμε πως η δυσκολία υλοποίησης και η πολυπλοκότητα μίας περίπτωσης χρήσης περιορίζεται μόνο από την εξειδίκευση του αναλυτή με την KQL.

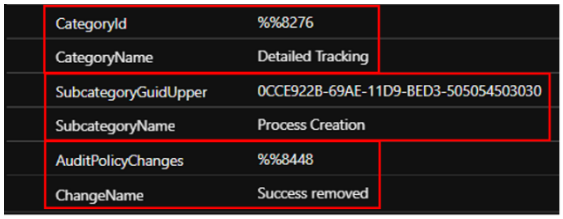
## *3.3 Αναζήτηση επί των γεγονότων και εμπλουτισμός δεδομένων*

Σε ένα SIEM σύστημα επίσης καθοριστικό ρόλο παίζουν οι δυνατότητες που παρέχονται και οι περιορισμοί που προκύπτουν σχετικά με την αναζήτηση επί των γεγονότων. Ειδικότερη σημασία λαμβάνουν οι παραπάνω παράμετροι σε ένα σύστημα όπως το Microsoft Sentinel του οποίου όπως έχουμε δει οι κανόνες διέγερσης περιστατικών ασφαλείας βασίζονται επί το πλείστων στις αναζητήσεις.

Όπως αναφέραμε στην προηγούμενη παράγραφο σύγκρισης, μπορεί το IBM QRadar να είναι περιοριστικό στον συνδυασμό γεγονότων κατά τη δημιουργία κανόνα συσχέτισης, δεν ισχύει όμως το ίδιο για την αναζήτηση επί των γεγονότων. Το γεγονός ότι όλα τα δεδομένα ανεξαρτήτως τύπου και πηγής αποθηκεύονται κανονικοποιημένα σε κοινή βάση δεδομένων, δίνει τη δυνατότητα στους αναλυτές με πολύ απλές συνθήκες αναζήτησης να φέρουν στα αποτελέσματα γεγονότα από διαφορετικών τύπων πηγές. Εν αντιθέσει στο Microsoft Sentinel, μπορεί να είναι εφικτή η αντίστοιχη αναζήτηση, ωστόσο αυτό προϋποθέτει τη σύνδεση πινάκων, γεγονός που αφενός απαιτεί μεγαλύτερο βαθμό εξοικείωσης με την KQL και αφετέρου περισσότερο υπολογιστικό κόστος και χρόνο αναζήτησης.

Ένας ακόμη παράγοντας κατά την αναζήτηση γεγονότων είναι ο εμπλουτισμός των αποτελεσμάτων με δεδομένα που ορίζει ο αναλυτής εφόσον αυτά δεν προσφέρονται άμεσα από τα γεγονότα. Στο IBM QRadar δεν δίνεται η δυνατότητα δημιουργίας επιπλέων πεδίων αποτελέσματος και δυναμική απόδοση τιμών σε αυτά με όρισμα τιμές από άλλα πεδία κατά την αναζήτηση. Με τις δυνατότητες δημιουργίας στατικών δεδομένων, επέκτασης πεδίων και ένωσης πινάκων που προσφέρει η KQL, ο εμπλουτισμός δεδομένων στο Microsoft Sentinel είναι πιο εφικτός.

Χαρακτηριστικό παράδειγμα αυτού αποτέλεσε η περίπτωση χρήσης που εξετάσαμε “Detected Audit Policy disable” [2.3.2.1.1] κατά την οποία παρατηρούμε ότι εγγενώς τα γεγονότα αναφέρονται τόσο στις κατηγορίες πολιτικών όσο και στις ενέργειες με κωδικοποιημένα αναγνωριστικά. Θεωρήσαμε λοιπόν σκόπιμο τον εμπλουτισμό των επιστρεφόμενων αποτελεσμάτων με τρία επιπλέον πεδία τα οποία θα λαμβάνουν την περιγραφή του αντίστοιχου κωδικού αναγνωριστικού.

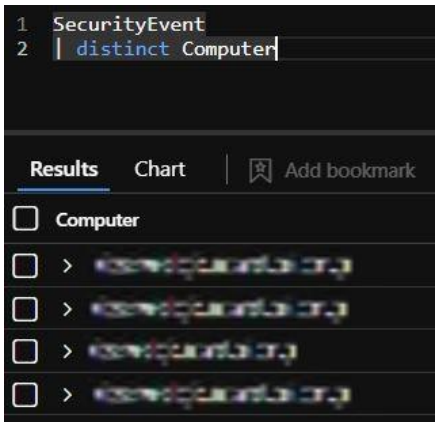



Ένας αναλυτής όπου εξετάζει κάθε τέτοιο γεγονός θα έπρεπε να αφιερώσει χρόνο αναζήτησης προκειμένου να αντιστοιχίσει τα κωδικοποιημένα αυτά αναγνωριστικά στις αντίστοιχες κατανοητές περιγραφές. Γενικότερα, είναι σημαντικό ένας αναλυτής που διερευνά ένα περιστατικό να έχει στη διάθεσή του άμεσα όσο περισσότερη χρήσιμη πληροφορία χρειάζεται, προκειμένου να αφιερώσει χρόνο σε ωφέλιμη αναζήτηση και συσχέτιση και ο χρόνος απόκρισης σε ένα περιστατικό να είναι μικρότερος.

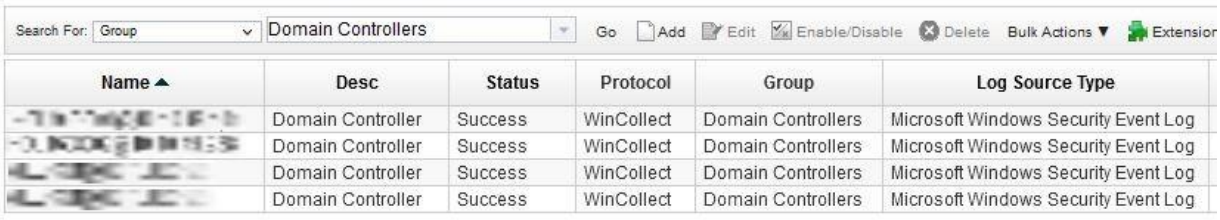
## *3.4 Ορατότητα, διαχείριση και παρακολούθηση πηγών δεδομένων*

Δεν θα ήταν εφικτό να αναφερθούμε στις διαφορετικές υποστηριζόμενες πηγές δεδομένων και στους τρόπους σύνδεσης αυτών με την κάθε εξεταζόμενη λύση αρχικά επειδή είναι αναρίθμητες οι πιθανές πηγές και έπειτα αποτελούν δεδομένα που μεταβάλλονται συνεχώς. Κρίνουμε ωστόσο σημαντικό να σημειωθεί μία ουσιώδης διαφορά ως προς την ορατότητα, τη διαχείριση και την παρακολούθηση των πηγών.

Το Microsoft Sentinel διαθέτει inventory με τους ενεργοποιημένους ή μη Data Connectors. Ένας Data Connector περιγράφει μία πηγή ως προς τον τύπο δεδομένων και όχι ως προς κάθε ένα διασυνδεδεμένο σύστημα από το οποίο αντλεί γεγονότα. Για παράδειγμα η ύπαρξη του Data Connector "Windows Security Events" υποδεικνύει ότι λαμβάνουμε αυτού του τύπου τα γεγονότα στον σχετικό πίνακα (SecurityEvent), αλλά δεν υπάρχουν σε κοινή θέα οι διαφορετικοί Servers από τους οποίους αντλούνται τα δεδομένα αυτά. Για να λάβει κάποιος τη γνώση αυτή, θα πρέπει να εκτελέσει κατάλληλο KQL query σε ένα ή περισσότερα Tables τα οποία σχετίζονται με τον αντίστοιχο Data Connector. Σε αυτό το σημείο πρέπει να κάνουμε την σημαντική διευκρίνιση ότι προκειμένου να εμφανιστεί μία πηγή στα αποτελέσματα, θα πρέπει να έχει στείλει τουλάχιστον ένα γεγονός για την χρονική περίοδο στην οποία περιορίζουμε την αναζήτηση, γεγονός που σημαίνει ότι εάν για τον οποιοδήποτε λόγο η λήψη γεγονότων από αυτή την πηγή έχει διακοπεί δεν θα λάβουμε στα αποτελέσματα την πηγή αυτή.

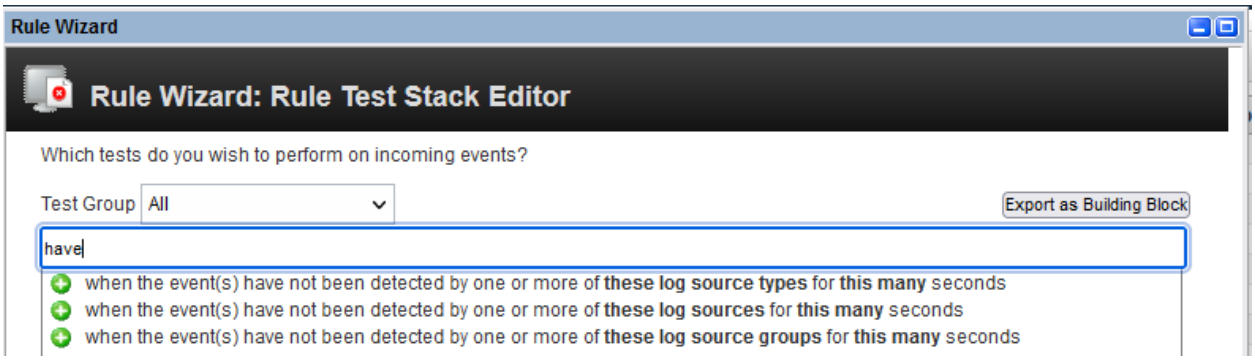

Το IBM QRadar από την άλλη διαθέτει ειδικό inventory των πηγών, στο οποίο αναφέρονται οι πηγές σε επίπεδο διασυνδεδεμένου συστήματος με τον αντίστοιχο τύπο δεδομένου καθώς και την ομάδα πηγών στην οποία ενδέχεται να έχουμε εντάξει την πηγή αυτή. Παρέχεται επίσης το πολύ σημαντικό πεδίο της Κατάστασης της πηγής το οποίο υποδηλώνει την ορθή λειτουργία της λήψης γεγονότων από την αντίστοιχη πηγή. Συμπεραίνουμε σε αυτό το σημείο πως μία παραμετροποιημένη πηγή θα εμφανίζεται στο Inventory αυτό ανεξάρτητα με την υγεία της διασύνδεσής της.




| Name | Desc | Status | Protocol | Group | Log Source Type |
|---|---|---|---|---|---|
| [redacted] | Domain Controller | Success | WinCollect | Domain Controllers | Microsoft Windows Security Event Log |
| [redacted] | Domain Controller | Success | WinCollect | Domain Controllers | Microsoft Windows Security Event Log |
| [redacted] | Domain Controller | Success | WinCollect | Domain Controllers | Microsoft Windows Security Event Log |
| [redacted] | Domain Controller | Success | WinCollect | Domain Controllers | Microsoft Windows Security Event Log |

Η βασικότερη προϋπόθεση για την ορθή λειτουργία ενός SIEM είναι η αδιάλειπτη συλλογή δεδομένων από τις ήδη παραμετροποιημένες πηγές. Εάν για οποιοδήποτε λόγο διακοπεί η συλλογή γεγονότων, διακόπτεται επίσης η ορατότητα της λύσης και κατά συνέπεια ο εντοπισμός περιστατικών. Δεδομένου του προαναφερόμενου, κρίνεται απαραίτητη η ύπαρξη της βασικής περίπτωσης χρήσης «Εντοπισμός διακοπής συλλογής δεδομένων» για κάθε πηγή.

Η υλοποίηση αυτής της περίπτωσης χρήσης είναι εύκολη σε ένα σύστημα όπως το IBM QRadar το οποίο πρωτίστως διαθέτει ξεκάθαρο inventory των πηγών και έπειτα παρέχει τις σχετικές προκαθορισμένες συνθήκες με τις οποίες μπορούμε να καλύψουμε μαζικά διαφορετικού τύπου πηγές κατά τη δημιουργία ενός και μόνο κανόνα.




Εν αντιθέσει στο Microsoft Sentinel, εάν λάβουμε υπόψη τα προαναφερόμενα, διαπιστώνουμε πως η κάλυψη της ίδιας περίπτωσης χρήσης απαιτεί μεγάλο διαχειριστικό κόστος καθώς για κάθε διαφορετικό τύπο πηγής θα πρέπει να έχουμε ξεχωριστό κανόνα του οποίου το KQL θα φέρει λογική της ακόλουθης μορφής.

```
SecurityEvent
| summarize arg_max(TimeGenerated, *) by Computer
| project
    Computer,
    ['Last Event Time'] = TimeGenerated,
    ['Hours Since Last Event'] = datetime_diff("Hour", now(), TimeGenerated)
| sort by ['Hours Since Last Event']
//Threshold of time range missing events
| where ['Hours Since Last Event'] >= 1
```

Results | Chart

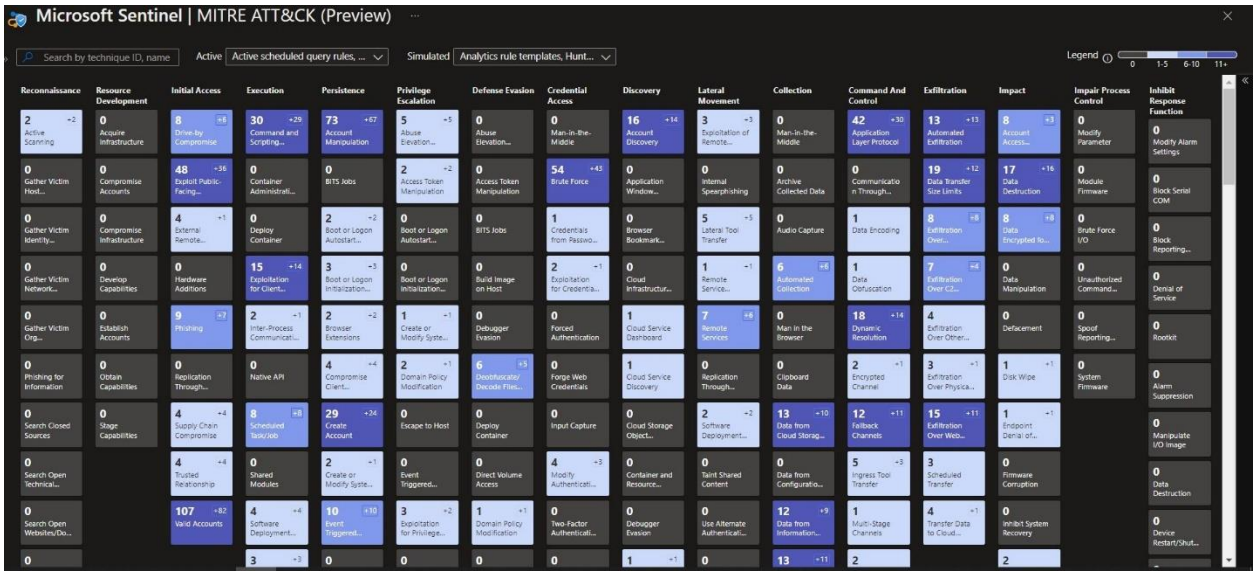
| Computer | Last Event Time [Local T... | Hours Since Last Event |
|---|---|---|
| [redacted] | 2/25/2023, 3:34:10.875 PM | 162 |
| [redacted] | 2/26/2023, 2:46:38.158 AM | 151 |
| [redacted] | 2/26/2023, 3:49:45.345 PM | 138 |
| [redacted] | 2/28/2023, 3:09:24.538 PM | 90 |

## *3.5 Use Cases & Mitre ATT&CK Framework*

Είναι ιδιαιτέρως σημαντικό ένα SOC να έχει επίγνωση των διαφορετικών κακόβουλων τακτικών και τεχνικών που μπορεί να εντοπίσει με τα ήδη υπάρχοντα use cases. Είναι όμως εξίσου, εάν όχι περισσότερο, σημαντικό να έχει επίγνωση αυτών που δεν εντοπίζει, είτε γιατί δεν έχει παραμετροποιηθεί η απαραίτητη συλλογή γεγονότων από κάποια πηγή, είτε γιατί απλώς δεν έχει δημιουργηθεί κατάλληλος κανόνας / use case ενώ τα δεδομένα ήδη συλλέγονται.

Το framework με το inventory των ζητούμενων τακτικών και τεχνικών υπάρχει και είναι το Mitre ATT&CK και το μόνο που απομένει για να επιτύχουμε τη ζητούμενη ορατότητα και γνώση είναι η αντιστοιχία του Framework με τα use cases.

Το Microsoft Sentinel διατηρεί updated inventory με τα Mitre Tactics & Techniques, τα οποία αποδίδονται τόσο στα out of the box, όσο και στα custom Analytics Rules. Επιπρόσθετα, παρέχεται ο γνωστός πίνακας του Mitre Att&ck με συγκεντρωτική απεικόνιση της τρέχουσας κάλυψης του Framework από τα υπάρχοντα Analytics Rules/Use Cases.




Εν αντιθέσει το IBM QRadar out of the box χρησιμοποιεί κάποια pre-defined values για τα πεδία High και Low Level Categories [9] τα οποία αποδίδονται στα γεγονότα και για τα οποία δεν υπάρχει ένα προς ένα αντιστοίχιση με τα Mitre Tactics & Techniques, γεγονός που καθιστά δύσκολη έως και αδύνατη την αξιοποίηση του Mitre Framework και την παρακολούθηση της κάλυψης αυτού.

# 4

# *Βιβλιογραφία - Πηγές*


[1] Miller, D. R., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2010). Security Information and Event Management (SIEM) Implementation (1st ed.). McGraw Hill.

[2] Devo. (2022, October 31). The 2022 Gartner® Magic QuadrantTM for SIEM. Devo.com. https://www.devo.com/resources/the-gartner-magic-quadrant-2022/

[3] MITRE ATT&CK®. (n.d.). https://attack.mitre.org/

[4] Metcalf, S. (2018, May 18). Beyond Domain Admins – Domain Controller & AD Administration. Active Directory Security. https://adsecurity.org/?p=3700

[5] Smith, R. (n.d.). Windows Security Log Event ID 4728: A member was added to a security-enabled global group. Ultimate Windows Security. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4728

[6] Smith, R. (n.d.). Windows Security Log Event ID 4719: System audit policy was changed. Ultimate Windows Security. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4719

[7] Smith, R. (n.d.). Windows Security Log Event ID 4688: A new process has been created. Ultimate Windows Security. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=6416

[8] Smith, R. (n.d.). Windows Security Log Event ID 6416: A new external device was recognized by the system.

[9] Event categories. (n.d.). https://www.ibm.com/docs/en/qradar-on-cloud?topic=administration-event-categories