ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών Κυβερνοασφάλειας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Attack Detection Methods Based on Windows Security Event Logs Correlated with SIEM

Γεώργιος Π. Ανδριανόπουλος
Α.Μ. cscyb21003

Εισηγήτρια: Ιωάννα Καντζάβελου, Επίκουρη Καθηγήτρια

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Attack Detection methods based on windows security event logs correlated with SIEM

Γεώργιος Π. Ανδριανόπουλος
Α.Μ. cscyb21003

Εισηγήτρια:

Ιωάννα Καντζάβελου, Επίκουρη Καθηγήτρια

Ioanna Kantzavelou
Digitally signed by Ioanna Kantzavelou
Date: 2024.06.03 12:02:10 +03'00'

Εξεταστική Επιτροπή:

Λέανδρος Μαγλαράς, Καθηγητης

Leandros Maglaras

Παναγιώτης Γιαννακόπουλος, Καθηγητης

Panagiotis Giannakopoulos
Digitally signed by Panagiotis Giannakopoulos
Date: 2024.06.05 16:48:47 +03'00'

Ημερομηνία εξέτασης

24/05/2024

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

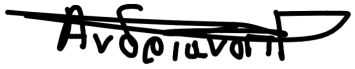
Ο/η κάτωθι υπογεγραμμένος **Ανδριανόπουλος Γεώργιος** του **Παναγιώτη**, με αριθμό μητρώου **cscyb21003** φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών **Κυβερνοασφάλειας** του Τμήματος **Μηχανικών Πληροφορικής και Υπολογιστών** της Σχολής **Μηχανικών** του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

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

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Ανδριανόπουλος Γεώργιος



ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της κυβερνοασφάλειας. Την προσπάθειά μου αυτή υποστήριξε η επιβλέπουσα καθηγήτρια μου, την οποία θα ήθελα να ευχαριστήσω. Τελευταίο αλλά όχι λιγότερο σημαντικό, θέλω να ευχαριστήσω εμένα, που πίστεψα σε μένα, για όλη τη σκληρή δουλειά που έκανα, που αφιέρωσα πολύ προσωπικό χρόνο και που δεν τα παράτησα ποτέ.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία επικεντρώνεται στην ανάλυση επιθέσεων σε συστήματα Windows, βασιζόμενη στις καταγραφές ασφαλείας και στους κανόνες συσχέτισης ενός συστήματος SIEM.

Αναδεικνύεται λεπτομερώς η σημασία της ύπαρξης ενός συστήματος SIEM και της αποστολής των καταγραφών των συστημάτων σε αυτό.

Η ύπαρξη κανόνων συσχέτισης αποτελεί βασική προϋπόθεση για την ανίχνευση επιθέσεων που μπορεί να συμβαίνουν στον οργανισμό και να μην είναι ορατές από τα υπόλοιπα συστήματα ασφαλείας.

Η εργασία περιλαμβάνει αναλυτική παρουσίαση της διαδικασίας εγκατάστασης και παραμετροποίησης των απαραίτητων συστημάτων, τη δημιουργία κανόνων συσχέτισης και την ανάλυση των επιθέσεων που πραγματοποιήθηκαν. Επιπλέον, συζητούνται οι προκλήσεις που αντιμετωπίζουν οι οργανισμοί στον τομέα της κυβερνοασφάλειας, καθώς και κάποια σενάρια επίθεσης που αναπτύχθηκαν σε εργαστηριακό περιβάλλον.

Με αυτόν τον τρόπο, η εργασία αποσκοπεί στη διερεύνηση της αποδοτικότητας των συστημάτων SIEM στην ανίχνευση και την ανάλυση επιθέσεων, προσφέροντας πολύτιμες γνώσεις για τη βελτίωση της ασφάλειας των πληροφοριακών συστημάτων.

Πίνακας περιεχομένων

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

SIEM	Security Information and Event Management
WSEL	Windows Security Event Logs
AD	Active Directory
DC	Domain Controller
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
WAF	Web Application Firewall
UEBA	User and Entity Behavior Analytics
ML	Machine Learning
AI	Artificial Intelligence
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
CE	Community Edition
GB	Gigabyte
CPU	Central Processing Unit
IP	Internet Protocol
GHz	GigaHertz
Bit	binary digit
GPU	Graphics Processing Unit
EPS	Events Per Second
MB	Megabyte
TCP	Transmission Control Protocol
RPC	Remote Procedure Call
TGT	Ticket-Granting Ticket
SID	System Identification
DPAPI	Data Protection Application Programming Interface
PNP	Plug and Play
DS	Directory Service
SACL	System Access Control List
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
WFP	Windows Filtering Platform
COM	Component Services
SAM	Security Account Manager
EFS	Encrypting File System
BCD	Boot Configuration Data

LSA	Local Security Authority
NTLM	Windows NT LAN Manager
LPC	Local Procedure Call
nmtui	Network Manager Text User Interface
DNS	Domain Name System
NTP	Network Time Protocol
SMB	Server Message Block

Κεφάλαιο 1

1.1 Εισαγωγή

Στη σημερινή ψηφιακή εποχή η ασφάλεια των δεδομένων και των Πληροφοριακών Συστημάτων είναι υποχρεωτική η ασφάλεια της πληροφορίας. Επαγγελματίες κυβερνοασφάλειας χρησιμοποιούν πολλαπλές μεθόδους για να ανιχνεύουν και να αντιδρούν σε περιστατικά ασφάλειας επιτυχημένα.

Πολύ σημαντικό στοιχείο της στρατηγικής αυτής είναι η συνεχής παρακολούθηση των δραστηριοτήτων των συστημάτων κάτι που είναι εφικτό μέσα από τις τα αρχεία καταγραφής συμβάντων ασφαλείας των Windows, των πολιτικών ελέγχου, των Συστημάτων πληροφοριών ασφαλείας και διαχείρισης συμβάντων (SIEM), των κανόνων συσχέτισης και των προηγμένων μεθόδων ανίχνευσης επιθέσεων.

Αρχεία καταγραφής συμβάντων ασφαλείας των Windows – Windows Security Event Logs

Τα αρχεία καταγραφής συμβάντων είναι από τα σημαντικότερα στοιχεία ενός λειτουργικού συστήματος που βασίζεται σε Windows. Αυτά τα αρχεία καταγραφής που συσχετίζονται με την ασφάλεια καταγραφούν όλες τις δραστηριότητες που συμβαίνουν εντός του λειτουργικού συστήματος, όπως προσπάθεια σύνδεσης, πρόσβαση σε αντικείμενα, αλλαγές δικαιωμάτων χρήστη, αλλαγές πολιτικών και πολλά άλλα. Το αρχείο καταγραφής ασφαλείας χρησιμεύει σαν ένα πολύ σημαντικό εργαλείο δεδομένων που μπορεί να αναλυθεί μεταγενέστερα ώστε να αποκαλυφθούν πιθανά περιστατικά ασφαλείας.

Πολιτικές ελέγχου των αρχείων καταγραφής των Windows – Windows Log Audit Policies

Για να αξιοποιηθούν πλήρως οι δυνατότητες των αρχείων καταγραφής συμβάντων ασφαλείας των Windows, υπάρχει η δυνατότητα διαμόρφωσης των πολιτικών ελέγχου ώστε να καθορίσουμε ποια συμβάντα θα καταγράφονται.

Αυτές οι πολιτικές επιτρέπουν τη λεπτομερή ρύθμιση των πληροφοριών που καταγράφονται διασφαλίζοντας ότι καταγράφονται οι πιο σημαντικές και σχετικές πληροφορίες στα συμβάντα ασφαλείας.

Προσαρμόζοντας στις πολιτικές ελέγχου, οργανισμοί μπορούν να τηρούν συγκεκριμένες απαιτήσεις συμμόρφωσης και να διατηρούν ένα λεπτομερές αρχείο καταγραφών για τα συστήματα τους.

Συστήματα Ασφαλείας Πληροφοριών και Διαχείρισης Συμβάντων – Security Information and Event Management (SIEM)

Τα συστήματα SIEM αποτελούν τη βάση των σύγχρονων Κέντρο Επιχειρήσεων Ασφάλειας. Λειτουργούν ως το κεντρικό σύστημα για τη συλλογή και την ανάλυση των δεδομένων από διαφορετικές πηγές, συμπεριλαμβανομένων των αρχείων καταγραφής συμβάντων ασφαλείας των Windows. Τα SIEM παρέχουν δυνατότητες συσχέτισης δεδομένων και παρακολούθησής τους σε πραγματικό χρόνο, προσφέροντας μία ολοκληρωμένη εικόνα για το εκάστοτε περιβάλλον. Τέτοιου είδους συστήματα είναι ιδανικά για τον εντοπισμό ανωμαλιών και πιθανών απειλών, τη μείωση του χρόνου απόκρισης σε συμβάντα ασφαλείας και τη συμμόρφωση με πολιτικές και κανονισμούς ασφαλείας.

Κανόνες συσχέτισης – Correlation Rules

Οι Κανόνες συσχέτισης που είναι γνωστοί και ως κανόνες ανίχνευσης, είναι η λογική πίσω από τα SIEM συστήματα. Ουσιαστικά είναι σύνολα λογικών δηλώσεων που χρησιμοποιούνται ώστε να αναλύσουν και να συσχετίσουν πολλαπλά συμβάντα ασφαλείας.

Με βάση αυτούς τους κανόνες τα SIEM είναι ικανά να εντοπίσουν μοτίβα επιθέσεων και ύποπτων δραστηριοτήτων που διαφορετικά θα μπορούσαν να περάσουν απαρατήρητα. Οι κανόνες συσχέτισης προσαρμόζονται ανάλογα τις ανάγκες του εκάστοτε οργανισμού και υπάρχει η δυνατότητα δημιουργίας νέων κανόνων συσχέτισης ανάλογα με τις εκάστοτε απαιτήσεις.

Μέθοδοι ανίχνευσης επιθέσεων – Attack Detection Methods

Οι μέθοδοι ανίχνευσης επιθέσεων αξιοποιούν τις πληροφορίες που βρίσκονται στα αρχεία καταγραφής συμβάντων ασφαλείας των Windows.

Αυτές οι μέθοδοι βασίζονται στην ανίχνευση ανωμαλιών, στην ανάλυση συμπεριφοράς, τη μηχανική μάθηση αλλά και την τεχνητή νοημοσύνη.

Βάση των παραπάνω μεθόδων είμαστε σε θέση για την έγκαιρη αναγνώριση των απειλών, τη δυνατότητα απόκρισης σε συμβάντα ασφαλείας γρηγορότερα, αλλά και την ελαχιστοποίηση των εσφαλμένων γεγονότων.

Στην κυβερνοασφάλεια η συνύπαρξη των αρχείων καταγραφής συμβάντων ασφαλείας των Windows, των πολιτικών ελέγχου, των SIEM, των κανόνων συσχέτισης και των μεθόδων ανίχνευσης επιθέσεων είναι μία εξαιρετική άμυνα απέναντι σε ένα συνεχώς εξελισσόμενο περιβάλλον απειλών.

Οι απειλές στον κυβερνοχώρο συνεχίζουν να αυξάνονται με ραγδαία μορφή και η κατανόηση η αξιοποίηση των εργαλείων αυτών θεωρείται αναγκαία για τους οργανισμούς που θέλουν να προστατεύσουν τα ψηφιακά δεδομένα και τις ευαίσθητες πληροφορίες τους.

1.2 Αρχεία καταγραφής συμβάντων ασφαλείας των Windows

Εισαγωγή στα Windows Security Event Logs

Τα Windows security event logs είναι ένα ενσωματωμένο κομμάτι στο λειτουργικό σύστημα των Windows. Τέτοιου είδους καταγραφές παίζουν πολύ σημαντικό ρόλο στην καταγραφή των συμβάντων ασφαλείας και των δραστηριοτήτων που συμβαίνουν στα Windows. Αναλύοντας αυτές τις καταγραφές μπορούμε να διατηρήσουμε την ασφάλεια, την ακεραιότητα και τη συμμόρφωση της υποδομής μας.

Τύποι των Windows Security Event Logs

1. Καταγραφές ασφαλείας: Το αρχείο καταγραφής ασφαλείας περιλαμβάνει πληροφορίες σχετικά με προσπάθειες σύνδεσης χρηστών, δικαιωμάτων χρηστών, πρόσβασης σε αντικείμενα, αλλαγές πολιτικής και άλλα. Το αρχείο καταγραφής ασφαλείας είναι από τα πιο σημαντικά αρχεία καταγραφής συμβάντων ασφάλειας. Τέτοιου είδους αρχεία είναι σημαντικά για τον εντοπισμό και τη διερεύνηση περιστατικών ασφαλείας.
2. Καταγραφές εφαρμογών: Το αρχείο καταγραφής εφαρμογών καταγράφει γεγονότα που δημιουργούνται από εφαρμογές που εκτελούνται στο σύστημα. Οι πληροφορίες που μπορεί να περιέχει είναι σφάλματα Εφαρμογών και προειδοποιήσεις. Ορισμένες φορές συμβάντα που σχετίζονται με την ασφάλεια εφαρμογών μπορεί να καταγράφονται και εδώ.

3. Καταγραφές συστήματος: Το αρχείο καταγραφής συστήματος καταγράφει γεγονότα που σχετίζονται με προγράμματα οδήγησης συσκευών και άλλο υλικό. Τα μηνύματα που περιλαμβάνει αφορούν την εκκίνηση του συστήματος και τον τερματισμό λειτουργίας του, σφάλματα προγραμμάτων οδήγησης και άλλες δραστηριότητες που σχετίζονται με το σύστημα. Δεν επικεντρώνεται στην ασφάλεια αλλά μπορεί να παρέχει πληροφορίες για τη αντιμετώπιση περιστατικών ασφαλείας.

Αναγνωριστικό συμβάντος- Event ID

Κάθε καταγραφή σε ένα Windows σύστημα συνδυάζεται με έναν μοναδικό αριθμό γνωστό σαν αναγνωριστικό συμβάντος (EventID). Τα αναγνωριστικά συμβάντων κατηγοριοποιούνται αντίστοιχα με το περιεχόμενο τους ώστε να υπάρχει η δυνατότητα αναζήτησης, φιλτραρίσματος και ανάλυσης των καταγραφών επιτυχημένα. Οι αναλυτές περιστατικών ασφαλείας συχνά ανατρέχουν σε αναγνωριστικά συμβάντων για την αντιμετώπιση ζητημάτων ασφαλείας.

Βασικές κατηγορίες συμβάντων ασφαλείας

1. Συμβάντα σύνδεσης και αποσύνδεσης: Τα αρχεία καταγραφής αποθηκεύουν πληροφορίες σχετικά με τη σύνδεση και την αποσύνδεση ενός χρήστη. Καταγράφονται τόσο επιτυχημένες όσο και αποτυχημένες προσπάθειες. Οι πληροφορίες αυτές βοηθούν στον έλεγχο μοτίβων και ταυτοποίησης χρηστών

2. Συμβάντα πρόσβασης αντικειμένου: Αυτά τα συμβάντα καταγράφουν πρόσβαση και αλλαγές σε αρχεία, φακέλους και άλλα αντικείμενα στο σύστημα. Παρέχουν μια διαδρομή ελέγχου για το ποιος είχε πρόσβαση σε ποιους πόρους και πότε.

3. Αλλαγές πολιτικής: Τα αρχεία καταγραφής ασφαλείας καταγράφουν αλλαγές σε πολιτικές ασφαλείας, αναθέσεις δικαιωμάτων χρήστη και ομάδων. Η παρακολούθηση των αλλαγών πολιτικής είναι απαραίτητη για τη διατήρηση μιας ασφαλούς υποδομής.

4. Διαχείριση λογαριασμών: Καταγράφονται συμβάντα που σχετίζονται με τη διαχείριση λογαριασμών χρηστών και ομάδων. Αυτό περιλαμβάνει τη δημιουργία λογαριασμού χρήστη, τη διαγραφή, τις αλλαγές κωδικού πρόσβασης και τις αλλαγές στις ομάδες του χρήστη.

5. Χρήση δικαιωμάτων: Τα αρχεία καταγραφής ασφαλείας μπορούν να περιέχουν πληροφορίες σχετικά με τη χρήση δικαιωμάτων χρήστη, βοηθώντας στον εντοπισμό κατάχρησης ή μη εξουσιοδοτημένης χρήσης αυξημένων δικαιωμάτων.

Διατήρηση και αποθήκευση

Τα αρχεία καταγραφής συμβάντων ασφαλείας των Windows αποθηκεύονται ως αρχεία καταγραφής συμβάντων με επέκταση .evtx. Οι οργανισμοί μπορούν να διαμορφώσουν πολιτικές διατήρησης αρχείων καταγραφής για να ελέγχουν το μέγεθος του αρχείου καταγραφής και τη διάρκεια διατήρησης των αρχείων καταγραφής. Οι στρατηγικές αρχειοθέτησης και δημιουργίας αντιγράφων ασφαλείας είναι απαραίτητες για τη διατήρηση ιστορικών δεδομένων ασφαλείας.

Εργαλείο προβολής συμβάντων

Η Microsoft παρέχει το εργαλείο προβολής συμβάντων, το οποίο προσφέρει μια γραφική απεικόνιση για την προβολή και τη διαχείριση αρχείων καταγραφής συμβάντων. Επιτρέπει στους χρήστες να φιλτράρουν, να αναζητούν και να αναλύουν αποτελεσματικά τα δεδομένα καταγραφής. Οι αναλυτές ασφαλείας και οι διαχειριστές χρησιμοποιούν συχνά τον Εργαλείο προβολής συμβάντων για ανάλυση αρχείων καταγραφής και αντιμετώπιση προβλημάτων.

Ενσωμάτωση με SIEM

Τα συστήματα πληροφοριών ασφαλείας και διαχείρισης συμβάντων (SIEM) συχνά ενσωματώνονται με αρχεία καταγραφής συμβάντων ασφαλείας των Windows. Τα SIEM ενισχύουν την ανάλυση αρχείων καταγραφής παρέχοντας δυνατότητες κεντρικής αποθήκευσης, συσχέτισης σε πραγματικό χρόνο, ειδοποίησης και αναφοράς. Αυτή η ενοποίηση είναι ζωτικής σημασίας για την αποτελεσματική παρακολούθηση της ασφάλειας και την αντιμετώπιση περιστατικών.

Θέματα απορρήτου

Ενώ τα αρχεία καταγραφής συμβάντων ασφαλείας των Windows είναι απαραίτητα για την ασφάλεια, μπορούν να περιέχουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια χρήστη. Οι κατάλληλοι έλεγχοι πρόσβασης και τα μέτρα κρυπτογράφησης είναι απαραίτητα για την προστασία των δεδομένων καταγραφής από μη εξουσιοδοτημένη πρόσβαση ή παραποίηση.

Συμπεράσματα

Συμπερασματικά, τα αρχεία καταγραφής συμβάντων ασφαλείας των Windows είναι ζωτικής σημασίας πόροι για οργανισμούς που επιδιώκουν να διατηρήσουν την ασφάλεια και τη συμμόρφωση των συστημάτων τους που βασίζονται στα Windows. Με αποτελεσματική παρακολούθηση και ανάλυση αυτών των αρχείων καταγραφής, οι οργανισμοί μπορούν να ανιχνεύουν και να ανταποκρίνονται σε συμβάντα ασφαλείας, να επιβάλλουν πολιτικές ασφαλείας και να διασφαλίζουν την ακεραιότητα των περιβαλλόντων πληροφορικής τους.

1.3 Διαχείριση πληροφοριών ασφαλείας και συμβάντων (SIEM)

Τα βασικά στοιχεία ενός συστήματος SIEM

Συλλογή δεδομένων: Τα συστήματα SIEM συλλέγουν τεράστιες ποσότητες δεδομένων από διαφορετικές πηγές. Αυτό περιλαμβάνει αρχεία καταγραφής από συσκευές δικτύου, διακομιστές, τείχη προστασίας, συστήματα ανίχνευσης εισβολών (IDS/IPS), και άλλα. Τα δεδομένα συλλέγονται σε πραγματικό.

Κανονικοποίηση δεδομένων: Τα δεδομένα που συλλέγονται συχνά κανονικοποιούνται για να διασφαλιστεί η συνέπεια. Αυτό περιλαμβάνει την τυποποίηση μορφών συμβάντων, χρονικών σημάνσεων και άλλων χαρακτηριστικών, καθιστώντας ευκολότερη την ανάλυση και τη συσχέτιση δεδομένων.

Αποθήκευση καταγραφής: Τα SIEM αποθηκεύουν τα δεδομένα σε ένα κεντρικό αποθετήριο για ιστορική ανάλυση και αναφορές συμμορφώσεων. Η αποθήκευση δεδομένων μπορεί να είναι εσωτερική, στο cloud ή σε υβριδικά περιβάλλοντα.

Ανάλυση και συσχέτιση δεδομένων: Τα SIEM χρησιμοποιούν μηχανές ανάλυσης και συσχέτισης δεδομένων για τον εντοπισμό προτύπων, ανωμαλιών και σχέσεων μεταξύ συμβάντων ασφαλείας. Αυτό βοηθά στον εντοπισμό πολύπλοκων επιθέσεων και πολλαπλών σταδίων.

Ειδοποιήσεις και ενημερώσεις: Τα SIEM παράγουν ειδοποιήσεις και ενημερώσεις όταν προκαθορισμένοι κανόνες ή μοτίβα υποδεικνύουν πιθανές απειλές ασφαλείας ή παραβιάσεις πολιτικής. Αυτές οι ειδοποιήσεις αποστέλλονται σε ομάδες ασφαλείας για περαιτέρω έρευνα και απάντηση.

Πίνακες εργαλείων και αναφορών: Τα SIEM παρέχουν προσαρμόσιμους πίνακες εργαλείων και δυνατότητες αναφορών. Αυτοί οι πίνακες ελέγχου προσφέρουν απεικονίσεις σε πραγματικό χρόνο των συμβάντων ασφαλείας και της κατάστασης συμμόρφωσης, ενώ οι αναφορές βοηθούν τους οργανισμούς να αποδείξουν τη συμμόρφωση με τις κανονιστικές απαιτήσεις.

Περιπτώσεις χρήσης των συστημάτων SIEM

Ανίχνευση απειλών: Το SIEM είναι οι ενορχηστρωτής για τον εντοπισμό πολλαπλών απειλών στον κυβερνοχώρο. Σε αυτές τις απειλές συμπεριλαμβάνονται το κακόβουλο λογισμικό, επιθέσεις ηλεκτρονικού ψαρέματος, παραβιάσεις δεδομένων και εσωτερικών απειλών. Πολλά από τα SIEM επιτρέπουν στους οργανισμούς να ανταποκρίνονται σε αυτές τις απειλές σε πραγματικό χρόνο.

Απόκριση συμβάντος: Τα συστήματα SIEM παίζουν μεγάλο ρόλο στην απόκριση των περιστατικών ασφαλείας, παρέχοντας λεπτομέρειες σχετικά με τα συμβάντα ασφαλείας. Οι πληροφορίες αυτές βοηθούν τις ομάδες ασφαλείας στην διερεύνηση των περιστατικών και τον προσδιορισμό της εξάπλωσης τους.

Διαχείριση συμμόρφωσης: Τα SIEM βοηθούν τους οργανισμούς να διατηρήσουν τη συμμόρφωση με τους κανονισμούς και τα πρότυπα του κλάδου. Παρακολουθούν τους ελέγχους ασφαλείας, δημιουργούν αναφορές συμμόρφωσης και παρέχουν αποδεικτικά στοιχεία συμμόρφωσης με τις πολιτικές ασφαλείας.

Διαχείριση αρχείων καταγραφής: Τα SIEM συγκεντρώνουν και διαχειρίζονται αρχεία καταγραφής από διαφορετικές πηγές. Αυτό απλοποιεί την αναζήτηση, την ανάλυση και τη μακροπρόθεσμη αποθήκευση αρχείων καταγραφής, τα οποία είναι απαραίτητα για τις εγκληματολογικές έρευνες και τους ελέγχους.

Προκλήσεις και προβληματισμοί

Πολλαπλές ειδοποιήσεις: Τα SIEM μπορούν να δημιουργήσουν πολλαπλές ειδοποιήσεις και είναι σημαντικό να υπάρχει συνεχής ρύθμιση ώστε να μειώνονται οι ψευδώς θετικές ειδοποιήσεις, ώστε οι αναλυτές να μπορούν να εστιάσουν σε πραγματικές απειλές.

Εξειδίκευση: Η διαχείριση και η δημιουργία ενός συστήματος SIEM απαιτεί εξειδίκευση στους τομείς της κυβερνοασφάλειας και σε λειτουργείς πληροφορικής. Απαιτείται εξειδικευμένο προσωπικό για να συντηρεί και να διαμορφώνει τα συστήματα όπως προβλέπεται από τους κατασκευαστές.

Κόστος: Οι λύσεις SIEM μπορεί να κοστίσουν πολλά χρήματα. Σε αυτά τα χρήματα περιλαμβάνεται η αρχική εγκατάσταση, το υλικό, οι άδειες χρήσης, η συνεχής συντήρηση αλλά και η αποθήκευση των καταγραφών. Οι οργανισμοί θα πρέπει να εξετάσουν προσεκτικά τον προϋπολογισμό και τις απαιτήσεις τους.

Εξέλιξη και τάσεις

Τεχνητή Νοημοσύνη και Μηχανική Μάθηση: Τα σύγχρονα SIEM ενσωματώνουν την τεχνητή νοημοσύνη και τη μηχανική μάθηση βελτιώνοντας τις δυνατότητες ανίχνευσης απειλών και μειώνοντας τα ψευδώς θετικά αποτελέσματα.

SIEM στο νέφος: Πολλές λύσεις SIEM έχουν εμφανιστεί και στο νέφος για να εξυπηρετήσουν οργανισμούς με υβριδικές υποδομές και υποδομές που βασίζονται στο νέφος. Προσφέρουν μεγαλύτερες ευελιξίες επεκτασιμότητας και είναι ιδανικά για δυναμικά περιβάλλοντα.

Ανάλυση συμπεριφοράς χρηστών και οντοτήτων (UEBA): Το UEBA ενσωματώνεται όλο και περισσότερο στα SIEM για τον εντοπισμό μη φυσιολογικών μοτίβων συμπεριφοράς χρηστών και οντοτήτων, βοηθώντας στον εντοπισμό εσωτερικών απειλών.

Ενσωμάτωση πληροφοριών απειλών: Τα SIEM ενσωματώνουν τροφοδοσίες πληροφοριών απειλών για τη βελτίωση της ανίχνευσης απειλών παρέχοντας πληροφορίες σε πραγματικό χρόνο για γνωστές απειλές και τρωτά σημεία.

Συμπεράσματα

Συμπερασματικά τα συστήματα SIEM είναι απαραίτητα εργαλεία για οργανισμούς που θέλουν να ενισχύσουν την ασφάλεια τους στον κυβερνοχώρο. Παρέχουν τα μέσα για τη συγκέντρωση δεδομένων ασφαλείας, στον εντοπισμό απειλών, τη διευκόλυνση της απόκρισης σε περιστατικά και τη διασφάλιση της συμμόρφωσης. Ωστόσο η επιτυχής εφαρμογή και λειτουργία ενός συστήματος SIEM απαιτεί προσεκτικό σχεδιασμό, εξειδικευμένο προσωπικό και δέσμευση για συνεχή συντήρηση και βελτιστοποίηση.

1.4 Κανόνες συσχέτισης

Οι κανόνες συσχέτισης αποτελούν θεμελιώδες στοιχείο των συστημάτων Διαχείρισης Πληροφοριών Ασφαλείας και Συμβάντων (SIEM) και παίζουν κρίσιμο ρόλο στον εντοπισμό πολύπλοκων απειλών ασφαλείας.

Κανόνες συσχέτισης στο SIEM

Ορισμός: Οι κανόνες συσχέτισης, είναι γνωστοί και ως αλγόριθμοι συσχέτισης ή κανόνες ανίχνευσης, είναι προκαθορισμένες ή προσαρμοσμένες λογικές δηλώσεις που χρησιμοποιούνται από συστήματα SIEM για την ανάλυση και τη συσχέτιση πολλαπλών συμβάντων ασφαλείας ή σημείων δεδομένων σε πραγματικό χρόνο. Αυτοί οι κανόνες βοηθούν τα SIEM να εντοπίζουν μοτίβα, ανωμαλίες και αλληλουχίες γεγονότων που μπορεί να υποδηλώνουν ένα περιστατικό ασφαλείας ή μια απειλή.

Σκοπός: Ο πρωταρχικός σκοπός των κανόνων συσχέτισης είναι να διερευνήσουν τον τεράστιο όγκο δεδομένων συμβάντων ασφαλείας που συλλέγονται από τα συστήματα SIEM και να εντοπίσουν δυνητικά κακόβουλες δραστηριότητες. Συσχετίζοντας μεμονωμένα συμβάντα ή σημεία δεδομένων, οι οργανισμοί μπορούν να εντοπίσουν απειλές που μπορεί να περάσουν απαρατήρητες κατά την ανάλυση γεγονότων μεμονωμένα.

Βασικά Χαρακτηριστικά

Αντιστοιχία μοτίβων: Οι κανόνες συσχέτισης χρησιμοποιούν τεχνικές αντιστοίχισης προτύπων για τον εντοπισμό συγκεκριμένων ακολουθιών γεγονότων ή μοτίβων δεδομένων που ευθυγραμμίζονται με γνωστά σενάρια επίθεσης ή ύποπτες συμπεριφορές.

Ανάλυση σε πραγματικό χρόνο: Οι κανόνες συσχέτισης εφαρμόζονται σε πραγματικό χρόνο καθώς τα συμβάντα ασφαλείας λαμβάνονται στο SIEM. Αυτό επιτρέπει την άμεση ανίχνευση και αντίδραση σε πιθανές απειλές.

Προσαρμογή: Οι οργανισμοί μπορούν να δημιουργήσουν προσαρμοσμένους κανόνες συσχέτισης ανάλογα με τις απαιτήσεις ασφαλείας και το περιβάλλον τους. Οι προσαρμοσμένοι κανόνες είναι συχνά απαραίτητοι για την αντιμετώπιση συγκεκριμένων απειλών ή αναγκών συμμόρφωσης.

Κοινοί τύποι κανόνων συσχέτισης

Συσχέτιση διαδοχικών γεγονότων: Αυτοί οι κανόνες προσδιορίζουν αλληλουχίες γεγονότων που, όταν συνδυάζονται, εγείρουν υποψίες. Για παράδειγμα, πολλές αποτυχημένες προσπάθειες σύνδεσης που ακολουθούνται από επιτυχή σύνδεση ενδέχεται να υποδηλώνουν επίθεση πολλαπλών δοκιμών σύνδεσης.

Συσχέτιση με βάση το όριο: Οι κανόνες με βάση τα όρια ενεργοποιούν ειδοποιήσεις όταν η συχνότητα ή ο όγκος συγκεκριμένων συμβάντων υπερβαίνει τα προκαθορισμένα όρια. Για παράδειγμα, μπορεί να δημιουργηθεί μια ειδοποίηση εάν ένας χρήστης κάνει έναν ασυνήθιστα υψηλό αριθμό αιτημάτων πρόσβασης σε αρχεία σε σύντομο χρονικό διάστημα.

Ομαδοποίηση συμβάντων: Οι κανόνες συσχέτισης μπορούν να ομαδοποιήσουν σχετικά συμβάντα που, όταν συνδυαστούν, υποδηλώνουν απειλή. Για παράδειγμα, μια σειρά από καταχωρίσεις αρχείου καταγραφής ενός τείχους προστασίας, που εμφανίζουν πολλαπλές εξερχόμενες συνδέσεις, σε γνωστές κακόβουλες διευθύνσεις IP μπορεί να υποδηλώνουν μόλυνση botnet.

Ανίχνευση ανωμαλίας: Ορισμένοι κανόνες συσχέτισης επικεντρώνονται στον εντοπισμό αποκλίσεων από τις καθορισμένες γραμμές βάσης. Για παράδειγμα, ένας κανόνας ανωμαλίας μπορεί να ειδοποιεί όταν ένας χρήστης αποκτά πρόσβαση σε πόρους με τους οποίους συνήθως δεν αλληλοεπιδρά.

Προκλήσεις και προβληματισμοί

Συντονισμός και ψευδώς θετικά αποτελέσματα: Ο συντονισμός των κανόνων είναι απαραίτητος για την μείωση των ψευδώς θετικών αποτελεσμάτων. Οι υπερβολικά ευαίσθητοι κανόνες μπορούν να κατακλύσουν τις ομάδες ασφαλείας με ειδοποιήσεις που μπορεί να μην είναι απειλές.

Συντήρηση κανόνων: Οι κανόνες συσχέτισης απαιτούν συνεχή συντήρηση για να παραμείνουν αποτελεσματικοί. Καθώς το οι απειλές εξελίσσονται, οι κανόνες μπορεί να χρειάζονται προσαρμογές και ενημερώσεις.

Πολυπλοκότητα κανόνων: Οι πολύπλοκοι κανόνες συσχέτισης μπορεί να απαιτούν υπολογιστικούς πόρους και να είναι δύσκολοι στη διαχείριση. Η απλότητα και η αποτελεσματικότητα πρέπει να εξισορροπούνται κατά τη δημιουργία κανόνων.

Πλεονεκτήματα

Πρώιμη ανίχνευση απειλών: Οι κανόνες συσχέτισης επιτρέπουν την έγκαιρη ανίχνευση εξελιγμένων απειλών που ενδέχεται να αποφύγουν τον εντοπισμό μέσω παρακολούθησης μεμονωμένων συμβάντων

Μειωμένες ειδοποιήσεις: Ομαδοποιώντας και συσχετίζοντας συμβάντα, τα συστήματα SIEM μπορούν να μειώσουν τον αριθμό των ειδοποιήσεων που παράγονται, βοηθώντας τις ομάδες ασφαλείας να επικεντρωθούν σε πραγματικές απειλές.

Προτεραιότητα συμβάντων: Οι κανόνες συσχέτισης βοηθούν στην ιεράρχηση των περιστατικών με βάση τη σοβαρότητα και τη συνάφειά τους, επιτρέποντας πιο αποτελεσματική απόκριση σε περιστατικά.

Συμπεράσματα

Οι κανόνες συσχέτισης είναι απαραίτητοι για τον εντοπισμό και την καταπολέμηση εξιδεικευμένων απειλών. Θα πρέπει να υπάρχει συνεχής συντήρηση τους για την αποφυγή ψευδός θετικών αποτελεσμάτων και θα πρέπει να τηρούνται οι οδηγίες δημιουργίας ώστε να μην επιβαρύνουν χωρίς λόγο το σύστημα SIEM μας.

1.5 Μέθοδοι ανίχνευσης επιθέσεων

Οι μέθοδοι ανίχνευσης επιθέσεων είναι τεχνικές και μηχανισμοί που χρησιμοποιούνται για τον εντοπισμό και την απόκριση σε κακόβουλες δραστηριότητες και κυβερνοεπιθέσεις σε συστήματα υπολογιστών, δίκτυα και ψηφιακά περιβάλλοντα. Αυτές οι μέθοδοι είναι απαραίτητες για τη διατήρηση της ασφάλειας και της ακεραιότητας των υποδομών τεχνολογίας πληροφοριών.

Βασικοί στόχοι

Πρώιμη αναγνώριση απειλής: Ανίχνευση επιθέσεων όσο το δυνατόν συντομότερα για την ελαχιστοποίηση πιθανών ζημιών και παραβιάσεων δεδομένων.

Ελαχιστοποίηση ψευδών θετικών: Μείωση του αριθμού των ψευδών ειδοποιήσεων για την αποφυγή συντριβής ομάδων ασφαλείας με μη κρίσιμες ειδοποιήσεις.

Ενίσχυση της απόκρισης σε περιστατικά: Παροχή πληροφοριών για τη διευκόλυνση της ταχείας και αποτελεσματικής απόκρισης και εξάλειψης των περιστατικών.

Παρακολούθηση και συμμόρφωση: Διασφάλιση ότι τα συστήματα και τα δίκτυα συμμορφώνονται με τις πολιτικές ασφαλείας, τους κανονισμούς και τα πρότυπα συμμόρφωσης.

Κοινές μέθοδοι ανίχνευσης επιθέσεων

Ανίχνευση βάση υπογραφών:

Ορισμός: Η ανίχνευση με βάση τις υπογραφές βασίζεται σε γνωστά μοτίβα ή υπογραφές γνωστών επιθέσεων. Αντιστοιχίζει τα εισερχόμενα δεδομένα ή τη συμπεριφορά με μια βάση δεδομένων με προκαθορισμένες υπογραφές επίθεσης.

Πλεονεκτήματα: Αποτελεσματικό στον εντοπισμό γνωστών απειλών, σχετικά χαμηλά ψευδώς θετικά.

Περιορισμοί: Αναποτελεσματικό έναντι νέων ή επιθέσεων μηδενικής ημέρας που δεν διαθέτουν γνωστές υπογραφές.

Ανίχνευση βάση ανωμαλιών:

Ορισμός: Η ανίχνευση που βασίζεται σε ανωμαλίες προσδιορίζει αποκλίσεις από τις καθιερωμένες βασικές γραμμές κανονικής συμπεριφοράς. Εγείρει ειδοποιήσεις όταν οι δραστηριότητες φαίνονται ασυνήθιστες ή απροσδόκητες.

Πλεονεκτήματα: Αποτελεσματικό στον εντοπισμό νέων και προηγουμένως μη ορατών απειλών, προσαρμοστικό στις αλλαγές τεχνικών επίθεσης.

Περιορισμοί: Μπορεί να δημιουργήσει ψευδώς θετικές ειδοποιήσεις για νόμιμες αποκλίσεις από τις γραμμές κανονικής συμπεριφοράς, απαιτεί ένα ισχυρό μοντέλο γραμμής βάσης.

Ανάλυση συμπεριφοράς:
Ορισμός: Η ανάλυση συμπεριφοράς παρακολουθεί τη συμπεριφορά των χρηστών, των εφαρμογών και των συστημάτων για τον εντοπισμό ανωμαλιών που μπορεί να υποδηλώνουν επίθεση.

Πλεονεκτήματα: Αποτελεσματικό στον εντοπισμό εσωτερικών απειλών, επιθέσεων μηδενικής ημέρας και εξελιγμένων απειλών.

Περιορισμοί: Είναι πολύπλοκο στη παραμετροποίηση του και μπορεί να δημιουργήσει ψευδώς θετικά αποτελέσματα.

Ευριστική Ανάλυση:
Ορισμός: Η ευρετική ανάλυση χρησιμοποιεί μεθόδους βασισμένες σε κανόνες ή αλγοριθμικές μεθόδους για τον εντοπισμό ύποπτων ή δυνητικά κακόβουλων δραστηριοτήτων με βάση προκαθορισμένα ευρετικά πρότυπα ή πρότυπα συμπεριφοράς.

Πλεονεκτήματα: Προσαρμόσιμο και προσαρμόσιμο σε συγκεκριμένα περιβάλλοντα, καλό για τον εντοπισμό προηγουμένως άγνωστων απειλών.

Περιορισμοί: Απαιτεί συνεχή βελτίωση και ρύθμιση και μπορεί να δημιουργήσει ψευδώς θετικά αποτελέσματα.

Μηχανική μάθηση και ανίχνευση βάσει τεχνητής νοημοσύνης:
Ορισμός: Οι τεχνικές μηχανικής μάθησης (ML) και τεχνητής νοημοσύνης (AI) χρησιμοποιούν αλγόριθμους για την ανάλυση τεράστιων ποσοτήτων δεδομένων και τον εντοπισμό μοτίβων ενδεικτικών επιθέσεων.

Πλεονεκτήματα: Αποτελεσματικό στον εντοπισμό περίπλοκων και εξελισσόμενων απειλών, μπορεί να προσαρμοστεί στις μεταβαλλόμενες τακτικές επίθεσης.

Περιορισμοί: Απαιτούνται μεγάλα και διαφορετικά σύνολα δεδομένων για εκπαίδευση, μπορεί να δημιουργήσει ψευδώς θετικά αποτελέσματα χωρίς ισχυρές βάσεις δεδομένων και μοντελοποίησης.

SIEM και ανάλυση καταγραφής:
Ορισμός: Συστήματα Ασφαλείας Πληροφοριών και Διαχείρισης Συμβάντων (SIEM) και εργαλεία ανάλυσης αρχείων καταγραφής συλλέγουν και αναλύουν δεδομένα καταγραφής από διάφορες πηγές για τον εντοπισμό και τη συσχέτιση συμβάντων ασφαλείας.

Πλεονεκτήματα: Κεντρική παρακολούθηση, συσχέτιση σε πραγματικό χρόνο και δυνατότητες ειδοποίησης.

Περιορισμοί: Εξάρτηση από ακριβή και έγκαιρα δεδομένα καταγραφής, πολυπλοκότητα στη διαμόρφωση κανόνων συσχέτισης.

Συστήματα ανίχνευσης εισβολής δικτύου (NIDS) και συστήματα ανίχνευσης εισβολής κεντρικού υπολογιστή (HIDS):

Ορισμός: Το NIDS και το HIDS είναι εξειδικευμένες λύσεις που παρακολουθούν την κυκλοφορία δικτύου και τις δραστηριότητες τερματικών, αντίστοιχα, για ενδείξεις εισβολής ή κακόβουλης συμπεριφοράς.

Πλεονεκτήματα: Επικεντρώνονται σε συγκεκριμένους φορείς επίθεσης, είναι αποτελεσματικά στον εντοπισμό απειλών σε επίπεδο δικτύου και τερματικών.

Περιορισμοί: Περιορίζονται στο εύρος της παρακολούθησής τους, ενδέχεται να μην εντοπίσουν επιθέσεις που συμβαίνουν και δεν είναι στο πεδίο ελέγχου τους.

Συμπεράσματα

Η εξισορρόπηση της ακρίβειας ανίχνευσης με τα ψευδώς θετικά ποσοστά είναι μια συνεχής πρόκληση στον εντοπισμό επιθέσεων.

Η συνεχής παρακολούθηση και οι τακτικές ενημερώσεις είναι απαραίτητες για την προσαρμογή στις εξελισσόμενες απειλές.

Το απόρρητο και τα νομικά ζητήματα πρέπει να λαμβάνονται υπόψη κατά την εφαρμογή ορισμένων μεθόδων ανίχνευσης, ειδικά εκείνων που αφορούν την παρακολούθηση της συμπεριφοράς των χρηστών.

Κεφάλαιο 2

2.1 Προτεινόμενα Συστήματα Ασφαλείας Πληροφοριών και Διαχείρισης Συμβάντων (SIEM)

Υπάρχουν πολλά αξιόπιστα συστήματα SIEM διαθέσιμα στην αγορά, το καθένα με το δικό του σύνολο χαρακτηριστικών και δυνατοτήτων. Ακολουθούν μερικά αξιοσημείωτα συστήματα SIEM:

IBM QRadar

Προμηθευτής: IBM Security

Βασικά Χαρακτηριστικά: Το QRadar είναι γνωστό για τις ισχυρές του ικανότητες στον εντοπισμό απειλών, την παρακολούθηση σε πραγματικό χρόνο και την απόκριση σε περιστατικά ασφαλείας. Προσφέρει προηγμένα στατιστικά στοιχεία, ανίχνευση ανωμαλιών και ενσωματωμένη ευφυΐα απειλών. Οι πληροφορίες ασφαλείας και οι λειτουργίες διαχείρισης συμβάντων του QRadar εκτιμώνται ιδιαίτερα για την επεκτασιμότητα και την αποτελεσματικότητά τους.

Splunk Enterprise Security

Προμηθευτής: Splunk

Βασικά Χαρακτηριστικά: Το Splunk είναι γνωστό για τις δυνατότητες διαχείρισης και ανάλυσης αρχείων καταγραφής.

Το Splunk Enterprise Security βασίζεται σε αυτό το θεμέλιο παρέχοντας δυνατότητες SIEM. Προσφέρει συσχέτιση συμβάντων σε πραγματικό χρόνο, ενσωμάτωση πληροφοριών απειλών, προσαρμόσιμους πίνακες εργαλείων και δυνατότητες αναζήτησης φιλικές προς το χρήστη. Το Splunk είναι γνωστό για την ευελιξία και την επεκτασιμότητα του.

LogRhythm

Προμηθευτής: LogRhythm

Βασικά Χαρακτηριστικά: Η LogRhythm προσφέρει μια ολοκληρωμένη πλατφόρμα SIEM με χαρακτηριστικά όπως παρακολούθηση σε πραγματικό χρόνο, αναλύσεις συμπεριφοράς, ευφυΐα απειλών και αυτοματοποίηση. Είναι γνωστό για τη φιλική προς τον χρήστη διεπαφή και τις προηγμένες δυνατότητες αναφοράς. Το LogRhythm παρέχει επίσης δυνατότητες παρακολούθησης και απόκρισης τελικού σημείου.

AlienVault USM Anywhere

Προμηθευτής: AlienVault

Βασικά χαρακτηριστικά: Το AlienVault USM Anywhere είναι μια λύση SIEM που βασίζεται στο υπολογιστικό σύννεφο που παρέχει ανίχνευση απειλών σε πραγματικό χρόνο, ανακάλυψη στοιχείων, αξιολόγηση ευπαθειών και παρακολούθηση συμπεριφοράς. Προσφέρει ενσωματωμένη ευφυΐα απειλών και λειτουργίες απόκρισης συμβάντων.

Elastic Security (formerly Elasticsearch ELK Stack with Elastic SIEM)

Προμηθευτής: Elastic

Βασικά χαρακτηριστικά: Το Elastic Security συνδυάζει το ELK Stack (Elasticsearch, Logstash και Kibana) με πρόσθετα χαρακτηριστικά ασφαλείας για να παρέχει δυνατότητες SIEM. Επιπροσθέτως παρέχει τη δυνατότητα ανάλυση αρχείων καταγραφής, ανίχνευση απειλών και δυνατότητες απεικόνισης.

Exabeam Security Management Platform

Προμηθευτής: Exabeam

Βασικά χαρακτηριστικά: Το Exabeam αναγνωρίζεται για τις δυνατότητές του στο User and Entity Behavior Analytics (UEBA). Επικεντρώνεται στον εντοπισμό εσωτερικών απειλών και προηγμένων επιθέσεων αναλύοντας τη συμπεριφορά των χρηστών. Η πλατφόρμα χρησιμοποιεί μηχανική μάθηση για να δημιουργήσει βασικές γραμμές κανονικής συμπεριφοράς και να εντοπίσει ανωμαλίες.

Microsoft Azure Sentinel

Προμηθευτής: Microsoft

Βασικά χαρακτηριστικά: Το Azure Sentinel είναι η εγγενής λύση SIEM της Microsoft στο cloud. Έχει σχεδιαστεί για να λειτουργεί άψογα με τις άλλες υπηρεσίες cloud της Microsoft, καθιστώντας το μια φυσική επιλογή για οργανισμούς με ισχυρό οικοσύστημα της Microsoft. Το Azure Sentinel αξιοποιεί την τεχνητή νοημοσύνη και την αυτοματοποίηση για τον εντοπισμό και την απόκριση απειλών.

Rapid7 InsightIDR

Προμηθευτής: Rapid7

Βασικά χαρακτηριστικά: Το Rapid7 InsightIDR είναι μια λύση SIEM που βασίζεται σε σύννεφο και δίνει έμφαση στην ανάλυση χρηστών και τελικών σημείων. Προσφέρει δυνατότητες ανίχνευσης, διερεύνησης και αυτοματισμού απειλών, καθιστώντας το κατάλληλο για οργανισμούς με απομακρυσμένο εργατικό δυναμικό.

2.2 Προδιαγραφές χρήσης συστήματος SIEM QRadar Community Edition (CE)

Το IBM QRadar Community Edition (CE) είναι μια δωρεάν έκδοση της λύσης διαχείρισης πληροφοριών και συμβάντων ασφαλείας QRadar της IBM (SIEM) που επιτρέπει σε άτομα και μικρούς οργανισμούς να εξερευνούν και να χρησιμοποιούν τις δυνατότητες του QRadar.

Ακολουθούν οι απαιτήσεις συστήματος για το IBM QRadar CE

Ελάχιστες απαιτήσεις υλικού

Ελάχιστες απαιτήσεις μνήμης

Απαιτούνται τουλάχιστον 8 GB RAM ή 10 GB όταν περιλαμβάνονται εφαρμογές.

Ελάχιστος χώρος στο δίσκο

Προτείνονται τουλάχιστον 250 GB διαθέσιμου χώρου στο δίσκο.

Ελάχιστες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει τουλάχιστον 2 πυρήνες για βέλτιστη απόδοση.

Συνδεσιμότητα δικτύου

Είναι επιτακτική ανάγκη να υπάρχει τουλάχιστον ένας προσαρμογέας δικτύου με πρόσβαση στο Διαδίκτυο.

Διαμόρφωση διευθύνσεων IP

Η εγκατάσταση του QRadar Community Edition απαιτεί τόσο στατικές δημόσιες όσο και ιδιωτικές διευθύνσεις IP.

Προδιαγραφές ονόματος κεντρικού υπολογιστή

Το εκχωρημένο όνομα κεντρικού υπολογιστή πρέπει να είναι ένα πλήρως αναγνωρισμένο όνομα τομέα.

Προτεινόμενες απαιτήσεις υλικού

Προτεινόμενες απαιτήσεις μνήμης

Προτείνονται τουλάχιστον 16 GB RAM ή 20 GB όταν περιλαμβάνονται εφαρμογές.

Προτεινόμενος χώρος στο δίσκο

Προτείνονται τουλάχιστον 500 GB διαθέσιμου χώρου στο δίσκο.

Προτεινόμενες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει 6 πυρήνες για βέλτιστη απόδοση.

Συνδεσιμότητα δικτύου

Είναι επιτακτική ανάγκη να υπάρχει τουλάχιστον ένας προσαρμογέας δικτύου με πρόσβαση στο Διαδίκτυο.

Διαμόρφωση διευθύνσεων IP

Η εγκατάσταση του QRadar Community Edition απαιτεί τόσο στατικές δημόσιες όσο και ιδιωτικές διευθύνσεις IP.

Προδιαγραφές ονόματος κεντρικού υπολογιστή

Το εκχωρημένο όνομα κεντρικού υπολογιστή πρέπει να είναι ένα πλήρως αναγνωρισμένο όνομα τομέα.

2.3 Προδιαγραφές Windows Server

Απαιτήσεις συστήματος για Windows Server 2016 (Standard and Datacenter εκδόσεις)

Σημείωση: Τα ακόλουθα είναι γενικές απαιτήσεις συστήματος. Οι συγκεκριμένες απαιτήσεις υλικού και πόρων ενδέχεται να διαφέρουν ανάλογα με το φόρτο εργασίας, τον αριθμό των χρηστών και τις δυνατότητες που θα εγκατασταθούν .

Ελάχιστες απαιτήσεις (χωρίς ρόλο ελεγκτή τομέα)

Ελάχιστες απαιτήσεις μνήμης

Απαιτούνται τουλάχιστον 512 MB RAM

Ελάχιστος χώρος στο δίσκο

Προτείνονται τουλάχιστον 32 GB διαθέσιμου χώρου στο δίσκο για την εγκατάσταση του λειτουργικού συστήματος. Ενδέχεται να απαιτείται επιπλέον χώρος για ενημερώσεις και αρχεία συστήματος

Ελάχιστες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει τουλάχιστον 1 πυρήνα με ταχύτητα 1,4 GHz και αρχιτεκτονική 64-bit.

Συνδεσιμότητα δικτύου

Είναι επιτακτική ανάγκη να υπάρχει τουλάχιστον ένας προσαρμογέας δικτύου με πρόσβαση στο Διαδίκτυο.

Προτεινόμενες απαιτήσεις (χωρίς ρόλο ελεγκτή τομέα)

Προτεινόμενες απαιτήσεις μνήμης

Προτείνονται τουλάχιστον 2 GB RAM

Προτεινόμενος χώρος στο δίσκο

Προτείνονται τουλάχιστον 40 GB διαθέσιμου χώρου στο δίσκο για την εγκατάσταση του λειτουργικού συστήματος. Ενδέχεται να απαιτείται επιπλέον χώρος για ενημερώσεις και αρχεία συστήματος.

Προτεινόμενες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει τουλάχιστον 2 πυρήνες με ταχύτητα 3,1 GHz και αρχιτεκτονική 64-bit.

Συνδεσιμότητα δικτύου

Είναι επιτακτική ανάγκη να υπάρχει τουλάχιστον ένας προσαρμογέας δικτύου με πρόσβαση στο Διαδίκτυο.

Ελάχιστες απαιτήσεις (με ρόλο ελεγκτή τομέα)

Ελάχιστες απαιτήσεις μνήμης

Απαιτούνται τουλάχιστον 2 GB RAM

Ελάχιστος χώρος στο δίσκο

Προτείνονται τουλάχιστον 32 GB διαθέσιμου χώρου στο δίσκο για την εγκατάσταση του λειτουργικού συστήματος. Ενδέχεται να απαιτείται επιπλέον χώρος για ενημερώσεις και αρχεία συστήματος

Ελάχιστες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει τουλάχιστον 1 πυρήνα με ταχύτητα 1,4 GHz και αρχιτεκτονική 64-bit.

Συνδεσιμότητα δικτύου

Είναι επιτακτική ανάγκη να υπάρχει τουλάχιστον ένας προσαρμογέας δικτύου με πρόσβαση στο Διαδίκτυο.

Προτεινόμενες απαιτήσεις (με ρόλο ελεγκτή τομέα)

Προτεινόμενες απαιτήσεις μνήμης

Προτείνονται τουλάχιστον 4 GB RAM

Προτεινόμενος χώρος στο δίσκο

Προτείνονται τουλάχιστον 40 GB διαθέσιμου χώρου στο δίσκο για την εγκατάσταση του λειτουργικού συστήματος. Ενδέχεται να απαιτείται επιπλέον χώρος για ενημερώσεις και αρχεία συστήματος.

Προτεινόμενες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει τουλάχιστον 2 πυρήνες με ταχύτητα 3,1 GHz και αρχιτεκτονική 64-bit.

Συνδεσιμότητα δικτύου

Είναι επιτακτική ανάγκη να υπάρχει τουλάχιστον ένας προσαρμογέας δικτύου με πρόσβαση στο Διαδίκτυο.

2.4 Προδιαγραφές Windows 10 Pro workstation (Vulnerable Host)

Ελάχιστες απαιτήσεις Windows 10 Pro

Ελάχιστες απαιτήσεις μνήμης

Απαιτούνται Τουλάχιστον 2 GB για συστήματα 64 bit ή 1 GB για συστήματα 32 bit

Ελάχιστος χώρος στο δίσκο

Προτείνονται τουλάχιστον μια μονάδα δίσκου συστήματος με τουλάχιστον 64 GB διαθέσιμου ελεύθερου χώρου. Ενδέχεται να απαιτείται πρόσθετος χώρος αποθήκευσης για την υποδοχή ενημερώσεων λογισμικού, εφαρμογών και δεδομένων που δημιουργούνται από τον χρήστη

Ελάχιστες προδιαγραφές CPU

Επεξεργαστής με ελάχιστη ταχύτητα ρολογιού 1 GHz, που διαθέτει τουλάχιστον δύο πυρήνες.

Ελάχιστες προδιαγραφές GPU

Συσκευή γραφικών συμβατή με DirectX 9 ή μεταγενέστερη.

Ανάλυση οθόνης

Οθόνη που μπορεί να αποδώσει ελάχιστη ανάλυση 800 x 600 pixel.

Προτεινόμενες απαιτήσεις Windows 10 Pro

Προτεινόμενες απαιτήσεις μνήμης

Προτείνονται τουλάχιστον 4 GB RAM για συστήματα 64-bit.

Προτεινόμενος χώρος στο δίσκο

Προτείνονται τουλάχιστον μια μονάδα δίσκου συστήματος με τουλάχιστον 128 GB διαθέσιμου ελεύθερου χώρου για βελτιωμένη απόδοση. Ενδέχεται να απαιτείται πρόσθετος χώρος αποθήκευσης για την υποδοχή ενημερώσεων λογισμικού, εφαρμογών και δεδομένων που δημιουργούνται από τον χρήστη

Προτεινόμενες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει τουλάχιστον 4 πυρήνες με ταχύτητα 2 GHz και αρχιτεκτονική 64-bit.

Ελάχιστες προδιαγραφές GPU

Συσκευή γραφικών συμβατή με DirectX 9 ή μεταγενέστερη.

Ανάλυση οθόνης

Μια οθόνη που μπορεί να αποδώσει ανάλυση 800 x 600 pixel ή μεγαλύτερη.

Συνδεσιμότητα δικτύου

Συνιστάται αξιόπιστη σύνδεση στο Διαδίκτυο για τη λήψη ενημερώσεων, την πρόσβαση σε διαδικτυακές υπηρεσίες και τη βελτίωση της συνολικής εμπειρίας χρήστη.

2.5 Προδιαγραφές Windows 10 Pro workstation (WinCollect Service)

Κατά την εγκατάσταση του WinCollect και τη διαμόρφωση της απομακρυσμένης παραλαβής πακέτων από άλλους κεντρικούς υπολογιστές σε περιβάλλον Windows, θα πρέπει να λάβουμε υπόψη τις απαιτήσεις συστήματος για τα Windows 10 και τις συγκεκριμένες απαιτήσεις για το την εφαρμογή WinCollect.

Προτεινόμενες προδιαγραφές CPU

Το σύστημα προτείνεται να έχει τουλάχιστον Intel Core i3 ή αντίστοιχο επεξεργαστή. Χρήση 0 – 35% του επεξεργαστή αναλόγως την ποσότητα των τερματικών που λαμβάνουμε δεδομένα.

Προτεινόμενες απαιτήσεις μνήμης

Προτείνονται τουλάχιστον 2-4 GB RAM για συστήματα 64-bit. Κατά προσέγγιση η μία καταγραφή ανά δευτερόλεπτο (Event Per Second - EPS) κοστίζει 10 MB μνήμης.

Προτεινόμενος χώρος στο δίσκο

100 MB για το λογισμικό και έως 100 MB για τα αρχεία. Ενδέχεται να απαιτούνται έως και 6 GB εάν τα συμβάντα αποθηκεύονται στο δίσκο.

Συνδεσιμότητα δικτύου

Επικοινωνία του Wincollect Agent με την κονσόλα του QRadar.

Όλοι οι WinCollect Agents επικοινωνούν με την κονσόλα QRadar για να προωθήσουν συμβάντα και ζητήσουν ενημερωμένες πληροφορίες. Οι WinCollect Agents που διαχειρίζονται από την κονσόλα ζητούν επίσης και λαμβάνουν ενημερωμένες αλλαγές κώδικα και διαμόρφωσης. Πρέπει να εξασφαλιστεί η επικοινωνία QRadar και WinCollect Agent σε επίπεδο τοπικών και εσωτερικών τοίχων προστασίας ώστε να επιτρέπεται η επικοινωνία στις ακόλουθες θύρες:

Θύρα 8413

Αυτή η θύρα χρησιμοποιείται για τη διαχείριση των WinCollect Agents για αίτηση και λήψη κώδικα διαμόρφωσης και ενημερώσεις. Η κίνηση ξεκινά πάντα από τον πράκτορα WinCollect και αποστέλλεται μέσω TCP. Η επικοινωνία είναι κρυπτογραφημένη χρησιμοποιώντας το δημόσιο κλειδί της κονσόλας QRadar και το αρχείο ConfigurationServer.PEM στο μέσο.

Θα πρέπει να δημιουργηθεί ένας κανόνας αμφίδρομης κατεύθυνσης για να επιτρέπεται η επικοινωνία από τον WinCollect Agent στο QRadar στη θύρα 8413.

Εάν ο κανόνας δεν είναι αμφίδρομος, η κυκλοφορία αποκλείεται. Το QRadar δεν θα αποστέλλει ενημερώσεις στο WinCollect πράκτορας στη θύρα 8413.

Θύρα 514

Αυτή η θύρα χρησιμοποιείται από τον πράκτορα WinCollect για να προωθήσει συμβάντα syslog στο QRadar.

Μπορείτε να διαμορφώσετε τις πηγές καταγραφής WinCollect ώστε να χρησιμοποιούν TCP ή UDP. Μπορείτε να αποφασίσετε ποιο πρωτόκολλο μετάδοσης θα χρησιμοποιήσετε για κάθε πηγή καταγραφής WinCollect. Η κίνηση της θύρας 514 ξεκινά πάντα από τον WinCollect Agent.

Οι WinCollect Agents που λαμβάνουν δεδομένα από απομακρυσμένα συστήματα Windows απαιτούν επιπλέον ανοιχτές θύρες επικοινωνίας. Οι παρακάτω θύρες θα πρέπει να είναι ανοιχτές στον υπολογιστή με τον Wincollect Agent και στους υπολογιστές που θα λαμβάνονται δεδομένα εξ αποστάσεως. Παρακάτω περιγράφονται οι θύρες που χρησιμοποιούνται.

- 135 – TCP - Microsoft Endpoint Mapper
- 137 – TCP - NetBIOS name service
- 138 – TCP - NetBIOS datagram service
- 139 – TCP - NetBIOS session service
- 445 – TCP - Microsoft Directory Services for file transfers that use Windows share
- 49152 - 65535 – TCP - Default dynamic port range for TCP/IP

Το πρωτόκολλο MSEVEN χρησιμοποιεί τη θύρα 445.

Οι θύρες NETBIOS (137 - 139) μπορούν να χρησιμοποιηθούν για την ανάλυση ονόματος κεντρικού υπολογιστή.

Όταν ο WinCollect Agent προσπαθεί να αποκτήσει ένα απομακρυσμένο αρχείο καταγραφής συμβάντων χρησιμοποιώντας το MSEVEN6, η αρχική επικοινωνία με το απομακρυσμένο

μηχάνημα πραγματοποιείται στη θύρα 135 (δυναμική αντιστοίχιση θυρών), η οποία εκχωρεί τη σύνδεση σε μια δυναμική θύρα.

Το προεπιλεγμένο εύρος θυρών για δυναμικές θύρες είναι μεταξύ της θύρας 49152 και της θύρας 65535, αλλά ενδέχεται να διαφέρει ανάλογα με τον τύπο διακομιστή. Για παράδειγμα, οι διακομιστές Exchange έχουν ρυθμιστεί για μια περιοχή θυρών 6005 – 58321 από προεπιλογή.

Για να επιτρέψετε την κυκλοφορία σε αυτές τις δυναμικές θύρες, ενεργοποιήστε και επιτρέψτε τους δύο ακόλουθους εισερχόμενους κανόνες στον απομακρυσμένο διακομιστή Windows

- Απομακρυσμένη διαχείριση αρχείων καταγραφής συμβάντων (RPC)
- Απομακρυσμένη διαχείριση αρχείων καταγραφής συμβάντων (RPC-EPMAP)

2.6 Προδιαγραφές Kali Linux

Το Kali Linux είναι μια εξειδικευμένη διανομή Linux που έχει σχεδιαστεί κυρίως για δοκιμές διείσδυσης, ηθικό hacking και εργασίες ασφάλειας στον κυβερνοχώρο. Ακολουθούν οι ελάχιστες και προτεινόμενες απαιτήσεις συστήματος για την εκτέλεση του Kali Linux.

Ελάχιστες απαιτήσεις συστήματος για Kali Linux

Επεξεργαστής (CPU)

Επεξεργαστής Pentium 4 1 GHz ή αντίστοιχος.

RAM

1 GB (για αρχιτεκτονική 32 bit) ή 2 GB (για αρχιτεκτονική 64 bit).

Αποθήκευση

Τουλάχιστον 20 GB διαθέσιμου χώρου στον σκληρό δίσκο για την εγκατάσταση. Πρόσθετος χώρος αποθήκευσης είναι απαραίτητος για τη διατήρηση δεδομένων, εργαλείων και εφαρμογών.

Γραφικά

Κάρτα γραφικών και οθόνη με ελάχιστη ανάλυση 800x600 pixel.

Δίκτυο

Διασύνδεση Ethernet ή κάρτα Wi-Fi με κατάλληλα προγράμματα οδήγησης και δυνατότητες για ασύρματη δικτύωση.

Προτεινόμενες Απαιτήσεις Συστήματος για Kali Linux:

Επεξεργαστής (CPU)

Ένας επεξεργαστής πολλαπλών πυρήνων με ταχύτητα ρολογιού τουλάχιστον 2 GHz συνιστάται για βελτιωμένη λειτουργική απόδοση, ιδιαίτερα κατά την εκτέλεση εργασιών με έντονη χρήση πόρων.

RAM

Συνιστώνται 4 GB ή περισσότερα για πιο ομαλή λειτουργία, ειδικά όταν εκτελείτε πολλά εργαλεία ή εικονικές μηχανές.

Αποθήκευση

40 GB διαθέσιμου χώρου στο σκληρό δίσκο ή περισσότερο παρέχει άφθονο χώρο αποθήκευσης για εργαλεία, δεδομένα και εφαρμογές. Πρόσθετος χώρος αποθήκευσης είναι απαραίτητος για τη διατήρηση δεδομένων, εργαλείων και εφαρμογών.

Γραφικά

Κάρτα γραφικών και οθόνη με υψηλότερη ανάλυση (π.χ. 1024x768 ή μεγαλύτερη) για καλύτερη οπτική ευκρίνεια.

Δίκτυο

Διασύνδεση Ethernet ή κάρτα Wi-Fi με κατάλληλα προγράμματα οδήγησης και δυνατότητες για ασύρματη δικτύωση.

Κεφάλαιο 3

3.1 Περιγραφή Υλοποίησης

Στο τρίτο κεφάλαιο της παρούσας διπλωματικής εργασίας, παρουσιάζονται λεπτομερώς οι διαδικασίες εγκατάστασης και παραμετροποίησης των χρησιμοποιούμενων συστημάτων. Η υλοποίηση πραγματοποιήθηκε σε εικονικές μηχανές, βασιζόμενες στα προϊόντα της VMWare.

Συνοπτικά παρουσιάζονται οι παρακάτω διαδικασίες:

1. Ρύθμιση των αρχείων καταγραφής, με λεπτομερή ανάλυση και περιγραφή κάθε διαθέσιμης επιλογής.
2. Ρύθμιση του συστήματος QRadar και προετοιμασία για λήψη καταγραφών από συστήματα Windows.
3. Ρύθμιση ενός συστήματος Windows 10 με τον εγκατεστημένο Wincollect agent ως ενδιάμεσος μεσολαβητής μεταξύ QRadar και Windows.
4. Ρύθμιση ενός Windows Server 2016 που έχει εξελιχθεί σε ελεγκτή τομέα (Domain Controller).
5. Ρύθμιση ενός παλαιού Windows 10 με σκοπό τη δημιουργία ευπαθειών και κενών ασφαλείας για ευαισθησία σε επιθέσεις.
6. Ρύθμιση της μηχανής επίθεσης, η οποία σε αυτήν την περίπτωση είναι ένα Kali Linux.

3.2 Παραμετροποίηση των αρχείων καταγραφής – Audit Logs Configuration

Τα αρχεία καταγραφής ελέγχου είναι μια θεμελιώδης πτυχή της διατήρησης της ασφάλειας και της συμμόρφωσης των διακομιστών Windows. Οι σωστά διαμορφωμένες πολιτικές ελέγχου επιτρέπουν στους οργανισμούς να παρακολουθούν και να καταγράφουν κρίσιμα συμβάντα ασφαλείας, επιτρέποντάς τους να εντοπίζουν ύποπτες δραστηριότητες, να διεξάγουν εγκληματολογική ανάλυση και να πληρούν τις κανονιστικές απαιτήσεις.

Για να παραμετροποιήσουμε τις πολιτικές των αρχείων καταγραφής ακολουθούμε τα παρακάτω βήματα: Αναζητούμε εισάγοντας “gpedit.msc” στην αναζήτηση της έναρξης, για τοπικές πολιτικές ή μέσω των Αντικειμένων πολιτικής ομάδας του Active Directory για πολιτικές σε επίπεδο τομέα.

Μεταβαίνουμε στην επιλογή "Προηγμένη διαμόρφωση πολιτικής ελέγχου" στην ενότητα "Διαμόρφωση υπολογιστή" και "Ρυθμίσεις ασφαλείας" για τοπικές πολιτικές ή εντός των αντικειμένων πολιτικής ομάδας του τομέα σας.

Account Logon – Σύνδεση λογαριασμού

Credential Validation - Επικύρωση διαπιστευτηρίων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από δοκιμές επικύρωσης στα διαπιστευτήρια σύνδεσης των λογαριασμών χρήστη. Τα συμβάντα αυτής της υποκατηγορίας εμφανίζονται μόνο στον υπολογιστή που είναι υπεύθυνος για αυτά τα διαπιστευτήρια. Για λογαριασμούς τομέα, υπεύθυνος είναι ο ελεγκτής τομέα. Για τοπικούς λογαριασμούς, υπεύθυνος είναι ο τοπικός υπολογιστής.

Αριθμός συμβάντων: Υψηλός σε ελεγκτές τομέα.

Προεπιλογή για εκδόσεις υπολογιστή-πελάτη: Χωρίς έλεγχο.

Προεπιλογή για εκδόσεις διακομιστή: Επιτυχία.

Kerberos Authentication Service - Υπηρεσία ελέγχου ταυτότητας Kerberos

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από αιτήσεις εκχώρησης εισιτηρίων (TGT) του Kerberos. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου μετά από μια αίτηση TGT ελέγχου ταυτότητας του Kerberos. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες αιτήσεις και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες αιτήσεις. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου μετά από μια αίτηση TGT ελέγχου ταυτότητας του Kerberos.

Αριθμός συμβάντων: Υψηλός σε διακομιστές διανομής κλειδιών Kerberos.

Προεπιλογή για εκδόσεις υπολογιστή-πελάτη: Χωρίς έλεγχο.

Προεπιλογή για εκδόσεις διακομιστή: Χωρίς έλεγχο.

Kerberos Service Ticket Operations - Λειτουργίες δελτίων από υπηρεσία Kerberos

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται από αιτήσεις εκχώρησης δελτίων ελέγχου ταυτότητας (TGT) του Kerberos που υποβάλλονται για λογαριασμούς χρηστών. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που υποβάλλονται αιτήσεις ελέγχου ταυτότητας TGT του Kerberos για λογαριασμούς χρηστών. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες αιτήσεις και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες αιτήσεις. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου μετά από μια αίτηση ελέγχου ταυτότητας TGT του Kerberos για ένα λογαριασμό χρήστη.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή για εκδόσεις υπολογιστή-πελάτη: Χωρίς έλεγχο.

Προεπιλογή για εκδόσεις διακομιστή: Επιτυχία.

Other Account Logon Events - Άλλα συμβάντα σύνδεσης λογαριασμών

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται από αποκρίσεις σε αιτήσεις διαπιστευτηρίων που υποβάλλονται για τη σύνδεση λογαριασμών χρηστών, τα οποία δεν σχετίζονται με την επικύρωση διαπιστευτηρίων ή με τα εισιτήρια του Kerberos. Προς το παρόν, δεν υπάρχουν συμβάντα σε αυτήν την υποκατηγορία.

Προεπιλογή: Χωρίς έλεγχο.

Account Management – Διαχείριση λογαριασμού

Application Group Management - Διαχείριση ομάδων εφαρμογών

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγξετε συμβάντα που δημιουργούνται από αλλαγές σε ομάδες εφαρμογών, όπως είναι οι εξής:

- Δημιουργία, αλλαγή ή διαγραφή μιας ομάδας εφαρμογών.
- Προσθήκη ή κατάργηση ενός μέλους από μια ομάδα εφαρμογών.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής μιας ομάδας εφαρμογών. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές σε μια ομάδα εφαρμογών.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

Computer Account Management - Διαχείριση λογαριασμού υπολογιστή

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται από αλλαγές σε λογαριασμούς υπολογιστών, όπως η δημιουργία, η αλλαγή ή η διαγραφή ενός λογαριασμού υπολογιστή. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής ενός λογαριασμού υπολογιστή. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές σε ένα λογαριασμό υπολογιστή.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή για εκδόσεις υπολογιστή-πελάτη: Χωρίς έλεγχο.

Προεπιλογή για εκδόσεις διακομιστή: Επιτυχία.

Distribution Group Management - Διαχείριση ομάδων διανομής

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται από αλλαγές στις ομάδες διανομής, όπως είναι οι εξής:

- Δημιουργία, αλλαγή ή διαγραφή μιας ομάδας διανομής.
- Προσθήκη ή κατάργηση ενός μέλους από μια ομάδα διανομής.
- Αλλαγή του τύπου της ομάδας διανομής.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής μιας ομάδας διανομής. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές σε μια ομάδα διανομής.

Σημείωση: τα συμβάντα αυτής της υποκατηγορίας καταγράφονται μόνο σε ελεγκτές τομέα.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

Other Account Management Events - Άλλα συμβάντα διαχείρισης λογαριασμών

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγξετε συμβάντα που έχουν δημιουργηθεί από αλλαγές λογαριασμών χρηστών που δεν καλύπτονται από αυτήν την κατηγορία, όπως είναι τα εξής:

- Προσπελάστηκε ο κατακερματισμός του κωδικού πρόσβασης ενός λογαριασμού χρήστη. Αυτό συμβαίνει συνήθως κατά τη μετεγκατάσταση ενός κωδικού πρόσβασης του εργαλείου διαχείρισης του Active Directory.
- Έγινε κλήση στο API ελέγχου πολιτικής κωδικού πρόσβασης. Οι κλήσεις προς αυτή τη συνάρτηση ενδέχεται να αποτελούν μέρος μιας επίθεσης κατά τη διάρκεια της οποίας μια κακόβουλη εφαρμογή δοκιμάζει την πολιτική προκειμένου να μειώσει τον αριθμό των προσπαθειών ως μέρος μιας επίθεσης με χρήση λεξικού.
- Έχουν γίνει αλλαγές στην πολιτική ομάδας προεπιλεγμένου τομέα χρησιμοποιώντας τις εξής διαδρομές πολιτικής ομάδας:
    - Ρύθμιση παραμέτρων υπολογιστή\Ρυθμίσεις των Windows\Ρυθμίσεις ασφαλείας\Πολιτικές λογαριασμών\Πολιτική κωδικού πρόσβασης
    - Ρύθμιση παραμέτρων υπολογιστή\Ρυθμίσεις των Windows\Ρυθμίσεις ασφαλείας\Πολιτικές λογαριασμών\Πολιτική αποκλεισμού λογαριασμών

Σημείωση: Το συμβάν ελέγχου ασφαλείας καταγράφεται κατά την εφαρμογή της ρύθμισης πολιτικής. Δεν εμφανίζεται κατά την τροποποίηση των ρυθμίσεων.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

Security Group Management - Διαχείριση ομάδων ασφαλείας

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται από αλλαγές στις ομάδες ασφαλείας, όπως είναι οι εξής:

- Δημιουργία, αλλαγή ή διαγραφή μιας ομάδας ασφαλείας.
- Προσθήκη ή κατάργηση μέλους από μια ομάδα ασφαλείας.
- Αλλαγή του τύπου της ομάδας.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής μιας ομάδας ασφαλείας. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές σε μια ομάδα ασφαλείας.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία.

User Account Management - Διαχείριση λογαριασμού χρήστη

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τις αλλαγές που γίνονται στους λογαριασμούς των χρηστών. Τα σχετικά συμβάντα είναι, μεταξύ άλλων, τα εξής:

- Η δημιουργία, η αλλαγή, η διαγραφή, η μετονομασία, η απενεργοποίηση, η ενεργοποίηση, το κλείδωμα ή το ξεκλείδωμα ενός λογαριασμού χρήστη.
- Ο ορισμός ή η αλλαγή ενός κωδικού πρόσβασης χρήστη.
- Η προσθήκη ενός αναγνωριστικού ασφαλείας (SID) στο ιστορικό SID ενός λογαριασμού χρήστη.
- Η ρύθμιση του κωδικού πρόσβασης της κατάστασης επαναφοράς υπηρεσιών καταλόγου.
- Η αλλαγή των δικαιωμάτων σε λογαριασμούς χρηστών με δυνατότητες διαχείρισης.

- Η δημιουργία αντιγράφου ασφαλείας ή η επαναφορά των διαπιστευτηρίων της Διαχείρισης διαπιστευτηρίων.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής ενός λογαριασμού χρήστη. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές σε έναν λογαριασμό χρήστη.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία.

Detailed Tracking – Λεπτομερής εντοπισμός

DPAPI Activity - Δραστηριότητα DPAPI

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται όταν γίνονται αιτήσεις κρυπτογράφησης ή αποκρυπτογράφησης στη διασύνδεση εφαρμογών προστασίας δεδομένων (DPAPI). Η διασύνδεση DPAPI χρησιμοποιείται για την προστασία κρυφών πληροφοριών όπως οι αποθηκευμένες πληροφορίες κωδικών πρόσβασης και κλειδιών. Αν ορίσετε αυτή τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται μια αίτηση κρυπτογράφησης ή αποκρυπτογράφησης στη διασύνδεση DPAPI. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες αιτήσεις και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες αιτήσεις. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται κλήσεις κρυπτογράφησης ή αποκρυπτογράφησης τη διασύνδεση DPAPI.

Αριθμός συμβάντων: Χαμηλός.

PNP Activity - Δραστηριότητα PNP

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει τον έλεγχο όταν η δυνατότητα τοποθέτησης και άμεσης λειτουργίας εντοπίζει μια εξωτερική συσκευή. Εάν ρυθμίσετε τις παραμέτρους αυτής της ρύθμισης πολιτικής, δημιουργείται συμβάν ελέγχου, κάθε φορά που η δυνατότητα τοποθέτησης και άμεσης λειτουργίας εντοπίζει μια εξωτερική συσκευή. Καταγράφονται μόνο οι έλεγχοι επιτυχιών για αυτήν την κατηγορία. Εάν δεν ρυθμίσετε τις παραμέτρους αυτής της ρύθμισης πολιτικής, δεν δημιουργείται κανένα συμβάν ελέγχου όταν εντοπίζεται εξωτερική συσκευή από τη δυνατότητα τοποθέτησης και άμεσης λειτουργίας.

Όγκος: Χαμηλός

Process Creation - Δημιουργία διεργασιών

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται όταν γίνεται εκκίνηση ή δημιουργία μιας διεργασίας. Ελέγχεται επίσης το όνομα της εφαρμογής ή του χρήστη που δημιούργησε τη διεργασία. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που δημιουργείται μια διεργασία. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν δημιουργείται μια διεργασία.

Αριθμός συμβάντων: Ανάλογα με τη χρήση του υπολογιστή.

Process Termination - Τερματισμός διεργασίας

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται όταν τερματίζεται μια διεργασία. Αν ορίσετε αυτή τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που τερματίζεται μια διεργασία. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν τερματίζεται μια διεργασία.

Αριθμός συμβάντων: Ανάλογα με τη χρήση του υπολογιστή.

RPC Events - Συμβάντα RPC

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τις εισερχόμενες συνδέσεις κλήσεων απομακρυσμένων διαδικασιών (RPC). Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται προσπάθεια επίτευξης μιας απομακρυσμένης σύνδεσης RPC. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνεται προσπάθεια επίτευξης απομακρυσμένης σύνδεσης RPC.

Αριθμός συμβάντων: Υψηλός σε διακομιστές RPC.

Token Right Adjustment Event - Συμβάν προσαρμογής δικαιωμάτων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται με την προσαρμογή των προνομίων ενός διακριτικού.

Όγκος: Υψηλός.

Προεπιλογή: Χωρίς έλεγχο.

DS Access – Πρόσβαση DS

Detailed Directory Service Replication - Λεπτομερής αναπαραγωγή της υπηρεσίας καταλόγου

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από λεπτομερή αναπαραγωγή υπηρεσιών τομέα Active Directory (AD DS).

Αριθμός συμβάντων: Υψηλός.

Προεπιλογή: Χωρίς έλεγχο.

Directory Service Access - Πρόσβαση στις υπηρεσίες καταλόγου

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται όταν πραγματοποιείται πρόσβαση σε ένα αντικείμενο των υπηρεσιών τομέα Active Directory (AD DS). Καταγράφονται μόνο αντικείμενα των AD DS τα οποία έχουν αντιστοιχιστεί με μία λίστα ελέγχου πρόσβασης συστήματος (SACL). Τα συμβάντα σε αυτήν την υποκατηγορία είναι παρόμοια με τα συμβάντα υπηρεσιών καταλόγου που ήταν διαθέσιμα σε προηγούμενες εκδόσεις των Windows.

Αριθμός συμβάντων: Υψηλός σε ελεγκτές τομέα. Μηδενικός σε υπολογιστές-πελάτες.

Προεπιλογή για εκδόσεις υπολογιστή-πελάτη: Χωρίς έλεγχο.

Προεπιλογή για εκδόσεις διακομιστή: Επιτυχία.

Active Directory Domain Services Object Changes - Αλλαγές αντικειμένων υπηρεσιών τομέα Active Directory

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από αλλαγές αντικειμένων στις υπηρεσίες τομέα Active Directory (AD DS). Τα συμβάντα καταγράφονται όταν ένα αντικείμενο δημιουργείται, διαγράφεται, τροποποιείται, μετακινείται ή καταργείται η διαγραφή του. Όταν είναι δυνατόν, τα συμβάντα που καταγράφονται σε αυτήν την υποκατηγορία υποδεικνύουν τις νέες και τις προηγούμενες τιμές των ιδιοτήτων του αντικειμένου. Τα συμβάντα σε αυτήν την υποκατηγορία καταγράφονται μόνο σε ελεγκτές τομέων, ενώ καταγράφονται μόνο αντικείμενα στις υπηρεσίες AD DS που έχουν αντιστοιχιστεί με μια λίστα ελέγχου πρόσβασης συστήματος (SACL).

Σημείωση: Οι ενέργειες σε μερικά αντικείμενα και ιδιότητες δεν προκαλούν τη δημιουργία συμβάντων ελέγχου λόγω των ρυθμίσεων στην κλάση αντικειμένων στο σχήμα.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται προσπάθεια αλλαγής ενός αντικειμένου στις υπηρεσίες AD DS. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες.

Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται προσπάθειες αλλαγής ενός αντικειμένου στις υπηρεσίες AD DS.

Αριθμός συμβάντων: Υψηλός μόνο σε ελεγκτές τομέα.

Προεπιλογή: Χωρίς έλεγχο

Directory Service Replication - Αναπαραγωγή υπηρεσιών καταλόγου

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε την αναπαραγωγή μεταξύ δύο ελεγκτών τομέα των υπηρεσιών τομέα Active Directory (AD DS). Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου όταν γίνεται αναπαραγωγή των υπηρεσιών AD DS. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες αναπαραγωγές και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες αναπαραγωγές.

Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου κατά την αναπαραγωγή υπηρεσιών AD DS.

Σημείωση: Τα συμβάντα σε αυτήν την υποκατηγορία καταγράφονται μόνο σε ελεγκτές τομέα.

Αριθμός συμβάντων: Μέτριος σε ελεγκτές τομέα. Μηδενικός σε υπολογιστές-πελάτες.

Προεπιλογή: Χωρίς έλεγχο.

Logon/Logoff – Σύνδεση/Αποσύνδεση

Account Lockout - Κλείδωμα λογαριασμού

Αυτή η ρύθμιση πολιτικής επιτρέπει τον έλεγχο συμβάντων που δημιουργούνται από μια αποτυχημένη προσπάθεια σύνδεσης σε έναν λογαριασμό που έχει κλειδωθεί. Εάν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που ένας λογαριασμός δεν μπορεί να συνδεθεί σε έναν υπολογιστή, επειδή ο λογαριασμός είναι κλειδωμένος. Οι έλεγχοι επιτυχιών καταγράφουν επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες.

Τα συμβάντα είναι απαραίτητα για την κατανόηση της δραστηριότητας των χρηστών και για τον εντοπισμό πιθανών επιθέσεων.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία.

User / Device Claims - Ισχυρισμοί χρήστη / συσκευής

Αυτή η πολιτική σάς επιτρέπει να ελέγχετε πληροφορίες ισχυρισμών χρήστη και συσκευής στο διακριτικό σύνδεσης χρήστη. Τα συμβάντα σε αυτήν την υποκατηγορία δημιουργούνται στον υπολογιστή στον οποίο δημιουργείται περίοδος λειτουργίας σύνδεσης. Για αλληλεπιδραστική σύνδεση, το συμβάν ελέγχου ασφαλείας δημιουργείται στον υπολογιστή στον οποίο είναι συνδεδεμένος ο χρήστης. Για σύνδεση δικτύου, όπως η πρόσβαση σε έναν κοινόχρηστο φάκελο στο δίκτυο, το συμβάν ελέγχου ασφαλείας δημιουργείται στον υπολογιστή στον οποίο φιλοξενείται ο πόρος.

Οι ισχυρισμοί χρήστη προστίθενται σε ένα διακριτικό σύνδεσης όταν οι ισχυρισμοί περιλαμβάνονται με τα χαρακτηριστικό ενός λογαριασμού χρήστη στην υπηρεσία καταλόγου Active Directory. Οι ισχυρισμοί συσκευής προστίθενται στο διακριτικό σύνδεσης όταν οι ισχυρισμοί περιλαμβάνονται με τα χαρακτηριστικά λογαριασμού υπολογιστή μιας συσκευής στην υπηρεσία καταλόγου Active Directory. Επιπλέον, πρέπει να είναι ενεργοποιημένη σύνθετη ταυτότητα για τον τομέα και στον υπολογιστή στον οποίο έχει συνδεθεί ο χρήστης.

Όταν ρυθμίζεται αυτή η παράμετρος, δημιουργούνται ένα ή περισσότερα συμβάντα ελέγχου ασφαλείας για κάθε επιτυχή σύνδεση. Αν οι πληροφορίες ισχυρισμών συσκευής και χρήστη δεν μπορούν να χωρέσουν σε ένα μόνο συμβάν ελέγχου ασφαλείας, δημιουργούνται πολλά συμβάντα.

Αριθμός συμβάντων: Χαμηλός σε υπολογιστή-πελάτη. Μέτριος σε ελεγκτή τομέα ή σε διακομιστή δικτύου

Προεπιλογή: Χωρίς έλεγχο.

Group Membership - Συμμετοχή σε ομάδα

Αυτή η πολιτική σάς επιτρέπει να ελέγξετε τις πληροφορίες συμμετοχής σε ομάδα στο διακριτικό σύνδεσης του χρήστη. Τα συμβάντα αυτής της υποκατηγορίας δημιουργούνται στον υπολογιστή στον οποίο δημιουργείται η περίοδος λειτουργίας σύνδεσης. Για αλληλεπιδραστική σύνδεση, το συμβάν ελέγχου ασφάλειας δημιουργείται στον υπολογιστή στον οποίο συνδέθηκε ο χρήστης. Για σύνδεση δικτύου, όπως η πρόσβαση σε κοινόχρηστο φάκελο στο δίκτυο, το συμβάν ελέγχου ασφάλειας δημιουργείται στον υπολογιστή που φιλοξενεί τον πόρο. Όταν διαμορφώνεται αυτή η ρύθμιση, δημιουργείται ένα ή περισσότερα συμβάντα ελέγχου ασφάλειας για κάθε επιτυχημένη σύνδεση. Πρέπει, επίσης, να ενεργοποιήσετε τη ρύθμιση ελέγχου σύνδεσης στην περιοχή Ρύθμιση παραμέτρων πολιτικής ελέγχου για προχωρημένους\Πολιτικές ελέγχου συστήματος\Σύνδεση/αποσύνδεση. Δημιουργούνται πολλά συμβάντα αν οι πληροφορίες συμμετοχής ομάδας δεν είναι δυνατό να χωρέσουν σε ένα μόνο συμβάν ελέγχου ασφάλειας.

Όγκος: Χαμηλός σε υπολογιστή-πελάτη. Μέτριος σε ελεγκτή τομέα ή διακομιστή δικτύου

Προεπιλογή: Κανένας έλεγχος.

IPsec Extended Mode - Εκτεταμένη λειτουργία IPsec

Αυτή η πολιτική ασφαλείας σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από το πρωτόκολλο ανταλλαγής κλειδιών Internet (IKE) και το πρωτόκολλο Internet με έλεγχο ταυτότητας (AuthIP) κατά τη διάρκεια διαπραγματεύσεων εκτεταμένης λειτουργίας. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κατά τη διάρκεια των διαπραγματεύσεων εκτεταμένης λειτουργίας IPsec. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου κατά τη διάρκεια των διαπραγματεύσεων εκτεταμένης λειτουργίας IPsec.

Αριθμός συμβάντων: Υψηλός.

Προεπιλογή: Χωρίς έλεγχο.

IPsec Main Mode - Κύρια λειτουργία IPsec

Αυτή η πολιτική ασφαλείας σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από το πρωτόκολλο ανταλλαγής κλειδιών Internet (IKE) και το πρωτόκολλο Internet με έλεγχο ταυτότητας (AuthIP) κατά τη διάρκεια διαπραγματεύσεων κύριας λειτουργίας. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργούνται συμβάντα ελέγχου κατά τη διάρκεια των διαπραγματεύσεων κύριας λειτουργίας IPsec. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου κατά τη διάρκεια των διαπραγματεύσεων κύριας λειτουργίας IPsec.

Αριθμός συμβάντων: Υψηλός.

Προεπιλογή: Επιτυχία.

IPsec Quick Mode - Γρήγορη λειτουργία IPsec

Αυτή η πολιτική ασφαλείας σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από το πρωτόκολλο ανταλλαγής κλειδιών Internet (IKE) και το πρωτόκολλο Internet με έλεγχο ταυτότητας (AuthIP) κατά τη διάρκεια διαπραγματεύσεων γρήγορης λειτουργίας. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργούνται συμβάντα ελέγχου κατά τη διάρκεια των διαπραγματεύσεων γρήγορης λειτουργίας IPsec. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου κατά τη διάρκεια των διαπραγματεύσεων γρήγορης λειτουργίας IPsec.

Αριθμός συμβάντων: Υψηλός.

Προεπιλογή: Χωρίς έλεγχο.

Logoff – Αποσύνδεση

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγξετε τα συμβάντα που δημιουργούνται από το κλείσιμο μιας περιόδου λειτουργίας σύνδεσης. Αυτά τα συμβάντα εμφανίζονται στον υπολογιστή στον οποίο έγινε πρόσβαση. Για κάθε διαδραστική διεργασία αποσύνδεσης, το συμβάν ελέγχου ασφαλείας δημιουργείται στον υπολογιστή στον οποίο είχε συνδεθεί ο λογαριασμός χρήστη. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, δημιουργείται ένα συμβάν ελέγχου όταν κλείνει μια περίοδος λειτουργίας σύνδεσης. Οι έλεγχοι επιτυχιών καταγράφουν επιτυχημένες προσπάθειες για το κλείσιμο περιόδων λειτουργίας και οι έλεγχοι αποτυχιών καταγράφουν αποτυχημένες προσπάθειες για το κλείσιμο περιόδων λειτουργίας. Αν δεν

ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν κλείνει μια περίοδος λειτουργίας σύνδεσης.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία.

Logon - Έλεγχος σύνδεσης

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγξετε τα συμβάντα που δημιουργούνται από τις προσπάθειες σύνδεσης των λογαριασμών χρηστών στον υπολογιστή. Τα συμβάντα σε αυτήν την υποκατηγορία σχετίζονται με τη δημιουργία περιόδων λειτουργίας και εμφανίζονται στον υπολογιστή στον οποίον έγινε πρόσβαση. Για κάθε διαδραστική διαδικασία σύνδεσης, το συμβάν ελέγχου ασφαλείας δημιουργείται στον υπολογιστή στον οποίο συνδέθηκε ο λογαριασμός χρήστη. Για τις συνδέσεις μέσω δικτύου, όπως η πρόσβαση σε έναν κοινόχρηστο φάκελο στο δίκτυο, το συμβάν ελέγχου δημιουργείται στον υπολογιστή που φιλοξενεί τον πόρο. Συμπεριλαμβάνονται τα εξής συμβάντα:

- Επιτυχημένες προσπάθειες σύνδεσης.
- Αποτυχημένες προσπάθειες σύνδεσης.
- Προσπάθειες σύνδεσης με χρήση ρητών διαπιστευτηρίων.

Αυτό το συμβάν δημιουργείται όταν μια διεργασία προσπαθεί να συνδεθεί σε έναν λογαριασμό προσδιορίζοντας ρητά τα διαπιστευτήρια του λογαριασμού. Αυτό συμβαίνει συνήθως σε ρυθμίσεις παραμέτρων συνδέσεων δέσμης, όπως είναι οι προγραμματισμένες εργασίες ή η χρήση της εντολής RUNAS.

- Έγινε φιλτράρισμα των αναγνωριστικών ασφαλείας (SID) και δεν επιτράπηκε η σύνδεσή τους

Αριθμός συμβάντων: Χαμηλός σε έναν υπολογιστή-πελάτη. Μέτριος σε έναν ελεγκτή τομέα ή σε έναν διακομιστή δικτύου.

Προεπιλογή για εκδόσεις υπολογιστή-πελάτη: Επιτυχία.

Προεπιλογή για εκδόσεις διακομιστή: Επιτυχία, αποτυχία.

Network Policy Server - Διακομιστής πολιτικής δικτύου

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από τις αιτήσεις πρόσβασης χρηστών μέσω του RADIUS (IAS) και της Προστασίας πρόσβασης δικτύου (NAP). Αυτές οι αιτήσεις μπορούν να είναι Αποδοχή, Άρνηση, Απόρριψη, Καραντίνα, Κλείδωμα και Ξεκλείδωμα. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου για κάθε αίτηση χρήστη μέσω του IAS και του NAP. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες αιτήσεις πρόσβασης χρηστών και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτή τη ρύθμιση πολιτικής, δεν θα ελέγχονται οι αιτήσεις πρόσβασης χρηστών μέσω του IAS και του NAP.

Αριθμός συμβάντων: Μέτριος ή υψηλός στο διακομιστή NPS και IAS. Δεν επιβαρύνονται άλλοι υπολογιστές.

Προεπιλογή: Επιτυχία, αποτυχία.

Other Logon/Logoff Events - Άλλα συμβάντα σύνδεσης/αποσύνδεσης

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγξετε άλλα συμβάντα σύνδεσης/αποσύνδεσης που δεν καλύπτονται από τη ρύθμιση πολιτικής "Σύνδεση/αποσύνδεση", όπως είναι τα εξής:

- Αποσυνδέσεις περιόδου λειτουργίας υπηρεσιών τερματικού.
- Νέες περίοδοι λειτουργίας υπηρεσιών τερματικού.
- Το κλείδωμα ή το ξεκλείδωμα ενός σταθμού εργασίας.
- Η κλήση προφύλαξη οθόνης
- Η ακύρωση προφύλαξης οθόνης.
- Εντοπισμός μιας επίθεσης επανάληψης μέσω του Kerberos, κατά την οποία μια αίτηση του Kerberos λαμβάνεται εις διπλούν με τα ίδια ακριβώς στοιχεία. Αυτή η κατάσταση θα μπορούσε να οφείλεται σε εσφαλμένη ρύθμιση των παραμέτρων του δικτύου.
- Επιτράπηκε η πρόσβαση ενός λογαριασμού χρήστη ή υπολογιστή σε ένα ασύρματο δίκτυο.
- Επιτράπηκε η πρόσβαση ενός λογαριασμού χρήστη ή υπολογιστή σε ένα ενσύρματο δίκτυο 802.1x.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

Special Logon – Ειδική σύνδεση

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από ειδικές συνδέσεις, όπως είναι τα εξής :

- Η χρήση μιας ειδικής σύνδεσης, δηλαδή μιας σύνδεσης που έχει δικαιώματα ισοδύναμα με αυτά ενός διαχειριστή, η οποία μπορεί να χρειαστεί για την ανύψωση των δικαιωμάτων μιας διεργασίας σε υψηλότερο επίπεδο.
- Η σύνδεση ενός μέλους μιας ειδικής ομάδας. Οι ειδικές ομάδες σάς επιτρέπουν να ελέγχετε τα συμβάντα που δημιουργούνται όταν ένα μέλος μιας συγκεκριμένης ομάδας έχει συνδεθεί στο δίκτυό σας. Μπορείτε να ορίσετε στο μητρώο μια λίστα με αναγνωριστικά ασφαλείας ομάδας (SID). Αν κάποιο από αυτά τα SID προστεθεί σε ένα διακριτικό κατά τη διάρκεια της σύνδεσης και αν η υποκατηγορία έχει ενεργοποιηθεί, θα γίνει καταγραφή ενός συμβάντος.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία.

Object Access – Πρόσβαση αντικειμένων

Application Generated - Συμβάντα που δημιουργούνται από εφαρμογές

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε εφαρμογές που δημιουργούν συμβάντα κάνοντας χρήση των διασυνδέσεων προγραμματισμού εφαρμογών (API) του Ελέγχου των Windows. Οι εφαρμογές που έχουν σχεδιαστεί για να κάνουν χρήση του API του Ελέγχου των Windows χρησιμοποιούν αυτήν την υποκατηγορία για τη καταγραφή συμβάντων ελέγχου που σχετίζονται με τη λειτουργία τους.

- Τα συμβάντα αυτής της υποκατηγορίας περιλαμβάνουν, μεταξύ άλλων, τα εξής:
- Δημιουργία ενός περιβάλλοντος πελάτη εφαρμογής.
- Διαγραφή ενός περιβάλλοντος πελάτη εφαρμογής.

- Προετοιμασία ενός περιβάλλοντος πελάτη εφαρμογής.
- Άλλες λειτουργίες εφαρμογών που χρησιμοποιούν τα API του Ελέγχου των Windows.

Αριθμός συμβάντων: Εξαρτάται από τις εφαρμογές που δημιουργούν τα συμβάντα.

Certification Services - Υπηρεσίες πιστοποίησης

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τις λειτουργίες των Υπηρεσιών πιστοποιητικού της υπηρεσίας καταλόγου Active Directory (AD CS).

Οι λειτουργίες των AD CS περιλαμβάνουν τις εξής:

- Εκκίνηση/τερματισμός λειτουργίας/δημιουργία αντιγράφων ασφαλείας/επαναφορά των AD CS.
- Αλλαγές στη λίστα ανάκλησης πιστοποιητικών (CRL).
- Αίτηση νέου πιστοποιητικού.
- Έκδοση ενός πιστοποιητικού.
- Ανάκληση ενός πιστοποιητικού.
- Αλλαγές στις ρυθμίσεις της Διαχείρισης πιστοποιητικών για τις AD CS.
- Αλλαγές στη ρύθμιση παραμέτρων των AD CS.
- Αλλαγές σε ένα πρότυπο των Υπηρεσιών πιστοποιητικών.
- Εισαγωγή ενός πιστοποιητικού.
- Δημοσίευση ενός πιστοποιητικού αρχής έκδοσης πιστοποιητικών για τις υπηρεσίες τομέα Active Directory.
- Αλλαγές στα δικαιώματα ασφαλείας για τις AD CS.
- Αρχειοθέτηση ενός κλειδιού.
- Εισαγωγή ενός κλειδιού.
- Ανάκτηση ενός κλειδιού.
- Εκκίνηση της υπηρεσίας απόκρισης του πρωτοκόλλου κατάστασης ηλεκτρονικών πιστοποιητικών (OCSP).
- Διακοπή της λειτουργίας της υπηρεσίας απόκρισης του πρωτοκόλλου κατάστασης ηλεκτρονικών πιστοποιητικών (OCSP).

Αριθμός συμβάντων: Μέτριος ή χαμηλός σε υπολογιστές που εκτελούν Υπηρεσίες πιστοποιητικών Active Directory.

Detailed File Share - Λεπτομερής κοινή χρήση αρχείων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε προσπάθειες απόκτησης πρόσβασης σε αρχεία και φακέλους σε έναν κοινόχρηστο φάκελο. Η ρύθμιση "Λεπτομερής κοινή χρήση αρχείων" καταγράφει ένα συμβάν κάθε φορά που πραγματοποιείται πρόσβαση σε ένα αρχείο ή έναν φάκελο, ενώ η ρύθμιση "Κοινή χρήση αρχείων" καταγράφει μόνο ένα συμβάν για οποιαδήποτε σύνδεση πραγματοποιείται μεταξύ ενός υπολογιστή-πελάτη και ενός κοινόχρηστου πόρου αρχείων. Τα συμβάντα ελέγχου της λεπτομερούς κοινής χρήσης αρχείων περιλαμβάνουν λεπτομερείς πληροφορίες σχετικά με τα δικαιώματα ή άλλα κριτήρια που χρησιμοποιούνται για παραχώρηση ή άρνηση πρόσβασης. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται προσπάθεια απόκτησης πρόσβασης σε ένα αρχείο ή φάκελο σε κοινόχρηστο πόρο. Ο διαχειριστής μπορεί να καθορίσει εάν θα ελέγχονται μόνο επιτυχίες, μόνο αποτυχίες ή τόσο επιτυχίες όσο και αποτυχίες.

Σημείωση: Δεν υπάρχουν λίστες ελέγχου πρόσβασης συστήματος (SACL) για κοινόχρηστους φακέλους. Αν ενεργοποιηθεί αυτή η ρύθμιση πολιτικής, θα ελέγχεται η πρόσβαση σε όλα τα κοινόχρηστα αρχεία και τους φακέλους στο σύστημα.

Αριθμός συμβάντων: Υψηλός σε ένα διακομιστή αρχείων ή για σε έναν ελεγκτή τομέα λόγω της πρόσβασης δικτύου SYSVOL που απαιτείται από την πολιτική ομάδας.

File Share - Κοινή χρήση αρχείων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε προσπάθειες απόκτησης πρόσβασης σε έναν κοινόχρηστο φάκελο. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται προσπάθεια απόκτησης πρόσβασης σε έναν κοινόχρηστο φάκελο. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, ο διαχειριστής θα μπορεί να καθορίσει εάν θα ελεγχθούν μόνο επιτυχίες, μόνο αποτυχίες ή τόσο οι επιτυχίες όσο και οι αποτυχίες.

Σημείωση: Δεν υπάρχουν λίστες ελέγχου πρόσβασης συστήματος (SACL) για κοινόχρηστους φακέλους. Αν ενεργοποιηθεί αυτή η ρύθμιση πολιτικής, θα ελέγχεται η πρόσβαση σε όλους τους κοινόχρηστους φακέλους του συστήματος.

Αριθμός συμβάντων: Υψηλός σε ένα διακομιστή αρχείων ή για σε έναν ελεγκτή τομέα λόγω της πρόσβασης δικτύου SYSVOL που απαιτείται από την Πολιτική δικτύου.

File System - Σύστημα αρχείων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε της προσπάθειες των χρηστών για πρόσβαση στα αντικείμενα του συστήματος αρχείων. Δημιουργείται ένα συμβάν ελέγχου ασφαλείας μόνο για τα αντικείμενα για τα οποία έχουν οριστεί λίστες ελέγχου πρόσβασης συστήματος (SACL) και μόνο αν ο τύπος πρόσβασης που έχει ζητηθεί, όπως Εγγραφή, Ανάγνωση ή Τροποποίηση, καθώς και ο λογαριασμός που κάνει την αίτηση αντιστοιχούν στις ρυθμίσεις της SACL. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που ένας λογαριασμός αποκτά πρόσβαση σε ένα αντικείμενο του συστήματος αρχείων με την αντίστοιχη SACL. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν ένας λογαριασμός αποκτά πρόσβαση σε ένα αντικείμενο του συστήματος αρχείων με αντίστοιχη SACL.

Σημείωση: Μπορείτε να ορίσετε μια SACL σε ένα αντικείμενο συστήματος αρχείων χρησιμοποιώντας την καρτέλα "Ασφάλειας" στο παράθυρο διαλόγου "Ιδιότητες" του συγκεκριμένου αντικειμένου.

Αριθμός συμβάντων: Εξαρτάται από τη ρύθμιση των παραμέτρων των SACL του συστήματος αρχείων.

Windows Filtering Platform Connection - Σύνδεση πλατφόρμας φιλτραρίσματος των Windows

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τις συνδέσεις που επιτρέπονται ή αποκλείονται από την Πλατφόρμα φιλτραρίσματος των Windows (WFP). Συμπεριλαμβάνονται τα εξής συμβάντα:

- Η υπηρεσία Τείχους προστασίας των Windows δεν επιτρέπει σε μια εφαρμογή να δεχτεί εισερχόμενες συνδέσεις στο δίκτυο.
- Η πλατφόρμα WFP επιτρέπει μια σύνδεση.
- Η πλατφόρμα WFP αποκλείει μια σύνδεση.

- Η πλατφόρμα WFP επιτρέπει τη σύνδεση σε μια τοπική θύρα.
- Η πλατφόρμα WFP αποκλείει μια σύνδεση σε μια τοπική θύρα.
- Η πλατφόρμα WFP επιτρέπει μια σύνδεση.
- Η πλατφόρμα WFP αποκλείει μια σύνδεση.
- Η πλατφόρμα WFP επιτρέπει σε μια εφαρμογή ή υπηρεσία την ακρόαση σε μια θύρα για εισερχόμενες συνδέσεις.
- Η πλατφόρμα WFP δεν επιτρέπει σε μια εφαρμογή ή υπηρεσία την ακρόαση σε μια θύρα για εισερχόμενες συνδέσεις.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που η πλατφόρμα WFP επιτρέπει ή αποκλείει συνδέσεις. Οι έλεγχοι επιτυχιών καταγράφουν συμβάντα που δημιουργούνται όταν επιτρέπονται συνδέσεις και οι έλεγχοι αποτυχιών καταγράφουν συμβάντα που δημιουργούνται όταν αποκλείονται συνδέσεις.

Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν η πλατφόρμα WFP επιτρέπει ή αποκλείει συνδέσεις.

Αριθμός συμβάντων: Υψηλός.

Windows Filtering Platform Packet Drop - Πακέτα που έχουν απορριφθεί από την Πλατφόρμα φιλτραρίσματος των Windows

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγξετε τα πακέτα που απορρίπτονται από την Πλατφόρμα φιλτραρίσματος των Windows (WFP).

Αριθμός συμβάντων: Υψηλός.

Handle Manipulation - Εκμετάλλευση χειρισμού

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται όταν ανοίγει ή κλείνει ο χειρισμός ενός αντικειμένου. Μόνο αντικείμενα με μια αντιστοιχισμένη λίστα ελέγχου πρόσβασης συστήματος (SACL) δημιουργούν συμβάντα ελέγχου ασφάλειας. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται εκμετάλλευση ενός χειρισμού. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν όταν γίνονται εκμεταλλεύσεις χειρισμών.

Σημείωση: Τα συμβάντα σε αυτήν την υποκατηγορία δημιουργούν συμβάντα μόνο για τύπους αντικειμένων για τους οποίους έχει ενεργοποιηθεί η αντίστοιχη υποκατηγορία πρόσβασης αντικειμένων. Για παράδειγμα, αν έχει ενεργοποιηθεί η πρόσβαση αντικειμένων διαχείρισης αρχείων, δημιουργούνται συμβάντα ελέγχου ασφαλείας εκμετάλλευσης χειρισμού. Αν η πρόσβαση αντικειμένων μητρώου δεν έχει ενεργοποιηθεί, δεν θα δημιουργηθούν συμβάντα ελέγχου εκμετάλλευσης χειρισμού.

Αριθμός συμβάντων: Εξαρτάται από τη ρύθμιση παραμέτρων των SACL.

Kernel Object - Αντικείμενο πυρήνα

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε προσπάθειες απόκτησης πρόσβασης στον πυρήνα, οι οποίες περιλαμβάνουν mutex και σηματοφορείς. Μόνο τα αντικείμενα

πυρήνα με κατάλληλη λίστα ελέγχου πρόσβασης συστήματος (SACL) δημιουργούν συμβάντα ελέγχου ασφαλείας.

Σημείωση: Ο έλεγχος: Έλεγχος της πρόσβασης καθολικών στοιχείων ελέγχου αντικειμένων ρύθμισης σε σχέση με την προεπιλεγμένη SACL των αντικειμένων πυρήνα.

Αριθμός συμβάντων: Υψηλός αν έχει ενεργοποιηθεί ο έλεγχος πρόσβασης των καθολικών αντικειμένων συστήματος.

Other Object Access Events - Άλλα συμβάντα πρόσβασης αντικειμένων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από τις εργασίες του χρονοδιαγράμματος εργασιών ή των αντικειμένων COM+.

Για τις εργασίες του χρονοδιαγράμματος, ελέγχονται τα εξής:

- Δημιουργία εργασίας.
- Διαγραφή εργασίας.
- Ενεργοποίηση εργασίας.
- Απενεργοποίηση εργασίας.
- Ενημέρωση εργασίας.

Για αντικείμενα COM+, ελέγχονται τα εξής:

- Προσθήκη αντικειμένου καταλόγου.
- Ενημέρωση αντικειμένου καταλόγου.
- Διαγραφή αντικειμένου καταλόγου.

Αριθμός συμβάντων: Χαμηλός.

Registry – Μητρώο

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τις προσπάθειες πρόσβασης αντικειμένων του μητρώου. Δημιουργείται ένα συμβάν ελέγχου ασφαλείας μόνο για τα αντικείμενα για τα οποία έχουν οριστεί λίστες ελέγχου πρόσβασης συστήματος (SACL) και μόνο αν ο τύπος πρόσβασης που έχει ζητηθεί, όπως Εγγραφή, Ανάγνωση ή Τροποποίηση, καθώς και ο λογαριασμός που κάνει την αίτηση αντιστοιχούν στις ρυθμίσεις της SACL. Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που ένας λογαριασμός αποκτά πρόσβαση σε ένα αντικείμενο του μητρώου με αντίστοιχη SACL. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν ένας λογαριασμός αποκτά πρόσβαση σε ένα αντικείμενο του μητρώου με αντίστοιχη SACL.

Σημείωση: Μπορείτε να ορίσετε μια SACL για ένα αντικείμενο μητρώου χρησιμοποιώντας το παράθυρο διαλόγου "Δικαιώματα".

Αριθμός συμβάντων: Εξαρτάται από τη ρύθμιση των παραμέτρων των SACL του μητρώου.

Removable storage - Αφαιρούμενος χώρος αποθήκευσης

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τις απόπειρες χρηστών για πρόσβαση στα αντικείμενα συστημάτων αρχείων σε μια συσκευή αφαιρούμενου χώρου αποθήκευσης. Δημιουργείται ένα συμβάν ελέγχου ασφάλειας μόνο για όλα τα αντικείμενα, για όλους τους τύπους πρόσβασης που έχουν ζητηθεί. Εάν διαμορφώσετε αυτήν την πολιτική ρύθμισης, θα δημιουργείται ένα συμβάν ελέγχου όποτε ένας λογαριασμός αποκτάει πρόσβαση σε ένα

αντικείμενο συστήματος αρχείων σε έναν αφαιρούμενο χώρο αποθήκευσης. Οι επιτυχημένοι έλεγχοι καταγράφουν επιτυχείς προσπάθειες και οι αποτυχημένοι έλεγχοι καταγράφουν μη επιτυχείς προσπάθειες. Εάν δεν διαμορφώσετε αυτήν την πολιτική ρύθμισης, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν ένας λογαριασμός αποκτάει πρόσβαση σε ένα αντικείμενο συστήματος αρχείων σε έναν αφαιρούμενο χώρο αποθήκευσης.

SAM (Security Account Manager) - Διαχείριση λογαριασμού ασφαλείας

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από απόπειρες πρόσβασης σε αντικείμενα της Διαχείρισης λογαριασμών ασφαλείας (SAM).

Τα αντικείμενα SAM περιλαμβάνουν τα εξής:

- SAM_ALIAS --Μια τοπική ομάδα.
- SAM_GROUP -- Μια ομάδα που δεν είναι τοπική.
- SAM_USER – Ένα λογαριασμό χρήστη.
- SAM_DOMAIN – Έναν τομέα.
- SAM_SERVER – Ένα λογαριασμό υπολογιστή.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται προσπάθεια απόκτησης πρόσβασης σε ένα αντικείμενο πυρήνα. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται προσπάθειες απόκτησης πρόσβασης σε αντικείμενα πυρήνα.

Σημείωση: Μπορεί να τροποποιηθεί μόνο η λίστα ελέγχου πρόσβασης συστήματος (SACL) για το λογαριασμό SAM_SERVER.

Αριθμός συμβάντων: Υψηλός σε ελεγκτές τομέα.

Central Access Policy Staging - Κεντρική πολιτική πρόσβασης ενδιάμεσου σταδίου

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε αιτήσεις πρόσβασης όταν το δικαίωμα που εκχωρείται ή δεν επιτρέπεται από μια προτεινόμενη πολιτική διαφέρει από την τρέχουσα κεντρική πολιτική πρόσβασης σε ένα αντικείμενο. Εάν διαμορφώσετε αυτήν την πολιτική ρύθμισης, θα δημιουργείται ένα συμβάν ελέγχου όποτε ένας χρήστης αποκτάει πρόσβαση σε ένα αντικείμενο και το δικαίωμα που εκχωρείται από την τρέχουσα πολιτική πρόσβασης στο αντικείμενο διαφέρει από εκείνο που εκχωρείται από την προτεινόμενη πολιτική. Το συμβάν ελέγχου που θα προκύψει θα δημιουργηθεί ως εξής:

- Επιτυχημένοι έλεγχοι, όταν ρυθμίζονται οι παράμετροι, καταγράφουν απόπειρες πρόσβασης όταν η τρέχουσα κεντρική πολιτική πρόσβασης εκχωρεί πρόσβαση, αλλά η προτεινόμενη πολιτική δεν επιτρέπει την πρόσβαση.
- Αποτυχημένοι έλεγχοι, όταν ρυθμίζονται οι παράμετροι, καταγράφουν απόπειρες πρόσβασης όταν:
    - Η τρέχουσα κεντρική πολιτική πρόσβασης δεν εκχωρεί πρόσβαση, αλλά η προτεινόμενη πολιτική εκχωρεί πρόσβαση.
    - Μια αρχή ζητάει τα μέγιστα δικαιώματα πρόσβασης που επιτρέπονται και τα δικαιώματα πρόσβασης που εκχωρούνται από την τρέχουσα κεντρική πολιτική πρόσβασης είναι διαφορετικά από τα δικαιώματα πρόσβασης που εκχωρούνται από την προτεινόμενη πολιτική.

Αριθμός συμβάντων: Πιθανώς υψηλός σε ένα διακομιστή αρχείων όταν η προτεινόμενη πολιτική διαφέρει σημαντικά από την τρέχουσα κεντρική πολιτική πρόσβασης.

Προεπιλογή: Χωρίς έλεγχο

Policy Change – Αλλαγή πολιτικής

Audit Policy Change - Έλεγχος αλλαγής πολιτικής

- Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε αλλαγές στις ρυθμίσεις πολιτικής ελέγχου ασφαλείας, όπως είναι οι εξής:
- Δικαιώματα ρυθμίσεων και ρυθμίσεις ελέγχου στο αντικείμενο πολιτικής ελέγχου
- Αλλαγές στην πολιτική ελέγχου του συστήματος
- Καταχώρηση των προελεύσεων συμβάντων ασφαλείας
- Κατάργηση καταχώρησης προελεύσεων συμβάντων ασφαλείας
- Αλλαγές στις ρυθμίσεις ελέγχου ανά χρήστη
- Αλλαγές στην τιμή του CrashOnAuditFail
- Αλλαγές στη λίστα ελέγχου πρόσβασης συστήματος σε ένα σύστημα αρχείων ή αντικείμενο μητρώου
- Αλλαγές στη λίστα ειδικών ομάδων

Σημείωση: Ο έλεγχος αλλαγών στη λίστα ελέγχου πρόσβασης συστήματος (SACL) γίνεται όταν αλλάζει η SACL για ένα αντικείμενο ενώ είναι ενεργοποιημένη η κατηγορία αλλαγής πολιτικής. Οι αλλαγές στη λίστα διακριτικού ελέγχου πρόσβασης (DACL) και οι αλλαγές κυριότητας ελέγχονται όταν είναι ενεργοποιημένος ο έλεγχος πρόσβασης αντικειμένων και η SACL του αντικειμένου έχει ρυθμιστεί για τον έλεγχο αλλαγών της DACL ή του κατόχου.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου όταν γίνονται προσπάθειες για την επίτευξη απομακρυσμένης σύνδεσης RPC. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχίες καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου κατά την απόπειρα επίτευξης απομακρυσμένης σύνδεσης RPC.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία.

Authentication Policy Change - Αλλαγές πολιτικής ελέγχου ταυτότητας

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από αλλαγές στην πολιτική ελέγχου ταυτότητας, όπως είναι τα εξής:

- Δημιουργία σχέσεων αξιοπιστίας δασών και τομέων
- Τροποποίηση σχέσεων αξιοπιστίας δασών και τομέων.
- Κατάργηση σχέσεων αξιοπιστίας δασών και τομέων.
- Αλλαγές στην πολιτική του Kerberos μέσω της διαδρομής Ρύθμιση παραμέτρων υπολογιστή\Ρυθμίσεις Windows\Ρυθμίσεις ασφαλείας\Πολιτικές λογαριασμού\Πολιτική Kerberos.
- Η εκχώρηση ενός από τα παρακάτω δικαιώματα χρήστη σε έναν χρήστη ή ομάδα:
- Πρόσβαση σε αυτόν τον υπολογιστή μέσω δικτύου.
- Να επιτρέπεται η σύνδεση τοπικά.
- Να επιτρέπονται συνδέσεις μέσω Υπηρεσιών τερματικού.

- Σύνδεση ως διαδικασία δέσμης.
- Σύνδεση σε μια υπηρεσία
- Διένεξη στο χώρο ονομάτων. Όπως, για παράδειγμα, όταν μια νέα σχέση αξιοπιστίας έχει το ίδιο όνομα με ένα υπάρχον όνομα του χώρου ονομάτων.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται προσπάθεια αλλαγής της πολιτικής ελέγχου ταυτότητας. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ρυθμίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές στην πολιτική ελέγχου ταυτότητας.

Σημείωση: Το συμβάν ελέγχου ασφαλείας καταγράφεται όταν εφαρμόζεται η πολιτική ομάδας. Δεν εμφανίζεται όταν τροποποιούνται οι ρυθμίσεις.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία.

Authorization Policy Change - Αλλαγή πολιτικής εξουσιοδότησης

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από αλλαγές στην πολιτική ελέγχου ταυτότητας, όπως είναι οι εξής:

- Εκχώρηση δικαιωμάτων χρήστη (προνόμια), όπως το SeCreateTokenPrivilege, τα οποία δεν ελέγχονται μέσω της υποκατηγορίας. “Αλλαγές πολιτικής ελέγχου ταυτότητας”
- Κατάργηση δικαιωμάτων χρηστών (προνομίων), όπως το SeCreateTokenPrivilege, τα οποία δεν ελέγχονται μέσω της υποκατηγορίας. “Αλλαγές πολιτικής ελέγχου ταυτότητας”
- Αλλαγές στην πολιτική κρυπτογράφησης συστήματος αρχείου (EFS).
- Αλλαγές στα χαρακτηριστικά πόρου ενός αντικειμένου.
- Αλλαγές στην κεντρική πολιτική πρόσβασης (CAP) που εφαρμόζεται σε ένα αντικείμενο.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής της πολιτικής ελέγχου ταυτότητας. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές στην πολιτική ελέγχου ταυτότητας.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

Filtering Platform Policy Change - Αλλαγές πολιτικής πλατφόρμας φιλτραρίσματος

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από αλλαγές που γίνονται στην πλατφόρμα φιλτραρίσματος των Windows (WFP), όπως είναι οι εξής:

- Κατάσταση υπηρεσιών IPsec.
- Αλλαγές στις ρυθμίσεις πολιτικής IPsec.

- Αλλαγές στις ρυθμίσεις πολιτικής του Τείχους προστασίας των Windows.
- Αλλαγές στη μηχανή και στις υπηρεσίες παροχής της WFP.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής της WFP. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές στη WFP.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

MPSSVC Rule-Level Policy Change - Αλλαγή πολιτικής επιπέδου κανόνων MPSSVC

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται από αλλαγές στους κανόνες πολιτικής που χρησιμοποιεί η Υπηρεσία προστασίας της Microsoft (MPSSVC). Αυτή η υπηρεσία χρησιμοποιείται από το Τείχος προστασίας των Windows. Τα συμβάντα περιλαμβάνουν τα εξής:

- Αναφορά ενεργών πολιτικών κατά την εκκίνηση της υπηρεσίας Τείχους προστασίας των Windows.
- Αλλαγές στους κανόνες του Τείχους προστασίας των Windows.
- Αλλαγές στη λίστα εξαιρέσεων του Τείχους προστασίας των Windows.
- Αλλαγές στις ρυθμίσεις του Τείχους προστασίας των Windows.
- Κανόνες που έχουν παραλειφθεί ή δεν έχουν εφαρμοστεί από την υπηρεσία Τείχους προστασίας των Windows.
- Αλλαγές στις ρυθμίσεις της πολιτικής ομάδας του Τείχους προστασίας των Windows.

Αν ορίσετε αυτή τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται απόπειρα αλλαγής των κανόνων πολιτικής που χρησιμοποιεί το MPSSVC. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτή τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αλλαγές στους κανόνες πολιτικές που χρησιμοποιεί το MPSSVC.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

Other Policy Change Events - Άλλα συμβάντα αλλαγής πολιτικής

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγξετε συμβάντα που παράγονται από άλλες αλλαγές πολιτικής ασφάλειας οι οποίες δεν ελέγχονται στην κατηγορία αλλαγή πολιτικής, όπως οι εξής:

- Αλλαγές ρύθμισης παραμέτρων αξιόπιστης μονάδας πλατφόρμας (TPM).
- Αυτοέλεγχοι κρυπτογράφησης λειτουργίας πυρήνα.
- Λειτουργίες της υπηρεσίας παροχής κρυπτογράφησης.
- Λειτουργίες ή τροποποιήσεις του περιβάλλοντος κρυπτογράφησης.
- Αλλαγές στις εφαρμοσμένες πολιτικές κεντρικής πρόσβασης (CAPs).
- Τροποποιήσεις δεδομένων ρύθμισης παραμέτρων εκκίνησης (BCD).

Όγκος: Χαμηλός.

Προεπιλογή: Κανένας έλεγχος.

Privilege Use – Χρήση δικαιώματος

Non Sensitive Privilege Use - Χρήση μη ευαίσθητων δικαιωμάτων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που δημιουργούνται από τη χρήση μη ευαίσθητων δικαιωμάτων (χρήστη).

Τα παρακάτω δικαιώματα είναι μη ευαίσθητα:

- Πρόσβαση στη Διαχείριση διαπιστευτηρίων ως αξιόπιστος καλών.
- Πρόσβαση αυτού του υπολογιστή από το δίκτυο.
- Προσθήκη σταθμών εργασίας στον τομέα.
- Ρύθμιση ορίων μεγέθους μνήμης για μια διεργασία.
- Να επιτρέπεται η σύνδεση τοπικά.
- Να επιτρέπεται η σύνδεση μέσω των Υπηρεσιών τερματικού.
- Παράκαμψη ελέγχου διέλευσης.
- Αλλαγή της ώρας του συστήματος.
- Δημιουργία αρχείου σελιδοποίησης.
- Δημιουργία καθολικών αντικειμένων.
- Δημιουργία μόνιμων κοινόχρηστων αντικειμένων.
- Δημιουργία συμβολικών συνδέσεων.
- Να μην επιτρέπεται η πρόσβαση σε αυτόν τον υπολογιστή από το δίκτυο.
- Άρνηση σύνδεσης ως εργασία δέσμης.
- Άρνηση σύνδεσης ως υπηρεσία.
- Άρνηση τοπικής σύνδεσης.
- Άρνηση σύνδεσης μέσω Υπηρεσιών τερματικού.
- Επιβολή τερματισμού λειτουργίας από απομακρυσμένο σύστημα.
- Αύξηση συνόλου εργασιών διεργασίας.
- Αύξηση της προτεραιότητας προγραμματισμού.
- Κλείδωμα σελίδων στη μνήμη.
- Σύνδεση ως εργασία δέσμης.
- Σύνδεση ως υπηρεσία.
- Τροποποίηση της ετικέτας ενός αντικειμένου.
- Εκτέλεση ενεργειών συντήρησης τόμου.
- Απλή διεργασία προφίλ.
- Προφίλ απόδοσης συστήματος.
- Αφαίρεση υπολογιστή από σταθμό αγκύρωσης.
- Τερματισμός λειτουργίας του συστήματος.
- Συγχρονισμός δεδομένων υπηρεσίας καταλόγου.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται κλήση ενός μη ευαίσθητου δικαιώματος. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες κλήσεις και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες κλήσεις. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνεται κλήση ενός μη ευαίσθητου δικαιώματος.

Αριθμός συμβάντων: Πολύ υψηλός.

Other Privilege Use Events – Άλλα συμβάντα δικαιωμάτων

Δεν χρησιμοποιείται.

Sensitive Privilege Use - Χρήση ευαίσθητων δικαιωμάτων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται όταν γίνεται χρήση ευαίσθητων δικαιωμάτων (χρήστη), όπως είναι τα εξής:

- Κλήση μιας προνομιακής υπηρεσίας.
- Γίνεται κλήση ενός από τα παρακάτω δικαιώματα:
- Ενέργεια ως μέρος του λειτουργικού συστήματος.
- Δημιουργία αντιγράφων ασφαλείας για αρχεία και καταλόγους.
- Δημιουργία ενός αντικειμένου διακριτικού.
- Εντοπισμός σφαλμάτων σε προγράμματα.
- Χαρακτηρισμός λογαριασμών υπολογιστών και χρηστών ως αξιόπιστων για ανάθεση.
- Δημιουργία ελέγχων ασφαλείας.
- Μίμηση ενός υπολογιστή-πελάτη μετά τον έλεγχο ταυτότητας.
- Φόρτωση και αναίρεση φόρτωσης προγραμμάτων οδήγησης συσκευών.
- Διαχείριση του αρχείου καταγραφής ελέγχων και ασφαλείας.
- Τροποποίηση των τιμών περιβάλλοντος υλικολογισμικού.
- Αντικατάσταση ενός διακριτικού επιπέδου διεργασίας.
- Επαναφορά αρχείων και καταλόγων.
- Ανάληψη κυριότητας αρχείων ή άλλων αντικειμένων.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνονται αιτήσεις ευαίσθητων δικαιωμάτων. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες αιτήσεις και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες αιτήσεις. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνονται αιτήσεις ευαίσθητων δικαιωμάτων.

Αριθμός συμβάντων: Υψηλός.

System – Σύστημα

IPsec Driver - Πρόγραμμα οδήγησης IPsec

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα ελέγχου που δημιουργούνται από το πρόγραμμα οδήγησης φίλτρων του IPsec, όπως είναι τα εξής:

- Εκκίνηση και τερματισμός των υπηρεσιών IPsec.
- Πακέτα δικτύου που απορρίφθηκαν λόγω αποτυχίας ελέγχου ακεραιότητας.
- Πακέτα δικτύου που απορρίφθηκαν λόγω αποτυχίας ελέγχου επανάληψης.
- Πακέτα δικτύου που απορρίφθηκαν λόγω του ότι περιείχαν απλό κείμενο.
- Πακέτα δικτύου που παραλείφθηκαν με εσφαλμένη ένδειξη παραμέτρων ασφαλείας (SPI). Αυτό μπορεί να σημαίνει ότι η κάρτα δικτύου δεν λειτουργεί σωστά ή ότι το πρόγραμμα οδήγησης χρειάζεται ενημέρωση.
- Αδυναμία επεξεργασίας φίλτρων IPsec.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου για κάθε λειτουργία του προγράμματος οδήγησης του φίλτρου IPsec. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, οι λειτουργίες του προγράμματος οδήγησης φίλτρου IPSec δεν θα δημιουργούν συμβάντα ελέγχου.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Χωρίς έλεγχο.

Other System Events - Άλλα συμβάντα συστήματος

- Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε οποιοδήποτε από τα εξής συμβάντα:
- Εκκίνηση και τερματισμός της υπηρεσίας και του προγράμματος οδήγησης του Τείχους προστασίας των Windows.
- Επεξεργασία της πολιτικής ασφαλείας από την υπηρεσία Τείχους προστασίας των Windows.
- Λειτουργίες αρχείου κλειδιού κρυπτογράφησης και μετεγκατάστασης.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Επιτυχία, αποτυχία.

Security State Change - Αλλαγή κατάστασης ασφαλείας

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που δημιουργούνται από αλλαγές στην κατάσταση ασφαλείας του υπολογιστή, όπως είναι τα εξής:

- Εκκίνηση και τερματισμός λειτουργίας του υπολογιστή.
- Αλλαγή της ώρας του συστήματος.
- Επαναφορά του συστήματος από σφάλμα CrashOnAuditFail, το οποίο καταγράφεται μετά την επανεκκίνηση του συστήματος όταν το αρχείο καταγραφής συμβάντων ασφαλείας είναι πλήρες και η καταχώρηση μητρώου CrashOnAuditFail έχει ρυθμιστεί.

Αριθμός συμβάντων: Χαμηλός

Προεπιλογή: Επιτυχία.

Security System Extension - Επέκταση συστήματος ασφαλείας

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε τα συμβάντα που σχετίζονται με επεκτάσεις ή υπηρεσίες συστήματος ασφάλειας, όπως είναι οι εξής:

- Φόρτωση και καταχώρηση στην τοπική αρχή ασφαλείας (LSA) μιας επέκτασης συστήματος ασφαλείας, όπως ένα πακέτο ελέγχου ταυτότητας, ειδοποίησης ή ασφάλειας. Χρησιμοποιείται για τον έλεγχο ταυτότητας σε προσπάθειες σύνδεσης, για την υποβολή αιτήσεων σύνδεσης και για οποιεσδήποτε αλλαγές σε λογαριασμούς και κωδικούς πρόσβασης. Παραδείγματα επεκτάσεων συστήματος ασφαλείας είναι οι Kerberos και NTLM.
- Εγκατάσταση και καταχώρηση μιας υπηρεσίας στη Διαχείριση ελέγχου υπηρεσιών. Το αρχείο καταγραφής ελέγχου περιέχει πληροφορίες σχετικά με το όνομα, τα δυαδικά δεδομένα, τον τύπο, τον τύπο εκκίνησης και το λογαριασμό της υπηρεσίας.

Αν ορίσετε αυτήν τη ρύθμιση πολιτικής, θα δημιουργείται ένα συμβάν ελέγχου κάθε φορά που γίνεται προσπάθεια φόρτωσης μιας επέκτασης συστήματος ασφαλείας. Οι έλεγχοι επιτυχιών καταγράφουν τις επιτυχημένες προσπάθειες και οι έλεγχοι αποτυχιών καταγράφουν τις αποτυχημένες προσπάθειες. Αν δεν ορίσετε αυτήν τη ρύθμιση πολιτικής, δεν θα δημιουργείται κανένα συμβάν ελέγχου όταν γίνεται προσπάθεια φόρτωσης μιας επέκτασης συστήματος ασφάλειας.

Αριθμός συμβάντων: Χαμηλός. Τα συμβάντα επεκτάσεων συστήματος ασφαλείας δημιουργούνται πιο συχνά σε ελεγκτές τομέα, παρά σε υπολογιστές-πελάτες ή διακομιστές-μέλη.

Προεπιλογή: Χωρίς έλεγχο.

System Integrity - Ακεραιότητα συστήματος

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να ελέγχετε συμβάντα που παραβιάζουν την ακεραιότητα του υποσυστήματος ασφαλείας, όπως είναι τα εξής:

- Συμβάντα που δεν ήταν δυνατό να εγγραφούν στο αρχείο καταγραφής συμβάντος λόγω προβλήματος στο σύστημα ελέγχου.
- Μια διεργασία που χρησιμοποιεί μια μη έγκυρη θύρα κλήσης τοπικής διαδικασίας (LPC) προσπαθώντας να μιμηθεί έναν υπολογιστή-πελάτη παρέχοντας αποκρίσεις, διαβάζοντας ή γράφοντας δεδομένα προς ή από το χώρο διευθύνσεων ενός υπολογιστή-πελάτη.
- Ο εντοπισμός μιας κλήσης απομακρυσμένης διαδικασίας (RPC) που θέτει σε κίνδυνο την ακεραιότητα του συστήματος.
- Ο εντοπισμός μιας τιμής κατακερματισμού ενός εκτελέσιμου αρχείου που δεν είναι έγκυρη σύμφωνα με την Ακεραιότητα κώδικα.
- Λειτουργίες κρυπτογράφησης που θέτουν σε κίνδυνο την ακεραιότητα του συστήματος.

Αριθμός συμβάντων: Χαμηλός.

Προεπιλογή: Αποτυχία.

Global Object Access Auditing – Έλεγχος καθολικής πρόσβασης αντικειμένων

Audit file system global object access - Έλεγχος πρόσβασης καθολικού αντικειμένου συστήματος αρχείων

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να εφαρμόσετε μια αναλυτική πολιτική ελέγχου πρόσβασης αντικειμένου σε κάθε αρχείο και φάκελο στο σύστημα αρχείων ενός υπολογιστή. Η διαμόρφωση αυτής της ρύθμισης σάς επιτρέπει επίσης να δείξετε ότι κάθε αρχείο και φάκελος στον υπολογιστή παρακολουθείται από μια πολιτική ελέγχου που η διαχείρισή της γίνεται από κεντρική θέση.

Αυτή η ρύθμιση εφαρμόζει μια καθολική λίστα ελέγχου πρόσβασης συστήματος (SACL) σε κάθε αρχείο και φάκελο. Εάν έχουν ρυθμιστεί στον υπολογιστή τόσο μια λίστα SACL μητρώου όσο και μια καθολική λίστα SACL, η λίστα SACL σε ισχύ προκύπτει από τον συνδυασμό της λίστας SACL μητρώου και της καθολικής λίστας SACL. Αυτό σημαίνει ότι δημιουργείται ένα συμβάν ελέγχου εάν μια δραστηριότητα συμφωνεί είτε με τη λίστα SACL του κλειδιού μητρώου είτε με την καθολική λίστα SACL.

Για να ρυθμίσετε τις παραμέτρους μιας καθολικής πολιτικής πρόσβασης αντικειμένου, πρέπει να επιλέξετε τη ρύθμιση "Ορισμός αυτής της πολιτικής" και να κάνετε κλικ στην επιλογή "Ρύθμιση παραμέτρων" για να προσθέσετε τουλάχιστον ένα χρήστη ή ομάδα στην καθολική SACL. Επίσης, πρέπει να ενεργοποιήσετε τη ρύθμιση "Έλεγχος συστήματος αρχείων", στην περιοχή "Ρύθμιση παραμέτρων εξελιγμένης πολιτικής ελέγχου"\Πολιτικές ελέγχου συστήματος\Πρόσβαση αντικειμένων.

Τόμος: Εξαρτάται από την ισχύουσα λίστα SACL και το επίπεδο δραστηριότητας χρήστη.

Registry global object access - Έλεγχος πρόσβασης καθολικού αντικειμένου μητρώου

Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να εφαρμόσετε μια καθολική πολιτική ελέγχου πρόσβασης αντικειμένου στο μητρώο για έναν ολόκληρο υπολογιστή. Αυτή η ρύθμιση πολιτικής σάς επιτρέπει να δείξετε ότι κάθε αντικείμενο μητρώου στον υπολογιστή προστατεύεται από μια πολιτική ελέγχου που η διαχείρισή της γίνεται από κεντρική θέση.

Αυτή η ρύθμιση εφαρμόζει μια καθολική λίστα ελέγχου πρόσβασης συστήματος (SACL) σε κάθε αντικείμενο μητρώου. Εάν έχουν ρυθμιστεί στον υπολογιστή τόσο μια λίστα SACL μητρώου όσο και μια καθολική λίστα SACL, η λίστα SACL σε ισχύ προκύπτει από τον συνδυασμό της λίστας SACL μητρώου και της καθολικής λίστας SACL. Αυτό σημαίνει ότι δημιουργείται ένα συμβάν ελέγχου εάν μια δραστηριότητα συμφωνεί είτε με τη λίστα SACL του κλειδιού μητρώου είτε με την καθολική λίστα SACL.

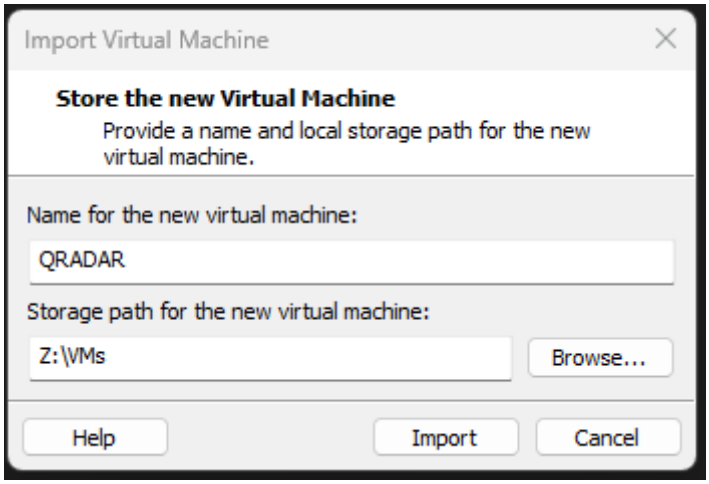
Για να ρυθμίσετε τις παραμέτρους μιας καθολικής πολιτικής πρόσβασης αντικειμένου, πρέπει να επιλέξετε τη ρύθμιση "Ορισμός αυτής της πολιτικής" και να κάνετε κλικ στην επιλογή "Ρύθμιση παραμέτρων" για να προσθέσετε τουλάχιστον ένα χρήστη ή ομάδα στην καθολική SACL. Επίσης, πρέπει να ενεργοποιήσετε τη ρύθμιση "Έλεγχος μητρώου", στην περιοχή "Ρύθμιση παραμέτρων εξελιγμένης πολιτικής ελέγχου"\Πολιτικές ελέγχου συστήματος\Πρόσβαση αντικειμένων.

Τόμος: Εξαρτάται από την ισχύουσα λίστα SACL και το επίπεδο δραστηριότητας χρήστη.

3.3 Παραμετροποίηση του SIEM QRadar CE

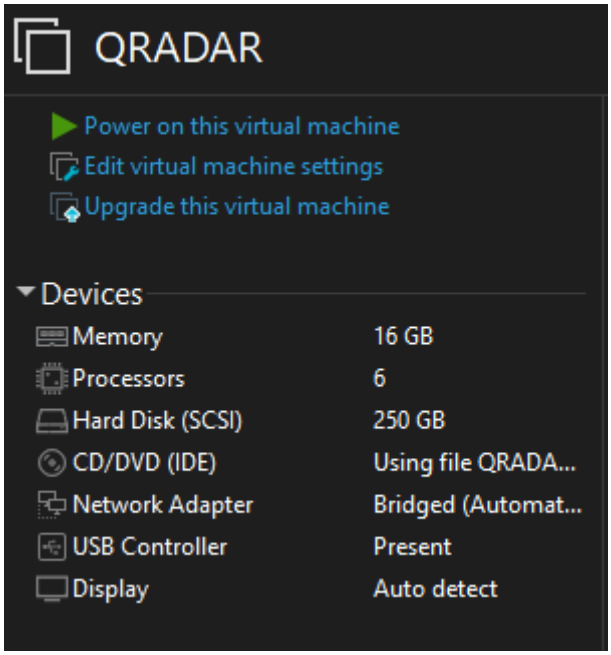
Στο παρακάτω υποκεφάλαιο, θα παρουσιάσουμε τη διαδικασία εγκατάστασης και τη βασική παραμετροποίηση του IBM QRadar CE.

Μετά τη λήψη του αρχείου εγκατάστασης από την επίσημη ιστοσελίδα της IBM, ακολουθούμε τη διαδικασία εισαγωγής του σε μια πλατφόρμα εικονικοποίησης. Στη συγκεκριμένη περίπτωση, χρησιμοποιούμε το VMware Workstation.



Εικόνα 3.3.1: Εισαγωγή εικονικής μηχανής

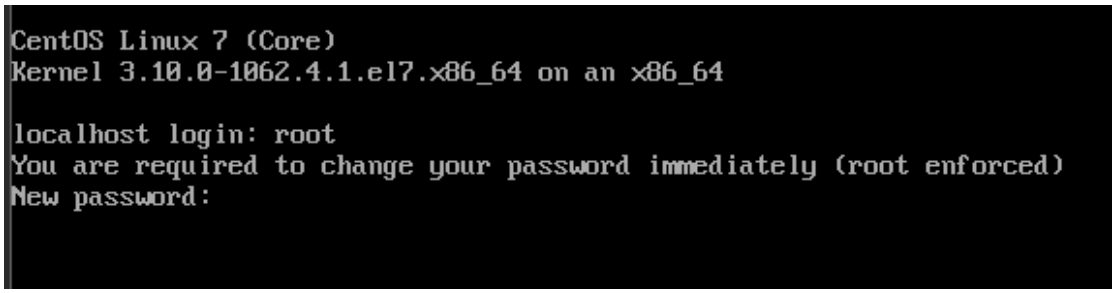
Αφού ολοκληρωθεί η διαδικασία εισαγωγής της εικονικής μηχανής, προχωρούμε στη διαμόρφωση και ενδεχομένως στην αύξηση των πόρων της, ανάλογα με τις ανάγκες μας και τις δυνατότητες του κύριου συστήματος που θα τη φιλοξενήσει.



Εικόνα 3.3.2: Παραμετροποίηση υλικού εικονικής μηχανής

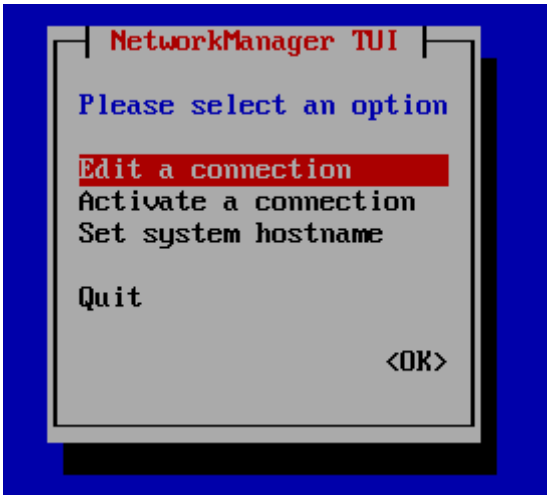
Ξεκινούμε τη λειτουργία της εικονικής μηχανής μας και στη συνέχεια ακολουθούμε τα βήματα εγκατάστασης, όπως αναφέρονται στο επίσημο εγχειρίδιο της IBM.

Χρησιμοποιούμε τον χρήστη "root" για να συνδεθούμε και δημιουργούμε έναν νέο κωδικό πρόσβασης, όπως παρουσιάζεται στην ακόλουθη οθόνη:



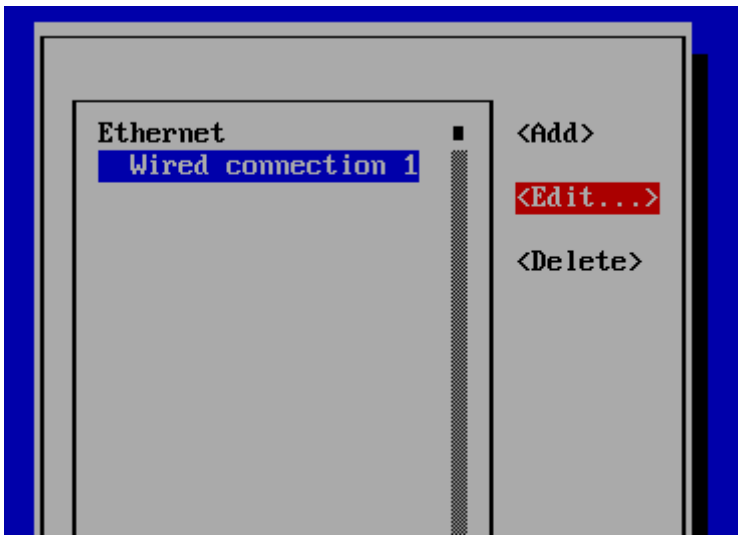
Εικόνα 3.3.3: Δημιουργία κωδικού του χρήστη root

Συνεχίζουμε τη διαμόρφωση των δικτυακών ρυθμίσεων πριν την εγκατάσταση, προκειμένου να διασφαλίσουμε τον πλήρη έλεγχο τους. Για αυτήν τη διαδικασία, χρησιμοποιούμε την εντολή "nmtui" (Network Manager Text User Interface).



Εικόνα 3.3.4: Παραμετροποίηση δικτυακών ρυθμίσεων

Επιλέγουμε τη δικτυακή κάρτα που θα χρησιμοποιήσουμε και προχωρούμε σε επεξεργασία (edit).

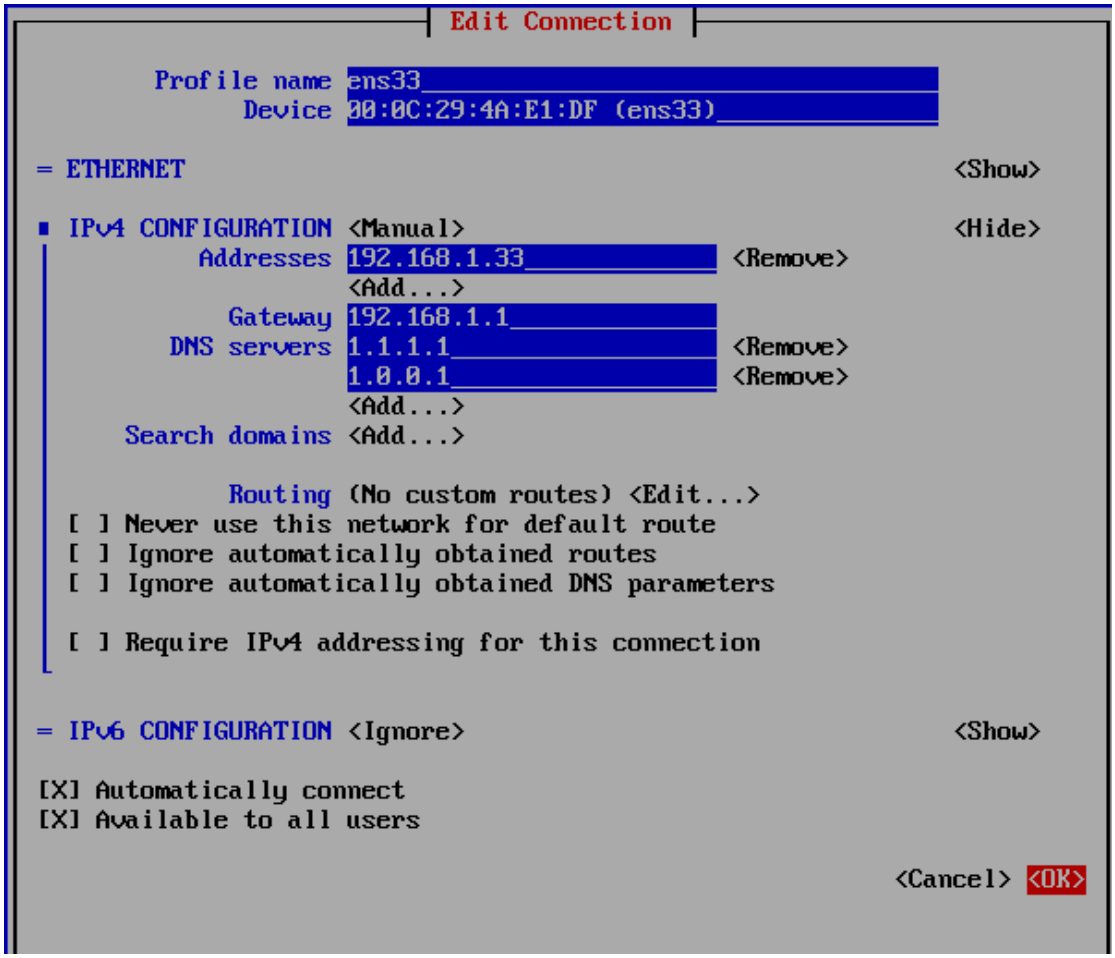


Εικόνα 3.3.5: Παραμετροποίηση δικτυακών ρυθμίσεων

Αλλάζουμε το όνομα του προφίλ ανάλογα με το όνομα που εμφανίζεται στο δεύτερο πεδίο "device," σε αυτή την περίπτωση "ens33". Στη συνέχεια, για τη ρύθμιση του IPv4 Configuration, επιλέγουμε τη λειτουργία "manual" και καθορίζουμε τα παρακάτω:

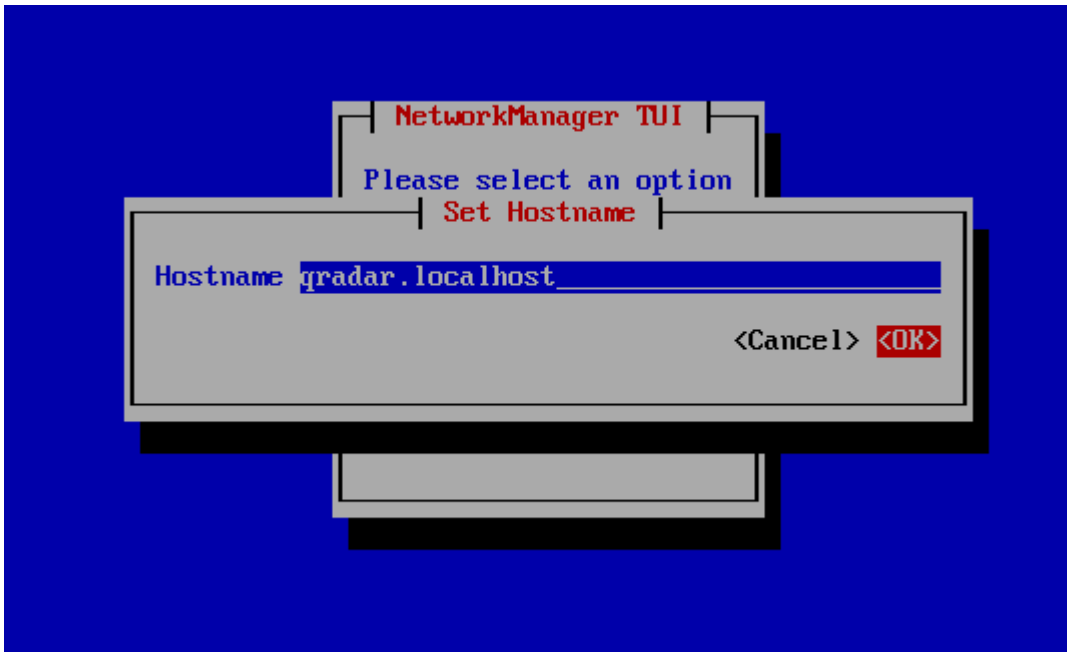
- Εσωτερική διεύθυνση IP που θα χρησιμοποιήσουμε.
- Την πύλη (gateway) του δικτύου μας.
- Τους διακομιστές DNS που θέλουμε να χρησιμοποιήσουμε.

Στη συνέχεια, απενεργοποιούμε το IPv6 Configuration, επιλέγοντας την επιλογή "Ignore."



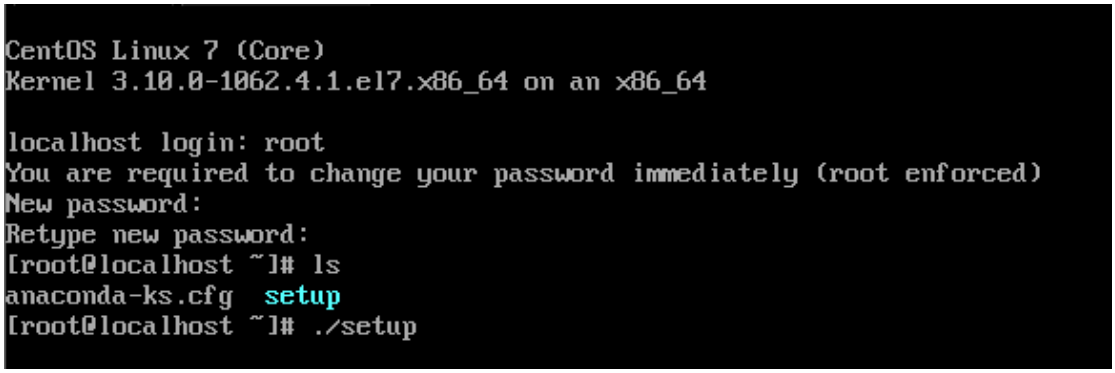
Εικόνα 3.3.6: Παραμετροποίηση δικτυακών ρυθμίσεων

Στη συνέχεια, επιστρέφουμε στην προηγούμενη οθόνη και επιλέγουμε "Set system hostname" για να ορίσουμε το όνομα του υπολογιστή μας.



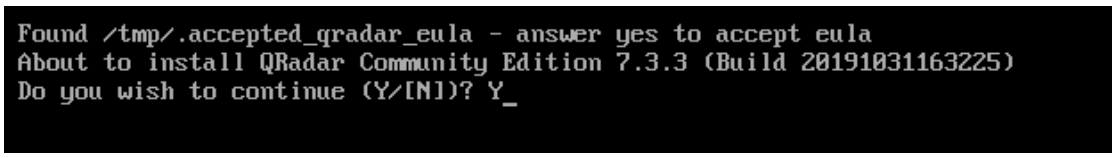
Εικόνα 3.3.7: Παραμετροποίηση ονόματος εικονικής μηχανής

Στη συνέχεια, εκτελούμε τη διαδικασία εγκατάστασης εκκινώντας το setup για να ξεκινήσει η εγκατάσταση.



Εικόνα 3.3.8: Διαδικασία εγκατάστασης

Αποδεχόμαστε τους όρους χρήσης.



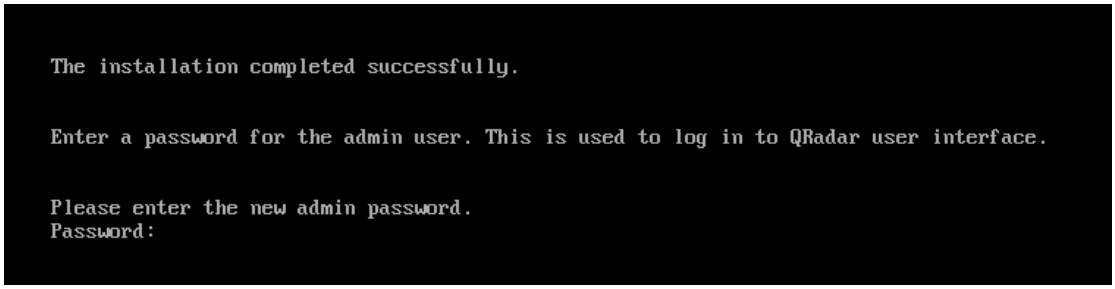
Εικόνα 3.3.9: Διαδικασία εγκατάστασης

Παρακάτω παρατηρούμε ένα στιγμιότυπο από τη διαδικασία εγκατάστασης και περιμένουμε να ολοκληρωθεί.

```
  Updating   : libblkid-2.23.2-61.el7.x86_64                              42/329
  Updating   : 2:shadow-utils-4.6-5.el7.x86_64                            43/329
  Updating   : libmount-2.23.2-61.el7.x86_64                              44/329
  Updating   : glib2-2.56.1-5.el7.x86_64                                  45/329
  Updating   : libssh2-1.8.0-3.el7.x86_64                                 46/329
  Installing : 32:bind-export-libs-9.11.4-9.P2.el7.x86_64                 47/329
  Updating   : 1:mariadb-libs-5.5.64-1.el7.x86_64                         48/329
  Updating   : logrotate-3.8.6-17.el7.x86_64                              49/329
  Updating   : nss-pem-1.0.3-7.el7.x86_64                                 50/329
  Updating   : nss-3.44.0-4.el7.x86_64                                    51/329
  Updating   : nss-sysinit-3.44.0-4.el7.x86_64                            52/329
  Updating   : nss-tools-3.44.0-4.el7.x86_64                              53/329
  Updating   : openldap-2.4.44-21.el7_6.x86_64                            54/329
  Updating   : libcurl-7.29.0-54.el7.x86_64                               55/329
  Installing : geoipupdate-2.5.0-1.el7.x86_64                             56/329
  Updating   : GeoIP-1.5.0-14.el7.x86_64                                  57/329
  Updating   : binutils-2.27-41.base.el7_7.1.x86_64                       58/329
  Updating   : 2:tar-1.26-35.el7.x86_64                                   59/329
  Installing : libnet-1.1.6-7.el7.x86_64                                  60/329
  Updating   : libndp-1.2-9.el7.x86_64                                    61/329
  Installing : libsmartcols-2.23.2-61.el7.x86_64                          62/329
  Updating   : kbd-legacy-1.15.5-15.el7.noarch                            63/329
  Updating   : ipset-libs-7.1-1.el7.x86_64                                64/329
  Installing : eventlog-0.2.13-4.el7.x86_64                               65/329
  Updating   : 32:bind-license-9.11.4-9.P2.el7.noarch                     66/329
  Updating   : libteam-1.27-9.el7.x86_64                                  67/329
  Updating   : 2:vim-minimal-7.4.629-6.el7.x86_64                         68/329
  Updating   : kernel-tools-libs-3.10.0-1062.4.1.el7.x86_64               69/329
  Updating   : kbd-misc-1.15.5-15.el7.noarch                              70/329
  Installing : json-c-0.11-4.el7_0.x86_64                                 71/329
  Updating   : util-linux-2.23.2-61.el7.x86_64                            72/329
  Updating   : procps-ng-3.3.10-26.el7_7.1.x86_64                         73/329
  Updating   : kpartx-0.4.9-127.el7.x86_64                                74/329
  Updating   : 7:device-mapper-1.02.158-2.el7_7.2.x86_64                  75/329
  Updating   : 7:device-mapper-libs-1.02.158-2.el7_7.2.x86_64             76/329
  Updating   : cryptsetup-libs-2.0.3-5.el7.x86_64                         77/329
  Updating   : dracut-033-564.el7.x86_64                                  78/329
  Updating   : kmod-20-25.el7.x86_64                                      79/329
  Updating   : elfutils-libs-0.176-2.el7.x86_64                           80/329
  Updating   : systemd-libs-219-67.el7_7.2.x86_64                         81/329
  Updating   : 1:dbus-libs-1.10.24-13.el7_6.x86_64                        82/329
  Updating   : systemd-219-67.el7_7.2.x86_64                              83/329
  Updating   : 1:dbus-1.10.24-13.el7_6.x86_64                             84/329
  Updating   : elfutils-default-yama-scope-0.176-2.el7.noarch             85/329
  Updating   : initscripts-9.49.47-1.el7.x86_64                           86/329
  Updating   : systemd-sysv-219-67.el7_7.2.x86_64                         87/329
  Updating   : 7:device-mapper-event-libs-1.02.158-2.el7_7.2.x86_64       88/329
```

Εικόνα 3.3.10: Διαδικασία εγκατάστασης

Μόλις ολοκληρωθεί η εγκατάσταση με επιτυχία, ζητείται από εμάς να ορίσουμε έναν κωδικό πρόσβασης για τον χρήστη "admin." Ο χρήστης "admin" είναι ο διαχειριστικός χρήστης του γραφικού περιβάλλοντος του QRadar.

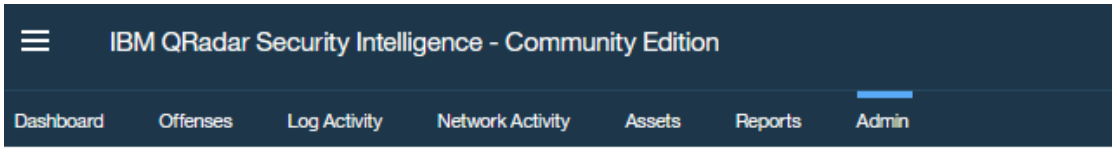


Εικόνα 3.3.11: Δημιουργία κωδικού χρήστη

Στη συνέχεια, κάνουμε επανεκκίνηση της εικονικής μηχανής μας, χρησιμοποιώντας την εντολή "reboot."

Μόλις το QRadar επανεκκινηθεί και όλες οι υπηρεσίες του είναι ενεργές, ανοίγουμε τον περιηγητή μας (browser) και επισκεπτόμαστε την εσωτερική διεύθυνση IP που έχουμε ορίσει στον υπολογιστή μας.

Αφού συνδεθούμε χρησιμοποιώντας τα διαπιστευτήρια που δημιουργήσαμε στο τελευταίο βήμα, επιλέγουμε την καρτέλα "Admin."



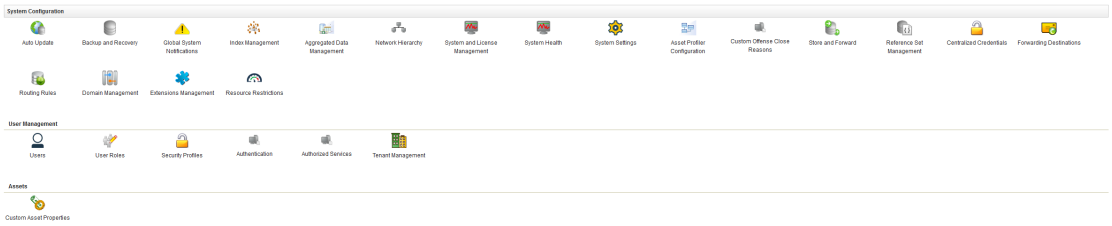
Εικόνα 3.3.12: Διαχειριστικό μέρος του QRadar

Από εκεί ξεκινάμε τη βασική διαμόρφωση για τη σωστή λειτουργία του συστήματός μας πριν λάβει οποιαδήποτε αρχεία καταγραφής (logs).

Τα βασικά σημεία που θα εξετάσουμε είναι τα εξής:

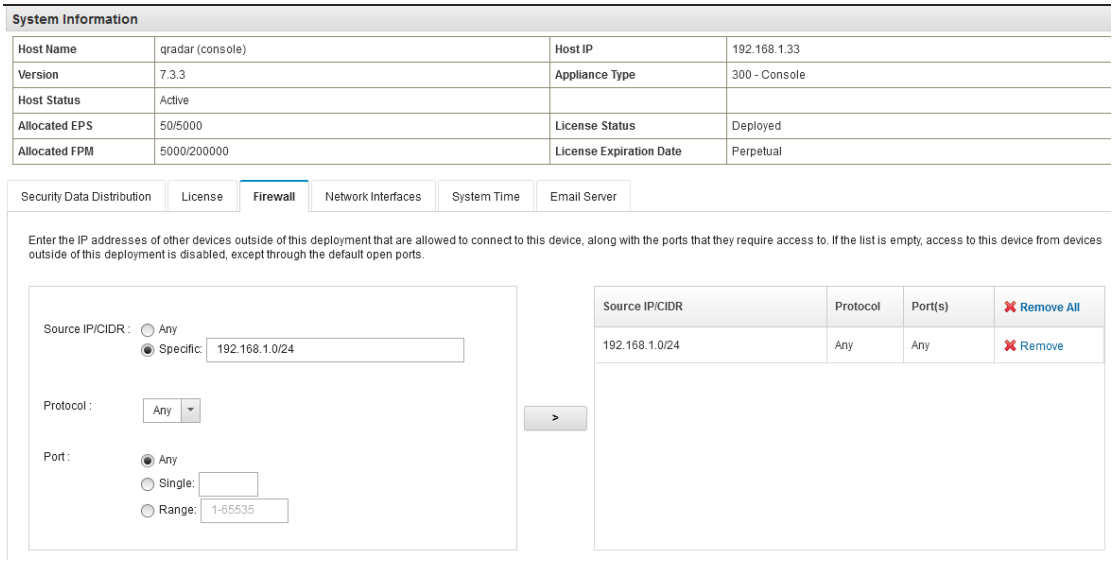
- Network Hierarchy (Δομή Δικτύου): Εδώ καταχωρούμε πληροφορίες σχετικά με τα εσωτερικά μας δίκτυα, έτσι ώστε το QRadar να γνωρίζει την τοπολογία του δικτύου μας.
- System and License Management (Διαχείριση Συστήματος και Άδειες): Εδώ διαχειριζόμαστε το σύστημα QRadar και τις άδειες χρήσης.

Αυτά τα βήματα είναι σημαντικά για να διασφαλίσουμε ότι το σύστημα είναι προετοιμασμένο και διαμορφωμένο σωστά πριν αρχίσει να λαμβάνει και να αναλύει καταγραφές.



Εικόνα 3.3.13: Διαχειριστικό μέρος του QRadar

Firewall (Διαμόρφωση τοπικού τείχους προστασίας): Επιλέγουμε την επιλογή firewall για να επιτρέψουμε το τοπικό firewall να επιτρέψει την κίνηση από τα δίκτυα από τα οποία θα λαμβάνουμε καταγραφές και θα υπάρχει πρόσβαση στο QRadar.

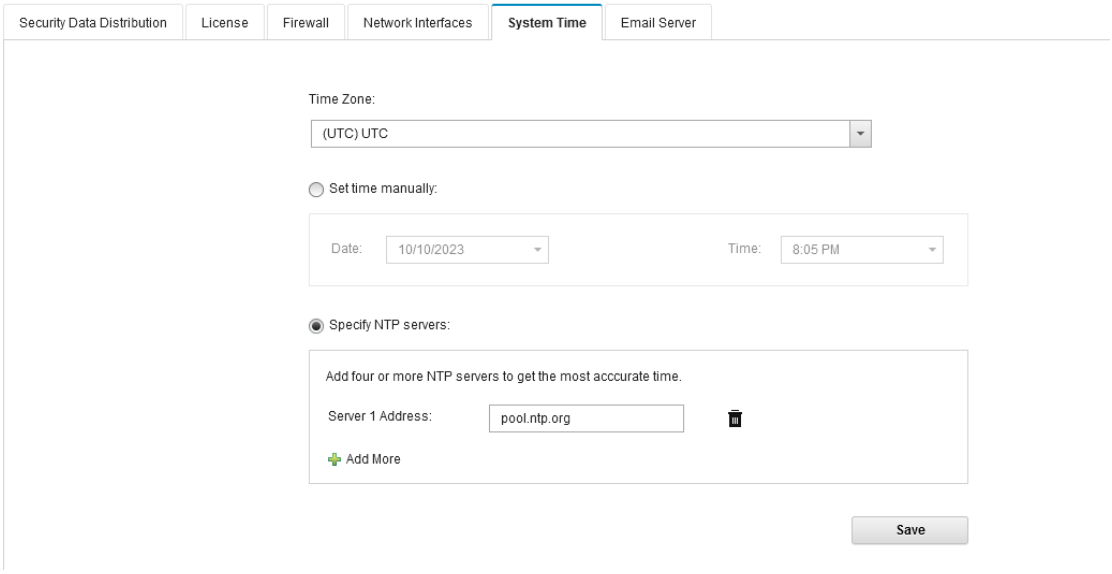


Εικόνα 3.3.14: Διαχειριστικό μέρος του QRadar για το τοπικό firewall

Για την ρύθμιση της ώρας του συστήματος, μπορούμε να το κάνουμε με τους εξής τρεις τρόπους:

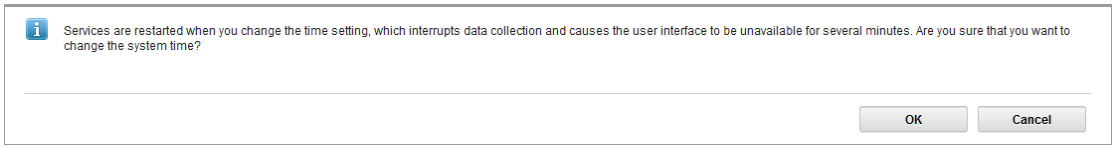
1. Χρήση της Ζώνης Ώρας της Χώρας: Μπορούμε να επιλέξουμε τη ζώνη ώρας της χώρας μας.
2. Χειροκίνητη Ρύθμιση Ώρας και Ημερομηνίας: Μπορούμε επίσης να ορίσουμε χειροκίνητα την ώρα και την ημερομηνία.
3. Χρήση NTP (Network Time Protocol) Servers: Μπορούμε να δηλώσουμε εσωτερικούς ή εξωτερικούς διακομιστές NTP για να συγχρονίσουμε την ώρα του συστήματός μας.

Τέλος, πατάμε το "Save" για να αποθηκεύσουμε τις ρυθμίσεις.



Εικόνα 3.3.15: Διαχειριστικό μέρος του QRadar για την παραμετροποίηση της ώρας

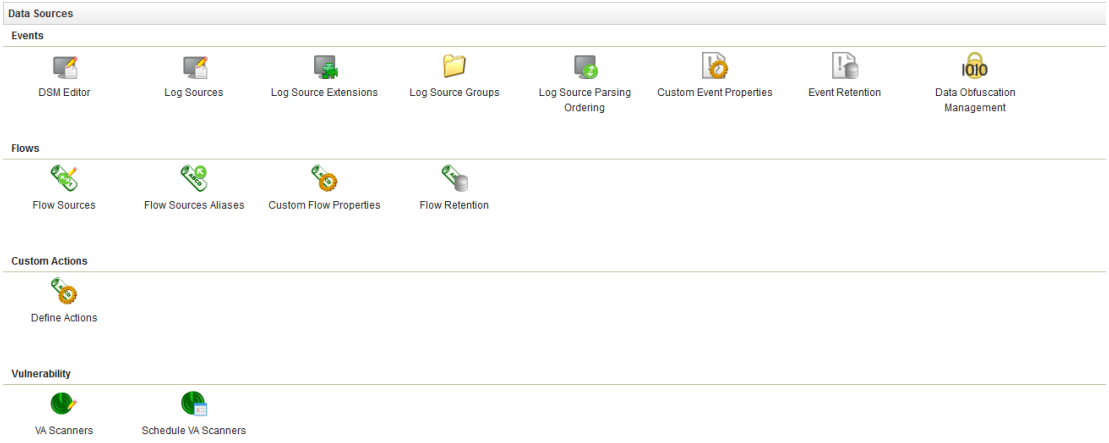
Αφού λάβουμε την ενημέρωση ότι θα γίνει επανεκκίνηση των υπηρεσιών, πατάμε το "OK" για να συνεχίσουμε.



Εικόνα 3.3.16: Διαχειριστικό μέρος του QRadar για την επιβεβαίωση των αλλαγών

Στην κατηγορία "Data Sources" (Πηγές Δεδομένων), μεταγενέστερα θα δούμε τις υποκατηγορίες "Log Sources" (Κατηγορίες Καταγραφής) και "Custom Event Properties" (Προσαρμοσμένες Ιδιότητες Συμβάντος).

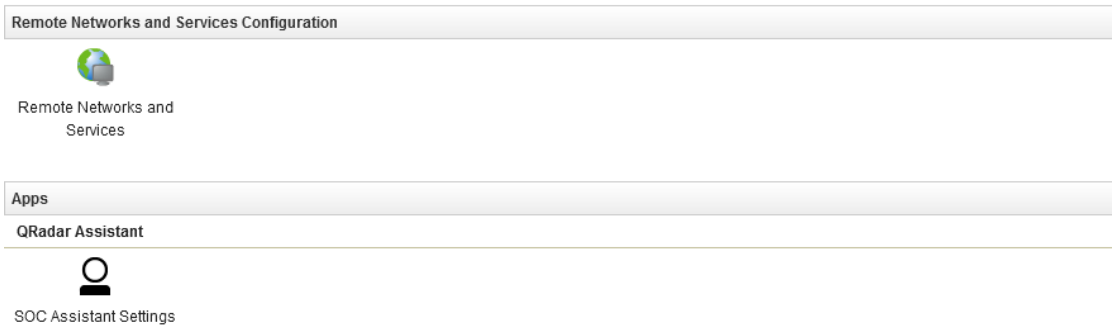
Από εκεί μπορούμε να διαμορφώσουμε τις ρυθμίσεις που σχετίζονται με τη συλλογή και την ανάλυση των καταγραφών και των προσαρμοσμένων ιδιοτήτων των συμβάντων.



Εικόνα 3.3.17: Διαχειριστικό μέρος του QRadar στην κατηγορία Data Sources

Τέλος, θα βρούμε επίσης τις κατηγορίες "Remote Networks and Services Configuration" (Απομακρυσμένες Δίκτυο και Ρυθμίσεις Υπηρεσιών) και "Applications" (Εφαρμογές).

Σε αυτές τις κατηγορίες μπορείτε να διαμορφώσετε τις ρυθμίσεις που σχετίζονται με την επικοινωνία με απομακρυσμένα δίκτυα και υπηρεσίες, καθώς και τις ρυθμίσεις που σχετίζονται με εφαρμογές που είναι εγκατεστημένες στο σύστημα.



Εικόνα 3.3.18: Διαχειριστικό μέρος του QRadar στην κατηγορία Remote Networks and Services Configuration

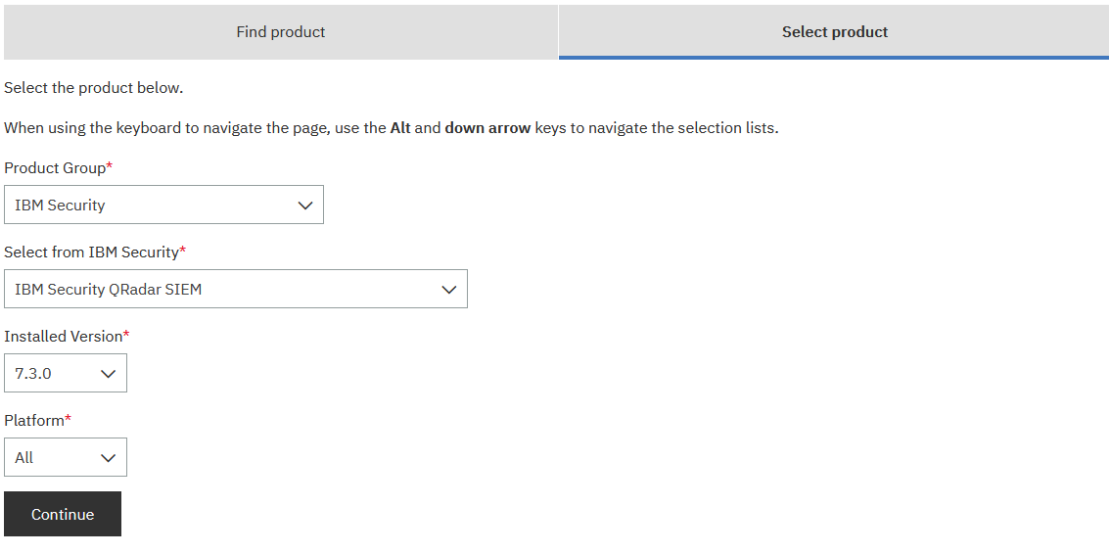
Για λεπτομερείς πληροφορίες και ενδεχομένως επιπλέον ρυθμίσεις στο IBM Security QRadar, μπορείτε να ανατρέξετε στο εγχειρίδιο διαχείρισης (Administration Guide) για την έκδοση 7.3.0 του προϊόντος. Αυτό το εγχειρίδιο θα περιλαμβάνει λεπτομερείς οδηγίες και ρυθμίσεις για όλες τις διαθέσιμες επιλογές και υποκατηγορίες, ώστε να μπορείτε να διαμορφώσετε το σύστημά σας όπως επιθυμείτε.

Για να εγκαταστήσετε το πακέτο WinCollect και να διαμορφώσετε τη λήψη καταγραφών από συστήματα Windows, πρέπει να συνδεθείτε μέσω SSH στην IP διεύθυνση που έχετε ορίσει στο QRadar σας. Χρησιμοποιήστε τον χρήστη "root" και τον κωδικό πρόσβασης που δημιουργήσατε κατά την εγκατάσταση.

Μόλις συνδεθείτε, μπορείτε να προχωρήσετε στην εγκατάσταση του πακέτου WinCollect και τη ρύθμιση της λήψης καταγραφών από τα Windows συστήματα σας. Ακολουθήστε τις οδηγίες στο εγχειρίδιο του QRadar για να ολοκληρώσετε αυτήν τη διαδικασία.

Για να αναζητήσετε τα διαθέσιμα προϊόντα για την έκδοση σας μέσω της ιστοσελίδας της.

Μπορείτε να περιηγηθείτε στην ιστοσελίδα της IBM και να βρείτε περισσότερες πληροφορίες σχετικά με τα προϊόντα και τις υπηρεσίες του QRadar που είναι διαθέσιμα για την εκδοσή σας.

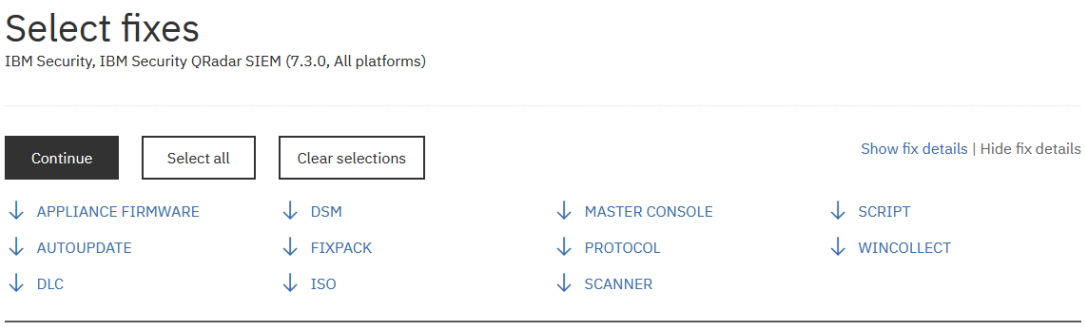


Εικόνα 3.3.19: Ιστοσελίδα λήψης Wincollect Agent

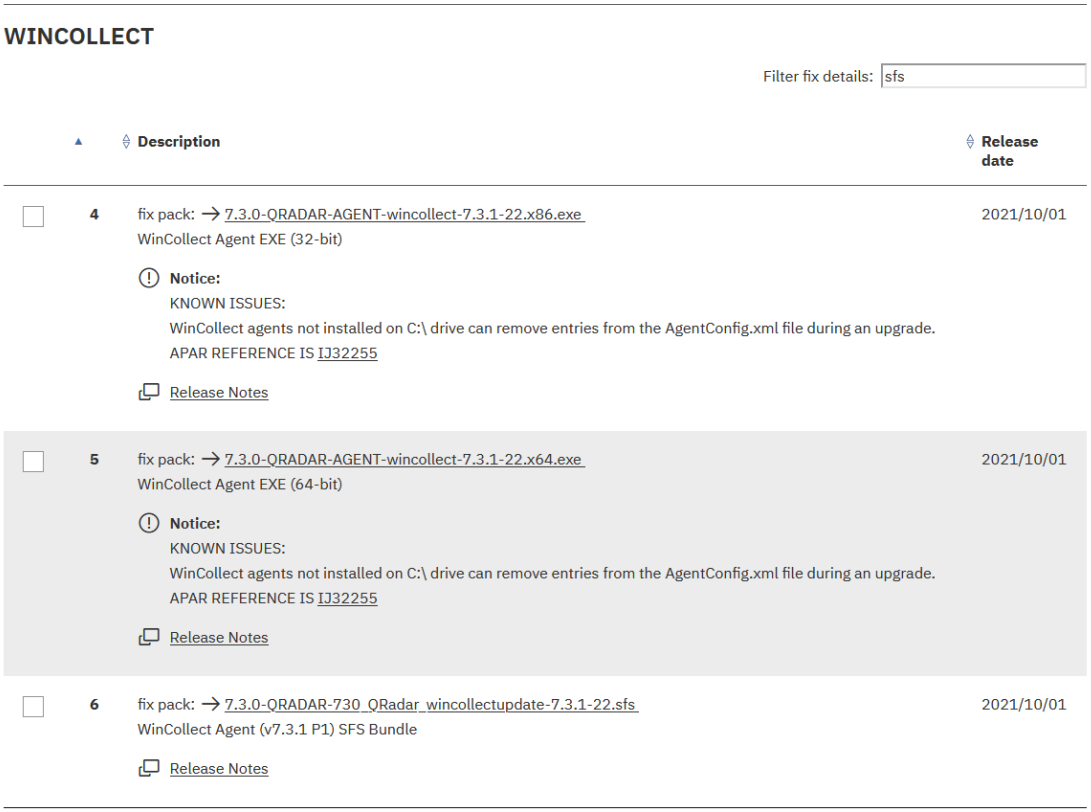
Για τη λήψη των απαιτούμενων αρχείων για την εγκατάσταση του WinCollect, ακολουθήστε αυτά τα βήματα:

1. Στην ιστοσελίδα της IBM όπου προβάλλετε τα προϊόντα του QRadar για τη συγκεκριμένη έκδοση, επιλέξτε "WinCollect."
2. Από εκεί, πρέπει να βρείτε ένα αρχείο .sfs για να εγκατασταθεί το Wincollect στο QRadar.
3. Κάντε κλικ στον αντίστοιχο σύνδεσμο λήψης για να ξεκινήσετε τη λήψη του αρχείου στον υπολογιστή σας.

Αφού κατεβάσετε τα αρχεία, θα μπορείτε να συνεχίσετε με τη διαδικασία εγκατάστασης του WinCollect στο QRadar και του επιπλέον WinCollect server στον υπολογιστή Windows.



Εικόνα 3.3.20: Ιστοσελίδα λήψης Wincollect Agent

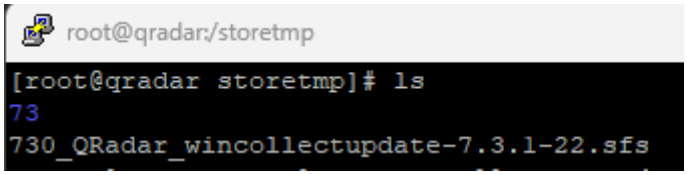


Εικόνα 3.3.21: Ιστοσελίδα λήψης Wincollect– επιλογή έκδοσης

Ακολουθώντας τις οδηγίες από τον οδηγό του WinCollect, θα πρέπει να δημιουργήσετε τους απαραίτητους φακέλους και να ανεβάσετε το αρχείο .sfs στον φάκελο /storetmp.

Ανέβετε το αρχείο .sfs στον φάκελο /storetmp

Αφού ανεβάσετε το αρχείο .sfs, μπορείτε να συνεχίσετε με τη διαδικασία εγκατάστασης του WinCollect στο QRadar σύμφωνα με τις οδηγίες από τον οδηγό WinCollect.



Εικόνα 3.3.22: Διαδικασία εγκατάστασης Wincollect στο Qradar

Η εντολή `mount` χρησιμοποιείται για τη σύνδεση (mount) ενός αρχείου στο σύστημα αρχείων ως αντίστοιχος κατάλογος, επιτρέποντάς σας να αποκτήσετε πρόσβαση στο περιεχόμενο του αρχείου. Στην περίπτωσή σας, θέλετε να κάνετε mount το αρχείο .sfs. Εδώ είναι πώς μπορείτε να το κάνετε:

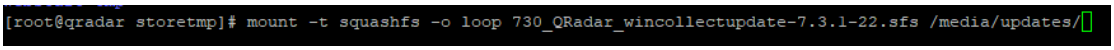
mount -t squashfs -o loop /storetmp/Installer_file_name.sfs /media/updates

Αυτή η εντολή κάνει τα εξής:

- Το `-t squashfs` καθορίζει τον τύπο του αρχείου (στην περίπτωσή σας, squashfs).

- Το `-o loop` χρησιμοποιεί τη συσκευή loopback για την εκτέλεση του mount.
- `/storetmp/Installer_file_name.sfs` είναι η διαδρομή προς το αρχείο .sfs που ανεβάσατε.
- `/media/updates` είναι ο κατάλογος προορισμού όπου το αρχείο θα γίνει mount.

Αφού εκτελέσετε αυτήν την εντολή, το αρχείο .sfs θα γίνει mount στον κατάλογο `/media/updates`, και θα μπορείτε να συνεχίσετε με τη διαδικασία εγκατάστασης στο QRadar σύμφωνα με τις οδηγίες από τον οδηγό WinCollect.

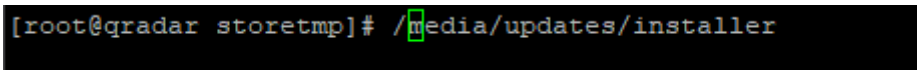


Εικόνα 3.3.23: Διαδικασία εγκατάστασης Wincollect στο Qradar

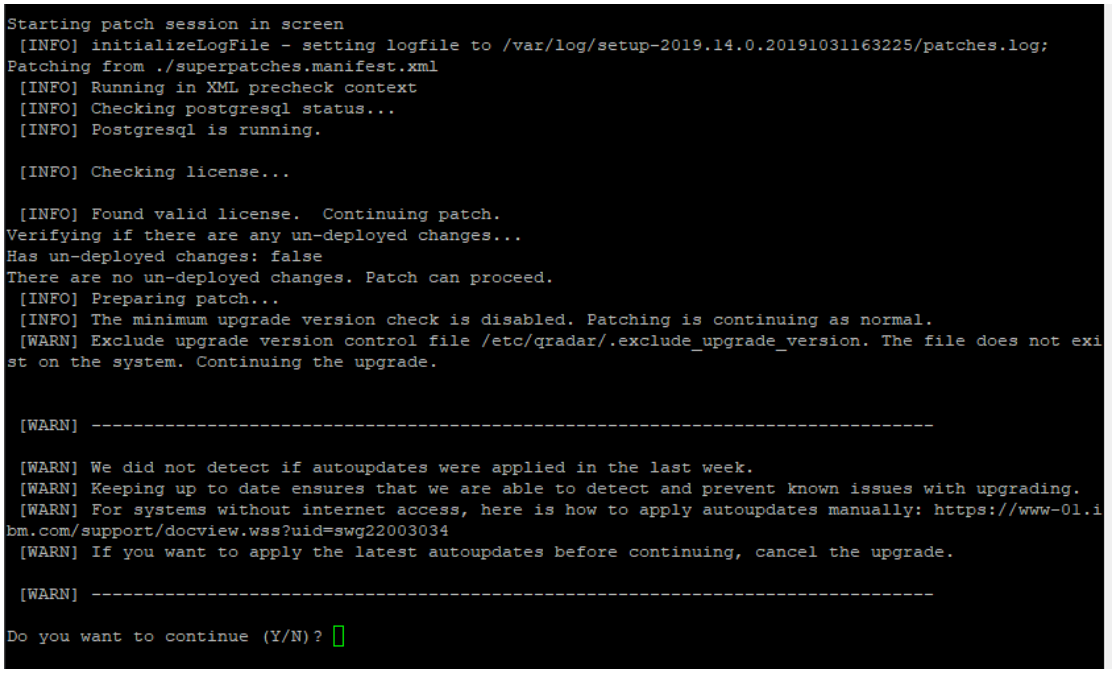
Με την εντολή `/media/updates/installer`, εκτελείτε τον εγκαταστάτη του WinCollect που έχετε προηγουμένως mount ως squashfs αρχείο. Αυτή η εντολή θα ξεκινήσει τη διαδικασία εγκατάστασης του WinCollect στο σύστημα σας, σύμφωνα με τις οδηγίες που παρέχονται από τον εγκαταστάτη.

Αναμένετε ώστε ο εγκαταστάτης να ολοκληρώσει τη διαδικασία εγκατάστασης και να ακολουθήσετε τις οδηγίες που εμφανίζονται στην οθόνη για να ρυθμίσετε το WinCollect όπως απαιτείται.

Μετά την εγκατάσταση, μπορείτε να συνεχίσετε με τη ρύθμιση του WinCollect για να λαμβάνει καταγραφές από τα συστήματα Windows όπως απαιτείται για την διαδικασία του QRadar.



Εικόνα 3.3.24: Διαδικασία εγκατάστασης Wincollect στο Qradar



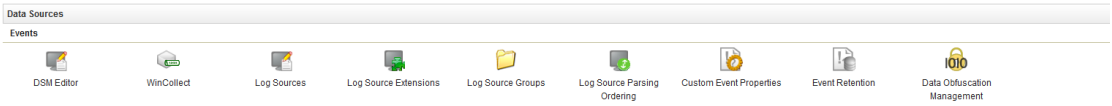
Εικόνα 3.3.25: Διαδικασία εγκατάστασης Wincollect στο Qradar

```
================================================================================
 Package                    Arch    Version            Repository            Size
================================================================================
Installing:
 AGENT-WINCOLLECT           noarch 7.3-20210928014626 qradar-upgrade-local 8.0 M
 PROTOCOL-WinCollectConfigServer
                            noarch 7.3-20210928014626 qradar-upgrade-local 157 k
 PROTOCOL-WinCollectFileForwarder
                            noarch 7.3-20210928014626 qradar-upgrade-local 193 k
 PROTOCOL-WinCollectJuniperSBR
                            noarch 7.3-20210928014626 qradar-upgrade-local 159 k
 PROTOCOL-WinCollectMicrosoftDHCP
                            noarch 7.3-20210928014626 qradar-upgrade-local 162 k
 PROTOCOL-WinCollectMicrosoftDNS
                            noarch 7.3-20210928014626 qradar-upgrade-local 228 k
 PROTOCOL-WinCollectMicrosoftExchange
                            noarch 7.3-20210928014626 qradar-upgrade-local 104 k
 PROTOCOL-WinCollectMicrosoftIAS
                            noarch 7.3-20210928014626 qradar-upgrade-local 208 k
 PROTOCOL-WinCollectMicrosoftIIS
                            noarch 7.3-20210928014626 qradar-upgrade-local 100 k
 PROTOCOL-WinCollectMicrosoftISA
                            noarch 7.3-20210928014626 qradar-upgrade-local 171 k
 PROTOCOL-WinCollectMicrosoftSQL
                            noarch 7.3-20210928014626 qradar-upgrade-local 133 k
 PROTOCOL-WinCollectNetAppDataONTAP
                            noarch 7.3-20210928014626 qradar-upgrade-local 244 k
 PROTOCOL-WinCollectWindowsEventLog
                            noarch 7.3-20210928014626 qradar-upgrade-local  13 M

Transaction Summary
================================================================================
Install  13 Packages
Total download size: 23 M
Installed size: 24 M
Downloading packages:
--------------------------------------------------------------------------------
Total                                           324 MB/s |  23 MB  00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing AGENT-WINCOLLECT-7.3-20210928014626  with Agent 7.3.1-22
  Installing : AGENT-WINCOLLECT-7.3-20210928014626.noarch                  1/13
Installed rpm AGENT-WINCOLLECT-7.3-20210928014626 with Agent 7.3.1-22
Installing PROTOCOL-WinCollectMicrosoftIAS-7.3-20210928014626
```

Εικόνα 3.3.26: Διαδικασία εγκατάστασης Wincollect στο Qradar

Το εικονίδιο "wincollect" που παρατηρείτε στην κατηγορία "Data Sources" σημαίνει ότι η εγκατάσταση του WinCollect ολοκληρώθηκε με επιτυχία και το WinCollect τώρα είναι διαθέσιμο ως πηγή δεδομένων για το QRadar. Από αυτό το σημείο, μπορείτε να ρυθμίσετε το WinCollect για να λαμβάνει καταγραφές από τα συστήματα Windows όπως απαιτείται για την διαδικασία του QRadar.

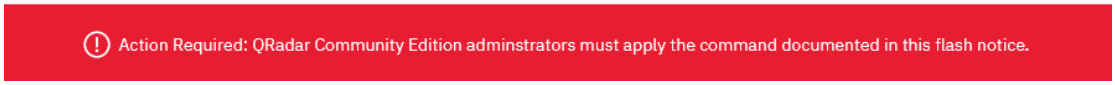


Εικόνα 3.3.27: Διαχειριστικό μέρος του QRadar στην κατηγορία Data Sources

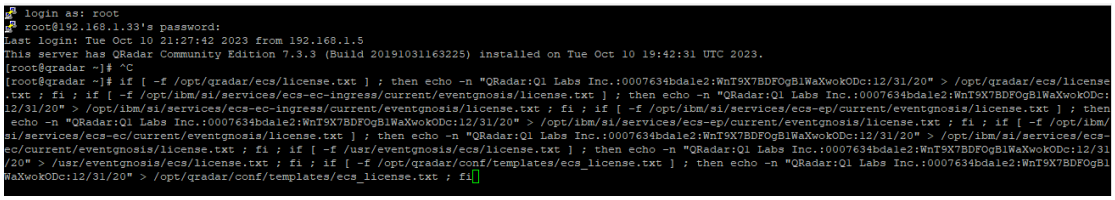
Τέλος ακολουθούμε την παρακάτω οδηγία της IBM για την αντιμετώπιση ενός προβλήματος που εμφανίστηκε στην έκδοση.

Ακολουθούμε τις οδηγίες που μας δίνονται στο παρακάτω σύνδεσμο για την επίλυση του προβλήματος.

https://www.ibm.com/support/pages/node/6395080



Εικόνα 3.3.28: Ενημέρωση σφάλματος για την έκδοση



Εικόνα 3.3.29: Εφαρμογή ενημέρωσης

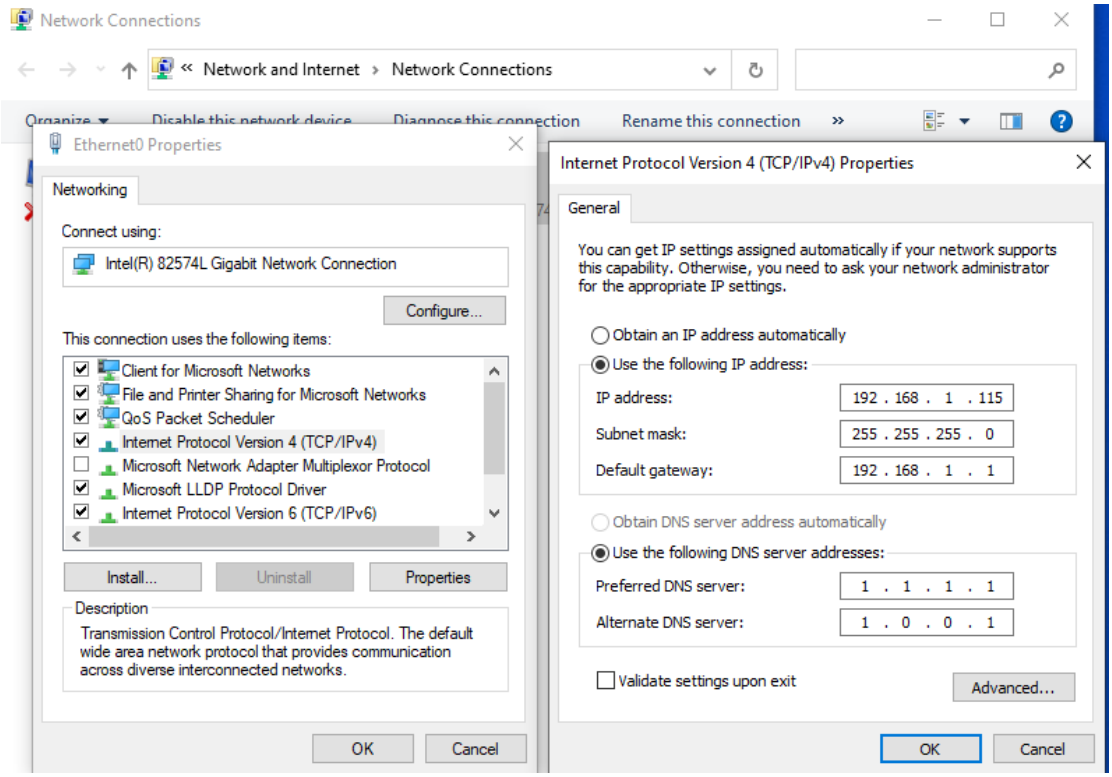
3.4 Παραμετροποίηση των Windows 10 WinCollect

Στο παρακάτω υποκεφάλαιο, θα παρουσιάσουμε τη διαδικασία εγκατάστασης και παραμετροποίησης του Wincollect Agent σε Windows 10 αλλά και τη σύνδεση του με το QRadar για την αποστολή καταγραφών.

Μετά τη λήψη του αρχείου εγκατάστασης από την επίσημη ιστοσελίδα της Microsoft, ακολουθούμε τη διαδικασία εγκατάστασης του λειτουργικού συστήματος Windows, η οποία θεωρείτε γνωστή. Στη συγκεκριμένη περίπτωση, χρησιμοποιούμε την έκδοση Windows 10 Professional 22H2 x64.

Στο επόμενο βήμα μας θα προχωρήσουμε στην παραμετροποίηση των αρχείων καταγραφής όπως περιεγράφηκε στο υποκεφάλαιο 3.2

Στη συνέχεια κάνουμε παραμετροποίηση τις δικτυακές ρυθμίσεις με σκοπό να θέσουμε μια σταθερή IP η οποία θα επικοινωνεί με το Qradar.

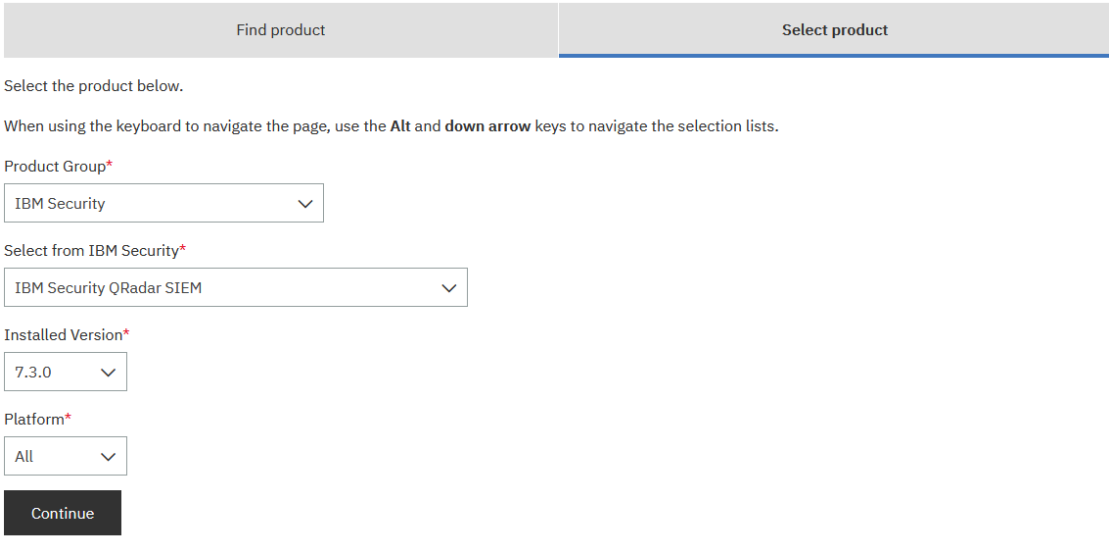


Εικόνα 3.4.1: Παραμετροποίηση δικτύου

Για να εγκαταστήσουμε τον WinCollect Agent και να προωθήσουμε τις καταγραφές στο QRadar θα πρέπει να μεταβούμε στην ιστοσελίδα της IBM και να κατεβάσουμε το εκτελέσιμο αρχείο που προσφέρει και ταιριάζει με την έκδοση που κατεβάσαμε και εγκαταστήσαμε στο QRadar

Αναζητούμε τα διαθέσιμα προϊόντα για την έκδοση σας μέσω της ιστοσελίδας της IBM.

Περιηγούμαστε στην ιστοσελίδα της IBM και να βρούμε περισσότερες πληροφορίες σχετικά με τα προϊόντα και τις υπηρεσίες του QRadar που είναι διαθέσιμα για την έκδοσή σας.

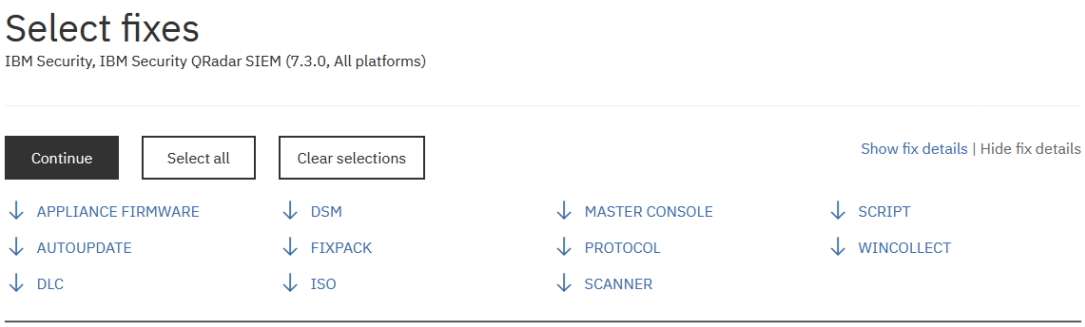


Εικόνα 3.4.2: Ιστοσελίδα λήψης Wincollect Agent

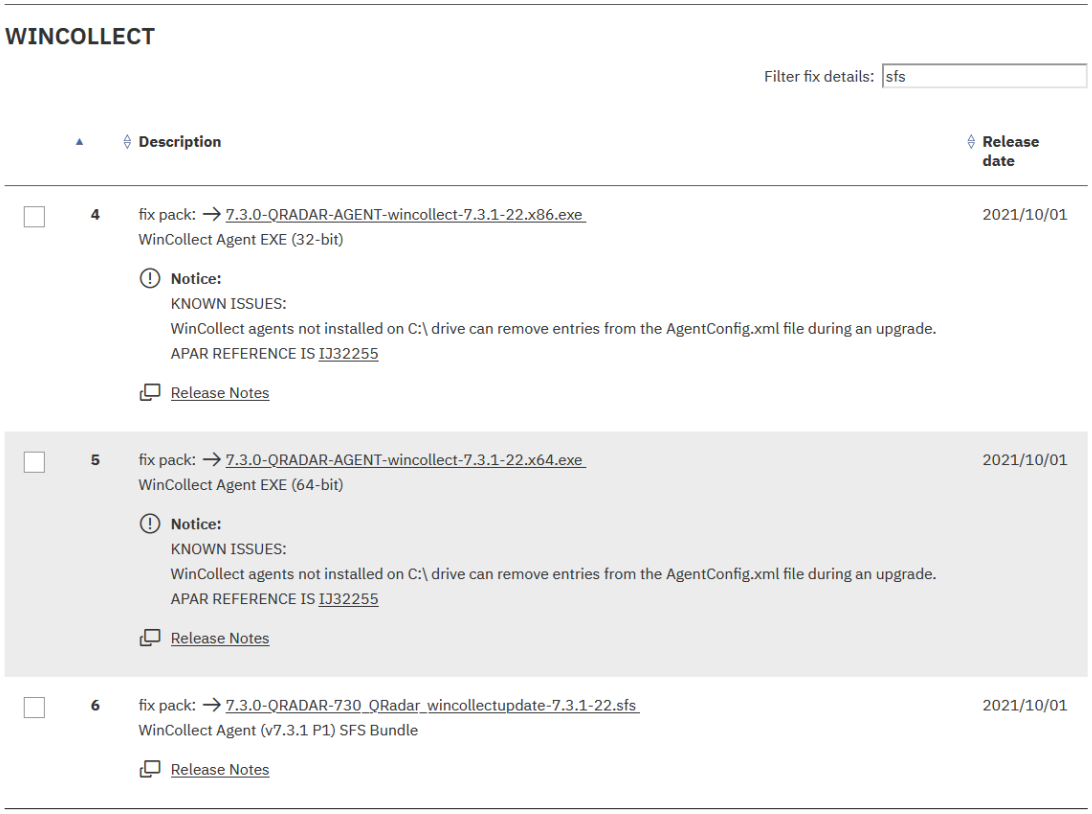
Για τη λήψη των απαιτούμενων αρχείων για την εγκατάσταση του WinCollect, ακολουθήστε αυτά τα βήματα:

1. Στην ιστοσελίδα της IBM όπου προβάλλετε τα προϊόντα του QRadar για τη συγκεκριμένη έκδοση, επιλέξτε "WinCollect."
2. Από εκεί, πρέπει να βρείτε ένα αρχείο .exe για να εγκατασταθεί το Wincollect στα Windows. Προσέχουμε η έκδοση των Windows να ταιριάζει με αυτή του QRadar που κατεβάσαμε και εγκαταστήσαμε.
3. Κάντε κλικ στον αντίστοιχο σύνδεσμο λήψης για να ξεκινήσετε τη λήψη του αρχείου στον υπολογιστή σας.

Αφού κατεβάσετε το αρχείο, θα μπορείτε να συνεχίσετε με τη διαδικασία εγκατάστασης του WinCollect Agent στον υπολογιστή Windows.

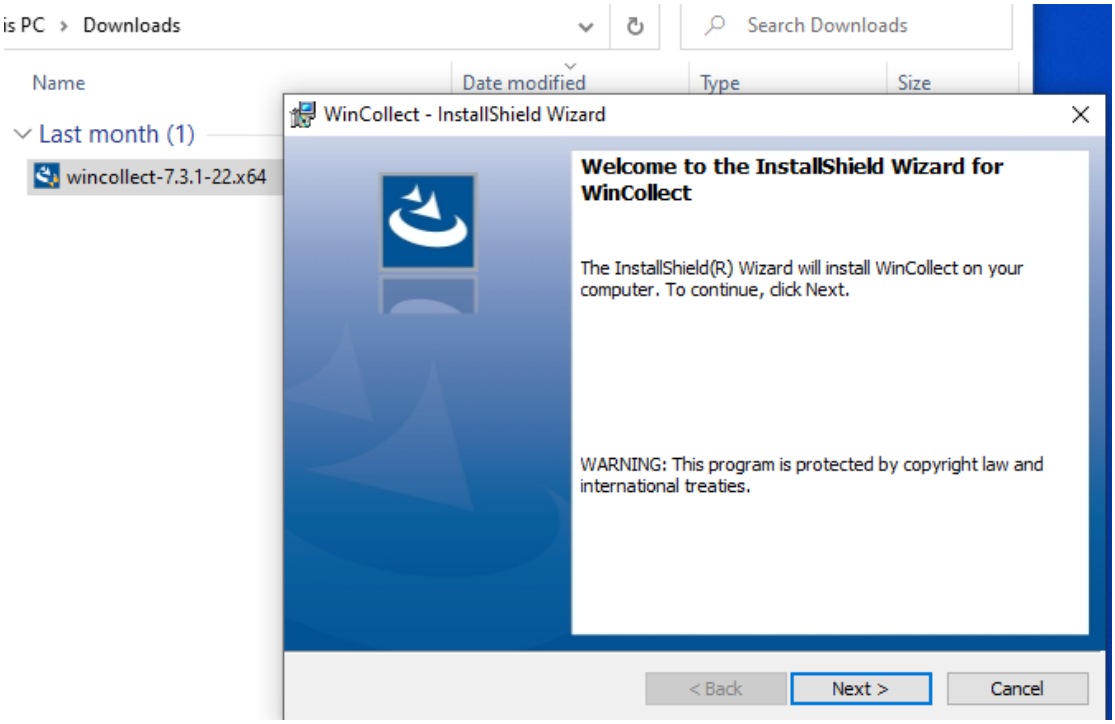


Εικόνα 3.4.3: Ιστοσελίδα λήψης Wincollect Agent



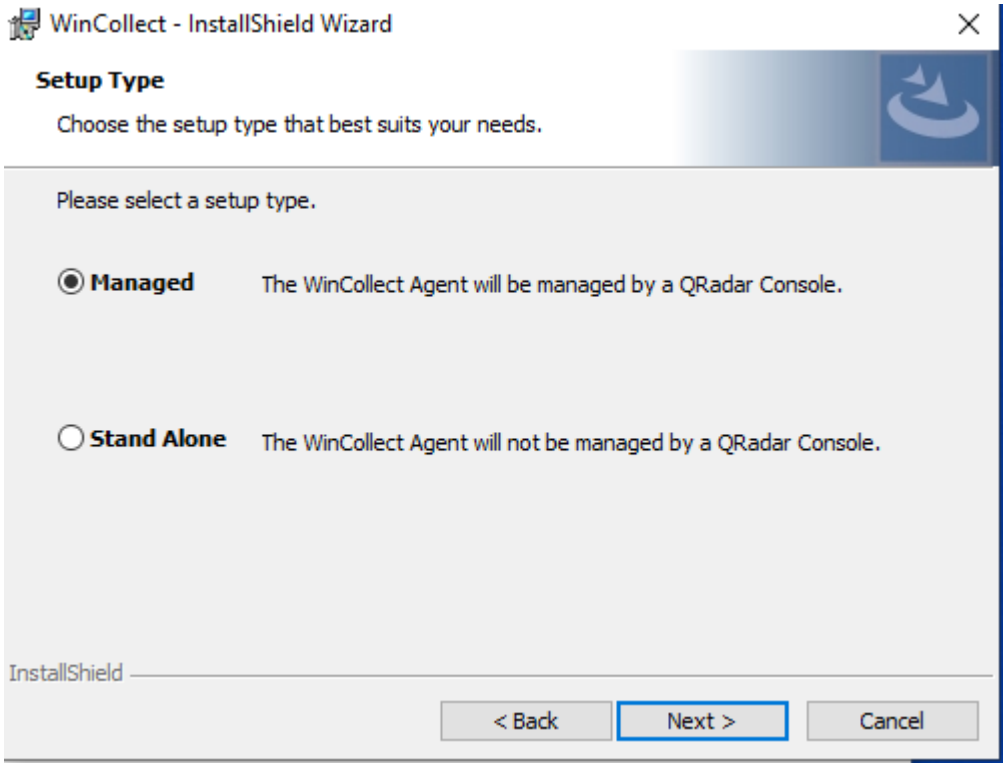
Εικόνα 3.4.4: Επιλογή έκδοσης Wincollect Agent

Ακολουθώντας τις οδηγίες από τον οδηγό εγκατάστασης του WinCollect, εκτελέσουμε το αρχείο που κατεβάσαμε με δικαιώματα διαχειριστή.



Εικόνα 3.4.5: Εγκατάσταση Wincollect Agent

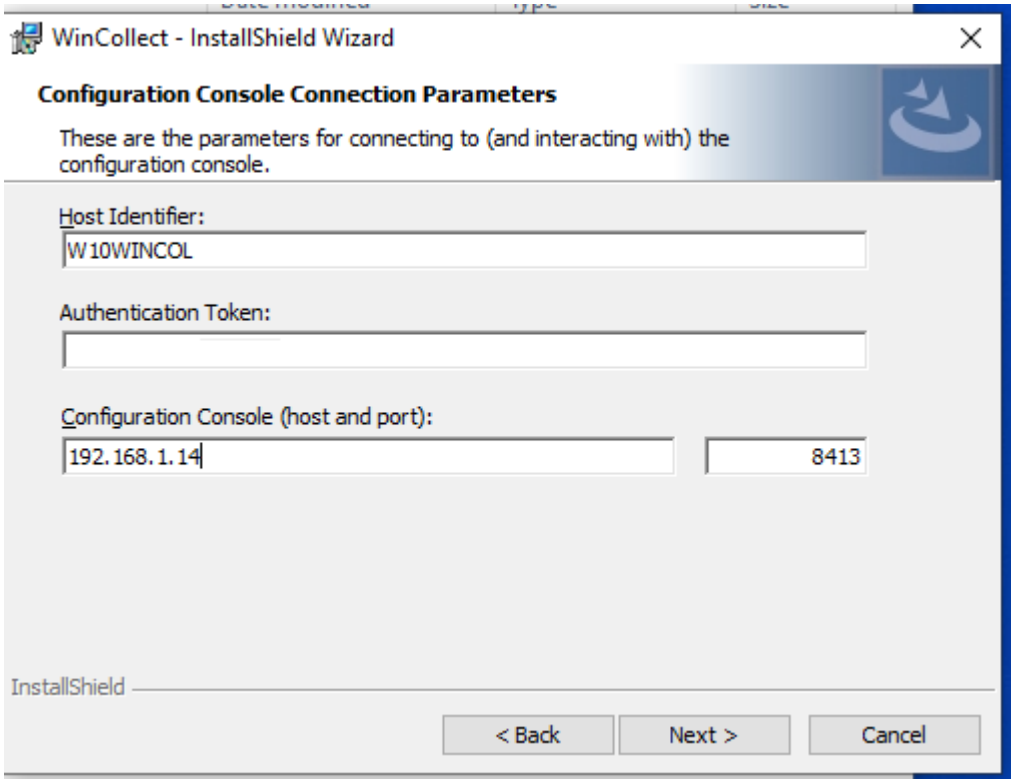
Συνεχίζουμε την εγκατάσταση και στο σημείο που μας ζητάει τον τύπο της εγκατάστασης επιλέγουμε Managed. Οι διαφορές τους περιγράφονται αναλυτικά στον οδηγό εγκατάστασης Wincollect



Εικόνα 3.4.6: Εγκατάσταση Wincollect Agent

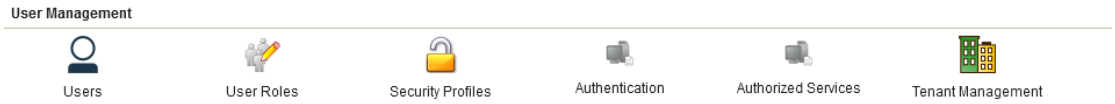
Στη συνέχεια θα μας ζητηθούν πληροφορίες παραμετροποίησης

- Host Identifier: Το όνομα του host όπως θα εμφανίζεται στο QRadar
- Authentication Token: Ένα service token το οποίο δημιουργούμε στην κονσόλα του QRadar και είναι υπεύθυνο για την αυθεντικοποίηση μεταξύ QRadar και Wicnollect Agent
- Configuration Console (host & port): Θέτουμε την IP της κονσόλας του QRadar όπου θα γίνει η επικοινωνία. Η πόρτα είναι προεπιλεγμένη και αναφέρεται στον οδηγό εγκατάστασης Wincollect



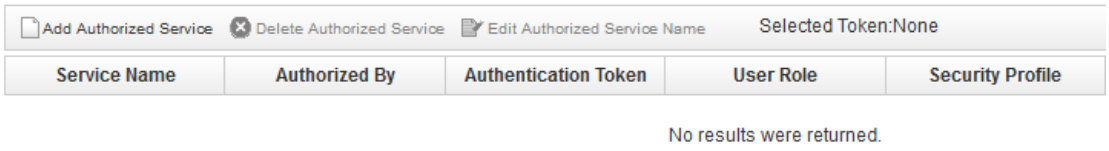
Εικόνα 3.4.7: Εγκατάσταση Wincollect Agent

Επιστρέφουμε στο QRadar για τη δημιουργία του Authentication Token. Στην ενότητα User Management επιλέγουμε Authentication Services



Εικόνα 3.4.8: Δημιουργία του Authentication Token

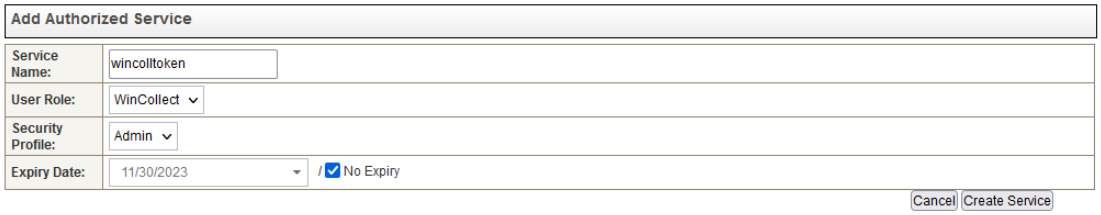
Στο νέο παράθυρο που θα ανοίξει επιλέγουμε Add Authorized Service



Εικόνα 3.4.9: Δημιουργία του Authentication Token

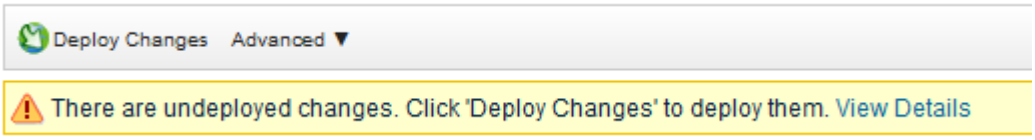
Στη συνέχεια συμπληρώνουμε τις επιλογές που μας δίνονται και επιλέγουμε Create Service

- Service Name: Δίνουμε ένα όνομα στο Service μας
- User Role: Ο ρόλος που επιλέγουμε είναι ο WinCollect
- Security Profile: Το Securty Profile είναι Admin
- Expiry Date: Σιγουρευόμαστε πως το No Expiry είναι επιλεγμένο



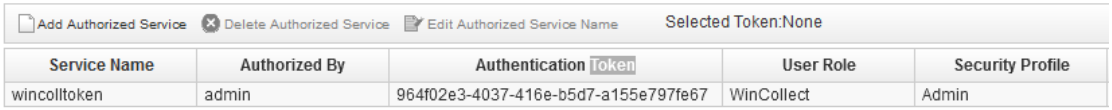
Εικόνα 3.4.10: Δημιουργία του Authentication Token

Μετά την παραπάνω διαδικασία μας έχει εμφανιστεί ένα μήνυμα στο QRadar όπου μας ενημερώνει πως υπάρχουν αλλαγές στο σύστημα και μας ζητάει Deploy το οποίο και κάνουμε.



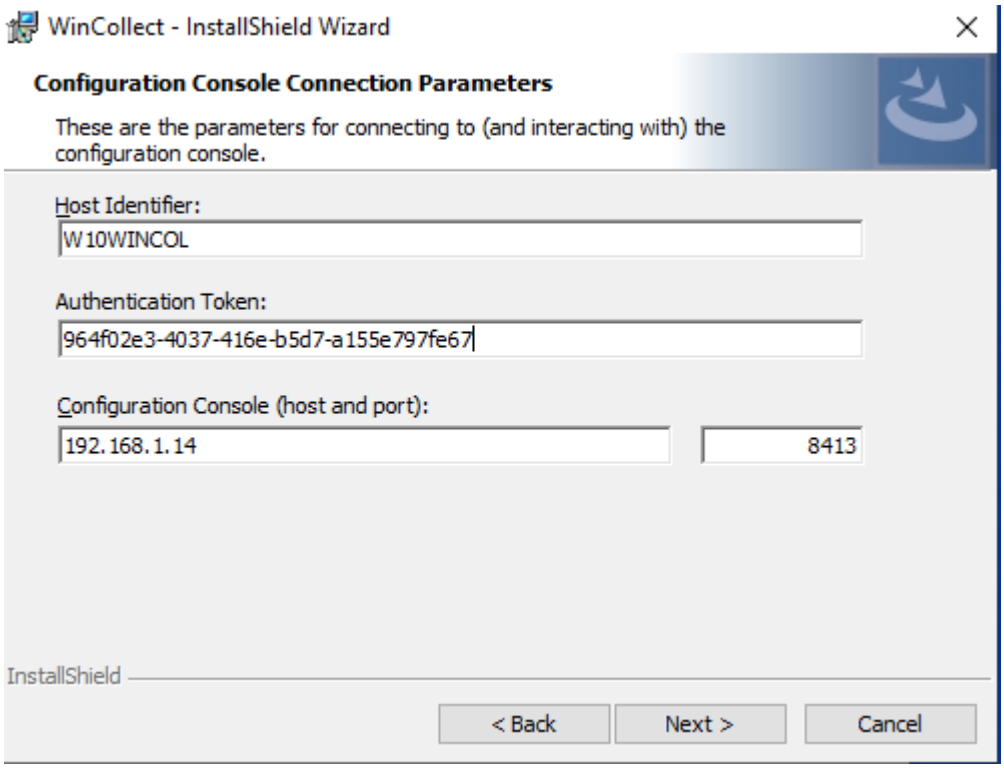
Εικόνα 3.4.11: Διαδικασία Deploy μετά τις αλλαγές

Μόλις ολοκληρωθεί το Deploy επιστρέφουμε στα Authorized Services και παίρνουμε το Token για να το χρησιμοποιήσουμε στη συνέχεια της εγκατάστασης.



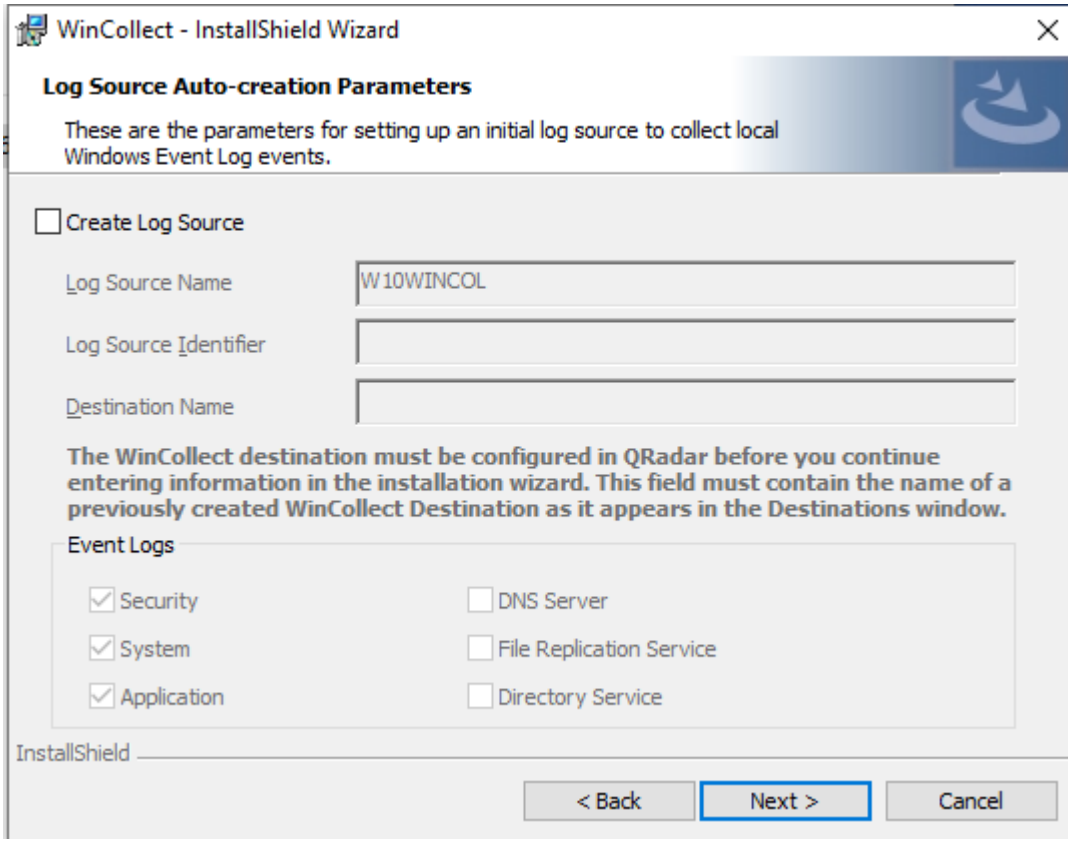
Εικόνα 3.4.12: Authentication Token

Συνεχίζουμε την εγκατάσταση χρησιμοποιώντας το Token που δημιουργήσαμε



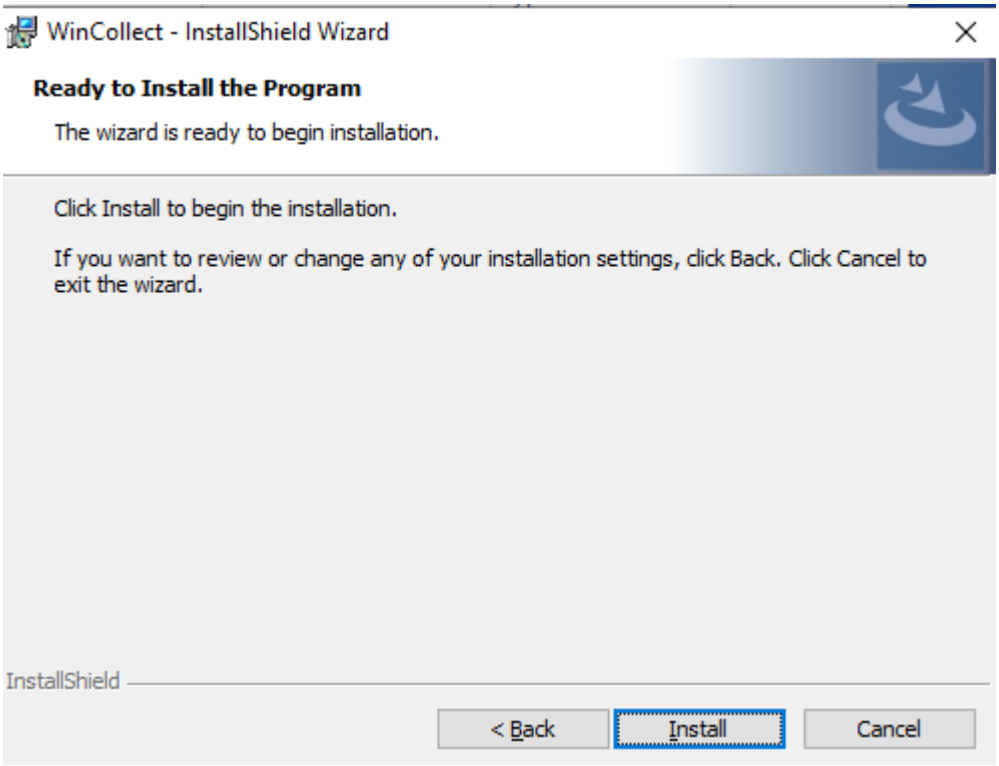
Εικόνα 3.4.13: Εγκατάσταση Wincollect Agent

Σιγουρευόμαστε πως στο επόμενο βήμα δε θα δημιουργήσουμε Log Source αυτόματα και συνεχίζουμε την εγκατάσταση.



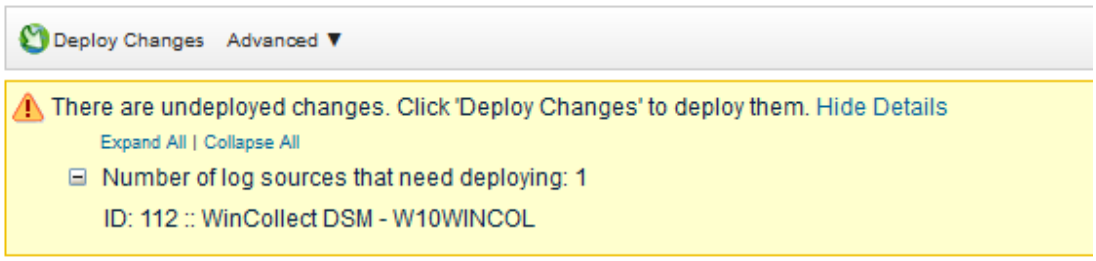
Εικόνα 3.4.14: Εγκατάσταση Wincollect Agent

Επιλέγουμε Install και περιμένουμε να ολοκληρωθεί.



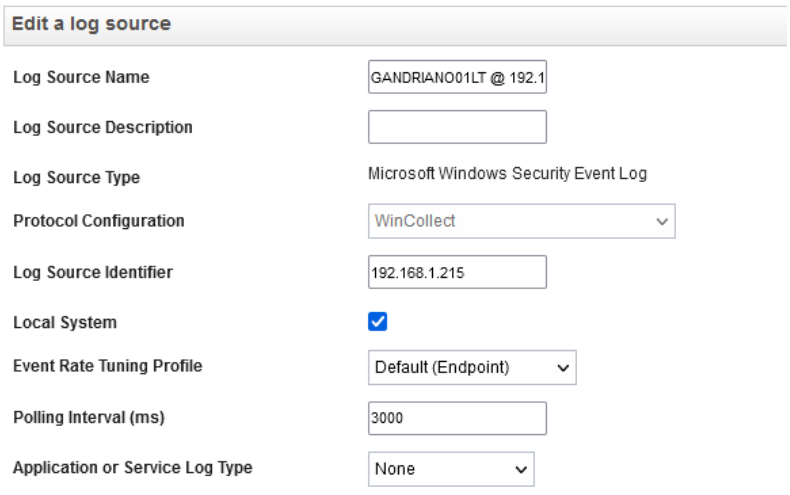
Εικόνα 3.4.15: Εγκατάσταση Wincollect Agent

Μόλις ολοκληρωθεί η εγκατάσταση επιστρέφουμε στο QRadar και βλέπουμε πως υπάρχουν νέες αλλαγές που περιέχουν το όνομα που δώσαμε κατά την εγκατάσταση. Πραγματοποιούμε το Deploy.

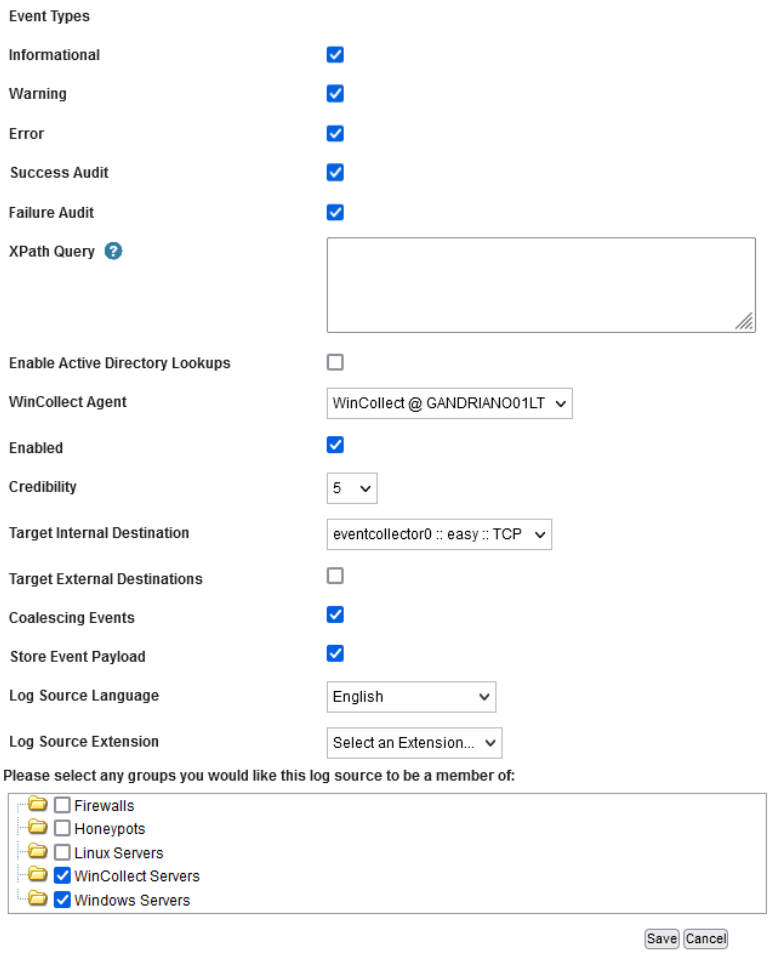


Εικόνα 3.4.16: Διαδικασία Deploy μετά τις αλλαγές

Στη διαχειριστική καρτέλα του QRadar έχουμε την επιλογή Log Sources. Την επιλέγουμε και δημιουργούμε ένα νέο όπως φαίνεται στις παρακάτω εικόνες. Με αυτό τον τρόπο θα πάρουμε τις καταγραφές από το Windows 10 host που έχει τοπικά εγκατεστημένο τον WInCollect Agent. Επιλέγουμε αποθήκευση και κάνουμε Deploy για άλλη μια φορά. Με αυτό τον τρόπο ολοκληρώσαμε την εγκατάσταση και την παραμετροποίηση του Agent αλλά και την αποστολή των καταγραφών του στο QRadar



Εικόνα 3.4.17: Δημιουργία Log Source



Εικόνα 3.4.18: Δημιουργία Log Source

3.5 Παραμετροποίηση των Windows Server 2016

Στο παρακάτω υποκεφάλαιο, θα παρουσιάσουμε τη διαδικασία παραμετροποίησης του Wincollect Agent σε Windows Server 2016 με σκοπό την αποστολή καταγραφών στο QRadar με τη μέθοδο remote polling. Ουσιαστικά οι καταγραφές θα αποστέλλονται στο QRadar μέσο του υπάρχοντος WinCollect που εγκαταστήσαμε στο Windows 10 μηχάνημα μας.

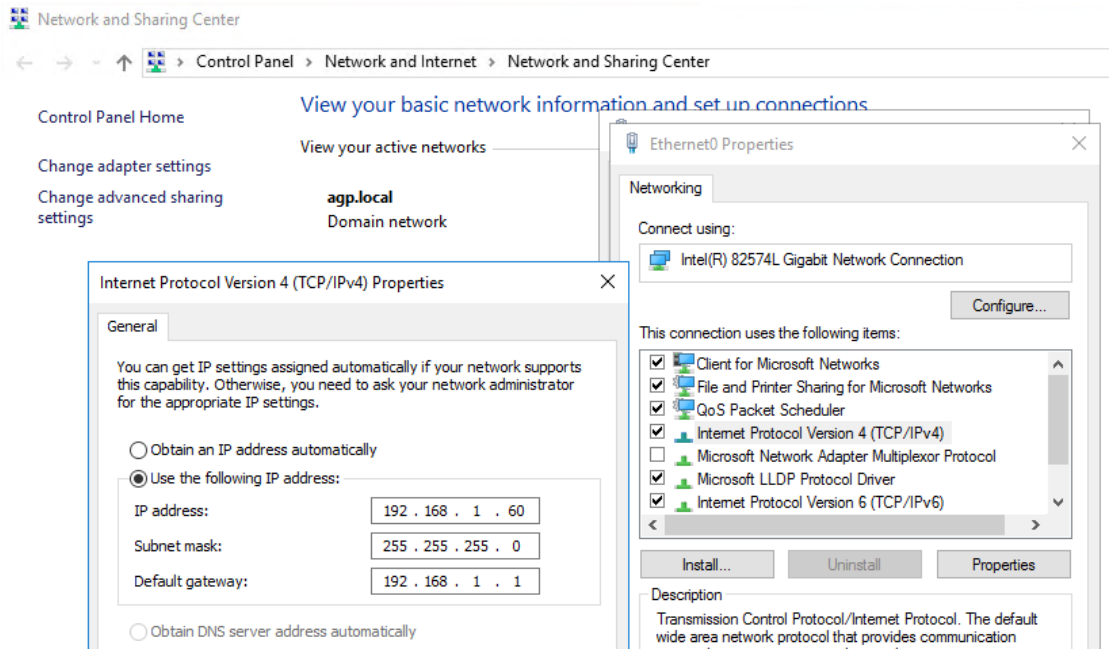
Μετά τη λήψη του αρχείου εγκατάστασης από την επίσημη ιστοσελίδα της Microsoft, ακολουθούμε τη διαδικασία εγκατάστασης του λειτουργικού συστήματος Windows, η οποία θεωρείτε γνωστή. Στη συγκεκριμένη περίπτωση, χρησιμοποιούμε την έκδοση Windows Server 2016.

Το αμέσως επόμενο βήμα μας είναι να προάγουμε το Server αυτό σε ελεγκτή τομέα (Domain Controller).

Μετά την απαραίτητη διαδικασία θα έχουμε δημιουργήσει τον τομέα agp.local

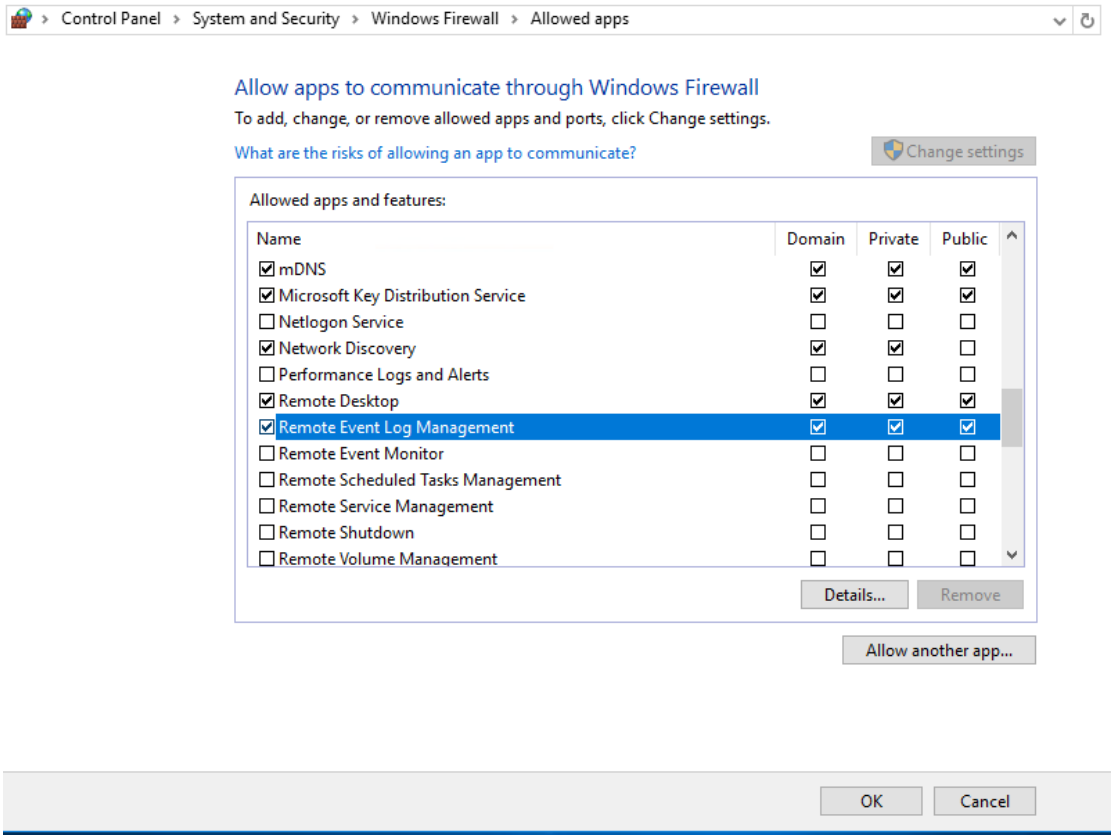
Θεωρούμε γνωστή την παραπάνω διαδικασία και προχωράμε στις ρυθμίσεις για την λήψη των καταγραφών στον WinCollect και από εκει στο QRadar.

Προχωράμε στην παραμετροποίηση των δικτυακών ρυθμίσεων με σκοπό να θέσουμε μια σταθερή IP.



Εικόνα 3.5.1: Παραμετροποίηση δικτύου

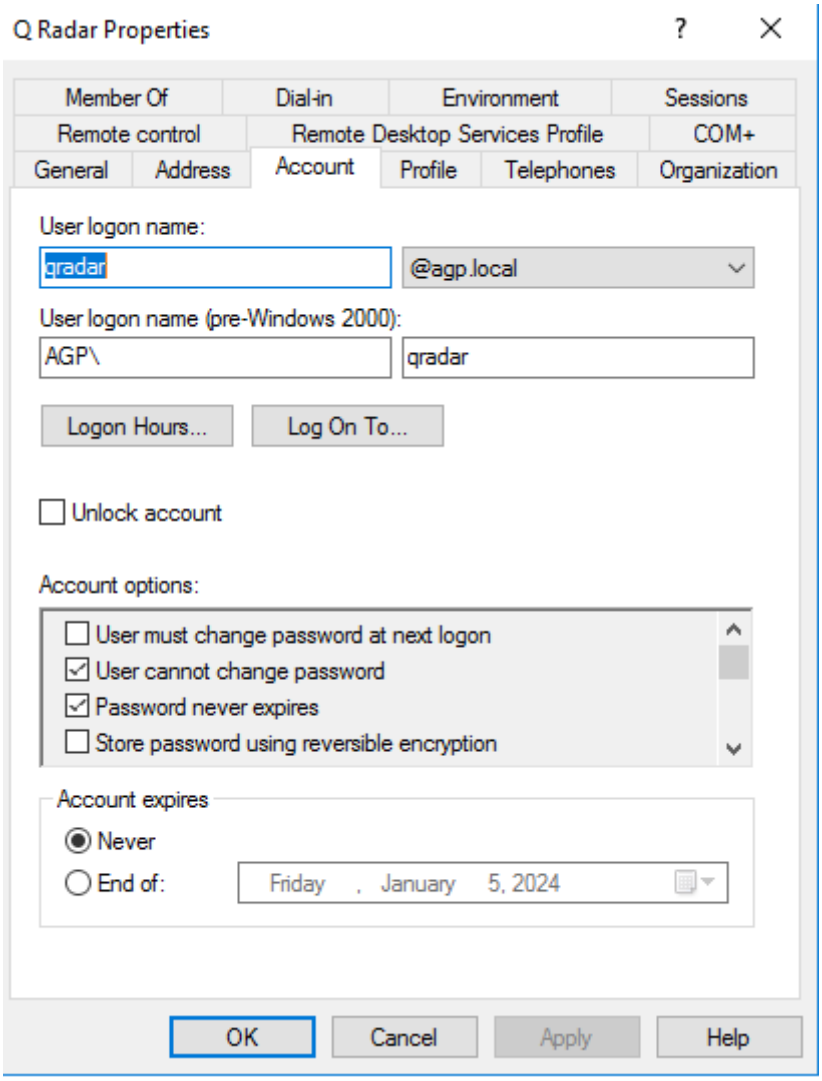
Στη συνέχεια θα πρέπει να παραμετροποιήσουμε το Firewall μας ώστε να επιτρέπεται το remote polling όπως περιγράφετε αναλυτικά στον οδηγό της IBM. Ουσιαστικά θα επιτρέψουμε την κίνηση στην εφαρμογή των Windows Remote Event Log Management.



Εικόνα 3.5.2: Παραμετροποίηση εσωτερικού firewall

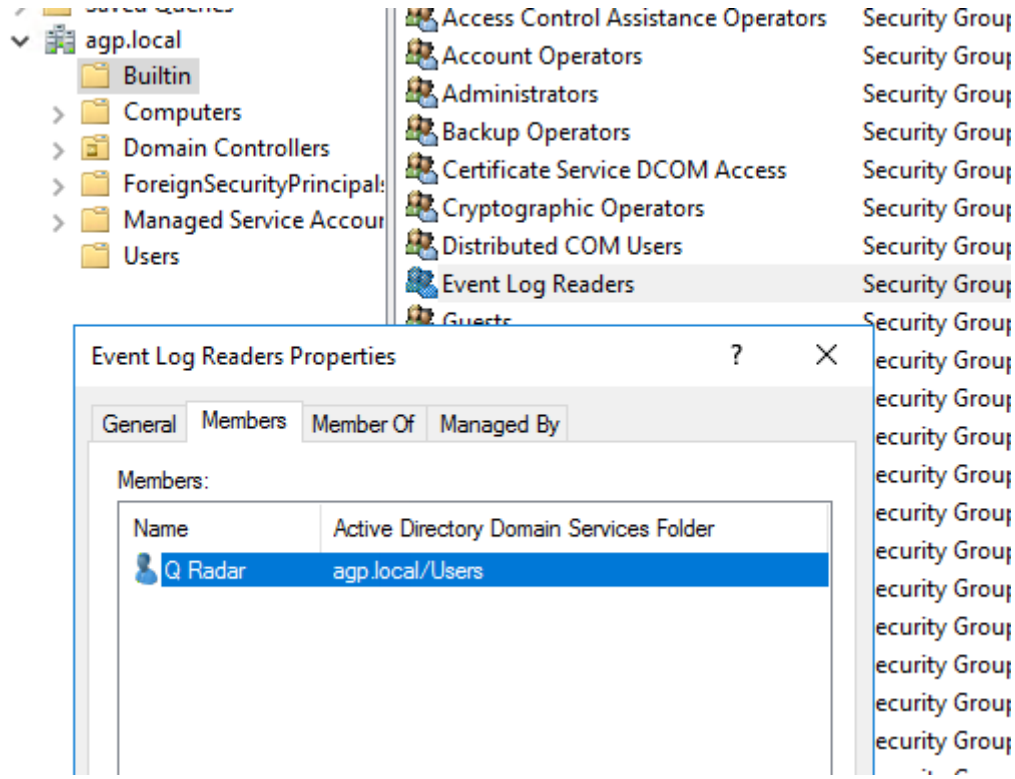
Στη συνέχεια θα δημιουργήσουμε ένα χρήστη στον τομέα μας ο οποίος θα είναι υπεύθυνος για την λήψη των καταγραφών και τα δικαιώματα που χρειάζεται είναι αυτά του τοπικού group Event Log Readers.

Δίνουμε μεγάλη σημασία στην παραμετροποίηση ώστε ο χρήστης να μην μπορεί να αλλάξει τον κωδικό του και ο κωδικός αυτός να μη λήγει γιατί διαφορετικά θα σταματήσουμε να λαμβάνουμε καταγραφές.



Εικόνα 3.5.3: Δημιουργία χρήστη

Το επόμενο βήμα μας είναι να τον προσθέσουμε στο τοπικό group Event Log Readers.

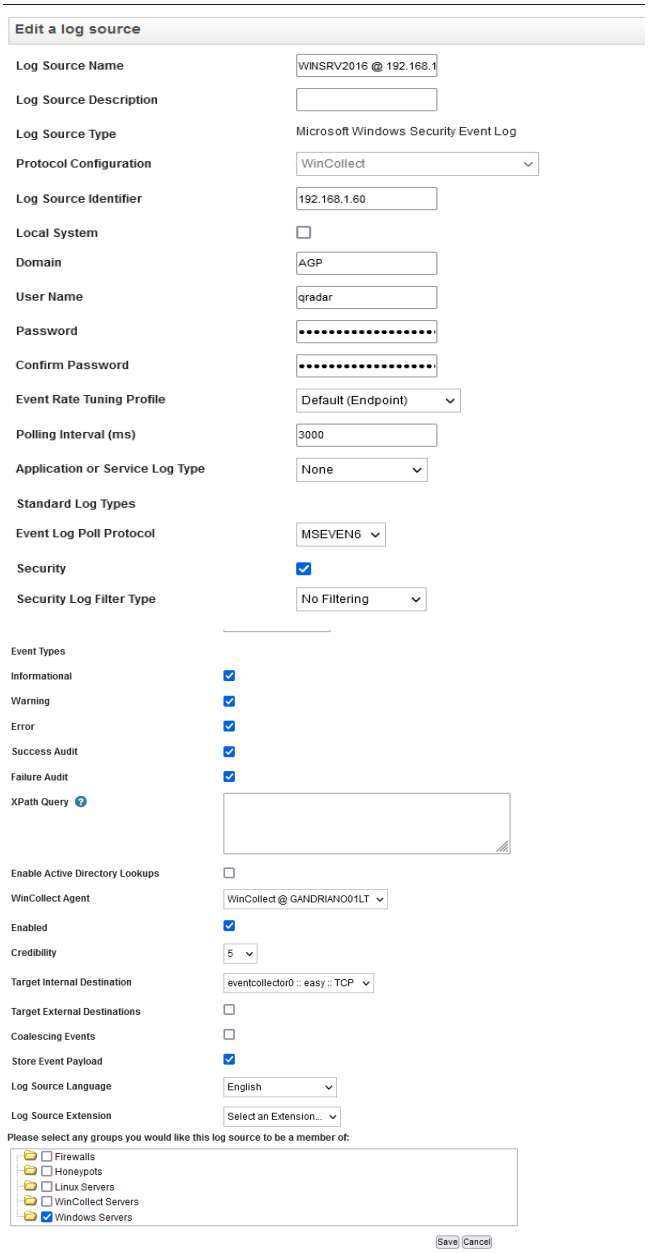


Εικόνα 3.5.4: Προσθήκη χρήστη στην τοπική ομάδα Event Log Readers

Στη διαχειριστική καρτέλα του QRadar έχουμε την επιλογή Log Sources. Την επιλέγουμε και δημιουργούμε ένα νέο όπως φαίνεται στις παρακάτω εικόνες. Με αυτό τον τρόπο θα πάρουμε τις καταγραφές απομακρυσμένα από το Windows Server 2016.

Επιλέγουμε αποθήκευση και κάνουμε Deploy. Με αυτό τον τρόπο ολοκληρώσαμε παραμετροποίηση του Windows Server αλλά και την λήψη των καταγραφών του στο QRadar.

Στο συγκεκριμένο Log Source έχουμε συμπεριλάβει τον τομέα του χρήστη, τον χρήστη και τον κωδικό του με σκοπό να λαμβάνει απομακρυσμένα τις καταγραφές.



Εικόνα 3.5.5: Δημιουργία Log Source

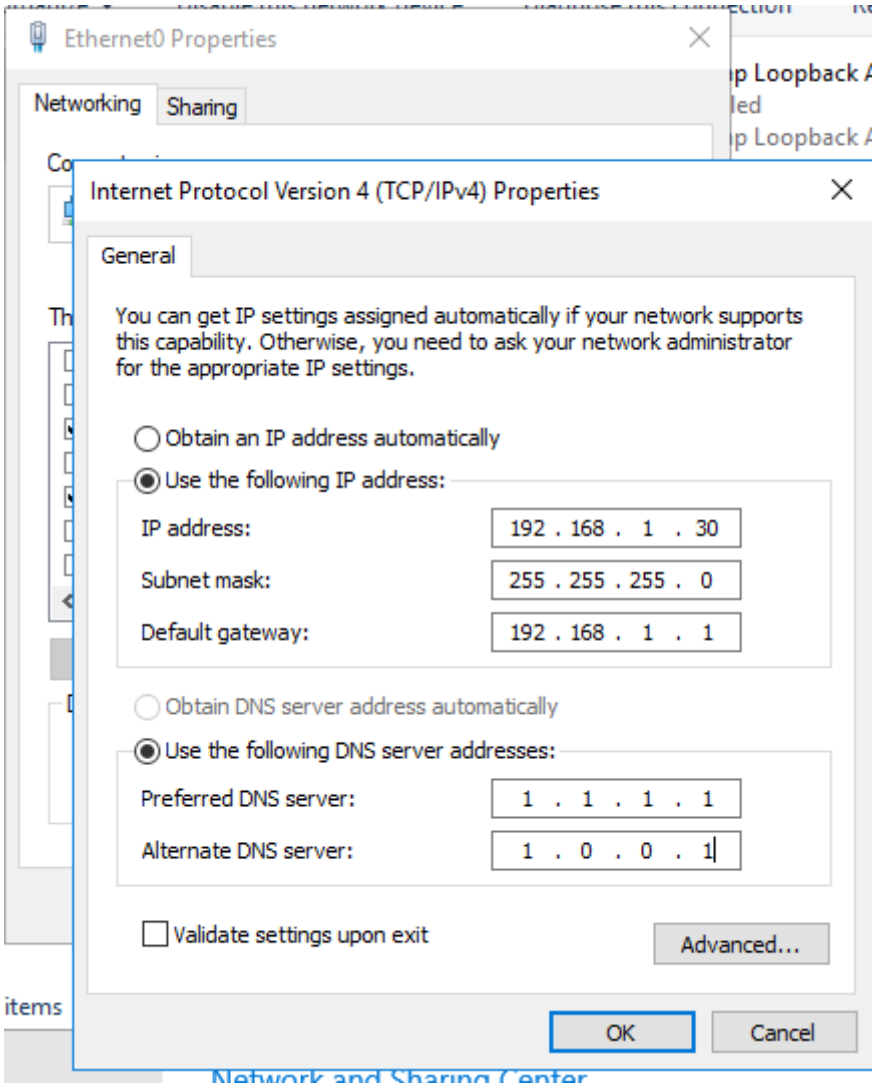
3.6 Παραμετροποίηση των Windows 10 Workstation (Vulnerable)

Στο παρακάτω υποκεφάλαιο, θα παρουσιάσουμε τη διαδικασία παραμετροποίησης του Wincollect Agent σε Windows 10 με σκοπό την αποστολή καταγραφών στο QRadar με τη μέθοδο remote polling και την εγκατάσταση ευάλωτων εφαρμογών που θα μας επιτρέψουν τη μη εξουσιοδοτημένη πρόσβαση. Οι καταγραφές θα αποστέλλονται στο QRadar μέσο του υπάρχοντος WinCollect που εγκαταστήσαμε στο Windows 10 μηχάνημα μας.

Μετά τη λήψη του αρχείου εγκατάστασης από την επίσημη ιστοσελίδα της Microsoft, ακολουθούμε τη διαδικασία εγκατάστασης του λειτουργικού συστήματος Windows, η οποία θεωρείτε γνωστή. Στη συγκεκριμένη περίπτωση, χρησιμοποιούμε την έκδοση Windows 10 Enterprise 1803 x64.

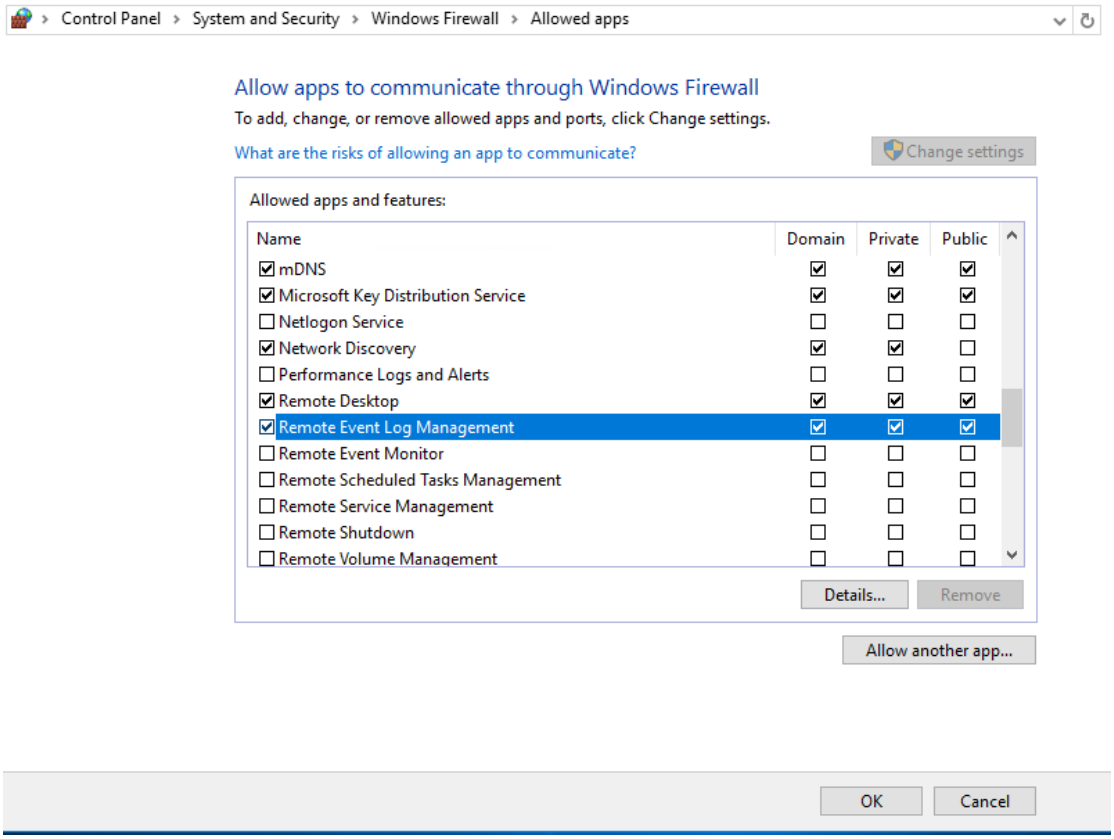
Θεωρούμε γνωστή την παραπάνω διαδικασία και προχωράμε στις ρυθμίσεις για την λήψη των καταγραφών στον WinCollect και από εκει στο QRadar.

Προχωράμε στην παραμετροποίηση των δικτυακών ρυθμίσεων με σκοπό να θέσουμε μια σταθερή IP.



Εικόνα 3.6.1: Παραμετροποίηση δικτύου

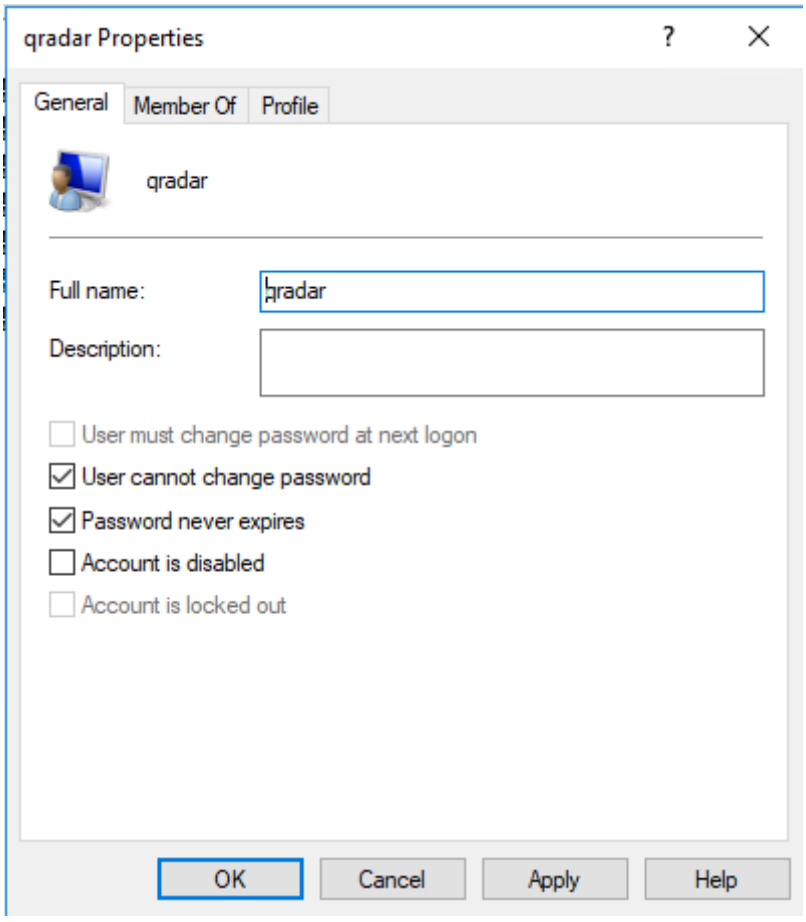
Στη συνέχεια θα πρέπει να παραμετροποιήσουμε το Firewall μας ώστε να επιτρέπεται το remote polling όπως περιγράφετε αναλυτικά στον οδηγό της IBM. Ουσιαστικά θα επιτρέψουμε την κίνηση στην εφαρμογή των Windows Remote Event Log Management.



Εικόνα 3.6.2: Παραμετροποίηση τοπικού firewall

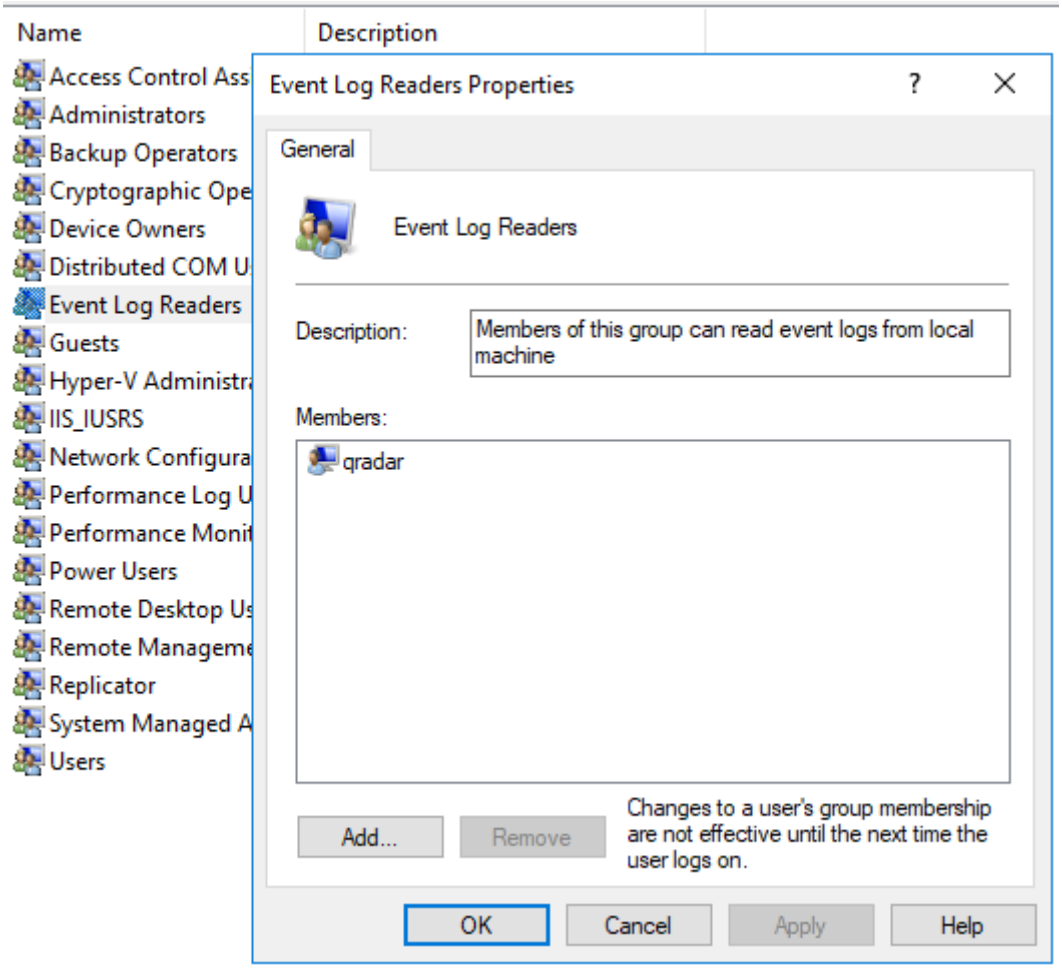
Στη συνέχεια θα δημιουργήσουμε ένα χρήστη στο workstation μας ο οποίος θα είναι υπεύθυνος για την λήψη των καταγραφών και τα δικαιώματα που χρειάζεται είναι αυτά του τοπικού group Event Log Readers.

Δίνουμε μεγάλη σημασία στην παραμετροποίηση ώστε ο χρήστης να μην μπορεί να αλλάξει τον κωδικό του και ο κωδικός αυτός να μη λήγει γιατί διαφορετικά θα σταματήσουμε να λαμβάνουμε καταγραφές.



Εικόνα 3.6.3: Δημιουργία χρήστη

Το επόμενο βήμα μας είναι να τον προσθέσουμε στο τοπικό group Event Log Readers.

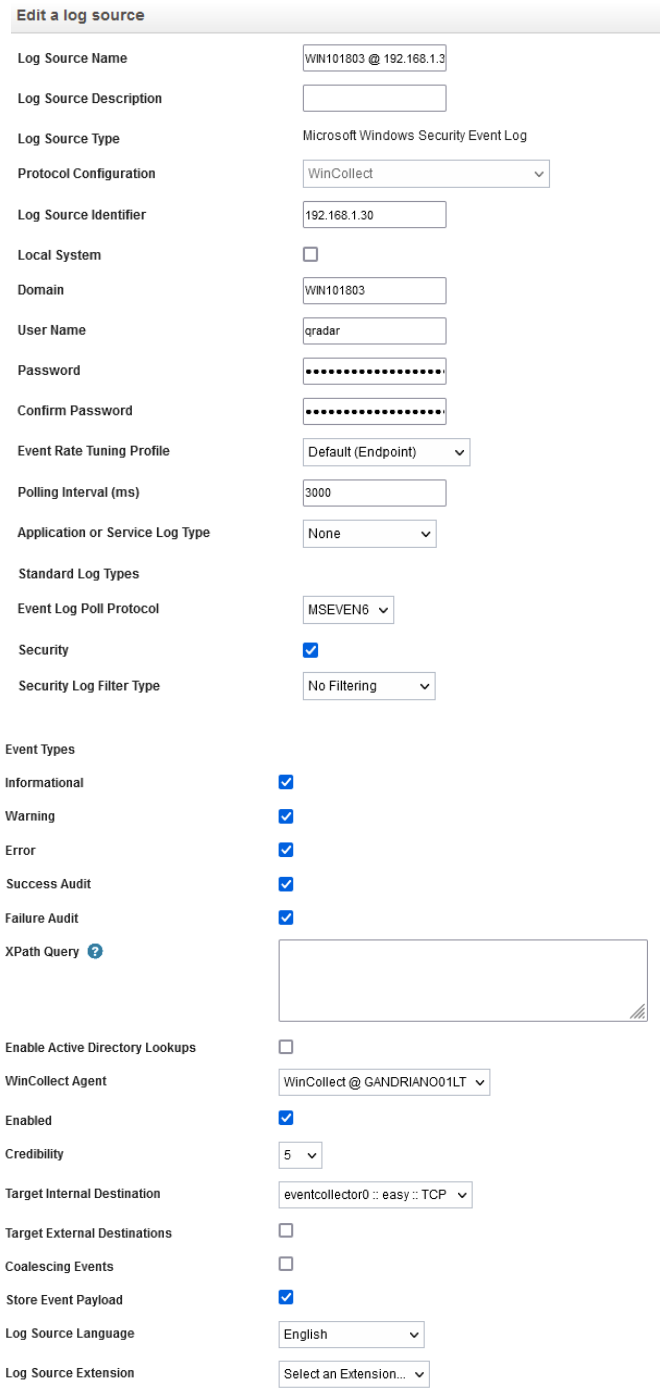


Εικόνα 3.6.4: Προσθήκη χρήστη στην τοπική ομάδα Event Log Readers

Στη διαχειριστική καρτέλα του QRadar έχουμε την επιλογή Log Sources. Την επιλέγουμε και δημιουργούμε ένα νέο όπως φαίνεται στις παρακάτω εικόνες. Με αυτό τον τρόπο θα πάρουμε τις καταγραφές απομακρυσμένα από το Windows Server 2016.

Επιλέγουμε αποθήκευση και κάνουμε Deploy. Με αυτό τον τρόπο ολοκληρώσαμε παραμετροποίηση του Windows Server αλλά και την λήψη των καταγραφών του στο QRadar.

Στο συγκεκριμένο Log Source έχουμε συμπεριλάβει τον τομέα του χρήστη, τον χρήστη και τον κωδικό του με σκοπό να λαμβάνει απομακρυσμένα τις καταγραφές.



Εικόνα 3.6.5: Δημιουργία Log Source

Τέλος για να κάνουμε αυτό το σταθμό εργασίας ακόμα πιο ευάλωτο σε επιθέσεις θα προχωρήσουμε στις παρακάτω ενέργειες:

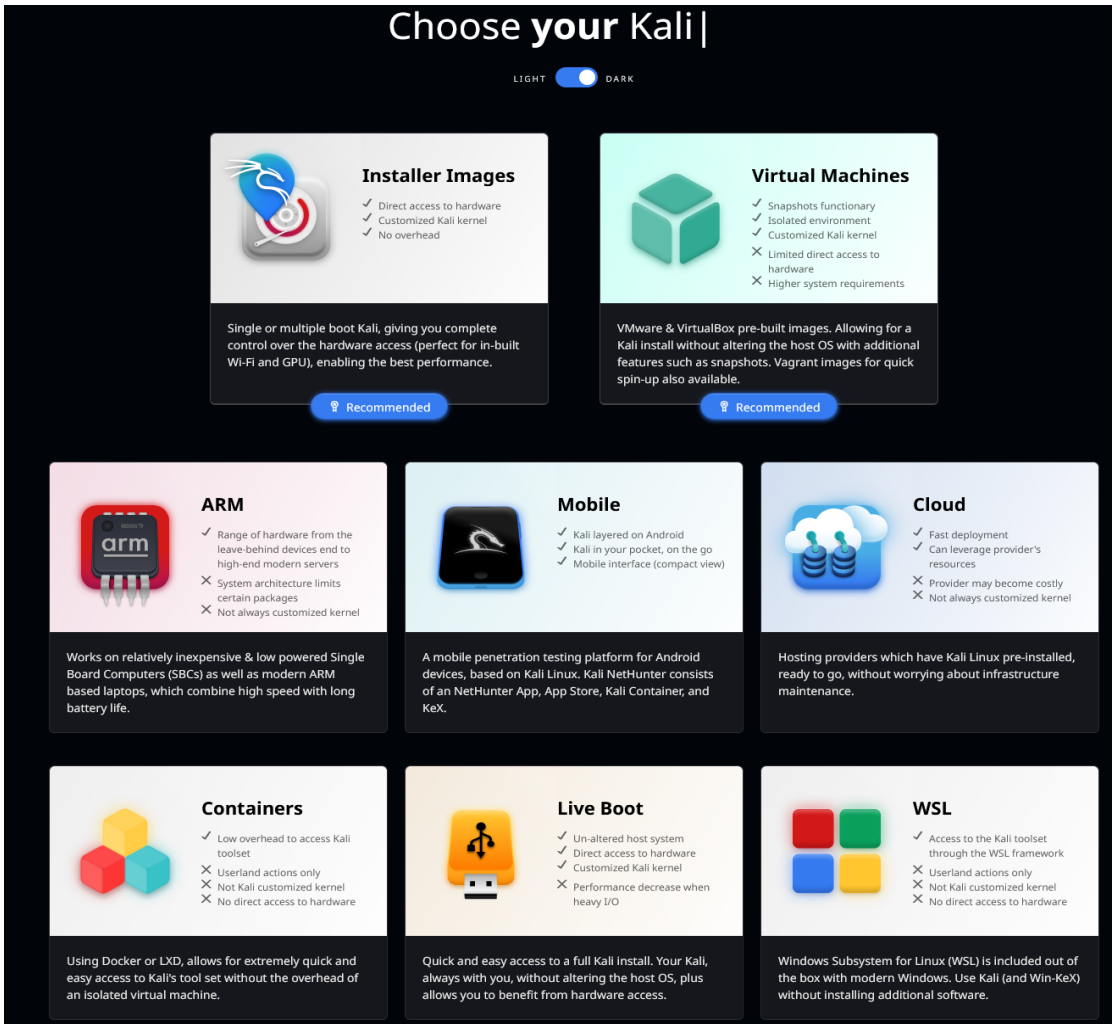
- Απενεργοποίηση του firewall
- Απενεργοποίηση του antivirus
- Αφαίρεση ενημερώσεων ασφαλείας
- Εγκατάσταση γνωστών ευάλωτων εφαρμογών

3.7 Παραμετροποίηση του συστήματος Kali Linux

Στο παρακάτω υποκεφάλαιο, θα παρουσιάσουμε τη διαδικασία εγκατάστασης και τη βασική παραμετροποίηση του Kali Linux.

Μετά τη λήψη του αρχείου εγκατάστασης από την επίσημη ιστοσελίδα της του Kali Linux, ακολουθούμε τη διαδικασία εισαγωγής του σε μια πλατφόρμα εικονικοποίησης. Στη συγκεκριμένη περίπτωση, χρησιμοποιούμε το VMware Workstation. Η έκδοση που κατεβάσαμε είναι έτοιμη εικόνα για την πλατφόρμα VMware.

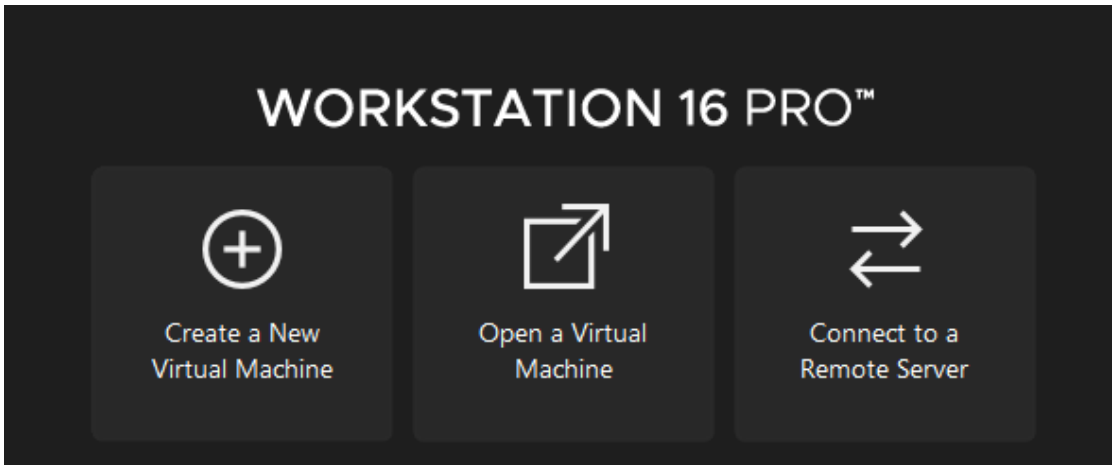
Όπως βλέπουμε παρακάτω μας δίνονται πολλές λύσεις εγκατάστασης ανάλογα με τις προδιάγραφες μας.



Εικόνα 3.7.1: Επιλογές λήψης του Kali Linux

Στην περίπτωση μας θα κατεβάσουμε και θα χρησιμοποιήσουμε ένα Virtual Machine για VMware.

Αφού το κατεβάσουμε και το αποσυμπιέσουμε παμε στην εφαρμογή VMWare και επιλέγουμε Open a Virtual Macine



Εικόνα 3.7.2: Άνοιγμα της εικονικής μηχανής

Στη συνέχεια επιλέγουμε το αρχείο που αντιστοιχεί στην εικονική μηχανή του kali linux και την ανοίγουμε.

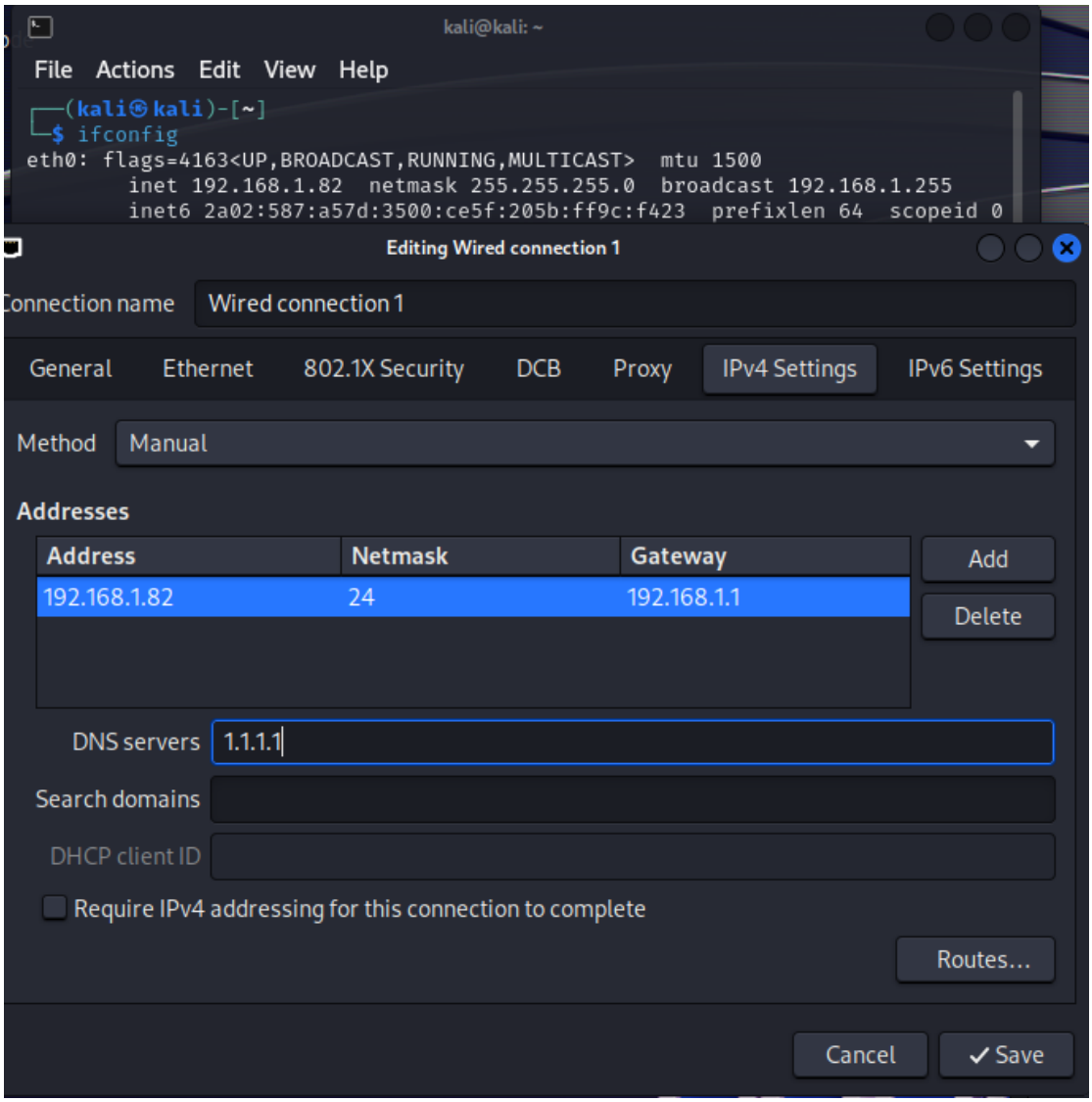
Το σύστημα μας είναι έτοιμο για χρήση

Εικόνα 3.7.3: Επιφάνεια εργασίας του Kali Linux

Το λειτουργικό σύστημα μας παρέχει πολλαπλές εφαρμογές ανίχνευσης ευπαθών προεγκατεστημένες και γι' αυτό το προτιμήσαμε.

Προσθέσαμε μόνο την εγκατάσταση του Nessus Essentials για να προσμοιάσουμε όσο το δυνατόν περισσότερο ένα εταιρικό περιβάλλον αλλά και γιατί μας παρέχει ιστορικό των σαρώσεων που έχουμε πραγματοποιήσει.

Τέλος θέσαμε στατική IP ώστε να γνωρίσουμε κατά τη διάρκεια των επιθέσεων ότι είναι το δικό μας μηχάνημα.



Εικόνα 3.7.4: Δικτυακή παραμετροποίηση του Kali Linux

Κεφάλαιο 4

4.1 Περιγραφή υλοποίησης

Στο παρακάτω κεφάλαιο θα περιγράψουμε 4 βασικές επιθέσεις που πραγματοποιεί κάποιος σε συστήματα Windows και δικτύων. Στα συστήματα δικτύων θα βασιστούμε στις καταγραφές που δημιουργούν τα τοπικά Windows Firewalls των συστημάτων.

Οι κανόνες που θα δημιουργήσουμε για την ανίχνευση των επιθέσεων αυτών είναι με βάση τη συμπεριφορά των καταγραφών όπως αυτές εντοπίζονται από το QRadar αλλά και με βάση των κωδικών καταγραφής.

Οι επιθέσεις που θα διεξάγουμε είναι οι παρακάτω:

- Internal Port Scanning - Εσωτερική σάρωση θυρών
- SMB Enumeration

- Audit Log Clear - Διαγραφή αρχείου καταγραφής ελέγχου

4.2 Ανάλυση επιθέσεων

Internal Port Scanning

Η εσωτερική σάρωση θυρών στον τομέα της κυβερνοεπίθεσης αναφέρεται στη διαδικασία εξαγωγής συστηματικής αξιολόγησης και εντοπισμού ανοικτών θυρών εντός του εσωτερικού δικτύου ενός οργανισμού. Αυτή η τεχνική αποτελεί επιθετικό μέτρο που σκοπεύει στην αποκάλυψη της υποδομής του δικτύου, παρέχοντας συγκεκριμένες πληροφορίες για πιθανές εισβολές.

Κατά τη διάρκεια της εσωτερικής σάρωσης θυρών, εκμεταλλεύονται εξειδικευμένα εργαλεία για την ανάλυση και τον έλεγχο της κατάστασης των θυρών σε συσκευές εντός του επιτιθέμενου δικτύου. Αυτά τα εργαλεία, με προηγμένη λειτουργικότητα, αλληλοεπιδρούν συστηματικά με κάθε θύρα για να καθορίσουν εάν είναι ανοικτή, κλειστή ή ανενεργή, προσφέροντας πληροφορίες που επιτρέπουν την ανακάλυψη της δομής του δικτύου και των πιθανών σημείων εισόδου.

Ο στόχος αυτής της κυβερνοεπίθεσης είναι η εντοπισμός ανεξουσιοδότητων ή περιττών ανοικτών θυρών που θα μπορούσαν να αξιοποιηθούν από επιθετικούς παράγοντες για εισβολές ή ανεξουσιοδότητες εντός του εσωτερικού δικτύου.

Τα ευρήματα αυτής της επίθεσης προσφέρουν σημαντική ενίσχυση στον ρόλο του επιτιθέμενου, δίνοντας του τη δυνατότητα:

Ανίχνευσης Ευπαθειών: Αναγνώρισης ανοικτών θυρών που μπορεί να αποκαλύψουν ευπάθειες εντός του εσωτερικού δικτύου, παρέχοντας ευκαιρίες για επιθετικές ενέργειες.

Κατανόησης του Δικτύου: Απόκτησης ενδιαφέρουσας εικόνας της δομής του εσωτερικού δικτύου για αποτελεσματικότερο σχεδιασμό και εκτέλεση επιθέσεων.

SMB Enumeration

Η εξερεύνηση του πρωτοκόλλου SMB στον χώρο της κυβερνοασφάλειας αντιπροσωπεύει ένα συστηματικό προσεγγιστικό που χρησιμοποιείται από κακόβουλους επιτιθέμενους για τη συγκέντρωση λεπτομερών πληροφοριών σχετικά με ένα δίκτυο-στόχο, εκμεταλλευόμενοι το πρωτόκολλο Server Message Block (SMB).

Αυτή η τεχνική, που χρησιμοποιείται από την πλευρά του επιτιθέμενου, περιλαμβάνει την εξαγωγή ουσιαστικών δεδομένων σχετικά με τους κοινόχρηστους πόρους του δικτύου, τους λογαριασμούς χρηστών και άλλες σχετικές πληροφορίες προσβάσιμες μέσω του πρωτοκόλλου SMB.

Το πρωτόκολλο Server Message Block, που χρησιμοποιείται ευρέως σε περιβάλλοντα Windows, διευκολύνει τον κοινόχρηστο χώρο αρχείων, εκτυπωτών και άλλων πόρων σε ένα δίκτυο. Στο πλαίσιο μιας επίθεσης εξερεύνησης, ο επιτιθέμενος εκμεταλλεύεται ευπάθειες ή λανθασμένες ρυθμίσεις εντός του πρωτοκόλλου SMB για την εξαγωγή σημαντικών πληροφοριών, με στόχο τον εντοπισμό πιθανών σημείων εισόδου και ευπαθειών εντός του στοχευμένου δικτύου.

Οι κύριοι στόχοι της εξερεύνησης του πρωτοκόλλου SMB από την πλευρά του επιτιθέμενου περιλαμβάνουν:

Αναγνώριση Κοινόχρηστων Πόρων: Ο επιτιθέμενος, εκμεταλλευόμενος την εξερεύνηση SMB, αναγνωρίζει τους κοινόχρηστους πόρους εντός του δικτύου, όπως συστήματα αρχείων και εκτυπωτές, κερδίζοντας έτσι κατανόηση της δομής των δεδομένων της οργάνωσης.

Εξαγωγή Πληροφοριών Λογαριασμών Χρηστών: Ο επιτιθέμενος στοχεύει στην εξαγωγή πληροφοριών σχετικά με τους λογαριασμούς χρηστών που υπάρχουν στο δίκτυο, συμπεριλαμβανομένων ονομάτων χρηστών και πιθανώς κρυπτογραφημένων κωδικών πρόσβασης. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για μη εξουσιοδοτημένες προσπάθειες πρόσβασης.

Χαρτογράφησης Τοπολογίας Δικτύου: Η εξερεύνηση SMB συμβάλλει στη χαρτογράφηση της τοπολογίας του δικτύου, αποκαλύπτοντας τις σχέσεις μεταξύ διάφορων συσκευών και συστημάτων εντός του στοχευμένου περιβάλλοντος. Αυτές οι πληροφορίες είναι κρίσιμες για τον σχεδιασμό επόμενων σταδίων μιας επίθεσης.

Εντοπισμού Ευπαθειών: Με τη χρήση του πρωτοκόλλου SMB, οι επιτιθέμενοι επιδιώκουν τον εντοπισμό πιθανών ευπαθειών ή λανθασμένων ρυθμίσεων εντός του δικτύου, παρέχοντας ευκαιρίες για εκμετάλλευση και μη εξουσιοδοτημένη πρόσβαση.

Audit Log Clear

Η διαγραφή των αρχείων καταγραφής ελέγχου (audit logs) στον χώρο της κυβερνοασφάλειας αντιπροσωπεύει μια σκόπιμη και κακόβουλη προσπάθεια από έναν επιτιθέμενο να εξαφανίσει ίχνη των δραστηριοτήτων του εντός ενός παραβιασμένου συστήματος ή δικτύου. Τα αρχεία καταγραφής ελέγχου αποτελούν κρίσιμο στοιχείο των μέτρων ασφαλείας, καταγράφοντας διάφορα συμβάντα και ενέργειες που λαμβάνουν χώρα εντός ενός πληροφοριακού συστήματος. Αυτά τα αρχεία είναι αναντικατάστατα για τη δικαστική ανάλυση, την αντιμετώπιση περιστατικών και τον εντοπισμό περιστατικών ασφαλείας.

Από την πλευρά του επιτιθέμενου, η διαγραφή των αρχείων καταγραφής ελέγχου αποτελεί μια στρατηγική κίνηση με σκοπό να κρύψει τη μη εξουσιοδοτημένη πρόσβαση του, των κακόβουλων δραστηριοτήτων ή οποιωνδήποτε ενδείξεων που θα μπορούσαν να οδηγήσουν στον εντοπισμό της παρουσίας του στο παραβιασμένο περιβάλλον. Αυτή η διαδικασία περιλαμβάνει συνήθως την εσκεμμένη διαγραφή ή παραποίηση καταχωρήσεων καταγραφής που σχετίζονται με τις ενέργειες του επιτιθέμενου, καθιστώντας το αποτέλεσμα του διακριτικού ίχνους ελλιπές ή ασαφές.

Οι κύριοι στόχοι της διαγραφής των αρχείων καταγραφής ελέγχου από την πλευρά του επιτιθέμενου περιλαμβάνουν:

Εξάλειψης των Στοιχείων: Οι επιτιθέμενοι επιδιώκουν να εξαλείψουν οποιαδήποτε ψηφιακά ίχνη ή στοιχεία που θα μπορούσαν να συνδέσουν τις δραστηριότητές τους με το παραβιασμένο σύστημα. Αυτό περιλαμβάνει τη σκόπιμη διαγραφή καταχωρήσεων στα αρχεία καταγραφής που θα μπορούσαν να αποκαλύψουν τη σειρά των ενεργειών που πραγματοποιήθηκαν κατά τη μη εξουσιοδοτημένη πρόσβαση.

Αποφυγής της Ανίχνευσης: Με τη διαγραφή των αρχείων καταγραφής ελέγχου, οι επιτιθέμενοι στοχεύουν στην αποφυγή της ανίχνευσης από εργαλεία παρακολούθησης ασφαλείας και δικαστική ανάλυση. Η απουσία σχετικών καταχωρήσεων καθιστά πιο προβληματικό τον εντοπισμό από τους επαγγελματίες κυβερνοασφάλειας και επιβραδύνει την αντίδραση στην παραβίαση ασφαλείας.

Επιμήκυνση της Μη Εξουσιοδοτημένης Πρόσβασης: Η διαγραφή των αρχείων καταγραφής εντάσσεται σε μια ευρύτερη στρατηγική για την επιμήκυνση της μη εξουσιοδοτημένης πρόσβασης. Με το να εξαφανίζουν τα ίχνη της παρουσίας τους, οι επιτιθέμενοι αυξάνουν την πιθανότητα παραμονής τους ανακαλυπτόμενους για μεγαλύτερο χρονικό διάστημα, επιτρέποντας τη συνέχιση της εκμετάλλευσης του παραβιασμένου συστήματος.

Ασάφεια Τεχνικών Επιθέσεων: Οι επιτιθέμενοι μπορεί να διαγράφουν τα αρχεία καταγραφής ελέγχου για να αποσαφηνίσουν τις συγκεκριμένες τεχνικές και μεθόδους που χρησιμοποίησαν κατά τη διάρκεια της παραβίασης. Αυτή η εσκεμμένη ασάφεια δυσκολεύει την εργασία των ειδικών κυβερνοασφάλειας στην ανακατασκευή του χρονολογίου της επίθεσης και στον πλήρη κατανοητό της εύρος του περιστατικού.

Η πράξη της διαγραφής των αρχείων καταγραφής ελέγχου υπογραμμίζει τη σημασία της υιοθέτησης αποτελεσματικών μέτρων κυβερνοασφάλειας για τη διαφύλαξη της ακεραιότητας και διαθεσιμότητας των αρχείων καταγραφής. Προληπτικά μέτρα ασφαλείας, όπως η παρακολούθηση σε πραγματικό χρόνο, η ασφαλής αποθήκευση των αρχείων καταγραφής και η εφαρμογή μηχανισμών ανίχνευσης παραποίησης αποτελούν ουσιώδεις παράγοντες για την μείωση του κινδύνου παραποίησης των αρχείων καταγραφής από κακόβουλους επιτιθέμενους. Η κατανόηση της προοπτικής του επιτιθέμενου σχετικά με τη διαγραφή των αρχείων καταγραφής ελέγχου είναι ουσιώδης για την ανάπτυξη αποτελεσματικών μέτρων αντιμετώπισης και για την ενίσχυση της συνολικής ανθεκτικότητας της κυβερνοασφάλειας.

4.3 Παραδείγματα δοκιμών της κάθε επίθεσης

Internal Port Scanning

Πραγματοποιώντας μια εσωτερική σάρωση σε μια διεύθυνση IP του δικτυού μας παρατηρούμε τη συμπεριφορά της επίθεσης με την μορφή καταγραφών. Επειδή το σύστημα μας είναι windows σύστημα τις λαμβάνουμε από το τοπικό του firewall.

Βάση των καταγράφων που έχουμε λάβει παρατηρούμε πως έχουμε πολλαπλά στοιχεία ώστε να αξιοποιήσουμε για τη δημιουργία του κανόνα μας

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	37711	192.168.1.215	7946
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	44155	192.168.1.215	7952
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	43645	192.168.1.215	7955
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	40225	192.168.1.215	7951
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	34189	192.168.1.215	7945
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	35877	192.168.1.215	7948
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	35903	192.168.1.215	7941
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	33075	192.168.1.215	7949
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	38493	192.168.1.215	7944
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	35125	192.168.1.215	7950
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	45899	192.168.1.215	7943
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	33973	192.168.1.215	7947
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	37929	192.168.1.215	7956
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	34655	192.168.1.215	7959
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	39283	192.168.1.215	7958
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	44867	192.168.1.215	7960
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	40381	192.168.1.215	7953
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	41395	192.168.1.215	7957
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	38851	192.168.1.215	7954
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	42831	192.168.1.215	7961
Failure Audit: The Windows Filtering Platform blocked a packet	GANDRIANO01LT @ 192.168.1.215	1	Jan 27, 2024, 6:41:09 PM	Access Denied	192.168.1.82	38701	192.168.1.215	7973

Εικόνα 4.3.1: Παρουσίαση καταγραφών στο QRadar

Παραθέτουμε ενδεικτικά 2 καταγραφές στην ανεπεξέργαστη μορφή τους με την πλήρη πληροφορία που λαμβάνουμε. Η μια καταγραφή αφορά την άρνηση κίνησης και η δεύτερη την επιτρεπόμενη κίνηση.

<13>Jan 27 18:27:45 192.168.1.215 AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.5.1.22 Source=Microsoft-Windows-Security-Auditing Computer=GANDRIANO01LT OriginatingComputer=GANDRIANO01LT User= Domain= EventID=5152 EventIDCode=5152 EventType=16 EventCategory=12809 RecordNumber=76307155 TimeGenerated=1706372864 TimeWritten=1706372864 Level=Log Always Keywords=Audit Failure Task=SE_ADT_OBJECTACCESS_FIREWALLPACKETDROPS Opcode=Info Message=The Windows Filtering Platform has blocked a packet. Application Information: Process ID: 0 Application Name: - Network Information: Direction: Inbound Source Address: 192.168.1.82 Source Port: 48169 Destination Address: 192.168.1.215 Destination Port: 22 Protocol: 6 Filter Information: Filter Run-Time ID: 327481 Layer Name: Transport Layer Run-Time ID: 13

Εικόνα 4.3.2: Μεμονωμένη καταγραφή σε ανεπεξέργαστη μορφή

```
<13>Jan 27 18:27:45 192.168.1.215 AgentDevice=WindowsLog
        AgentLogFile=Security PluginVersion=7.3.1.22
        Source=Microsoft-Windows-Security-Auditing
        Computer=GANDRIANO01LT OriginatingComputer=GANDRIANO01LT
        User= Domain= EventID=5152 EventIDCode=5152
        EventType=16 EventCategory=12809 RecordNumber=76307135
        TimeGenerated=1706372864 TimeWritten=1706372864
        Level=Log Always Keywords=Audit Failure
        Task=SE_ADT_OBJECTACCESS_FIREWALLPACKETDROPS Opcode=Info
        Message=The Windows Filtering Platform has blocked a packet.
Application Information: Process ID: 0 Application Name: - Network
Information: Direction: Inbound Source Address: 192.168.1.82
Source Port: 40169 Destination Address: 192.168.1.215 Destination
Port: 22 Protocol: 6 Filter Information: Filter Run-Time ID:
227401 Layer Name: Transport Layer Run-Time ID: 13
```

Εικόνα 4.3.3: Μεμονωμένη καταγραφή σε ανεπεξέργαστη μορφή

```
<13>Jan 27 18:33:24 192.168.1.215 AgentDevice=WindowsLog
        AgentLogFile=Security PluginVersion=7.3.1.22
        Source=Microsoft-Windows-Security-Auditing
        Computer=GANDRIANO01LT OriginatingComputer=GANDRIANO01LT
        User= Domain= EventID=5156 EventIDCode=5156
        EventType=8 EventCategory=12810 RecordNumber=76315477
        TimeGenerated=1706373202 TimeWritten=1706373202
        Level=Log Always Keywords=Audit Success
        Task=SE_ADT_OBJECTACCESS_FIREWALLCONNECTION Opcode=Info
        Message=The Windows Filtering Platform has permitted a
connection. Application Information: Process ID: 1432 Application
Name: \device\harddiskvolume2\windows\system32\svchost.exe Network
Information: Direction: Inbound Source Address: 192.168.1.82
Source Port: 41515 Destination Address: 192.168.1.215 Destination
Port: 3389 Protocol: 6 Filter Information: Filter Run-Time ID:
228886 Layer Name: Receive/Accept Layer Run-Time ID: 44
```

Αυτά που πραγματικά χρειαζόμαστε και μπορούμε να αξιοποιήσουμε είναι τα παρακάτω δεδομένα:

- Source IP
- Destination IP
- Destination Port
- Event Count
- Time

Βάση των καταγραφών παρατηρούμε το πως δουλεύει η επίθεση και περιγράφοντας την παρατηρούμε και βγάζουμε το παρακάτω συμπέρασμα.

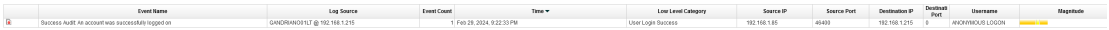
Μια Source IP δημιουργεί πολλαπλά Events προς μια Destination IP σε πολλαπλές Destination Ports σε σύντομο χρονικό διάστημα.

Σε περίπτωση που γίνεται scan ενός ολόκληρου υποδικτύου κάθε σύστημα θα αναφέρετε ξεχωριστά και θα δημιουργεί τις δικές του καταγραφές.

SMB Enumeration

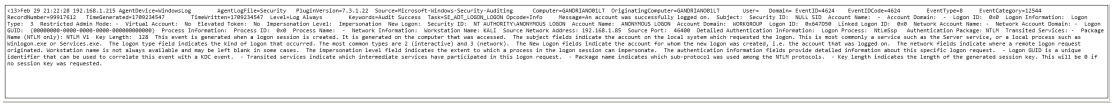
Πραγματοποιώντας ένα Enumeration σε μια διεύθυνση IP του δικτιού μας παρατηρούμε τη συμπεριφορά της επίθεσης με την μορφή καταγραφών.

Βάση των καταγράφων που έχουμε λάβει παρατηρούμε πως έχουμε πολλαπλά στοιχεία ώστε να αξιοποιήσουμε για τη δημιουργία του κανόνα μας



Εικόνα 4.3.4: Παρουσίαση καταγραφών στο QRadar

```
<13>Feb 29 21:22:28 192.168.1.215 AgentDevice=WindowsLog
        AgentLogFile=Security PluginVersion=7.3.1.22
        Source=Microsoft-Windows-Security-Auditing
        Computer=GANDRIANO01LT OriginatingComputer=GANDRIANO01LT
        User= Domain= EventID=4624 EventIDCode=4624
        EventType=8 EventCategory=12544 RecordNumber=99917612
        TimeGenerated=1709234547 TimeWritten=1709234547
        Level=Log Always Keywords=Audit Success
        Task=SE_ADT_LOGON_LOGON Opcode=Info Message=An
account was successfully logged on. Subject: Security ID: NULL
SID Account Name: - Account Domain: - Logon ID: 0x0 Logon
Information: Logon Type: 3 Restricted Admin Mode: - Virtual
Account: No Elevated Token: No Impersonation Level: Impersonation
New Logon: Security ID: NT AUTHORITY\ANONYMOUS LOGON Account Name:
ANONYMOUS LOGON Account Domain: WORKGROUP Logon ID: 0x647D50
Linked Logon ID: 0x0 Network Account Name: - Network Account
Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information: Process ID: 0x0 Process Name: - Network
Information: Workstation Name: KALI Source Network Address:
192.168.1.85 Source Port: 46400 Detailed Authentication
Information: Logon Process: NtLmSsp Authentication Package: NTLM
Transited Services: - Package Name (NTLM only): NTLM V1 Key Length:
128 This event is generated when a logon session is created. It is
generated on the computer that was accessed. The subject fields
indicate the account on the local system which requested the logon.
This is most commonly a service such as the Server service, or a
local process such as Winlogon.exe or Services.exe. The logon type
field indicates the kind of logon that occurred. The most common
types are 2 (interactive) and 3 (network). The New Logon fields
indicate the account for whom the new logon was created, i.e. the
account that was logged on. The network fields indicate where a
remote logon request originated. Workstation name is not always
available and may be left blank in some cases. The impersonation
level field indicates the extent to which a process in the logon
session can impersonate. The authentication information fields
provide detailed information about this specific logon request. -
Logon GUID is a unique identifier that can be used to correlate this
event with a KDC event. - Transited services indicate which
intermediate services have participated in this logon request. -
Package name indicates which sub-protocol was used among the NTLM
protocols. - Key length indicates the length of the generated session
key. This will be 0 if no session key was requested.
```



Εικόνα 4.3.5: Μεμονωμένη καταγραφή σε ανεπεξέργαστη μορφή

Αυτά που πραγματικά χρειαζόμαστε και μπορούμε να αξιοποιήσουμε είναι τα παρακάτω δεδομένα:

- Source IP
- Destination IP
- Time
- Username
- EventID

Βάση των καταγραφών παρατηρούμε το πως συμπεριφέρεται η παραπάνω ενέργεια και περιγράφοντας την παρατηρούμε και βγάζουμε το παρακάτω συμπέρασμα.

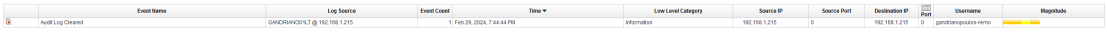
Μια Source IP επικοινωνεί με μια Destination IP χρησιμοποιώντας ένα συγκεκριμένο username για να αυθεντικοποιηθεί επιτυχώς .

Το παραπάνω event σαν μοναδικό αριθμό τύπου καταγραφής έχει το 4624

Audit Log Clear

Πραγματοποιώντας ένα καθαρισμό των καταγραφών τοπικά σε ένα από τα τερματικά του δικτύου μας μας παρατηρούμε παρατηρούμε ότι έχουμε λάβει μια καταγραφή για το συγκεκριμένο περιστατικό.

Βάση της καταγραφής που έχουμε λάβει παρατηρούμε πως έχουμε πολλαπλά στοιχεία ώστε να αξιοποιήσουμε για τη δημιουργία του κανόνα μας



Εικόνα 4.3.6: Παρουσίαση καταγραφών στο QRadar

```
<13>Feb 29 19:42:28 192.168.1.215 AgentDevice=WindowsLog
        AgentLogFile=Security PluginVersion=7.3.1.22
        Source=Microsoft-Windows-Eventlog
        Computer=GANDRIANO01LT OriginatingComputer=GANDRIANO01LT
        User= Domain= EventID=1102 EventIDCode=1102
        EventType=4 EventCategory=104 RecordNumber=99890359
        TimeGenerated=1709228546 TimeWritten=1709228546
        Level=Informational Keywords=AuditSuccess
        Task=el:LogClear Opcode=Info Message=The audit log
was cleared. Subject: Security ID: GANDRIANO01LT\gandrianopoulos-
remo Account Name: gandrianopoulos-remo Domain Name: GANDRIANO01LT
Logon ID: 0x12A0F8
```

Εικόνα 4.3.5: Μεμονωμένη καταγραφή σε ανεπεξέργαστη μορφή

Αυτά που πραγματικά χρειαζόμαστε και μπορούμε να αξιοποιήσουμε είναι τα παρακάτω δεδομένα:

- Source IP
- Destination IP
- Time
- Username
- EventID

Βάση των καταγραφών παρατηρούμε το πως συμπεριφέρεται η παραπάνω ενέργεια και περιγράφοντας την παρατηρούμε και βγάζουμε το παρακάτω συμπέρασμα.

Μια Source IP διαγράφει το αρχείο καταγραφών στην Destination IP χρησιμοποιώντας το αντίστοιχο Username.

Το παραπάνω event σαν μοναδικό αριθμό τύπου καταγραφής έχει το 1102

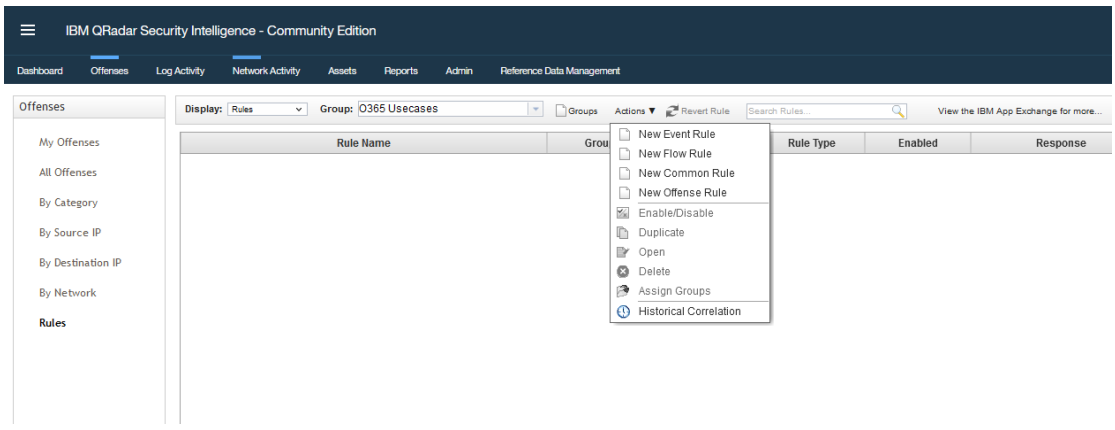
4.4 Δημιουργία κανόνων λογικής της κάθε επίθεσης

Βασική δημιουργία κανόνων

Για να μπορέσουμε να λάβουμε μια ειδοποίηση για αυτό το περιστατικό ασφαλείας θα πρέπει να δημιουργήσουμε έναν κανόνα συσχέτισης των καταγραφών. Το QRadar μας δίνει τη δυνατότητα να δημιουργήσουμε τέτοιου είδους κανόνες με τη χρήση λογικής.

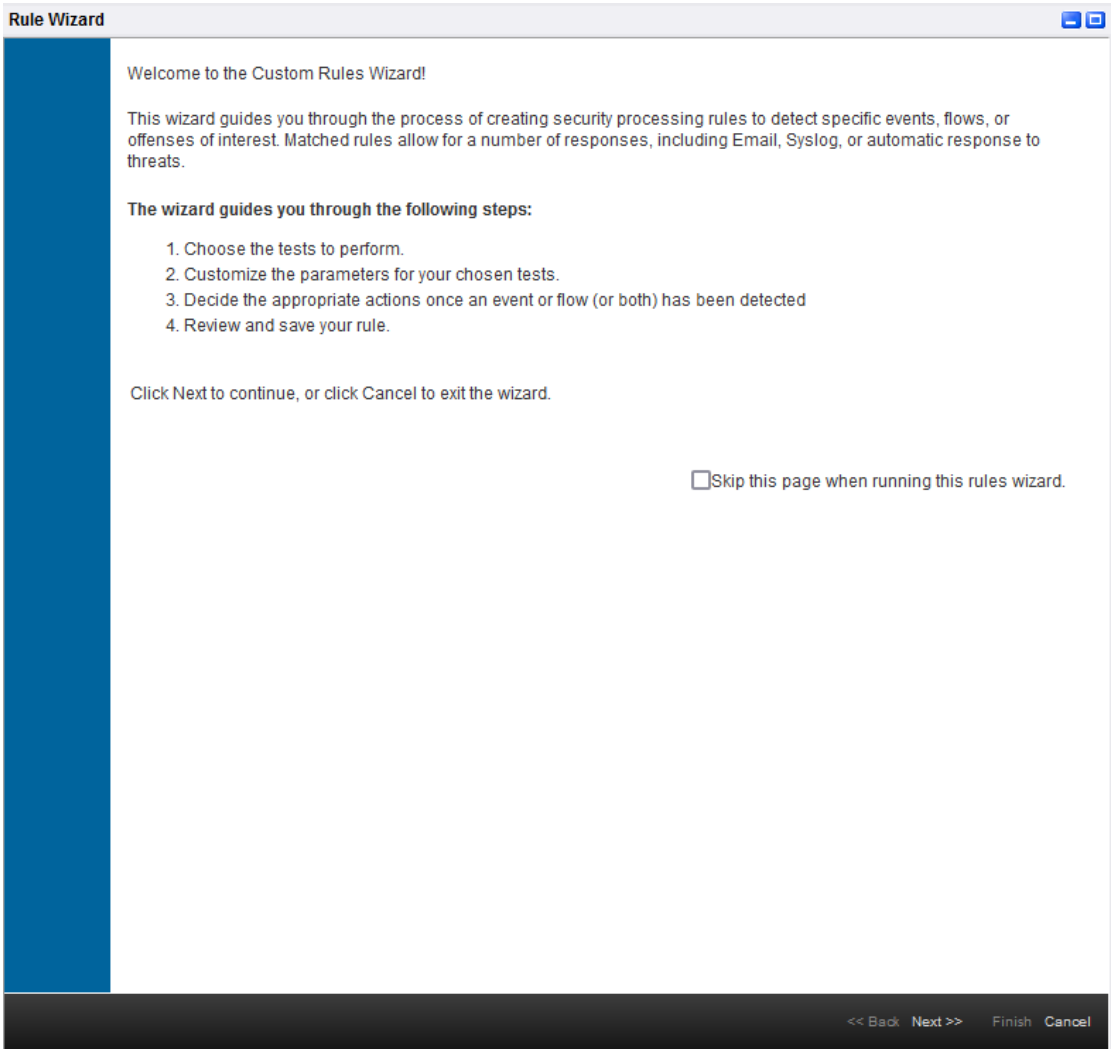
Για να το πραγματοποιήσουμε αυτό θα πρέπει να πάμε στην καρτέλα Offenses και από εκεί επιλέγουμε την κατηγορία Rules και μετά Actions. Εμφανίζονται πολλαπλές επιλογές για το είδους κανόνα θέλουμε να δημιουργήσουμε.

Στα δικά μας παραδείγματα βασιζόμαστε σε Events άρα σε κάθε περίπτωση θα επιλέγουμε New Event Rule



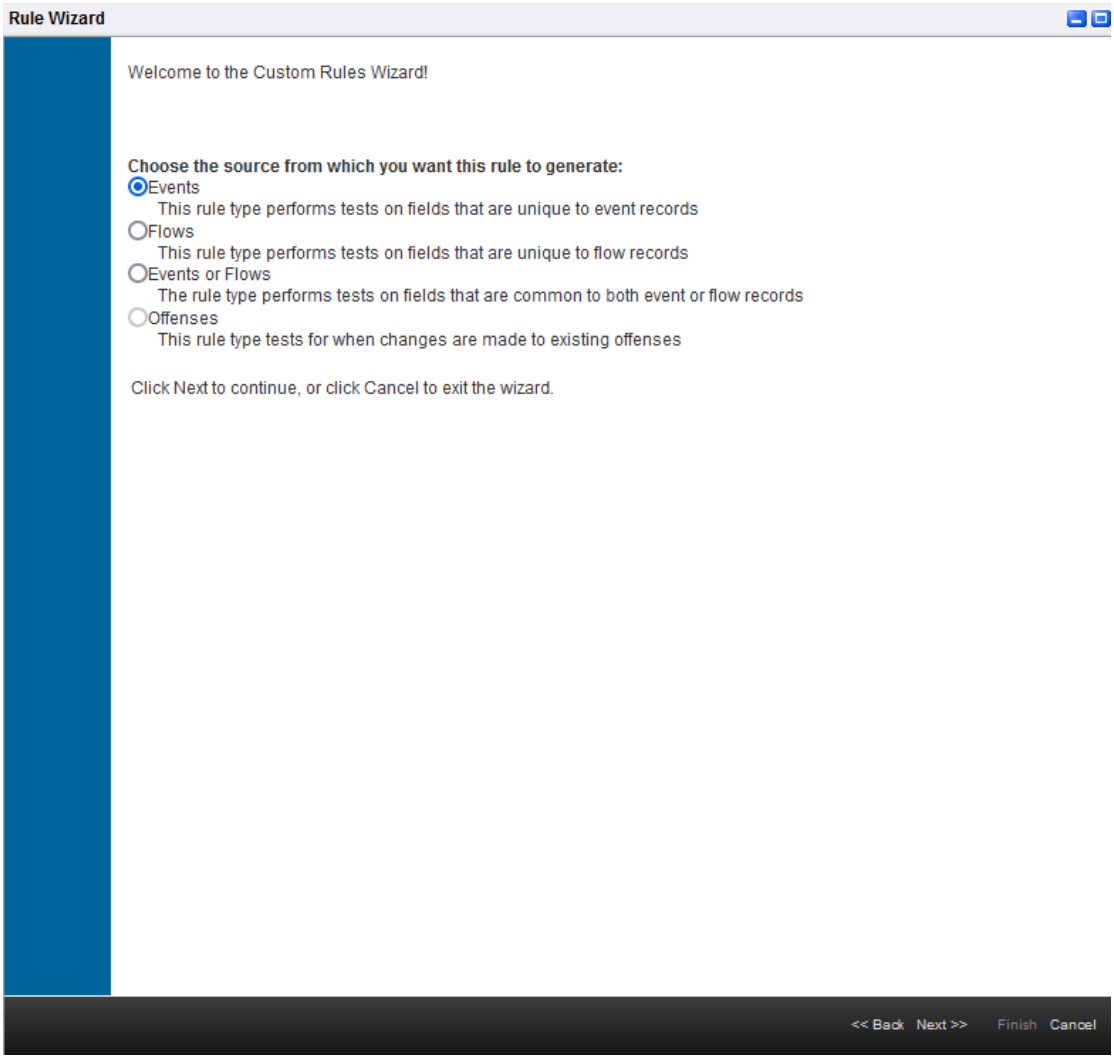
Εικόνα 4.4.1: Δημιουργία νέου κανόνα συσχέτισης

Στο παράθυρο που θα μας εμφανιστεί ακολουθούμε τα βήματα όπως μας παρουσιάζονται πατώντας Next



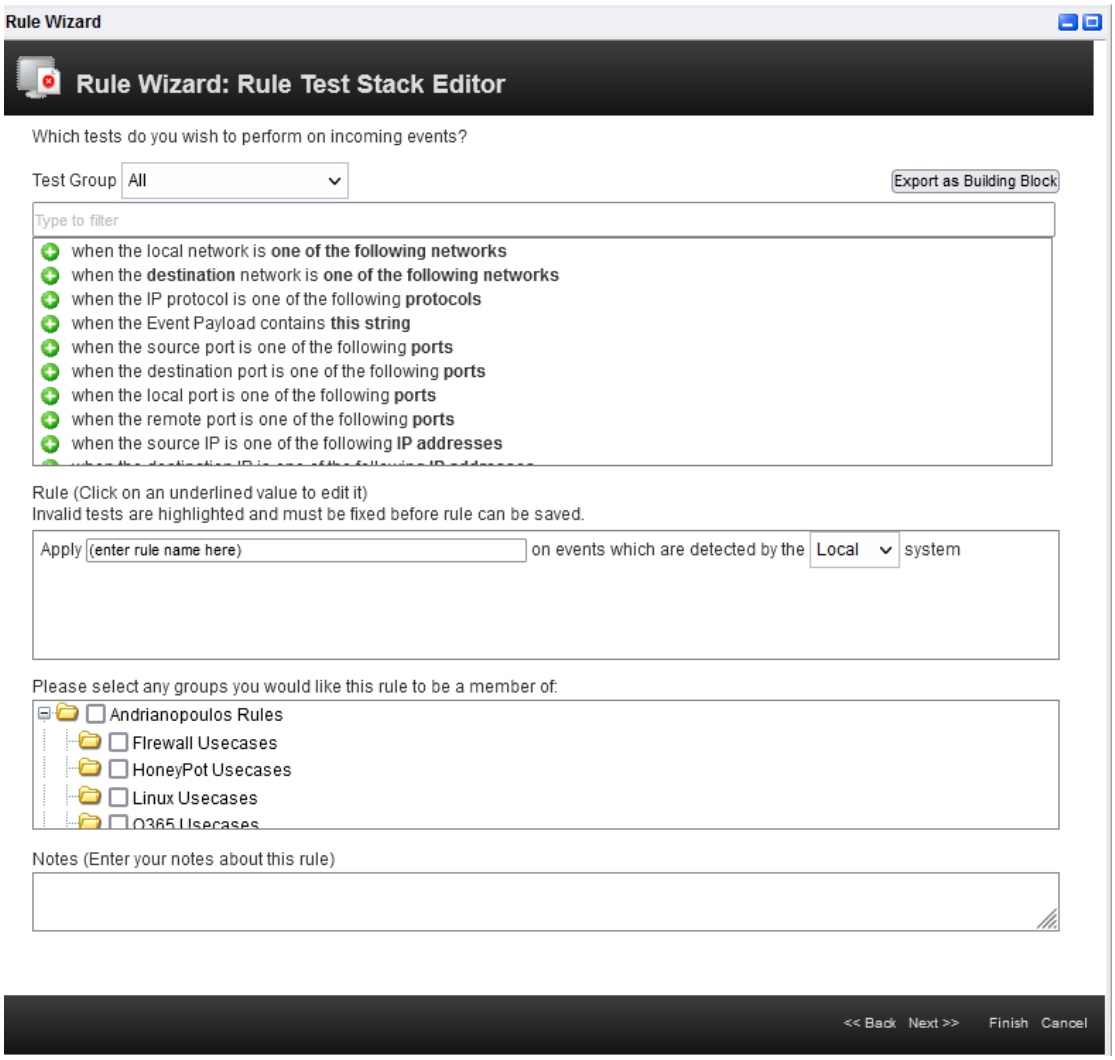
Εικόνα 4.4.2: Δημιουργία νέου κανόνα συσχέτισης

Επιλέγουμε την πηγή των δεδομένων που θα χρησιμοποιήσουμε για τη δημιουργία του κανόνα



Εικόνα 4.4.3: Δημιουργία νέου κανόνα συσχέτισης

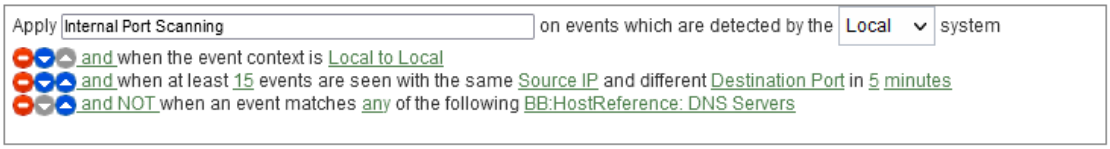
Τέλος μας εμφανίζεται το παράθυρο έτσι ώστε να δημιουργήσουμε τον κανόνα που επιθυμούμε.



Εικόνα 4.4.4: Δημιουργία νέου κανόνα συσχέτισης

Internal Port Scanning

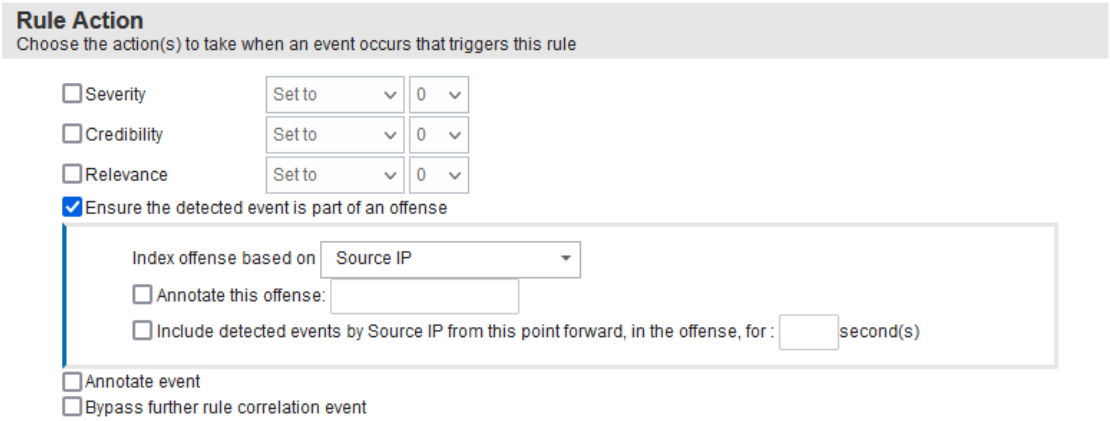
Περιεχόμενο κανόνα:



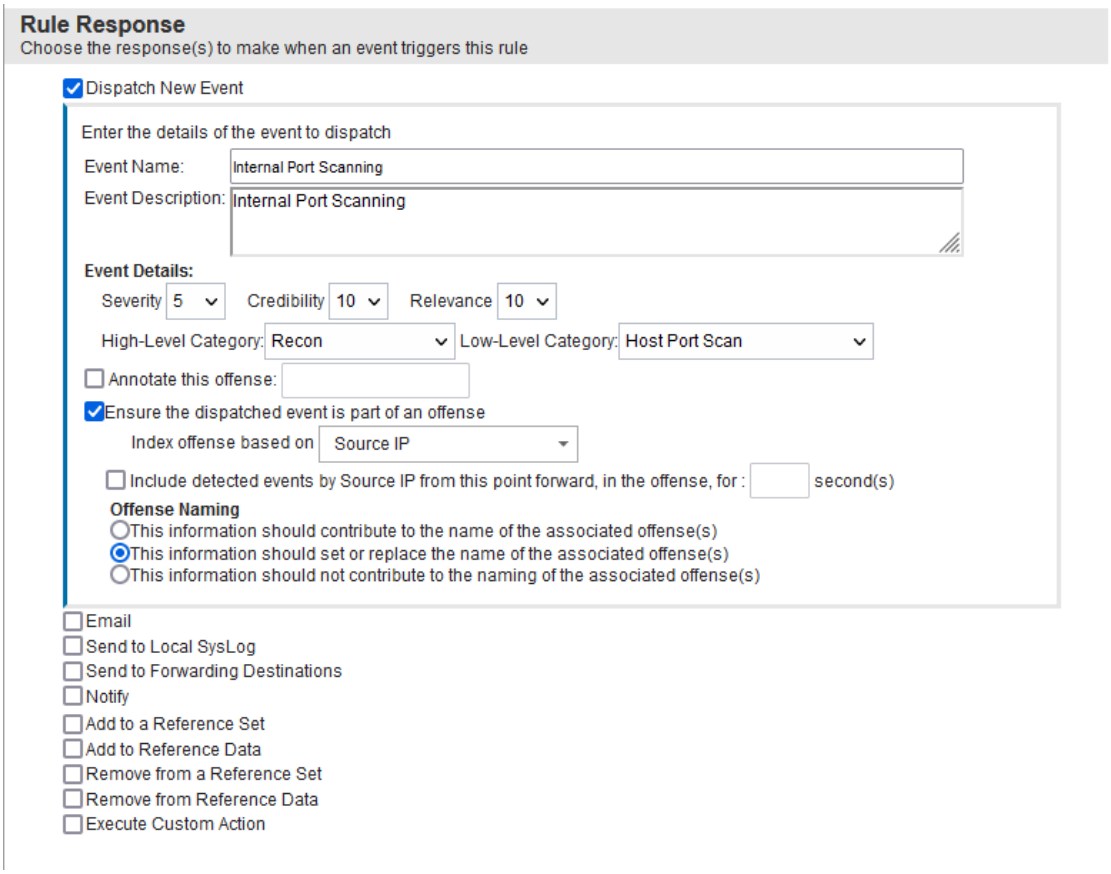
Εικόνα 4.4.5: Επεξεργασία κανόνα συσχέτισης

Apply Internal Port Scanning on events which are detected by the Local system and when at least 15 events are seen with the same Source IP and different Destination Port in 5 minutes and NOT when an event matches any of the following BB:HostReference: DNS Servers

Ενέργειες κανόνα:



Εικόνα 4.4.6: Επεξεργασία κανόνα συσχέτισης



Εικόνα 4.4.7: Επεξεργασία κανόνα συσχέτισης

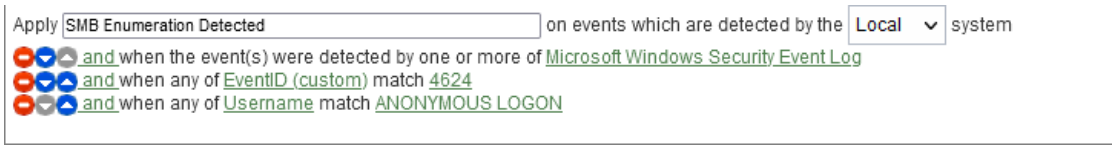
Εικόνα 4.4.8: Επεξεργασία κανόνα συσχέτισης

Σχόλια:

Έχει περαστεί μία μόνο εξαίρεση για να μην υπάρχει θόρυβος από False Positives. Η εξαίρεση είναι στο Building Block με όνομα **BB:HostReference: DNS Servers** και περιέχει τους DNS Servers όπου επικοινωνούν όλα τα τερματικά του δικτύου μας.

SMB Enumeration

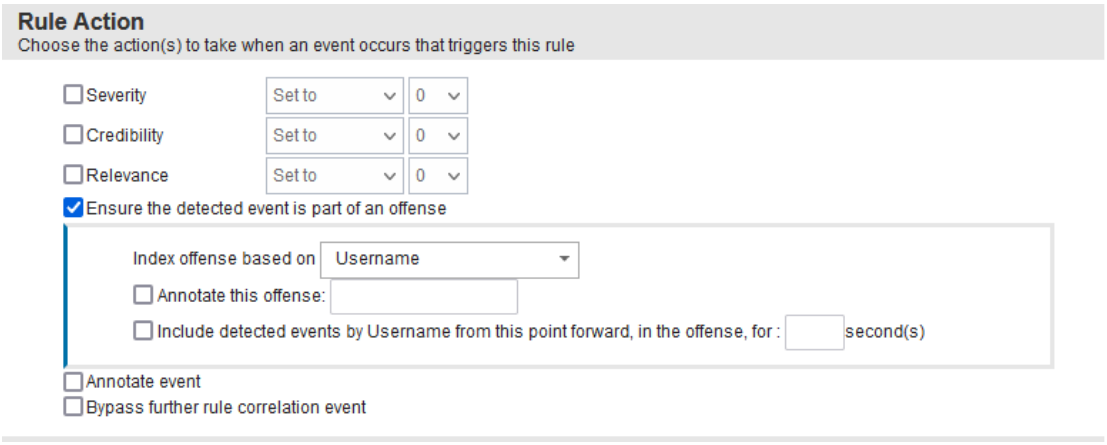
Περιεχόμενο κανόνα:



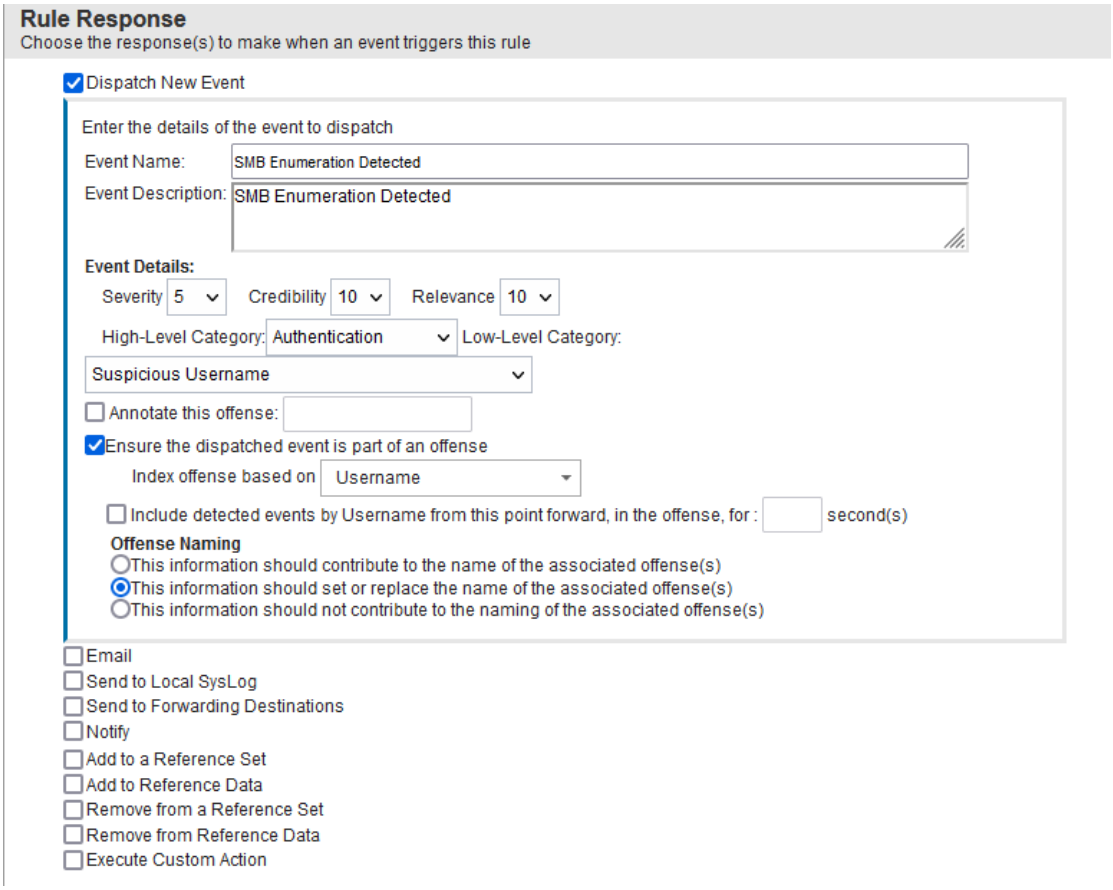
Εικόνα 4.4.9: Επεξεργασία κανόνα συσχέτισης

Apply SMB Enumeration Detected 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 4624 and when any of Username match ANONYMOUS LOGON

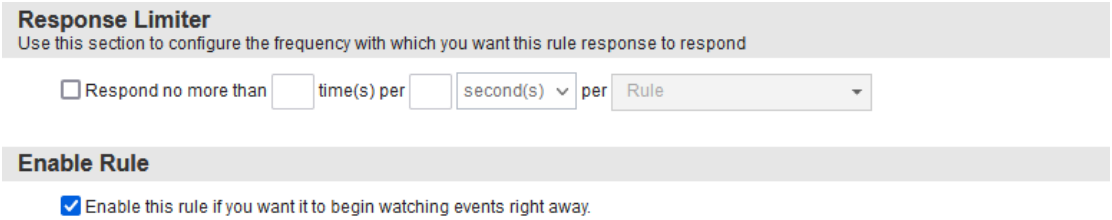
Ενέργειες κανόνα:



Εικόνα 4.4.10: Επεξεργασία κανόνα συσχέτισης



Εικόνα 4.4.11: Επεξεργασία κανόνα συσχέτισης



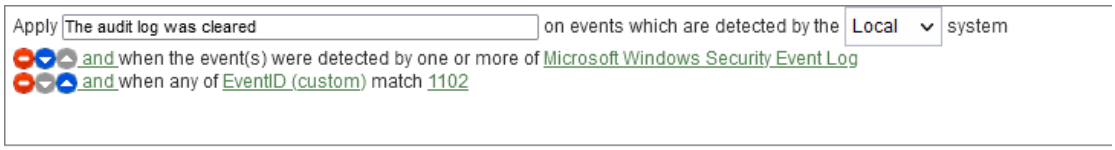
Εικόνα 4.4.12: Επεξεργασία κανόνα συσχέτισης

Σχόλια:

Ο κανόνας έχει δημιουργηθεί με βάση το Event ID και το Username που λαμβάνουμε κατά τη διεξαγωγή του Enumeration. Επιπροσθέτως έχουμε περιορίσει τον κανόνα μας να ελέγχει μόνο τα Microsoft Windows Security event logs.

Audit Log Clear

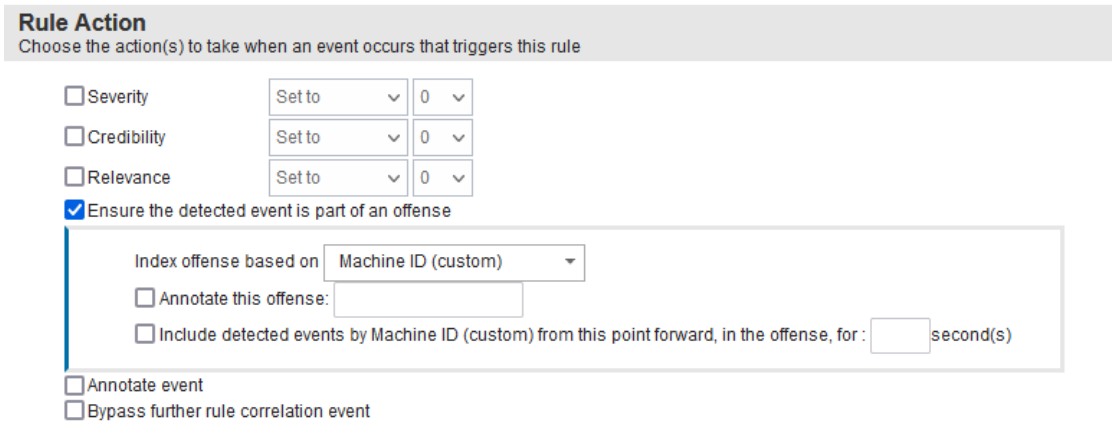
Περιεχόμενο κανόνα:



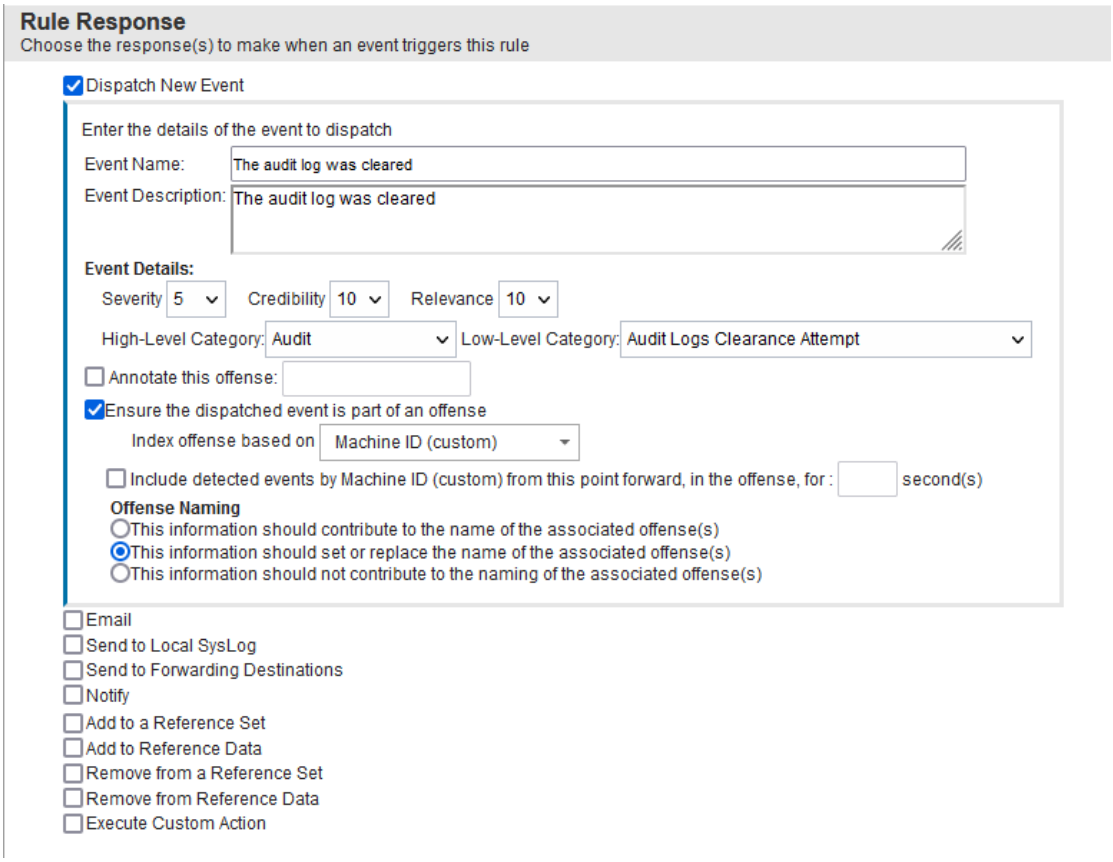
Εικόνα 4.4.13: Επεξεργασία κανόνα συσχέτισης

Apply The audit log was cleared 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 1102

Ενέργειες κανόνα:



Εικόνα 4.4.14: Επεξεργασία κανόνα συσχέτισης



Εικόνα 4.4.15: Επεξεργασία κανόνα συσχέτισης

Εικόνα 4.4.16: Επεξεργασία κανόνα συσχέτισης

Σχόλια:

Ο κανόνας έχει δημιουργηθεί με βάση το Event ID που λαμβάνουμε, επιπροσθέτως έχουμε περιορίσει τον κανόνα μας να ελέγχει μόνο τα Microsoft Windows Security event logs.

Κεφάλαιο 5

Συμπεράσματα

Συνοψίζοντας, η παρούσα διπλωματική εργασία εστιάστηκε στην ανάλυση επιθέσεων σε συστήματα Windows μέσω των καταγραφών ασφαλείας και των κανόνων συσχετισμού ενός συστήματος SIEM. Τα συμπεράσματα που προέκυψαν είναι πολυδιάστατα και αναδεικνύουν την πολυπλοκότητα και τη σημασία της αποτελεσματικής διαχείρισης της ασφάλειας σε πληροφοριακά συστήματα.

Πρώτον, τα αρχεία καταγραφής συμβάντων ασφαλείας των Windows αποτελούν ζωτικής σημασίας πόρους για τους οργανισμούς. Η αποτελεσματική παρακολούθηση και ανάλυση αυτών των καταγραφών επιτρέπει στους οργανισμούς να ανιχνεύουν και να ανταποκρίνονται σε συμβάντα ασφαλείας, να επιβάλλουν πολιτικές ασφαλείας και να διασφαλίζουν την ακεραιότητα των πληροφορικών τους περιβαλλόντων.

Δεύτερον, τα συστήματα SIEM αναδεικνύονται ως απαραίτητα εργαλεία για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Παρέχουν τα μέσα για τη συγκέντρωση δεδομένων ασφαλείας, την ανίχνευση απειλών, τη διευκόλυνση της απόκρισης σε περιστατικά και τη διασφάλιση της συμμόρφωσης. Ωστόσο, η επιτυχής εφαρμογή και λειτουργία ενός συστήματος SIEM απαιτεί προσεκτικό σχεδιασμό, εξειδικευμένο προσωπικό και δέσμευση για συνεχή συντήρηση και βελτιστοποίηση.

Οι κανόνες συσχέτισης είναι κρίσιμοι για τον εντοπισμό και την καταπολέμηση εξειδικευμένων απειλών. Απαιτείται συνεχής συντήρηση των κανόνων αυτών για την αποφυγή ψευδώς θετικών αποτελεσμάτων και πρέπει να τηρούνται οι βέλτιστες πρακτικές δημιουργίας τους ώστε να μην επιβαρύνεται υπερβολικά το σύστημα SIEM. Η εξισορρόπηση της ακρίβειας ανίχνευσης με τα ψευδώς θετικά ποσοστά αποτελεί μια συνεχή πρόκληση στον εντοπισμό επιθέσεων.

Η συνεχής παρακολούθηση και οι τακτικές ενημερώσεις είναι απαραίτητες για την προσαρμογή στις εξελισσόμενες απειλές. Το απόρρητο και τα νομικά ζητήματα πρέπει επίσης να λαμβάνονται υπόψη κατά την εφαρμογή ορισμένων μεθόδων ανίχνευσης, ιδιαίτερα αυτών που αφορούν την παρακολούθηση της συμπεριφοράς των χρηστών.

Η εργασία αυτή περιέλαβε την ανάπτυξη και υλοποίηση ενός συστήματος ανίχνευσης επιθέσεων σε Windows συστήματα, βασισμένου στις καταγραφές που αποστέλλονται σε ένα SIEM. Η ανάλυση περιλάμβανε τις διαδικασίες εγκατάστασης και παραμετροποίησης των απαραίτητων συστημάτων, καθώς και τη δημιουργία κανόνων συσχέτισης και την ανάλυση επιθέσεων που πραγματοποιήθηκαν.

Η διαδικασία ελέγχου ευπαθειών, η διαγραφή των αρχείων καταγραφής ελέγχου και ο έλεγχος κοινόχρηστων φακέλων και χρηστών του δικτύου, αναδεικνύοντας την επιθετική προοπτική, προσέφεραν ενδιαφέρουσες πτυχές στην κυβερνοασφάλεια. Αυτή η προσέγγιση αναδεικνύει τη σημασία της συνολικής κατανόησης του κυβερνοασφαλούς περιβάλλοντος και της ανάγκης για διαρκή ενημέρωση και προσαρμογή των μέτρων ασφαλείας.

Στη διαμόρφωση του συστήματος SIEM και την προετοιμασία του για λήψη καταγραφών από Windows συστήματα, καθώς και στην παραμετροποίηση επιλεγμένων Windows συστημάτων με στόχο τη δημιουργία ευάλωτων σημείων για ανάλυση επιθέσεων, αποκαλύπτεται η σημασία της προαγωγής της ασφάλειας σε κάθε επίπεδο του συστήματος.

Τέλος, η διπλωματική εργασία αναδεικνύει την ανάγκη για συνεχείς προσπάθειες εκπαίδευσης και ενημέρωσης στον τομέα της κυβερνοασφάλειας, καθώς οι απειλές εξελίσσονται συνεχώς. Η συνολική προσέγγιση που υιοθετήθηκε στην εργασία αυτή αποτελεί ένα βήμα προς την κατανόηση και την αντιμετώπιση των προκλήσεων που παρουσιάζονται στον σύγχρονο κυβερνοχώρο.

Με βάση τα ανωτέρω, η εργασία αυτή συμβάλλει σημαντικά στην κατανόηση των σύγχρονων προκλήσεων στην κυβερνοασφάλεια και στην ανάπτυξη αποτελεσματικών στρατηγικών για την αντιμετώπιση τους, προσφέροντας πρακτικές λύσεις και συστάσεις για την βελτίωση της ασφάλειας των πληροφοριακών συστημάτων.

Βιβλιογραφία

Beheshti, H. M. (2018, June). A study on penetration testing process and tools,. Ανάκτηση February 2024, από https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8378035&isnumber=8378007

Bertino, E. (2012). Security Information and Event Management and Auditing. *Synthesis Lectures on Data Management* . Ανάκτηση March 2024, από https://link.springer.com/chapter/10.1007/978-3-031-01890-9_5

Boudhayan Chakrabarty, S. R. (2019-2021). *Securing Data on Threat Detection by Using IBM Spectrum Scale and IBM QRadar.* IBM Redbooks.

IBM . (2018, June 17). *IBM Security QRadar Hardware Guide.* Ανάκτηση January 2024, από IBM Security QRadar Hardware Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_QRadar_hardware_guide.pdf

IBM. (2018, June 17). *IBM Security QRadar Administration Guide.* Ανάκτηση January 2024, από IBM Security QRadar Administration Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_qradar_admin_guide.pdf

IBM. (2018, June 17). *IBM Security QRadar Application Configuration Guide.* Ανάκτηση January 2024, από IBM Security QRadar Application Configuration Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_defappcfg_guide.pdf

IBM. (2018, June 17). *IBM Security QRadar Architecture and Deployment Guide.* Ανάκτηση January 2024, από IBM Security QRadar Architecture and Deployment Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_siem_deployment.pdf

IBM. (2018, June 17). *IBM Security QRadar DSM Configuration Guide.* Ανάκτηση January 2024, από IBM Security QRadar DSM Configuration Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/iTeam_addendum/b_dsm_guide.pdf

IBM. (2018, June 17). *IBM Security QRadar Installation Guide.* Ανάκτηση January 2024, από IBM Security QRadar Installation Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_siem_inst.pdf

IBM. (2018, June 17). *IBM Security QRadar Quick Start Guide.* Ανάκτηση January 2024, από IBM Security QRadar Quick Start Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_qradar_qsg.pdf

IBM. (2018, June 17). *IBM Security QRadar Security Technical Installation Guide (STIG).* Ανάκτηση January 2024, από IBM Security QRadar Security Technical Installation Guide (STIG):

http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_STIG.pdf

IBM. (2018, June 17). *IBM Security QRadar SIEM Users Guide.* Ανάκτηση January 2024, από IBM Security QRadar SIEM Users Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_qradar_users_guide.pdf

IBM. (2018, June 17). *IBM Security QRadar Troubleshooting and System Notifications Guide.* Ανάκτηση January 2024, από IBM Security QRadar Troubleshooting and System Notifications Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_qradar_system_notifications.pdf

IBM. (2018, June 17). *IBM Security QRadar Tuning Guide.* Ανάκτηση January 2024, από IBM Security QRadar Tuning Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_qradar_tuning_guide.pdf

IBM. (2018, June 17). *IBM Security QRadar WinCollect User Guide.* Ανάκτηση January 2024, από IBM Security QRadar WinCollect User Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/iTeam_addendum/b_wincollect.pdf

IBM. (2018, June 17). *QRadar Log Manager to QRadar SIEM Migration Guide.* Ανάκτηση January 2024, από QRadar Log Manager to QRadar SIEM Migration Guide: http://public.dhe.ibm.com/software/security/products/qradar/documents/7.3.0/en/b_qlm_migration.pdf

IBM. (2019). *IBM QRadar Community Edition.* Ανάκτηση January 2024, από IBM QRadar Community Edition: https://www.ibm.com/community/101/wp-content/uploads/sites/5/2020/11/b_qradar_community_edition_7.3.3GA_v1.0.pdf

IBM. (2022). *IBM QRadar WinCollect.* Ανάκτηση January 2024, από IBM QRadar WinCollect: https://www.ibm.com/docs/en/SS42VS_SHR/pdf/b_wincollect.pdf

Kumar, R. T. (2019). Internal Network Penetration Testing Using Free/Open Source Tools: Network and System Administration Approach. Ανάκτηση February 2024, από https://doi.org/10.1007/978-981-13-3143-5_22

Microsoft. (2018, April). *Windows 10 system requirments*. Ανάκτηση March 2024, από Windows 10 system requirments: https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715

Microsoft. (2024, March 8). *Hardware requirements for Windows Server*. Ανάκτηση March 2024, από Hardware requirements for Windows Server: https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?tabs=cpu

PGI. (2019, September 16). *What's the difference between a vulnerability assessment and a penetration test?* Ανάκτηση March 2024, από What's the difference between a vulnerability assessment and a penetration test?:

https://www.pgitl.com/insights/whats-the-difference-between-a-vulnerability-assessment-and-a-penetration-test

Tidy, J. (2021, July). Swedish Coop supermarkets shut due to US ransomware cyber-attack. *Swedish Coop supermarkets shut due to US ransomware cyber-attack*. (B. News, Επιμ.) Ανάκτηση February 2024, από https://www.bbc.com/news/technology-57707530