Τεχνολογία ανίχνευσης σε ένα Cyber Range-AD

CSP011_W

ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ, ΕΡΓΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΧΡΙΣΤΟΣ ΛΑΖΑΡΙΔΗΣ

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

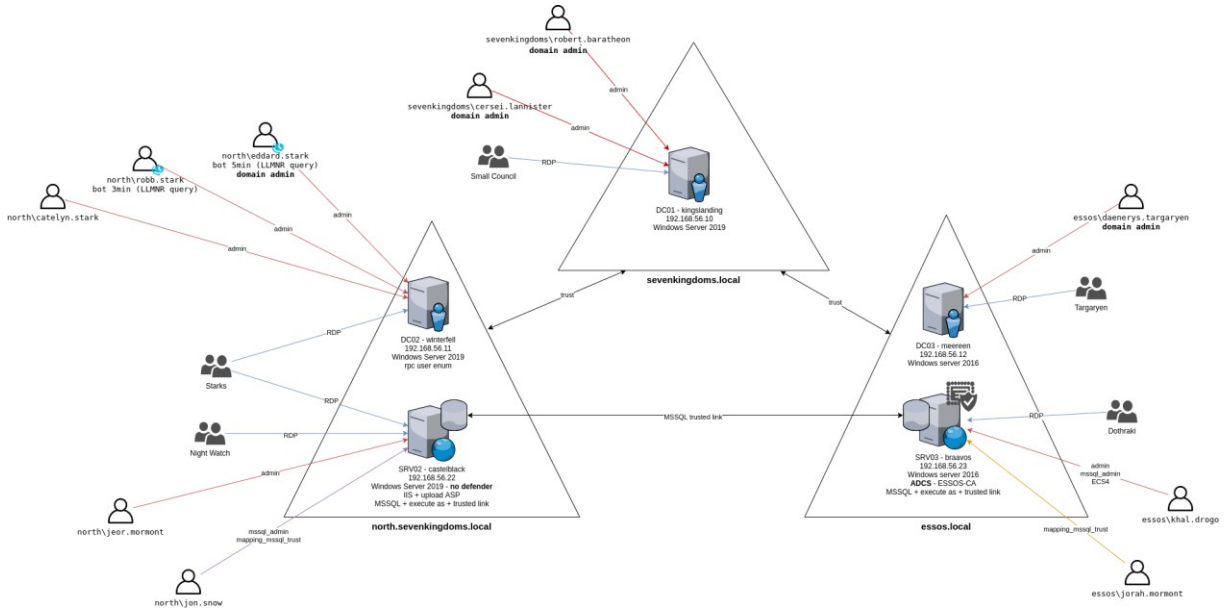
Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

ΕΡΓΑΣΤΗΡΙΟ - Εισαγωγή στο περιβάλλον του εργαστ

- Η αρχική εγκατάσταση βασίζεται στο ανοιχτού κώδι
  GOAD
  - Game of Active Directory (GOAD)
- 3 Τομείς:
  - sevenkingdoms – 1 Ελεγκτής Τομέα (kingslanding)
  - essos – 1 ελεγκτής τομέα (meereen), 1 διακομιστής ADCS (braavos)
  - north – 1 ελεγκτής τομέα (winterfell), 1 διακομιστής IIS (castelblack)



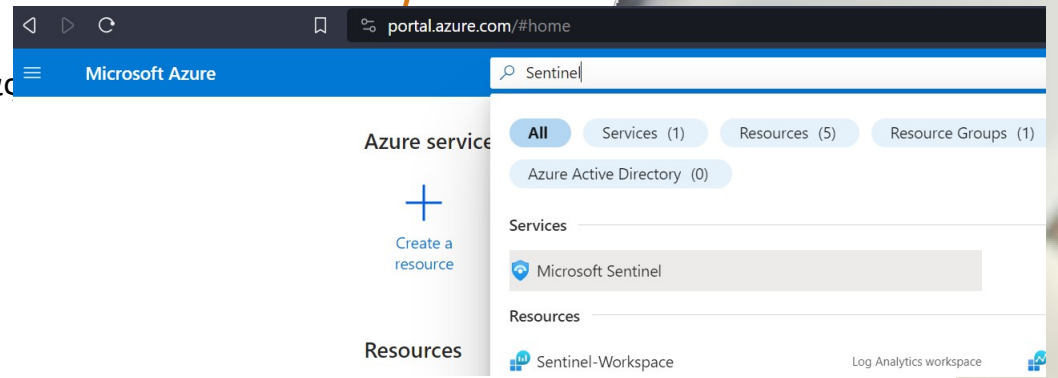
ΕΡΓΑΣΤΗΡΙΟ - Υποδομή Goad

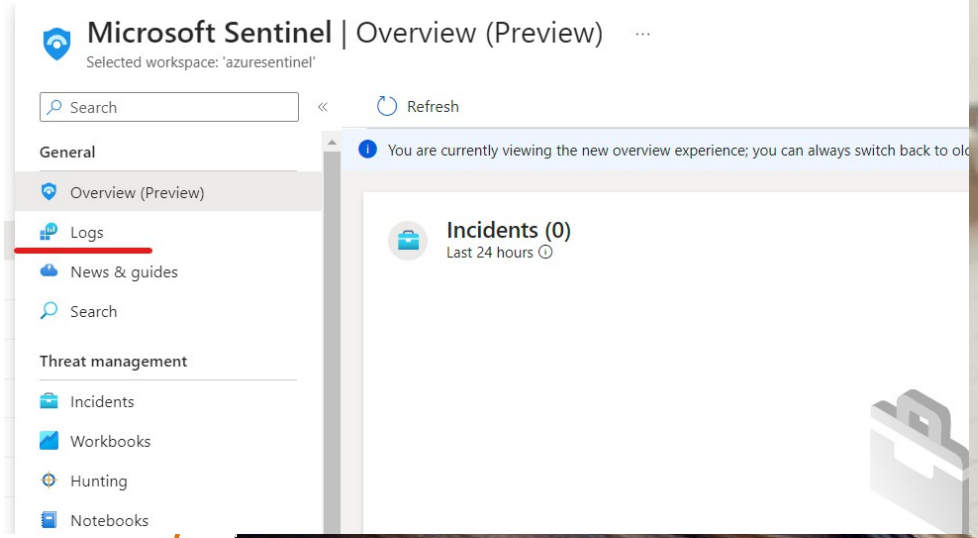
Διεύθυνση IP	Λειτουργία	Λειτουργικό σύστημα	Όνομα	Τομέας
192.168.56.10	Τομέας Windows Ελεγκτής	Windows Server 2019	dc01 - kingslanding	sevenkingdoms
192.168.56.11	Ελεγκτής τομέα Windows	Windows Server 2016	dc02 - winterfell	north.sevenkingdo ms
192.168.56.12	Τομέας Windows Ελεγκτής	Windows Server 2016	dc03 - meereen	essos
192.168.56.22	Διακομιστής Web	Windows Server 2016	srv01 - castelblack	north.sevenkingdoms
192.168.56.23	Διακομιστής ADCS	Windows Server 2016	srv02 - bravoos	essos
192.168.56.100	• Τείχος προστασίας • Σύστημα ανίχνευσης εισβολών - Suricata • Προεπιλεγμένη πύλη • Διακομιστής OpenVPN	PfSense	-	-

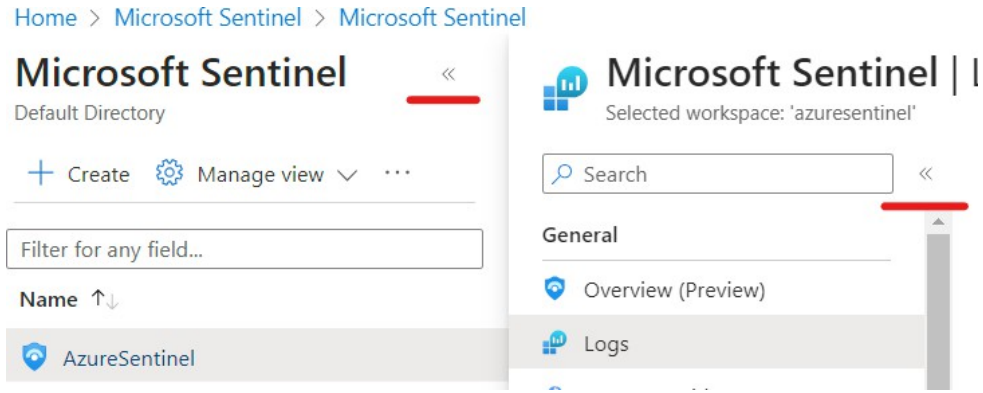
ΕΡΓΑΣΤΗΡΙΟ

Πρόσβαση στο Azure Sentinel

- Πρόσβαση στο Sentinel
  - Ανοίξτε μια ιδιωτική καρτέλα ή ένα προφίλ επισκέπτη στον περιηγητή σας
  - https://portal.azure.com
  - Όνομα χρήστη: [παρέχεται] Κωδικός πρόσβασης: [παρέχεται]
  - Μεταβείτε στο πεδίο αναζήτησης στο πάνω μέρος της σελίδας, πληκτρολογήστε «Sentinel» και κάντε κλικ στο «Microsoft Sentinel»
  - Στη στήλη «Όνομα», κάντε κλικ στο AzureSentinel
  - Στη νέα καρτέλα, μεταβείτε στην ενότητα «Logs»
  - Κλείστε τυχόν αναδυόμενα παράθυρα που εμφανίζονται και αποκρύψτε τυχόν μενού για να έχετε πλήρη οθόνη στα αρχεία καταγραφής



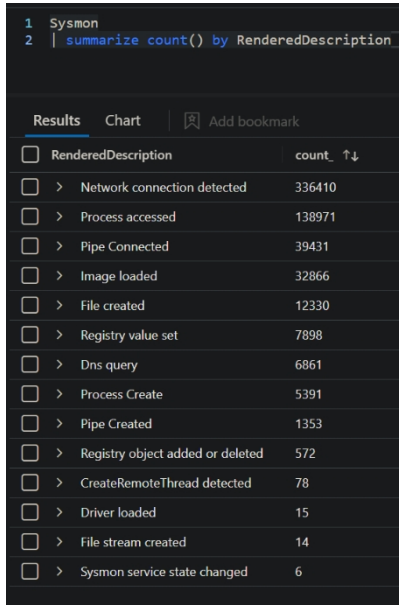


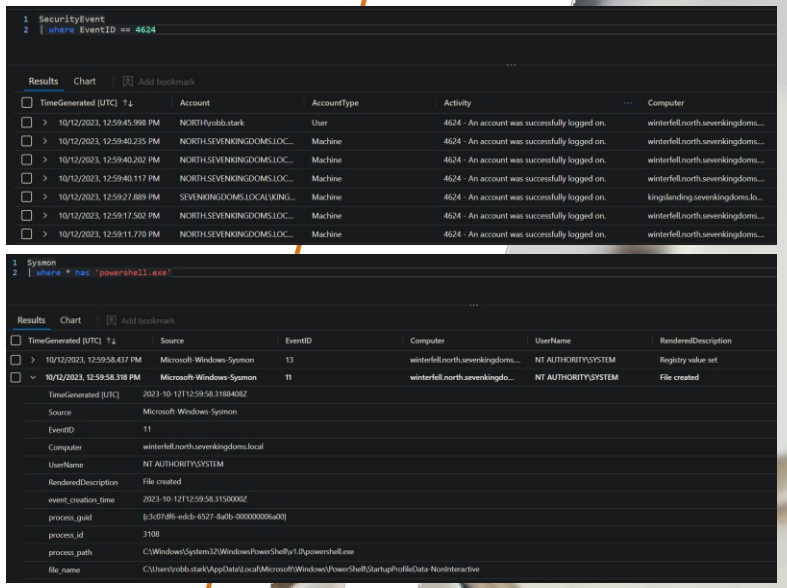


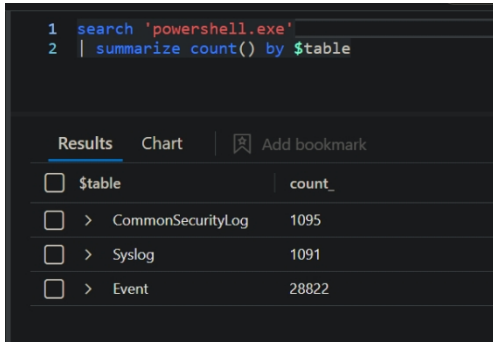
ΕΡΓΑΣΤΗΡΙΟ

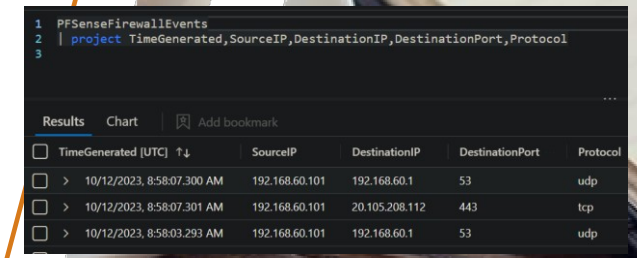
Ανάλυση καταγραφών με τη γλώσσα ερωτημάτων Kusto

- Πίνακες συμβάντων σε περιβάλλον Lab
  - SecurityEvent
  - Sysmon (με βάση το Event)
  - Suricata
  - PFSenseFirewallEvents
- Φιλτράρισμα συμβάντων
  - Φιλτράρισμα κατά συνθήκη (where)
  - Έλεγχος αν κάποια στήλη περιέχει συμβολοσειρά (όπου * έχει)
  - Επιλογή υποσύνολου στηλών (project)
  - Λίστα μοναδικών τιμών (distinct)
  - Τελεστής αναζήτησης
  - Τελεστές σε συμβολοσειρές (==, !=, has, contains)
- Συγκέντρωση συμβάντων
  - Χρήση του τελεστή συνοψίσεως (summarize)
  - Υπολογισμός σειρών υπό όρους (countif())
  - Διακριτές τιμές (dcount())
  - Ομαδοποίηση δεδομένων σε κατηγορίες (bin())
  - Ανάλυση χρονοσειρών (make-series)
- Οπτικοποίηση
  - Οπτικοποίηση αποτελεσμάτων ερωτήματος (render)







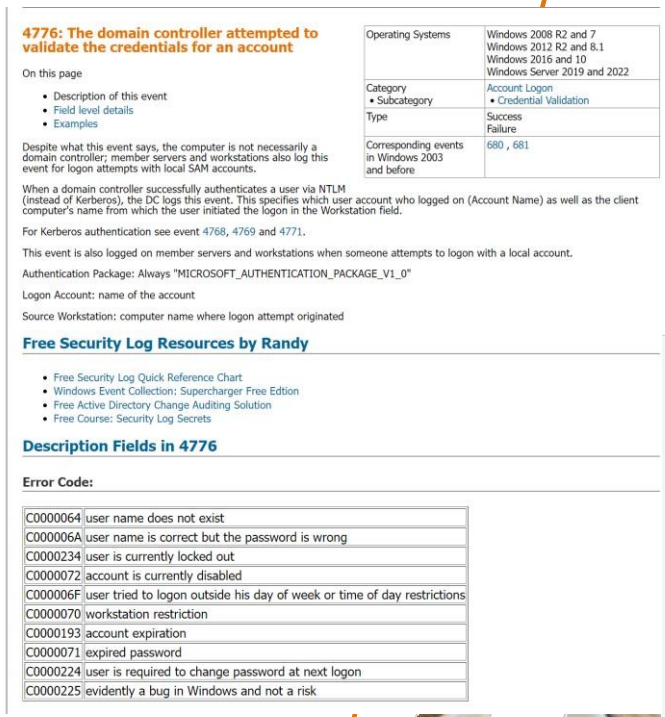


ΕΡΓΑΣΤΗΡΙΟ

Συγκεκριμένα χαρακτηριστικά καταγραφής - SecurityEvent

- Παροχή πληροφοριών ελέγχου σχετικά με δραστηριότητες που λαμβάνουν χώρα σε λειτουργικά συστήματα Windows
- Τύποι συμβάντων:
  - KQL:

    SecurityEvent | distinct Activity
- Περισσότερες πληροφορίες σχετικά με κάθε τύπο καταγραφής μπορείτε να βρείτε στους παρακάτω συνδέσμους
  - Συμβάντα του αρχείου καταγραφής ασφαλείας των Windows



4776: The domain controller attempted to validate the credentials for an account

On this page

- Description of this event
- Field level details
- Examples

Despite what this event says, the computer is not necessarily a domain controller; member servers and workstations also log this event for logon attempts with local SAM accounts.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category • Subcategory	Account Logon • Credential Validation
Type	Success Failure
Corresponding events in Windows 2003 and before	680 , 681

When a domain controller successfully authenticates a user via NTLM (instead of Kerberos), the DC logs this event. This specifies which user account who logged on (Account Name) as well as the client computer's name from which the user initiated the logon in the Workstation field.

For Kerberos authentication see event 4768, 4769 and 4771.

This event is also logged on member servers and workstations when someone attempts to logon with a local account.

Authentication Package: Always "MICROSOFT_AUTHENTICATION_PACKAGE_V1_0"

Logon Account: name of the account

Source Workstation: computer name where logon attempt originated

Free Security Log Resources by Randy

- Free Security Log Quick Reference Chart
- Windows Event Collection: Supercharger Free Edtion
- Free Active Directory Change Auditing Solution
- Free Course: Security Log Secrets

Description Fields in 4776

Error Code:

C0000064	user name does not exist
C000006A	user name is correct but the password is wrong
C0000234	user is currently locked out
C0000072	account is currently disabled
C000006F	user tried to logon outside his day of week or time of day restrictions
C0000070	workstation restriction
C0000193	account expiration
C0000071	expired password
C0000224	user is required to change password at next logon
C0000225	evidently a bug in Windows and not a risk

```
1  SecurityEvent | distinct Activity
```

Results | Chart | Add bookmark

Activity
4672 - Special privileges assigned to new logon.
4624 - An account was successfully logged on.
4634 - An account was logged off.
4768 - A Kerberos authentication ticket (TGT) was requested.
4769 - A Kerberos service ticket was requested.
4648 - A logon was attempted using explicit credentials.
4799 - A security-enabled local group membership was enumerated
4662 - An operation was performed on an object.
4670 - Permissions on an object were changed.
5379
5061 - Cryptographic operation.
4770 - A Kerberos service ticket was renewed.
4776 - The domain controller attempted to validate the credentials for an account.
5058 - Key file operation.
5059 - Key migration operation.
4798 - A user's local group membership was enumerated.
4616 - The system time was changed.

Logon Type:

This is a valuable piece of information as it tells you HOW the user just logged on:

Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication") See this article for more information.
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see 4648. MS says "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections."
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

ΕΡΓΑΣΤΗΡΙΟ

Χρήση του MITRE ATT&CK για την ανίχνευση - SecurityEvent

- Τύπος τακτικών ATT&CK που ανιχνεύθηκαν
  - Πρόσβαση σε διαπιστευτήρια
    - Brute Force (Αναγνωριστικό συμβάντος: 4625 ή 5379)
    - Κλοπή ή πλαστογράφηση εισιτηρίων Kerberos: Kerberoasting (Αναγνωριστικό συμβάντος: 4769)
    - Αποθήκευση διαπιστευτηρίων λειτουργικού συστήματος: DCSync (Αναγνωριστικό συμβάντος: 4662)
  - Εκτέλεση
    - Διερμηνέας εντολών και σεναρίων: Κέλυφος εντολών των Windows (Αναγνωριστικό συμβάντος: 4688)
  - Επιμονή
    - Προγραμματισμένη εργασία/εργασία (Αναγνωριστικό συμβάντος: 4
    - Υπηρεσίες συστήματος (Αναγνωριστικό συμβάντος: 4697)
  - Αύξηση προνομίων
    - Τροποποίηση πολιτικής ομάδας (Αναγνωριστικό συμβάντος: 513
  - Πλευρική μετακίνηση
    - Πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (RDP) (Αν
  - Αποφυγή άμυνας
    - Χρήση εναλλακτικού υλικού πιστοποίησης: Pass the Hash (Αναγνωριστικό συμβάντος: 4769, 4624)

Detection

ID	Data Source	Data Component	Detects
DS0026	Active Directory	Active Directory Object Creation	Monitor for newly constructed active directory objects, such as Windows EID 5137.
		Active Directory Object Deletion	Monitor for unexpected deletion of an active directory object, such as Windows EID 5141.
		Active Directory Object Modification	Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).

Detection

ID	Data Source	Data Component	Detects
DS0026	Active Directory	Active Directory Credential Request	Monitor for anomalous Kerberos activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]).

DS0002	User Account	User Account Authentication	Monitor for user authentication attempts. From a classic Pass-The-Hash perspective, this technique uses a hash through the NTLMv1 / NTLMv2 protocol to authenticate against a compromised endpoint. This technique does not touch Kerberos. Therefore, NTLM LogonType 3 authentications that are not associated to a domain login and are not anonymous logins are suspicious. From an Over-Pass-The-Hash perspective, an adversary wants to exchange the hash for a Kerberos authentication ticket (TGT). One way to do this is by creating a sacrificial logon session with dummy credentials (LogonType 9) and then inject the hash into that session which triggers the Kerberos authentication process.

ΕΡΓΑΣΤΗΡΙΟ

Συγκεκριμένα χαρακτηριστικά καταγραφής - Sysmon

- Το Sysmon είναι ενεργοποιημένο σε όλους τους κεντρικούς υπολογιστές Windows
  - Παρέχει ορατότητα σε επίπεδο τερματικού
- Τύποι συμβάντων:
  - KQL:

    Sysmon | distinct RenderedDescription
- Περισσότερες πληροφορίες για κάθε τύπο αρχείου καταγραφής μπορείτε να βρείτε στους παρακάτω συνδέσμους
  - Τύποι αρχείων καταγραφής Sysmon
  - Συμβάντα καταγραφής ασφάλειας των Windows (Sysmon)

```
1  Sysmon
2  | distinct RenderedDescription
```

Results | Chart | Add bookmark

RenderedDescription
File stream created
Driver loaded
Registry object added or deleted
Sysmon service state changed
CreateRemoteThread detected
Pipe Created
Registry value set
Dns query
Process Create
File created
Image loaded
Pipe Connected
Process accessed
Network connection detected

Event ID 7: Image loaded

The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the "`-l`" option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading. This event should be configured carefully, as monitoring all image load events will generate a significant amount of logging.

Event ID 8: CreateRemoteThread

The `CreateRemoteThread` event detects when a process creates a thread in another process. This technique is used by malware to inject code and hide in other processes. The event indicates the source and target process. It gives information on the code that will be run in the new thread: `StartAddress`, `StartModule` and `StartFunction`. Note that `StartModule` and `StartFunction` fields are inferred, they might be empty if the starting address is outside loaded modules or known exported functions.

Event ID 9: RawAccessRead

The `RawAccessRead` event detects when a process conducts reading operations from the drive using the `\\.\` denotation. This technique is often used by malware for data exfiltration of files that are locked for reading, as well as to avoid file access auditing tools. The event indicates the source process and target device.

ΕΡΓΑΣΤΗΡΙΟ

Χρήση του MITRE ATT&CK για την ανίχνευση - Sysmon

- Τύπος τακτικών ATT&CK που ανιχνεύθηκαν
  - Αρχική πρόσβαση
    - Phishing
    - Drive-by Compromise
  - Εκτέλεση
    - Διερμηνέας εντολών και σεναρίων
    - Εκτέλεση από χρήστη
  - Επιμονή
    - Προγραμματισμένη εργασία/εργασία
    - Παραβίαση ροής εκτέλεσης: Πλευρική φόρτωση DLL
    - Συστατικό λογισμικού διακομιστή: Web Shell
  - Παράκαμψη άμυνας
    - Απενεργοποίηση ή τροποποίηση εργαλείων
    - Κρυπτογραφημένα αρχεία ή πληροφορίες
  - Πρόσβαση σε διαπιστευτήρια
    - Αποθήκευση διαπιστευτηρίων λειτουργικού συστήματος
- Ανακάλυψη
  - Ανακάλυψη πληροφοριών συστήματος
  - Ερώτηση μητρώου
- Πλευρική μετακίνηση
  - Πρωτόκολλο απομακρυσμένης επιφάνειας ε
  - Μεταφορά εργαλείων πλευρικής κίνησης
- Επίδραση
  - Καταστροφή δεδομένων
  - Διαγραφή δίσκου
- Συλλογή
  - Δεδομένα από τοπικό σύστημα
  - Δεδομένα από αφαιρούμενα μέσα
- Διαρροή
  - Διαρροή μέσω καναλιού C2

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored.
DS0022	File	File Access	Monitor for hash dumpers opening the Security Accounts Manager (SAM) on the local file system (`%SystemRoot%/system32/config/SAM`). Some hash dumpers will open the local file system as a device and parse to the SAM table to avoid file access defenses. Others will make an in-memory copy of the SAM table before reading hashes. Detection of compromised Valid Accounts in-use by adversaries may help as well.

Detection

ID	Data Source	Data Component	Detects
DS0022	File	File Creation	Monitor for newly constructed files in common folders on the computer system.
		File Modification	Monitor for changes made to files for unexpected modifications to access permissions and attributes
DS0011	Module	Module Load	Monitor DLL/PE file events, specifically creation of these binary files as well as the loading of DLLs into processes. Look for DLLs that are not recognized or not normally loaded into a process.
DS0009	Process	Process Creation	Monitor newly constructed processes for unusual activity (e.g., a process that does not use the network begins to do so) as well as the introduction of new files/programs.

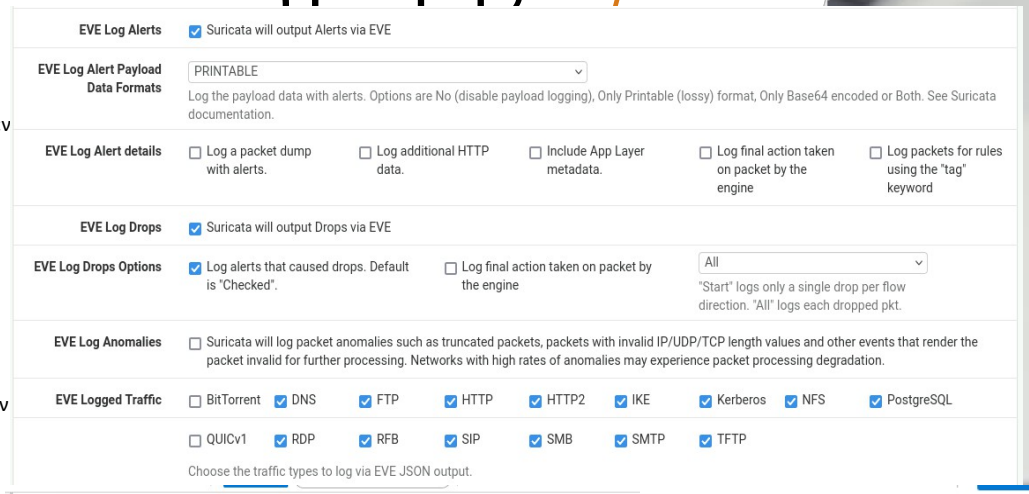
Process Access	Monitor for unexpected processes interacting with LSASS.exe.[95] Common credential dumpers such as Mimikatz access LSASS.exe by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.

ΕΡΓΑΣΤΗΡΙΟ

Συγκεκριμένα χαρακτηριστικά καταγραφής - Suricata

- Η καταγραφή του Suricata είναι ενεργοποιημένη
  - Παρέχει εξαιρετική ορατότητα σε επίπεδο δικτύου
  - Εκτός από τις ειδοποιήσεις, μπορεί επίσης να δημιουργεί αρχεία καταγραφής με βάση συγκεκριμέν
- Τύποι συμβάντων:
  - KQL:

    Suricata | distinct event_type
    | όπου event_type != ‘’
- Επέκταση
  - Μπορούν να εξαχθούν επιπλέον πληροφορίες από συγκεκριμένες στήλες με βάση τους τύπους των

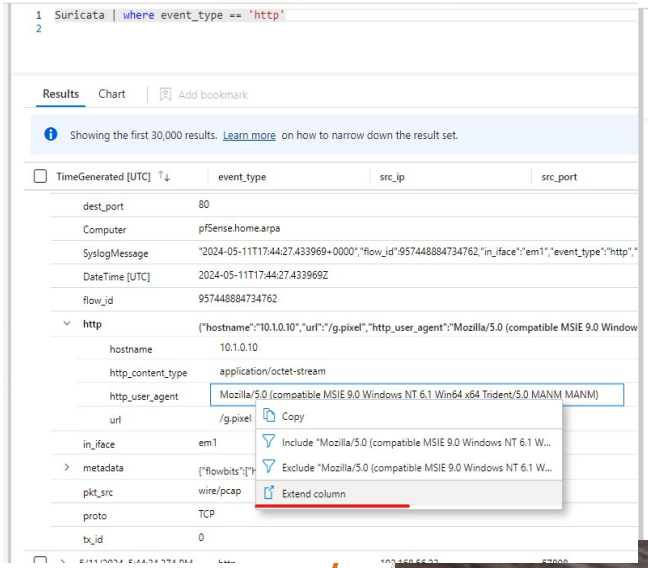


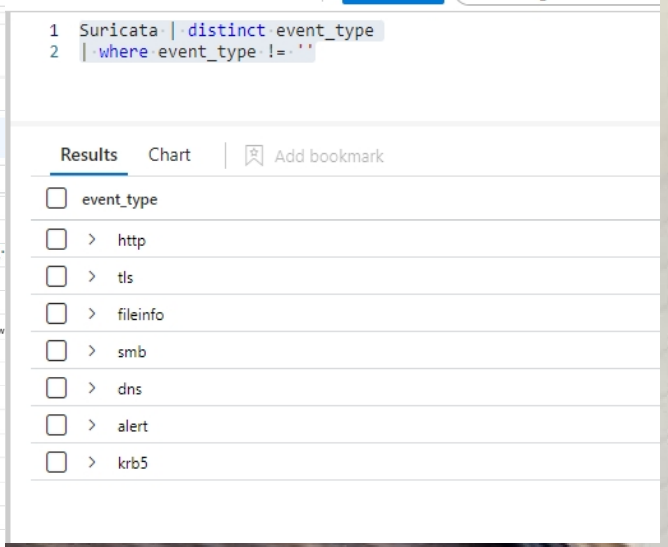

```
1  Suricata | where event_type == 'http'
2  | extend http_user_agent_ = tostring(http.http_user_agent)
```

Results | Chart | Add bookmark

Showing the first 30,000 results. Learn more on how to narrow down the result set.

TimeGenerated [UTC]	http_user_agent_	event_type
5/11/2024, 5:44:34.378 PM	Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 Trident/5.0) LBBROWSER	http
5/11/2024, 5:44:34.378 PM	Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 Win64 x64 Trident/5.0 MANM MANM)	http
5/11/2024, 5:44:34.378 PM	Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 Trident/5.0) LBBROWSER	http
5/11/2024, 5:44:34.377 PM	Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 WOW64 Trident/5.0 MALC)	http
5/11/2024, 5:44:34.377 PM	Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 WOW64 Trident/5.0 MANM MANM)	http
5/11/2024, 5:44:34.376 PM	Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 WOW64 Trident/5.0 MANM MANM)	http





ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Εκτέλεση αυτόματης εκκίνησης κατά την εκκίνηση ή τη σύνδεση: Κλειδιά εκτέλεσης μητρώου / Φάκελος εκκίνησης

Εκτέλεση αυτόματης εκκίνησης κατά την εκκίνηση ή τη σύνδεση: Κλειδιά εκτέλεσης μητρώου / Φάκελος εκκίνησης

- Η τοποθέτηση ενός προγράμματος σε φάκελο εκκίνησης θα έχει ως αποτέλεσμα την εκτέλεση του προγράμματος αυτού κατά τη σύνδεση ενός χρήστη. Υπάρχει ένας φάκελος εκκίνησης για κάθε μεμονωμένο λογαριασμό χρήστη, καθώς και ένας φάκελος εκκίνησης σε επίπεδο συστήματος, ο οποίος ελέγχεται ανεξάρτητα από το ποιος λογαριασμός χρήστη συνδέεται.
- Η διαδρομή του φακέλου εκκίνησης για τον τρέχοντα χρήστη είναι **C:\Users\[Όνομα χρήστη]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**.
- Η διαδρομή του φακέλου εκκίνησης για όλους τους χρήστες είναι **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp**.

Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τη λογική πίσω από τι

E: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: Sysmon

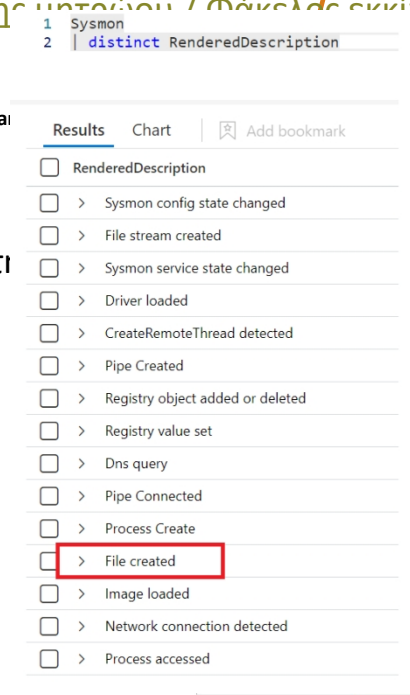
E: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων του Sysmon; A: Δημιουργία αρχείου

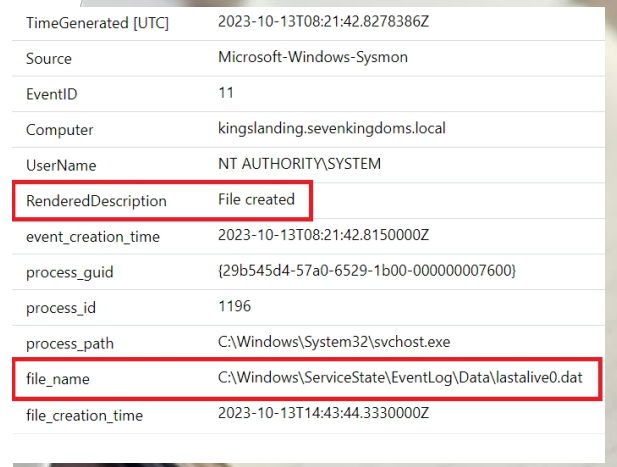
E: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο; A: Βασίζεται σε συμβάντα

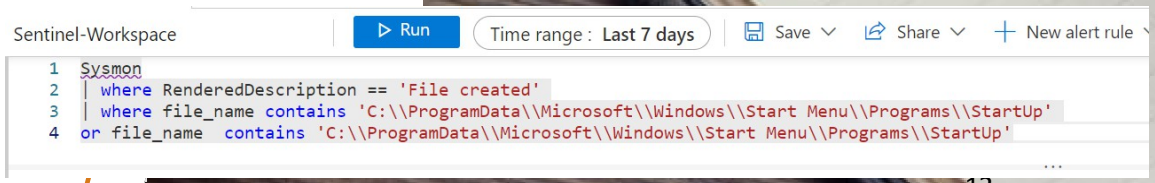
E: Ποιες στήλες είναι σημαντικές ώστε να τις χρησιμοποιήσουμε ως φίλτρα; A: Rendered Description, file_name

E: Τι φίλτρο θα βάλω στις σημαντικές στήλες:
A: 1. Η περιγραφή (Rendered Description) ισούται με «Δημιουργία αρχείου»
2. Το file_name περιέχει «\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup» ή το file_name περιέχει «C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\StartUp» *

*Συμβουλή σύνταξης KQL: Αντικαταστήστε το \ με \\ επειδή η κάθετος χρησιμοποιείται για την διαφυγή χαρακτήρων







ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Διαρροή μέσω υπηρεσίας Web

Διαρροή δεδομένων μέσω υπηρεσίας Web

- Οι εχθροί ενδέχεται να χρησιμοποιούν μια υπάρχουσα, νόμιμη εξωτερική υπηρεσία Web για την εξάτμιση δεδομένων αντί του κύριου καναλιού εντολών και ελέγχου τους. Οι δημοφιλείς υπηρεσίες Web που λειτουργούν ως μηχανισμός εξάτμισης ενδέχεται να παρέχουν σημαντική κάλυψη, λόγω της πιθανότητας οι κεντρικοί υπολογιστές εντός ενός δικτύου να επικοινωνούν ήδη μαζί τους πριν από την παραβίαση. Ενδέχεται επίσης να υπάρχουν ήδη κανόνες τείχους προστασίας που επιτρέπουν την κυκλοφορία προς αυτές τις υπηρεσίες.
- Οι πάροχοι υπηρεσιών Web χρησιμοποιούν επίσης συνήθως κρυπτογράφηση SSL/TLS, παρέχοντας στους εχθρούς ένα επιπλέον επίπεδο προστασίας.

Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τ

Ε: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; Α: Sysmon ή PFSenseFirewallEvents

Ε: Ποιος από τους δύο πίνακες δεδομένων παρέχει πληροφορίες σχετικά με τον αριθμό των μεταφερθέντων byte; Α: PFSenseFirewallEvents

Ε: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο; Α: Βασίζεται σε όγκο

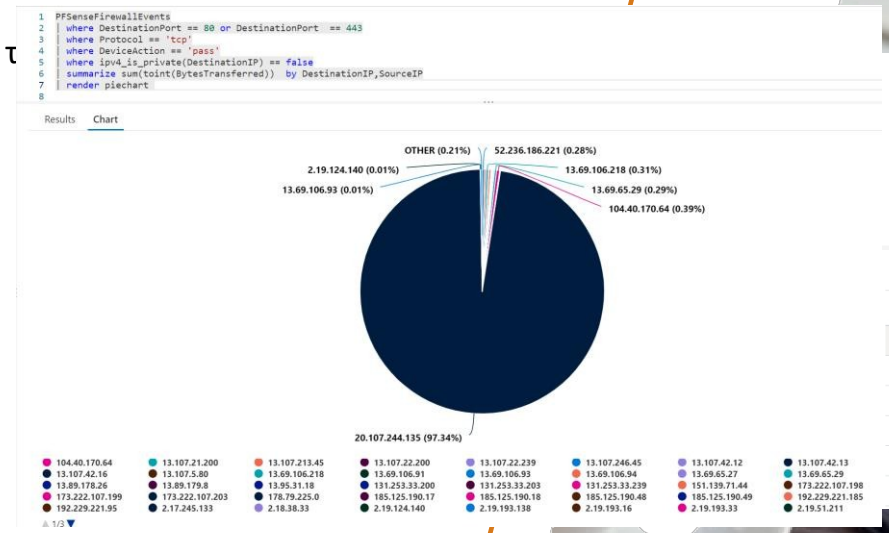
Ε: Ποια λειτουργία του SIEM είναι σημαντική για τις ανιχνεύσεις βάσει όγκου; Α: Συγκέντρωση συμβάντων (σύνοψη)

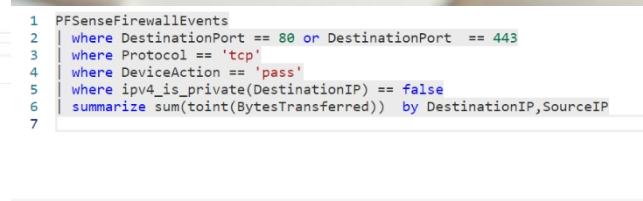
Ε: Ποιες στήλες είναι σημαντικές ώστε να τις χρησιμοποιήσουμε ως φίλτρα; Α: Οι στήλες DestinationPort, Protocol, DeviceAction και Destination IP πρέπει να είναι δημόσιες

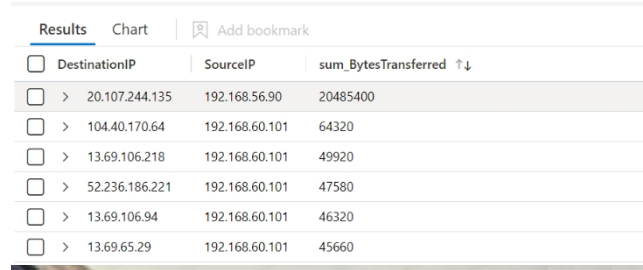
Ε: Ποιες στήλες είναι σημαντικές για τη συγκέντρωση; Α: SourceIP, DestinationIP, BytesTransferred

Ε: Πώς πρέπει να συγκεντρώσουμε τα αποτελέσματα; Α: Αθροίζοντας τα BytesTransferred ανά IP προορισμού και πηγής

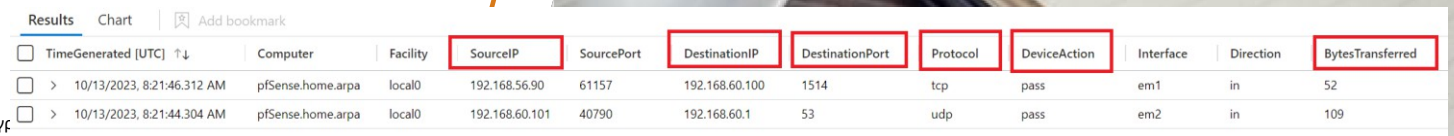
Ε (ΜΠΟΝΟΥΣ): Είναι καλύτερο να εμφανίζονται τα συγκεντρωτικά αποτελέσματα ως δεδομένα ή ως γρ







DestinationIP	SourceIP	sum_BytesTransferred
20.107.244.135	192.168.56.90	20485400
104.40.170.64	192.168.60.101	64320
13.69.106.218	192.168.60.101	49920
52.236.186.221	192.168.60.101	47580
13.69.106.94	192.168.60.101	46320
13.69.65.29	192.168.60.101	45660



TimeGenerated [UTC]	Computer	Facility	SourceIP	SourcePort	DestinationIP	DestinationPort	Protocol	DeviceAction	Interface	Direction	BytesTransferred
10/13/2023, 8:21:46.312 AM	pfSense.home.arpa	local0	192.168.56.90	61157	192.168.60.100	1514	tcp	pass	em1	in	52
10/13/2023, 8:21:44.304 AM	pfSense.home.arpa	local0	192.168.60.101	40790	192.168.60.1	53	udp	pass	em2	in	109

ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Εντοπισμός λογαριασμού: Λογαριασμός τομέα

- Ανακάλυψη λογαριασμών: Λογαριασμός τομέα
  - Οι εχθροί ενδέχεται να προσπαθήσουν να αποκτήσουν μια λίστα λογαριασμών τομέα. Αυτές οι πληροφορίες μπορούν να βοηθήσουν τους εχθρούς να προσδιορίσουν ποιοι λογαριασμοί τομέα υπάρχουν, ώστε να διευκολύνουν τις επακόλουθες ενέργειές τους, όπως η στόχευση συγκεκριμένων λογαριασμών που διαθέτουν συγκεκριμένα προνόμια.
  - Εντοπίζει έγκυρα ονόματα χρήστη μέσω αναζήτησης με τη μέθοδο της «brute force», δοκιμάζοντας πιθανά ονόματα χρήστη σε μια υπηρεσία Kerberos. Όταν ζητείται ένα μη έγκυρο όνομα χρήστη, ο διακομιστής θα απαντήσει χρησιμοποιώντας τον κωδικό σφάλματος Kerberos KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN, επιτρέποντάς μας να προσδιορίσουμε ότι το όνομα χρήστη ήταν μη έγκυρο. Τα έγκυρα ονόματα χρήστη θα προκαλέσουν είτε το TGT σε μια απόκριση AS-REP είτε το σφάλμα KRB5KDC_ERR_PREAUTH_REQUIRED, σηματοδοτώντας ότι ο χρήστης πρέπει να εκτελέσει προ-αυθεντικοποίηση
  - Εργαλεία: krbrute, nmap, crackmapexec

- Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τη λογική πίσω από την ανίχνευση – Επίπεδο τερματικού

Ε: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; Α: SecurityEvents

Ε: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων SecurityEvents;
Α: 4768 - Ζητήθηκε ένα εισιτήριο πιστοποίησης Kerberos (TGT).

Ε: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο δεδομένων; Α: Σε όγκο δεδομένων

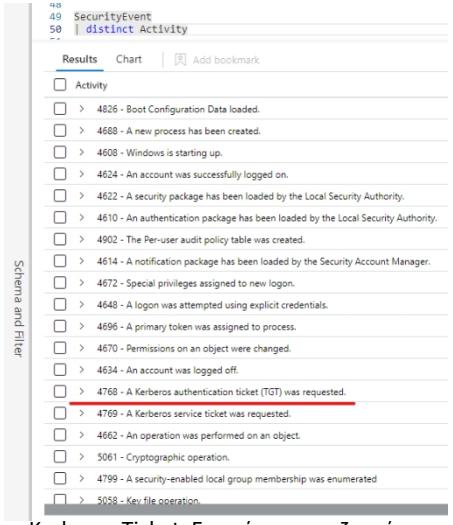
Ε: Ποια λειτουργία του SIEM είναι σημαντική για τις ανιχνεύσεις βάσει όγκου; Α: Συγκέντρωση συμβάντων (σύνοψη)

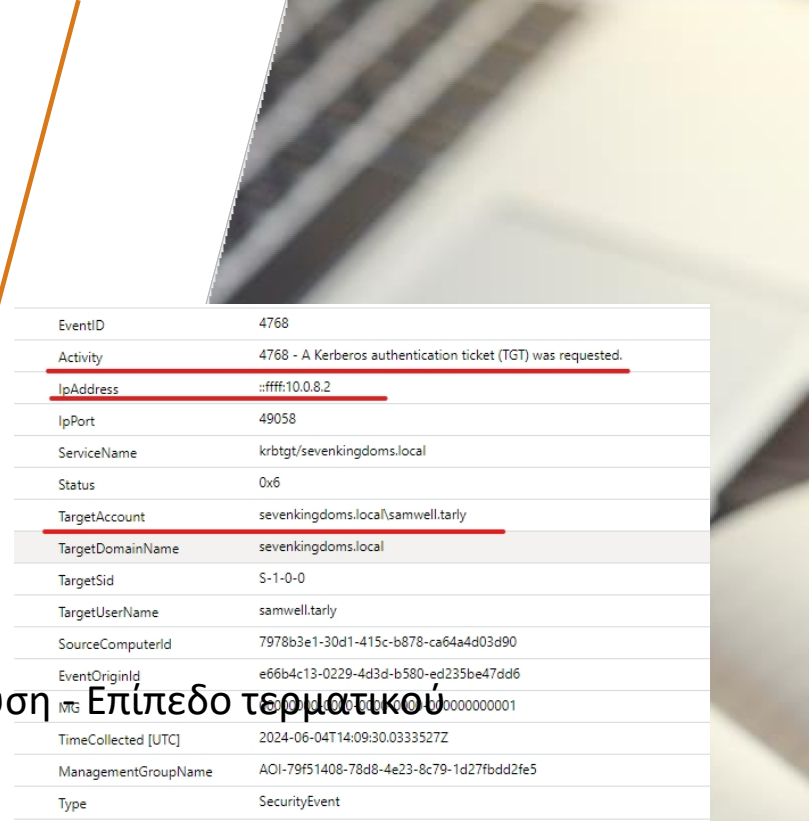
Ε: Ποιες στήλες είναι σημαντικές ώστε να τις χρησιμοποιήσουμε ως φίλτρα; Α: Δραστηριότητα

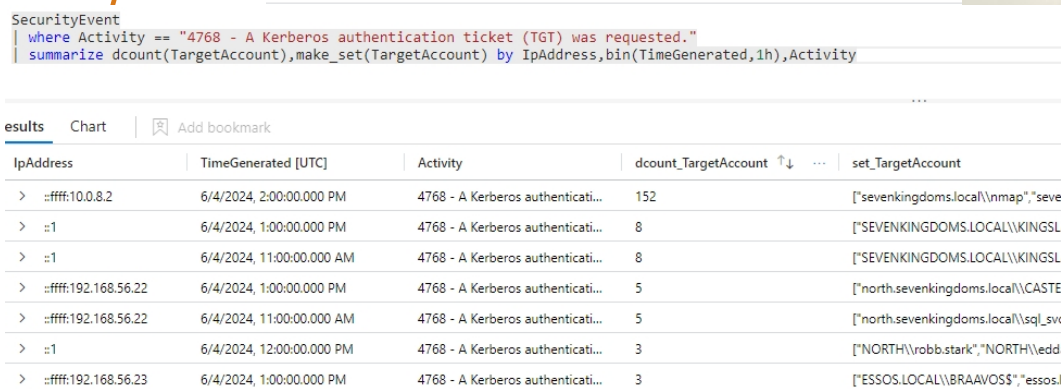
Ε: Ποιες στήλες είναι σημαντικές για τη συγκέντρωση;
Α: IpAddress, TargetAccount, TimeGenerated

Ε: Πώς πρέπει να συγκεντρώσουμε τα αποτελέσματα;
Α: Το πεδίο IP Address προέρχεται από το σημείο από όπου προέρχονται τα αιτήματα Kerberos Ticket. Επομένως, αναζητούμε διευθύνσεις IP με αιτήματα Kerberos Ticket για πολλούς διαφορετικούς λογαριασμούς.

Ε (ΕΠΙΠΛΕΟΝ): Είναι καλύτερο να εμφανίζονται τα αποτελέσματα της συγκέντρωσης ως δεδομένα ή ως γραφήματα; Α: Γραφήματα (render columnchart)







ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Brute Force: Password Spraying

Brute Force: Password Spraying

- Οι εχθροί μπορεί να χρησιμοποιήσουν έναν ή λίγους κωδικούς πρόσβασης που χρησιμοποιούνται συχνά σε πολλούς διαφορετικούς λογαριασμούς, προκειμένου να αποκτήσουν έγκυρα διαπιστευτήρια λογαριασμού. Το password spraying χρησιμοποιεί έναν κωδικό πρόσβασης (π.χ. «Password01») ή μια μικρή λίστα συχνά χρησιμοποιούμενων κωδικών πρόσβασης, οι οποίοι ενδέχεται να ανταποκρίνονται στην πολιτική πολυπλοκότητας του τομέα. Γίνονται προσπάθειες σύνδεσης με αυτόν τον κωδικό πρόσβασης σε **πολλούς διαφορετικούς λογαριασμούς** σε ένα δίκτυο, προκειμένου να αποφευχθεί ο αποκλεισμός λογαριασμών που θα συνέβαινε κανονικά κατά τη χρήση της μεθόδου brute force σε έναν μόνο λογαριασμό με πολλούς κωδικούς πρόσβασης.

Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τη λογική πίσω από την αν

E: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες;

A: SecurityEvents

E: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων SecurityEvents; A:

4625 - Αποτυχία σύνδεσης λογαριασμού.

E: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο;

A: Βασίζεται στον όγκο

E: Ποια λειτουργία του SIEM είναι σημαντική για τις ανιχνεύσεις βάσει όγκου; A:

Συγκέντρωση συμβάντων (σύνοψη)

E: Ποιες στήλες είναι σημαντικές ώστε να τις χρησιμοποιήσουμε ως φίλτρα;

A: Καμία, στην πραγματικότητα. Φιλτράροντας για το EventID 4625, έχουμε το σύνολο δεδομένων που θέλουμε να διερευνήσουμε.

E: Ποιες στήλες είναι σημαντικές για τη συγκέντρωση; A:

IPAddress, Account.

E: Πώς πρέπει να συγκεντρώσουμε τα αποτελέσματα;

A: Το πεδίο «Διεύθυνση IP» αφορά την τοποθεσία από την οποία πραγματοποιούνται οι αποτυχημένες προσπάθειες σύνδεσης. Επομένως, αναζητούμε διευθύνσεις IP με πολλαπλές αποτυχημένες προσπάθειες σύνδεσης σε διαφορετικούς λογαριασμούς. *

Ε (ΜΠΟΝΟΥΣ): Είναι καλύτερο να εμφανίζονται τα συγκεντρωτικά αποτελέσματα

ως δεδομένα ή ως γραφήματα; A: Γραφήματα

*Καταγραφή ελέγχου ταυτότητας τομέα:

Ορισμένα πρωτόκολλα, όπως το NTLM, απαιτούν επιπλέον διαμόρφωση για να παρέχουν τη διεύθυνση IP προέλευσης της αποτυχημένης πιστοποίησης

```
SecurityEvent
| distinct Activity
```

Results | Chart | Add bookmark

Activity
1100 - The event logging service has shut down.
4608 - Windows is starting up.
4610 - An authentication package has been loaded by the Local Security Authority.
4611 - A trusted logon process has been registered with the Local Security Authority.
4614 - A notification package has been loaded by the Security Account Manager.
4616 - The system time was changed.
4622 - A security package has been loaded by the Local Security Authority.
4624 - An account was successfully logged on.
4625 - An account failed to log on.
4634 - An account was logged off.
4647 - User initiated logoff.
4648 - A logon was attempted using explicit credentials.
4662 - An operation was performed on an object.
4670 - Permissions on an object were changed.
4672 - Special privileges assigned to new logon.
4675 - SIDs were filtered.
4688 - A new process has been created.


```
SecurityEvent
| where Activity == '4625 - An account failed to log on.'
| summarize dcount(Account) by IpAddress
```

Results | Chart | Add bookmark

IpAddress	dcount_Account
192.168.56.90	4
127.0.0.1	2
-	4
::1	2

```
SecurityEvent
| where Activity == "4625 - An account failed to log on."
| summarize dcount(TargetAccount),make_set(TargetAccount) by IpAddress,bin(TimeGenerated,1h),Activity
```

esults | Chart | Add bookmark

IpAddress	TimeGenerated [UTC]	Activity	dcount_TargetAccount	set_TargetAccount
10.0.8.2	6/4/2024, 2:00:00.000 PM	4625 - An account failed to log on.	9	["north.sevenkingdoms.local\\
-	6/4/2024, 1:00:00.000 PM	4625 - An account failed to log on.	1	["NORTH\\robb.stark"]
10.0.8.2	6/4/2024, 1:00:00.000 PM	4625 - An account failed to log on.	1	["\\"]
-	6/4/2024, 11:00:00.000 AM	4625 - An account failed to log on.	2	["-\\-","NORTH\\robb.stark"]

ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Στοιχειό λογισμικού διακομιστή: Web Shell

- Συστατικό λογισμικού διακομιστή: Web Shell
  - Ένα Web shell είναι ένα σενάριο ιστού που **τοποθετείται** σε έναν ελεύθερα προσβάσιμο διακομιστή ιστού, ώστε να επιτρέπει σε έναν εισβολέα να αποκτήσει πρόσβαση στον διακομιστή ιστού ως πύλη εισόδου σε ένα δίκτυο. Ένα Web shell **μπορεί να παρέχει ένα σύνολο λειτουργιών προς εκτέλεση** ή **μια διεπαφή γραμμής εντολών** στο σύστημα που φιλοξενεί τον διακομιστή ιστού.
  - **Η παρακολούθηση αρχείων** μπορεί να χρησιμοποιηθεί για την ανίχνευση αλλαγών σε αρχεία στον **κατάλογο Web ενός διακομιστή Web** που δεν αντιστοιχούν σε ενημερώσεις του περιεχομένου του διακομιστή Web και μπορεί να υποδηλώνουν την εγκατάσταση ενός σενάριου Web shell.

- Βήματα που πρέπει να ακολουθηθούν για τη δημιουργία της λογικής πίσω από την ανίχνευση - Δημιουργία αρχείου

E: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: Sysmon

E: Τι είδους συμβάντα θέλουμε να εξάγουμε από τον πίνακα δεδομένων Sysmon; A: Δημιουργία αρχείου

E: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο; A: Βασίζεται σε συμβάντα

E: Ποιες στήλες είναι σημαντικές ώστε να τις χρησιμοποιήσουμε ως φίλτρα; A: Rendered Description, file_name
Η στήλη file_name εμφανίζει το αρχείο που δημιουργήθηκε με την πλήρη διαδρομή.

E: Τι φίλτρο θα βάλω στις σημαντικές στήλες:
A: 1. Η περιγραφή εμφάνισης ισούται με «Δημιουργήθηκε αρχείο»
2. Το file_name ξεκινά με {Web Server Directory}
3. Το file_name τελειώνει με {Webshell file extension}
(Συμβουλή: Συνήθεις επεκτάσεις αρχείων Webshell: php, asp, aspx, cfm, jsp)

```
Sysmon
| where RenderedDescription == "File created"
| where file_name startswith "C:\\xampp\\"
| where file_name endswith ".asp" or file_name endswith ".aspx" or file_name endswith ".cfm" or file_name endswith ".jsp" or file_name endswith ".php"
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	Source	EventID	Computer	UserName	RenderedDescription
6/4/2024, 10:50:18.369 PM	Microsoft-Windows-Sysmon	11	castelblack.north.sevenkingdo...	NT AUTHORITY\SYSTEM	File created

TimeGenerated [UTC]	2024-06-04T22:50:18.3691025Z
Source	Microsoft-Windows-Sysmon
EventID	11
Computer	castelblack.north.sevenkingdoms.local
UserName	NT AUTHORITY\SYSTEM
RenderedDescription	File created
event_creation_time	2024-06-04T22:50:18.3660000Z
process_guid	{35604ab1-1752-665f-5000-000000009f00}
process_id	3404
process_path	C:\xampp\tomcat\bin\tomcat8.exe
file_name	C:\xampp\tomcat\webapps\cmd\cmd.jsp
file_creation_time	2024-06-04T22:50:18.3660000Z

```
1  Sysmon
2  | distinct RenderedDescription
```

Results | Chart | Add bookmark

- RenderedDescription
- Sysmon config state changed
- File stream created
- Sysmon service state changed
- Driver loaded
- CreateRemoteThread detected
- Pipe Created
- Registry object added or deleted
- Registry value set
- Dns query
- Pipe Connected
- Process Create
- File created
- Image loaded
- Network connection detected
- Process accessed

*Συμβουλή για τη σύνταξη KQL: Αντικαταστήστε το \ με \\, καθώς η κάθετος χρησιμοποιείται για την διαφυγή χαρακτήρων

ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Στοιχειό λογισμικού διακομιστή: Web Shell

- Συστατικό λογισμικού διακομιστή: Web Shell
  - Ένα Web shell είναι ένα σενάριο Web που **τοποθετείται** σε έναν ανοιχτά προσβάσιμο διακομιστή Web για να επιτρέπει σε έναν εχθρό να έχει πρόσβαση στον διακομιστή Web ως πύλη εισόδου σε ένα δίκτυο. Ένα Web shell **μπορεί να παρέχει ένα σύνολο λειτουργιών προς εκτέλεση** ή **μια διεπαφή γραμμής εντολών** στο σύστημα που φιλοξενεί τον διακομιστή Web.
  - **Η παρακολούθηση διεργασιών** μπορεί να χρησιμοποιηθεί για τον εντοπισμό διακομιστών ιστού που εκτελούν ύποπτες ενέργειες, όπως η εκκίνηση του cmd.exe ή η πρόσβαση σε αρχεία που δεν βρίσκονται στον κατάλογο του ιστού.
  - Ένα web shell είναι ένα σενάριο ιστού που τοποθετείται σε έναν ανοιχτά προσβάσιμο διακομιστή ιστού για να επιτρέπει σε έναν εχθρό να χρησιμοποιήσει τον διακομιστή ως πύλη σε ένα δίκτυο. Καθώς λειτουργεί το shell, **θα εκδίδονται εντολές από το εσωτερικό της εφαρμογής ιστού προς το ευρύτερο λειτουργικό σύστημα του διακομιστή**.

- Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τη λογική πίσω από την ανίχνευση - Δημιουργία διεργασίας

E: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες;
A: Sysmon

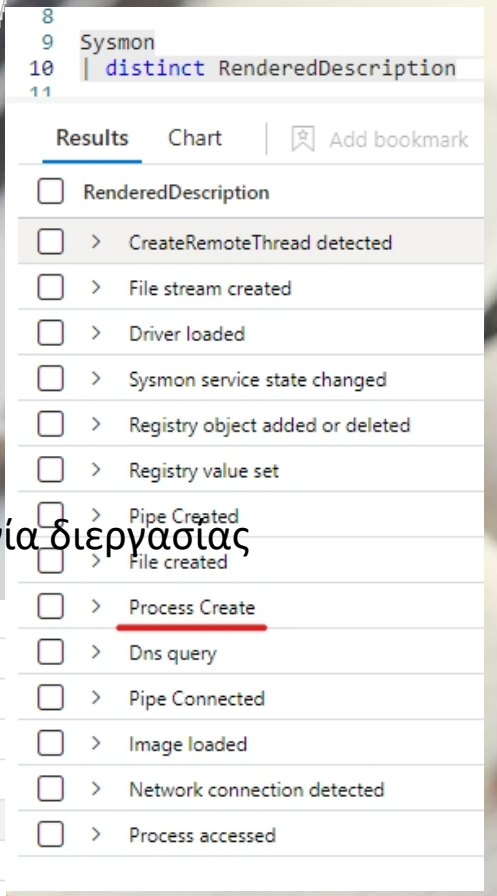
E: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων του Sysmon; A: Δημιουργία διεργασίας

E: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο δεδομένων; A: Βασίζεται σε συμβάντα

E: Ποιες στήλες είναι σημαντικές ώστε να τις χρησιμοποιήσουμε ως φίλτρα;
A: Rendered Description, process_parent_command_line, process_command_line Οι διεργασίες γραμμής εντολών που εκτελούνται από διεργασίες διακομιστή ιστού αποτελούν ισχυρό δείκτη εκτέλεσης Web Shell.

E: Τι φίλτρο θα βάλω στις σημαντικές στήλες:
A: 1. Η Περιγραφή που εμφανίζεται ισούται με «Δημιουργία διεργασίας»
2. Το process_parent_command_line περιέχει κοινές διεργασίες διακομιστή ιστού
3. Το process_command_line περιέχει κοινές διεργασίες γραμμής εντολών
(Συμβουλή: Κοινές διεργασίες διακομιστή ιστού: w3wp.exe, httpd.exe, tomcat.exe, nginx.exe) (Συμβουλή 2: Κοινές διεργασίες γραμμής εντολών: cmd, powershell, netstat, systeminfo, ipconfig, whoami κ.λπ.)

*Συμβουλή για τη σύνταξη KQL: Αντικαταστήστε το \ με \\, καθώς η κάθετος χρησιμοποιείται ως χαρακτήρας διαφυγής.



file_version	10.0.17763.1 (WinBuild.160101.0800)
file_description	TCP/IP Netstat Command
file_product	Microsoft® Windows® Operating System
file_company	Microsoft Corporation
file_name	netstat.exe
process_command_line	netstat -abno
file_directory	C:\xampp\tomcat\bin\
user_name	NT AUTHORITY\SYSTEM
user_logon_guid	{35604ab1-79b4-665f-e703-000000000000}
user_logon_id	0x3e7
user_session_id	0
process_integrity_level	System
process_parent_guid	{35604ab1-1752-665f-5000-000000009f00}
process_parent_id	3404
process_parent_path	C:\xampp\tomcat\bin\tomcat8.exe
process_parent_command_line	C:\xampp\tomcat\bin\tomcat8.exe //RS//Tomcat

ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Στοιχειό λογισμικού διακομιστή: Web Shell

- Συστατικό λογισμικού διακομιστή: Web Shell
  - Ένα Web shell είναι ένα σενάριο Web που **τοποθετείται** σε έναν ανοιχτά προσβάσιμο διακομιστή Web για να επιτρέπει σε έναν εχθρό να έχει πρόσβαση στον διακομιστή Web ως πύλη εισόδου σε ένα δίκτυο. Ένα Web shell **μπορεί να παρέχει ένα σύνολο λειτουργιών προς εκτέλεση** ή **μια διεπαφή γραμμής εντολών** στο σύστημα που φιλοξενεί τον διακομιστή Web.
  - Παρακολούθηση και ανάλυση **των προτύπων κυκλοφορίας και έλεγχος πακέτων** που σχετίζονται με πρωτόκολλα τα οποία δεν συμμορφώνονται με τα αναμενόμενα πρότυπα πρωτοκόλλου και τις ροές κυκλοφορίας (π.χ. παρεμβαλλόμενα πακέτα που δεν ανήκουν σε καθιερωμένες ροές, περιττές ή ανώμαλες ροές κυκλοφορίας, ανώμαλη σύνταξη ή δομή).

- Βήματα που πρέπει να ακολουθηθούν για τη δημιουργία της λογικής πίσω από Περιεχόμενο

E: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: Suricata

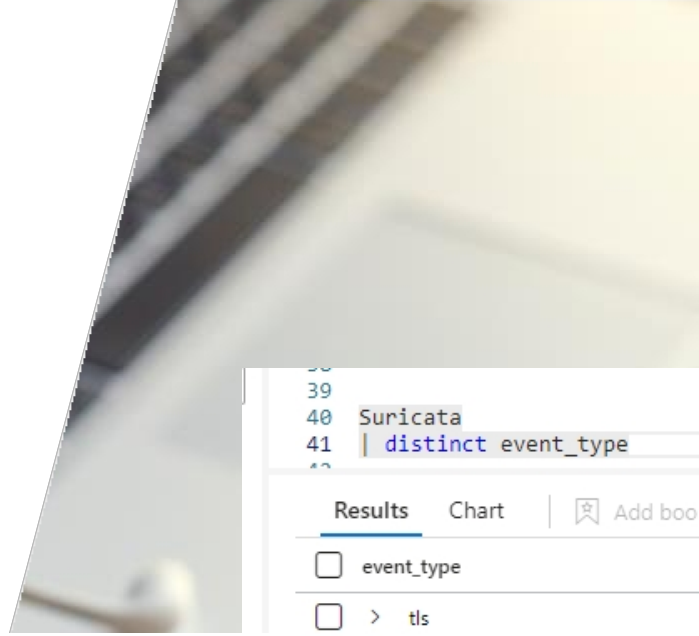
E: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων Sysmon;
A: event_type > http

E: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο; A:
Βασίζεται σε συμβάντα

E: Ποιο ένθετο πεδίο είναι σημαντικό μέσα στο στοιχείο http;
A: url
Ορισμένα Web shells λειτουργούν λαμβάνοντας τις ύποπτες εντολές ως παραμέτρους στη διεύθυνση UR

E: Τι φίλτρο θα βάλω στις σημαντικές στήλες: A: 1.
event_type ισούται με 'http'
2. url περιέχει οποιαδήποτε από τις ύποπτες εντολές

E: Έδωσε το Suricata κάποια ειδοποίηση σχετικά με αυτή τη δραστηριότητα;
A: Suricata | όπου event_type == 'alert' και app_proto == 'http'



```
39
40 Suricata
41 | distinct event_type
```

Results | Chart | Add boo

event_type
tls
smb
dns
krb5
fileinfo
http
alert
rdp

http	{"hostname":"192.168.56.22","http_port":8081,"url":"/cmd/c
hostname	192.168.56.22
http_content_type	text/html
http_port	8081
http_user_agent	Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firef
url	/cmd/cmd.jsp?cmd=dir
in_iface	em1
pkt_src	wire/pcap
proto	TCP
src_ip	10.0.8.2
src_port	59106

Copy
Include "/cmd/cmd.jsp?cmd=dir"
Exclude "/cmd/cmd.jsp?cmd=dir"
Extend column

```
1 Suricata
2 | where event_type == 'http'
3 | extend url_ = tostring(http.url)
4 | where url_ has_any ('systeminfo','whoami','netstat','hostname')
```

Results | Chart | Add bookmark

TimeGenerated [UTC]	url_	Computer	RawData	Type
6/4/2024, 10:58:23.000 PM	/cmd/cmd.jsp?cmd=netstat+-abno	goad-VirtualBox	{"timestamp":"2024-06-04T22:5...	Suricata_CL
6/4/2024, 10:53:46.000 PM	/cmd/cmd.jsp?cmd=systeminfo	goad-VirtualBox	{"timestamp":"2024-06-04T22:5...	Suricata_CL
6/4/2024, 10:53:27.000 PM	/cmd/cmd.jsp?cmd=hostname	goad-VirtualBox	{"timestamp":"2024-06-04T22:5...	Suricata_CL
6/4/2024, 10:53:03.000 PM	/cmd/cmd.jsp?cmd=whoami+%2Fall	goad-VirtualBox	{"timestamp":"2024-06-04T22:5...	Suricata_CL
6/4/2024, 10:52:41.000 PM	/cmd/cmd.jsp?cmd=whoami+%2Fall	goad-VirtualBox	{"timestamp":"2024-06-04T22:5...	Suricata_CL

ΕΡΓΑΣΤΗΡΙΟ

Παραδείγματα - Στοιχεία λογισμικού διακομιστή: Web Shell

- Κλοπή ή πλαστογράφηση εισιτηρίων Kerberos: AS-REP Roasting

  Οι εισβολείς ενδέχεται να αποκαλύψουν τα διαπιστευτήρια λογαριασμών στους οποίους έχει απενεργοποιηθεί **η προ-αυθεντικοποίηση Kerberos,** μέσω της παραβίασης κωδικών πρόσβασης στα μηνύματα Kerberos. Για κάθε λογαριασμό που εντοπίζεται χωρίς προαυθεντικοποίηση, ένας εχθρός μπορεί να στείλει ένα μήνυμα AS-REQ χωρίς την κρυπτογραφημένη χρονική σήμανση και **να λάβει ένα μήνυμα AS-REP με δεδομένα TGT τα οποία ενδέχεται να είναι κρυπτογραφημένα με έναν μη ασφαλή αλγόριθμο όπως το RC4**. Τα ανακτηθέντα κρυπτογραφημένα δεδομένα ενδέχεται να είναι ευάλωτα σε επιθέσεις παραβίασης κωδικών πρόσβασης εκτός σύνδεσης, παρόμοια με το Kerberoasting, και να εκθέτουν διαπιστευτήρια σε μορφή απλού κειμένου. Ένας λογαριασμός που έχει καταχωρηθεί σε έναν τομέα, με ή χωρίς ειδικά δικαιώματα, μπορεί να χρησιμοποιηθεί καταχρηστικά για την καταγραφή όλων των λογαριασμών του τομέα στους οποίους έχει απενεργοποιηθεί η προ-αυθεντικοποίηση, χρησιμοποιώντας εργαλεία των Windows όπως το PowerShell με ένα φίλτρο LDAP**. Εναλλακτικά, ο εισβολέας μπορεί να στείλει ένα μήνυμα AS-REQ για κάθε χρήστη. Εάν ο DC απαντήσει χωρίς σφάλματα, ο λογαριασμός δεν απαιτεί προ-αυθεντικοποίηση και το μήνυμα AS-REP θα περιέχει ήδη τα κρυπτογραφημένα δεδομένα.**

- Βήματα που πρέπει να ακολουθηθούν για τη δημιουργία της λογικής πίσω από την ανίχνευση

  Ε: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; Α: Το Suricata

  Ε: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων Sysmon;
  Α: event_type > krb5

  Ε: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκο; Α: Βασίζεται σε συμβάντα

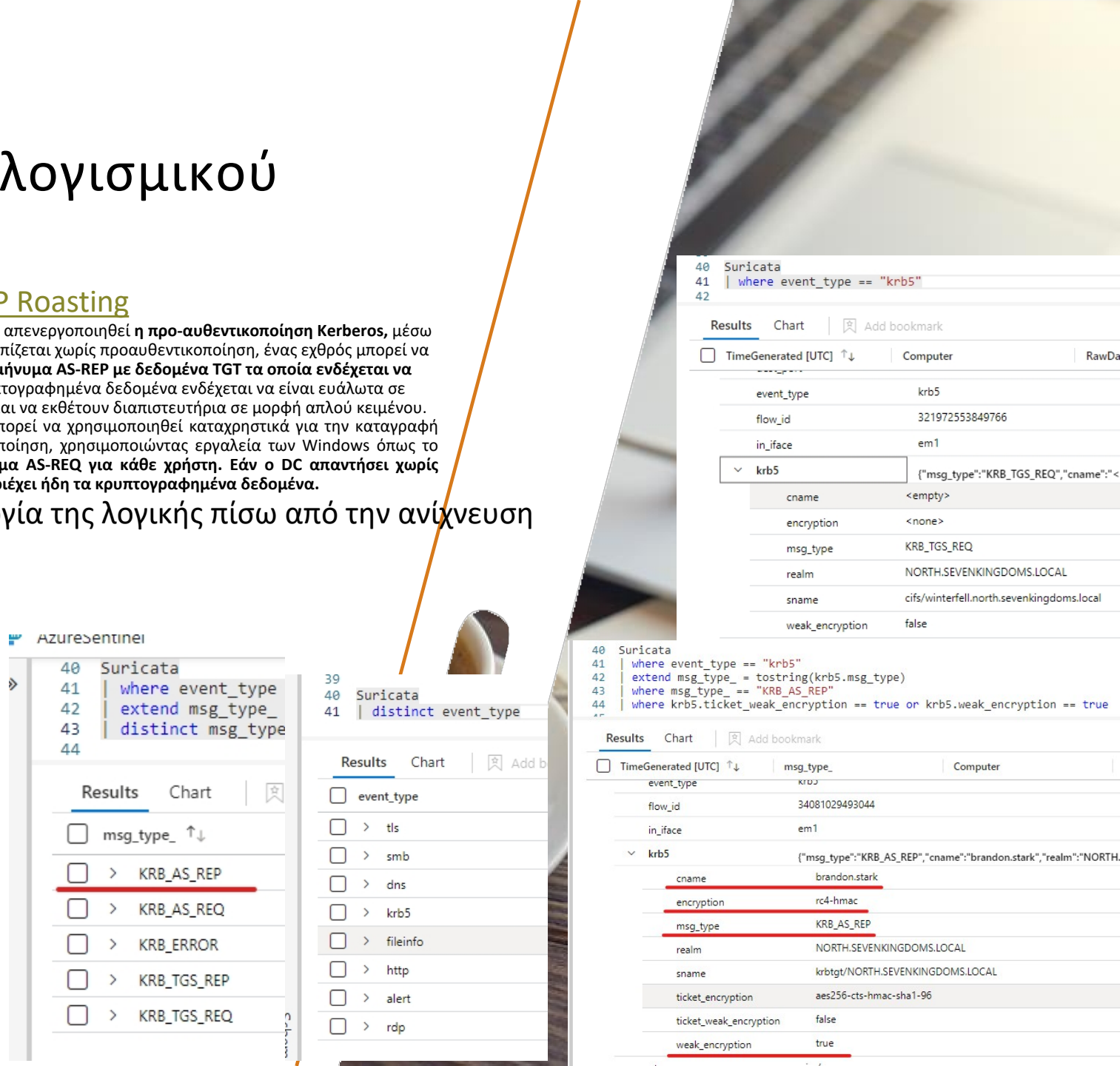
  Ε: Ποιο ένθετο πεδίο είναι σημαντικό μέσα στο στοιχείο krb5;
  Α: msg_type, weak_encryption, ticket_weak_encryption

  Ε: Ποιες στήλες είναι σημαντικές ώστε να τις χρησιμοποιήσουμε ως φίλτρα;
  Α: event_type, msg_type_ , weak_encryption_, ticket_weak_encryption_

  Ε: Τι φίλτρο θα βάλω στις σημαντικές στήλες:
  Α: 1. event_type = krb5
  2. ticket_weak_encryption_ = true ή weak_encryption_ = true

  Ε: Ποιος ήταν ο λογαριασμός που αποκαλύφθηκε και ήταν ευάλωτος σε επίθεση AS-REP Roasting; Α: Η ένθετη στήλη cname > brandon.stark

  Ε: Ποια είναι η στήλη που εμφανίζει την προέλευση της επίθεσης;
  Α: src_ip > 10.0.8.2



Ευχαριστώ για την προσοχή σας

Παρουσίαση από:

Χρήστος Λαζαρίδης
(Συντονιστής)

CyberSecPro