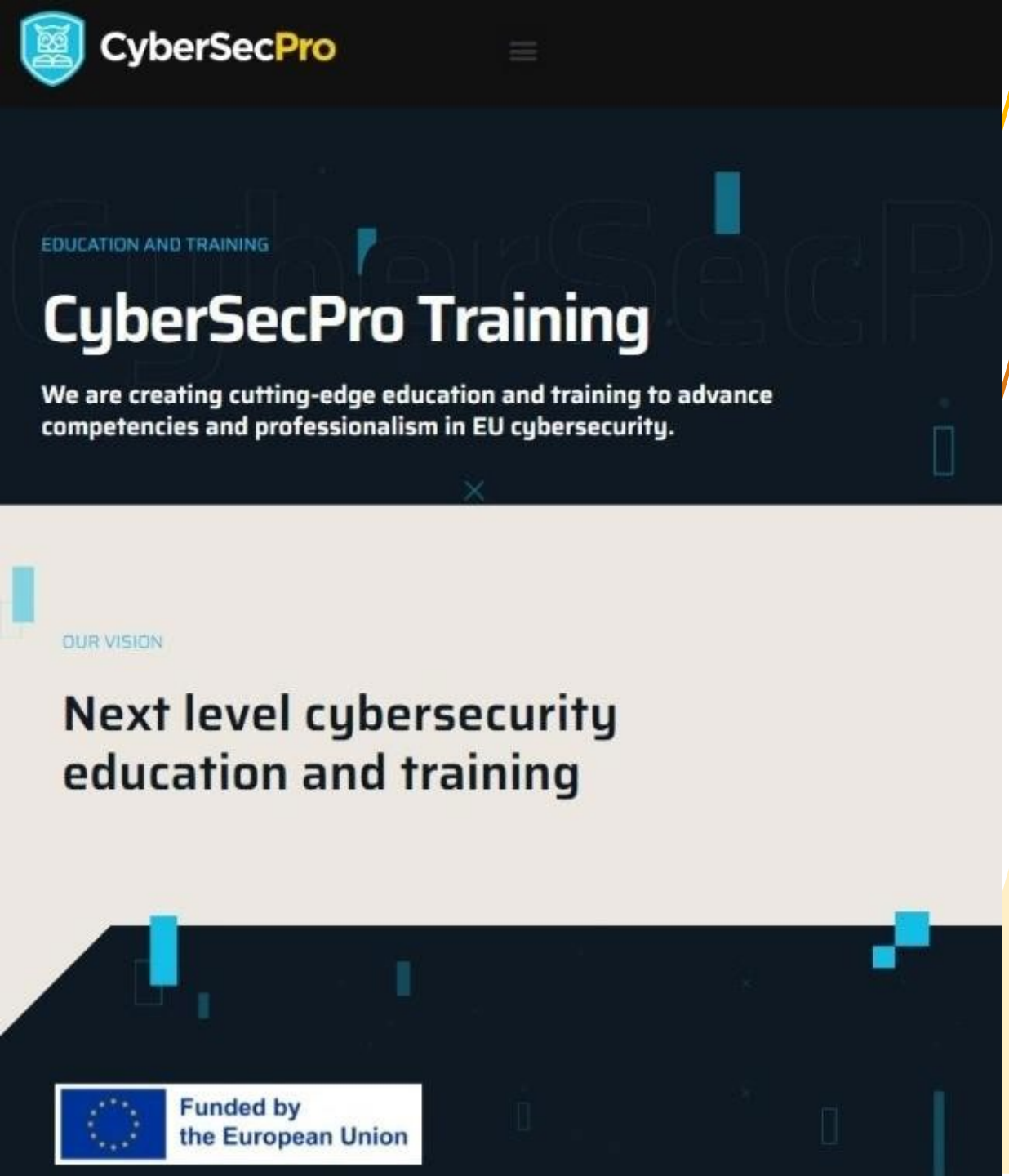


Μηχανική Ανίχνευσης για Υποδομές Πληροφορικής Υγείας

CSP011_W_H

CHRISTOS LAZARIDIS
FOCAL POINT

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

Εισαγωγή στη Μηχανική Ανίχνευσης στην Ασφάλεια Υγείας

Στόχος: Εξερεύνηση του ρόλου της μηχανικής ανίχνευσης στην προστασία των συστημάτων πληροφοριών υγείας.

Γιατί:

- Τα ισχυρά μέτρα ασφαλείας είναι κρίσιμα για την προστασία ευαίσθητων δεδομένων ασθενών στις ψηφιακές υπηρεσίες υγείας.
- Οι αυξημένες δυναμικές κυβερνοαπειλές θέτουν κινδύνους για την ασφάλεια και την ιδιωτικότητα των ασθενών.
- Η μηχανική ανίχνευσης εντοπίζει, παρακολουθεί και μετριάζει αποτελεσματικά τις κυβερνοαπειλές και προσαρμόζεται στις δυναμικές απειλές.

Υπηρεσίες υγειονομικής περίθαλψης που μπορούν να παρακολουθούνται

Συνδεδεμένες Υπηρεσίες Υγειονομικής Περίθαλψης:

- **Πύλες Ιατρού-Ασθενή:** Πλατφόρμες για επικοινωνία, προγραμματισμό ραντεβού και πρόσβαση σε ιατρικά αρχεία.
- **Χειρισμός Ιατρικού Εξοπλισμού εξ Αποστάσεως:** Παρακολούθηση και έλεγχος ιατρικών συσκευών που χρησιμοποιούνται εξ αποστάσεως για τη φροντίδα των ασθενών.
- **Κρίσιμο για την τηλεϊατρική και τις εξ αποστάσεως διαγνώσεις.**
- **Συστήματα Ηλεκτρονικών Ιατρικών Αρχείων (EHR):** Κεντρική αποθήκευση και σημείο πρόσβασης για ιατρικά δεδομένα ασθενών, διασυνδεδεμένα με AD για αυστηρούς ελέγχους πρόσβασης.

Αυτές οι υπηρεσίες είναι ζωτικής σημασίας για την παροχή σύγχρονης υγειονομικής περίθαλψης, αλλά είναι ευάλωτες σε κυβερνοεπιθέσεις.

Ενσωμάτωση Υπηρεσιών Υγειονομικής Περίθαλψης με το Active Directory

- Οι ψηφιακές υπηρεσίες υγειονομικής περίθαλψης χρησιμοποιούν το Active Directory (AD) για τη διαχείριση ταυτότητας και τον έλεγχο πρόσβασης.
- Οι ψηφιακές υπηρεσίες υγειονομικής περίθαλψης αναπτύσσονται σε περιβάλλοντα AD.
- Οι ευπάθειες στο AD μπορούν να θέσουν σε κίνδυνο την ασφάλεια των διασυνδεδεμένων υπηρεσιών υγειονομικής περίθαλψης.
- Η ασφάλεια των περιβαλλόντων AD είναι δύσκολη αλλά κρίσιμη για την προστασία των διασυνδεδεμένων εφαρμογών υγειονομικής περίθαλψης.

Εγγενείς ευπάθειες του AD που μπορούν μόνο να παρακολουθούνται και όχι να μετριάζονται

Steal or Forge Kerberos Tickets

Sub-techniques (4)

ID	Name
T1558.001	Golden Ticket
T1558.002	Silver Ticket
T1558.003	Kerberoasting
T1558.004	AS-REP Roasting

Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable Pass the Ticket. Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as "realms", there are three basic participants: client, service, and Key Distribution Center (KDC).[1] Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access.

Ο Ρόλος της Μηχανικής Ανίχνευσης στην Κυβερνοασφάλεια της Υγειονομικής Περίθαλψης

- Η μηχανική ανίχνευσης παρέχει ορατότητα στις επιθέσεις κατά των ψηφιακών περιουσιακών στοιχείων υγειονομικής περίθαλψης.

- Η παρακολούθηση των αλληλεπιδράσεων μεταξύ των συστημάτων υγειονομικής περίθαλψης και των περιβαλλόντων AD ανιχνεύει ύποπτες δραστηριότητες νωρίς.

- Οι συνεχείς ενημερώσεις στις στρατηγικές ανίχνευσης είναι κρίσιμες για την αντιμετώπιση των προηγμένων επίμονων απειλών (APTs), με εργαλεία όπως το Microsoft Sentinel ή άλλες λύσεις SIEM.

Active directory Detection Workshop

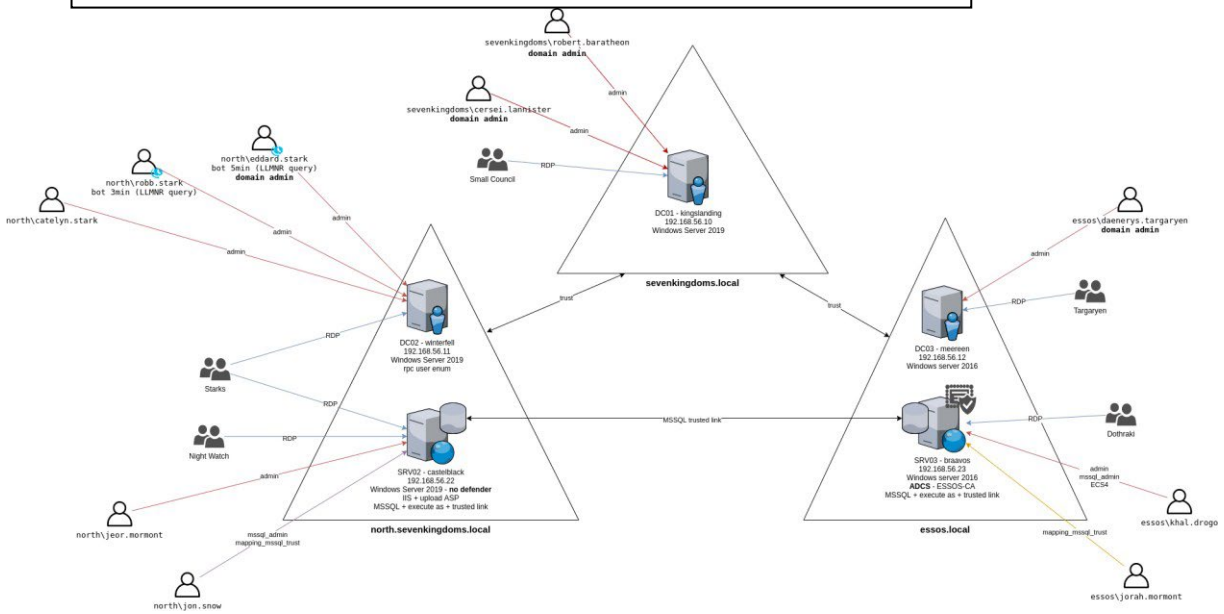
Workshop - Εισαγωγή στο εργαστηριακό περιβάλλον

Η αρχική ρύθμιση βασίζεται στο έργο ανοιχτού κώδικα GOAD

Game of Active Directory (GOAD)

3 Τομείς:

- sevenkingdoms – 1 Domain Controller (kingslanding)
- essos – 1 Domain Controller (meereen), 1 ADCS Server (braavos)
- north – 1 Domain Controller (winterfell), 1 IIS Server (castelblack)



WORKSHOP - Goad υποδομή

IP Address	Function	OS	Name	Domain
192.168.56.10	Windows Domain Controller	Windows Server 2019	dc01 - kingslanding	sevenkingdoms
192.168.56.11	Windows Domain Controller	Windows Server 2016	dc02 - winterfell	north.sevenkingdoms
192.168.56.12	Windows Domain Controller	Windows Server 2016	dc03 - meereen	essos
192.168.56.22	Web Server	Windows Server 2016	srv01 - castelblack	north.sevenkingdoms
192.168.56.23	ADCS Server	Windows Server 2016	srv02 - bravoos	essos
192.168.56.100	• Firewall • Intrusion Detection System - Suricata • Default Gateway • OpenVPN Server	PfSense	-	-

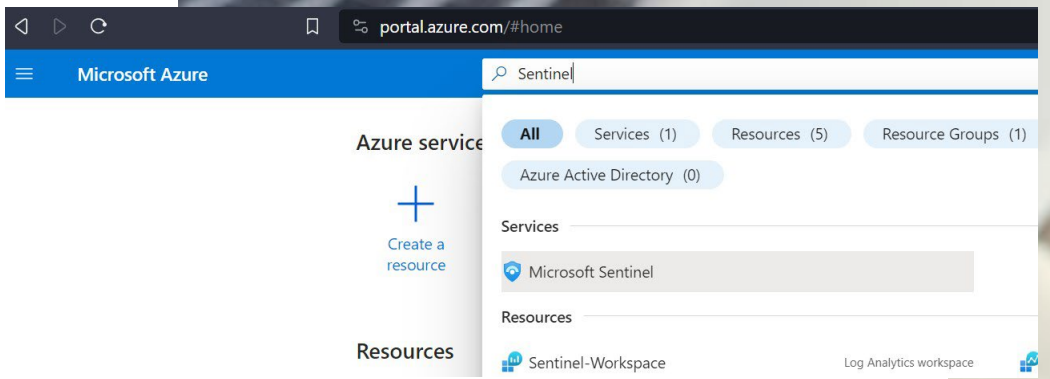
WORKSHOP

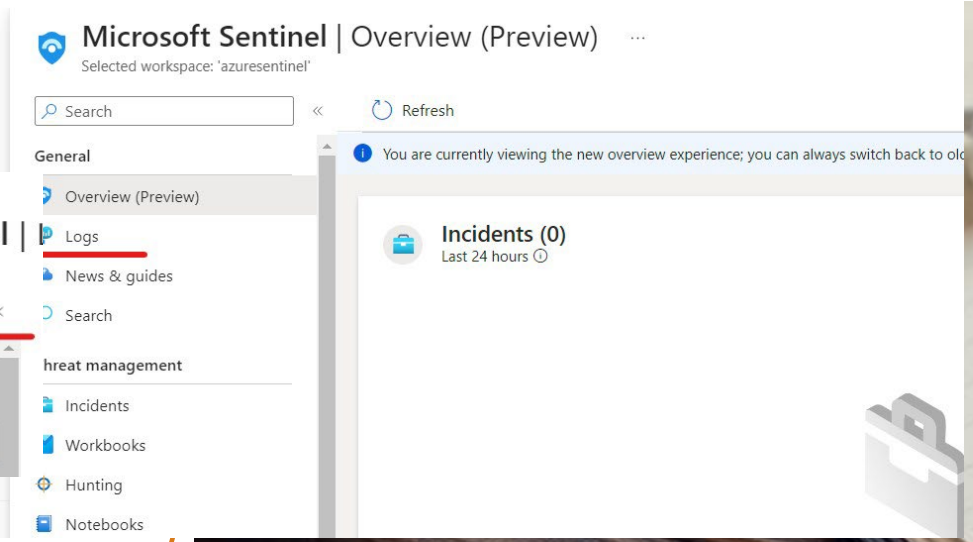
Πρόσβαση στο Azure Sentinel

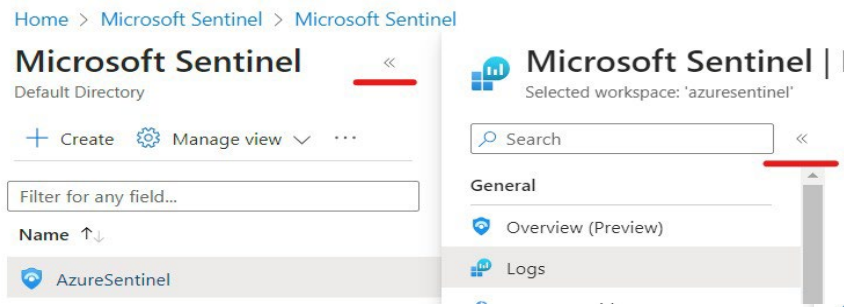
◦ Sentinel Πρόσβαση

◦ Ανοίξτε μια ιδιωτική καρτέλα ή ένα προφίλ επισκέπτη στον περιηγητή σας

- https://portal.azure.com
- Όνομα χρήστη: [παρέχεται] Κωδικός πρόσβασης: [παρέχεται]
- Μεταβείτε στην αναζήτηση στην κορυφή της σελίδας και γράψτε Sentinel και κάντε κλικ στο Microsoft Sentinel
- Στη στήλη όνομα κάντε κλικ στο AzureSentinel
- Στη νέα καρτέλα μεταβείτε στα Logs
- Κλείστε οποιαδήποτε αναδυόμενα παράθυρα που εμφανίζονται και αποκρύψτε οποιοδήποτε μενού για να έχετε πλήρη οθόνη εμπειρία στα logs







WORKSHOP

Log analysis με Kusto Query Language

Πίνακες συμβάντων στο εργαστηριακό περιβάλλον

- **SecurityEvent**
- **Sysmon (based on Event)**
- **Suricata**
- **PFSenseFirewallEvents**

Φιλτράρισμα συμβάντων

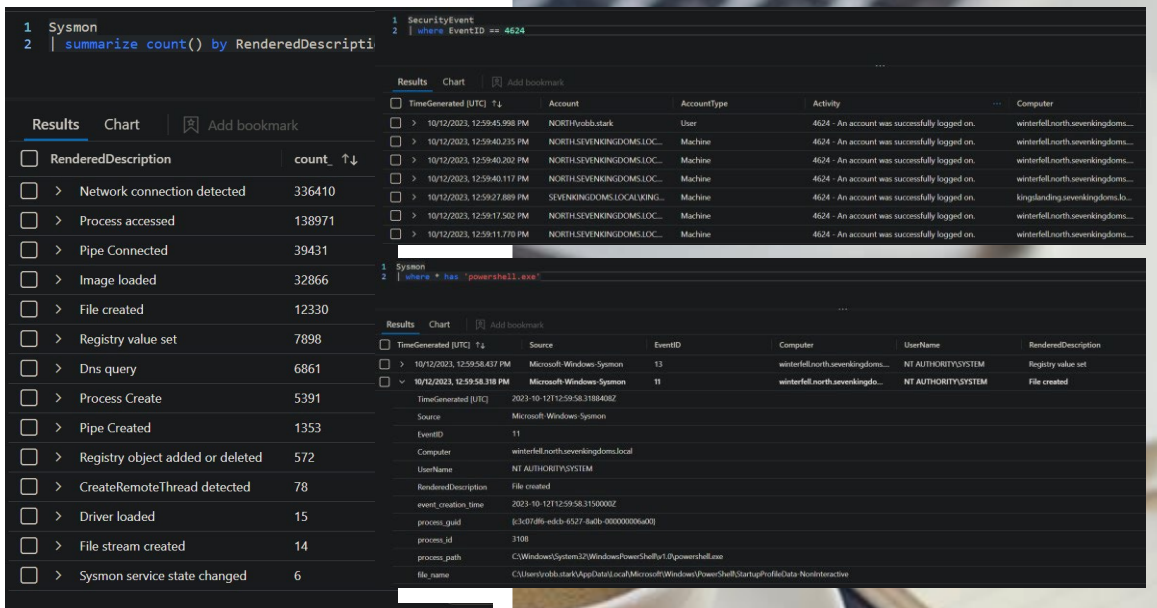
- Φιλτράρισμα κατά συνθήκη (where)
- Έλεγχος αν κάποια στήλη περιέχει συμβολοσειρά (where * has)
- Επιλογή υποσυνόλου στηλών (project)
- Λίστα μοναδικών τιμών (distinct)
- Λειτουργία αναζήτησης
- Λειτουργίες σε συμβολοσειρές (==, != , has, contains)

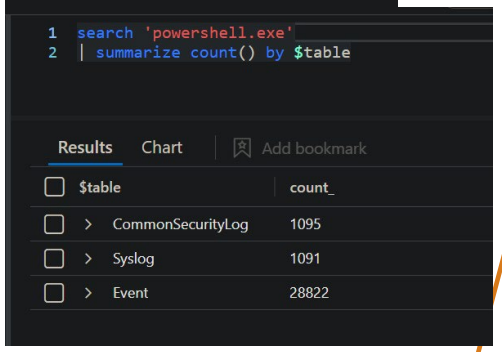
Συγκέντρωση συμβάντων

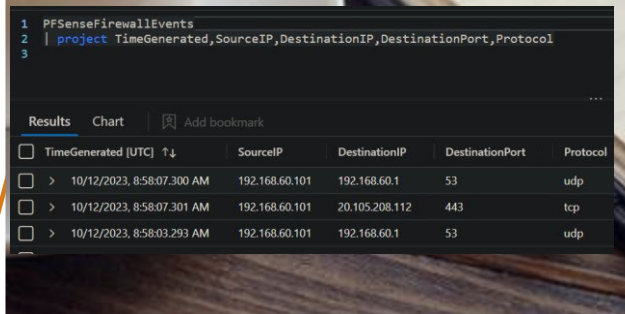
- Χρήση της λειτουργίας summarize (summarize)
- Υπολογισμός γραμμών υπό συνθήκη (countif())
- Μοναδικές τιμές (dcount())
- Ομαδοποίηση δεδομένων σε κάδους (bin())
- Ανάλυση χρονοσειρών (make-series)

Οπτικοποίηση

- Οπτικοποίηση αποτελεσμάτων ερωτημάτων (render)







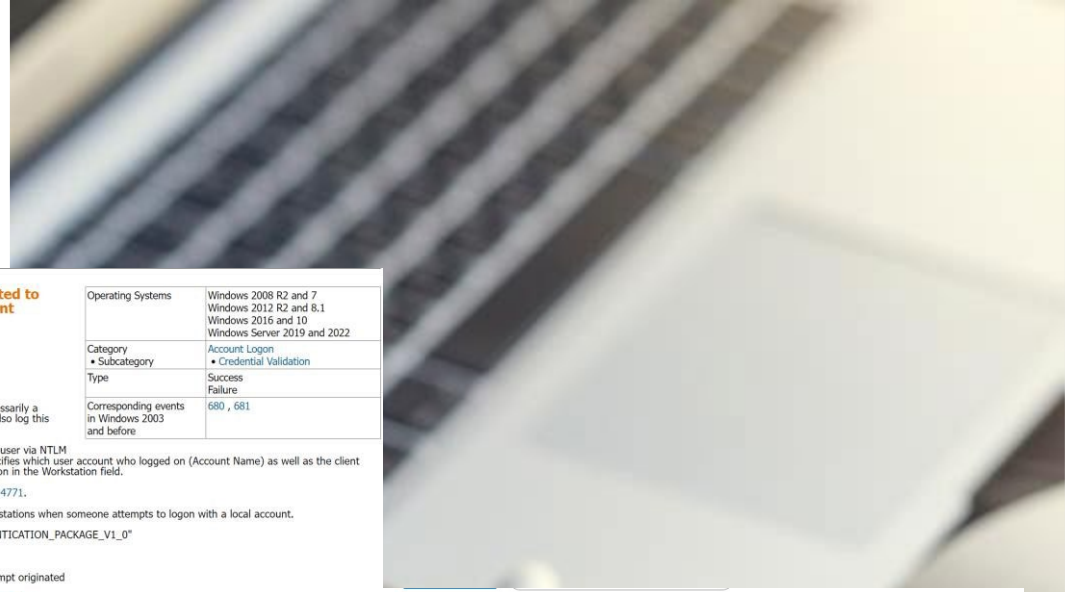
WORKSHOP

Συγκεκριμένα χαρακτηριστικά καταγραφής - SecurityEvent

- Provide audit information related to activities occurring on Windows Operating Systems
- Types of Events:
  - KQL:

    SecurityEvent | ξεχωριστή Διεργασία

    Περισσότερες πληροφορίες για το κάθε είδος log μπορεί να βρεθεί εδώ: Windows Security Log Events



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

On this page
- Description of this event
- Field level details
- Examples

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

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.

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
```

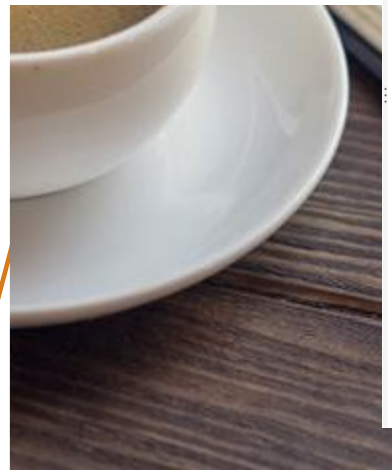
Results | Chart | Add bookmark

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)



WORKSHOP

Χρήση MITRE ATT&CK για τον Μηχανικό Εντοπισμό – Security Event

- Είδη ATT&CK Τακτικών που εντοπίστηκαν
  - Πρόσβαση Στοιχείων
    - Brute Force (Event ID: 4625 or 5379)
    - Steal or Forge Kerberos Tickets: Kerberoasting (Event ID: 4769)
    - OS Credential Dumping: DCSync (Event ID: 4662)
  - Εκτέλεση
    - Command and Scripting Interpreter: Windows Command Shell (Event ID: 4688)
    - System Services (Event ID: 4697)
  - Επιμονή
    - Scheduled Task/Job (Event ID
    - System Services (Event ID: 4
  - Κλιμάκωση Προνομίων
    - Group Policy Modification (E
  - Πλευρική Κίνηση
    - Remote Desktop Protocol (R
  - Αμυντική Αποφυγή
    - Use Alternate Authentication (Event ID: 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.

WORKSHOP

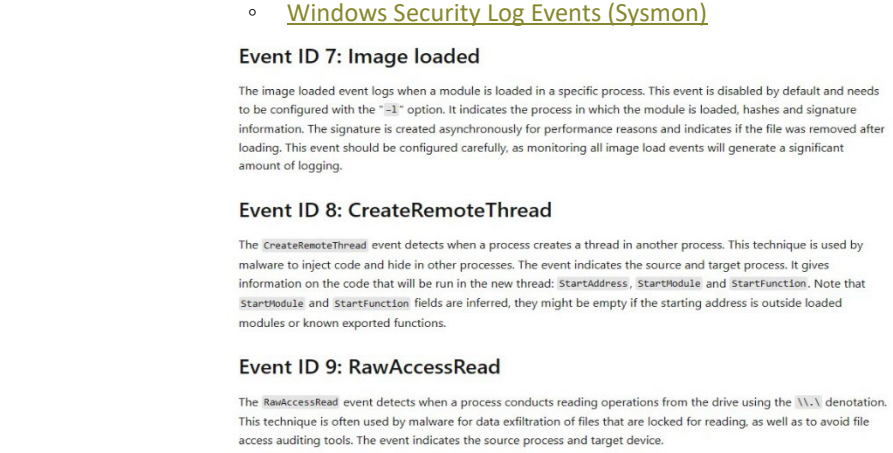
Συγκεκριμένα χαρακτηριστικά καταγραφής - Sysmon

- Sysmon is enabled on all Windows hosts
  - Provides Endpoint-level visibility

- Types of Events:
  - KQL:

    Sysmon | distinct RenderedDescription

- Περισσότερες πληροφορίες για κάθε είδος τύπου log μπορούν να βρεθούν στους παρακάτω συνδέσμους:
  - Sysmon log types
  - Windows Security Log Events (Sysmon)



Event ID 7: Image loaded

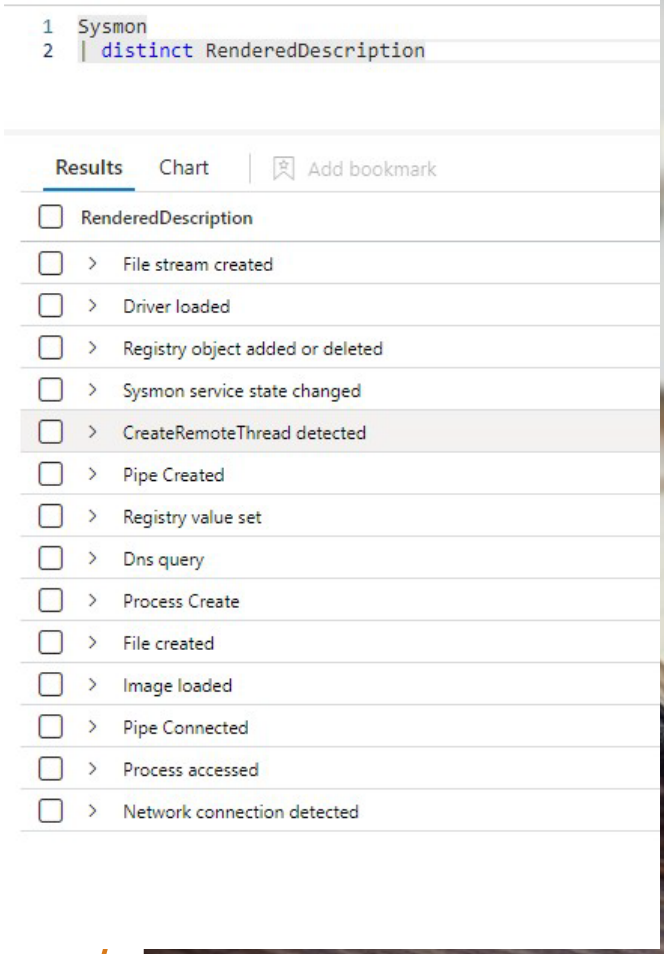
The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the "`-l`" option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance 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

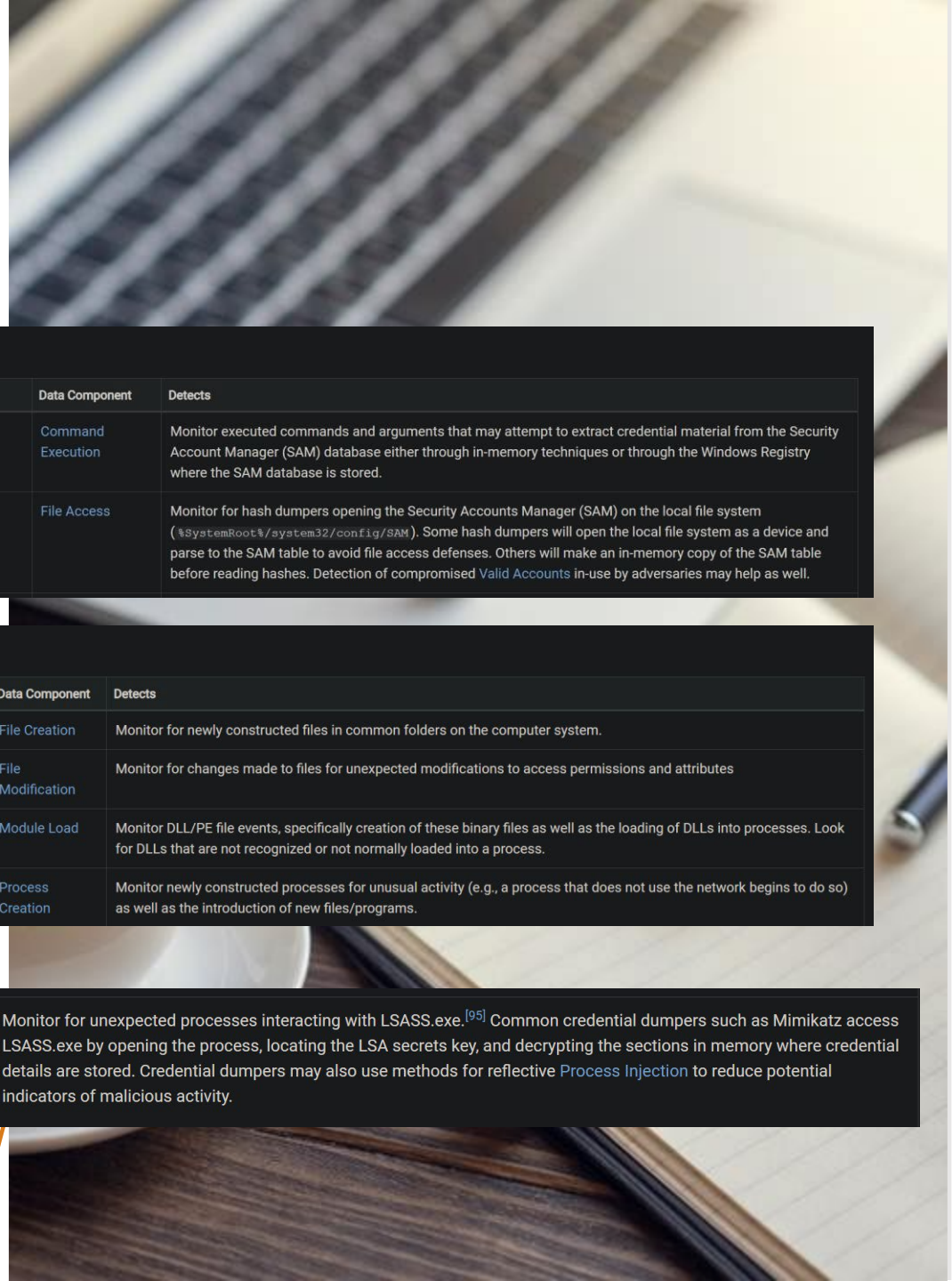
The `RawAccessRead` event detects when a process conducts reading operations from the drive using the `\\.\` denotation. This technique is often used by malware for data exfiltration of files that are locked for reading, as well as to avoid file access auditing tools. The event indicates the source process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



WORKSHOP

Χρήση MITRE ATT&CK για τον Μηχανικό Εντοπισμό - Sysmon

- Είδη ATT&CK Τακτικών που εντοπίστηκαν
  - Ανακάλυψη
    - Phising
    - Drive-by Compromise
  - Εκτέλεση
    - Command and Scripting Interpreter
    - User Execution
  - Επιμονή
    - Scheduled Task/Job
    - Hijack Execution Flow: DLL Side-Loading
    - Server Software Component: Web Shell
  - Αμυντική αποφυγή
    - Disable or Modify Tools
    - Obfuscated Files or Information
  - Αποδιήθηση
    - OS Credential Dumping
  - Ανακάλυψη
    - System Information Discovery
    - Query Registry
  - Πλευρική Κίνηση
    - Remote Desktop Protocol
    - Lateral Tool Transfe r
  - Αντίκτυπο
    - Data Destruction
    - Disk Wipe
  - Συλλογή
    - Data from Local System
    - Data from Removable Media
  - Αποδιήθηση
    - Exfiltration Over C2 Channel



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.

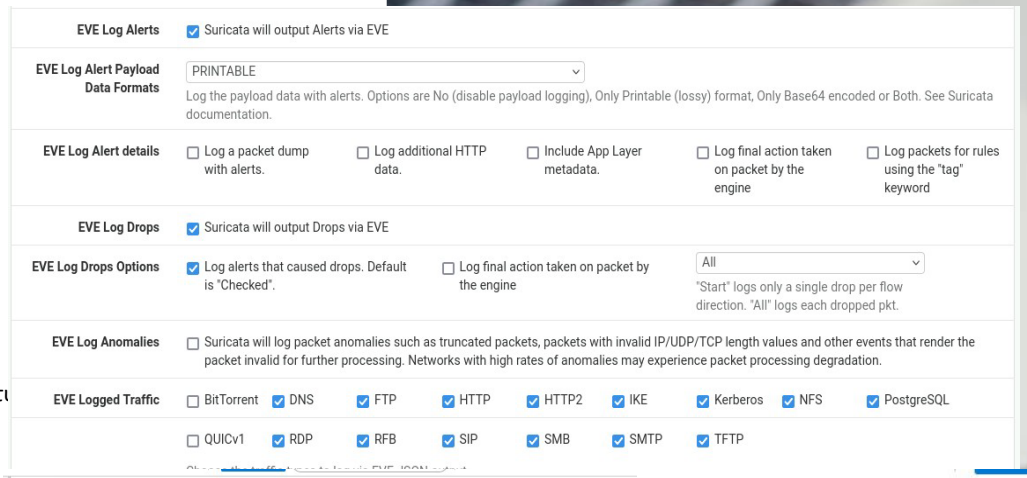
WORKSHOP

Ειδικά χαρακτηριστικά logs - Suricata

- Suricata logging ενεργό
  - Παρέχει άψογη ορατότητα στο επίπεδο Δικτύου
  - Εκτός από τις ειδοποιήσεις, μπορεί επίσης να παράγει αρχεία καταγραφής με βάση συγκεκριμένη επισκεψιμότητα, π.χ. HTTP.
- Types of Events:
  - KQL:

```
Suricata | distinct event_type
| where event_type != ''
```

- Επεκτίνοντας
  - Επιπλέον πληροφορίες μπορούν να εξαχθούν από συγκεκριμένες στήλες με βάση τους τ

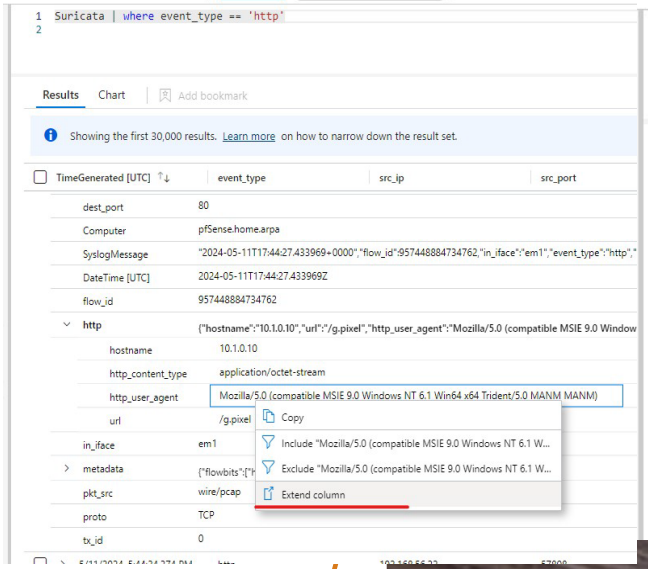


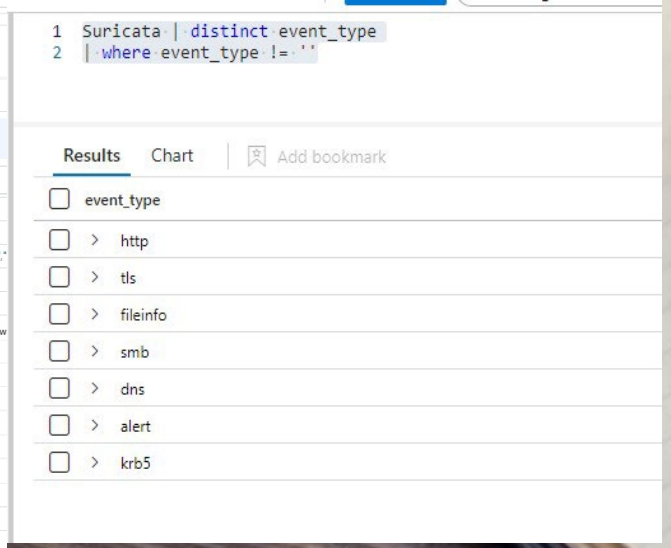

```
1 Suricata | where event_type == 'http'
2 | extend http_user_agent_ = tostring(http.http_user_agent)
```

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





WORKSHOP

Παραδείγματα - Εκτέλεση αυτόματης εκκίνησης ή σύνδεσης: Κλειδιά εκτέλεσης Registry / Φάκελος εκκίνησης

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

◦ Η τοποθέτηση ενός προγράμματος σε έναν φάκελο εκκίνησης θα προκαλέσει επίσης την εκτέλεση αυτού του προγράμματος όταν ένας χρήστης συνδεθεί. Υπάρχει μια θέση φακέλου εκκίνησης για μεμονωμένους λογαριασμούς χρηστών, καθώς και ένας φάκελος εκκίνησης σε ολόκληρο το σύστημα που θα ελεγχθεί 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 την ανίχνευση

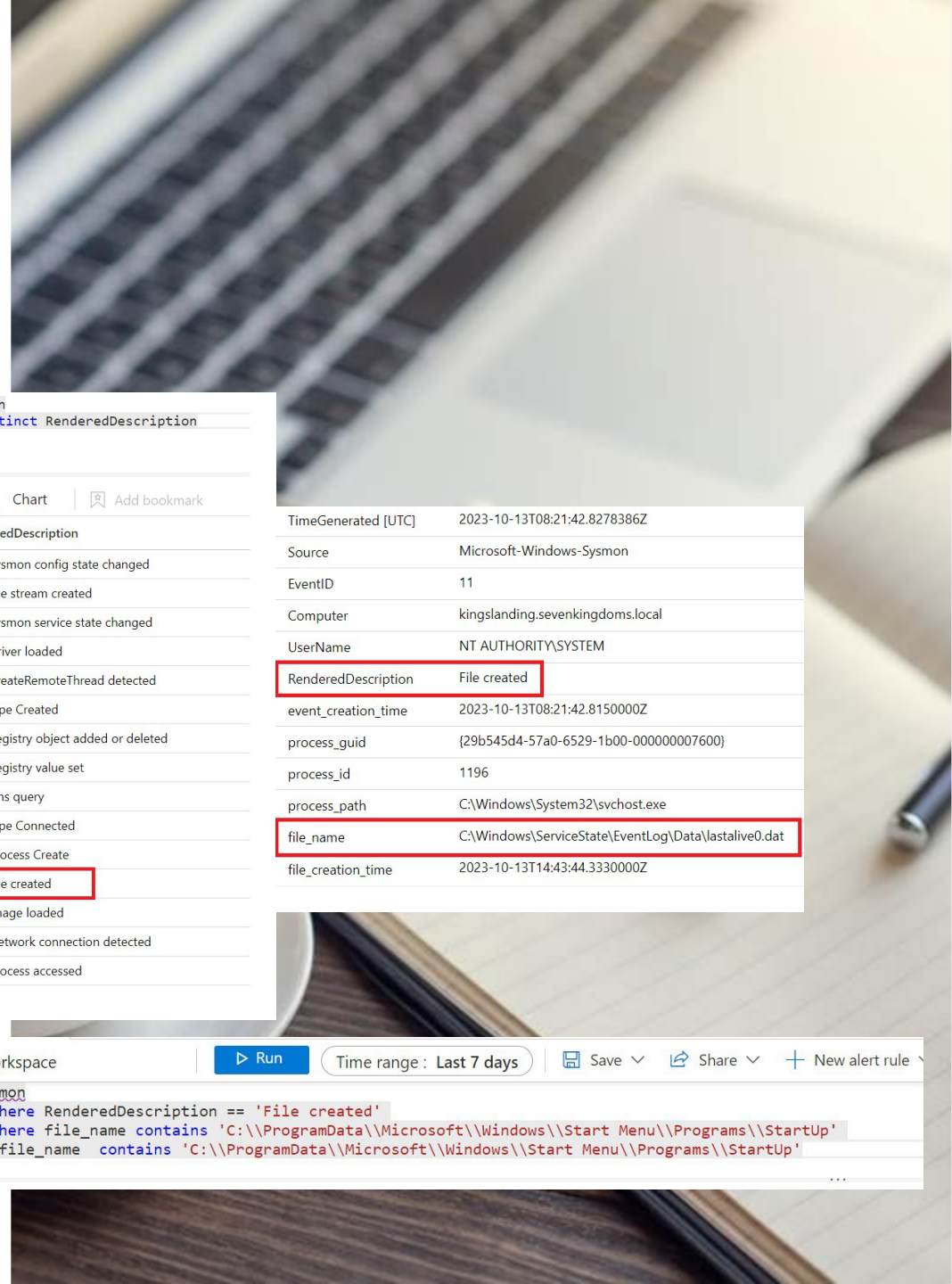
Q: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες;
A: Sysmon

Q: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων Sysmon;
A: Αρχείο Δημιουργήθηκε

Q: Η ανίχνευση βασίζεται σε συμβάντα ή σε όγκους;
A: Event-based

Q: Ποιες στήλες είναι σημαντικές ώστε να μπορούμε να τις χρησιμοποιήσουμε ως φίλτρα;
A: Rendered Περιγραφή, file_name

Q: Ποιο φίλτρο θα βάλω στις σημαντικές στήλες:
A: 1 Αρχείο Δημιουργήθηκε ισούται ‘Αρχείο Δημιουργήθηκε’
2. file_name περιέχει '\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup' or file_name περιέχει 'C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\StartUp’ * *KQL syntax tip: Αντικατάσταση \ with \\ διότι το backslash χρησιμοποιείται για την ορθή διατύπωση χαρακτήρων



WORKSHOP

Παραδείγματα – Αποδιήθηση στην υπηρεσία Ιστού

Exfiltration Over Web Service

◦ Οι αντίπαλοι μπορεί να χρησιμοποιήσουν μια υπάρχουσα, νόμιμη εξωτερική υπηρεσία Ιστού για να εξάγουν δεδομένα αντί για το κύριο κανάλι εντολών και ελέγχου τους. Οι δημοφιλείς υπηρεσίες Ιστού που λειτουργούν ως μηχανισμός εξαγωγής μπορεί να παρέχουν σημαντική κάλυψη λόγω της πιθανότητας ότι οι υπολογιστές εντός ενός δικτύου ήδη επικοινωνούν με αυτές πριν από την παραβίαση. Οι κανόνες του τείχους προστασίας μπορεί επίσης να υπάρχουν ήδη για να επιτρέπουν την κυκλοφορία σε αυτές τις υπηρεσίες.

◦ Οι πάροχοι υπηρεσιών Ιστού χρησιμοποιούν επίσης συνήθως κρυπτογράφηση SSL/TLS, παρέχοντας στους αντιπάλους ένα επιπλέον επίπεδο προστασίας.

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

Q: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες;
A: Sysmon ή PFSenseFirewallEvents

Q: Από αυτούς τους 2 πίνακες δεδομένων που παρέχουν πληροφορίες σχετικά με τον αριθμό των byte που μεταφέρθηκαν
A: PFSenseFirewallEvents

Q: Η ανίχνευση βασίζεται σε event-based (γεγονότα) ή volume-based (μεγέθη);
A: Volume-based (μεγέθη)

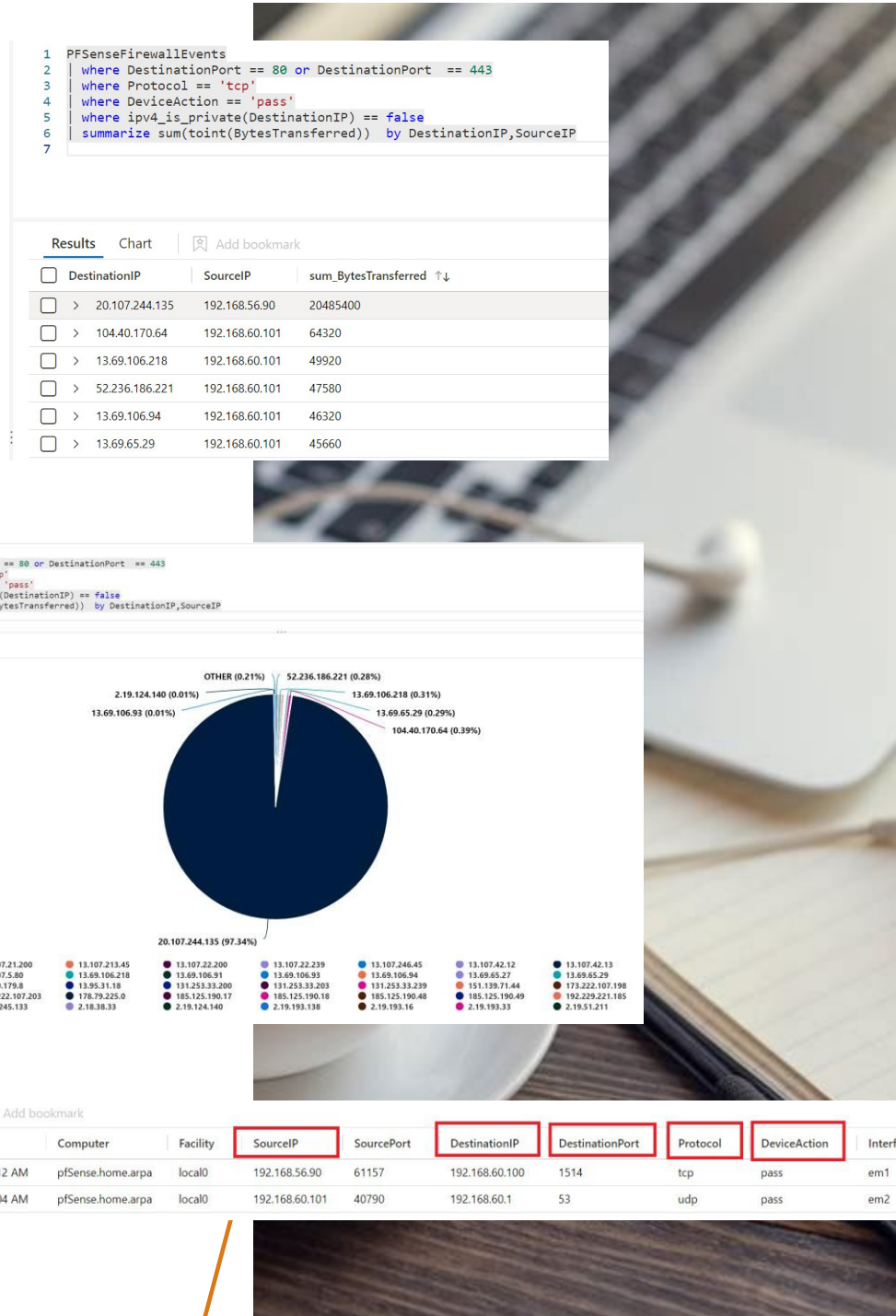
Q: Ποια λειτουργία του SIEM είναι σημαντική για τις ανιχνεύσεις που βασίζονται volume-based;
A: Συγκέντρωση Συμβάντων (σύνοψη)

Q: Ποιες στήλες είναι σημαντικές ώστε να μπορούμε να τις χρησιμοποιήσουμε ως φίλτρα;
A: DestinationPort, Protocol, DeviceAction και η Destination IP πρέπει να είναι δημόσια

Q: Ποιες στήλες είναι σημαντικές για τη συγκέντρωση;
A: SourceIP, DestinationIP, BytesTransferred

Q: Πώς πρέπει να συναθροίσουμε τα αποτελέσματα?
A: Αθροίζοντας τα bytes που μεταφέρθηκαν ανα Destination και Source IP

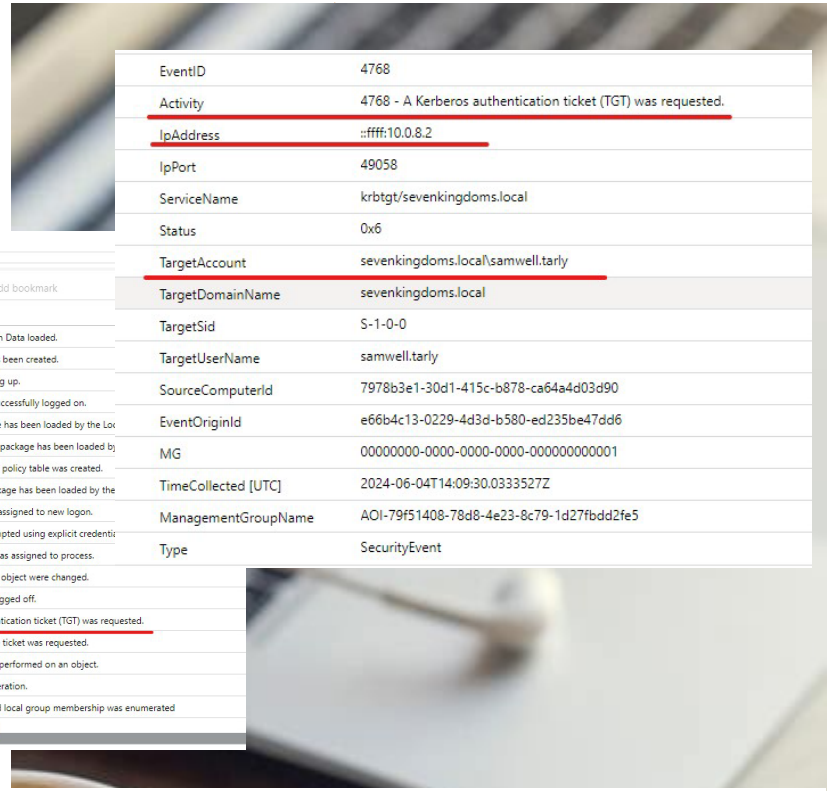
Q (BONUS): Είναι καλύτερο να εμφανίζονται τα αποτελέσματα της συγκέντρωσης ως δεδομένα ή ως γραφήματα;



WORKSHOP

Παραδείγματα – Ανακάλυψη Λογαριασμού: Τομέας Λογαριασμός

- Account Discovery: Domain Account
- Οι αντίπαλοι ενδέχεται να επιχειρήσουν να αποκτήσουν μια λίστα με λογαριασμούς τομέα. Αυτές οι πληροφορίες μπορούν να βοηθήσουν τους αντιπάλους να προσδιορίσουν ποιοι λογαριασμοί τομέα υπάρχουν για να βοηθήσουν σε περαιτέρω συμπεριφορές, όπως η στόχευση συγκεκριμένων λογαριασμών που διαθέτουν συγκεκριμένα προνόμια. Ανακαλύπτει έγκυρα ονόματα χρήστη μέσω ωμής βίας, αναζητώντας 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 διαπιστώσουμε ότι το όνομα χρήστη δεν ήταν έγκυρο. Τα έγκυρα ονόματα χρήστη θα παραβιάσουν είτε το TGT σε μια απόκριση AS-REP είτε το σφάλμα KRB5KDC_ERR_PREAUTH_REQUIRED, σηματοδοτώντας ότι ο χρήστης πρέπει να εκτελέσει προ-έλεγχο ταυτότητας. •Tools: krbrute, nmap, crackmapexec



- Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τη λογική πίσω από την ανίχνευση - Επίπεδο τελικού σημείου

  Q: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: SecurityEvents

  Q: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων SecurityEvents; A: 4768 - A Kerberos αυθεντικοποίησης ticket (TGT) αιτήθηκε.

  Q: Ο εντοπισμός είναι event-based ή volume-based; A: Volume-based

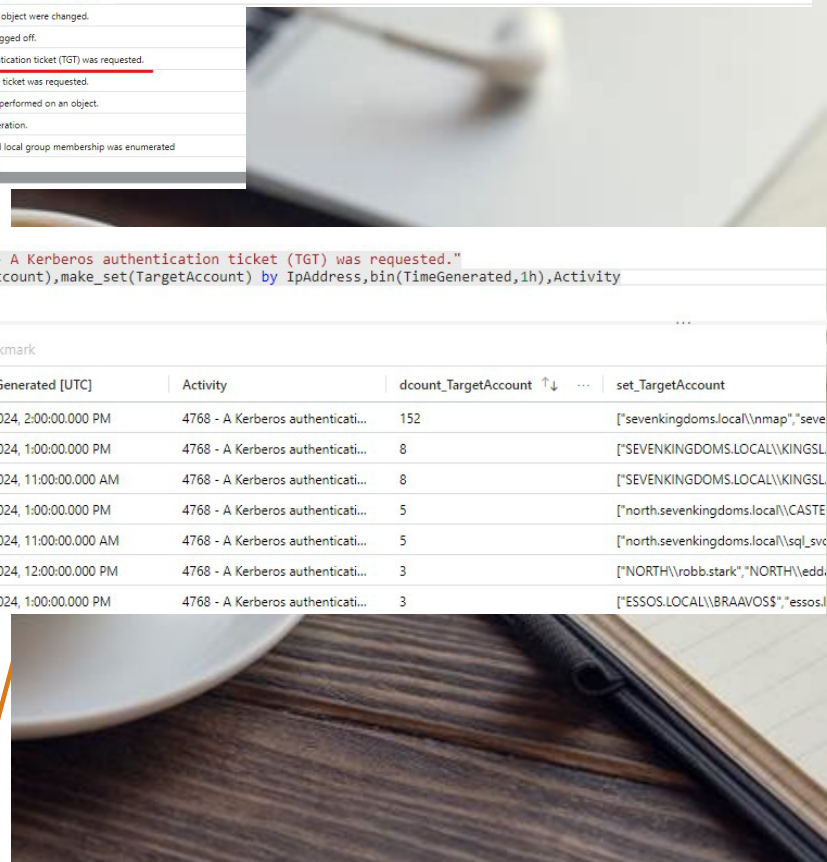
  Q: Ποια λειτουργία του SIEM είναι σημαντική για τις ανιχνεύσεις volume-based; A: Συγκέντρωση Συμβάντων (σύνοψη)

  Q: Ποιες στήλες είναι σημαντικές ώστε να μπορούμε να τις χρησιμοποιήσουμε ως φίλτρα; A: Δραστηριότητα

  Q: Ποιες στήλες είναι σημαντικές για τη συγκέντρωση; A: IpAddress, TargetAccount, TimeGenerated

  Q: Πώς πρέπει να συναθροίσουμε τα αποτελέσματα;
  A: Το πεδίο Διεύθυνση IP είναι από όπου προέρχονται τα αιτήματα Kerberos Ticket. Επομένως, αναζητούμε διευθύνσεις IP με αιτήματα Kerberos Ticket για πολλούς διαφορετικούς λογαριασμούς.

  Q (BONUS): Είναι καλύτερο να εμφανίζονται τα αποτελέσματα συγκέντρωσης ως δεδομένα ή γραφήματα; A: Γραφήματα (απόδοση γραφήματος στηλών)



WORKSHOP

Παραδείγματα - Brute Force: Password Spraying

Brute Force: Password Spraying (Πολλαπλές Δοκιμές)

- Οι αντίπαλοι ενδέχεται να χρησιμοποιήσουν έναν μόνο ή μια μικρή λίστα με κοινά χρησιμοποιούμενους κωδικούς πρόσβασης σε πολλούς διαφορετικούς λογαριασμούς, για να προσπαθήσουν να αποκτήσουν έγκυρα διαπιστευτήρια λογαριασμού. Η διαδικασία ψεκασμού κωδικών πρόσβασης χρησιμοποιεί έναν κωδικό πρόσβασης (π.χ., 'Password01') ή μια μικρή λίστα με κοινά χρησιμοποιούμενους κωδικούς πρόσβασης, που μπορεί να ταιριάζουν με την πολιτική πολυπλοκότητας του τομέα. Γίνονται προσπάθειες σύνδεσης με αυτόν τον κωδικό πρόσβασης σε πολλούς διαφορετικούς λογαριασμούς σε ένα δίκτυο, για να αποφευχθούν τα κλειδώματα λογαριασμών που θα συνέβαιναν κανονικά κατά την άσκηση βίαιης επιβολής σε έναν μόνο λογαριασμό με πολλούς κωδικούς πρόσβασης.

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

Q: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: SecurityEvents

Q: Τι τύπο συμβάντος θέλουμε από τον πίνακα δεδομένων SecurityEvents; A: 4625 - Η σύνδεση σε έναν λογαριασμό απέτυχε.

Q: Το συμβάν ανίχνευσης είναι event-based ή σε Volume-based; A: Volume-based

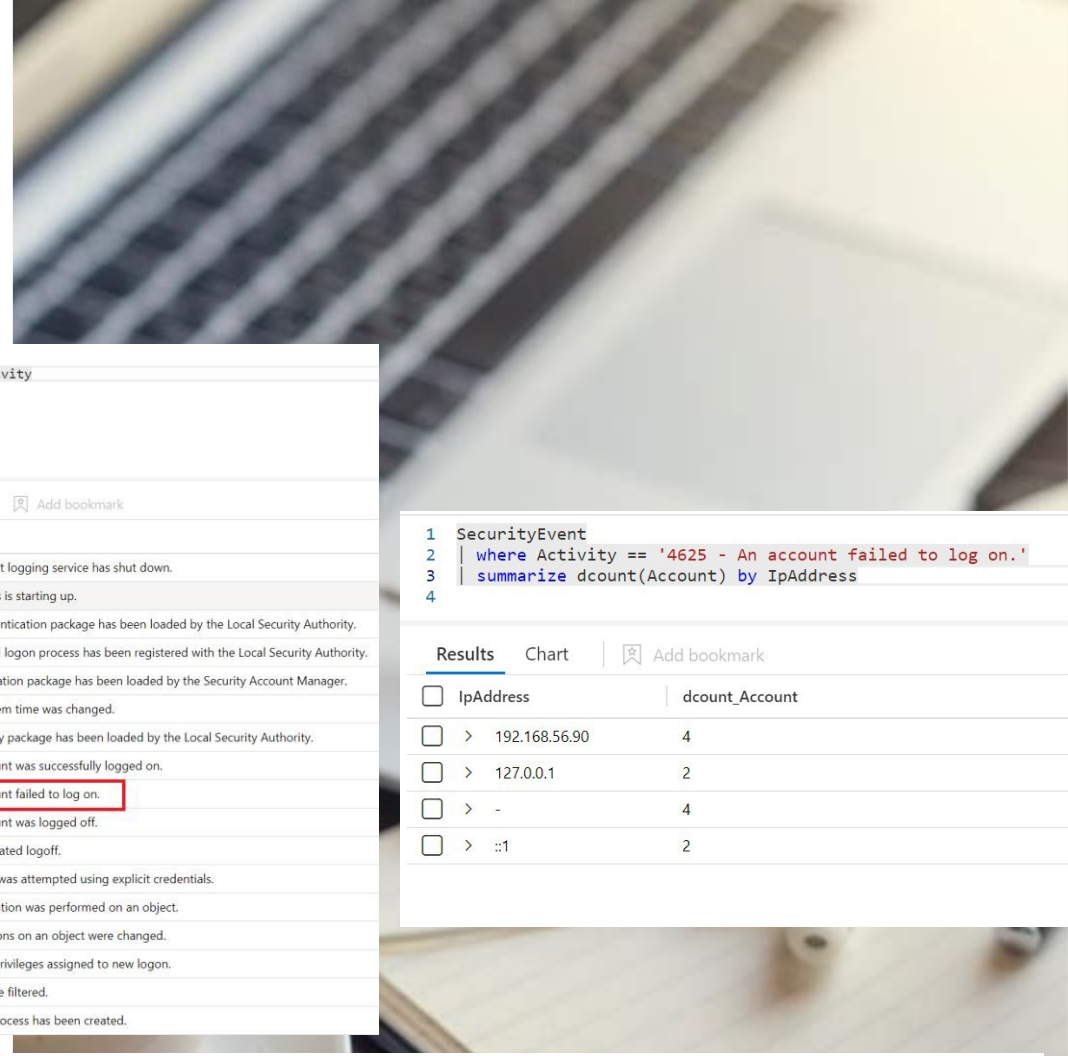
Q: Ποια λειτουργία του SIEM είναι σημαντική για τις ανιχνεύσεις που είναι volume-based;
A: Συγκέντρωση Συμβάντων (σύνοψη)

Q: Ποιες στήλες είναι σημαντικές ώστε να μπορούμε να τις χρησιμοποιήσουμε ως φίλτρα;
A: Καμία στην πραγματικότητα. Φιλτράροντας για το EventID 4625 έχουμε το σύνολο δεδομένων που θέλουμε να διερευνήσουμε.

Q: Ποιες στήλες είναι σημαντικές για τη συνάθροιση; A: IPAddress, Account.

Q: Πώς πρέπει να συναθροίσουμε τα αποτελέσματα;
A: Το πεδίο IP Address είναι από το σημείο όπου συμβαίνουν οι αποτυχημένες συνδέσεις. Έτσι, αναζητούμε διευθύνσεις IP με πολλαπλές αποτυχημένες συνδέσεις με διαφορετικούς λογαριασμούς. *
Q (BONUS) : Is it better to display aggregation results as data or graphs;
A: Γραφήματα

* Καταγραφή ελέγχου ταυτότητας τομέα: Ορισμένα πρωτόκολλα όπως το NTLM απαιτούν επιπλέον διαμόρφωση για να παρέχουν την IP πηγής του αποτυχημένου ελέγχου ταυτότητας



WORKSHOP

Παραδείγματα – Λογισμικό Διακομιστή: Web Shell

- Server Software Component: Web Shell
- Ένα κέλυφος ιστού (Web shell) είναι ένα σενάριο ιστού (Web script) που τοποθετείται σε έναν ελεύθερα προσβάσιμο διακομιστή ιστού για να επιτρέψει σε έναν κακόβουλο χρήστη να έχει πρόσβαση στον διακομιστή ιστού ως πύλη εισόδου σε ένα δίκτυο. Ένα κέλυφος ιστού (Web shell) μπορεί να παρέχει ένα σύνολο συναρτήσεων 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 ταιριάζουν με τις ενημερώσεις στο περιεχόμενο του διακομιστή Web και ενδέχεται να υποδηλώνουν εμφύτευση ενός σεναρίου κελύφους Web.

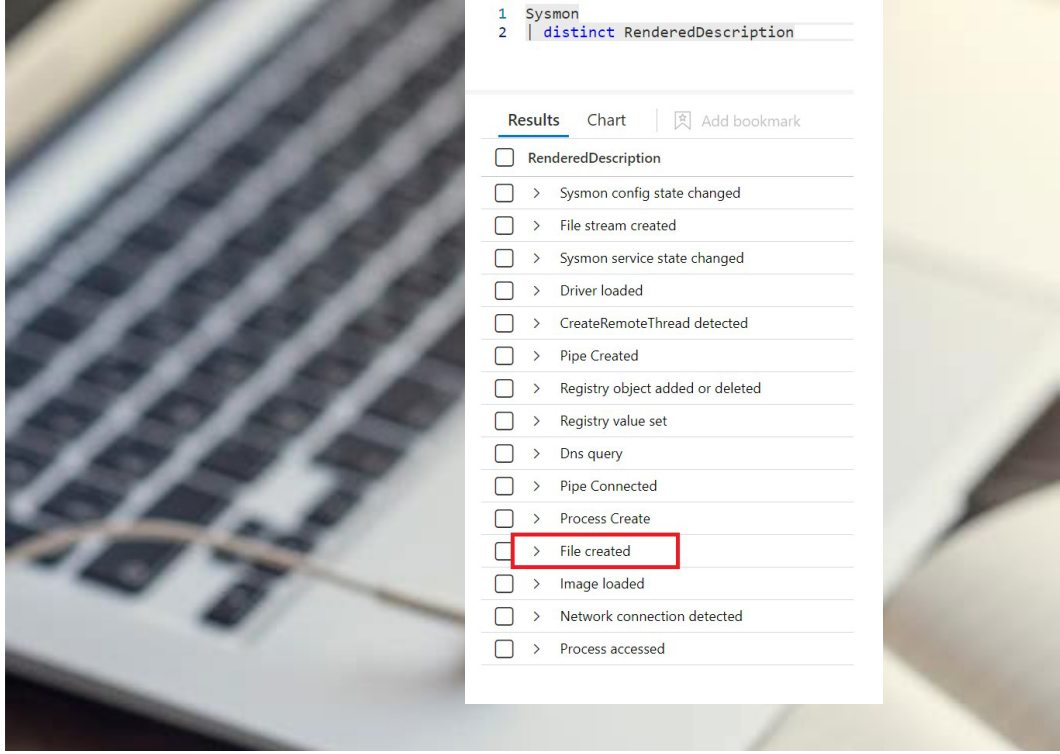
- Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τη λογική πίσω από την ανίχνευση - Δημιουργία αρχείου

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

Q: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων; A: Αρχείο Δημιουργήθηκε

Q: Ο εντοπισμός event-based ή volume-based; A: Event-based

Q: Ποιες στήλες είναι σημαντικές ώστε να μπορούμε να τις χρησιμοποιήσουμε ως φίλτρα; A: Rendered Περιγραφή, file_name
Η στήλη file_name εμφανίζει το αρχείο που δημιουργήθηκε με την πλήρη διαδρομή.
Q: Ποιο φίλτρο θα βάλω στις σημαντικές στήλες;
A: 1. Rendered Περιγραφή ισούται ‘Αρχείο Δημιουργήθηκε’
2. file_name αρχίζει με {Web Server Directory}
3. file_name λήγει με {Webshell file extension}
(Tip: Κοινή Webshell file επεκτάσεις: php, asp, aspx, cfm, jsp)
*KQL syntax tip: Replace \ with \\ because the backslash is used to escape characters




```
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

WORKSHOP

- Παραδείγματα – Λογισμικό Διακομιστή: Web Shell

  Server Software Component: Web Shell

- Ένα κέλυφος ιστού (Web shell) είναι ένα σενάριο ιστού (Web script) που τοποθετείται σε έναν ελεύθερα προσβάσιμο διακομιστή ιστού για να επιτρέψει σε έναν κακόβουλο χρήστη να έχει πρόσβαση στον διακομιστή ιστού ως πύλη εισόδου σε ένα δίκτυο. Ένα κέλυφος ιστού (Web shell) μπορεί να παρέχει ένα σύνολο συναρτήσεων προς εκτέλεση ή μια διεπαφή γραμμής εντολών στο σύστημα που φιλοξενεί τον διακομιστή ιστού.
  Η παρακολούθηση διεργασιών μπορεί να χρησιμοποιηθεί για την ανίχνευση διακομιστών Web που εκτελούν ύποπτες ενέργειες, όπως η δημιουργία cmd.exe ή η πρόσβαση σε αρχεία που δεν βρίσκονται στον κατάλογο Web.

- Ένα κέλυφος ιστού είναι ένα σενάριο ιστού που τοποθετείται σε έναν ελεύθερα προσβάσιμο διακομιστή ιστού για να επιτρέψει σε έναν κακόβουλο χρήστη να χρησιμοποιήσει τον διακομιστή ως πύλη σε ένα δίκτυο. Καθώς λειτουργεί το κέλυφος, θα εκδίδονται εντολές από την εφαρμογή ιστού στο ευρύτερο λειτουργικό σύστημα του διακομιστή.

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

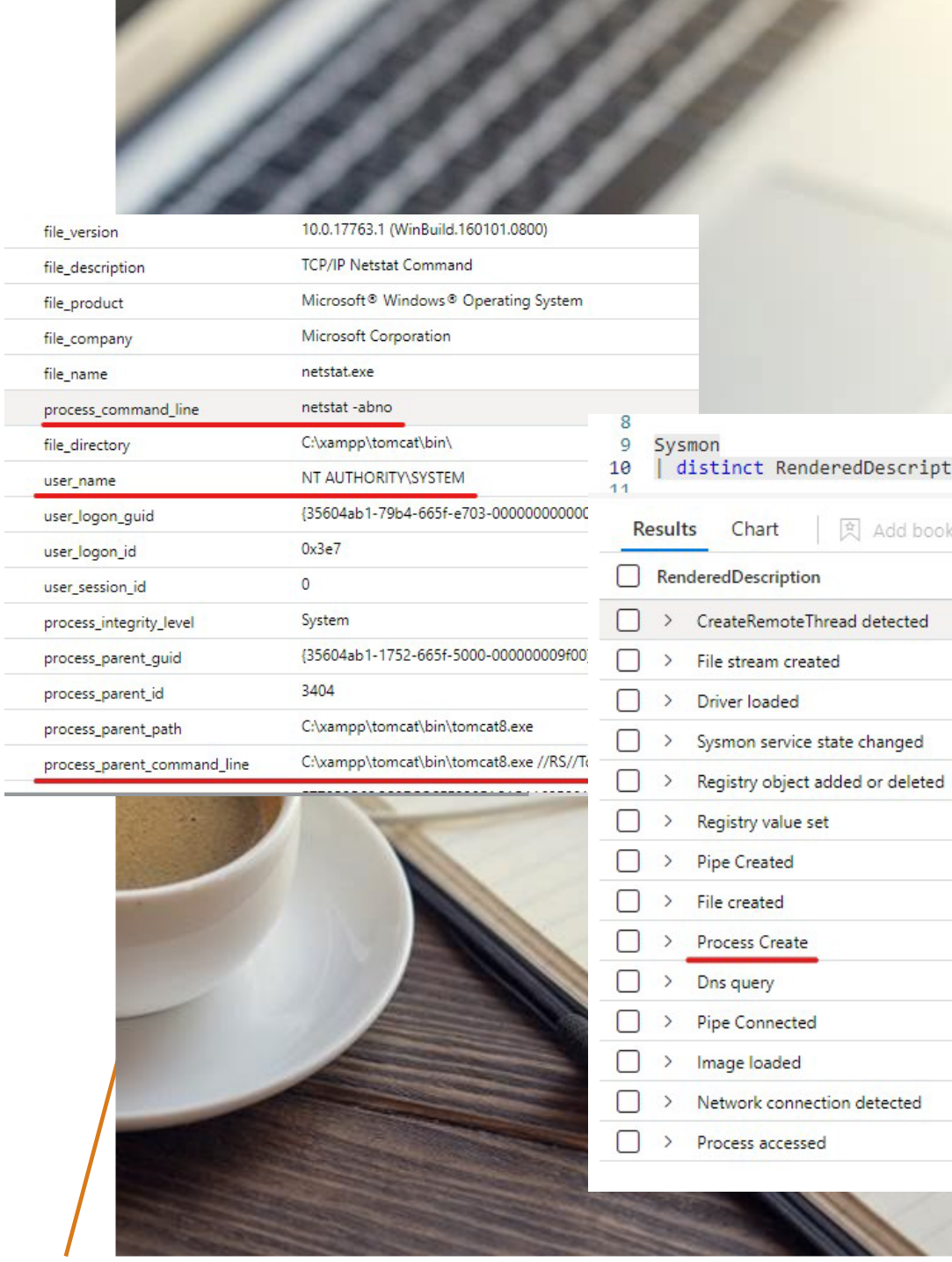
Q: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: Sysmon

Q: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων Sysmon; A: Διαδικασία Δημιουργία

Q: Ο εντοπισμός είναι event-based ή volume-based? A: Event-based

Q: Ποιες στήλες είναι σημαντικές ώστε να μπορούμε να τις χρησιμοποιήσουμε ως φίλτρα;
A: Rendered Περιγραφή, process_parent_command_line, process_command_line Command-line διεργασίες που εκτελούνται από τον διακομιστή ιστού διεργασίες processes is a high indicator of Web Shell execution.

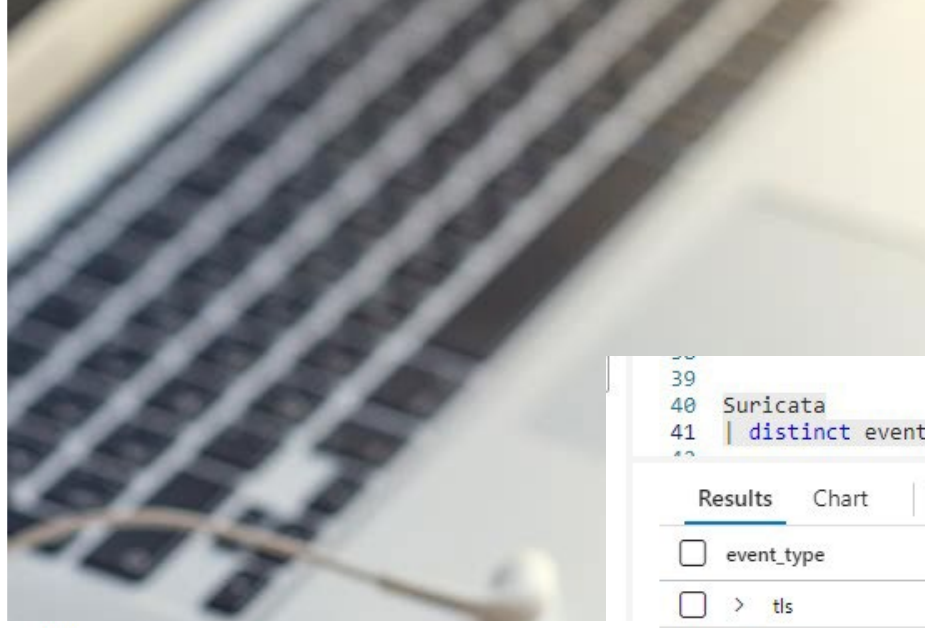
Q: Ποιο φίλτρο θα βάλω στις σημαντικές στήλες;
A: 1. Rendered Περιγραφή ισούται 'Process Create'
2. process_parent_command_line περιέχει συνηθισμένες Web Server διεργασίες 3. process_command_line περιέχει common command-line processes
(Tip: Common Web Server processes: w3wp.exe, httpd.exe, tomcat.exe, nginx.exe) (Tip2: Common command-line processes: cmd, powershell, netstat, systeminfo, ipconfig, whoami etc.) *KQL syntax tip: Replace \ with \\ because the backslash is used to escape characters



WORKSHOP

Παραδείγματα – Λογισμικό Διακομιστή: Web Shell

- Server Software Component: Web Shell
- Ένα κέλυφος ιστού (Web shell) είναι ένα σενάριο ιστού (Web script) που τοποθετείται σε έναν ελεύθερα προσβάσιμο διακομιστή ιστού για να επιτρέψει σε έναν κακόβουλο χρήστη να έχει πρόσβαση στον διακομιστή ιστού ως πύλη εισόδου σε ένα δίκτυο. Ένα κέλυφος ιστού (Web shell) μπορεί να παρέχει ένα σύνολο συναρτήσεων προς εκτέλεση ή μια διεπαφή γραμμής εντολών στο σύστημα που φιλοξενεί τον διακομιστή ιστού. Παρακολούθηση και ανάλυση μοτίβων κυκλοφορίας και επιθεώρησης πακέτων που σχετίζονται με πρωτόκολλα που δεν ακολουθούν τα αναμενόμενα πρότυπα πρωτοκόλλου και ροές κυκλοφορίας (π.χ. περιττά πακέτα που δεν ανήκουν σε καθιερωμένες ροές, άσκοπα ή ανώμαλα μοτίβα κυκλοφορίας, ανώμαλη σύνταξη ή δομή).



- **Βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε τη λογική πίσω από την ανίχνευση - Περιεχόμενο κίνησης δικτύου**

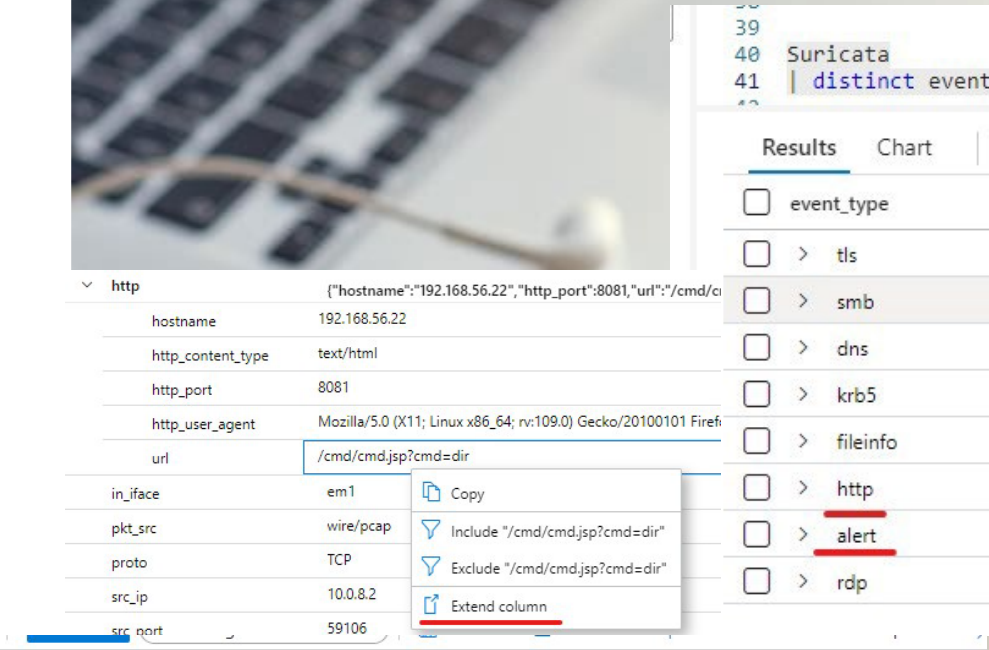
  Q: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: Suricata

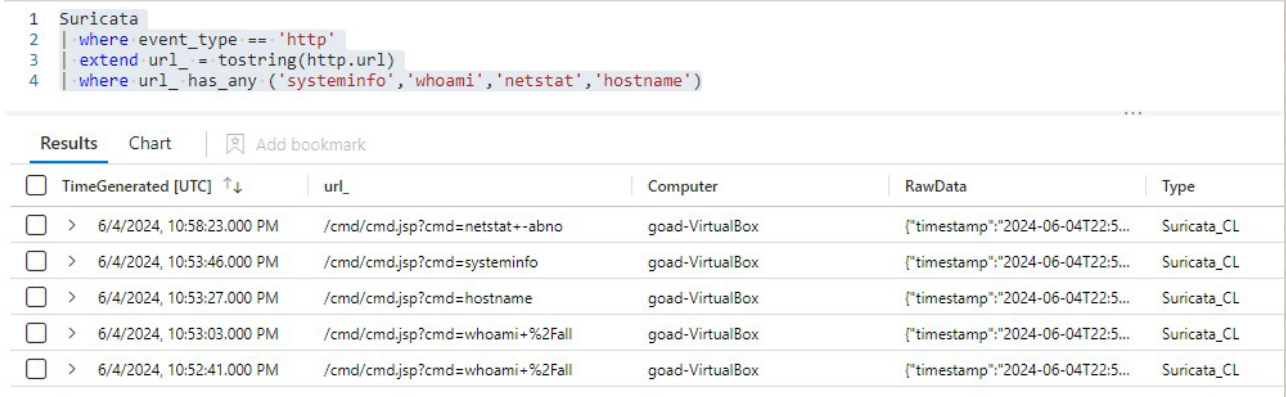
  Q: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων Sysmon; A: event_type > http

  Q: Ο εντοπισμός είναι event-based ή volume-based? A: Event-based

  Q: Ποιο ένθετο πεδίο είναι σημαντικό μέσα στο στοιχείο http;
  A: url
  Ορισμένα κελύφη ιστού λειτουργούν λαμβάνοντας τις ύποπτες εντολές ως παραμέτρους στη διεύθυνση URL.
  Q: Ποιο φίλτρο θα βάλω στις σημαντικές στήλες;
  A: 1. event_type equals 'http'
  2. Η διεύθυνση URL περιέχει οποιαδήποτε από τις ύποπτες εντολές

  Q: Το Suricata εξέδωσε κάποια προειδοποίηση σχετικά με αυτήν τη δραστηριότητα;
  A: Suricata | όπου event_type == 'alert' και app_proto == 'http'





WORKSHOP

Παραδείγματα – Λογισμικό Διακομιστή: Web Shell

Κλοπή ή παραποίηση Kerberos Tickets: AS-REP Roasting

Οι αντίπαλοι ενδέχεται να αποκαλύψουν τα διαπιστευτήρια λογαριασμών που έχουν απενεργοποιήσει τον προέλεγχο ταυτότητας Kerberos μέσω μηνυμάτων Kerberos που έχουν διαρρεύσει με κωδικό πρόσβασης. Για κάθε λογαριασμό που βρίσκεται χωρίς προέλεγχο ταυτότητας, ένας αντίπαλος 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 ανακτημένα κρυπτογραφημένα δεδομένα ενδέχεται να είναι ευάλωτα σε επιθέσεις εκτός σύνδεσης με το διαρρήξιμο κωδικού πρόσβασης, παρόμοια με το Kerberoasting, και να εκθέσουν διαπιστευτήρια απλού κειμένου.

Ένας λογαριασμός που είναι εγγεγραμμένος σε έναν τομέα, με ή χωρίς ειδικά δικαιώματα, μπορεί να χρησιμοποιηθεί για να καταχωρίσει όλους τους λογαριασμούς τομέα που έχουν απενεργοποιήσει τον προέλεγχο ταυτότητας, χρησιμοποιώντας εργαλεία των Windows όπως το PowerShell με φίλτρο LDAP. Εναλλακτικά, ο αντίπαλος μπορεί να στείλει ένα μήνυμα AS-REQ για κάθε χρήστη. Εάν ο ελεγκτής τομέα απαντήσει χωρίς σφάλματα, ο λογαριασμός δεν απαιτεί προέλεγχο ταυτότητας και το μήνυμα AS-REP θα περιέχει ήδη τα κρυπτογραφημένα δεδομένα.

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

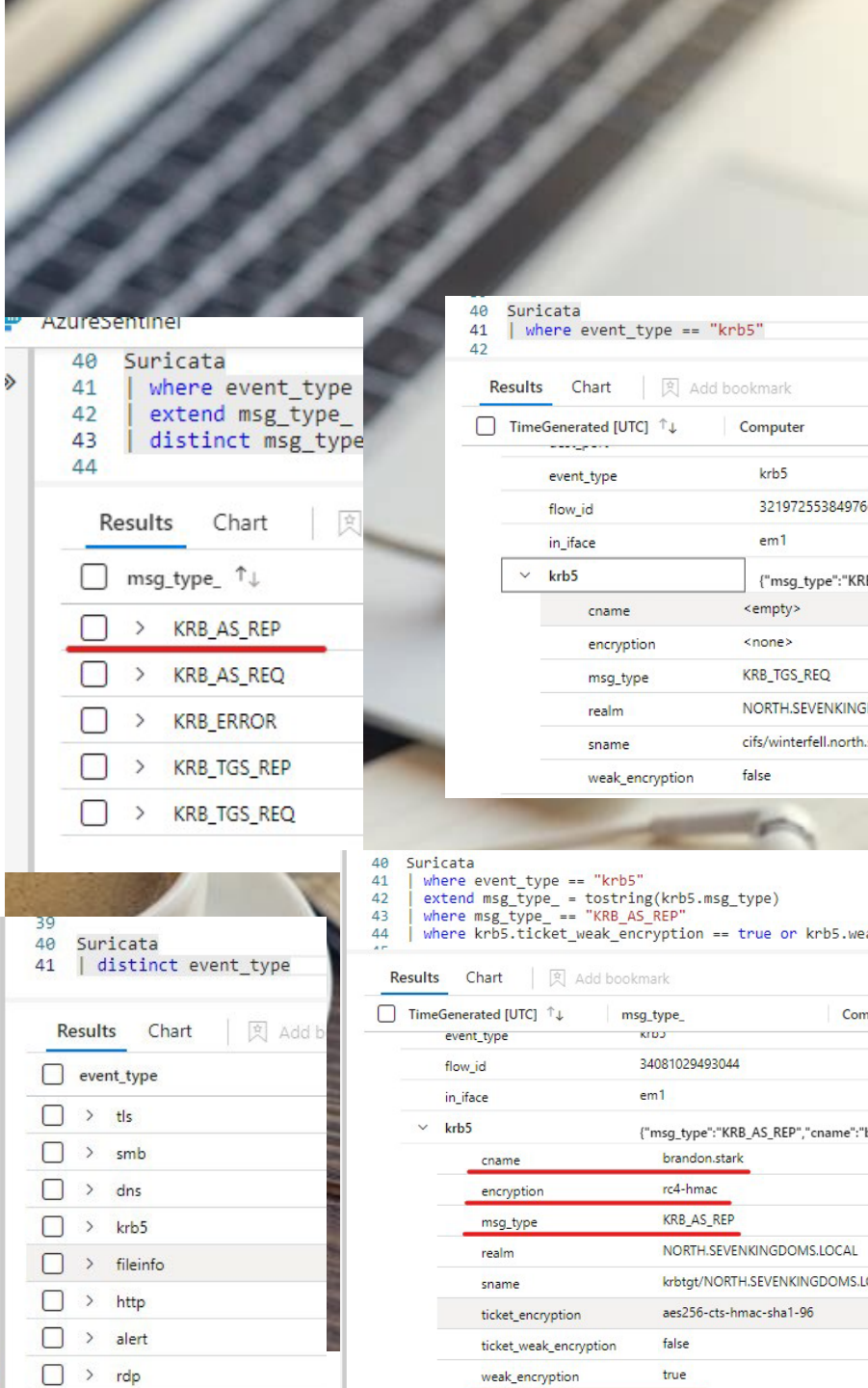
Q: Ποιος τύπος δεδομένων θα μας παρέχει αυτές τις πληροφορίες; A: Suricata
Q: Τι είδους συμβάν θέλουμε από τον πίνακα δεδομένων Sysmon; A: event_type > krb5

Q: Ο εντοπισμός είναι event-based ή volume-based? A: Event-based
Q: Ποια εμφωλευμένα αρχεία είναι σημαντικά μέσα στο krb5 αντικείμενο?

A: msg_type, weak_encryption, ticket_weak_encryption
Q: Ποιες στήλες είναι σημαντικές ώστε να μπορούμε να τις χρησιμοποιήσουμε ως φίλτρα; A: event_type, msg_type_ , weak_encryption_, ticket_weak_encryption_

Q: Ποιο φίλτρο θα βάλω στις σημαντικές στήλες;
A: 1. event_type = krb5
2. ticket_weak_encryption_ = true or weak_encryption_ = true

Q: Ποιος ήταν ο λογαριασμός που εκτέθηκε και ήταν ευάλωτος στην Roasting επίθεση AS-REP; A: cname εμφωλευμένη στήλη > brandon.stark
Q: Ποια είναι η στήλη που εμφανίζει την προέλευση της επίθεσης; A: src_ip > 10.0.8.2



Σας ευχαριστώ για την προσοχή σας!

Παρουσίαση από:

Christos Lazaridis
(Focal Point)

CyberSecPro