Ingegneria di rilevamento per le infrastrutture IT sanitarie

CSP011_W_H

CHRISTOS LAZARIDIS
PUNTO FOCALE

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

Introduzione all'ingegneria di rilevamento nella sicurezza sanitaria

Obiettivo: Esplorare il ruolo dell'ingegneria del rilevamento nella salvaguardia dei sistemi informativi sanitari.

Perché:

- Misure di sicurezza solide sono fondamentali per proteggere i dati sensibili dei pazienti nei servizi digitali sanitari.
- L'aumento delle minacce informatiche dinamiche comporta rischi per i pazienti sicurezza e privacy.
- L'ingegneria di rilevamento identifica, monitora e mitiga efficacemente le minacce alla sicurezza informatica e si adatta alle minacce dinamiche.

Servizi sanitari che possono essere monitorati

- **Servizi sanitari connessi:**
  - **Portali medico-paziente:** Piattaforme per la comunicazione, la programmazione degli appuntamenti e l'accesso alle cartelle cliniche.
  - **Manipolazione remota di apparecchiature mediche:**
    - Monitoraggio e controllo dei dispositivi medici utilizzati in remoto per la cura del paziente.
    - Critico per la telemedicina e la diagnostica a distanza.
  - **Sistemi di cartelle cliniche elettroniche (EHR):** Punto di archiviazione e accesso centrale per i dati medici dei pazienti, interfacciandosi con l'AD per un controllo rigoroso degli accessi.

Questi servizi sono fondamentali per la moderna erogazione dell'assistenza sanitaria, ma sono vulnerabili agli attacchi informatici.

Integrazione dei servizi sanitari con Active Directory

- I servizi sanitari digitali utilizzano Active Directory (AD) per l'identità. gestione e controllo degli accessi.
- I servizi di assistenza sanitaria digitale sono distribuiti in ambienti AD
- Le vulnerabilità in AD possono compromettere la sicurezza di servizi sanitari interconnessi.
- La sicurezza degli ambienti AD è impegnativa ma fondamentale per la protezione delle applicazioni sanitarie interconnesse.

Vulnerabilità intrinseche di AD che possono essere solo monitorate, non mitigate.

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.

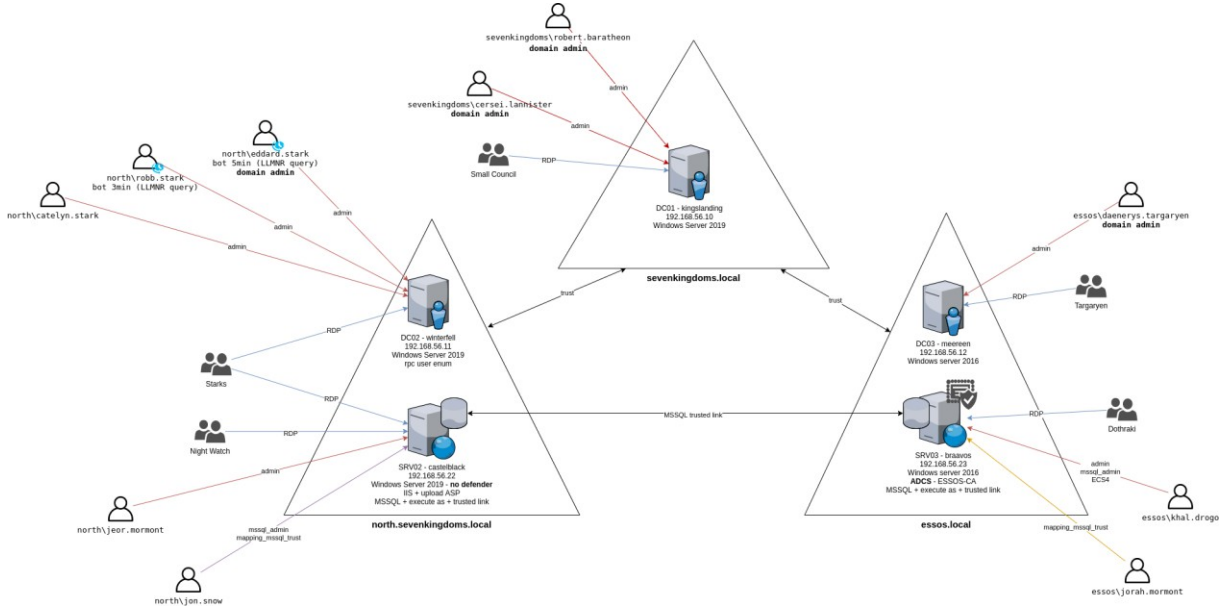
Il ruolo dell'ingegneria di rilevamento nella sicurezza informatica dell'assistenza sanitaria

- L'ingegneria di rilevamento fornisce visibilità sugli attacchi contro beni digitali della sanità.
- Il monitoraggio delle interazioni tra i sistemi sanitari e gli ambienti AD rileva tempestivamente le attività sospette.
- Gli aggiornamenti continui delle strategie di rilevamento sono fondamentali per rispondere alle minacce persistenti avanzate (APT), con strumenti come Microsoft Sentinel o altre soluzioni SIEM.

Workshop sul rilevamento di Active Directory

WORKSHOP - Introduzione all'ambiente di laboratorio

- La configurazione iniziale si basa sul software open-sou
  progetto GOAD
  - Gioco di Active Directory (GOAD)
- 3 domini:
  - sevenkingdoms - 1 controller di dominio (kingslanding)
  - essos - 1 controller di dominio (meereen), 1 server ADCS (braavos)
  - nord - 1 controller di dominio (winterfell), 1 server IIS (castelblack)



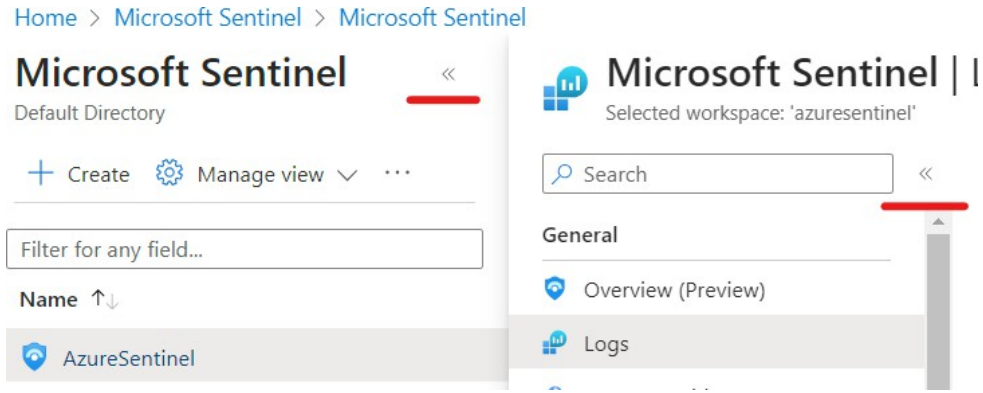
WORKSHOP - Infrastruttura Goad

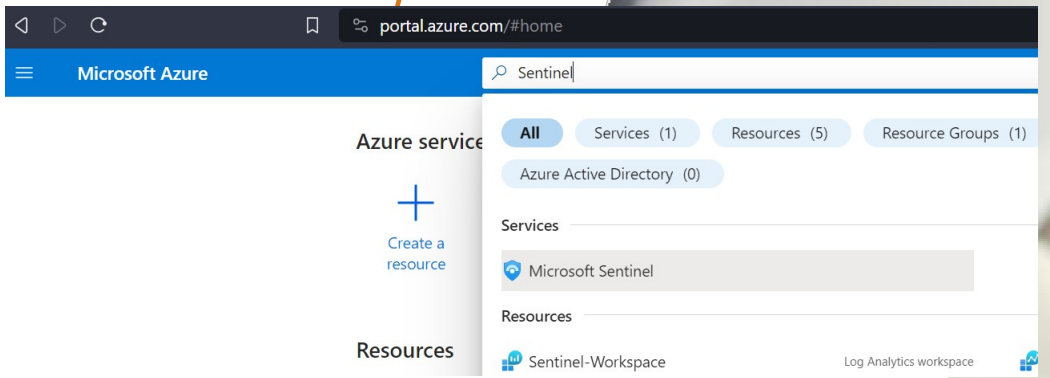
Indirizzo IP	Funzione	OS	Nome	Dominio
192.168.56.10	Dominio Windows Controllore	Server Windows 2019	dc01 - relanding	sette regni
192.168.56.11	Controllore di dominio Windows	Windows Server 2016	dc02 - winterfell	nord.sevenkingdo ms
192.168.56.12	Dominio Windows Controllore	Server Windows 2016	dc03 - meereen	essos
192.168.56.22	Server web	Windows Server 2016	srv01 - castelblack	nord.setteregni
192.168.56.23	Server ADCS	Windows Server 2016	srv02 - bravoos	essos
192.168.56.100	• Firewall • Sistema di rilevamento delle intrusioni - Suricata • Gateway predefinito • Server OpenVPN	PfSense	-	-

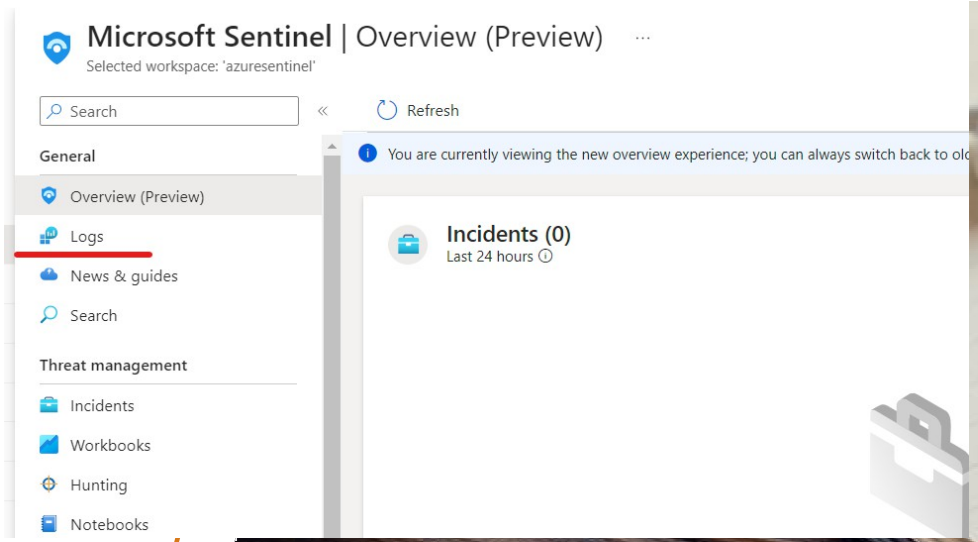
WORKSHOP

Accesso a Azure Sentinel

- Accesso Sentinel
  - Aprire una scheda privata o un profilo ospite nel browser.
  - https://portal.azure.com
  - Nome utente: [fornito] Password: [fornito]
  - Andate a cercare nella parte superiore della pagina, scrivete Sentinel e fate clic su Microsoft Sentinel.
  - Nel nome della colonna fare clic su AzureSentinel
  - Nella nuova scheda andare su Registri
  - Chiudete tutti i pop-up che appaiono e nascondete i menu per avere un'esperienza a schermo intero sui registri.



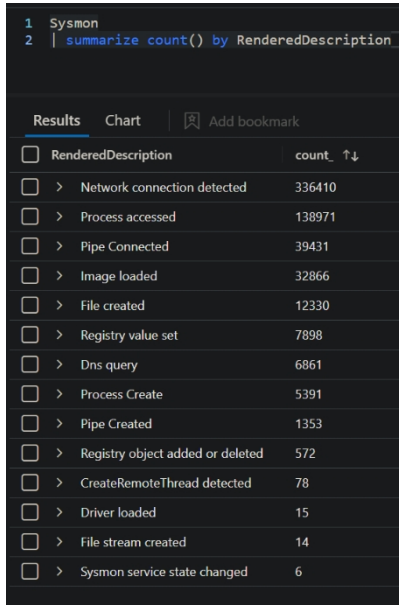


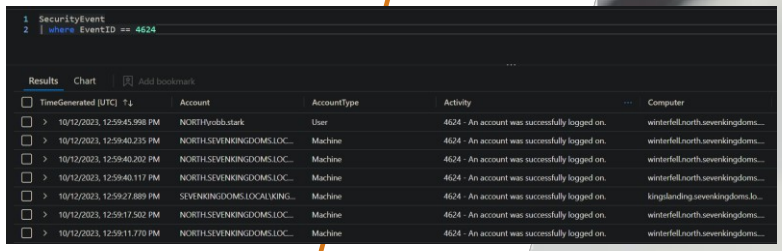


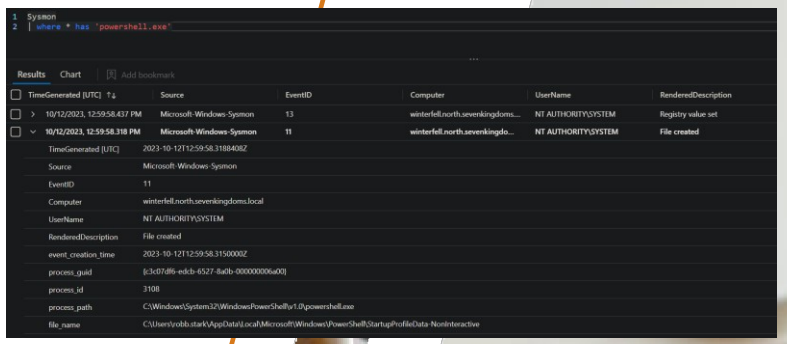
WORKSHOP

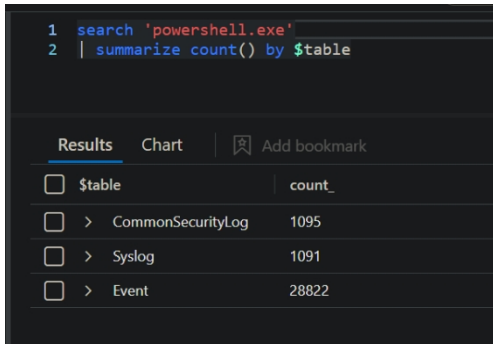
Analisi dei log con Kusto Query Language

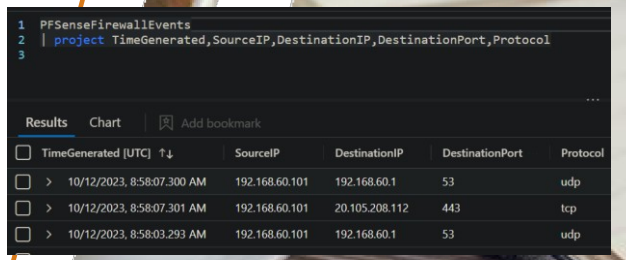
- Tabelle di eventi in ambiente di laboratorio
  - Evento di sicurezza
  - Sysmon (basato su Evento)
  - Suricata
  - PFSenseFirewallEvents
- Filtraggio degli eventi
  - Filtrare per condizione (dove)
  - Controlla se una colonna contiene una stringa (dove * ha)
  - Selezionare un sottoinsieme di colonne (progetto)
  - Elenco dei valori unici (distinti)
  - operatore di ricerca
  - Operatori sulle stringhe (==, != , ha, contiene)
- Aggregazione di eventi
  - Usare l'operatore di riepilogo (summarize)
  - Conteggio condizionato delle righe (countif())
  - Valori distinti (dcount())
  - Raggruppa i dati in bins (bin())
  - Analisi delle serie temporali (make-series)
- Visualizzazione
  - Visualizzare i risultati della query (rendering)











WORKSHOP

Caratteristiche specifiche del registro - SecurityEvent

- Fornisce informazioni di audit relative alle attività svolte sui sistemi operativi Windows.
- Tipi di eventi:
  - KQL:

    SecurityEvent| attività distinta
- Per ulteriori informazioni su ciascun tipo di registro, consultare i seguenti link
  - Eventi del registro di sicurezza di Windows

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)

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.

WORKSHOP

Utilizzo di MITRE ATT&CK per l'ingegneria del rilevamento - SecurityEvent

- Tipo di tattica ATT&CK rilevata
  - Accesso alle credenziali
    - Forza bruta (ID evento: 4625 o 5379)
    - Rubare o falsificare i biglietti Kerberos: Kerberoasting (ID evento: 4769)
    - Dumping delle credenziali del sistema operativo: DCSync (ID evento: 4662)
  - Esecuzione
    - Interprete di comandi e scripting: di Windows Command Shell (ID evento: 4688)
    - Servizi di sistema (ID evento: 4697)
  - Persistenza
    - Attività pianificata/lavoro (ID evento: 4698 e 4700)
    - Servizi di sistema (ID evento: 4697)
  - Escalation dei privilegi
    - Modifica dei criteri di gruppo (ID evento: 5136, 5137, 5141)
  - Movimento laterale
    - Protocollo desktop remoto (RDP) (ID evento: 4624)
  - Difesa Evasione
    - Utilizzare materiale di autenticazione alternativo: Passare l'hash (ID evento: 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

Caratteristiche specifiche dei log - Sysmon

- Sysmon è abilitato su tutti gli host Windows
  - Fornisce visibilità a livello di endpoint
- Tipi di eventi:
  - KQL:

    Sysmon| distinto RenderedDescription
- Per ulteriori informazioni su ciascun tipo di registro, consultare i seguenti link
  - Tipi di log Sysmon
  - Eventi del registro di sicurezza di 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.

WORKSHOP

Utilizzo di MITRE ATT&CK per l'ingegneria del rilevamento - Sysmon

- Tipo di tattica ATT&CK rilevata
  - Accesso iniziale
    - Phishing
    - Compromesso in corsa
  - Esecuzione
    - Interprete di comandi e scripting
    - Esecuzione da parte dell'utente
  - Persistenza
    - Attività pianificata/lavoro
    - Flusso di esecuzione del dirottamento: caricamento laterale di DLL
    - Componente software del server: Guscio Web
  - Difesa Evasione
    - Disattivare o modificare gli strumenti
    - File o informazioni offuscate
  - Accesso alle credenziali
    - Dumping delle credenziali del sistema operativo
- Scoperta
  - Scoperta delle informazioni di sistema
  - Registro delle interrogazioni
- Movimento laterale
  - Protocollo desktop remoto
  - Trasferimento laterale degli utensili
- Impatto
  - Distruzione dei dati
  - Pulizia del disco
- Collezione
  - Dati del sistema locale
  - Dati da supporti rimovibili
- Esfiltrazione
  - Esfiltrazione attraverso il canale 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.

WORKSHOP

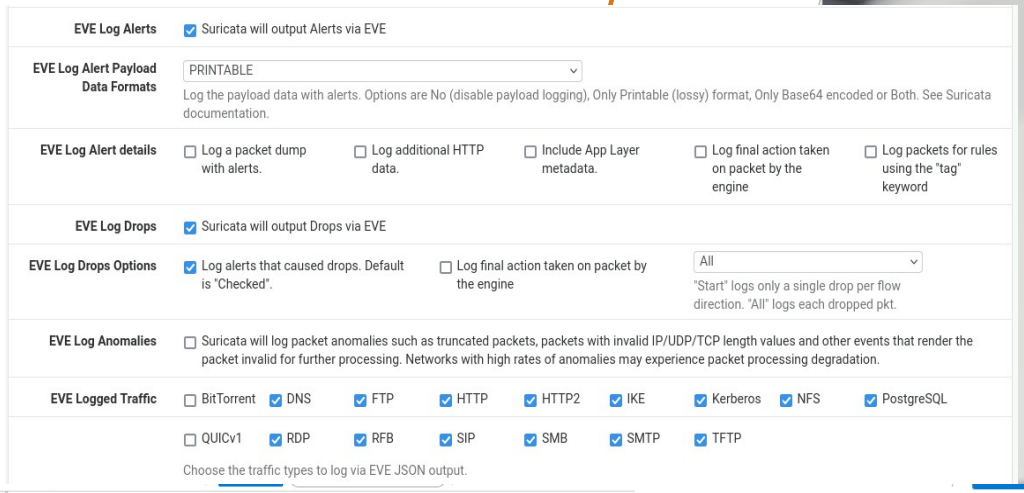
Caratteristiche specifiche del tronco - Suricata

- La registrazione di Suricata è abilitata
  - Fornisce un'eccellente visibilità a livello di rete
  - Oltre agli avvisi, può anche produrre registri basati su un traffico specifico, ad esempio HTTP

- Tipi di eventi:
  - KQL:

    Suricata| distinto tipo_evento
    | dove tipo_evento != ''

- Estensione
  - È possibile estrarre informazioni aggiuntive da colonne specifiche in base ai tipi di eventi.

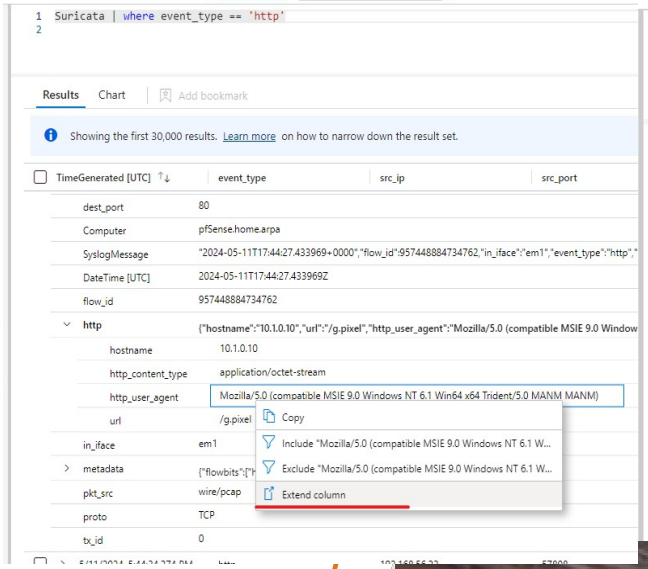



```
1  Suricata | where event_type == 'http'
2  | extend http_user_agent_ = tostring(http.http_user_agent)
```

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




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

Results | Chart | Add bookmark

event_type
http
tls
fileinfo
smb
dns
alert
krb5

WORKSHOP

Esempi - Esecuzione dell'avvio automatico all'avvio o al logon: Tasti di esecuzione del registro / Cartella di avvio

Esecuzione dell'avvio automatico all'avvio o al logon: Tasti di esecuzione del Registro di sistema / Cartella di avvio

- La collocazione di un programma all'interno di una cartella di avvio ne determina l'esecuzione anche al momento dell'dell'utente. Esiste una posizione della cartella di avvio per i singoli account utente e una cartella di avvio a livello di sistema che viene controllata indipendentemente dall'account utente che accede.
- Il percorso della cartella di avvio per l'utente corrente è **C:\Users\[Nome utente]\AppData\Roaming\Microsoft\Windows\Start Menu/Programmi/Avvio**.
- Il percorso della cartella di avvio per tutti gli utenti è **C:\ProgramData\Microsoft\Windows\Start Menu\Programmi\StartUp**.

Passi da seguire per creare la logica alla base del rilevamento

D: Quale tipo di dati ci fornirà queste informazioni? R: Sysmon

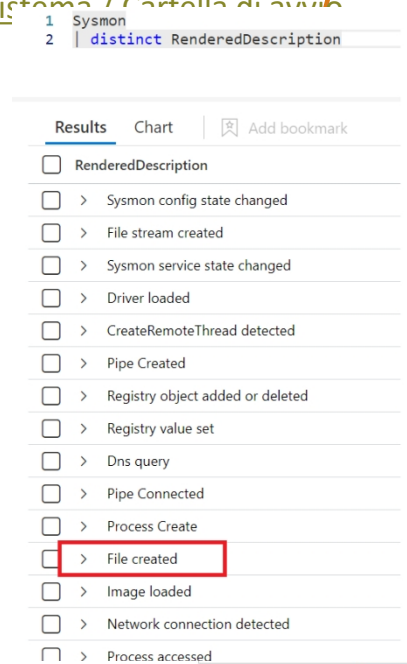
D: Che tipo di evento vogliamo dalla tabella dati di Sysmon? R: File creato

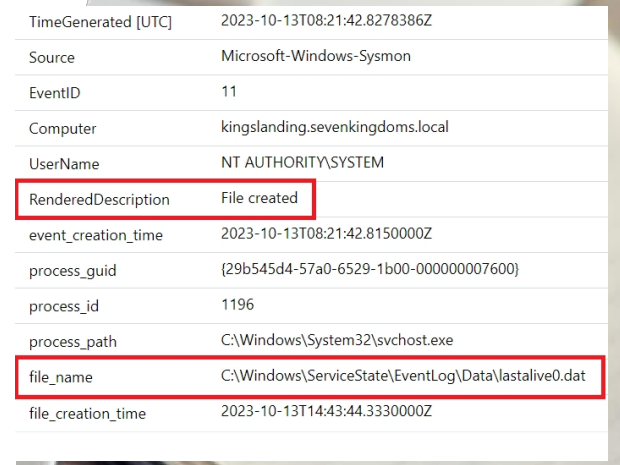
D: Il rilevamento è basato sugli eventi o sui volumi? R: Basato sugli eventi

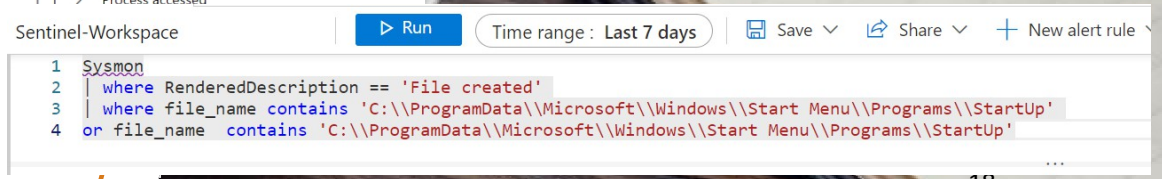
D: Quali colonne sono importanti per poterle utilizzare come filtri? R: Descrizione renderizzata, nome_file

D: Quale filtro inserire nelle colonne importanti:
R: 1. Descrizione resa uguale a "File creato".
2. Il nome del file contiene '\AppData\\Roaming\Microsoft\Windows\Start Menu\Programmi\Startup' o nome del file contiene 'C:´ProgramData´´Microsoft´´Windows´´Start Menu´´Programs´´StartUp´´.

*Suggerimento per la sintassi del KQL: sostituire \ con \ perché il backslash è usato per sfuggire ai caratteri.







WORKSHOP

Esempi - Esfiltrazione tramite servizio web

Esfiltrazione tramite servizio web

- Gli avversari possono utilizzare un servizio Web esterno esistente e legittimo per esfiltrare i dati piuttosto che il loro canale primario di comando e controllo. I servizi Web più diffusi che fungono da meccanismo di esfiltrazione possono offrire una copertura significativa grazie alla probabilità che gli host all'interno di una rete stiano già comunicando con loro prima della compromissione. Potrebbero anche esistere regole di firewall che consentono il traffico verso questi servizi.
- Anche i fornitori di servizi Web utilizzano comunemente la crittografia SSL/TLS, offrendo agli avversari un ulteriore livello di protezione.

Passi da seguire per creare la logica alla base del rilevamento

D: Quale tipo di dati ci fornirà queste informazioni? R: Sysmon o
PFSenseFirewallEvents

D: Da queste due tabelle di dati, quale fornisce informazioni sul numero di byte trasferiti?
PFSenseFirewallEvents

D: Il rilevamento è basato sugli eventi o sui volumi? R:
Basato sul volume

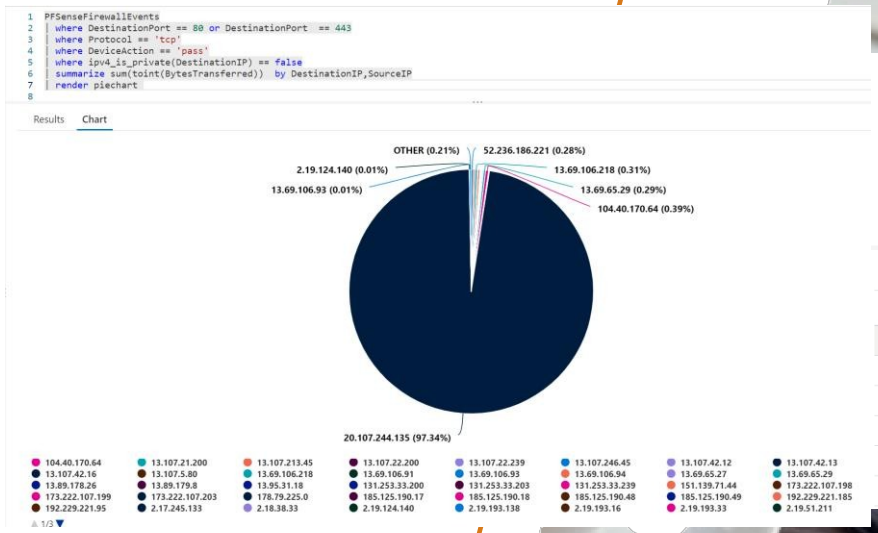
D: Quale funzione del SIEM è importante per i rilevamenti basati sui volumi? R:
Aggregazione degli eventi (riepilogo)

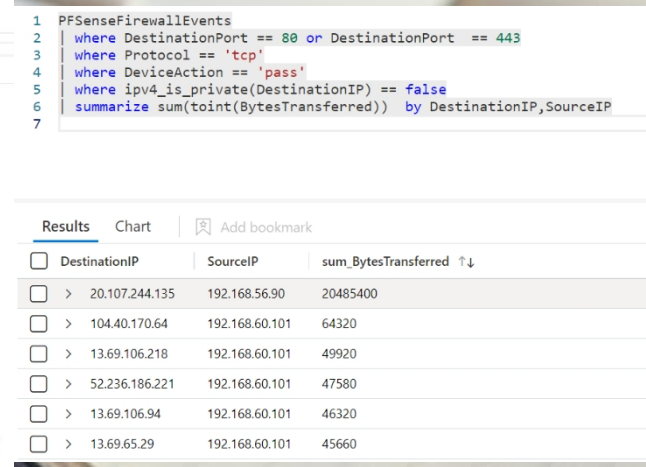
D: Quali colonne sono importanti per poterle utilizzare come filtri?
R: Porta di destinazione, Protocollo, DeviceAction e IP di destinazione devono essere pubblici.

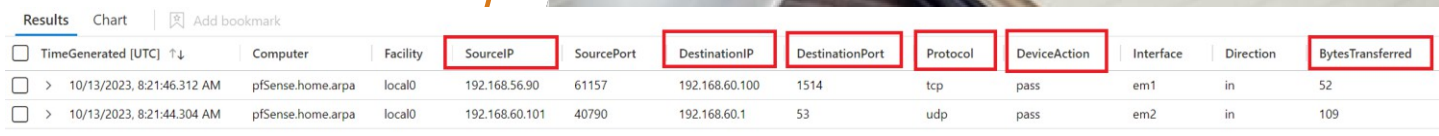
D: Quali colonne sono importanti per l'aggregazione? R: IP di
origine, IP di destinazione, Byte trasferiti

D: Come dobbiamo aggregare i risultati?
R: Sommando i BytesTransferred per IP di destinazione e di origine.

D (BONUS) : È meglio visualizzare i risultati dell'aggregazione come dati o come grafici?







WORKSHOP

Esempi - Scoperta dell'account: Account di dominio

- Scoperta dell'account: Account di dominio
  - Gli avversari possono cercare di ottenere un elenco degli account di dominio. Queste informazioni possono aiutare gli avversari a determinare quali account di dominio esistono per favorire un comportamento successivo, come prendere di mira account specifici che possiedono privilegi particolari.
  - Scopre i nomi utente validi interrogando a forza bruta i nomi utente probabili su un servizio Kerberos. Quando viene richiesto un nome utente non valido, il server risponde utilizzando il codice di errore Kerberos KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN, consentendo di determinare che il nome utente non è valido. I nomi utente validi implicano il TGT in una risposta AS-REP o l'errore KRB5KDC_ERR_PREAUTH_REQUIRED, che segnala che l'utente deve eseguire una pre-autenticazione.
  - Strumenti: krbrute, nmap, crackmapexec

- Passi da seguire per creare la logica alla base del rilevamento - Livello endpoint

D: Quale tipo di dati ci fornirà queste informazioni? R: Eventi di sicurezza

D: Che tipo di evento vogliamo dalla tabella di dati SecurityEvents?
R: 4768 - È stato richiesto un ticket di autenticazione Kerberos (TGT).

D: Il rilevamento è basato sugli eventi o sui volumi? R:
Basato sul volume

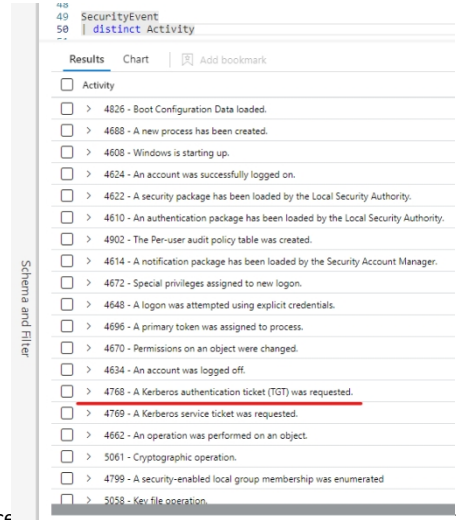
D: Quale funzione del SIEM è importante per i rilevamenti basati sui volumi? R:
Aggregazione degli eventi (riepilogo)

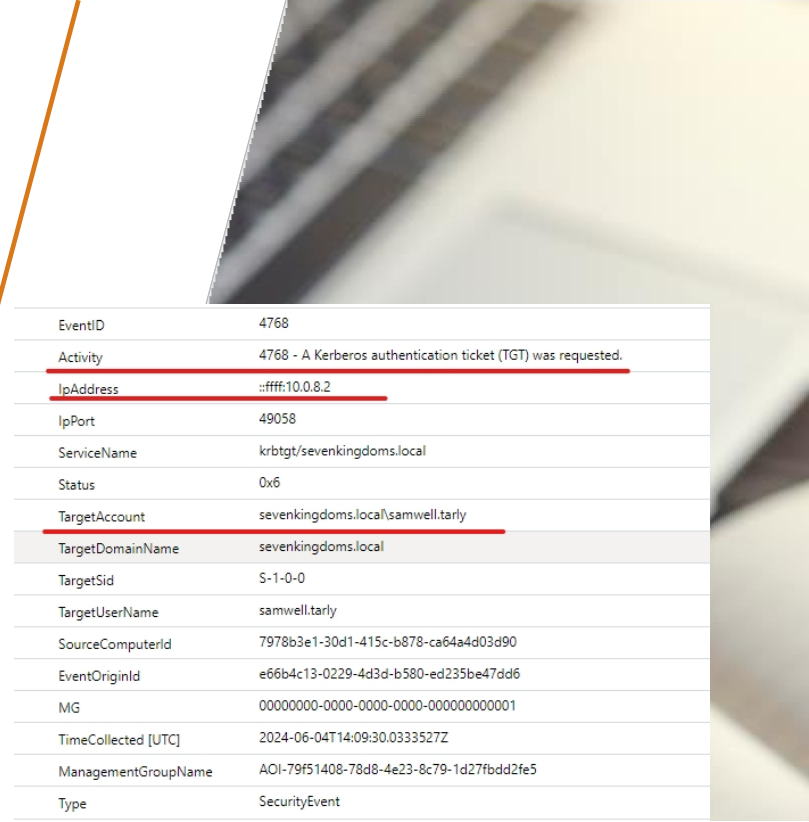
D: Quali colonne sono importanti per poterle utilizzare come filtri? R:
Attività

D: Quali colonne sono importanti per l'aggregazione?
A: IpAddress, TargetAccount, TimeGenerated

D: Come dobbiamo aggregare i risultati?
R: Il campo dell'indirizzo IP è quello da cui provengono le richieste di ticket Kerberos. Si cercano quindi gli indirizzi IP con richieste di ticket Kerberos per più account diversi.

D (BONUS) : È meglio visualizzare i risultati dell'aggregazione come dati o come grafici? R: Grafici (rendering di grafici a colonne)



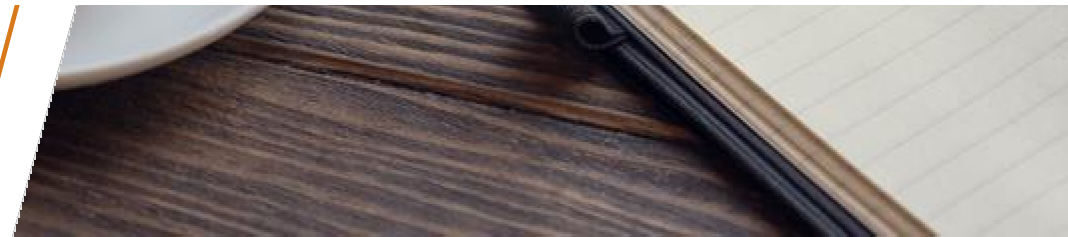


EventID	4768
Activity	4768 - A Kerberos authentication ticket (TGT) was requested.
IpAddress	::ffff:10.0.8.2
IpPort	49058
ServiceName	krbtgt/sevenkingdoms.local
Status	0x6
TargetAccount	sevenkingdoms.local\samwell.tarly
TargetDomainName	sevenkingdoms.local
TargetSid	S-1-0-0
TargetUserName	samwell.tarly
SourceComputerId	7978b3e1-30d1-415c-b878-ca64a4d03d90
EventOriginId	e66b4c13-0229-4d3d-b580-ed235be47dd6
MG	00000000-0000-0000-0000-000000000001
TimeCollected [UTC]	2024-06-04T14:09:30.0333527Z
ManagementGroupName	AOI-79f51408-78d8-4e23-8c79-1d27fbdd2fe5
Type	SecurityEvent

```
SecurityEvent
| where Activity == "4768 - A Kerberos authentication ticket (TGT) was requested."
| summarize dcount(TargetAccount),make_set(TargetAccount) by IpAddress,bin(TimeGenerated,1h),Activity
```

esults Chart Add bookmark

IpAddress	TimeGenerated [UTC]	Activity	dcount_TargetAccount	set_TargetAccount
::ffff:10.0.8.2	6/4/2024, 2:00:00.000 PM	4768 - A Kerberos authenticati...	152	["sevenkingdoms.local\\nmap","seve
::1	6/4/2024, 1:00:00.000 PM	4768 - A Kerberos authenticati...	8	["SEVENKINGDOMS.LOCAL\\KINGSL
::1	6/4/2024, 11:00:00.000 AM	4768 - A Kerberos authenticati...	8	["SEVENKINGDOMS.LOCAL\\KINGSL
::ffff:192.168.56.22	6/4/2024, 1:00:00.000 PM	4768 - A Kerberos authenticati...	5	["north.sevenkingdoms.local\\CASTE
::ffff:192.168.56.22	6/4/2024, 11:00:00.000 AM	4768 - A Kerberos authenticati...	5	["north.sevenkingdoms.local\\sql_sv
::1	6/4/2024, 12:00:00.000 PM	4768 - A Kerberos authenticati...	3	["NORTH\\robb.stark","NORTH\\edd
::ffff:192.168.56.23	6/4/2024, 1:00:00.000 PM	4768 - A Kerberos authenticati...	3	["ESSOS.LOCAL\\BRAAVOS$","essos.l



WORKSHOP

Esempi - Forza bruta: Spruzzatura di password

Forza bruta: Spruzzatura di password

- Gli avversari possono utilizzare una singola password o un piccolo elenco di password comunemente utilizzate per molti account diversi, nel tentativo di acquisire credenziali valide. Il password spraying utilizza una password (ad esempio, "Password01"), o un piccolo elenco di password comunemente utilizzate, che può corrispondere alla politica di complessità del dominio. Con questa password vengono tentati accessi a **molti account diversi** sulla rete per evitare i blocchi degli account che normalmente si verificherebbero con il brute forcing di un singolo account con molte password.

Passi da seguire per creare la logica alla base del rilevamento

D: Quale tipo di dati ci fornirà queste informazioni? R: Eventi di sicurezza

D: Che tipo di evento vogliamo dalla tabella dati SecurityEvents? R: 4625 - Un account non è riuscito ad accedere.

D: Il rilevamento è basato sugli eventi o sui volumi?
A: Basato sul volume

D: Quale funzione del SIEM è importante per i rilevamenti basati sui volumi? R: Aggregazione degli eventi (riepilogo)

D: Quali colonne sono importanti per poterle utilizzare come filtri?
R: In realtà nessuna. Filtrando per l'EventID 4625 abbiamo il set di dati che vogliamo analizzare.

D: Quali colonne sono importanti per l'aggregazione? R: Indirizzo IPA, Conto.

D: Come dobbiamo aggregare i risultati?
R: Il campo dell'indirizzo IP è il luogo in cui si verificano gli accessi non riusciti. Quindi, cerchiamo gli indirizzi IP con più accessi falliti con account diversi. *

D (BONUS) : È meglio visualizzare i risultati dell'aggregazione come dati o come grafici? R: Grafici

*Registrazione dell'autenticazione del dominio:

Alcuni protocolli, come NTLM, richiedono una configurazione aggiuntiva per fornire l'IP di origine dell'autenticazione fallita.

```
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.

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

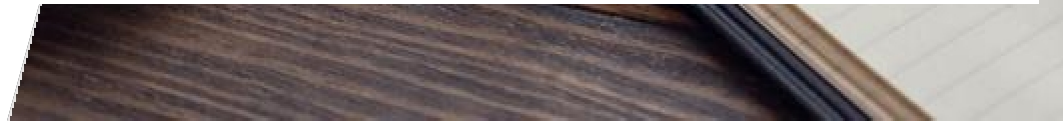
Results | Chart | Add bookmark

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"]



WORKSHOP

Esempi - Componente software del server: Guscio Web

- Componente software del server: Guscio Web
  - Una shell Web è uno script Web che **viene inserito** in un server Web apertamente accessibile per consentire a un avversario di accedere al server Web gateway in una rete. Una shell Web **può fornire una serie di funzioni da eseguire** o un'**interfaccia a riga di comando** sul sistema che ospita il server Web.
  - **Il monitoraggio dei file** può essere utilizzato per rilevare le modifiche ai file nella **directory Web di un server Web** che non corrispondono agli aggiornamenti del contenuto del server Web e possono indicare l'installazione di uno script di shell Web.

- Passi da seguire per creare la logica dietro il rilevamento - Creazione del file

  D: Quale tipo di dati ci fornirà queste informazioni? R: Sysmon

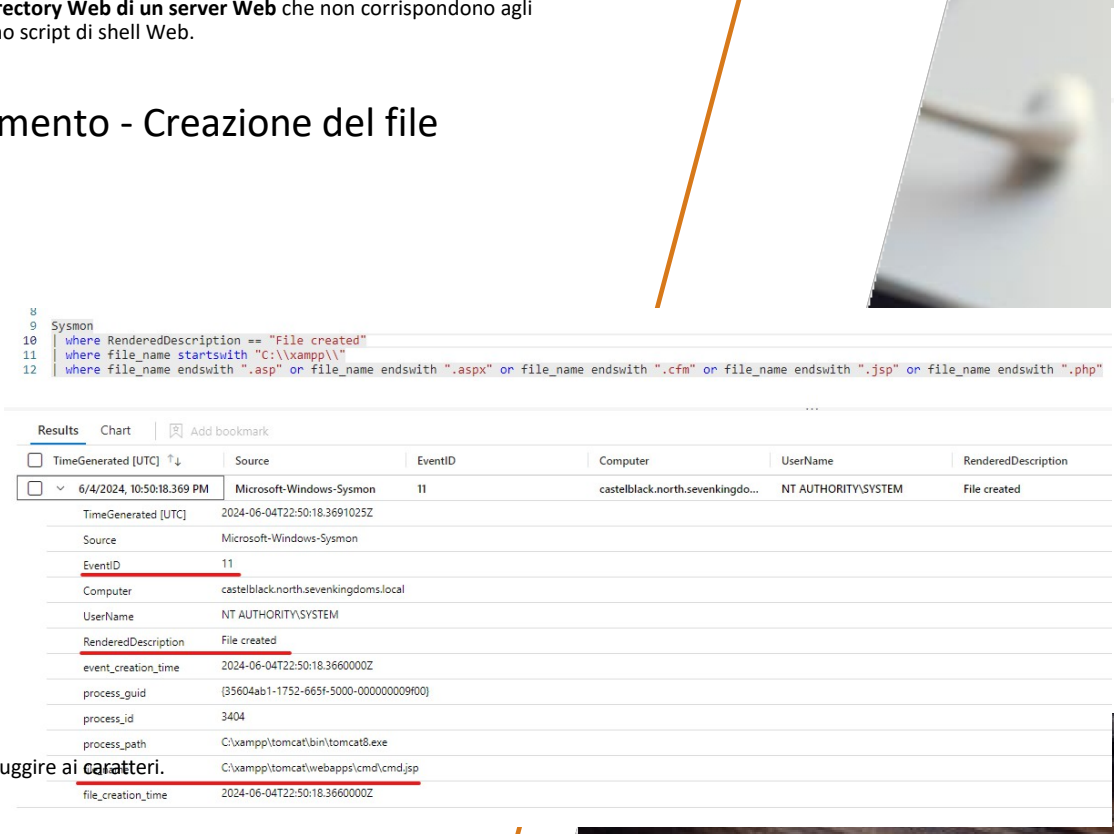
  D: Che tipo di evento vogliamo dalla tabella dei dati Sysmon?
  R: File creato

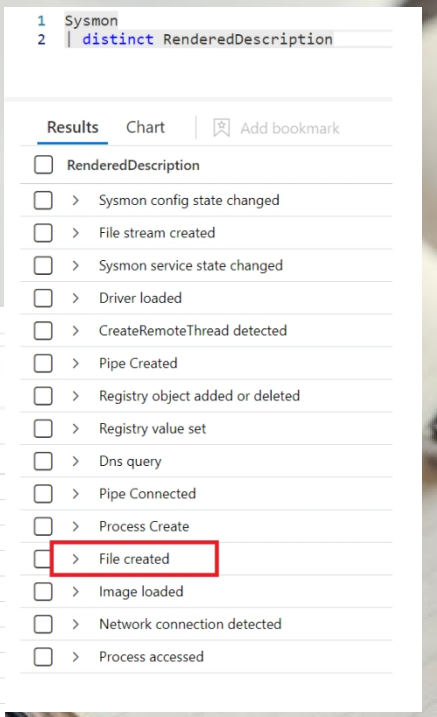
  D: Il rilevamento è basato sugli eventi o sui volumi? R:
  Basato sugli eventi

  D: Quali colonne sono importanti per poterle utilizzare come filtri? R:
  Descrizione renderizzata, nome_file
  La colonna nome_file visualizza il file creato con il percorso completo.

  D: Quale filtro inserire nelle colonne importanti:
  R: 1. Descrizione resa uguale a "File creato".
  2. nome_file inizia con {directory del server web}
  3. Il nome del file termina con {estensione del file di webshell}.
  (Suggerimento: estensioni di file Webshell comuni: php, asp, aspx, cfm, jsp)

*Suggerimento per la sintassi del KQL: sostituire \ con \ perché il backslash è usato per sfuggire ai caratteri.





WORKSHOP

Esempi - Componente software del server: Guscio Web

- Componente software del server: Guscio Web
  - Una shell Web è uno script Web che **viene inserito** in un server Web apertamente accessibile per consentire a un avversario di accedere al server Web gateway in una rete. Una shell Web **può fornire una serie di funzioni da eseguire** o un'**interfaccia a riga di comando** sul sistema che ospita il server Web.
  - **Il monitoraggio dei processi** può essere utilizzato per rilevare i server Web che eseguono azioni sospette, come la generazione di cmd.exe o l'accesso a file non presenti nella directory Web.
  - Una shell Web è uno script Web collocato su un server Web apertamente accessibile per consentire a un avversario di utilizzare il server come gateway in una rete. Durante il funzionamento della shell, i **comandi vengono emessi dall'interno dell'applicazione Web nel sistema operativo del server più ampio**.

- Passi da seguire per creare la logica dietro il rilevamento - Creazione del processo

D: Quale tipo di dati ci fornirà queste informazioni?
A: Sysmon

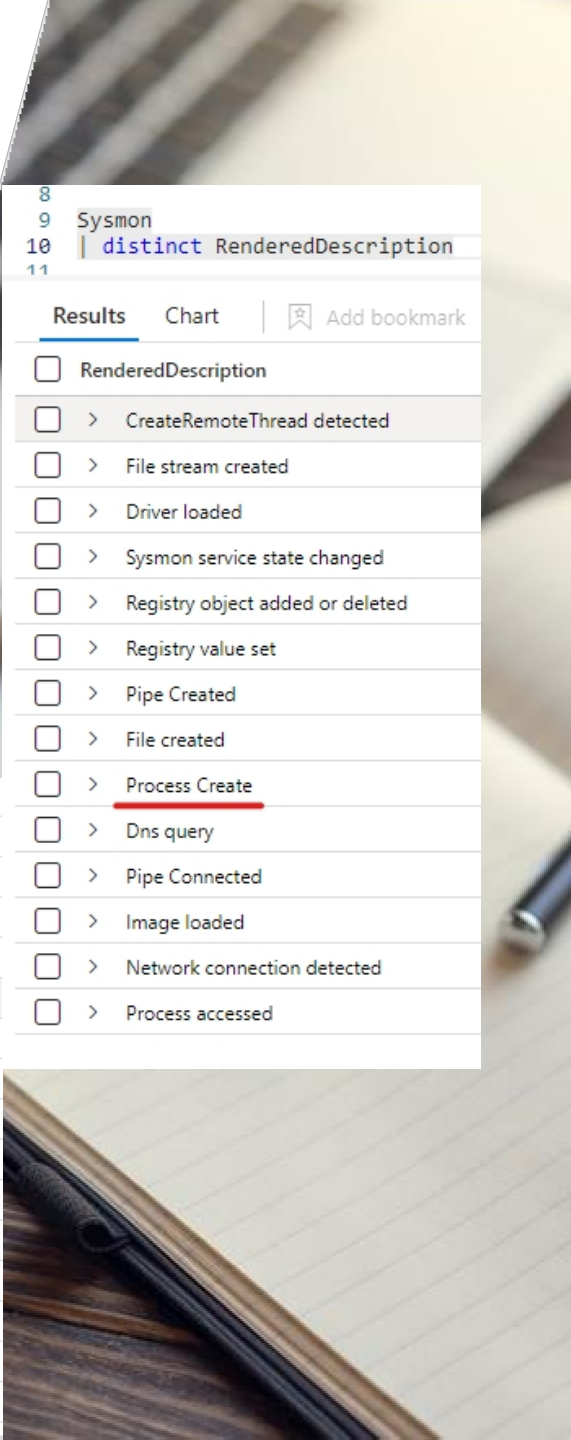
D: Che tipo di evento vogliamo dalla tabella dei dati Sysmon? R:
Creazione di un processo

D: Il rilevamento è basato sugli eventi o sui volumi? R:
Basato sugli eventi

D: Quali colonne sono importanti per poterle utilizzare come filtri?
A: Descrizione resa, process_parent_command_line, process_command_line Processi della riga di comando che vengono eseguiti dai processi del server web
è un indicatore elevato dell'esecuzione di Web Shell.

D: Quale filtro inserire nelle colonne importanti:
R: 1. La descrizione resa è uguale a "Processo di creazione".
2. process_parent_command_line contiene processi comuni del server web
3. process_command_line contiene processi comuni a riga di comando
(Suggerimento: processi comuni del server Web: w3wp.exe, httpd.exe, tomcat.exe, nginx.exe)
(Suggerimento2: processi comuni della riga di comando: cmd, powershell, netstat, systeminfo, ipconfig, whoami ecc.)

*Suggerimento per la sintassi del KQL: sostituire \ con \ perché il backslash è usato per sfuggire ai caratteri.



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

WORKSHOP

Esempi - Componente software del server: Guscio Web

- Componente software del server: Guscio Web
  - Una shell Web è uno script Web che **viene inserito** in un server Web apertamente accessibile per consentire a un avversario di accedere al server Web gateway in una rete. Una shell Web **può fornire una serie di funzioni da eseguire** o un'**interfaccia a riga di comando** sul sistema che ospita il server Web.
  - Monitorare e analizzare **i modelli di traffico e l'ispezione dei pacchetti** associati ai protocolli che non seguono gli standard di protocollo e i flussi di traffico previsti (ad esempio pacchetti estranei che non appartengono ai flussi stabiliti, modelli di traffico gratuiti o anomali, sintassi o struttura anomale).

- Passi da seguire per creare la logica dietro il rilevamento - Traffico di rete

Contenuto

D: Quale tipo di dati ci fornirà queste informazioni? R: Suricata

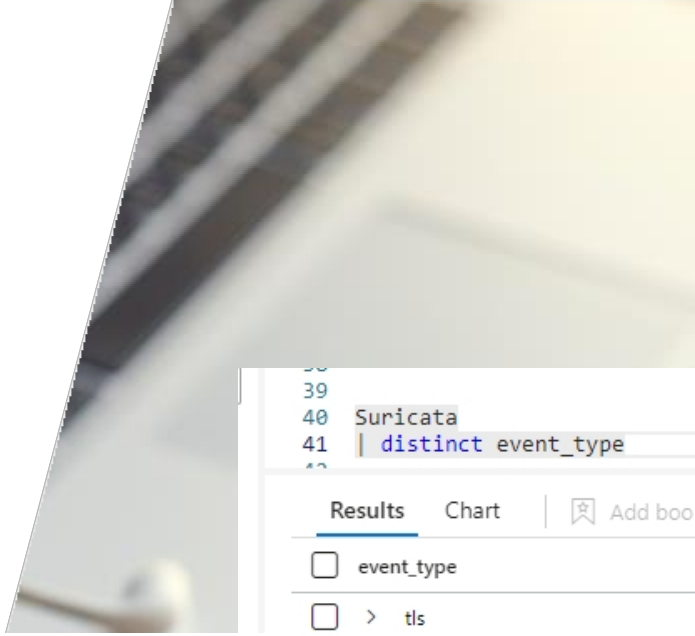
D: Che tipo di evento vogliamo dalla tabella dati di Sysmon? R:
Tipo_evento > http

D: Il rilevamento è basato sugli eventi o sui volumi? R:
Basato sugli eventi

D: Quale campo annidato è importante all'interno dell'elemento http?
A: url
Alcune shell Web funzionano ricevendo i comandi sospetti come parametri nell'URL

D: Quale filtro inserire nelle colonne importanti? R: 1. il
tipo di evento è uguale a 'http'.
2. l'url contiene uno qualsiasi dei comandi sospetti

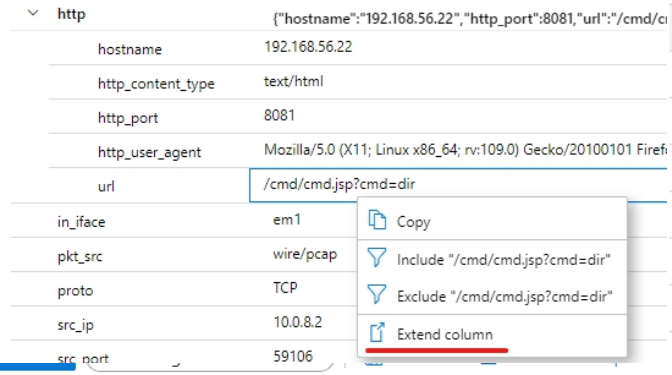
D: Suricata ha prodotto qualche segnalazione relativa a questa attività?
A: Suricata| dove event_type== 'alert' e app_proto== 'http'



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

Results | Chart | Add boo

event_type
tls
smb
dns
krb5
fileinfo
http
alert
rdp




```
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

WORKSHOP

Esempi - Componente software del server: Guscio Web

- Rubare o falsificare i biglietti Kerberos: Arrosto AS-REP

  Gli avversari possono rivelare le credenziali degli account che hanno disattivato **la preautenticazione Kerberos** mediante messaggi Kerberos Password Cracking. Per ogni account trovato senza preautenticazione, un avversario può inviare un messaggio AS-REQ senza il timestamp crittografato e **ricevere un messaggio AS-REP con i dati TGT che possono essere crittografati con un algoritmo non sicuro come RC4**. I dati crittografati recuperati possono essere vulnerabili agli attacchi offline di Password Cracking in modo simile a Kerberoasting ed esporre le credenziali in chiaro.
  Un account registrato in un dominio, con o senza privilegi speciali, può essere abusato per elencare tutti gli account di dominio che hanno la preautenticazione disabilitata utilizzando strumenti Windows come PowerShell con un filtro LDAP**. In alternativa, l'avversario può inviare un messaggio AS-REQ per ogni utente. Se il DC risponde senza errori, l'account non richiede la preautenticazione e il messaggio AS-REP conterrà già i dati crittografati.**

- Passi da seguire per creare la logica alla base del rilevamento

  D: Quale tipo di dati ci fornirà queste informazioni? R: Suricata

  D: Che tipo di evento vogliamo dalla tabella dati di Sysmon? R:
  Tipo_evento > krb5

  D: Il rilevamento è basato sugli eventi o sui volumi? R:
  Basato sugli eventi

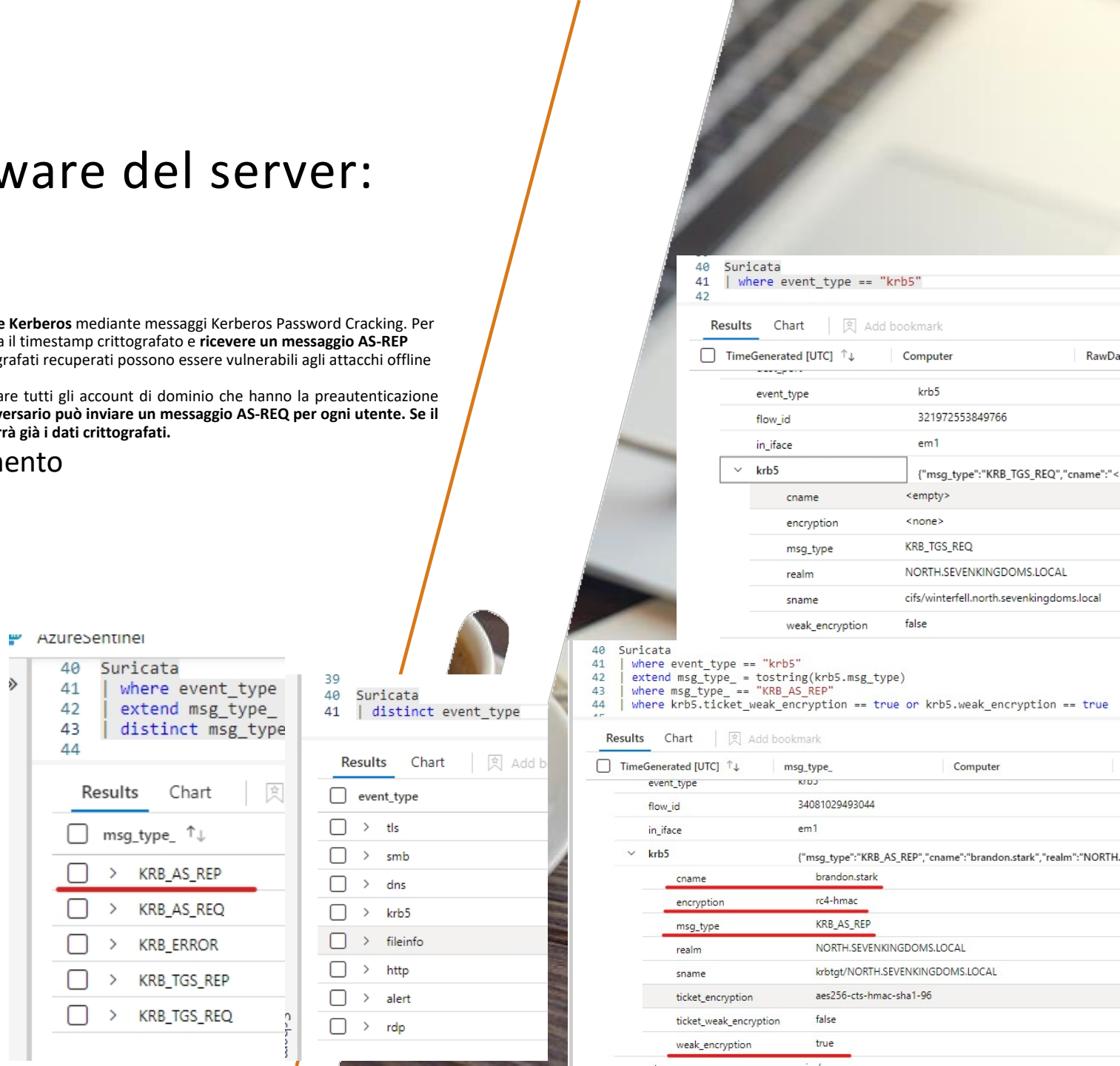
  D: Quale campo annidato è importante all'interno dell'elemento krb5? A: msg_type, weak_encryption, ticket_weak_encryption

  D: Quali colonne sono importanti per poterle utilizzare come filtri?
  A: event_type, msg_type_ , weak_encryption_, ticket_weak_encryption_

  D: Quale filtro inserire nelle colonne importanti:
  A: 1. tipo_evento= krb5
  2. ticket_weak_encryption_= true o weak_encryption_= true

  D: Qual è l'account che è esposto e vulnerabile all'attacco AS-REP Roasting? R: cname colonna annidata > brandon.stark

  D: Qual è la colonna che mostra l'origine dell'attacco? R: src_ip > 10.0.8.2



Grazie per l'attenzione

Presentazione a cura di:

Christos Lazaridis (Punto focale)

CyberSecPro