

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Ingegneria di rilevamento su un raggio d'azione cibernetico - AD

CSP011_W

GESTIONE DEGLI ELEMENTI ESSENZIALI DI CYBERSECURITY, STRUMENTI E TECNOLOGIE DI CYBERSECURITY

CHRISTOS LAZARIDIS



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



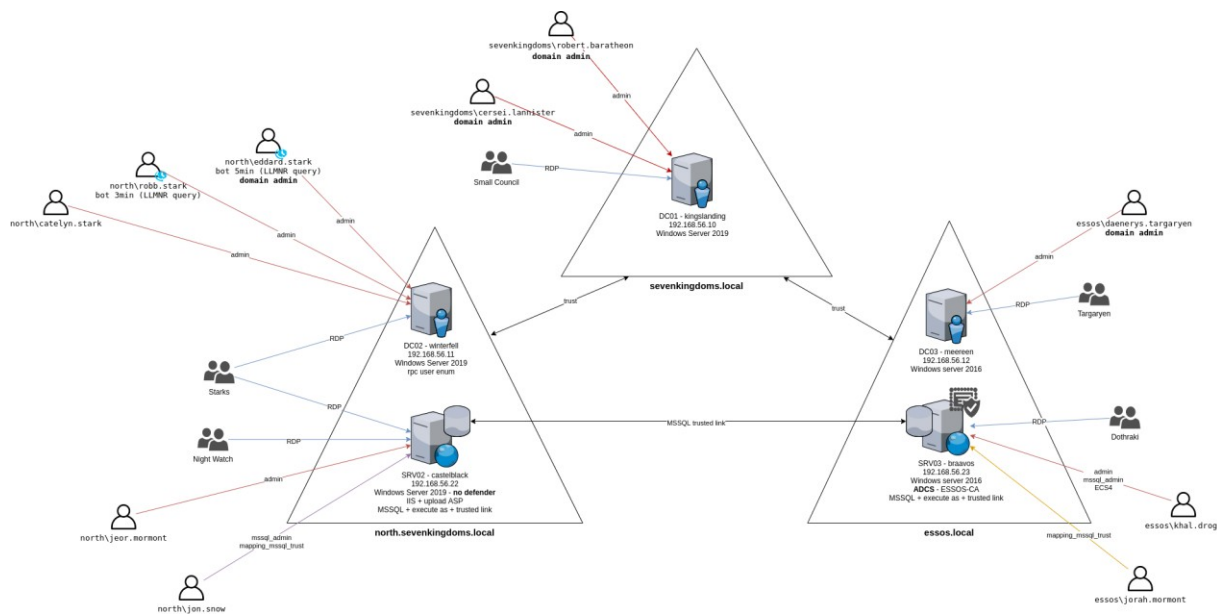
Funded by
the European Union

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

WORKSHOP - Introduzione all'ambiente di laboratorio

- La configurazione iniziale si basa sul software open source 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	<ul style="list-style-type: none">• 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.

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel

Default Directory

+ Create ⚙️ Manage view ⌵ ⋮

Filter for any field...

Name ↑↓

AzureSentinel

Microsoft Sentinel | I

Selected workspace: 'azuresentinel'

Search

General

Overview (Preview)

Logs

The image shows two screenshots of the Microsoft Azure portal. The top screenshot shows the search bar with 'Sentinel' entered, and the search results for 'Microsoft Sentinel' are displayed. The bottom screenshot shows the 'Microsoft Sentinel | Overview (Preview)' page, which includes a search bar, a refresh button, and a list of navigation options: Overview (Preview), Logs, News & guides, Search, Threat management, Incidents, Workbooks, Hunting, and Notebooks. The 'Incidents (0)' section is highlighted, showing 'Last 24 hours'.

WORKSHOP

Analisi dei log con Kusto Query Language

- Tabelle di eventi in ambiente di laboratorio
 - Evento di sicurezza
 - Sysmon (basato su Evento)
 - Suricata
 - Eventi PFSenseFirewall
- 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
 - [Utilizzare 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)

```
1 Sysmon
2 | summarize count() by RenderedDescription
```

RenderedDescription	count_ ↑↓
> Network connection detected	336410
> Process accessed	138971
> Pipe Connected	39431
> Image loaded	32866
> File created	12330
> Registry value set	7898
> Dns query	6861
> Process Create	5391
> Pipe Created	1353
> Registry object added or deleted	572
> CreateRemoteThread detected	78
> Driver loaded	15
> File stream created	14
> Sysmon service state changed	6

```
1 SecurityEvent
2 | where EventID == 4624
```

TimeGenerated [UTC] ↑↓	Account	AccountType	Activity	Computer
> 10/12/2023, 12:59:45.998 PM	NORTH\yobba.stak	User	4624 - An account was successfully logged on.	winterfell.north.sevenkingdoms...
> 10/12/2023, 12:59:40.235 PM	NORTH.SEVENKINGDOMS.LOC...	Machine	4624 - An account was successfully logged on.	winterfell.north.sevenkingdoms...
> 10/12/2023, 12:59:40.202 PM	NORTH.SEVENKINGDOMS.LOC...	Machine	4624 - An account was successfully logged on.	winterfell.north.sevenkingdoms...
> 10/12/2023, 12:59:40.117 PM	NORTH.SEVENKINGDOMS.LOC...	Machine	4624 - An account was successfully logged on.	winterfell.north.sevenkingdoms...
> 10/12/2023, 12:59:27.889 PM	SEVENKINGDOMS.LOCAL\KING...	Machine	4624 - An account was successfully logged on.	kingoflandings.sevenkingdoms.lo...
> 10/12/2023, 12:59:17.502 PM	NORTH.SEVENKINGDOMS.LOC...	Machine	4624 - An account was successfully logged on.	winterfell.north.sevenkingdoms...
> 10/12/2023, 12:59:11.770 PM	NORTH.SEVENKINGDOMS.LOC...	Machine	4624 - An account was successfully logged on.	winterfell.north.sevenkingdoms...

```
1 Sysmon
2 | where * has 'powershell.exe'
```

TimeGenerated [UTC] ↑↓	Source	EventID	Computer	UserName	RenderedDescription
> 10/12/2023, 12:59:58.437 PM	Microsoft Windows-Sysmon	13	winterfell.north.sevenkingdoms...	NT AUTHORITY\SYSTEM	Registry value set
> 10/12/2023, 12:59:58.318 PM	Microsoft Windows-Sysmon	11	winterfell.north.sevenkingdo...	NT AUTHORITY\SYSTEM	File created

TimeGenerated [UTC] 2023-10-12T12:59:58.3180000Z
Source Microsoft Windows-Sysmon
EventID 11
Computer winterfell.north.sevenkingdoms.local
UserName NT AUTHORITY\SYSTEM
RenderedDescription File created
event_creation_time 2023-10-12T12:59:58.3150000Z
process_guid {c3c07d96-eddb-6527-846b-000000000000}
process_id 3108
process_path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
file_name C:\Users\yobba.stak\AppData\Local\Microsoft\Windows\PowerShell\StartUpProfileData\Noninteractive

```
1 search 'powershell.exe'
2 | summarize count() by $table
```

\$table	count_
> CommonSecurityLog	1095
> Syslog	1091
> Event	28822

```
1 PFSenseFirewallEvents
2 | project TimeGenerated, SourceIP, DestinationIP, DestinationPort, Protocol
3
```

TimeGenerated [UTC] ↑↓	SourceIP	DestinationIP	DestinationPort	Protocol
> 10/12/2023, 8:58:07.300 AM	192.168.60.101	192.168.60.1	53	udp
> 10/12/2023, 8:58:07.301 AM	192.168.60.101	20.105.208.112	443	tcp
> 10/12/2023, 8:58:03.293 AM	192.168.60.101	192.168.60.1	53	udp

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](#)

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.

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

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

Free Security Log Resources by Randy

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

Description Fields in 4776

Error Code:	Description
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. unattended 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

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 \(Sysmon\)](#)

Event ID 7: Image loaded

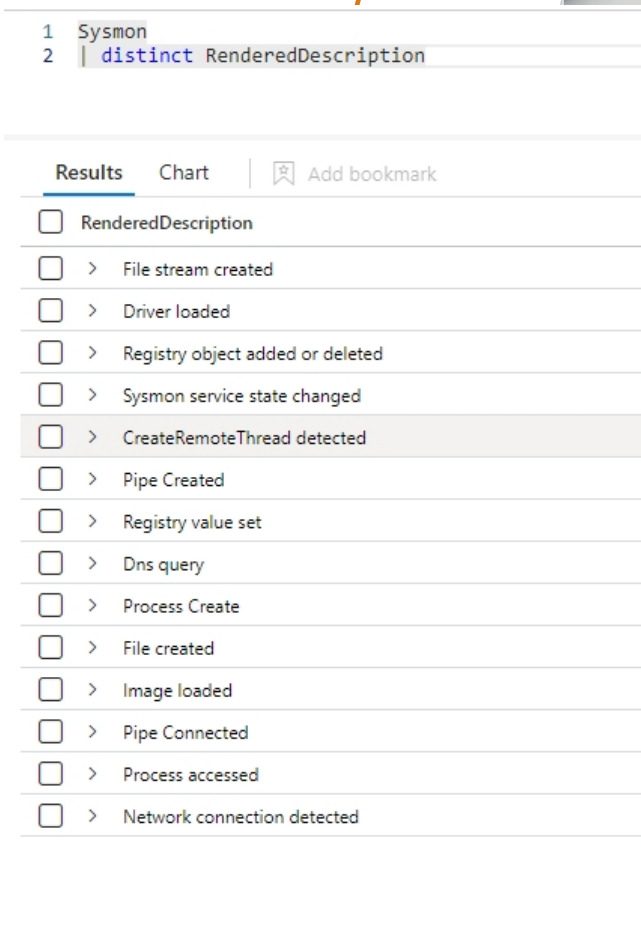
The `Image loaded` event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the `-1` option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance 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.



The screenshot shows a KQL query interface with the following content:

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

Below the query, there are tabs for "Results" and "Chart", and a link to "Add bookmark". A list of event types is displayed, each with a checkbox and a right-pointing arrow:

- 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

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 (<code>%SystemRoot%/system32/config/SAM</code>). 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

EVE Log Alerts Suricata will output Alerts via EVE

EVE Log Alert Payload Data Formats
Log the payload data with alerts. Options are No (disable payload logging), Only Printable (lossy) format, Only Base64 encoded or Both. See Suricata documentation.

EVE Log Alert details Log a packet dump with alerts. Log additional HTTP data. Include App Layer metadata. Log final action taken on packet by the engine. Log packets for rules using the "tag" keyword

EVE Log Drops Suricata will output Drops via EVE

EVE Log Drops Options Log alerts that caused drops. Default is "Checked". Log final action taken on packet by the engine.
"Start" logs only a single drop per flow direction. "All" logs each dropped pkt.

EVE Log Anomalies Suricata will log packet anomalies such as truncated packets, packets with invalid IP/UDP/TCP Length values and other events that render the packet invalid for further processing. Networks with high rates of anomalies may experience packet processing degradation.

EVE Logged Traffic BitTorrent DNS FTP HTTP HTTP2 IKE Kerberos NFS PostgreSQL
 QUICv1 RDP RFB SIP SMB SMTP TFTP
Choose the traffic types to log via EVE JSON output.

```
1 Suricata | where event_type == 'http'  
2
```

Results Chart Add bookmark

Showing the first 30,000 results. [Learn more](#) on how to narrow down the result set.

TimeGenerated [UTC] ↑↓	event_type	src_ip	src_port
dest_port	80		
Computer	pSense.home.arpa		
SyslogMessage	"2024-05-11T17:44:27.433969+0000";"flow_id":"957448884734762";"in_iface":"em1";"event_type":"http";		
DateTime [UTC]	2024-05-11T17:44:27.433969Z		
flow_id	957448884734762		
http	["hostname":"10.1.0.10";"url":"/g.pixel";"http_user_agent":"Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 Win64 x64 Trident/5.0 MANM MANM)"]		
hostname	10.1.0.10		
http_content_type	application/octet-stream		
http_user_agent	Mozilla/5.0 (compatible MSIE 9.0 Windows NT 6.1 Win64 x64 Trident/5.0 MANM MANM)		
url	/g.pixel		
in_iface	em1		
metadata	["flowbits":"T"]		
pkt_src	wire/pcap		
proto	TCP		
tx_id	0		

```
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'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. La descrizione resa è 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.`

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

Results Chart Add bookmark

<input type="checkbox"/>	RenderedDescription
<input type="checkbox"/>	> Sysmon config state changed
<input type="checkbox"/>	> File stream created
<input type="checkbox"/>	> Sysmon service state changed
<input type="checkbox"/>	> Driver loaded
<input type="checkbox"/>	> CreateRemoteThread detected
<input type="checkbox"/>	> Pipe Created
<input type="checkbox"/>	> Registry object added or deleted
<input type="checkbox"/>	> Registry value set
<input type="checkbox"/>	> Dns query
<input type="checkbox"/>	> Pipe Connected
<input type="checkbox"/>	> Process Create
<input checked="" type="checkbox"/>	> File created
<input type="checkbox"/>	> Image loaded
<input type="checkbox"/>	> Network connection detected
<input type="checkbox"/>	> Process accessed

TimeGenerated [UTC]	2023-10-13T08:21:42.8278386Z
Source	Microsoft-Windows-Sysmon
EventID	11
Computer	kingslanding.sevenkingdoms.local
UserName	NT AUTHORITY\SYSTEM
RenderedDescription	File created
event_creation_time	2023-10-13T08:21:42.8150000Z
process_guid	{29b545d4-57a0-6529-1b00-000000007600}
process_id	1196
process_path	C:\Windows\System32\svchost.exe
file_name	C:\Windows\ServiceState\EventLog\Data\lastalive0.dat
file_creation_time	2023-10-13T14:43:44.3330000Z

Sentinel-Workspace

Run

Time range : Last 7 days

Save

Share

New alert rule

```
1 Sysmon
2 | where RenderedDescription == 'File created'
3 | where file_name contains 'C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup'
4 or file_name contains 'C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup'
```

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

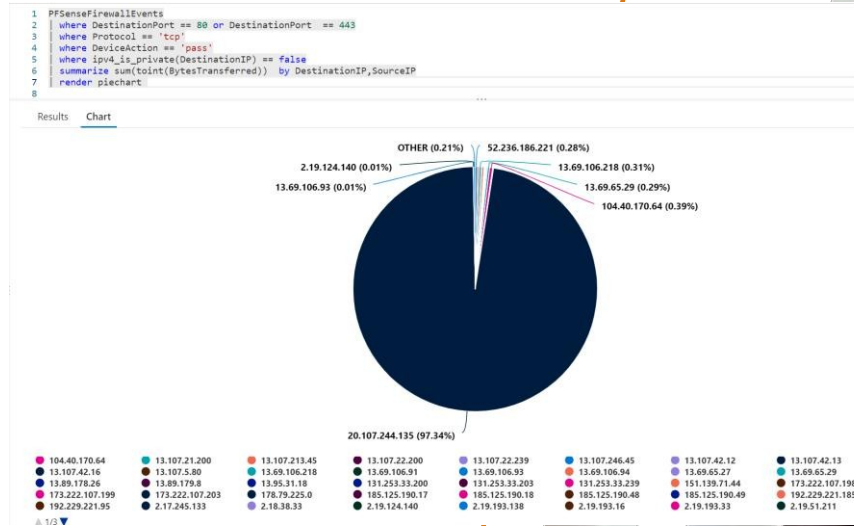
D: Quale funzione del SIEM è importante per i rilevamenti basati sui volumi?
R: Aggregazione degli eventi (riepilogo)

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?



```
1 PFSenseFirewallEvents
2 where DestinationPort == 80 or DestinationPort == 443
3 where Protocol == 'tcp'
4 where DeviceAction == 'pass'
5 where ipv4_is_private(DestinationIP) == false
6 summarize sum(toint(BytesTransferred)) by DestinationIP,SourceIP
7
8
```

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

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 quello di colpire 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 dietro il 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)

Activity
> 4826 - Boot Configuration Data loaded.
> 4688 - A new process has been created.
> 4608 - Windows is starting up.
> 4624 - An account was successfully logged on.
> 4622 - A security package has been loaded by the Local Security Authority.
> 4610 - An authentication package has been loaded by the Local Security Authority.
> 4902 - The Per-user audit policy table was created.
> 4614 - A notification package has been loaded by the Security Account Manager.
> 4672 - Special privileges assigned to new logon.
> 4648 - A logon was attempted using explicit credentials.
> 4696 - A primary token was assigned to process.
> 4670 - Permissions on an object were changed.
> 4634 - An account was logged off.
> 4768 - A Kerberos authentication ticket (TGT) was requested.
> 4769 - A Kerberos service ticket was requested.
> 4662 - An operation was performed on an object.
> 5061 - Cryptographic operation.
> 4799 - A security-enabled local group membership was enumerated.
> 5058 - Key file operation.

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-79f51408-78d8-4e23-8c79-1d27fbd2fe5
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
```

IPAddress	TimeGenerated [UTC]	Activity	dcount_TargetAccount	set_TargetAccount
> ::ffff:10.0.8.2	6/4/2024, 2:00:00.000 PM	4768 - A Kerberos authentici...	152	["sevenkingdoms.local\\nmap","seve...
> ::1	6/4/2024, 1:00:00.000 PM	4768 - A Kerberos authentici...	8	["SEVENKINGDOMS.LOCAL\\KINGSLS...
> ::1	6/4/2024, 11:00:00.000 AM	4768 - A Kerberos authentici...	8	["SEVENKINGDOMS.LOCAL\\KINGSLS...
> ::ffff:192.168.56.22	6/4/2024, 1:00:00.000 PM	4768 - A Kerberos authentici...	5	["north.sevenkingdoms.local\\CASTE...
> ::ffff:192.168.56.22	6/4/2024, 11:00:00.000 AM	4768 - A Kerberos authentici...	5	["north.sevenkingdoms.local\\sql_sve...
> ::1	6/4/2024, 12:00:00.000 PM	4768 - A Kerberos authentici...	3	["NORTH\\robb.stark","NORTH\\eddi...
> ::ffff:192.168.56.23	6/4/2024, 1:00:00.000 PM	4768 - A Kerberos authentici...	3	["ESSOS.LOCAL\\BRAAVOSS","essos...

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.

```
1 SecurityEvent
2 | distinct Activity
3
```

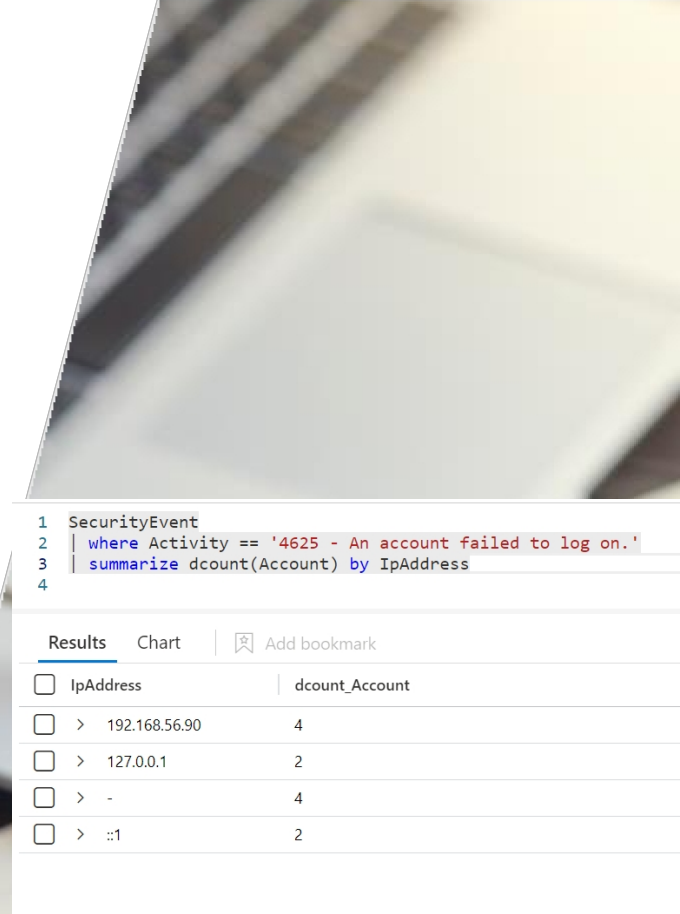
Results Chart Add bookmark

- 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(TargetAccount),make_set(TargetAccount) by IPAddress,bin(TimeGenerated,1h),Activity
```

Results 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)

```
8 Sysmon
9
10 | where RenderedDescription == "File created"
11 | where file_name startswith "C:\\xampp\\"
12 | 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"
```

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
```

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

*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 impartiti dall'applicazione Web al 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 da 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

8	
9	Sysmon
10	distinct RenderedDescription
11	

Results Chart Add bookmark

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

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'

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

<input type="checkbox"/>	TimeGenerated [UTC] ↑↓	url_	Computer	RawData	Type
<input type="checkbox"/>	> 6/4/2024, 10:58:23.000 PM	/cmd/cmd.jsp?cmd=netstat+-abno	goad-VirtualBox	["timestamp": "2024-06-04T22:5...	Suricata_CL
<input type="checkbox"/>	> 6/4/2024, 10:53:46.000 PM	/cmd/cmd.jsp?cmd=systeminfo	goad-VirtualBox	["timestamp": "2024-06-04T22:5...	Suricata_CL
<input type="checkbox"/>	> 6/4/2024, 10:53:27.000 PM	/cmd/cmd.jsp?cmd=hostname	goad-VirtualBox	["timestamp": "2024-06-04T22:5...	Suricata_CL
<input type="checkbox"/>	> 6/4/2024, 10:53:03.000 PM	/cmd/cmd.jsp?cmd=whoami+%2Fall	goad-VirtualBox	["timestamp": "2024-06-04T22:5...	Suricata_CL
<input type="checkbox"/>	> 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** tramite i 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 visualizza l'origine dell'attacco? R:

src_ip > 10.0.8.2

Azure Sentinel

```
40 Suricata
41 | where event_type
42 | extend msg_type_
43 | distinct msg_type_
44
```

Results	Chart	Add bookmark
<input type="checkbox"/> event_type		
<input type="checkbox"/> > tls		
<input type="checkbox"/> > smb		
<input type="checkbox"/> > dns		
<input type="checkbox"/> > krb5		
<input type="checkbox"/> > fileinfo		
<input type="checkbox"/> > http		
<input type="checkbox"/> > alert		
<input type="checkbox"/> > rdp		

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

Results	Chart	Add bookmark
<input type="checkbox"/> event_type		
<input type="checkbox"/> > tls		
<input type="checkbox"/> > smb		
<input type="checkbox"/> > dns		
<input type="checkbox"/> > krb5		
<input type="checkbox"/> > fileinfo		
<input type="checkbox"/> > http		
<input type="checkbox"/> > alert		
<input type="checkbox"/> > rdp		

```
40 Suricata
41 | where event_type == "krb5"
42
```

Results	Chart	Add bookmark
<input type="checkbox"/> TimeGenerated [UTC] ↑↓		Computer
event_type		krb5
flow_id		321972553849766
in_iface		em1
krb5		{ "msg_type": "KRB_TGS_REQ", "cname": "<empty>"
cname		<empty>
encryption		<none>
msg_type		KRB_TGS_REQ
realm		NORTH.SEVENKINGDOMS.LOCAL
sname		cifs/winterfell.north.sevenkingdoms.local
weak_encryption		false

```
40 Suricata
41 | where event_type == "krb5"
42 | extend msg_type_ = tostring(krb5.msg_type)
43 | where msg_type_ == "KRB_AS_REQ"
44 | where krb5.ticket_weak_encryption == true or krb5.weak_encryption == true
```

Results	Chart	Add bookmark
<input type="checkbox"/> TimeGenerated [UTC] ↑↓		msg_type_
event_type		krb5
flow_id		34081029493044
in_iface		em1
krb5		{ "msg_type": "KRB_AS_REQ", "cname": "brandon.stark", "realm": "NORTH.S<...>"
cname		brandon.stark
encryption		rc4-hmac
msg_type		KRB_AS_REQ
realm		NORTH.SEVENKINGDOMS.LOCAL
sname		krbtgt/NORTH.SEVENKINGDOMS.LOCAL
ticket_encryption		aes256-cts-hmac-sha1-96
ticket_weak_encryption		false
weak_encryption		true



Grazie per l'attenzione

Presentazione a cura di:

Christos Lazaridis
(Punto focale)