Configuring Your Sentinel and Defender Environment

By Grant Knoetze

- It is a Security Incident and Event Management Tool.
- It allows an organization to collect data (logs), analyse, and perform security operations on its computer systems, that can be hardware applications, applications, or both.



- In its simplest form, a SIEM solution allows you to:
 - Collect and query logs.
 - Do correlation and anomaly detection.
 - Create alerts and incidents based on your findings.
- A SIEM solution can also:
 - Perform log management the ability to collect, store, and query the log data from resources within your environment.
 - Alerting A proactive look inside the log data for potential security incidents and anomalies.
 - Visualization graphs and dashboards that provide visual insights into your log data.



- Incident Management The ability to create, update, assign, and investigate incidents that have been identified.
- Querying data Using KQL, you can query and understand your data.



- A cloud native SIEM system that a security operations team can use to:
 - Get security insights across the enterprise by collecting data from virtually any source.
 - Detect and investigate threats quickly by using built in machine learning and Microsoft threat intelligence.
 - Automate threat responses by using playbooks and by integrating Azure log apps.



What is Microsoft Sentinel

 Unlike with traditional SIEM solutions, you don't need to install any servers either on-premises or in the cloud to run Microsoft Sentinel. Microsoft Sentinel is a service that you deploy in Azure. You can get up and running with Sentinel in just a few minutes in the Azure portal.



- Microsoft Sentinel is tightly integrated with other cloud services. Not only can you quickly ingest logs, but you can also use other cloud services natively (for example, authorization and automation).
- Microsoft Sentinel helps you enable end-to-end security operations including collection, detection, investigation, and response:



What is Microsoft Sentinel

Collect	Det	tect	Investigate	Respond
		88	\	\$
Visibility	Analytics	Hunting	Incidents	Automation



MalTrak.com

What is Microsoft Sentinel: Data Connectors

=	Microsoft Azure	P Search resources, services, and docs (G+/)	۶.	Q	٨	?	ন্দ	grant@digitalinvestigati DIGITAL INVESTIGATIONS PRO (
Hon	ne > Microsoft Sentinel							
»	Microsoft Sentinel Selected workspace: 'traininginstance'	Data connectors						
		🕐 Refresh 🛛 🕅 Guides & Feedback						
	∨ General	Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. <u>Click here</u> to reinstate in use "content source = gallery content" templates.						
	 Overview (Preview) Logs Nows & quides 	14						
	 A least of galaxies Search Threat management 	Search by name or provider Providers : Microsoft Data Types : All Status : All						
	 Content management Configuration 	Status Connector name ↑						
	Workspace manager (Preview)	Azure Activity						
	Data connectors Analytics	Microsoft Defender for Cloud Apps						
	 Summary rules (Preview) Watchlist 	Microsoft Defender for Endpoint						
	 Automation Settings 	Microsoft Defender for Identity			No	Conr	necto	or selected
		Microsoft Defender for Office 365 (Preview)		Sele	ct a C	onneo	tor to	view more details
		Microsoft Defender Threat Intelligence (Preview)						
		Microsoft Defender XDR						
		Security Events via Legacy Agent						
		O Subscription-based Microsoft Defender for Cloud (Legacy) 🗸						



MalTrak.com

What is Microsoft Sentinel: Data Connectors

 The first thing to do is to have your data ingested into Microsoft Sentinel. Data connectors let you do just that. You connect Data connectors by first installing Content hub solutions. Once installed, you can add some services, such as Azure activity logs, just by selecting a button. Others, such as syslog, require more configuration. There are data connectors that cover all scenarios and sources, including but not limited to:



What is Microsoft Sentinel: Data Connectors

- syslog
- Common Event Format (CEF)
- Trusted Automated eXchange of Indicator Information (TAXII) (for threat intelligence)
- Azure Activity
- Microsoft Defender services
- Amazon Web Services (AWS) and Google Cloud Platform (GCP)

Log Retention

After data is ingested into Microsoft Sentinel, the data is stored in the Log Analytics workspace. The benefits of using Log Analytics include the ability to use the Kusto Query Language (KQL) to query your data. KQL is a rich query language that gives you the power to dive into and gain insights from our data.



Log Retention

■ Microsoft Azure		$\mathcal P$ Search resources, services, a	nd docs (G+/)	🐶 Copilot		ଦ 🐵 🕐 🕅	grant@digit DIGITAL INVEST	talinvestigati
Home > Microsoft Sentinel Microsoft Sentinel «	Microsoft Sentinel	Logs						×
Digital Investigations Pro (digitalinvestigations.pro) + Create Manage view ∨ ···· Filter for any field Name ↑↓ TrainingInstance	Selected workspace: 'traininginstance' Selected workspace: 'traininginstance' Search o « General Overview (Preview) Cortext (Preview) Search Search Shreat management Content management	*** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** **** *** **** *** **** *** **** *** ***** **** ********** **** ************************************	Run Time range : Last 24 hours Event	G Save ∨ 🖒 S	In the new Log Analy Ithare ∨ + New alert rule ∨ →	tics ♥ Feedback Export ∨ 📌 Pin to	ST Queries hub	at query ····
< Page 1 v of 1 >	 Configuration Workspace manager (Preview) Data connectors Analytics Summary rules (Preview) Watchlist Automation Settings 	You can add tavorites by clicking on the ☆ icon • LogManagement • 田 Event • 田 Peration • 田 Usage • Microsoft Sentinel • Security and Audit • SecurityCenterFree	Results Chart X Add bookmark TimeGenerated [UTC] \$ Source > 10/8/2024, 10:40:55.855 AM Microsc > 10/8/2024, 10:40:55.789 AM Microsc > 10/8/2024, 10:40:55.372 AM Microsc > 10/8/2024, 10:40:55.372 AM Microsc > 10/8/2024, 10:40:55.372 AM Microsc > 10/8/2024, 10:40:55.164 AM Microsc > 10/8/2024, 10:40:55.164 AM Microsc > 10/8/2024, 10:40:51.093 AM Microsc > 10/8/2024, 10:40:51.271 AM Microsc > 10/8/2024, 10:39.02.015 AM Microsc > 10/8/2024, 10:39.02.015 AM Microsc > 10/8/2024, 10:39.1.955 AM Microsc > 10/8/2024, 10:38.11.902 AM Microsc	e oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon oft-Windows-Sysmon	EventLog Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational Microsoft-Windows-Sysmon/Operational	Computer DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC DESKTOP-5DBAPQC	EventLevel 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	EventLevelNa Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Informatior Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information

₩ HalTrak

MalTrak.com

Log Retention

■ Microsoft Azure			nd docs (G+/)	📀 Copilot	区 Q @ Q A	grant@digitalinvestigati DIGITAL INVESTIGATIONS PRO (
Home > Microsoft Sentinel Microsoft Sentinel « Digital Investigations Pro (digitalinvestigations.pro)	Microsoft Sentinel Selected workspace: 'traininginstance'	Logs				×
+ Create	 Search General Overview (Preview) Cogs News & guides Search Threat management Content management Configuration 	Image: New Query 1* × + Image: TrainingInstance Image: TrainingInstance Tables Queries Functions ··· « Image: Tables Queries Functions ··· « Image: Post state Image: Tables Image: Tables ··· « Image: Post state Image: Tables Image: Tables ··· « Image: Post state Image: Tables ··· « ··· « Image: Post state Image: Tables ··· « ··· « Image: Post state Image: Tables ··· « ··· « Image: Post state Image: Tables ··· « ··· « Image: Post state Image: Tables ··· « ··· « Image: Post state ··· « ··· « ··· « Image: Post state ··· « ··· « ··· « ··· « Image: Post state ··· « ··· « ··· « ··· « ··· « Image: Post state ··· « ··· « ··· « ··· « ··· « Image: Post state ··· « ··· « ··· « ··· « ··· « ··· «	P Run Time range : Last 24 hours 1 Event Results Chart Add bookmark	Ø T Save ∨ I Share ∨ + Nev	ry the new Log Analytics v alert rule → Export × $\not \Rightarrow$ Pin to	Pueries hub Image: Comparison of the second
	 Workspace manager (Preview) Data connectors Analytics Summary rules (Preview) Watchlist Automation Settings 	 LogManagement ■ Event ■ Deration ■ Usage Microsoft Sentinel Security and Audit SecurityCenterFree 	TimeGenerated [UTC] ↑↓ Source > 10/8/2024, 10:40:55.855 AM Microsoft-W > 10/8/2024, 10:40:55.855 AM Microsoft-W > 10/8/2024, 10:40:55.789 AM Microsoft-W > 10/8/2024, 10:40:55.789 AM Microsoft-W > 10/8/2024, 10:40:55.782 AM Microsoft-W > 10/8/2024, 10:40:55.372 AM Microsoft-W > 10/8/2024, 10:40:55.372 AM Microsoft-W > 10/8/2024, 10:40:55.093 AM Microsoft-W > 10/8/2024, 10:40:55.093 AM Microsoft-W > 10/8/2024, 10:40:51.461 AM Microsoft-W > 10/8/2024, 10:40:51.227 AM Microsoft-W > 10/8/2024, 10:40:51.227 AM Microsoft-W > 10/8/2024, 10:40:51.227 AM Microsoft-W > 10/8/2024, 10:38:19.51 AM Microsoft-W > 10/8/2024, 10:38:18.011 AM Microsoft-W > 10/8/2024, 10:38:18.011 AM Microsoft-W > 10/8/2024, 10:38:11.902 AM Microsoft-W	EventLog indows-Sysmon Microsoft-Windows- indows-Sysmon Microsoft-Windows-	Computer jysmon/Operational DESKTOP-5DBAPQC jysmon/Operational DESKTOP-5DBAPQC	EventLevel EventLevelNa Image: Comparison of the second s

₩ HalTrak

MalTrak.com



Azure Data Explorer

• Unless you have access to Azure, use the data explorer online free tool and upload the logs there:

<u>https://dataexplorer.azure.com/clusters/kvc-</u> <u>shs865gjpream59ar2.northeurope/databases/MyDatabase</u>



Azure Data Explorer

						_				
Azure Data Explorer 📔 🌅	New connection pane	e 🖵 Query							S % \$	Grant (
MyFreeCluster.MyData 🖉 🕂	+									6 1
Connections e «	⊳ Run 🗸	🕞 Recall 🛛 🐺 KQL tools 🗸	MyFreeCluster/MyDatab	pase			🖍 Pin to d	lashboard 🕒 Open	~ 🛛 Сору ~	→ Expor
+ Add ~ Q 6 🗃	1 2 ["New Tab	le "]								
Favorites										
- 🗸 🖟 MyFreeCluster										
✓ ☐ MyDatabase ② ···										
> 🌐 New										
> 🖽 New Data										
m										
> III New lable										
	TT New Table	Add South & Gate				0.0.1				<u> </u>
	Ⅲ New Table +	- Add visual 💿 Stats				,∕⊃ Search	ⓒ UTC 🗐 Cach	ned (24.316 s) 💷 140,	,077 records 🛛 💿	Ê
	EntryNumber ≡	- Add visual ③ Stats SequenceNumber ≡ Int	Use ≡ ParentEntryNumber ≡	ParentSequenceNumber ≡	ParentPath		 O UTC ☐ Cach Extension ≡ 	ned (24.316 s) 💷 140, FileSize = 🗌 Reference	.077 records 💿	È E
	III New Table + EntryNumber ≡ >	- Add visual ③ Stats SequenceNumber ≡ Ini	Use ≡ ParentEntryNumber ≡	ParentSequenceNumber ≡	ParentPath ParentPath	,	 Outc □ Cach Extension ≡ Extension 	ned (24.316 s) 140, FileSize ≡ Reference	,077 records 👁 eCount :	Ê E ≡ Rep Rep
	Image: New Table + Image: EntryNumber Image: New Table + New Table	Add visual ③ Stats SequenceNumber ≡ Ini 1 tru	Use ≡ ParentEntryNumber ≡ ue 104,070	ParentSequenceNumber ≡ 1	ParentPath ParentPath .\Windows\SoftwareDistribution\SLS\2881F18F-356C-4FA1	 ✓ Search FileName FileName sls.cab 	⊙ UTC ☐ Cact Extension	ned (24.316 s) 🐵 140, FileSize 📄 Reference 24.344	,077 records 👁 eCount :	■ ■ ■ Rep 1
		Add visual @ Stats SequenceNumber ≡ Inti 1 tru 2 tru	Use ParentEntryNumber = ue 104,070 ue 105,274	ParentSequenceNumber ≡ 1 3	ParentPath ParentPath \Windows\SoftwareDistribution\SL\$\2881F18F-356C-4FA1 \Windows\SoftwareDistribution\SL\$\9482F484-E343-4386		UTC Cacl Extension Extension cab cab	ned (24.316 s) 💷 140, FileSize = Reference 24.344 30,987	.077 records 👁	■ ■ ■ Rep 1 1
		Add visual © Stats SequenceNumber ≡ Init 1 tru 2 tru 2 tru 2 tru	Use ≡ ParentEntryNumber ≡ ue 104,070 ue 105,274 ue 105,312	ParentSequenceNumber ≡ 1 3 3	ParentPath Entert ParentPath	✓ Search FileName ≡ FileName sls.cab sls.cab sls.cab	UTC Cach Extension Extension cab cab cab cab	ned (24.316 s) 💷 140, FileSize 24.344 30.987 34.893	1077 records	■ ■ ■ Rep 1 1 1
		Add visual ③ Stats SequenceNumber ≡ Ini 1 tru 2 tru 2 tru 2 tru 2 tru	Use	ParentSequenceNumber ≡ 1 3 3 2	ParentPath ParentPath \Windows\SoftwareDistribution\SL5\2881F18F-356C-4FA1 \Windows\SoftwareDistribution\SL5\8558A7C-EC84-4CA3 \Windows\SoftwareDistribution\SL5\8558A7C-EC84-4CA3 \Windows\SoftwareDistribution\SL5\8588A7C-EC84-4CA3	✓ Search FileName FileName sls.cab sls.cab sls.cab	UTC Cach Extension zab .cab	ned (24.316 s) 💷 140, FileSize	.077 records 👁	■ ■ ■ Rep 1 1 1 1 1
	Image: New Table EntryNumber Image: New Table > 104,073 105,293 105,330 105,407 106,405	Add visual ③ Stats SequenceNumber ≡ Ini 1 tru 2 tru 2 tru 2 tru 2 tru 2 tru 2 tru 2 tru	Use	ParentSequenceNumber ≡ 1 1 3 3 2 2 2 2	ParentPath ■ ParentPath	✓ Search FileName Sis.cab sis.cab sis.cab sis.cab sis.cab	 O UTC □ Cach Extension = Extension cab cab cab cab cab cab 	red (24.316 s) 140. FileSize ≡ Reference 24.344 30.987 34.893 30.982 25.457	.077 records 👁	Rep Rep 1 1 1 1 1 1
	Image: New Table Image: New Table EntryNumber Image: New Table > 104,073 > 105,293 > 105,330 > 105,407 > 106,405 > 103,931	Add visual ③ Stats SequenceNumber ≡ Int 1 tru 2 tru	Use ≡ ParentEntryNumber ≡ ue 104,070 ue 105,274 ue 105,312 ue 105,388 ue 106,404 ue 103,932	ParentSequenceNumber ≡ 1 3 3 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ParentPath ■ ParentPath	✓ Search FileName ≡ FileName ≡ sls.cab sls.cab sls.cab sls.cab sls.cab sls.cab sls.cab sls.cab	 UTC Cach Extension Extension cab cab cab cab cab cab schema 	red (24.316 s) III 140. FileSize Reference 24.344 30,987 34,893 30,982 25,457 150	.077 records 👁	Rep Rep 1 1 1 1 1 1 1 1 1
	Image: Image of the state of the	Add visual ③ Stats SequenceNumber ≡ Int 1 tru 2 tru 2 tru 2 tru 2 tru 2 tru 2 tru 1 tru 1 tru	Use	ParentSequenceNumber ≡ 1 1 3 3 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ParentPath ■ ParentPath		UTC Cach Extension Cab	red (24.316 s) III 140, FileSize I Reference 24.344 30.987 34.893 30.982 25.457 150 31.582	.077 records 👁	■ Rep Rep 1 1 1 1 1 1 1 1 1 1
	Image: New Table + EntryNumber ≡ > > 104,073 > 105,293 > 105,407 > 106,407 > 106,407 > 103,330 > 103,931 > 103,936 > 103,936	Add visual © Stats SequenceNumber ≡ Init 1 tru 2 tru 2 tru 2 tru 2 tru 2 tru 1 tru	Use ParentEntryNumber = ue 104,070 ue 105,274 ue 105,312 ue 105,388 ue 106,404 ue 103,932 ue 103,932	ParentSequenceNumber ≡ 1 1 3 3 2 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1	ParentPath ParentPath Windows\SoftwareDistribution\SL5\2881F18F-356C-4FA1 \Windows\SoftwareDistribution\SL5\9482F484-E343-4386 \Windows\SoftwareDistribution\SL5\9482F484-E343-4386 \Windows\SoftwareDistribution\SL5\9482F484-E343-4386 \Windows\SoftwareDistribution\SL5\948248027-1DEF-8A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-8A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Windows\SoftwareDistribution\SL5\878248027-1DEF-9A88 \Users\Installer\AppDataLocal\Packages\MicrosoftWindo \Users\Installer\AppData\Local\Packages\MicrosoftWindo \Users\Installer\AppData\Local\Packages\MicrosoftWindo	P Search FileName FileName Sis.cab Sis.cab Sis.cab Sis.cab Sis.cab Sis.cab aps.schema apps.schema	UTC Cach Extension cab cab	ned (24.316 s) III 140, FileSize I Reference 24.344 30.987 34.693 30.982 25.457 150 31.582 162	.077 records eCount :	■ Rep Rep 1 1 1 1 1 1 1 1 1 1 1
	■ New Table + EntryNumber = > > 104,073 > 105,293 > 105,300 > 105,407 > 105,407 > 105,407 > 103,938 > 103,938 > 103,938	Add visual © Stats SequenceNumber ≡ Ini 1 tru 2 tru 2 tru 2 tru 2 tru 2 tru 1 tru 1 tru 1 tru 1 tru 1 tru 1 tru	Use ■ ParentEntryNumber ■ ue 104,070 ue 105,274 ue 105,312 ue 105,388 ue 106,404 ue 103,932 ue 103,932 ue 103,932 ue 103,932	ParentSequenceNumber ≡ 1 1 3 3 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ParentPath ■ ParentPath	✓ Search FileName ≡ FileName sls.cab <psls.cab< p=""> <</psls.cab<>	UTC Cach Extension Extension cab	ned (24.316 s) III 140, FileSize Reference 24,344 30,987 34,893 30,982 25,457 150 31,582 162 31,582	.077 records 🔹	Rep. Rep. 1 1 1 1 1 1 1 1 1 1 1 1 1
	Image: New Table Image: New Table EntryNumber ≡ > > 104,073 > 105,293 > 105,300 > 105,407 > 106,405 > 103,936 > 103,938 > 103,938 > 103,939 > 107,211	Add visual ③ Stats SequenceNumber Int	Use ≡ ParentEntryNumber ≡ ue 104,070 ue 105,274 ue 105,312 ue 105,388 ue 106,404 ue 103,932 ue 103,932 ue 103,932 ue 103,932 ue 103,932 ue 103,932	ParentSequenceNumber ≡ 1 1 3 3 2 2 1 1 1 1 1 1 2 2 2 2 2 2 2 2	ParentPath ■ ParentPath ■ \Windows\SoftwareDistribution\SLS\2881F18F-356C-4FA1 \Windows\SoftwareDistribution\SLS\9482F484-E343-3486 \Windows\SoftwareDistribution\SLS\9482F484-E343-3486 \Windows\SoftwareDistribution\SLS\9482F484-E343-3486 \Windows\SoftwareDistribution\SLS\9482F484-E343-3486 \Windows\SoftwareDistribution\SLS\9582F4847-ECE4-4C3 \Windows\SoftwareDistribution\SLS\828248027-1DEE-8A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-8A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Windows\SoftwareDistribution\SLS\82848027-1DEE-9A88 \Users\Installer\AppData\Local\Packages\MicrosoftWindo \Users\Installer\AppData\Local\Packages\MicrosoftWindo \Users\Installer\AppData\Local\Packages\MicrosoftWindo \Users\Installer\AppData\Local\Packages\MicrosoftWindo \Users\Installer\AppData\Local\Packages\MicrosoftWindo \Users\Installer\AppData\Local\Packages\MicrosoftWindo	✓ Search FileName ≡ FileName sls.cab <psls.cab< p=""> <</psls.cab<>	 OUTC □ Cach Extension = Extension Extension cab cab cab cab cab cab schema tht schema 	red (24.316 s) ⊞ 140, FileSize ≡ Reference 24,344 30,987 34,893 30,982 25,457 150 31,582 162 31,582 150	.077 records 👁	■ Rep Rep 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1



MalTrak.com

hid01.ir Onboarding in Defender for Advanced Hunting

• Device Discovery and Onboarding is the process of connecting devices to Microsoft Defender for Endpoint.

Go to:

Settings -> Endpoints -> Device Management -> Onboarding.

- ->Select the Operating System Type
- ->Select the Connectivity Type
- ->Select the Deployment Method



Search for Endpoints Communicating with a Specific Domain: Mitre Attack TTP: T1059.005

Malware communicates with command and control servers and malicious domains, use the following KQL query to detect what machines are communicating with a specific domain:



hid01.ir Search for Endpoints Communicating with a Specific Domain

• Query:

let Domain = "<u>http://domain.com</u>";

DeviceNetworkEvents

| where Timestamp > ago(7d) and RemoteUrl contains Domain

| project Timestamp, DeviceName, RemotePort, RemoteUrl

| top 100 by Timestamp desc



Search for Created Scheduled Tasks

Scheduled Tasks are often used by attackers as a means of maintaining persistence. Use the following Query to search for all created scheduled tasks.



Search for Created Scheduled Tasks

Query

DeviceProcessEvents

| where FolderPath endswith "\\schtasks.exe" and

ProcessCommandLine has

"/create " and AccountName != "system"

| where Timestamp > ago(7d)



Malicious Documents / Macros that tried to connect to a suspicious domain or website:

This query will identify any malicious documents that have been used to connect to a malicious domain.



Malicious Documents / Macros that tried to connect to a suspicious domain or website:

DeviceProcessEvents

| where ActionType == "ProcessCreated" and InitiatingProcessFileName endswith
".exe"

| where InitiatingProcessFileName in~ ("winword.exe", "excel.exe", "powerpnt.exe")

| where not (InitiatingProcessCommandLine contains ".microsoft.com" or InitiatingProcessCommandLine contains ".live.com" or InitiatingProcessCommandLine contains ".office.com")

project InitiatingProcessFileName, InitiatingProcessCommandLine



Or

- // Define the DeviceProcessEvents part of the query
- let processEvents = DeviceProcessEvents
- | where ActionType == "ProcessCreated"
- | where InitiatingProcessFileName in~ ("winword.exe", "excel.exe", "powerpnt.exe");





Or

// Define the DeviceNetworkEvents part of the query

let networkEvents = DeviceNetworkEvents

| where not (RemoteUrl has ".microsoft.com" or RemoteUrl has ".live.com" or RemoteUrl has ".office.com")

| project Timestamp, DeviceName, RemotePort, RemoteUrl, InitiatingProcessFileName, InitiatingProcessCommandLine;





Or

- // Join the two parts
- processEvents
- | join kind=inner (networkEvents) on InitiatingProcessFileName
- | project Timestamp, DeviceName, RemotePort, RemoteUrl, InitiatingProcessFileName, InitiatingProcessCommandLine

