Microsoft Security

SC-200 Microsoft Security Operations Analyst

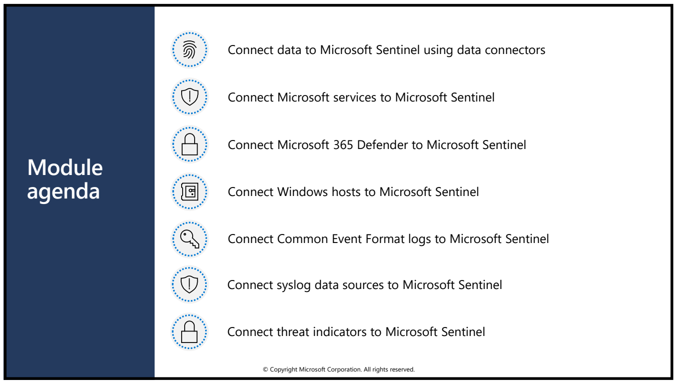
Ben McGee
11/20/2022

1

Microsoft Security

Module 6: Connect logs to Microsoft Sentinel

2



Module agenda

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft 365 Defender to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

3

Lesson 1: Connect data to Microsoft Sentinel using data connectors

4

Lesson introduction

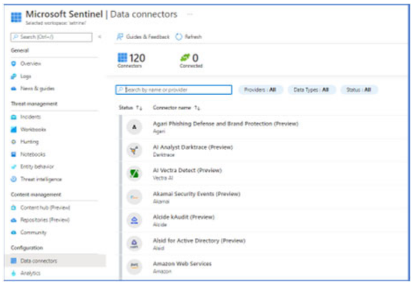
After this lesson, you will be able to:

- Explain the use of data connectors in Microsoft Sentinel
- Describe the Microsoft Sentinel data connector providers
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel

5

Ingest log data with data connectors

To collect log data, you need to connect your data sources with Microsoft Sentinel Connectors.

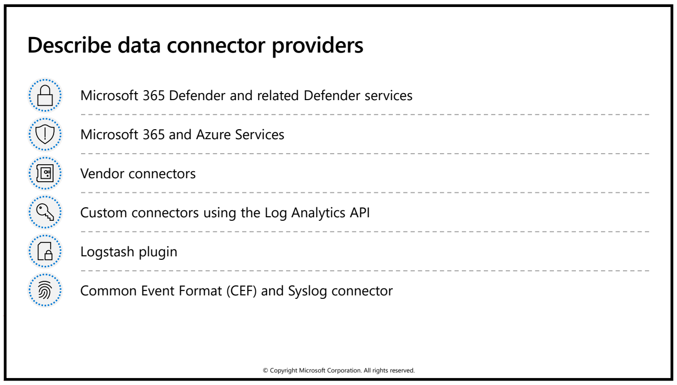


120 Connectors

0 Connected

Status	Connector name
	Agari Phishing Defense and Brand Protection (Preview) Agari
	AI Analyst Darktrace (Preview) Darktrace
	AI Vectra Detect (Preview) Vectra AI
	Akamai Security Events (Preview) Akamai
	Alcide kAudit (Preview) Alcide
	Alsid for Active Directory (Preview) Alsid
	Amazon Web Services Amazon

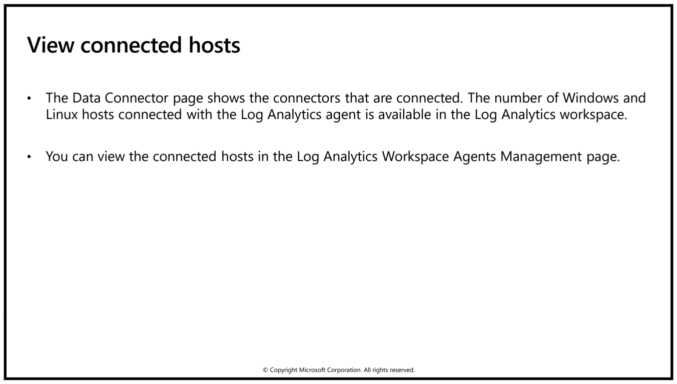
6



Describe data connector providers

- Microsoft 365 Defender and related Defender services
- Microsoft 365 and Azure Services
- Vendor connectors
- Custom connectors using the Log Analytics API
- Logstash plugin
- Common Event Format (CEF) and Syslog connector

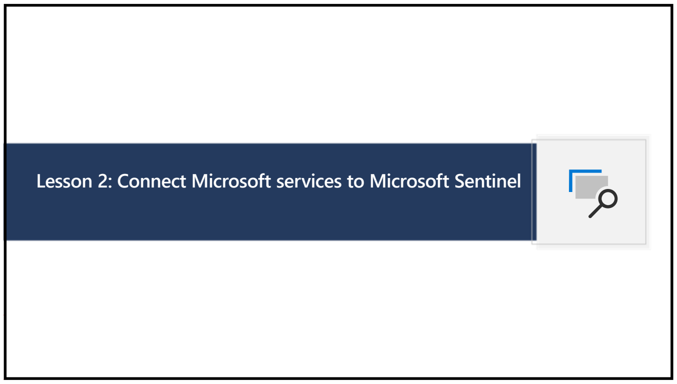
7



View connected hosts

- The Data Connector page shows the connectors that are connected. The number of Windows and Linux hosts connected with the Log Analytics agent is available in the Log Analytics workspace.
- You can view the connected hosts in the Log Analytics Workspace Agents Management page.

8



Lesson 2: Connect Microsoft services to Microsoft Sentinel

9

Lesson introduction

After this lesson, you will be able to:

- Connect Microsoft service connectors
- Explain how connectors auto-create incidents in Microsoft Sentinel

10

Plan for Microsoft services connectors

Prerequisites

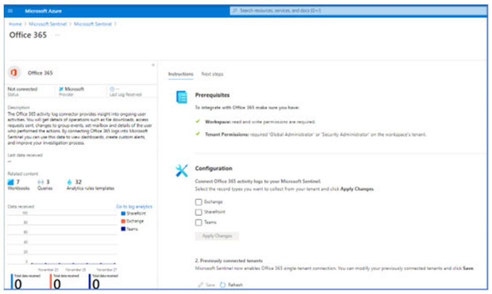
Configuration

Create incidents

11

Connect the Microsoft Office 365 connector

The Office 365 activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, access requests sent, changes to group events, set-mailbox, and details of the user who performed the actions.



The Office 365 activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, access requests sent, changes to group events, set-mailbox and details of the user who performed the actions. By connecting Office 365 logs into Microsoft Sentinel you can use this data to view dashboards, create custom alerts, and improve your investigation process.

To integrate with Office 365 make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Connect Office 365 activity logs to your Microsoft Sentinel.

Select the record types you want to collect from your tenant and click **Apply Changes**.

- □ Exchange
- □ SharePoint
- □ Teams

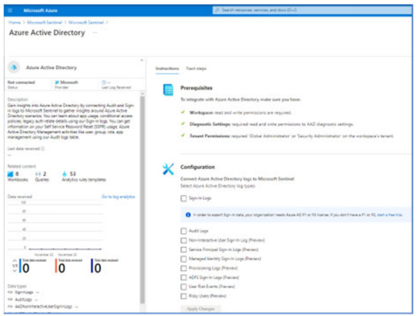
2. Previously connected tenants

Microsoft Sentinel now enables Office 365 single-tenant connection. You can modify your previously connected tenants and click **Save**.

12

Connect the Azure Active Directory connector

Gain insights into Azure Active Directory by connecting Audit and Sign in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios.



Description
Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Diagnostic Settings:** required read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel
Select Azure Active Directory log types:

- □ Sign-In Logs

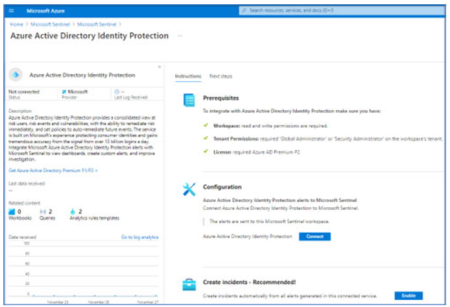
In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

- □ Audit Logs
- □ Non-Interactive User Sign-In Log (Preview)
- □ Service Principal Sign-In Logs (Preview)
- □ Managed Identity Sign-In Logs (Preview)
- □ Provisioning Logs (Preview)
- □ ADFS Sign-In Logs (Preview)
- □ User Risk Events (Preview)
- □ Risky Users (Preview)

13

Connect the Azure Active Directory Identity Protection connector

Azure Active Directory Identity Protection provides a consolidated view of at-risk users, risk events, and vulnerabilities, with the ability to remediate risk immediately and set policies to auto remediate future events.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
Azure Active Directory Identity Protection
Azure Active Directory Identity Protection
Not connected
Status
Microsoft
Provider
Last Log Received
Instructions
Next steps
Get Azure Active Directory Premium P1/P2 >
Related content
0
Workbooks
2
Queries
2
Analytics rules templates
Data received
Go to log analytics
Connect
Enable

Description
Azure Active Directory Identity Protection provides a consolidated view at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft's experience protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day. Integrate Microsoft Azure Active Directory Identity Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation.

Last data received

Prerequisites

To integrate with Azure Active Directory Identity Protection make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** required Azure AD Premium P2

Configuration

Azure Active Directory Identity Protection alerts to Microsoft Sentinel
Connect Azure Active Directory Identity Protection to Microsoft Sentinel.

The alerts are sent to this Microsoft Sentinel workspace.

Azure Active Directory Identity Protection

Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.

14

Lesson 3: Connect Microsoft 365 Defender to Microsoft Sentinel

15

Lesson introduction

After this lesson, you will be able to:

- Activate the Microsoft 365 Defender connector in Microsoft Sentinel
- Activate the Microsoft Defender for Endpoint connector in Microsoft Sentinel
- Activate the Microsoft Defender for Office 365 connector in Microsoft Sentinel

16

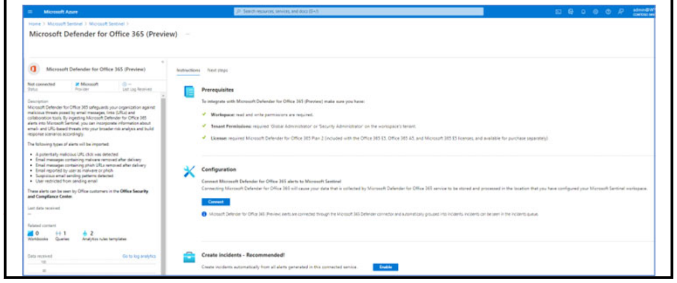
Plan for Microsoft 365 Defender connectors

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft 365 Defender
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft 365 Insider Risk Management (IRM) (Preview)

17

Connect alerts from Microsoft Defender for Office 365

With Microsoft Defender for Office 365 alerts, you can incorporate information about email-based and URL-based threats into your broader risk analysis and build response scenarios accordingly.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
Instructions
Next steps
Connect
Enable
Go to log analytics

Microsoft Defender for Office 365 (Preview)

Microsoft Defender for Office 365 (Preview)

Not connected — Status | Microsoft — Provider | Last Log Received

Description

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs) and collaboration tools. By ingesting Microsoft Defender for Office 365 alerts into Microsoft Sentinel, you can incorporate information about email- and URL-based threats into your broader risk analysis and build response scenarios accordingly.

The following types of alerts will be imported:

- A potentially malicious URL click was detected
- Email messages containing malware removed after delivery
- Email messages containing phish URLs removed after delivery
- Email reported by user as malware or phish
- Suspicious email sending patterns detected
- User restricted from sending email

These alerts can be seen by Office customers in the **Office Security and Compliance Center**.

Last data received

—

Related content

0 Workbooks | 1 Queries | 2 Analytics rules templates

Data received

Prerequisites

To integrate with Microsoft Defender for Office 365 (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** required Microsoft Defender for Office 365 Plan 2 (included with the Office 365 E5, Office 365 A5, and Microsoft 365 E5 licenses, and available for purchase separately)

Configuration

Connect Microsoft Defender for Office 365 alerts to Microsoft Sentinel

Connecting Microsoft Defender for Office 365 will cause your data that is collected by Microsoft Defender for Office 365 service to be stored and processed in the location that you have configured your Microsoft Sentinel workspace.

Microsoft Defender for Office 365 (Preview) alerts are connected through the Microsoft 365 Defender connector and automatically grouped into incidents. Incidents can be seen in the incidents queue.

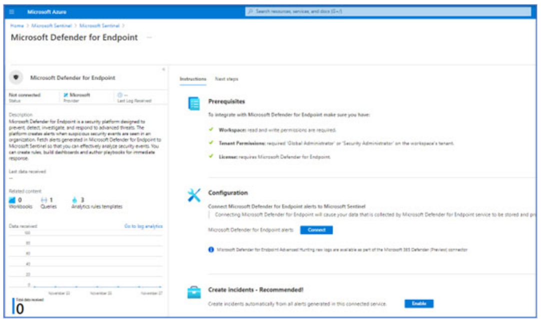
Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.

18

Connect alerts from Microsoft Defender for Endpoint

Fetch alerts generated in Microsoft Defender for Endpoint so that you can effectively analyze security events.



Microsoft Defender for Endpoint

Microsoft Defender for Endpoint

Not connected | Microsoft | --
Status | Provider | Last Log Received

Description
Microsoft Defender for Endpoint is a security platform designed to prevent, detect, investigate, and respond to advanced threats. The platform creates alerts when suspicious security events are seen in an organization. Fetch alerts generated in Microsoft Defender for Endpoint to Microsoft Sentinel so that you can effectively analyze security events. You can create rules, build dashboards and author playbooks for immediate response.

Last data received
--

Related content
0 Workbooks · 1 Queries · 3 Analytics rules templates

Data received

Total data received
0

Prerequisites

To integrate with Microsoft Defender for Endpoint make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** requires Microsoft Defender for Endpoint.

Configuration

Connect Microsoft Defender for Endpoint alerts to Microsoft Sentinel

Connecting Microsoft Defender for Endpoint will cause your data that is collected by Microsoft Defender for Endpoint service to be stored and pr

Microsoft Defender for Endpoint alerts

Microsoft Defender for Endpoint Advanced Hunting raw logs are available as part of the Microsoft 365 Defender (Preview) connector

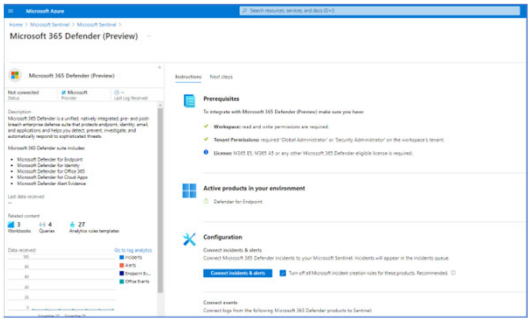
Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.

19

Connect the Microsoft 365 Defender connector (Preview)

The Microsoft 365 Defender connector lets you stream advanced hunting logs - a type of raw event data - from Microsoft 365 Defender.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
Instructions
Next steps
Go to log analytics
Incidents
Alerts
Endpoint Ev...
Office Events
Workbooks
Queries
Analytics rules templates
Connect incidents & alerts

Microsoft 365 Defender (Preview)

Microsoft 365 Defender (Preview)

Not connected | Microsoft | --
Status | Provider | Last Log Received

Description
Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence

Last data received
--

Related content
3 Workbooks · 4 Queries · 27 Analytics rules templates

Data received

Prerequisites

To integrate with Microsoft 365 Defender (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- **License:** M365 E5, M365 A5 or any other Microsoft 365 Defender eligible license is required.

Active products in your environment

Defender for Endpoint

Configuration

Connect incidents & alerts

Connect Microsoft 365 Defender incidents to your Microsoft Sentinel. Incidents will appear in the incidents queue.

☑ Turn off all Microsoft incident creation rules for these products. Recommended.

Connect events

Connect logs from the following Microsoft 365 Defender products to Sentinel:

20

Lesson 4: Connect Windows hosts to Microsoft Sentinel

21

Lesson introduction

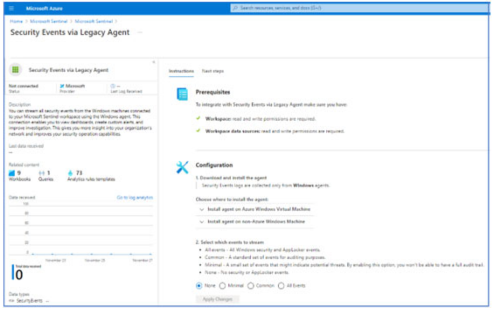
After this lesson, you will be able to:

- Connect Azure Windows Virtual Machines to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Configure Log Analytics agent to collect Sysmon events

22

Plan for Windows hosts security events connector

The Security Events connector lets you stream all security events from your Windows systems (servers and workstations, physical and virtual) to your Microsoft Sentinel workspace.



Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Prerequisites

To integrate with Security Events via Legacy Agent make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Workspace data sources:** read and write permissions are required.

Configuration

1. Download and install the agent

Security Events logs are collected only from **Windows** agents.

Choose where to install the agent:

- Install agent on Azure Windows Virtual Machine
- Install agent on non-Azure Windows Machine

2. Select which events to stream

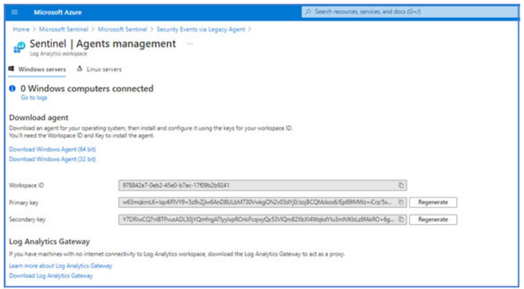
- All events - All Windows security and AppLocker events.
- Common - A standard set of events for auditing purposes.
- Minimal - A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.
- None - No security or AppLocker events.

● None ○ Minimal ○ Common ○ All Events

23

Connect non-Azure Windows Machines

When connecting non-Azure Windows hosts, you need to manually install the client agent.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel > Security Events via Legacy Agent >
Sentinel | Agents management
Log Analytics workspace
Windows servers
Linux servers
Go to logs
Download Windows Agent (64 bit)
Download Windows Agent (32 bit)
Regenerate
Regenerate
Learn more about Log Analytics Gateway
Download Log Analytics Gateway

0 Windows computers connected

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.
You'll need the Workspace ID and Key to install the agent.

Workspace ID: 978842e7-0eb2-45e0-b7ec-17f09b2b9241

Primary key: w63mqkmL6+lqc4lFlVY9+5z9vZjlw6AnD8ULbM730VwkgON2v03dYj0/zojBCQMckos6/Ep69lMWz+iCrz/5x...

Secondary key: Y7DRlwCQ7nl8TPvusADL30jYQmfngATlyyixpROrkiFcqwyQx53VlQm82XbXl4WqkdYlu3mNlKbLz6fAkRO+6g...

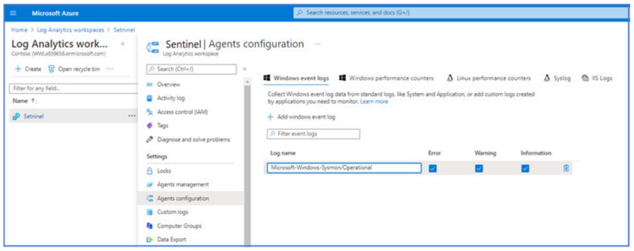
Log Analytics Gateway

If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway to act as a proxy.

24

Collect Sysmon event logs

The Microsoft-Windows-Sysmon/Operational entry is required in the Windows Event Logs.



Collect Windows event log data from standard logs, like System and Application, or add custom logs created by applications you need to monitor. Learn more

Log name	Error	Warning	Information
Microsoft-Windows-Sysmon/Operational	☑	☑	☑

25

Lesson 5: Connect Common Event Format logs to Microsoft Sentinel

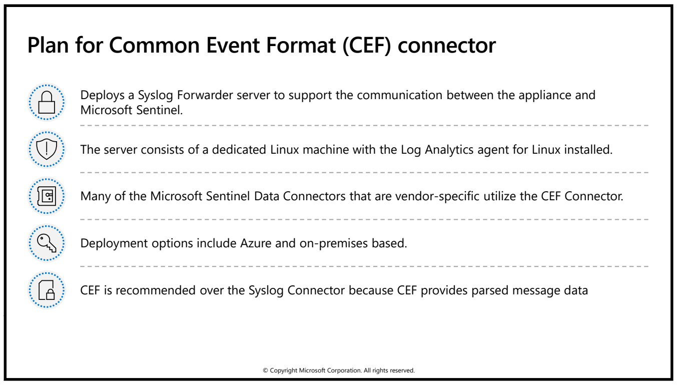
26

Lesson introduction

After this lesson, you will be able to:

- Explain the Common Event Format connector deployment options in Microsoft Sentinel
- Run the deployment script for the Common Event Format connector

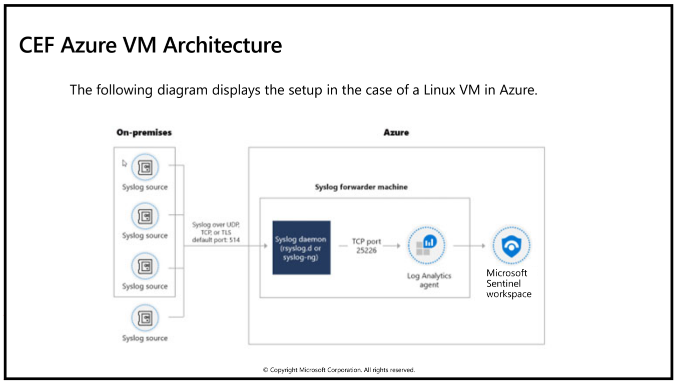
27



Plan for Common Event Format (CEF) connector

- Deploys a Syslog Forwarder server to support the communication between the appliance and Microsoft Sentinel.
- The server consists of a dedicated Linux machine with the Log Analytics agent for Linux installed.
- Many of the Microsoft Sentinel Data Connectors that are vendor-specific utilize the CEF Connector.
- Deployment options include Azure and on-premises based.
- CEF is recommended over the Syslog Connector because CEF provides parsed message data

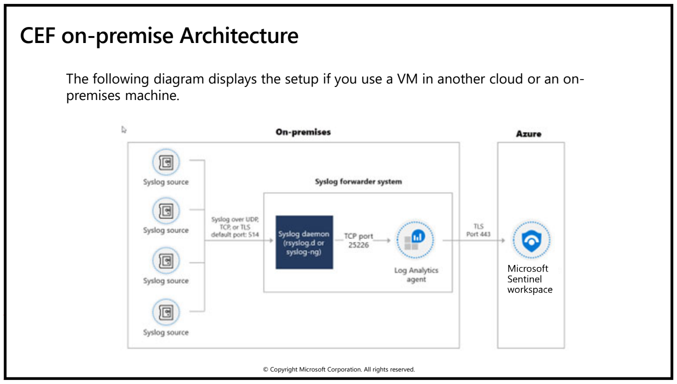
28



CEF Azure VM Architecture

The following diagram displays the setup in the case of a Linux VM in Azure.

29



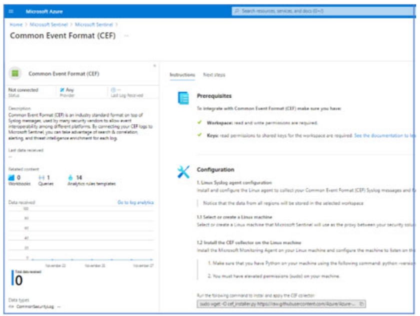
CEF on-premise Architecture

The following diagram displays the setup if you use a VM in another cloud or an on-premises machine.

30

Connect your external solution using the CEF connector

Using the link provided on the connector page, you will run a script on the designated machine.



Description

Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms. By connecting your CEF logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log.

Prerequisites

To integrate with Common Event Format (CEF) make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Keys:** read permissions to shared keys for the workspace are required. See the documentation to le

Configuration

1. Linux Syslog agent configuration

Install and configure the Linux agent to collect your Common Event Format (CEF) Syslog messages and f

Notice that the data from all regions will be stored in the selected workspace

1.1 Select or create a Linux machine

Select or create a Linux machine that Microsoft Sentinel will use as the proxy between your security solu

1.2 Install the CEF collector on the Linux machine

Install the Microsoft Monitoring Agent on your Linux machine and configure the machine to listen on th

1. Make sure that you have Python on your machine using the following command: python -versio
2. You must have elevated permissions (sudo) on your machine.

Run the following command to install and apply the CEF collector:

```
sudo wget -O cef_installer.py https://raw.githubusercontent.com/Azure/Azure-...
```

31

Lesson 6: Connect syslog data sources to Microsoft Sentinel

32

Lesson introduction

After this lesson, you will be able to:

- Describe the Syslog connector deployment options in Microsoft Sentinel
- Run the connector deployment script to send data to Microsoft Sentinel
- Configure the Log Analytics agent integration for Microsoft Sentinel
- Create a parse using KQL in Microsoft Sentinel

33

Plan for the syslog connector

Overview

Stream events from Linux-based, Syslog-supporting machines or appliances into Microsoft Sentinel using the Log Analytics agent for Linux.

The host's native Syslog daemon will collect local events of the specified types and forward them locally to the agent, which will stream them to your Log Analytics workspace.

How it works

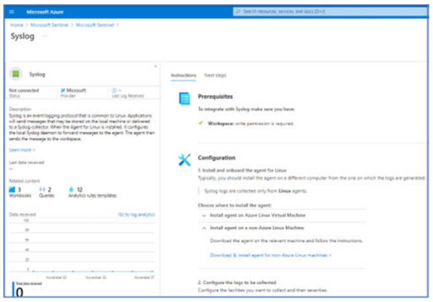
Syslog is an event logging protocol that is common to Linux. When the Log Analytics agent for Linux is installed on your VM or appliance, the installation routine configures the local Syslog daemon to forward messages to the agent on TCP port 25224.

The agent then sends the message to your Log Analytics workspace over HTTPS, where it is parsed into an event log entry in the Syslog table in *Microsoft Sentinel > Logs*.

34

Collect data from Linux-based sources using syslog

The Syslog connector has two deployment options: Azure Linux Virtual Machine and agent on a non-Azure Linux Machine.   Azure Linux VM is a simple connect button.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel >
Syslog
Syslog
Not connected
Status
Microsoft
Provider
--
Last Log Received

Description

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to the workspace.

Prerequisites

To integrate with Syslog make sure you have:

✓ Workspace: write permission is required.

Configuration

1. Install and onboard the agent for Linux

Typically, you should install the agent on a different computer from the one on which the logs are generated.

Syslog logs are collected only from Linux agents.

Choose where to install the agent:

- Install agent on Azure Linux Virtual Machine
- Install agent on a non-Azure Linux Machine

Download the agent on the relevant machine and follow the instructions.

Download & install agent for non-Azure Linux machines >

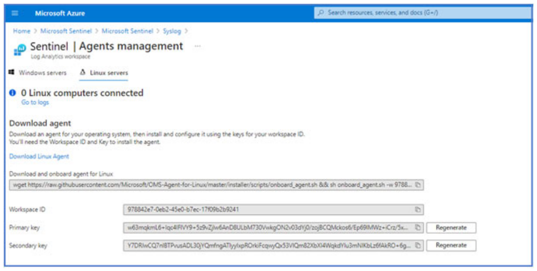
2. Configure the logs to be collected

Configure the facilities you want to collect and their severities.

35

Connect non-Azure Linux Hosts

When connecting non-Azure Linux hosts, you need to manually install the client agent.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Microsoft Sentinel > Syslog >
Sentinel | Agents management
Log Analytics workspace
Windows servers
Linux servers

0 Linux computers connected

Go to logs

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.
You'll need the Workspace ID and Key to install the agent.

Download Linux Agent

Download and onboard agent for Linux

```
wget https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/scripts/onboard_agent.sh && sh onboard_agent.sh -w 9788...
```

Workspace ID: 978842e7-0eb2-45e0-b7ec-17f09b2b9241

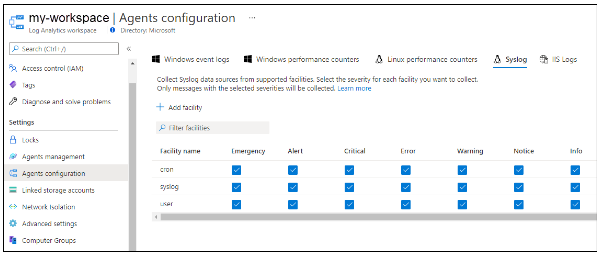
Primary key: w63mqkmL6+lqc4lRVY9+5z9vZjlw6AnD8ULbM730VwkgON2v03dYj0/zojBCQMckos6/Ep69lMWz+iCrz/5x... Regenerate

Secondary key: Y7DRlwCQ7nlBTPvusADL30jYQmfngATlyylxpROrkiFcqwyQx53VIQm82XbXl4WqkdYlu3mNIKbLz6fAkRO+6g... Regenerate

36

Configure the log analytics agent

The Log Analytics agent for Linux will only collect events with the facilities and severities that are specified in its configuration.



Collect Syslog data sources from supported facilities. Select the severity for each facility you want to collect. Only messages with the selected severities will be collected. Learn more

Facility name	Emergency	Alert	Critical	Error	Warning	Notice	Info
cron	☑	☑	☑	☑	☑	☑	☑
syslog	☑	☑	☑	☑	☑	☑	☑
user	☑	☑	☑	☑	☑	☑	☑

37

Parse syslog data with KQL

```
// save as a function named: MyParser

Syslog
| where ProcessName contains "squid"
| extend URL = extract("(([A-Z]+ [a-z]{4,5}:\\/\\/)|[A-Z]+ )([^
:]*)",3,SyslogMessage),
         SourceIP = extract("([0-9]+ )(([0-9]{1,3})\\.([0-9]{1,3})\\.([0-
9]{1,3})\\.([0-9]{1,3}))",2,SyslogMessage),
         User = extract("(CONNECT |GET )([^ ]* )([^ ]+)",3,SyslogMessage),
         RemotePort = extract("(CONNECT |GET )([^ ]*)(:)([0-9]*)",4,SyslogMessage),
         Domain = extract("(([A-Z]+ [a-z]{4,5}:\\/\\/)|[A-Z]+ )([^
:\\/]*)",3,SyslogMessage)
// use the function/parser
MyParser
```

38

Lesson 7: Connect threat indicators to Microsoft Sentinel

39

Lesson introduction

After this lesson, you will be able to:

- Configure the TAXII connector in Microsoft Sentinel
- Configure the Threat Intelligence Platform connector in Microsoft Sentinel
- View threat indicators in Microsoft Sentinel

40

Plan for threat intelligence connectors

Indicator Uses

- Generate alerts and incidents based on matches of log events from your threat indicators.
- Workbooks provide summarized information about the threat indicators
- Hunting queries allow security investigators to use threat indicators
- Notebooks can use threat indicators when you investigate anomalies and hunt for malicious behaviors.

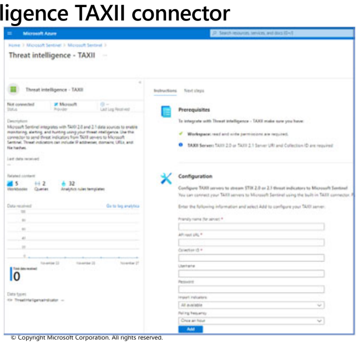
Threat Intelligence Connectors

- Threat intelligence - TAXII
- Threat Intelligence Platforms

41

Connect the threat intelligence TAXII connector

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence.



Description

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use the connector to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Prerequisites

To integrate with Threat intelligence - TAXII make sure you have:

- **Workspace:** read and write permissions are required.
- **TAXII Server:** TAXII 2.0 or TAXII 2.1 Server URI and Collection ID are required.

Configuration

Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Microsoft Sentinel

You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector.

Enter the following information and select Add to configure your TAXII server.

Friendly name (for server) *

API root URL *

Collection ID *

Username

Password

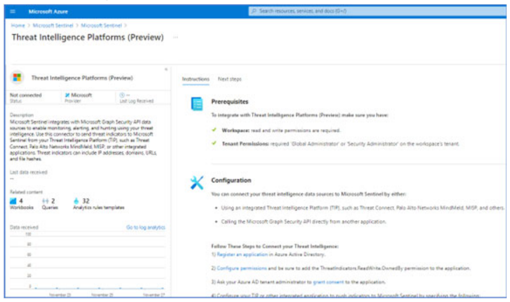
Import indicators: All available

Polling frequency: Once an hour

42

Connect the threat intelligence platforms connector

Microsoft Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Microsoft Sentinel from your Threat Intelligence Platform (TIP)



Threat Intelligence Platforms (Preview)

Threat Intelligence Platforms (Preview)

Description

Microsoft Sentinel integrates with Microsoft Graph Security API data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators to Microsoft Sentinel from your Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Last data received

--

Prerequisites

To integrate with Threat Intelligence Platforms (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

You can connect your threat intelligence data sources to Microsoft Sentinel by either:

- Using an integrated Threat Intelligence Platform (TIP), such as Threat Connect, Palo Alto Networks MindMeld, MISP, and others.
- Calling the Microsoft Graph Security API directly from another application.

Follow These Steps to Connect your Threat Intelligence:

1) Register an application in Azure Active Directory.

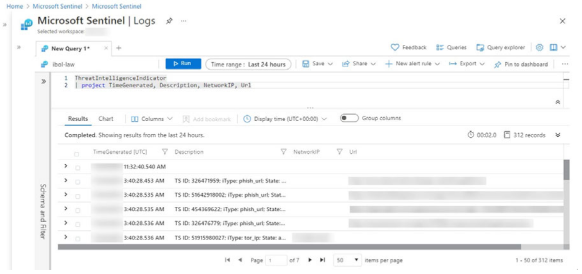
2) Configure permissions and be sure to add the ThreatIndicators.ReadWrite.OwnedBy permission to the application.

3) Ask your Azure AD tenant administrator to grant consent to the application.

4) Configure your TIP or other integrated application to push indicators to Microsoft Sentinel by specifying the following:

43

View your threat indicators



Microsoft Sentinel | Logs

Selected workspace: [redacted]

ibol-law

Time range : Last 24 hours

```
ThreatIntelligenceIndicator
| project TimeGenerated, Description, NetworkIP, Url
```

Completed. Showing results from the last 24 hours.

00:02.0 312 records

TimeGenerated [UTC]	Description	NetworkIP	Url
[redacted] 11:32:40.540 AM			
[redacted] 3:40:28.453 AM	TS ID: 326471959; iType: phish_url; State: ...		[redacted]
[redacted] 3:40:28.535 AM	TS ID: 51642918002; iType: phish_url; Stat...		[redacted]
[redacted] 3:40:28.535 AM	TS ID: 454369622; iType: phish_url; State:...		[redacted]
[redacted] 3:40:28.536 AM	TS ID: 326476779; iType: phish_url; State:...		[redacted]
[redacted] 3:40:28.536 AM	TS ID: 51915980027; iType: tor_ip; State: a...	[redacted]	

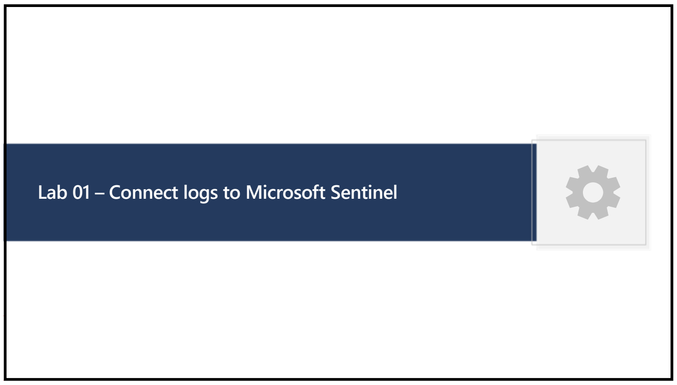
Page 1 of 7 50 items per page 1 - 50 of 312 items

44

Knowledge check

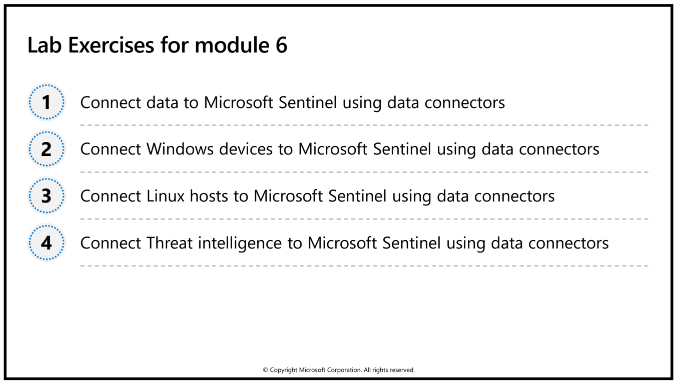
Check your knowledge with the module quiz in your course viewer

45



Lab 01 – Connect logs to Microsoft Sentinel

46



Lab Exercises for module 6

1. Connect data to Microsoft Sentinel using data connectors
2. Connect Windows devices to Microsoft Sentinel using data connectors
3. Connect Linux hosts to Microsoft Sentinel using data connectors
4. Connect Threat intelligence to Microsoft Sentinel using data connectors

47

Microsoft Security

48