Ofer_Shezaf Microsoft

Aug 13 2019 1

Azure Sentinel: The connectors grand (CEF, Syslog, Direct, Agent, Custom and more)

(Last updated Apr 20th, 2021)

Please note that as the built-in list of connectors in Azure Sentinel is growing, this list is not actively maintained anymore. Refer to the Azure Sentinel connector documentation for more information.

Source types

Built-in

Built-in connectors are included in the Azure Sentinel documentation and the data connectors pane in the product itself. Those connectors are based on one of the technologies listed below. Therefore a built-in connector will have a type: CEF, Syslog, Direct, and so forth.

Syslog and CEF

Most network and security systems support either Syslog or CEF (which stands for Common Event Format) over Syslog as means for sending data to a SIEM. This makes Syslog or CEF the most straightforward ways to stream security and networking events to Azure Sentinel.

- Want to learn more about best practices for CEF collection? see here.
- Want to scale CEF or Syslog collection? Use a VM scale set as described here.

The advantage of CEF over Syslog is that it ensures the data is normalized, making it more immediately useful for analysis using Sentinel. However, unlike many other SIEM products, Sentinel allows ingesting unparsed Syslog events and performing analytics on them using query time parsing.

The number of systems supporting Syslog or CEF is in the hundreds, making the table below by no means comprehensive. We will update this list continuously. The table provides links to the source device's vendor documentation for configuring the device to send events in Syslog or CEF.

```
Tip: Want to ingest test CEF data? here is how to do that.
```

Direct

Most Microsoft cloud sources and many other clouds and on-prem systems can send to Azure Sentinel natively. For Microsoft Azure sources, this often uses their diagnostics feature, on which you can read more here.

Agent

The Log Analytics agent can collect different types of events from servers and endpoints listed here. To learn more about the agent, read *Azure Sentinel Agent: Collecting telemetry from on-prem and IaaS server*.

Threat Intelligence (TI)

You can use one of the threat intelligence connectors:

- Platform, which uses the Graph Security API
- TAXII, which uses the TAXII 2.0 protocol

to ingest threat intelligence indicators, which are used by Azure Sentinel's built-in TI analytics rules, and to build your own rules. You can read more about the Threat Intelligence connectors in module #6 of the Azure Sentinel Ninja Training

Custom: Logic Apps, Logstash, Azure Functions, and others

In addition to CEF and Syslog, many solutions are based on Sentinel's data collector API and create custom log tables in the workspace. Those belong to 3 groups:

- Sources that support Logstash, which in turn has an output plug-in that can send the events to Azure Sentinel.
- Sources that have native support for the API.
- Sources for which there is a community or Microsoft field created solution that uses the API, usually using Logic Apps or an Azure function.

You can read more about custom connectors here.

Automation and integration

While all the types above focused on getting telemetry into Azure Sentinel, connectors marked as automation/integration enable Azure Sentinel to implement other use cases such as sending information to another system or performing an action on another system. Those might be API-based on integration or Logic App-based integrations.

The Grand List

Vendor	Product	Connector Type	Connecting and using

Agari	Phishing Defense and Brand Protection	Built-in (Function, Graph Security API)	Instructions
AI Vectra	Detect	Built-in (CEF)	Instructions
Akamai		Built-in (CEF)	Instructions
Alcide	kAudit	Built-in (API)	Instructions
AlgoSec	ASMS	CEF	Instructions and examples
Anomali	Limo	Built-in (TAXII)	Instructions
Anomali	ThreatStream	Built-in (TI Platform)	Instructions
Anomali	Match	Integration	Overview and instructions
Apache	httpd	Built-in (Agent custom logs)	Instructions Also, read using rsyslog or logger as a file forwarder for an alternative method.
Apache	Kafka	Logstash	See Logstash plug-in. Use to get events ser using Kafka, not for Kafka's own audit even
Aruba	ClearPass	CEF	Instructions
AT&T Cyber	AlienVault OTX	TI (Platform)	Using Logic Apps, See instructions
AWS	CloudTrail	Built-in	Sentinel built-in connector
AWS	CloudTrail S3 logs	Custom	Using an Azure Function. See here. Using an AWS Lambda Function. See here.
AWS	CloudWatch	Logstash	See Logstash Plug-in.
AWS	Kinesis	Logstash	See Logstash Plug-in.
AWS	Object Level S3 Logging	Logstash	See here.
AWS	Security Hub	Custom	Azure Function. See here.
Barracuda	WAF	Built-in (API)	Instructions
Barracuda	CloudGen Firewall	API	Sentinel built-in connector
BETTER Mobile	Threat Defense	Built-in (API)	Instructions
Beyond Security	beSECURE	Built-in (API)	Instructions
Carbon Black	Cloud Endpoint Standard (Cb Defense)	Built-in (Function) Syslog	Sentinel built-in connector Instructions
Carbon Black	(Cb Response)	Syslog	Instructions
Checkpoint		CEF	Sentinel Built-in connector
Cisco	ACS	Syslog	Instructions

Cisco	ASA	Cisco (CEF)	Sentinel built-in connector Notes: - Cisco ASA support uses Sentinel's CEF pipeline. However, Cisco's logging is not in CEF format. - Make sure you disable logging timestamp using "no logging timestamp". See here for more details.
Cisco	Cloud Security Gateway (CWS)	CEF	Use the Cisco Advanced Web Security Reporting.
Cisco	FTD	Cisco (CEF)	FTP Platform logs are compatible with ASA logs and can use the same connector (see here).
Cisco	IOS	Syslog	Instructions
Cisco	ISE (NAC)	Syslog	Instructions
Cisco	Web Security Appliance (WSA)	CEF	Use the Cisco Advanced Web Security Reporting.
Cisco	Meraki	Syslog	Instructions Event Types and Log Samples
Cisco	eStreamer	CEF	Using enCore
Cisco	Firepower Threat Defense	CEF Syslog	Using eStreamer enCore Instructions, Event reference
Cisco	FireSight	CEF	Using eStreamer enCore
Cisco	IronPort Web Security Appliance	Syslog	Instructions
Cisco	Nexus	Syslog	Instructions
Cisco	Umbrella	Built-in (Function)	Instructions Also, see this blog post for a custom solution
Cisco	Unified Computing System (UCS)	Built-in (Syslog)	Instructions
Cisco	Viptela SD-WAN	Syslog	Instructions
Citrix	Analytics	Built-in (Direct)	Instructions
Citrix	NetScaler	Syslog	Instructions Message format
Citrix	NetScaler App FW	Built-in (CEF)	Instructions
Clearswift	Web Security Gateway	Syslog	Instructions

Cloudflare			Use Cloudflare Logpush to send to storage and a custom connector to read events fror storage (for example, reading AWS S3 buckets).
Cribl	LogStream	Direct	Instructions
CrowdStrike	Falcon	CEF	Instructions. Use a SIEM connector installec on-premises.
CyberArk	Endpoint Privilege Manager (EPM)	Syslog Logstash	Instructions (for both)
CyberArk	Privileged Access Security (PTA)	CEF	Instructions Message format
Darktrace	Immune	CEF	See announcement. Contact vendor for instructions.
Digital Guardian		CEF	3rd party instructions
DocuSign	Monitor	Custom	See this blog post
Duo Security		CEF	Using Duo LogSync
Extrahop	Reveal	Built-in (CEF)	Instructions
F5	ASM (WAF)	Built-in (CEF)	Instructions
F5	BigIP (System, LTM, AFM, ASM, APM, AVR)	Built-in (Direct)	Instructions
Fastly	WAF	Custom	See this blog post (Logic Apps or Azure Function)
Forcepoint	Web Security (WebSense)	CEF	Instructions Detailed reference
Forcepoint	CASB	CEF	Sentinel built-in connector
Forcepoint	DLP	Direct	Sentinel built-in connector
Forcepoint	NGFW	CEF	Sentinel built-in connector
Forescout	CounterAct	CEF	Instructions
Fortinet		CEF	Sentinel built-in connector Log message reference CEF mapping and examples
Fortinet	FortiSIEM	CEF	Instructions
Fortinet	FortiSOAR	Integration	Instructions

GitHub		Custom	See connector, rules, and hunting queries here
GCP	Cloud Storage	Logstash	See Plug-in. Use to get events stored in GC Cloud Storage, not for Cloud Storage own audit events.
GCP	Pub/Sub	Logstash	See Plug-in. Use to get events sent using Pub/Sub, not for Pub/Sub own audit events
GCP	Stacdriver	Logstash Custom	Through GCP Cloud Storage or GCP Pub/Su as described above. Using GCP Cloud Function. See here.
Group-IB		Custom (TI Platform)	Using Logic Apps. See instructions
GuardiCore	Centra	CEF	Contact vendor for instructions
HP	Printers	Syslog	Instructions
IBM	iSeries	CEF	See here.
IBM	QRadar events	Syslog	Forward raw events or correlation events in raw, parsed, or JSON format. See instructio
IBM	QRadar offenses	Custom (Function)	Blog post
IBM	X-Force	TI (TAXII)	Instructions
IBM	zSecure	CEF	See What's new for zSecure V2.3.0 Note that it supports alerts only.
Illusive	Attack Management System	Syslog	Sentinel built-in connector
Imperva	SecureSphere	CEF	Instructions
Infoblox	NIOS	Built-in (Syslog)	Instructions
InSights		TI (TAXII)	TAXII Instructions and related workbook
Jamf	Pro	Syslog	Instructions
Juniper	ATP	CEF	Instructions
Juniper	JunOS based devices	Built-in (Syslog)	Instructions
Kaspersky	Security Center	CEF	Instructions
ManageEngine	AD Audit Plus	CEF	Instructions (use ArcSight instructions)
ManageEngine	Exchange Reporter Plus	Syslog	Instructions
McAfee	ePO	Syslog	Instructions (Note: TLS only (requires rsyslo TLS configuration)
McAfee	MVISION EDR	Syslog	Instructions

McAfee	Web Gateway	CEF	Instructions
Microfocus	Fortify AppDefender	CEF	Instructions (require authentication; contac vendor for further details).
Microsoft	Active Directory	Agent	Most AD events are logged as part of secur events. Also, See in this list: • LDAP auditing • SMBv1 auditing
Microsoft	Advanced Threat Protection (ATA)	CEF	• Instructions • Log reference
Microsoft	Azure Active Directory (AAD)	Built-in (Diagnostics)	• Instructions • Detections: Sign-in Logs, Audit Logs • Built-in workbooks: • Azure AD Audit Logs, • Azure AD Audit, Activity and Sig in Logs • Azure AD Sign-in logs • Webinars: • "A day in a SOC analyst life" (YouTube, MP4, Presentation) • "Tackling Identity" (YouTube, MP4, Presentation)
Microsoft	Azure Active Directory Domain Services	Diagnostics	• Instructions • Use Workbooks to analyze
Microsoft	Azure Active Directory Identity Protection		• Instructions • Alert information
Microsoft	Azure Azure Activity Azure Subscriptions Azure Management Groups	Direct	• Built-in connector, • Connect through the subscription diagnostic settings to ensure lower latency and broader collection. • For Management groups, Use the API to turn on diagnostics settings • Azure Activity schema • Detections
Microsoft	Application Insights	Direct	• Send to a sentinel workspace • Or use queries across workspaces

Microsoft	App Services & Web Application monitoring	Direct	Instructions and reference architecture
Microsoft	Azure B2B	Direct	Included as part of AAD events
Microsoft	Azure B2C	Direct	collect B2C logs from your B2C tenant to yo primary tenant AAD logs as described here
Microsoft	Azure Cosmos DB	Direct	Instructions
Microsoft	Azure Data Lake Gen 1	Direct	- Instructions - Query examples
Microsoft	Azure Data Factory	Direct	Instructions
Microsoft	Azure Databricks	Direct	Instructions
Microsoft	Azure DDOS	Built-in (diagnostics)	- Built-in connector - Diagnostics instructions - Enable collection using PowerShell - Webinar: Detecting and Responding t Threats using Azure Network Security tools and Azure Sentinel
Microsoft	Azure Defender and Azure Security Center (ASC)	Direct	- Built-in connector for getting ASC ale - Alert list and alert schema. - Use Azure Defender's continuous export feature to get recommendatio findings, secure score, and complianc data to Sentinel.
Microsoft	Azure Defender for IoT	Built-in (Direct)	- Instructions - Alerts Overview
Microsoft	Azure DevOps	Direct	Instructions
Microsoft	Azure Event Hub (subscription)	Logstash	See Logstash Plug-in. Use to get events ser using an Event Hub, not for Event Hub own audit events.
Microsoft	Azure Files	Direct (Diagnostics)	Instructions Schema information

Microsoft	Azure Firewall	Built-in (diagnostics)	• Built-in connector • Workbook • Enable collection using PowerShell or diagnostics • Webinar: Detecting and Responding t Threats using Azure Network Security tools and Azure Sentinel
Microsoft	Azure Front Door	Direct	Instructions
Microsoft	Azure Key Vault (AKV)	Built-in (Diagnostics)	Connect: • Instructions (Built-in, Using policy) • Enable AKV diagnostics using the por • Enable AKV diagnostics using PowerShell Use: • Log schema • Detection rules • Workbook
Microsoft	Azure Information Protection (Classic and Unified Labeling)	Built-in (Direct)	Instructions
Microsoft	Azure Kubernetes Service (AKS)	Direct	• Blog post: Monitoring Azure Kuberne Service (AKS) with Azure Sentinel • Documentation: Enable Azure Monito for containers
Microsoft	Azure Log Analytics	Direct	Collect query auditing and other metrics: Instructions
Microsoft	Azure Logic Apps	Direct	Instructions
Microsoft	Azure Network Security Groups (NSG)	Direct	• Flow logs • Rule activation • Webinar: Detecting and Responding t Threats using Azure Network Security tools and Azure Sentinel

Microsoft	Azure SQL	Built-in (diagnostics)	• Built-in connector • Diagnostics settings instructions
Microsoft	Azure SQL Managed Instance	Direct	Instructions
Microsoft	Azure Site Recovery	Direct	Instructions
Microsoft	Azure Storage	Direct	Instructions Blog: Blob and File Storage Investigations
Microsoft	Azure Storage Content	Custom (Azure Function)	Ingest the content of Azure Storage Blobs. See GitHub.
Microsoft	Azure Synapse	Direct	Instructions
Microsoft	Azure Web Application Firewall (WAF)	Built-in (Diagnostics)	• Blog post • Built-in connector • Webinar: Detecting and Responding t Threats using Azure Network Security tools and Azure Sentinel
Microsoft	BitLocker / MBAM	Agent	Using Windows Event collection. Blog post
Microsoft	Cloud App Security (Alerts, Discovery logs)	Built-in (Direct)	• Instructions • Alerts Information
Microsoft	Cloud App Security (Activity Log)	CEF	Instructions
Microsoft	Defender for Office	Built-in Custom	For AIRs alerts: instructions For other alerts: Use Either a Logic App or an Azure function custom connector. For th Azure Function connector, query for RecordType_d == "28", "41" or "47" .
Microsoft	Defender for Identity (Azure ATP) Alerts	Built-in	• Instructions (Direct) • Instructions (Microsoft 365 Defender) • Alerts overview
Microsoft	Defender for Identity (Azure ATP) Events	CEF	• Instructions • Log reference
Microsoft	Desktop Analytics	Direct	Connect
Microsoft	DNS	Agent	Sentinel built-in connector
Microsoft	Dynamics 365	Built-in	Sentinel built-in connector

Microsoft	Dynamics (not 365)	Agent	Using IIS logs Using Dynamics Trace Files
Microsoft	IIS	Agent	Instructions
Microsoft	Intune	Direct	Connect Use cases
Microsoft	LDAP (Windows Server)	Agent	Configure AD diagnostics logging and set "**16 LDAP Interface Events**" to 2 or above.
Microsoft	Office 365 (Exchange, SharePoint, OneDrive, DLP Alerts)	Built-in	Sentinel built-in connector For details about DLP alerts, read here.
Microsoft	Office 365 (Microsoft Defender for Office; formerly Office ATP, PowerBI, Yammer, Sway, Forms, eDiscovery, and others)	Custom (Azure Function, Logic Apps)	Use Either a Logic App or an Azure function custom connector
Microsoft	Office 365 e-mail trace logs	Custom (Logic Apps)	See Blog Post.
Microsoft	PowerBI Embedded	Direct (Diagnostics)	Instructions
Microsoft	SMBv1 (Windows Server)	Agent	See Enable Auditing on SMB Servers, and tl CmdLet reference
Microsoft	Teams (Call Logs)	Custom	Using Logic Apps

Microsoft	Teams (Management Activity)	Built-in	• Use the built-in Office 365 connector • Use the Hunting use cases or Graph Visualization of External MS Teams Collaborations. • Understand the Teams event schema • Use the custom Logic App or Azure function connectors for special use cases. • Expanding Microsoft Teams Log Data Azure Sentinel: • Extracting Teams file-sharing information • Mapping Teams logs to Teams c records • Merging Teams logs with sign-i activity to detect anomalous actions
Microsoft	Teams Shifts	Custom	Use Either a Logic App or an Azure function custom connector. For the Azure Function connector, query for RecordType_(== "73"
Microsoft	SCCM	Agent	Instructions
Microsoft	SQL Server	Agent	Instructions, parser, rules, and hunting queries You can also audit at the engine level.
Microsoft	Sysmon	Agent	Using Windows Event collection. Blog post
Microsoft	Windows (Security Events)	Agent	• Sentinel built-in connector • Enriching Windows Security Events wi Parameterized Function
Microsoft	Windows (Other Events, Sysmon)	Agent	Instructions
Microsoft	Windows network connections	Agent	VM Insights Wire Data
Microsoft	Windows Firewall	Agent	Sentinel built-in connector

Microsoft	Windows Virtual Desktop	Direct	• Connect using the portal and samples queries • Connect using PowerShell and Sample queries • Blog post covering connecting and using: Monitoring Windows Virtual Desktop environments • Common error codes
Mimecast		Agent	Announcement. For technical instructions, contact the vendor.
Minerva Labs		CEF	Please ask the vendor for instructions.
MISP		TI (Platform)	Sentinel built-in connector
NetApp	ONTAP	Syslog	Instructions Note that those are management activity audit logs and not file usage activity logs.
Netflow		Logstash	Use the Netflow codec plug-in
Nexthink		CEF	Instructions
Nozomi	Guardian	CEF	Contact vendor for details
NXlog		Direct	Instructions
Okta	SSO	Built-in (Function)	Instructions
One Identity	Safeguard	Built-in (CEF)	Instructions
Oracle	Cloud (OCI)	Custom (Azure Function)	Available Here
Oracle	DB	Syslog	Instructions
Orca		Built-in (API)	Instructions
OSSEC		CEF	Instructions
Pager Duty		Automation (Playbook)	Blog post
Palo Alto	Cloudgenix	Syslog	Instructions
Palo Alto	Minemeld	TI (Platform)	Sentinel built-in connector
Palo Alto	PanOS	CEF	Sentinel built-in connector
Palo Alto	Panorama	CEF	Instructions
Palo Alto	Prisma	Syslog Custom	Instructions, Fields Logic Apps using a Webhook and clarificati

Palo Alto	Traps through Cortex	Syslog	Instructions Notes: - Require rsyslog configuration to support RFC5424 - TLS only (requires rsyslog TLS configuratio - The certificate has to be signed by a publi CA
Palo Alto	XDR	CEF	Instructions
Palo Alto	XSOAR	Integration	Forward Azure Sentinel incidents to Palo Al XSOAR
Perimeter 81		Built-in (API)	Instructions
Ping Identity	Federate	CEF	Instructions
Ping Identity	Provisioner	CEF	Instructions
Postgress	DB	Syslog, Windows Event log	Instructions
Proofpoint	On Demand	Built-in (API)	Instructions
Proofpoint	TAP	Built-in (Function)	Instructions
Pulse	Connect	Built-in (Syslog)	Instructions
Qualys	VM	Built-in (Function)	Instructions
Radware	Cloud WAF	Logstash	Instructions
RedHat	OpenShift	Syslog API	Instructions for Syslog Fluentd Log Analytics plugin for API
RedHat	Azure OpenShift	Syslog Custom	Instructions for Syslog Fluentd Log Analytics plugin for API
RiskIQ		Action (Logic Apps)	Azure Logic-Apps built-in connector
Salesforce	Service Cloud	Built-in (Function)	Instructions
SAP	Hana	Syslog	Instructions (requires an SAP account)
SentinelOne		CEF	Please consult the vendor for instructions
SNMP		Syslog	Instructions
Snort		Agent	Instructions

SonicWall		CEF	Instructions Make sure you: - Select local use 4 as the facility. - Select ArcSight as the Syslog format.
Sophos	Central	CEF	Instructions. Note that the script provided b Sophos has to be scheduled using a cron jo which is not documented on the reference page.
Sophos	XF Firewall	Built-in (Syslog)	Instructions
Squadra	secRMM	Built-in (API)	Instructions
Squid Proxy		Built-in (Agent) Syslog	Instructions Configure access logs with either the TCP o UDP modules. Sentinel's built-in queries us the default log format.
Symantec	DLP	Syslog CEF	Instructions. Note that only UDP is support Instructions. Uses response automation.
Symantec	ICDX	Built-in (API)	Instructions
Symantec	Proxy SG (Bluecoat)	Built-in (Syslog)	Instructions
Symantec	Endpoint Protection Manager	Syslog	Instructions
Symantec	Cloud Workload Protection	API	Instructions
Symantec	VIP	Built-in (Syslog)	Instructions
TheHive		Integration	Send new incidents to TheHive
Thinkst	Canary	Syslog	Instructions
ThreatConnect		TI (Platform)	Sentinel built-in connector
ThreatQuotient		TI (Platform)	Sentinel built-in connector
Thycotic	Secret Server	CEF	Instructions
TitanHQ	WebTitan Cloud	Syslog	Instructions
Trend Micro		CEF	Using Control Manager Using LogForwarder
Trend Micro	Apax Central (Cloud and On-prem)	CEF	Instructions

Trend Micro	Deep Security	CEF	Sentinel built-in connector
Tufin	SecureTrack	Syslog	Instructions
Varonis	DatAlert	CEF	Instructions
WatchGuard		CEF	Instructions
Zimperium	Mobile Threat Defense	Built-in (API)	Instructions
zScaler	Internet Access (ZIA)	Built-in (CEF)	Instructions
zScaler	Private Access (ZPA)	Logstash	Use LSS. Since LSS sends raw TCP but not Syslog, you will have to use Logstash and n Azure Sentinel's native connector.
Zoom		Custom	Using Azure Function. See blog post.

11 Likes

Share

Comments

Fergie635 New Contributor

Aug 26 2019 06:17 AM

7 Likes

arvkris Frequent Visitor

Nov 15 2019 05:54 AM

0 Likes

Ofer_Shezaf Microsoft

Nov 17 2019 08:57 AM