



Welcome to the Azure Sentinel webinar

We will start at **2-3 minutes after** the scheduled time to accommodate those still connecting.

Questions? Feel free to type them in the instant message window at any time. Note that any questions you post will be public. You have the option to post questions anonymously. After the webinar, you can ask questions at <https://aka.ms/AzureSentinelCommunity>.

This webinar is being **recorded**. We'll post the recordings to our community forums at <https://aka.ms/SecurityWebinars>.

Teams Live Event currently doesn't support audio capability for the audience. Closed captions are available during the webinar and with the recordings.

Please give us your **feedback** on this webinar at <https://aka.ms/SecurityCommunityWebinarFeedback>.

Join our Community: <https://aka.ms/SecurityCommunity>

Azure Sentinel Webinar

Deep Dive on Threat Intelligence

Jason Wescott – Principal Program Manager, Azure Security
jwes@microsoft.com

Cyber Threat Intelligence (CTI) Overview


There are many forms of threat intelligence


- Both “indicators” and “observables” are often referenced as Tactical TI
- **Operational** TI includes richer contextual information such as tools, techniques, and procedures (TTPs)
- **Strategic** TI summarizes actor motivations, intentions, and capabilities
- Open standard formats include STIX and MISP




Threat Intelligence experiences in Azure Sentinel

Data connectors


**Threat Intelligence - TAXII (Preview)**
Microsoft

**Threat Intelligence Platforms (Preview)**
Microsoft

Workbooks

**Threat Intelligence**
MICROSOFT

Analytics

(Preview) TI map URL entity to OfficeActivity data  Scheduled


Hunting

↑↓	Query	↑↓	Provider	↑↓	Data Source
★	Preview - TI map File entity to Security Event		Microsoft		SecurityEvent

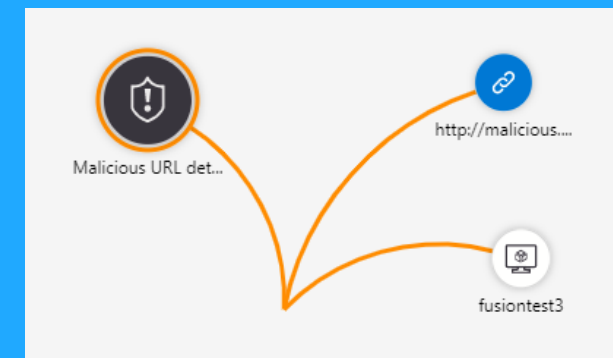
Incidents

Incident Id ↑↓	Title
3438	TI-based malicious URL related to razor threat

Notebooks

**Entity Explorer - Domain and URL**
Microsoft

Investigations

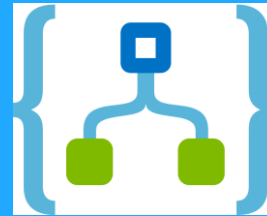


How do I bring threat intelligence to Azure Sentinel?

Integrated Threat Intelligence Platforms



Custom applications via Microsoft Graph Security API



Azure Logic App

(New) TAXII servers



Azure Sentinel data connectors



Threat Intelligence - TAXII (Preview)
Microsoft



Threat Intelligence Platforms (Preview)
Microsoft

Demo

Threat Intelligence Platforms data connector

Threat Intelligence Platforms data connector

Step by step

1. Register an app to represent your TIP or custom application
2. Configure your TIP or custom application to send threat indicators to Microsoft
3. Enable the Threat Intelligence Platforms data connector in Azure Sentinel

Demo

Threat Intelligence TAXII data connector

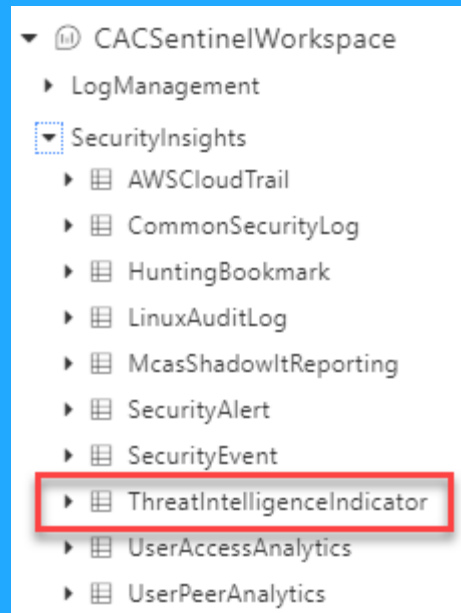
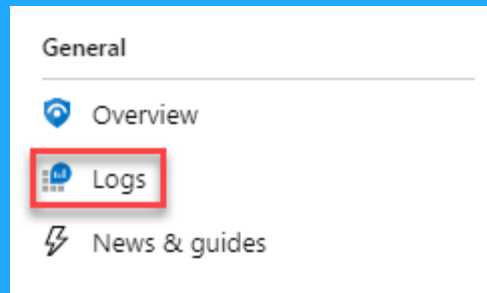
Threat Intelligence TAXII data connector

Step by step

1. Discover TAXII server collections
2. Enable TAXII data connector in Azure Sentinel for each collection

Where is my threat intelligence stored?

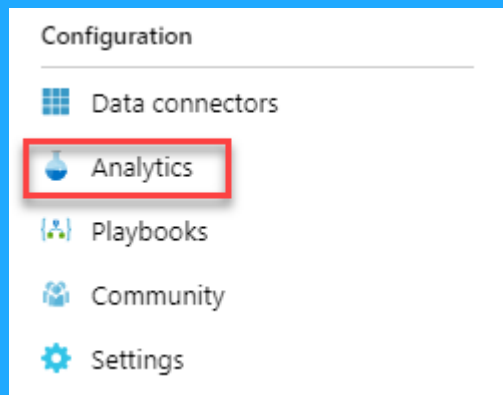
ThreatIntelligenceIndicator log table



SourceSystem	SecurityGraph
Action	alert
ActivityGroupNames	[]
ApplicationId	96B550D5-48A2-41FB-B42E-2E9F9C57E73C
AzureTenantId	69d28fd7-42a5-48bc-a619-af56397b9f28
ConfidenceScore	100
Description	URL indicator from urlhaus.URL
ExternalIndicatorId	URL:http://laveronicamagazine.com/wp-includes/js/jak/zaynn/kak.doc
ExpirationDateTime [UTC]	2019-12-10T19:13:52.044Z
IndicatorId	3B232ECC8DB2D9CE9B6639057F593F6D95BE1F04FD822A65E3682A04657471DD
ThreatType	Malware
Active	true
MalwareNames	[]
Tags	[]
TrafficLightProtocolLevel	green
Url	http://laveronicamagazine.com/wp-includes/js/jak/zaynn/kak.doc

Configure custom alert rules in Analytics

Included library of (26) rule templates for threat intelligence



NAME	↑↓	RULE TYPE
FastTrack TI map IP entity to AzureActivity		Scheduled

Analytic rule details

Name	FastTrack TI map IP entity to AzureActivity
Description	Identifies a match in AzureActivity from any IP IOC from TI
Tactics	Impact
Severity	Medium
Status	Enabled

Analytic rule settings


Rule frequency	Every 1 hour
Rule period	Last 14 days data
Rule threshold	Trigger alert if query returns more than 0 results
Suppression	Not configured

Mapped entities

- IP
- Account

Investigate incidents with automatic URL detonation

- Alerts and incidents generated when observables (IP, Domain, URL, File) are matched with log data (Azure activity, AAD sign in, CEF, DNS, Office activity, security alerts, AWS Cloud Trail, syslog)
- URLs are automatically detonated using Microsoft threat intelligence

 **Malicious URL detected**
Incident Id: 3823

Medium
SEVERITY

▼

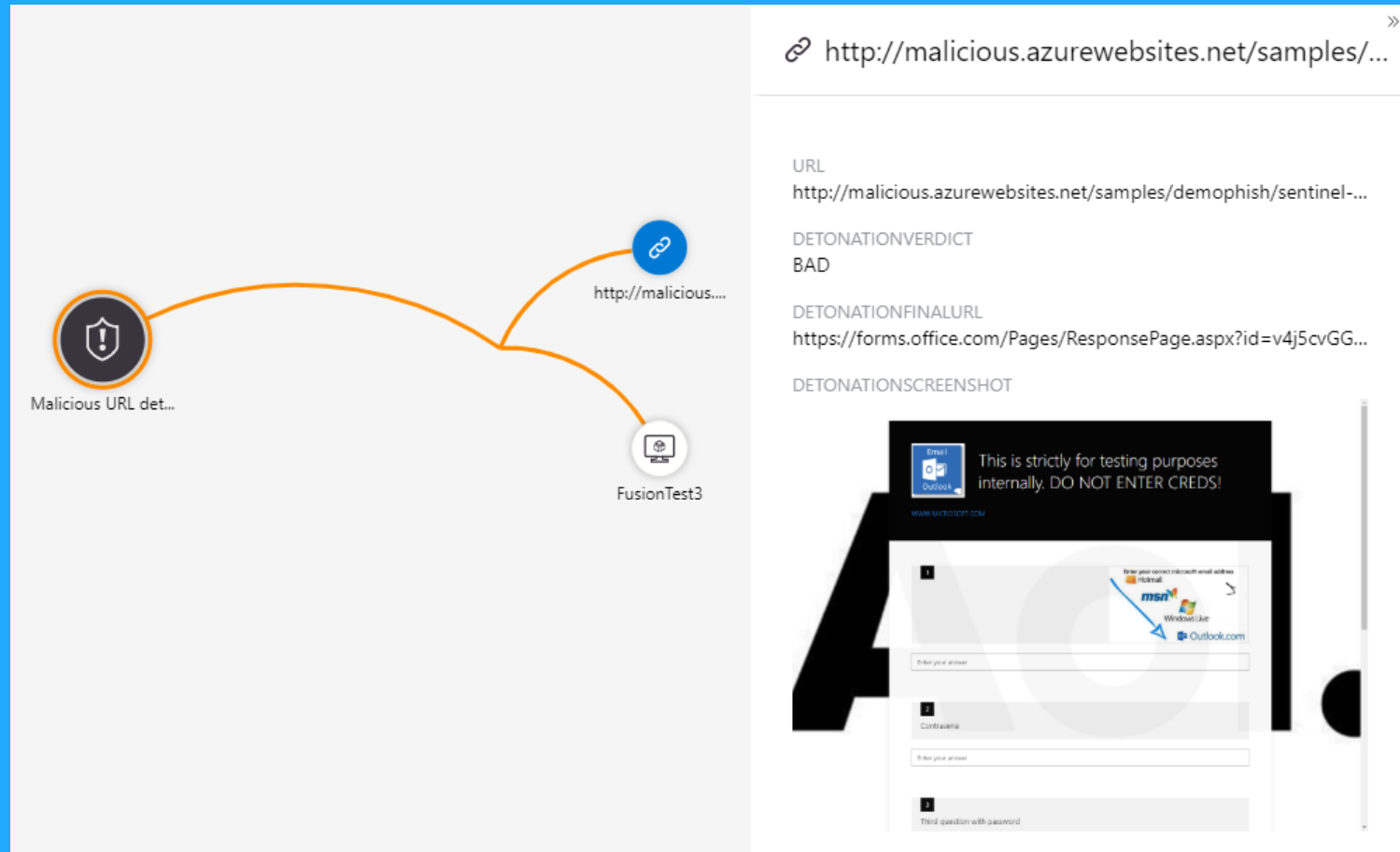
New
STATUS

▼

Unassigned
OWNER

Evidence
1 1 0
Events Alerts Bookmarks

Entities
0 1 0 1
Account Host IP URL



Malicious URL det...

http://malicious...

FusionTest3

http://malicious.azurewebsites.net/samples/...

URL
http://malicious.azurewebsites.net/samples/demophish/sentinel-...

DETONATIONVERDICT
BAD

DETONATIONFINALURL
https://forms.office.com/Pages/ResponsePage.aspx?id=v4j5cvGG...

DETONATIONSCREENSHOT

This is strictly for testing purposes internally. DO NOT ENTER CRED!

msn

Windows Live

Outlook.com

Enter your answer

Contraseña

Enter your answer

Third question with password

View threat intelligence metrics in the TI Workbook



Threat Intelligence MICROSOFT

Gain insights into threat indicators, including type and severity of threats, threat activity over time, and correlation with other data sources, including Office 365 and firewalls.

Required data types: ⓘ



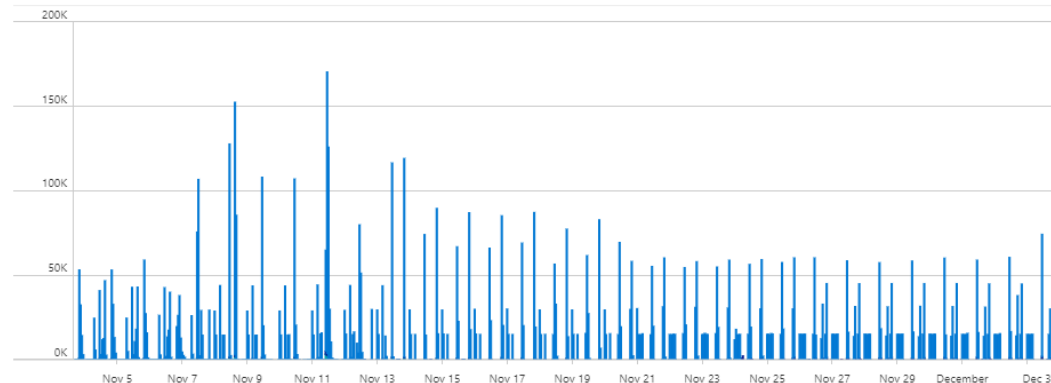
ThreatIntelligenceIndicator

- View the Azure Sentinel activity related to threat intelligence
- A template is provided but everything in the workbook is fully customizable

Threat Intelligence overview

TimeRange: Last 30 days ▾

Indicators ingested into Sentinel by indicator type and date



Alert counts by indicator

Value	↑↓	ThreatType	↑↓	Description	↑↓	Alerts	↑↓
http://www. [redacted] /IVPLeHMT9/		Malware		URL indicator from urlhaus.URL		60	
http:// [redacted] .com/Client/Invoice-06-07-18/		Malware		URL indicator from urlhaus.URL		57	
http:// [redacted] .com/EN/CyberMonday/		Malware		URL indicator from urlhaus.URL		47	
http:// [redacted] .com/Document/US_us/Invoices-attached/		Malware		URL indicator from urlhaus.URL		46	
185.176. [redacted]		WatchList		One of the five RIRs announced a (new) location mapping...		43	
https:// [redacted] -catalana-hipica.us/server/bin_output30...		Malware		URL indicator from urlhaus.URL		41	
https:// [redacted] .uk/Remittance_121118FI06_PDF.jar		Malware		URL indicator from urlhaus.URL		39	
http:// [redacted] .com/733683H/BIZ/Commercial		Malware		URL indicator from urlhaus.URL		38	
http:// [redacted] .com/6kYDVzhpWoYLQ67g/BIZ/lhreSpark...		Malware		URL indicator from urlhaus.URL		34	
https:// [redacted] .com/Yeahok.exe		Malware		URL indicator from urlhaus.URL		33	
https://a. [redacted] se/KZilEgXz4rO1_CUENTA_DE_COBRO.zip		Malware		URL indicator from urlhaus.URL		28	

In Review...

Step by step

1. Bring your threat intelligence feeds to Azure Sentinel using the Threat Intelligence Platforms and TAXII data connectors
2. Use the built-in custom alert templates in Analytics to generate alerts and incidents
3. Leverage Microsoft threat intelligence with built-in URL detonation in investigations
4. View (and customize) the Threat Intelligence Workbook to understand how your threat intelligence is performing in Azure Sentinel
5. Utilize threat intelligence for ad-hoc Hunting queries (templates included)
6. Dive deep into your data and leverage threat intelligence with (Jupyter) Notebooks

Thank you!

Learn more in this Azure Sentinel Threat Intelligence blog post

<https://aka.ms/sentineltriblog>



Thank You for Joining Us!

Recordings will be posted to our community forums at <https://aka.ms/SecurityWebinars>.

Teams Live Event currently doesn't support audio capability for the audience. Closed captions are available during the webinar and with the recordings.

You can ask additional **questions** at <https://aka.ms/AzureSentinelCommunity>.

Please give us your **feedback** on this webinar at <https://aka.ms/SecurityCommunityWebinarFeedback>.

Join our Community: <https://aka.ms/SecurityCommunity>

For any questions or comments on our documentation (<https://docs.microsoft.com>) contact directly at MSsecuritydocs@microsoft.com