



Microsoft Secure



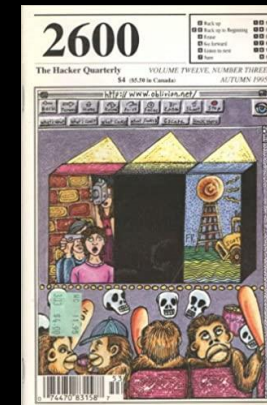
Threat intelligence: the next level of security

Daniel Donda
Alisson Araujo

Daniel Donda



- Over 25 years of experience in the IT field.
- Microsoft MVP since 2011
- Book Author
- Multiple certifications including *Microsoft MCP, MCSA, and MCSE, CompTIA Security+ and Cybersecurity Analyst, EC-Certified Ethical Hacker (CEH), and Certified Information System Security Professional (CISSP).*
- <https://danieldonda.com> 🇧🇷



Agenda

- Who is the actor ? The Threat Is Real?
- What is Cyber Threat Intelligence (CTI)?
- Which CTI type should I use?
- Where to start?
- Why Microsoft TI platform?

“Attackers are adapting and finding new ways to implement their techniques, increasing the complexity of how and where they host campaign operation infrastructure.”

-Amy Hogan-Burney, General Manager, Digital Crimes Unit

531,000

unique phishing URLs and 5,400 phish kits were taken down at the direction of our Digital Crimes Unit.

70 billion

email and identity threat attacks were blocked by Microsoft last year alone.

2.75 million

site registrations were successfully blocked by Microsoft to get ahead of criminal actors that planned to use them to engage in global cybercrime.

SPOTLIGHT ON HUMAN-OPERATED RANSOMWARE ATTACKS

Cybercriminal abuse of infrastructure

IoT devices are a popular target for cybercriminals using widespread botnets. Unpatched routers can be used to gain access to networks and execute malicious attacks.

Is hacktivism here to stay?

The war in Ukraine saw a surge in hacktivism, with volunteer hackers deploying tools to cause damage to political opponents, organizations, and even nation states.



Who is the actor ? The Threat Is Real?

The Threat Is Real

The Threat

- Geopolitical
- Cyber-espionage
- Industrial competition
- Sabotage
- Hacktivism
- Cryptojacking
- Ransomware/eCrime

The Threat Actors

- Criminal organizations
- Nation-state actors
- Hacktivists
- Competitors
- Insiders
- Private sector offensive actors



"Don't forget the fundamentals."


- ✓ Implement robust [security controls](#)
- ✓ Regularly update software and systems
- ✓ Educate employees
- ✓ Monitor networks and systems
- ✓ Regularly backup data

CYBER THREAT INTELLIGENCE





What is Cyber Threat Intelligence (CTI)?

A person wearing a dark hoodie is seen from behind, sitting at a desk in a dimly lit room. They are surrounded by several computer monitors. The monitors display various types of data: some show lines of code in a dark-themed editor, others show a world map with glowing connections, and one shows a flowchart with decision diamonds and process boxes. The overall atmosphere is technical and focused on cybersecurity or data analysis.

"Cyber Threat Intelligence is the superpower that empowers organizations to outsmart cybercriminals, stay ahead of evolving threats, and protect what matters most."

Why is threat intelligence important?

- **Unmasking** your likely **adversaries** and their motivations.
- **Exposing** an adversary's tactics, techniques, and procedures **TTPs**
- **Identifying** common indicators of compromise **IOCs** that signal an active breach.
- Suggesting a set of **actions to take when you are attacked**
- Automatically **blocking** entire **attacks**
- Informing your broader **security strategies** and workflows with rich threat data.

Which CTI type should I use?



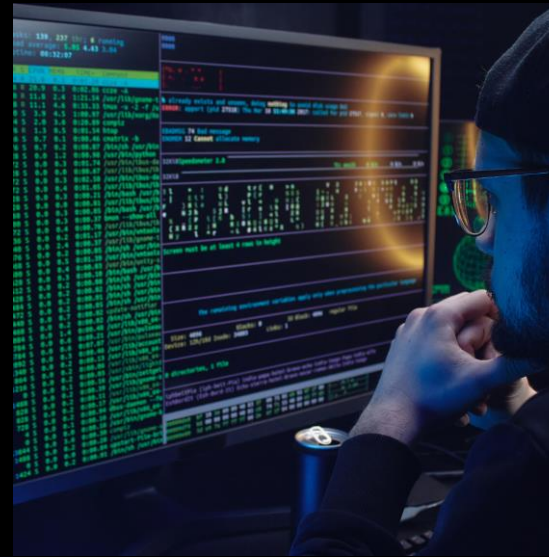
Strategic intelligence

The trends and patterns that are emerging in the world of cyber security



Tactical intelligence

Real-time information about current and imminent threats



Operational intelligence

Deeper understanding of the tactics, techniques, and procedures (TTPs)



Technical intelligence

Refers to signs that an attack is happening such as IOCs.

Where to start ?

THE WORLD NEWS

\$1.00

Since 1883

YOUR NUMBER ONE SOURCE FOR HEADLINES

WAR ENDS!

ENDS IN ALL

STREETS CROWDED AS
CELEBRATIONS BEGIN IN
MAJOR CITIES.

ALL HOSTILITIES TO
CEASE TODAY. 4 YEAR
WAR FINAL ENDS.

For information please
consult edition

Strategic intelligence

A year of Russian hybrid warfare in Ukraine

What we have learned about nation state tactics so far and what may be on the horizon

March 15, 2023



```
01000001 00100000 01111001  
01100101 01100001 01110010  
00100000 01101111 01100110  
00100000 01010010 01110101  
01110011 01110011 01101001  
01100001 01101110 00100000  
00001010 01101000 01111001  
01100010 01110010 01101001  
01100100 00100000 01110111  
01100001 01110010 01100110  
01100001 01110010 01100101  
00100000 01101001 01101110  
00100000 01010101 01101011  
01110010 01100001 01101001  
01101110 01100101
```





Tactical intelligence



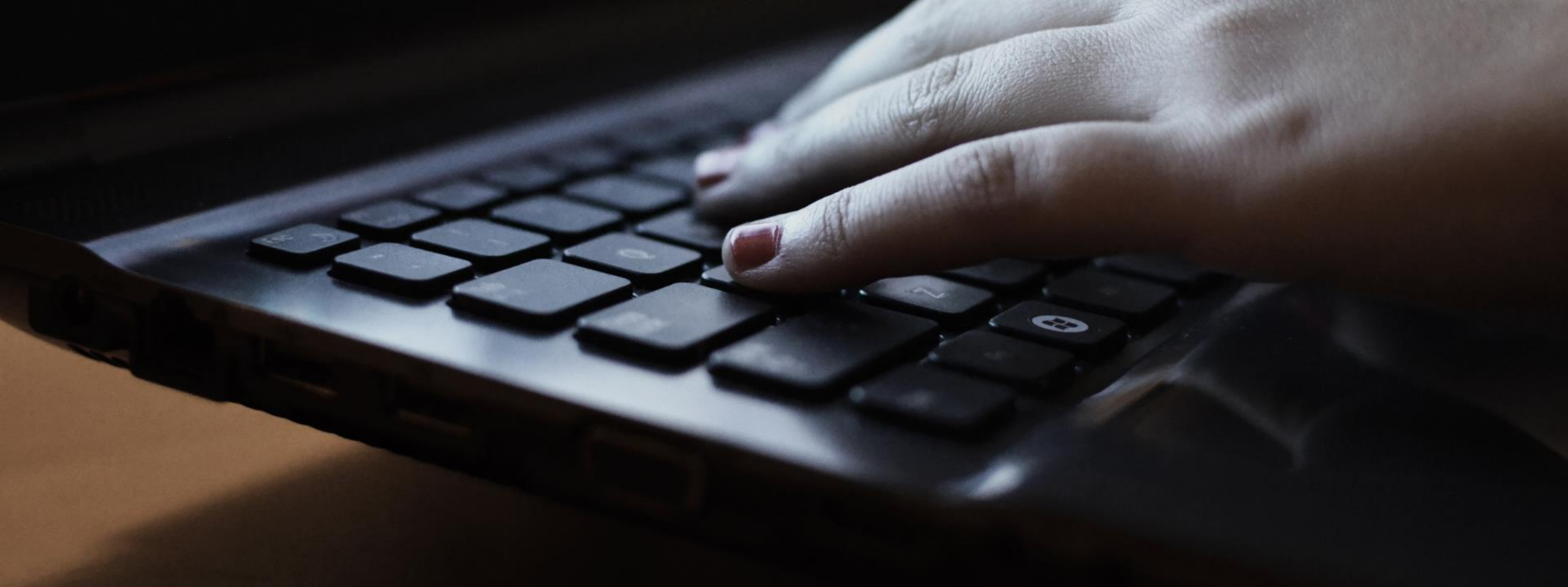
Operational intelligence



Technical Intelligence

What type of CTI should I use?

-All.



Why Microsoft TI platform?

Big Numbers

- **43 trillion** signals synthesized daily, using sophisticated data analytics and AI algorithms to understand and help protect against digital threats and criminal cyberactivity.
- **8,500+** engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across 77 countries.
- **15,000+** partners in our security ecosystem who increase cyber resilience for our customers.

Microsoft threat intelligence platform

Microsoft | Microsoft Security | Solutions | Products | Services | Partners | Resources | Contact Sales | Start free trial | All Microsoft | Search | Sign In

Microsoft security intelligence

Security research and threat intelligence from our global network of security experts.

Recent articles | Products and solutions | Topics | Series | Related blogs | Subscribe

Threat watch

The cyber and influence operations of the war in Ukraine's digital battlefield

Microsoft threat intelligence examines a year of cyber and influence operations in Ukraine, uncovers new trends in cyber threats, and what to expect as the war enters its second year.

[Read report](#)

Iran responsible for Charlie Hebdo attacks

Microsoft is attributing a recent influence operation targeting French magazine Charlie Hebdo to an Iranian nation-state actor Microsoft tracks as NEPTUNUM.

[Learn more](#)

Cyber Signals briefing: Growing vulnerabilities in IoT and OT

In our latest Cyber Signals briefing, we discuss the increasing prevalence of high-severity vulnerabilities in IoT and OT connectivity. Hear from threat intelligence experts on how to increase resilience against these threats.

[Watch video](#)

[View all Threat Watch articles >](#)

Microsoft | Microsoft Security | Solutions | Products | Services | Partners | Resources | Contact Sales | Start free trial | All Microsoft | Search | Sign In

Be among the first to see what an AI-powered future means for cybersecurity at Microsoft Secure on March 28. [Register now >](#)

Microsoft Defender Threat Intelligence

Help protect your organization from modern adversaries and threats like ransomware.

[Contact Sales](#)

Stop Ransomware with Microsoft Security

Don't just react to threats. Get ahead of them. Watch this digital expert to learn how to safeguard your organization from today's attacks – and be ready for tomorrow's.

[Watch now >](#)

Uncover your adversaries

Global threat activity

Countries or regions with the most malware encounters in the last 30 days

Search encyclopedia

Worldwide

87,106,836 devices with encounters

Top threats:

- HackTool:Win32/AutoKMS
- Trojan:Win32/Vicacac.A
- HackTool:Win32/ArmedMS
- HackTool:Win32/Kerygen
- Trojan:Script/Malwarec.H

Microsoft Sentinel

See and stop threats across your entire enterprise with intelligent security analytics.

[Try for free](#) [Contact Sales](#)

Microsoft named a Leader for SIEM by Gartner

See how Microsoft is recognized as a Leader in the 2022 Gartner® Magic Quadrant™ for Security Information and Event Management.

[Read the report >](#) [Read the blog >](#)

Microsoft | Microsoft Security | Solutions | Products | Services | Partners | Resources | Contact Sales | Start free trial | All Microsoft | Search | Sign In

Experiencing a cybersecurity attack? Microsoft can help. [Get incident response >](#)

Microsoft Defender Experts for Hunting

Proactive threat hunting that extends beyond the endpoint.

[Get started](#) [Learn more](#)

Microsoft Defender Experts for Hunting is generally available

Extend your team of experts and reduce risk with more accurate detection.

[Read the announcement >](#)

[Overview](#) [Included capabilities](#) [Resources](#)

Microsoft Sentinel | Threat intelligence

Selected workspace: 'msftsecure'

Search Refresh Add new Import Add tags Delete Columns Threat intelligence workbook Guides & Feedback

- General
 - Overview
 - Logs
 - News & guides
 - Search
- Threat management
 - Incidents
 - Workbooks
 - Hunting
 - Notebooks
 - Entity behavior
 - Threat intelligence
 - MITRE ATT&CK (Preview)
- Content management
 - Content hub (Preview)
 - Repositories (Preview)
 - Community
- Configuration
 - Data connectors
 - Analytics
 - Watchlist
 - Automation
 - Settings

0 TI alerts 1,3K TI indicators 1 TI sources

Search by name, values, description or tags

Type : All Source : All Threat Type : All Confidence : All Expiring Before : All

Name	Values	Type	Confidence	Alerts	Tags
<input type="checkbox"/>	OTX feed=Collection: ... renomesolar.com		--	0	...
<input type="checkbox"/>	OTX feed=Collection: ... palasedelareforma.com		--	0	...
<input type="checkbox"/>	OTX feed=Collection: ... noosaerty.com		--	0	...
<input type="checkbox"/>	OTX feed=Collection: ... mandalorecnote.com		--	0	...
<input type="checkbox"/>	OTX feed=Collection: ... ituitem.net		--	0	...
<input type="checkbox"/>	OTX feed=Collection: ... fae4e3388e95d2e71025...		--	0	...
<input type="checkbox"/>	OTX feed=Collection: ... f4c46cf9ffd25764a63bc...		--	0	...
<input type="checkbox"/>	OTX feed=Collection: ... f2ab26557364d548a40a...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... dcf2a4d0ee66d3f47d9f...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... d5332249cfef78250100...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... d1ac1a32c791141d89d...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... d02a84eb7972ce9e1a0...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... c823261b03d11d23e76...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... b1c1977b5d5b0705fa3e...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... accf567245e184467ead...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... acc3d0964c41f6553d3a...	file	OTX-API	0	...
<input type="checkbox"/>	OTX feed=Collection: ... a01a82f3edd13700ea85...	file	OTX-API	0	...

Type

- Select all
- file
- ipv4-addr
- domain-name
- url

OK Cancel

< Previous 1 - 100 Next >

OTX feed=Collection: user_AlienVault, pulse_name=URL fil...

Confidence Alerts domain-name Types

Values Tags

domain-name : renomesolar.com

Threat types Description

Name Revoked

OTX feed=Collection: user_AlienVault, pulse_name=URL files and WebDAV used for IcedID (Bokbot) infection

Confidence Source

-- OTX-API

Pattern Kill chains

[domain-namevalue = 'renomesolar.com']

Created Valid from

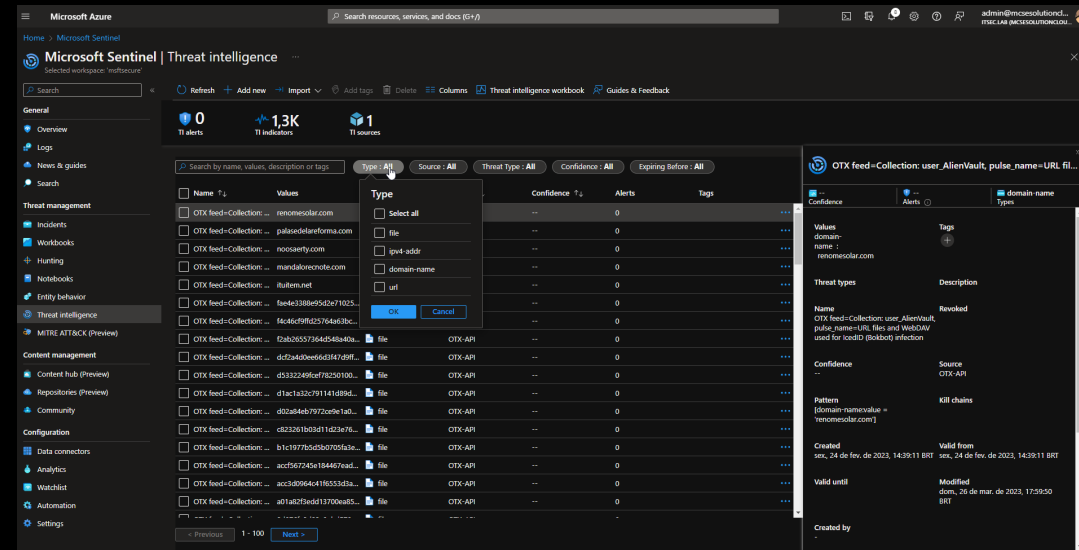
sex, 24 de fev. de 2023, 14:39:11 BRT sex, 24 de fev. de 2023, 14:39:11 BRT

Valid until Modified

dom, 26 de mar. de 2023, 17:59:50 BRT

Created by

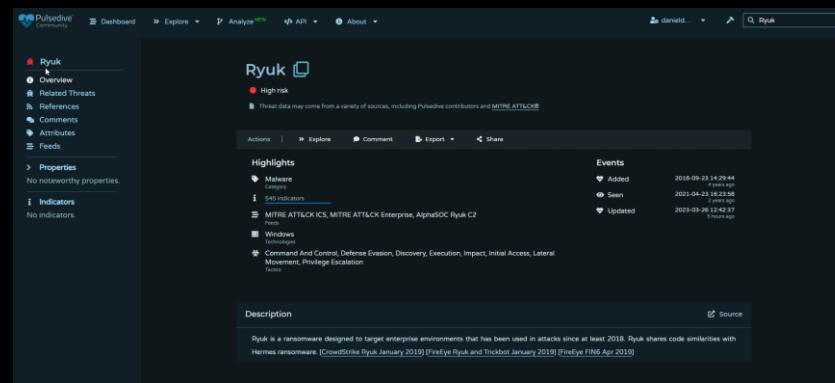
Threat intelligence – TAXII - Microsoft Sentinel integrates with **TAXII 2.0 and 2.1 data sources** to enable monitoring, alerting, and hunting using your threat intelligence.



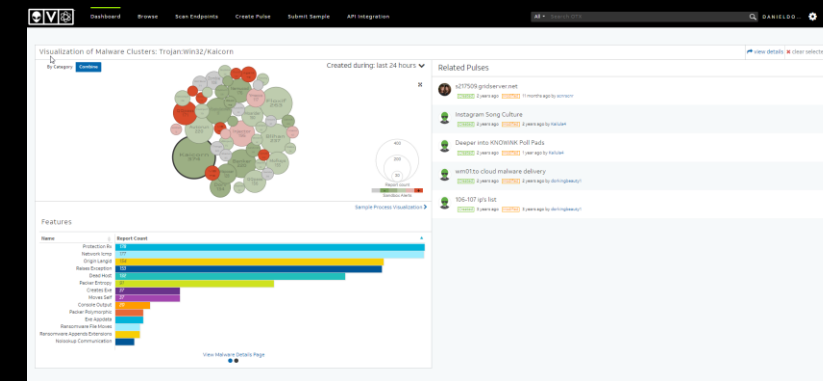
Threat Intelligence Platforms (Preview). Use this connector to send threat indicators to Microsoft Sentinel from your Threat Intelligence Platform (TIP), such as **Threat Connect, Palo Alto Networks MindMeld, MISP, or other integrated applications.** Threat indicators can include IP addresses, domains, URLs, and file hashes.



<https://www.misp-project.org/>



<https://pulsedive.com/>



<https://otx.alienvault.com/>



A step ahead



Thank you



Registration is now open!

Microsoft Secure

March 28, 2023

aka.ms/microsoftsecure





Thank you / Obrigado



Microsoft Secure