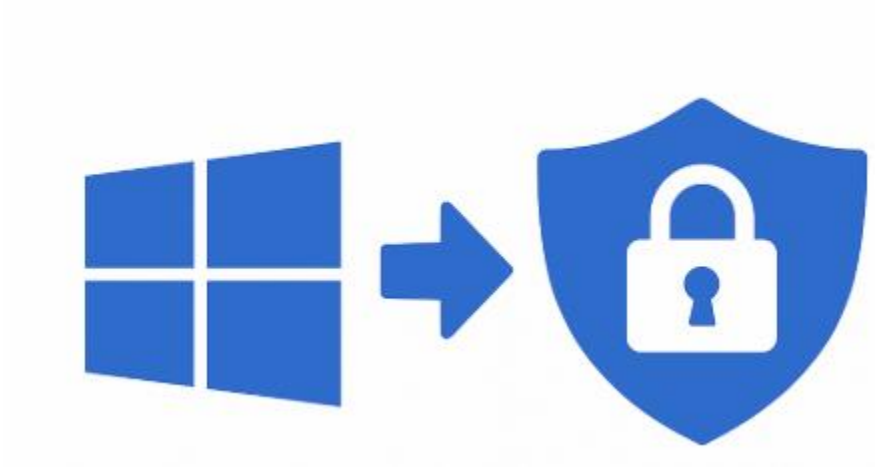


Feeding Sentinel With MS Defender Threat Intelligence, Creating IOC

Adrian Cortez

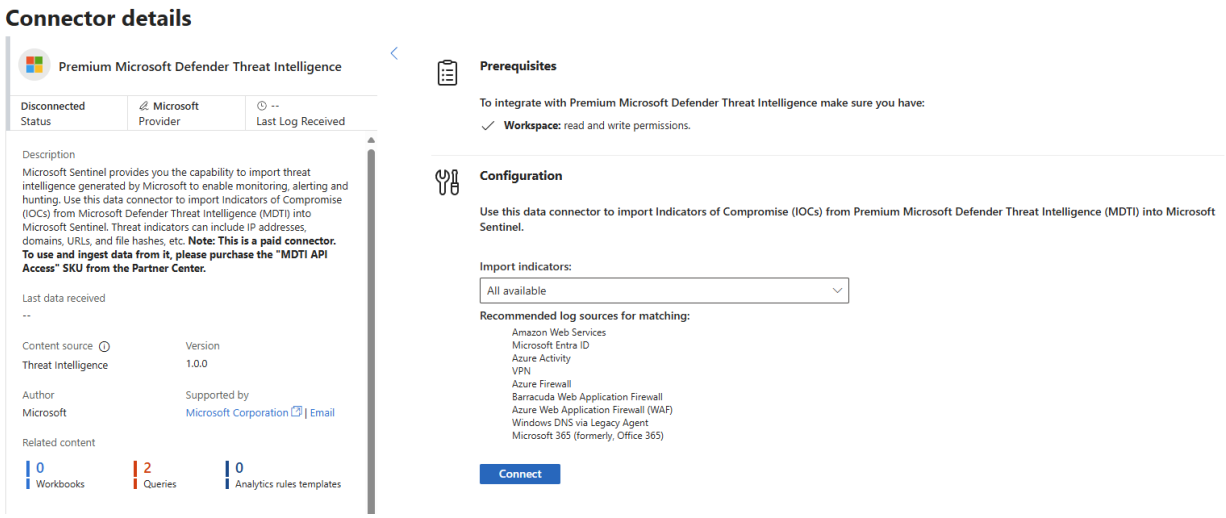
Overview

Feeding Defender threat intelligence into Sentinel makes your SIEM smarter and more effective at catching and responding to real threats faster. It provides the following:

- Enhanced Detection: Defender threat intelligence provides rich, up-to-date info on emerging threats, malware, indicators of compromise (IOCs), and attacker tactics. Feeding this into Sentinel helps improve detection accuracy.
- Contextual Awareness: Sentinel can correlate alerts and events with Defender's threat intel, giving more context to incidents, so security analysts can better understand the severity and scope.
- Proactive Defense: By ingesting Defender threat intelligence, Sentinel can trigger faster automated responses or alerts based on known bad actors or malicious activity patterns identified by Defender.
- Unified Security Monitoring: It creates a centralized place in Sentinel where data from Defender and other sources come together, improving visibility across your entire environment.

Onboard Microsoft Defender Threat Intelligence data connector

1. Sentinel > Configuration > Data Connectors > Premium Microsoft Defender Threat Intelligence (Connector Details) > Connect
2. This allows Sentinel to automatically ingest IOCs collected and curated with Defender



Manually Create Indicators of Compromise

For this exercise, I found a malicious IP address from AbuseIPDB

Creating an IOC includes classifying the indicator type, the kill chain and phase, severity level, traffic light protocol, and more.

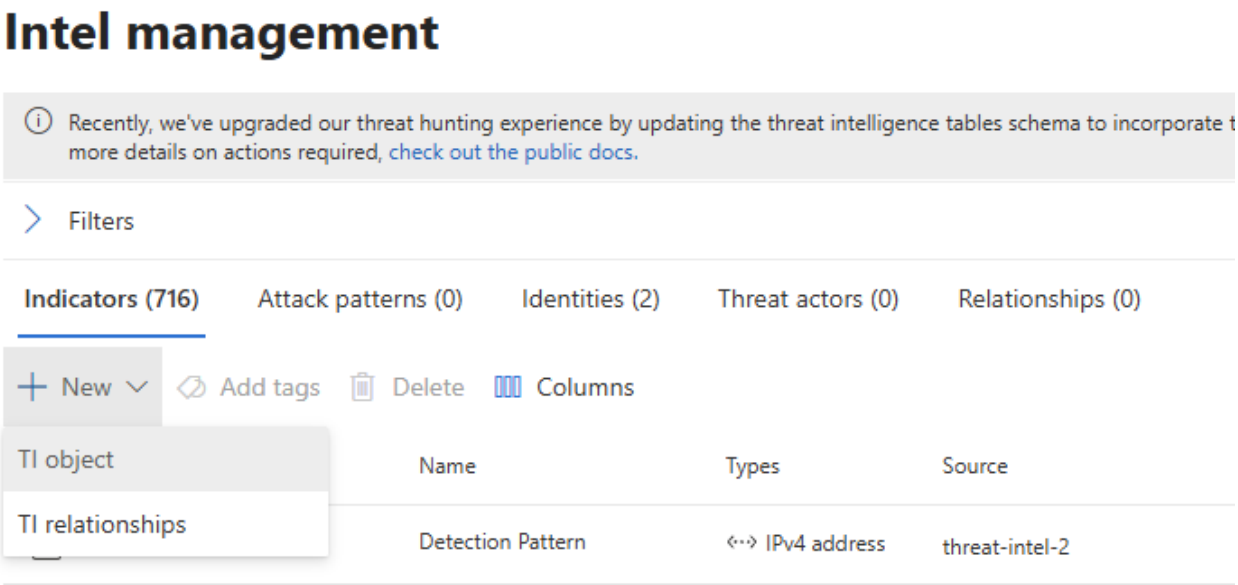
These fields can help security analysts understand what stage of the attack they are currently in and which incidents are more prioritized, which helps with response.

- Reconnaissance – attacker scanning your network.
- Command and Control (C2) – IP used to control infected machines.
- Actions on Objectives – IP used to exfiltrate data.

TLP ensures you can share indicators safely without violating agreements or leaking sensitive details.

- TLP:RED – only for specific recipients, no further sharing. Should be used for information that is highly sensitive and could cause harm if shared beyond specific individuals.
- TLP:AMBER – share within your organization. Should be used when information is sensitive but can be shared internally to support defensive actions.

- TLP:GREEN – share with peers/partners. Should be used when defending against threats and is safe to share within the organization, but not to the public.
- TLP:WHITE – share publicly.



New TI object

Object type *

Indicator

Pattern *

Pattern builder Free text

IPv4 address

IPv4 address value *

123.56.220.219

+ New observable

[ipv4-addr:value = '123.56.220.219']

Name

Web App Attack

Indicator types

Compromised, Malicious activity

Kill chains

Kill chain phase

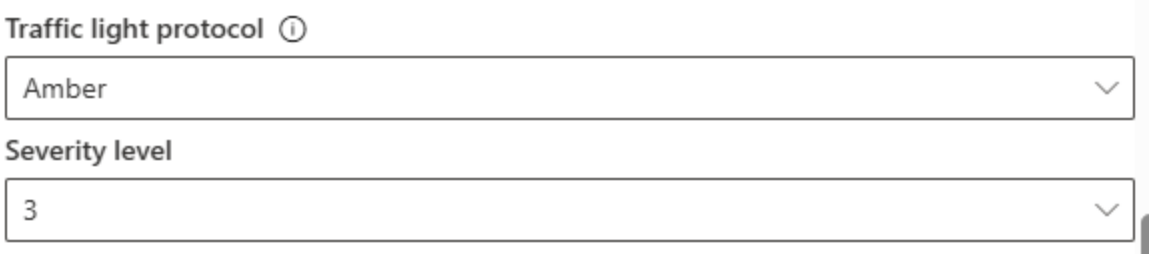
Kill chain *

Mitre

Phase name *

InitialAccess

+ Add kill chain



View Manual IOC and Defender IOC

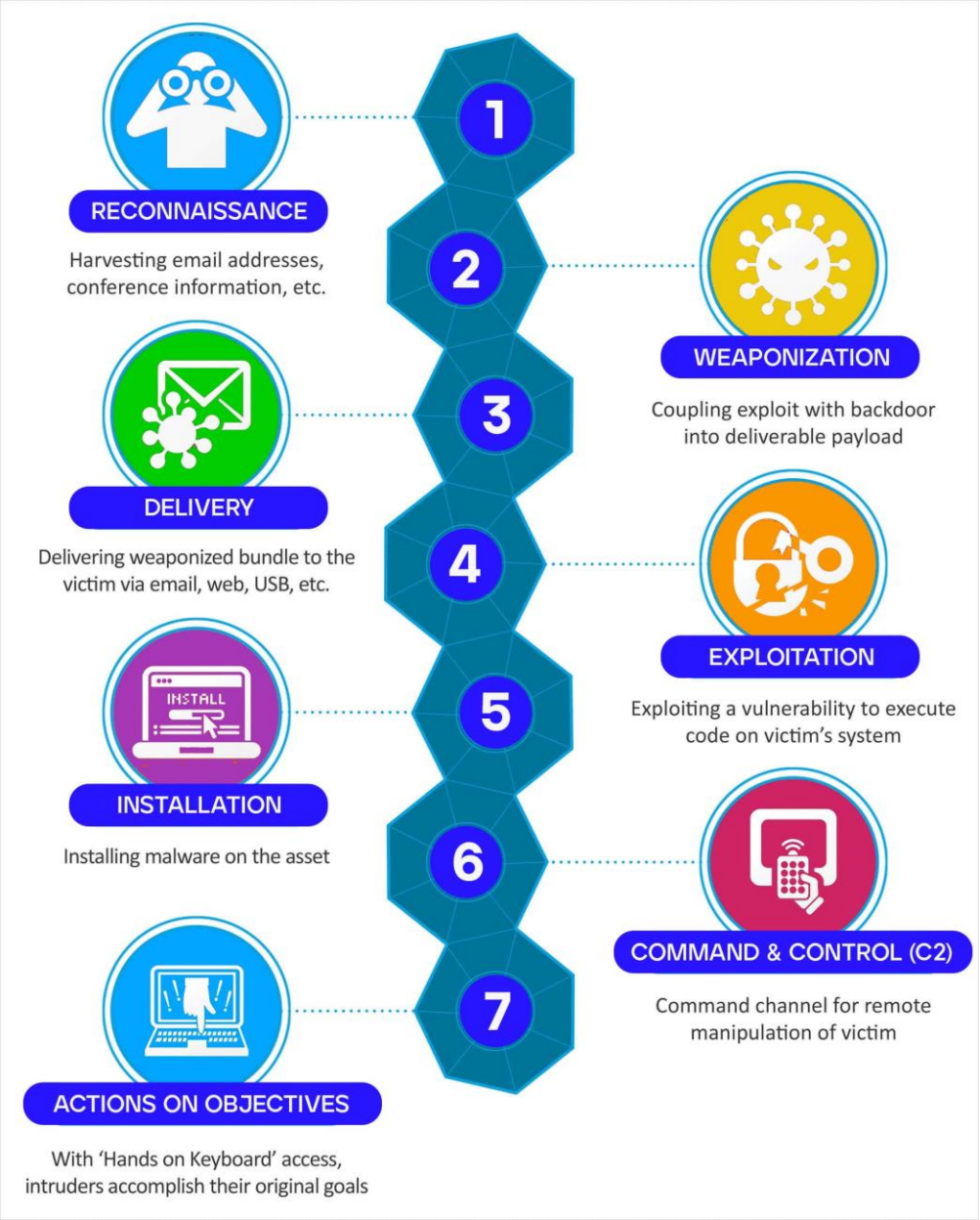
Indicators (1,062) | Attack patterns (0) | Identities (2) | Threat actors (--) | Relationships (0)

New | Add tags | Delete | Columns

Values	Name	Types	Source	Confidence	Alerts	Tags
123.56.220.219	Web App Attack	IPv4 address	AbuseIPDB	--	0	--
137.59.94.130	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot
8.221.141.179	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot
150.107.38.5	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot
104.248.26.60	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot
https://melamorri.co...	Microsoft Identified IOC	URL	Microsoft Defender Threat...	75	0	+3
'SHA-1':A4AAD0E2AC...	Microsoft Identified IOC	File	Microsoft Defender Threat...	75	0	+3
https://gohazeldale.c...	Microsoft Identified IOC	URL	Microsoft Defender Threat...	75	0	+3
190.133.173.74	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot
180.75.19.4	Microsoft Identified IOC	Network traffic	Microsoft Defender Threat...	100	0	honeypot

Review MITRE ATT&CK framework

Have a deep understanding of MITRE framework and TLP, so when creating IOC or viewing them, we can better understand how to respond.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals