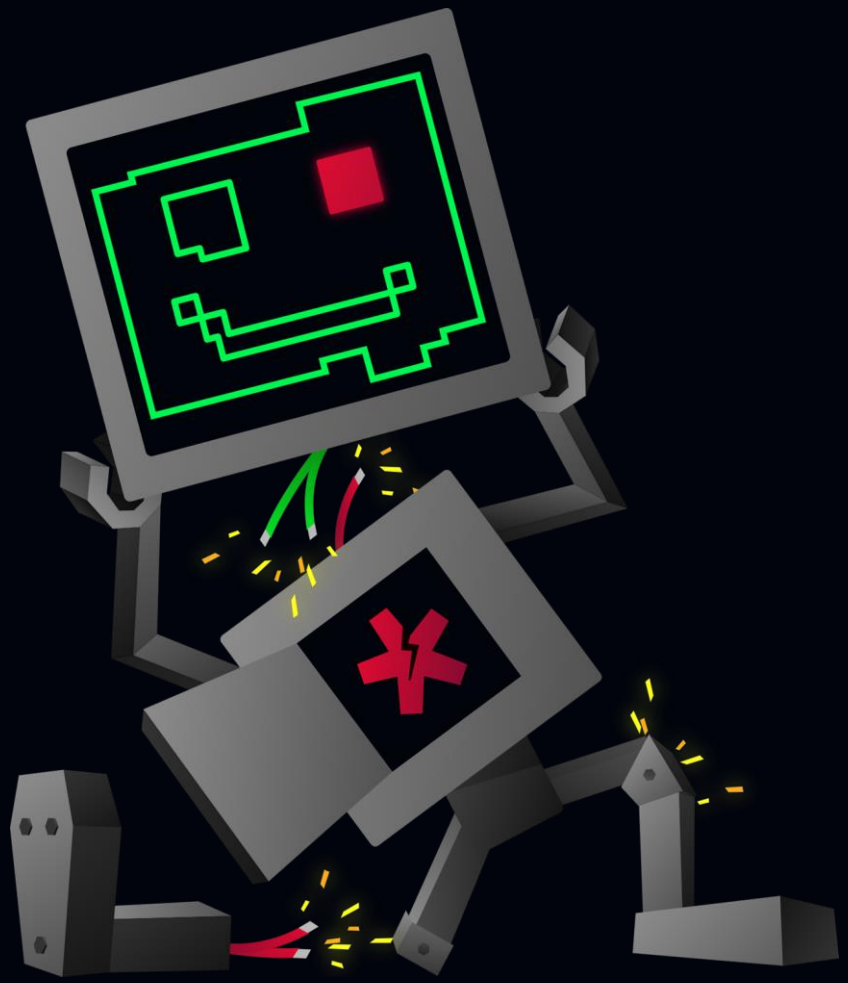
THE H@CK SUMMIT



C:\>

Microsoft Sentinel - nowości i integracja z innymi produktami

Konrad Sagała
Cloud Security Architect, Alior Bank

thehacksummit.com 19-20 października 2023 PGE Narodowy + Online

ORGANIZATORZY:

ACADEMIC PARTNERS

Trochę o sobie

- Cloud Security Architect - Azure
- Microsoft Certified Trainer
- Microsoft MVP since 2007 – M365 Apps & Services
- Twitter - @sagus
- LinkedIn - @konradsagala
- Github - https://github.com/ksagala
- Blog – https://pepugmaster.blogspot.com
- Hobby - Śpiew, Taniec, Podróże

Agenda

- Nowości w Sentinelu w ostatnich miesiącach
- Konektory
- Microsoft Defender Threat Inteligence

Co nowego w Sentinel?

Warto sprawdzać dwa źródła:

Sentinel – What's new?
https://learn.microsoft.com/en-us/azure/sentinel/whats-new

Microsoft Sentinel Blog

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/bg-p/MicrosoftSentinelBlog

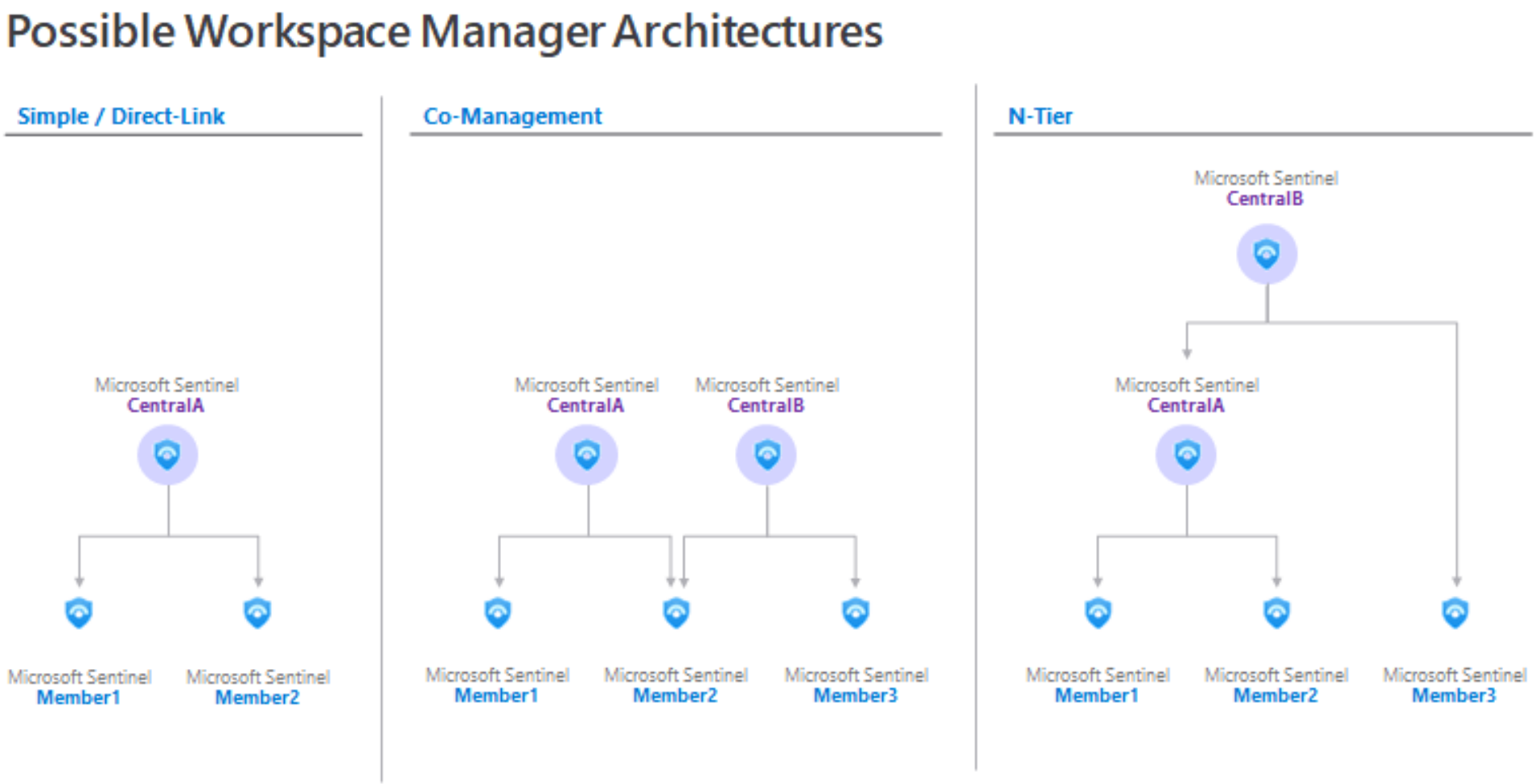
Co nowego w Sentinel?

- Improve SOX compliance with new workbook for SAP
- New incident investigation experience is now GA
- Updated MISP2Sentinel solution utilizes the new upload indicators API.
- New and improved entity pages
- Higher limits for entities in alerts and entity mappings in analytics rules
- Changes to Microsoft Defender for Office 365 connector alerts that apply when disconnecting and reconnecting
- Content Hub generally available and centralization changes released
- Deploy incident response playbooks for SAP
- Microsoft Sentinel solution for Dynamics 365 Finance and Operations (Preview)
- Simplified pricing tiers
- Monitor and optimize the execution of your scheduled analytics rules (Preview)
- Windows Forwarded Events connector is now generally available
- Connect multiple SAP System Identifiers via the UI
- Classic alert automation due for deprecation
- Microsoft Sentinel solution for SAP® applications: new systemconfig.json file
- RSA announcements
- Manage multiple workspaces with workspace manager

Co nowego w Sentinel – Top 5

- Content Hub generally available and centralization changes released
- New incident experience
- New health and auditing monitoring
- Workspace manager (still in preview)
- A lot of new solutions and workbooks

WORKSPACE MANAGER (PREVIEW)



WORKSPACE MANAGER (PREVIEW)

Możemy synchronizować z nadrzędnego workspace:

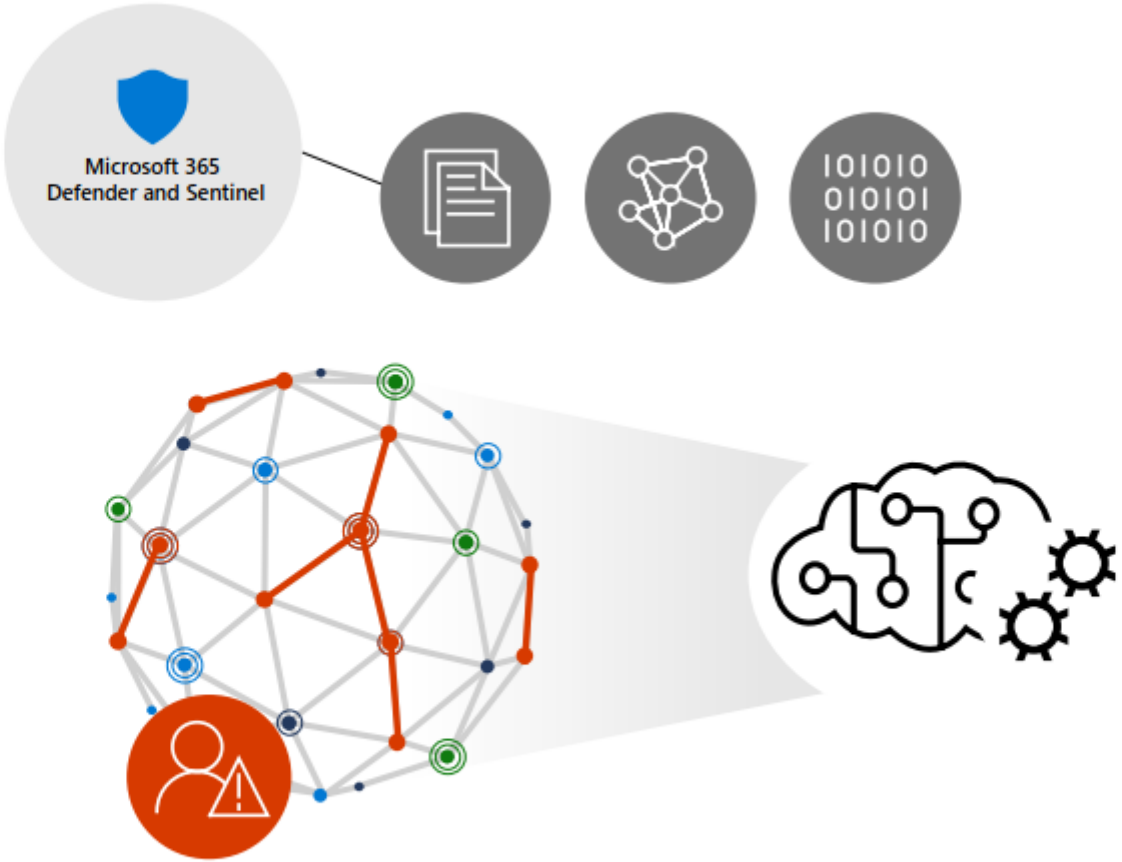
- Analytics rules
- Automation rules (excluding Playbooks)
- Parsers, Saved Searches and Functions
- Hunting and Livestream queries
- Workbooks

Ograniczenia (mogą ulec zmianie):

- Playbooks attributed or attached to analytics and automation rules aren't currently supported.
- Workbooks stored in bring-your-own-storage aren't currently supported.
- Workspace manager only manages content items published from the central workspace. It doesn't manage content created locally from member workspace(s).
- Currently, deleting content residing in member workspace(s) centrally via workspace manager isn't supported.

Microsoft Defender Threat Intelligence

How does it work?



1

Advanced internet reconnaissance

Crawlers and sensors scan the entire internet every day, looking for adversaries and their infrastructure

2

Analysis and automation

Machine learning and powerful AI process billions of requests across millions of webpages

3

Global internet graph

Adversary infrastructure and how it changes is revealed, unmasking attackers and their tools

4

Raw and finished TI

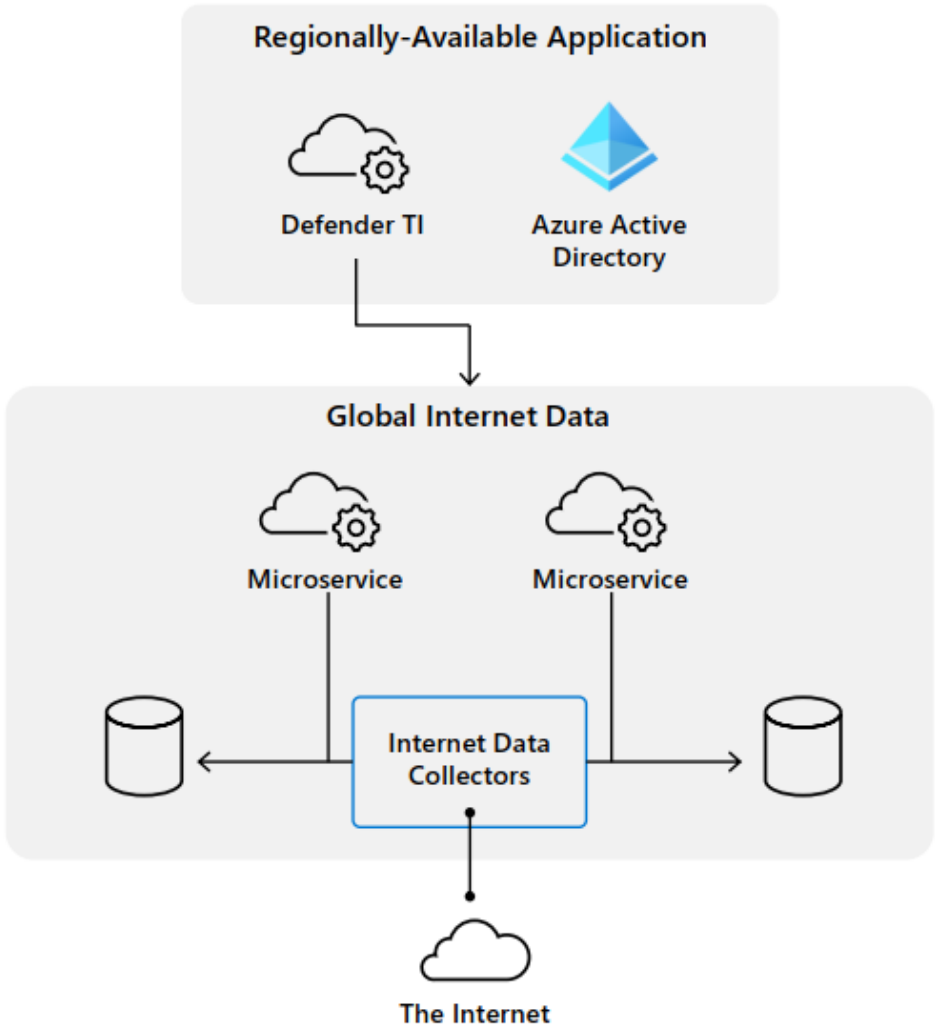
Articles keep you up to date of the evolving landscape and raw threat data can be exported to enhance SIEM+XDR and create incidents

MDTI architecture

MDTI empowers users to hunt through Internet data for attackers' infrastructure

This is powered by data in MDTI's map of the Internet

MDTI spent more than 11 years mapping the structure of the Internet to power this graph



Microsoft Defender Threat Inteligence

Introductory Blogpost:

- https://www.microsoft.com/security/blog/2022/08/02/microsoft-announces-new-solutions-for-threat-intelligence-and-attack-surfacemanagement/

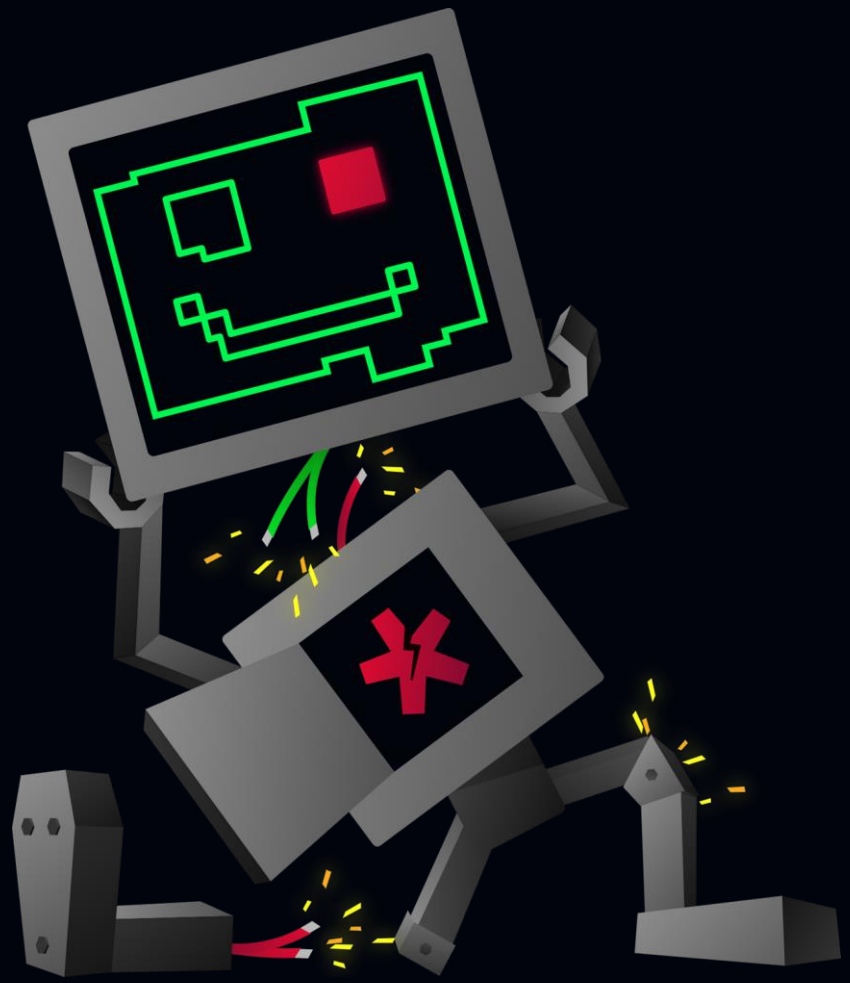
External Resources:

- https://docs.microsoft.com/en-us/defender/threat-intelligence/
- https://techcommunity.microsoft.com/t5/microsoft-defender-threat/bg-p/DefenderThreatIntelligence
- https://azure.microsoft.com/en-us/blog/track-adversaries-and-improve-posture-with-microsoft-threat-intelligence-solutions/

Product Information

- https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence

THE H@CK SUMMIT



Dziękujemy za uwagę!

Zapraszamy do zadawania pytań oraz oceny wystąpienia pod nagraniem.

https://thehacksummit.com/user.html#!/lecture/THS23-2a04/rate

thehacksummit.com | 19-20 października 2023 | PGE Narodowy + Online

ORGANIZATORZY:

ACADEMIC PARTNERS

DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI