TROCHĘ O SOBIE

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

Agenda

- Nowości w Sentinelu w ostatnich miesiącach
- SOC Optimization
- Microsoft Defender Threat Intelligence
- Unified SecOps platform

Co nowego w Sentinel?

Warto sprawdzać trzy 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

What's new in Microsoft's unified secops platform

https://learn.microsoft.com/en-us/unified-secops-platform/whats-new

Co nowego w Sentinel? 10-12.2024

- New SOC optimization recommendation based on similar organizations (Preview)
- Agentless deployment for SAP applications (Limited preview)
- Microsoft Sentinel workbooks available directly in the Microsoft Defender portal
- Unified Microsoft Sentinel solution for Microsoft Business Apps
- New documentation library for Microsoft's unified security operations platform
- New S3-based data connector for Amazon Web Services WAF logs (Preview)
- <mark>Microsoft Sentinel availability in Microsoft Defender portal</mark>
- Updates for the Microsoft Sentinel solution for Microsoft Power Platform

Co nowego w Sentinel? 1-3.2025

- Agentless connection to SAP now in public preview
- Optimize threat intelligence feeds with ingestion rules
- Matching analytics rule now generally available (GA)
- Threat intelligence management interface updated
- Unlock advanced hunting with new STIX objects by opting in to new threat intelligence tables
- Threat intelligence upload API now supports more STIX objects
- Microsoft Defender Threat Intelligence data connectors now generally available (GA)
- Bicep template support for repositories (Preview)
- SOC optimization updates for unified coverage management
- View granular solution content in the Microsoft Sentinel content hub

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

Microsoft 365 Defender and Sentinel
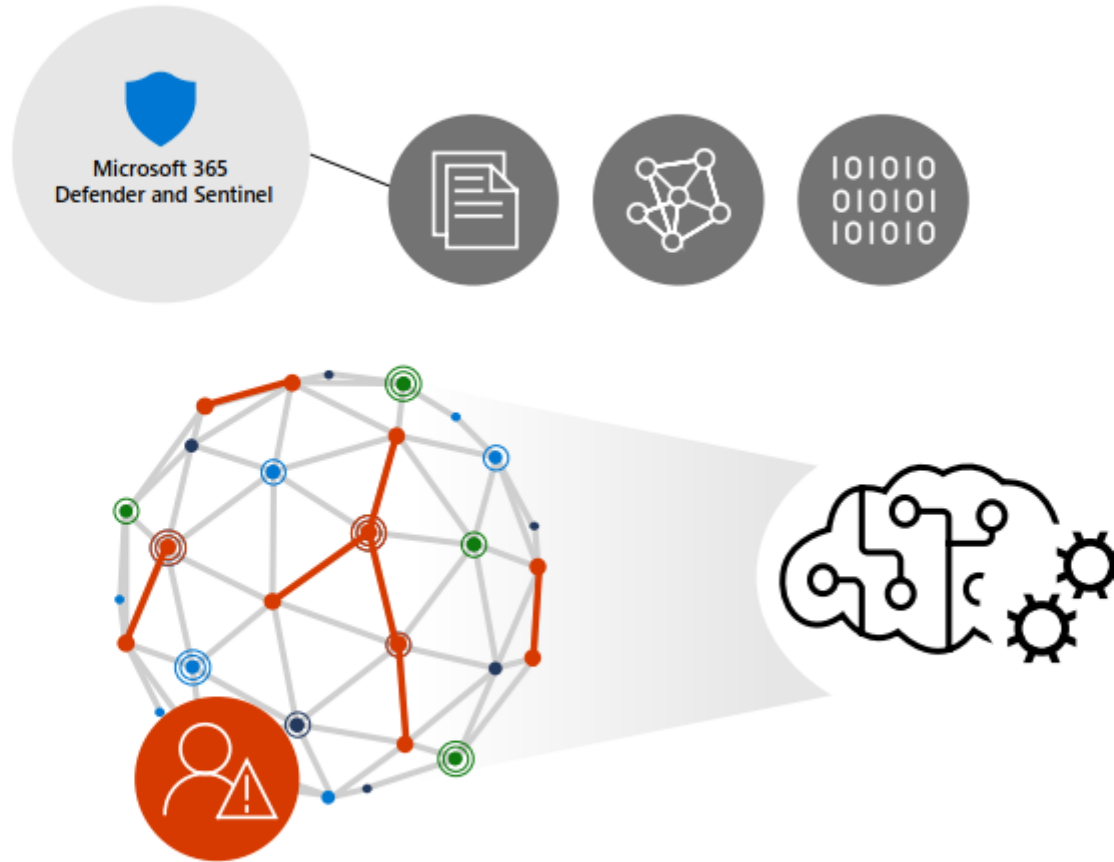
3

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

A unified security operations platform
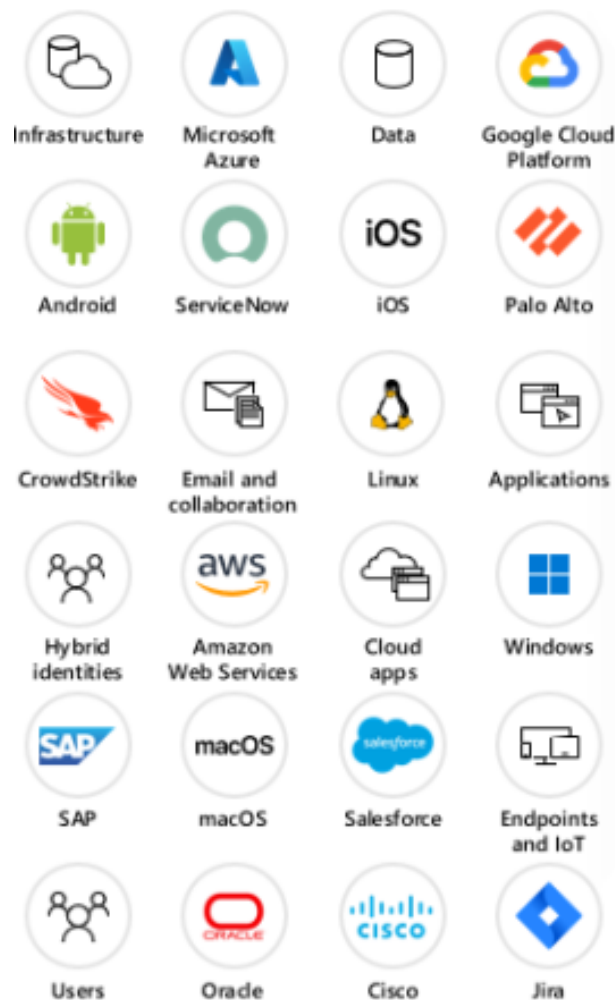## Microsoft Sentinel and Defender XDR together

300+ data sources including:

Infrastructure	Microsoft Azure	Data	Google Cloud Platform
Android	ServiceNow	iOS	Palo Alto
CrowdStrike	Email and collaboration	Linux	Applications
Hybrid identities	Amazon Web Services	Cloud apps	Windows
SAP	macOS	Salesforce	Endpoints and IoT
Users	Oracle	Cisco	Jira

Microsoft Security Copilot

SIEM + XDR

Visibility across your entire organization, plus depth of protection across end users and infrastructure

Microsoft Threat Intelligence

Prevent

Detect

Investigate

Respond

Microsoft Security Experts
Managed services offering

Trochę dodatkowych informacji

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

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/
- https://learn.microsoft.com/en-us/unified-secops-platform/overview-unified-security

Product Information:
- https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence
- https://learn.microsoft.com/en-us/unified-secops-platform/overview-unified-security

Questions?

LIVE

Azure
Summit 2025
All about cloud technologies   ONLINE

27.03.2025

azuresummit.pl

Konrad Sagała

Nowości w Microsoft Sentinel

Britenet   Demant   techevents   kursy FABRIC   TECHNOLOGY INNOVATION DATA KNOWLEDGE tidk