Unified SecOps Operation Center czyli co nowego w bezpieczeństwie chmurowym

Konrad Sagała

Cloud Security Architect

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

- Unified SecOps Operation Center
- Integration with Defender EASM
- Integration with Defender Threat Inteligence
- Integration with Microsoft Sentinel
- What’s new?

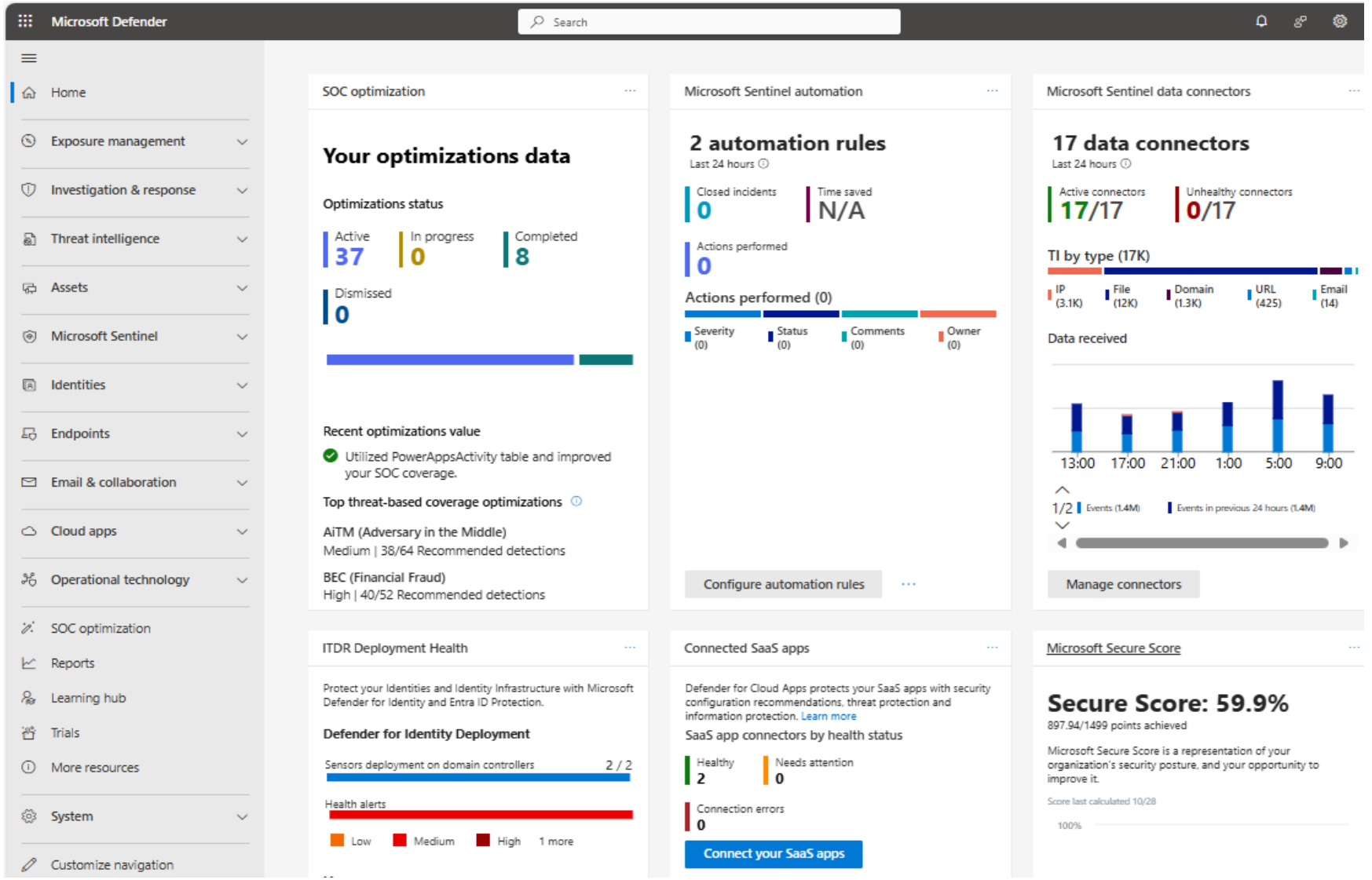
Unified SecOps Operation Center

A unified security operations platform

Microsoft Sentinel and Defender XDR together

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

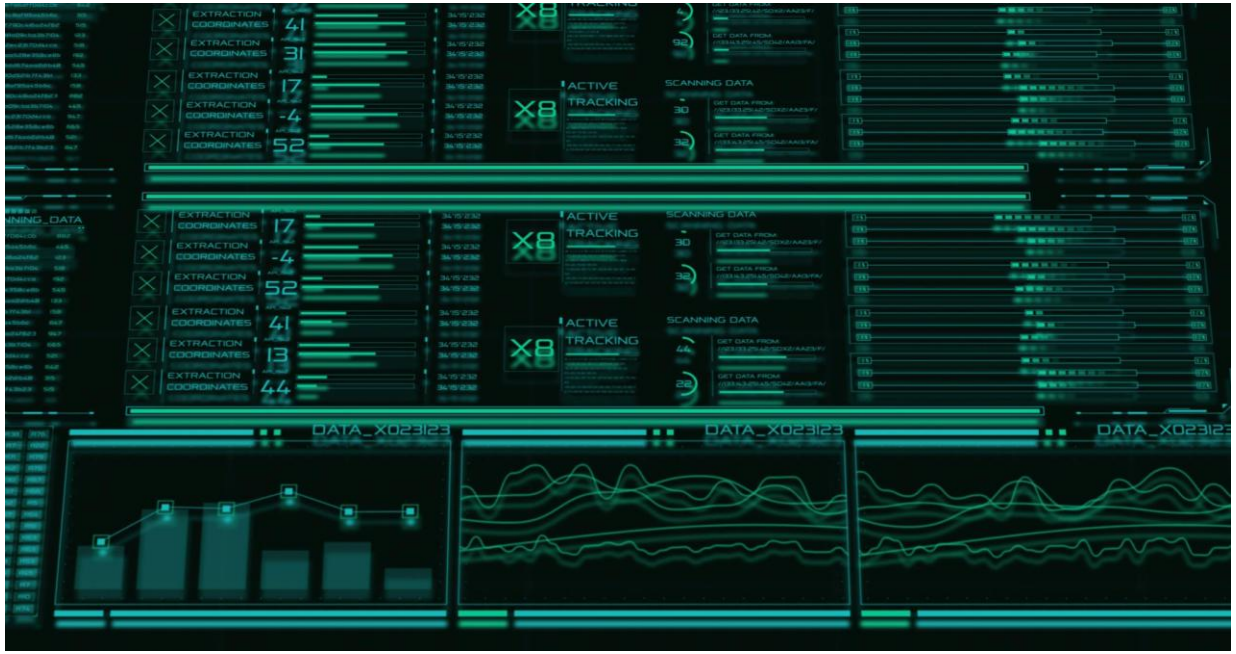
A unified security operations platform



Integration with Defender for Threat Intelligence

Understanding Defender Threat Intelligence

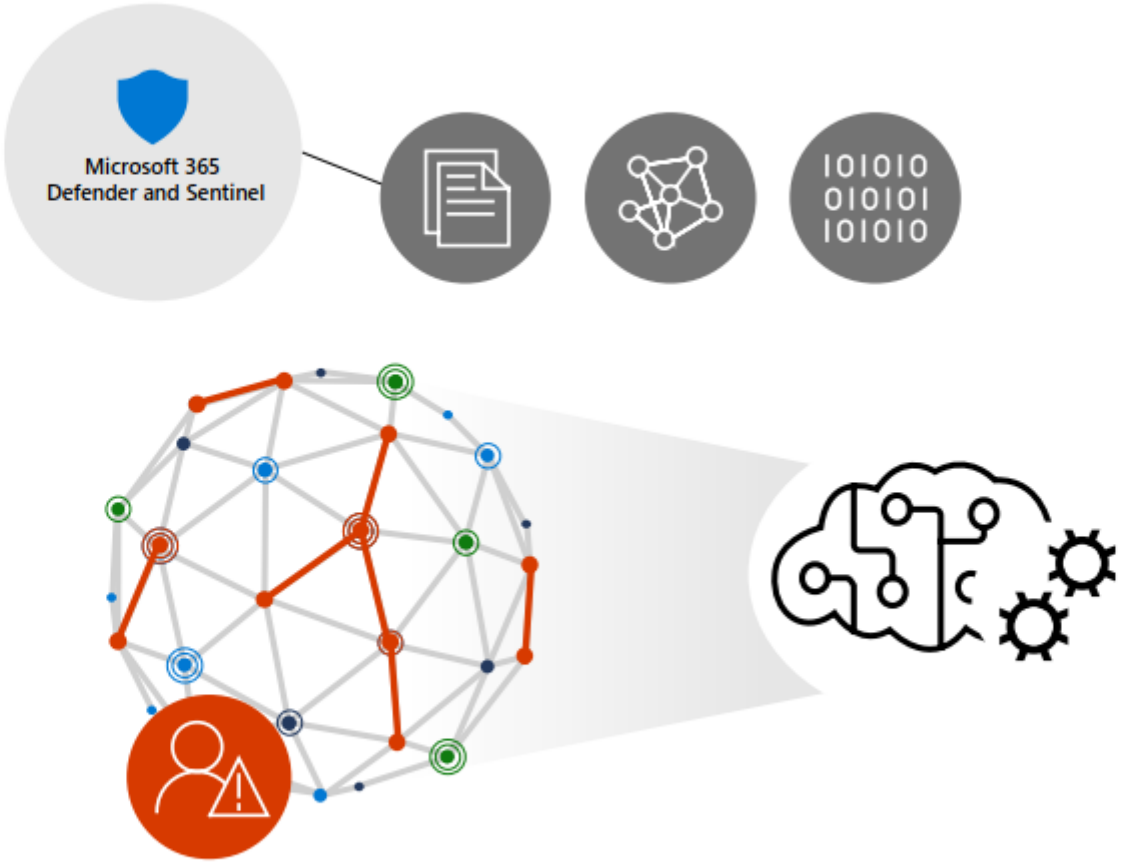
- Included in Microosft offer from 2021
- Defender Threat Intelligence provides real-time threat insights.
- It assists in identifying and prioritizing vulnerabilities.
- The integration enhances incident response capabilities.
- It leverages global threat data for proactive defense strategies.



[Microsoft acquired RiskIQ to strengthen cybersecurity of digital transformation and hybrid work | Microsoft Security Blog]

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

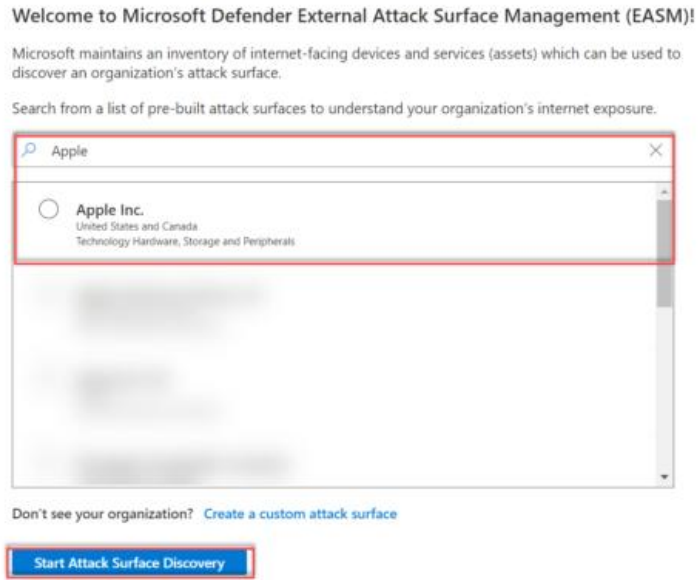
4

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

Integration with Defender EASM

Overview of External Attack Surface Management (EASM)



Understanding EASM
EASM helps organizations identify their external vulnerabilities and understand potential attack vectors, enhancing their security posture.

Proactive Security Measures
By using EASM, organizations can implement proactive security measures to mitigate risks before they are exploited by attackers.

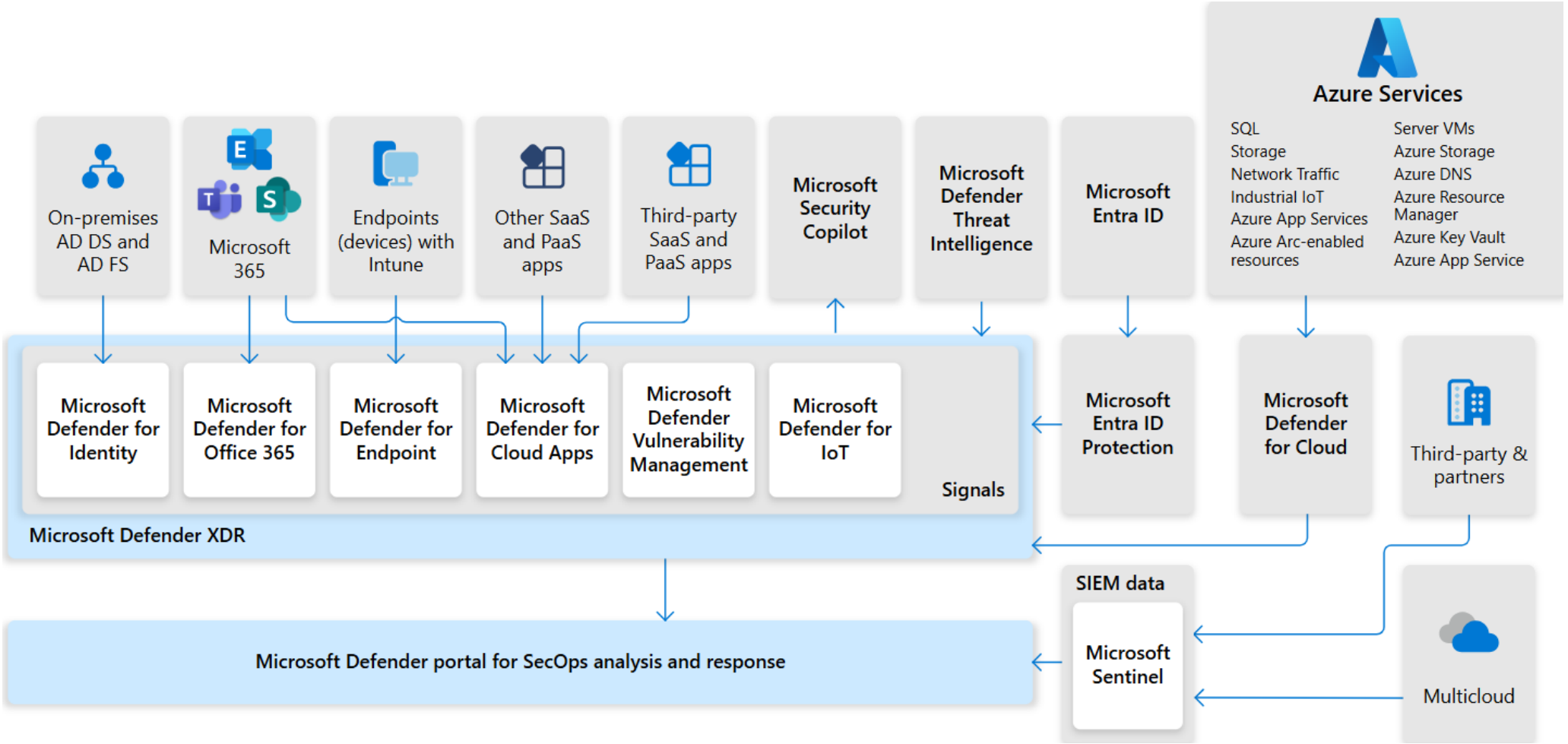
Risk Management Insights
EASM provides critical insights for organizations to manage risks effectively and strengthen their overall security framework.

---

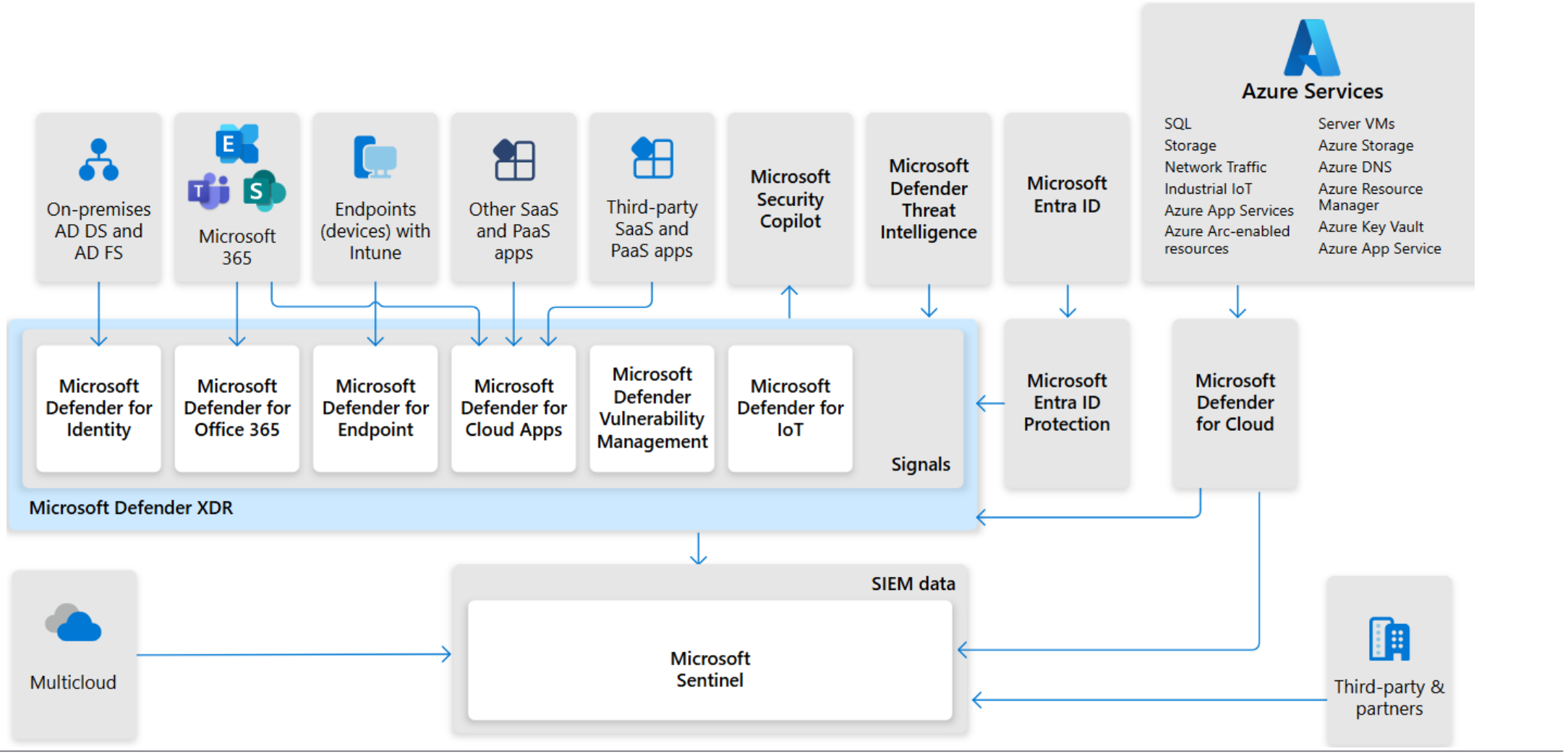
https://learn.microsoft.com/en-us/security-exposure-management/microsoft-security-exposure-management

Integration with Microsoft Sentinel

Seamless Integration with Defender XDR



Seamless Integration with Defender XDR from Azure



What’s new?

Potential Improvements in Defender XDR

Enhanced Adaptability

Defender XDR will evolve to better adapt to emerging threats, ensuring comprehensive protection against new vulnerabilities.

Third-Party Integration

Better integration with third-party security solutions will enhance functionality and provide a more comprehensive security posture.

Continuous Algorithm Updates

Continuous updates to detection algorithms will improve threat detection capabilities, keeping up with the evolving threat landscape.

Co nowego w Unified SecOps i 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

What's new in Defender for Cloud

https://learn.microsoft.com/en-us/azure/defender-for-cloud/release-notes

Questions and Answers

Dziekuję za uwagę