



CSP Masters Program in person series

Technical training

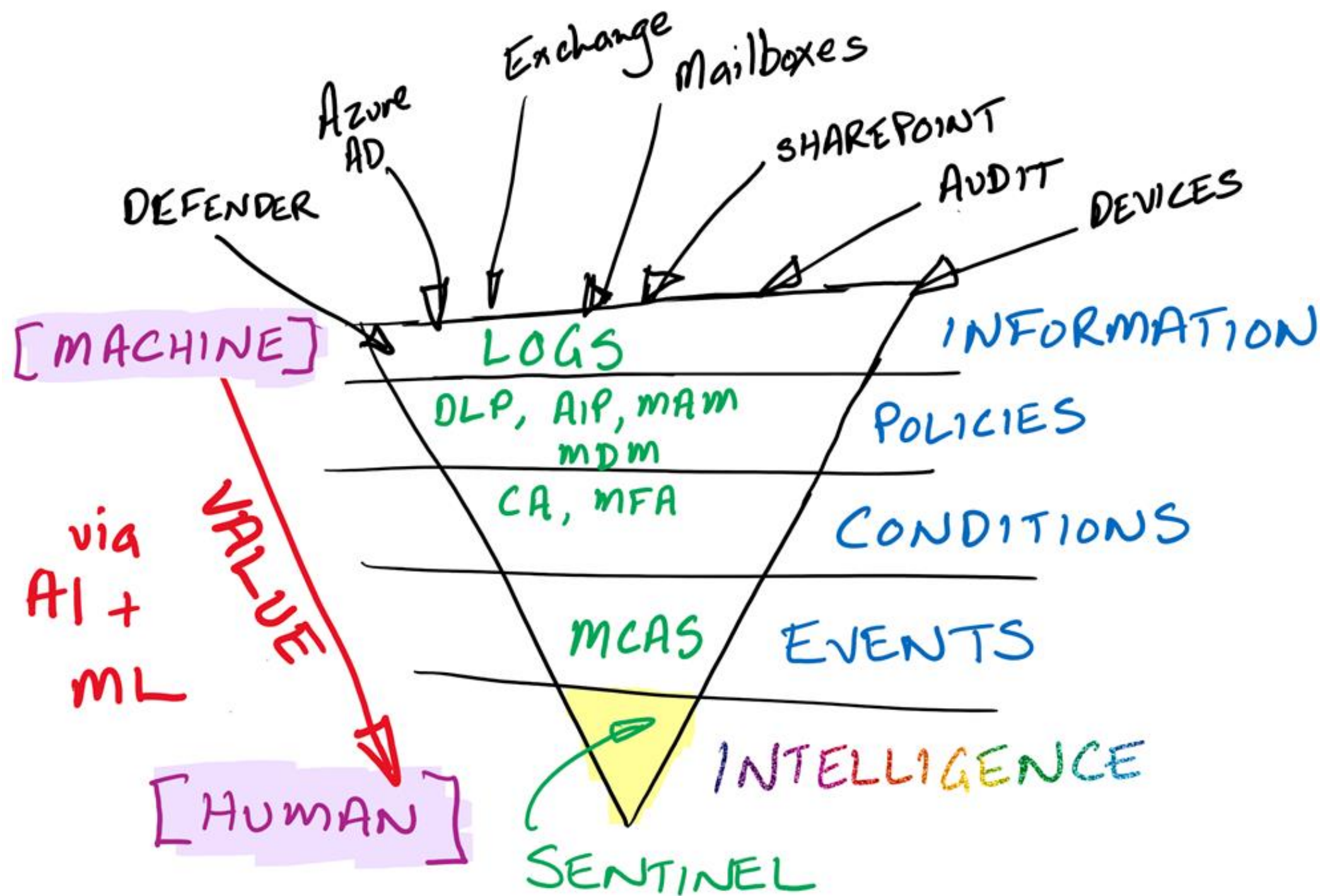


Sentinel

Acronyms

- SIEM – Security Information and Event Management
- SOAR – Security, Orchestration, Automation and Response

Intelligence vs Information



Introducing Microsoft Sentinel

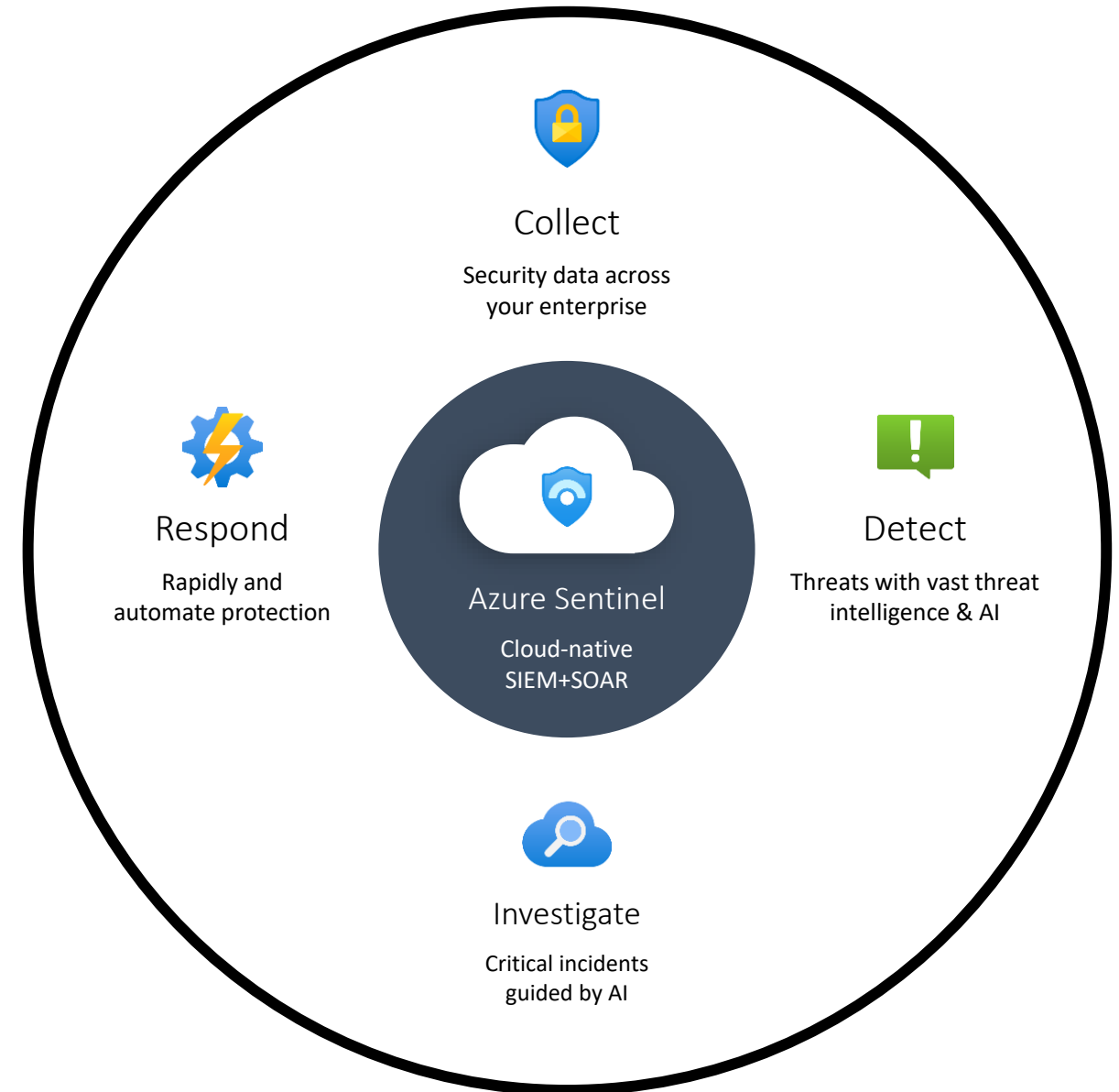
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your Office 365 + M365 Alerts for Free

Easy integration with your existing tools

Faster threat protection with AI by your side



General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks (Preview)

Entity behavior

Threat intelligence (Preview)

Configuration

Data connectors

Analytics

Watchlist (Preview)

Playbooks

Community

Settings

12.4K 94
Events

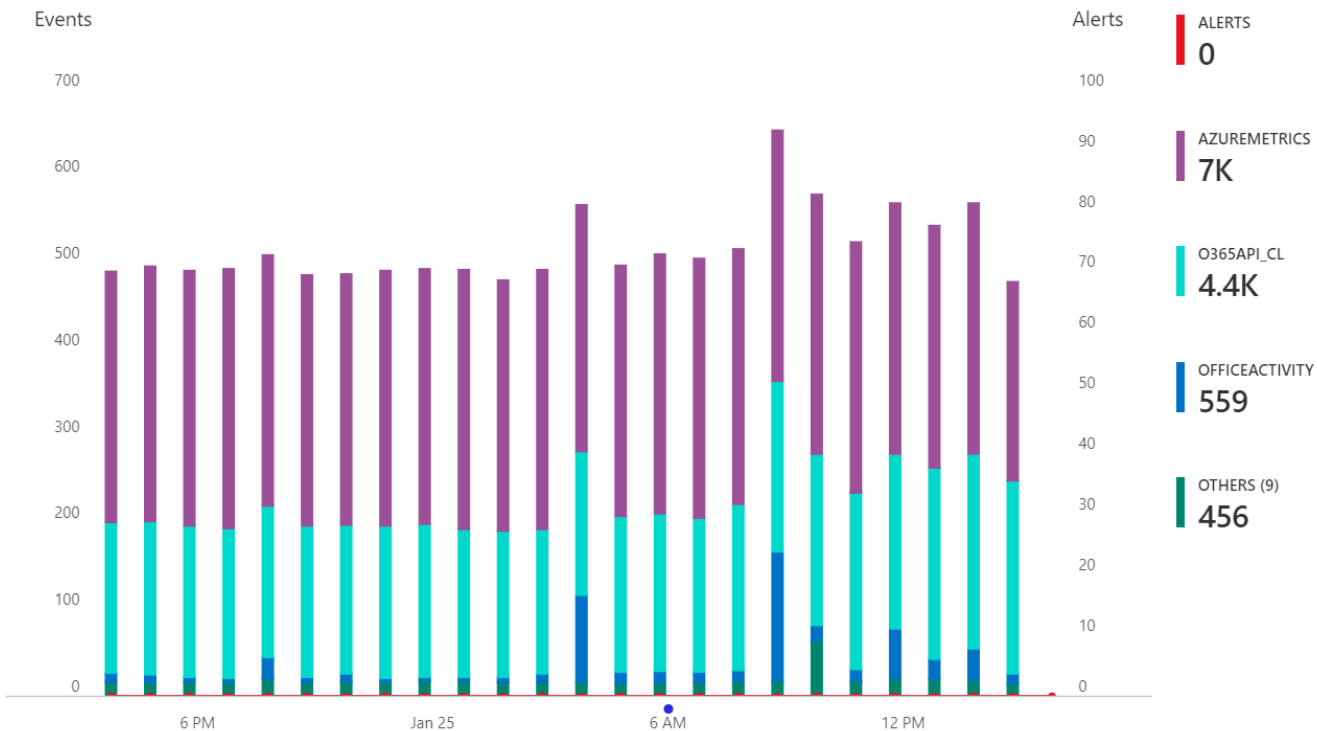
0
Alerts

1 5
Incidents

Incidents by status

New (1) Active (0) Closed (True Positive) (0) Closed (False Positive) (0)

Events and alerts over time



Potential malicious events



POTENTIAL
MALICIOUS
EVENTS
0

OUTBOUND
0 ▲

INBOUND AND
UNKNOWN
0 ▼

Recent incidents

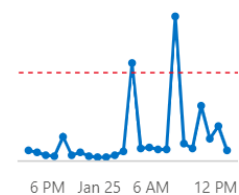
Medium

Failed logins from external

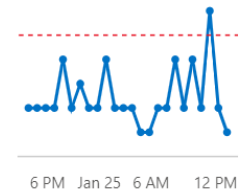
1 AI

Data source anomalies

OfficeActivity



Usage

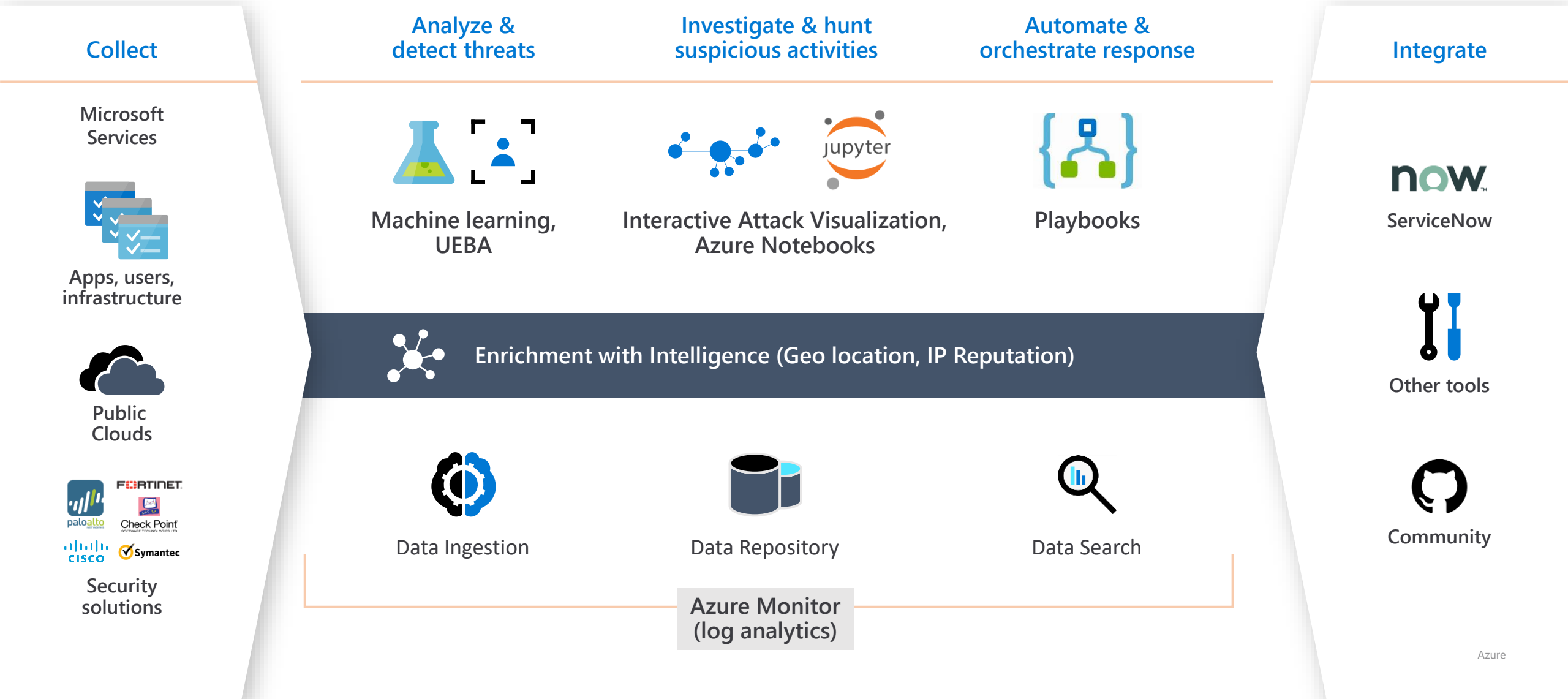


Democratize ML for your SecOps



Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

Core capabilities



What is Microsoft Sentinel?

No infrastructure costs, Only *pay for what you use*

Predictable Billing with capacity reservations

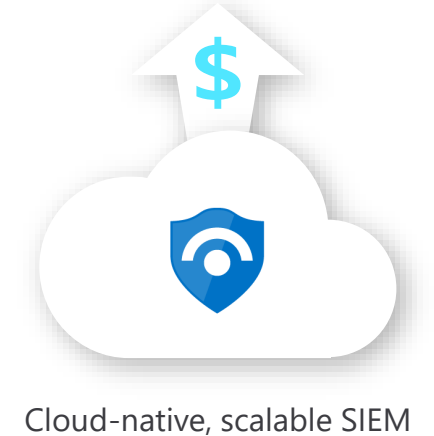
Flexible model, no annual commitments

Free ingestion for O365 Audit Logs, Azure Activity Logs and M365 Security Alerts

Traditional



Sentinel



And how it plays into the larger story...

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

Proven log platform with more than
10 petabytes of daily ingestion



Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Playbooks
- Community
- Settings

Search

Severity : All

Rule Type : All

Status : All

Tactics : All

SEVERITY ↑↓ NAME ↑↓ RULE TYPE ↑↓ STATUS ↑↓ TACTICS

<input type="checkbox"/>	High	Known Strontium group domains	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	High	Known IRIDIUM IP	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	High	Known Phosphorus group domains/IP	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	High	Create incidents based on Azure Security Center al...	Microsoft Secur...	Enabled	
<input type="checkbox"/>	High	Create incidents based on Azure Active Directory I...	Microsoft Secur...	Enabled	
<input type="checkbox"/>	High	Advanced Multistage Attack Detection	Fusion	Enabled	Command and Control
<input type="checkbox"/>	High	Create incidents based on Azure Advanced Threat ...	Microsoft Secur...	Enabled	
<input type="checkbox"/>	High	Create incidents based on Microsoft Defender Adv...	Microsoft Secur...	Enabled	
<input type="checkbox"/>	High	Create incidents based on Microsoft Cloud App Se...	Microsoft Secur...	Enabled	
<input type="checkbox"/>	High	Known Manganese IP and UserAgent activity	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	High	Create incidents based on Office 365 Advanced Th...	Microsoft Secur...	Enabled	
<input type="checkbox"/>	High	Suspicious application consent similar to O365 Att...	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	High	First access credential added to Application or Ser...	Scheduled	Enabled	Credential Dumping
<input type="checkbox"/>	Medium	Failed AzureAD logons but success logon to host	Scheduled	Enabled	Credential Dumping
<input type="checkbox"/>	Medium	Malware in the recycle bin	Scheduled	Enabled	Defense Evasion
<input type="checkbox"/>	Medium	CIAOPS - URL detonation	Scheduled	Enabled	
<input type="checkbox"/>	Medium	Suspicious number of resource creation or deploy...	Scheduled	Enabled	Impact
<input type="checkbox"/>	Medium	SSH Potential Brute Force	Scheduled	Enabled	Credential Dumping
<input type="checkbox"/>	Medium	Rare high NXDomain count	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	Medium	SharePointFileOperation via devices with previous...	Scheduled	Enabled	Exfiltration
<input type="checkbox"/>	Medium	Process executed from binary hidden in Base64 en...	Scheduled	Enabled	Defense Evasion
<input type="checkbox"/>	Medium	Brute force attack against Azure Portal	Scheduled	Enabled	Credential Dumping
<input type="checkbox"/>	Medium	SSH newly internet-exposed endpoints	Scheduled	Enabled	Initial Access
<input type="checkbox"/>	Medium	Multiple users email forwarded to same destination	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	Medium	User account created and deleted within 10 mins	Scheduled	Enabled	Command and Control
<input type="checkbox"/>	Medium	Similar forward IP that the destination is not a black...	Scheduled	Enabled	Command and Control

High
Severity

Enabled
Status

Id

d0fe6fe9-d84d-4186-aab1-f05ca5c32994

Description

Matches domain name IOCs related to Phosphorus group activity with CommonSecurityLog, DnsEvents, OfficeActivity and VMConnection dataTypes. References: <https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/>.

Tactics

Command and Control

Rule query

```
let timeframe = 1d;  
let DomainNames = dynamic(["yahoo-verification.org",  
"accounts-web-mail.com", "customer-certificate.com", "  
"yahoo-verification.net", "yahoo-verify.net", "outlook  
"com-identifier-servicelog.name", "microsoft-update.b  
"confirm-session-identifier.info", "session-managemen
```

Rule frequency

Run query every **1 day**

Rule period

Last **1 day** data

Rule threshold

Trigger alert if query returns **more than 0** results

Event grouping

Group all events into a single alert

Suppression

Not configured

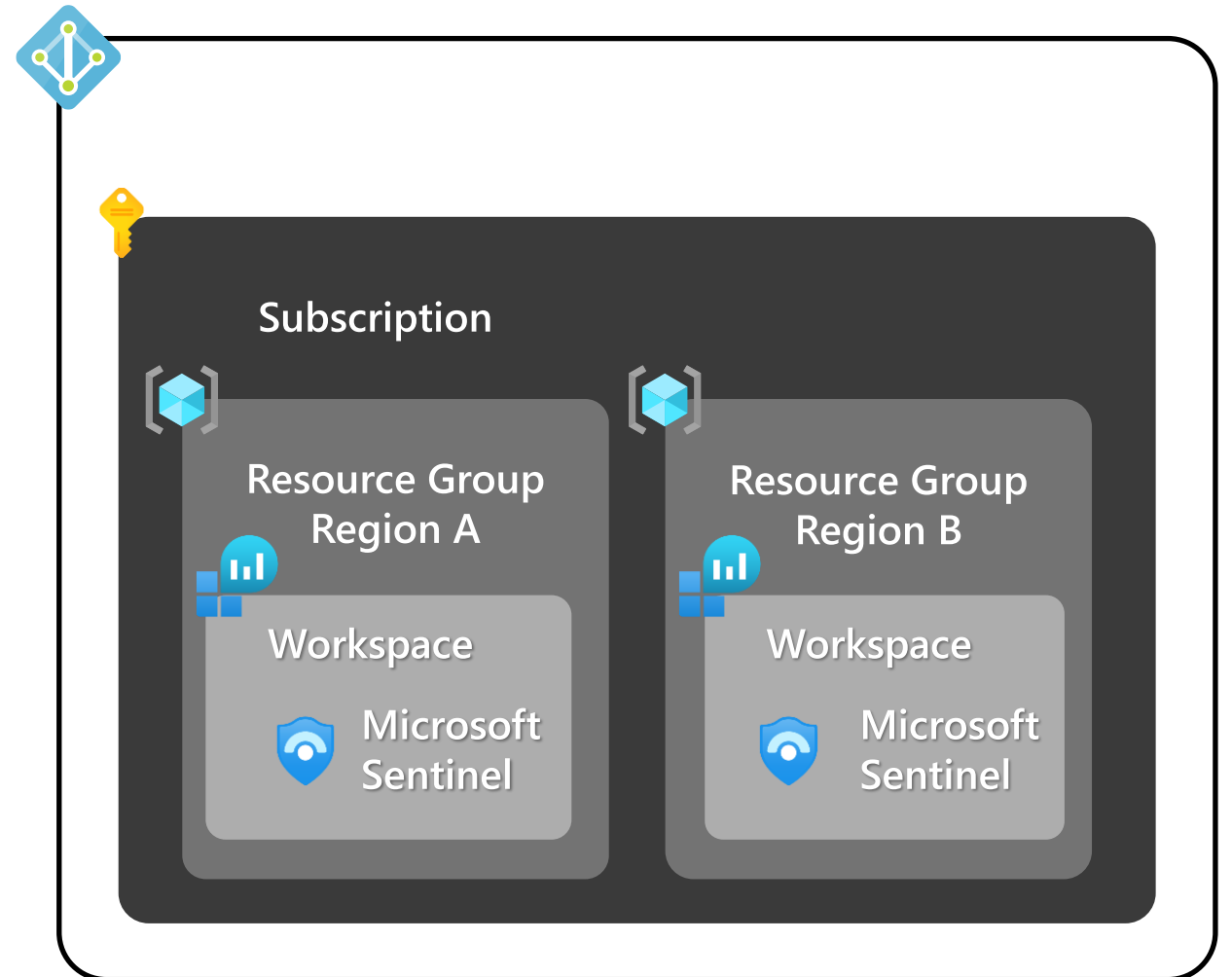
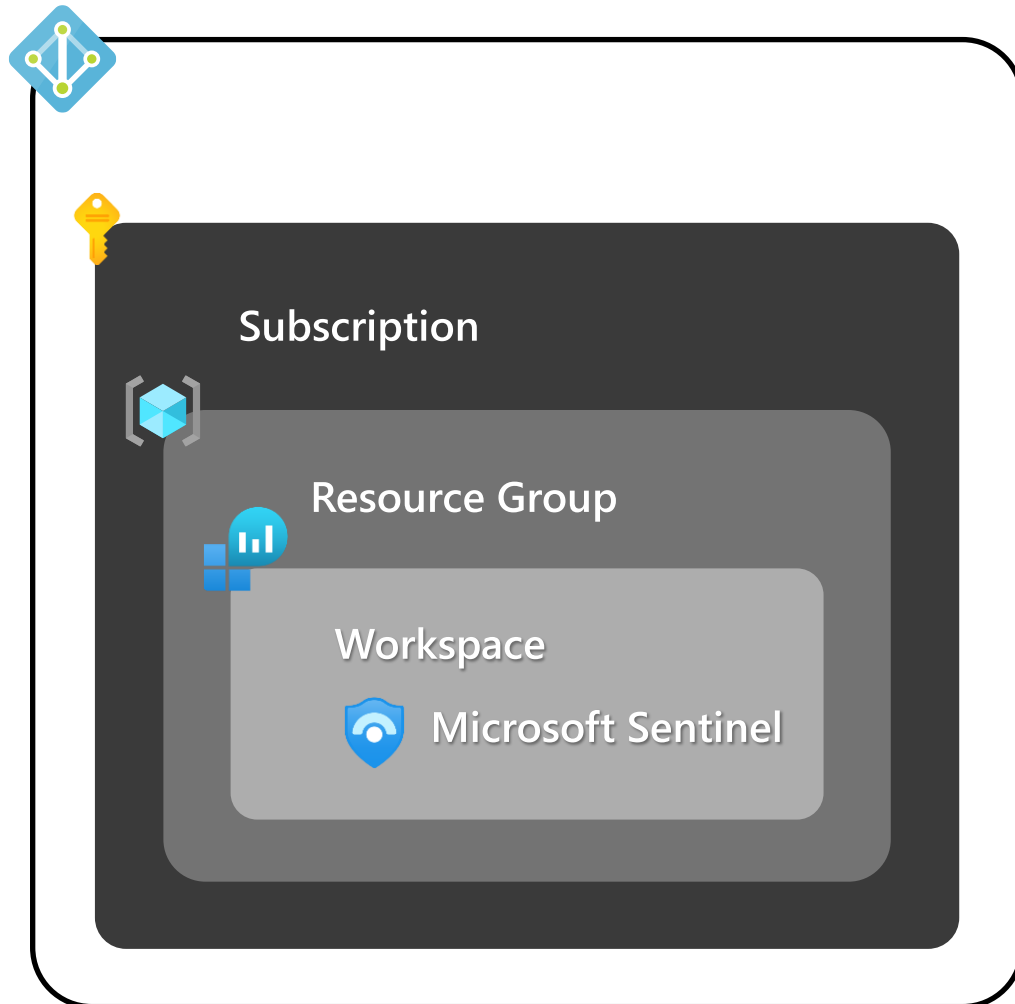
Create incidents from this rule

Enabled

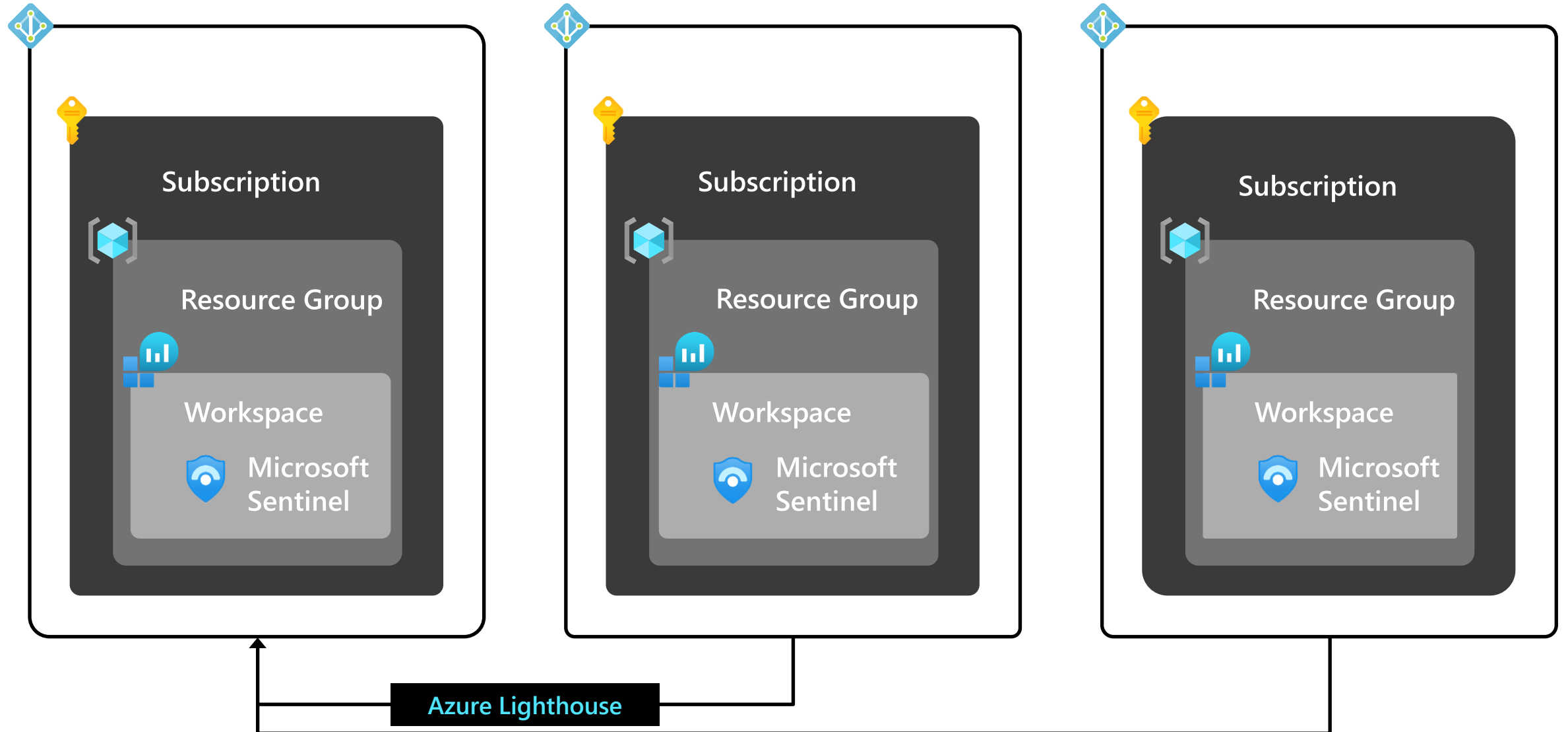
Alert grouping

Disabled

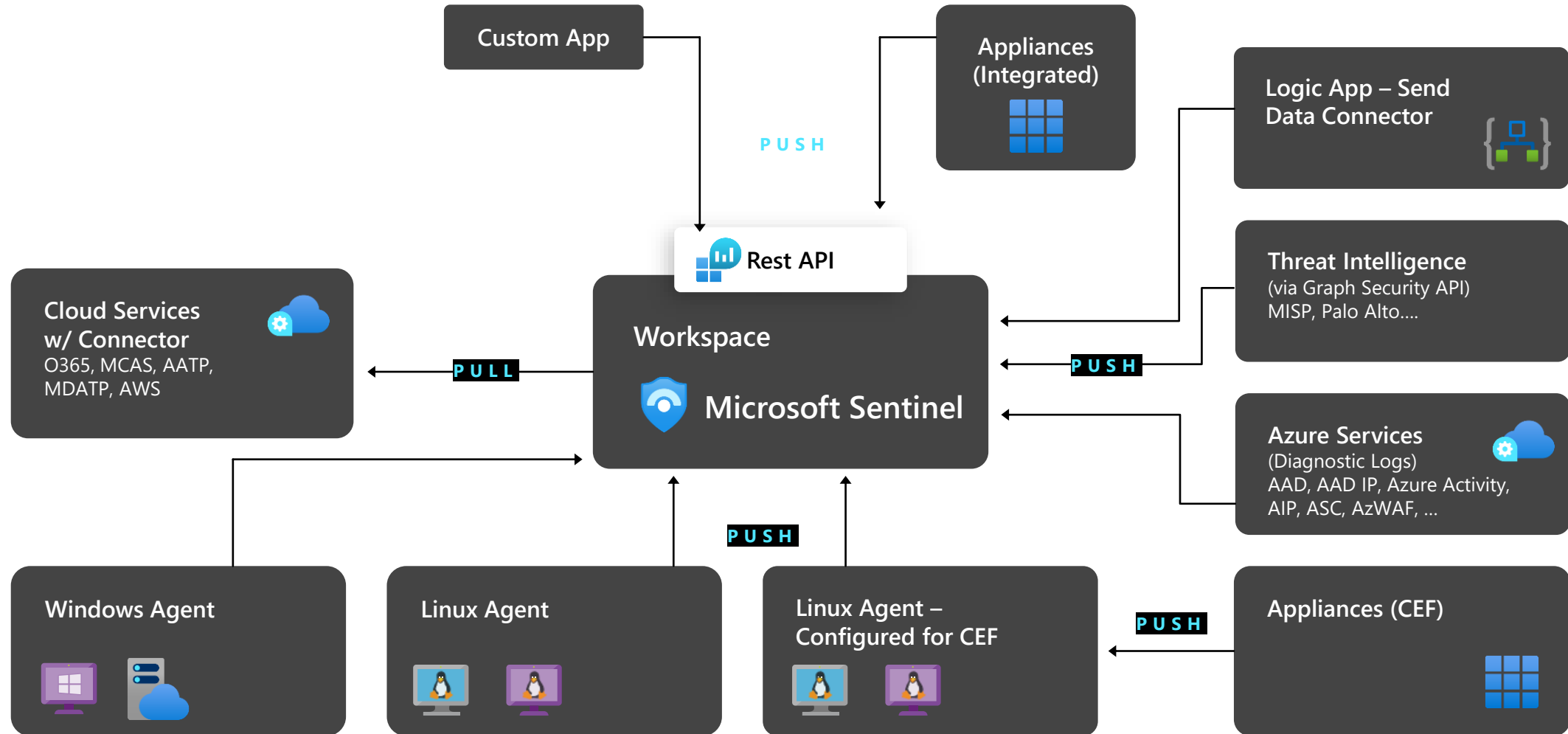
Workspace Design (Single Tenant)



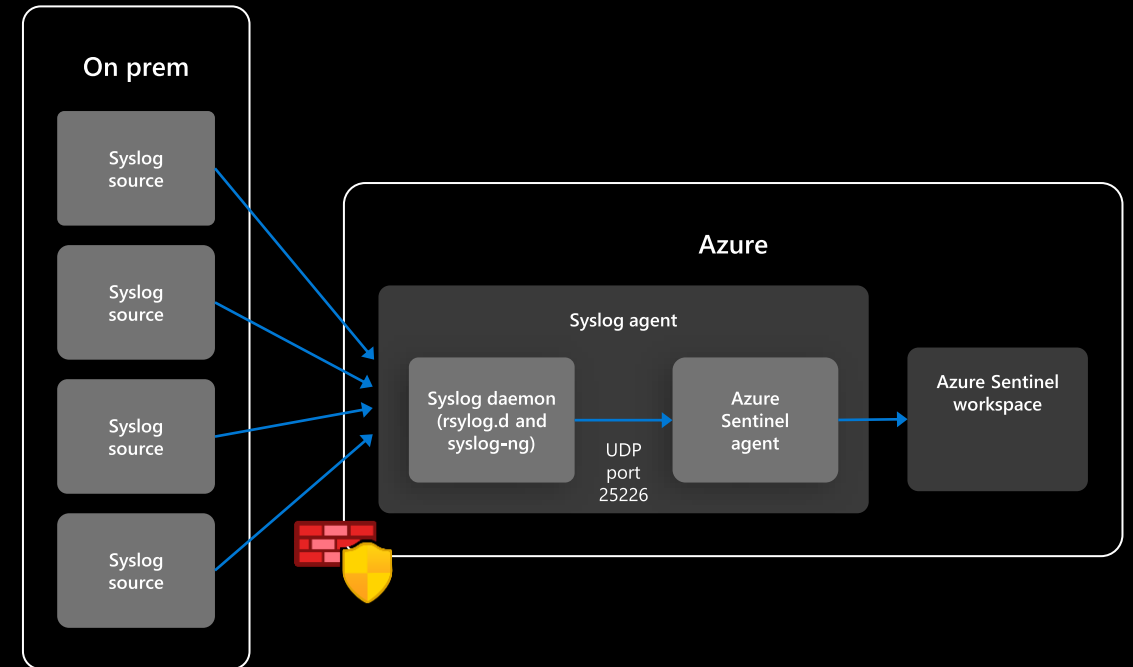
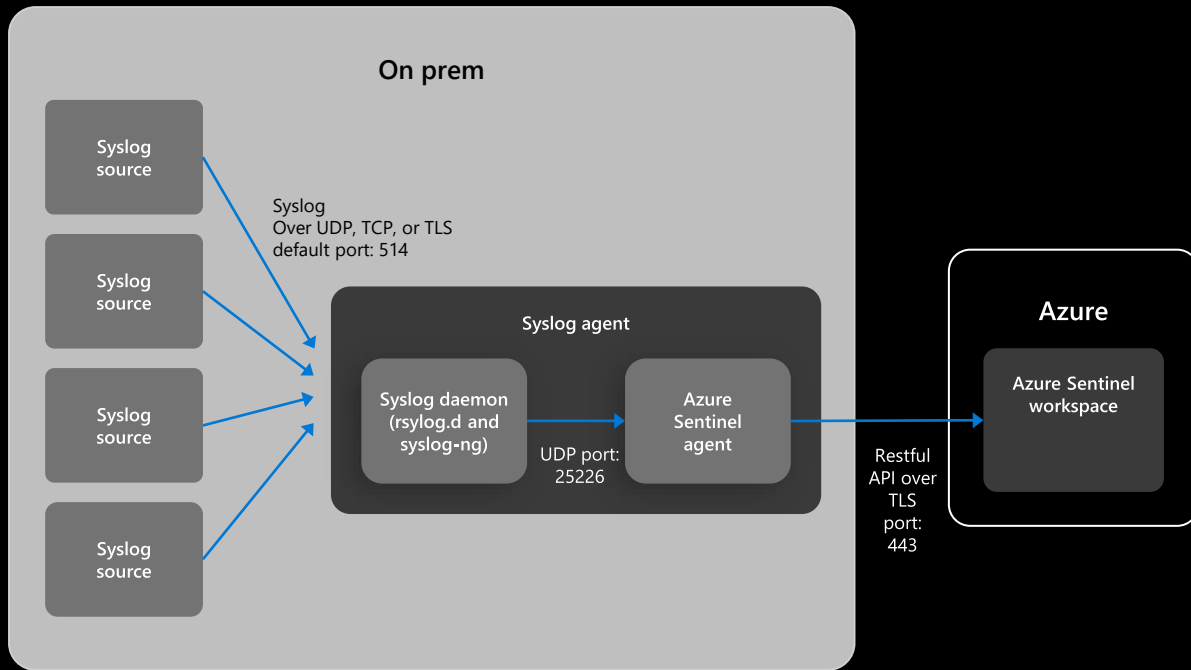
Workspace Design (Multi-Tenant)



All the ways data gets in



CEF architecture



Data Collectors (Quick Wins)

BEST PRACTICE

Enable 1st Party Connectors that are running in the environment

Most are free

- O365
- Azure Activity
- 1st Party Alerts – MCAS, AATP, MDATP, AAD IP

Connect AWS

Connect / Configure Azure Diagnostic Logs (Policy)

Deploy Windows/Linux Agent in Azure (built-in Policy)

What data can be ingested at no cost with Microsoft Sentinel?



Azure Activity Logs, Office 365 Audit Logs (all SharePoint activity and Exchange admin activity) and alerts from Microsoft Defender products (Azure Defender, Microsoft 365 Defender, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint), Azure Security Center and Microsoft Cloud App Security can be ingested at no additional cost into both Microsoft Sentinel and Azure Monitor Log Analytics.

Please Note: Azure Active Directory (AAD) audit data is not free and is billed for ingestion into both Microsoft Sentinel and Azure Monitor Log Analytics.

Data Collectors (Next Steps)

Deploy Windows/Linux Agent on-prem /
other clouds

Deploy CEF Collection

- Configure CEF collector using configuration script
- Configure source devices – ensure they support RFC and CEF.
- See the “Grand List”
<https://techcommunity.microsoft.com/t5/Azure-Sentinel/Azure-Sentinel-The-Syslog-and-CEF-source-configuration-grand/ba-p/803891>

Integrate Threat Intelligence

BEST PRACTICE

DEMO

Resources

- Sentinel Quickstart - <https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard>
- Connect data sources - <https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>
- Tutorial: Investigate incidents – <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases>
- Become an Azure Sentinel Ninja – <https://techcommunity.microsoft.com/t5/azure-sentinel/become-an-azure-sentinel-ninja-the-complete-level-400-training/ba-p/1246310>
- Azure Sentinel on Microsoft Learn - <https://techcommunity.microsoft.com/t5/itops-talk-blog/learn-azure-sentinel-on-microsoft-learn/ba-p/2006346>
- Visualise your data - <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data>
- Azure Sentinel Workbooks 101 - <https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-workbooks-101-with-sample-workbook/ba-p/1409216>