Introduction to Microsoft Sentinel

June 2022

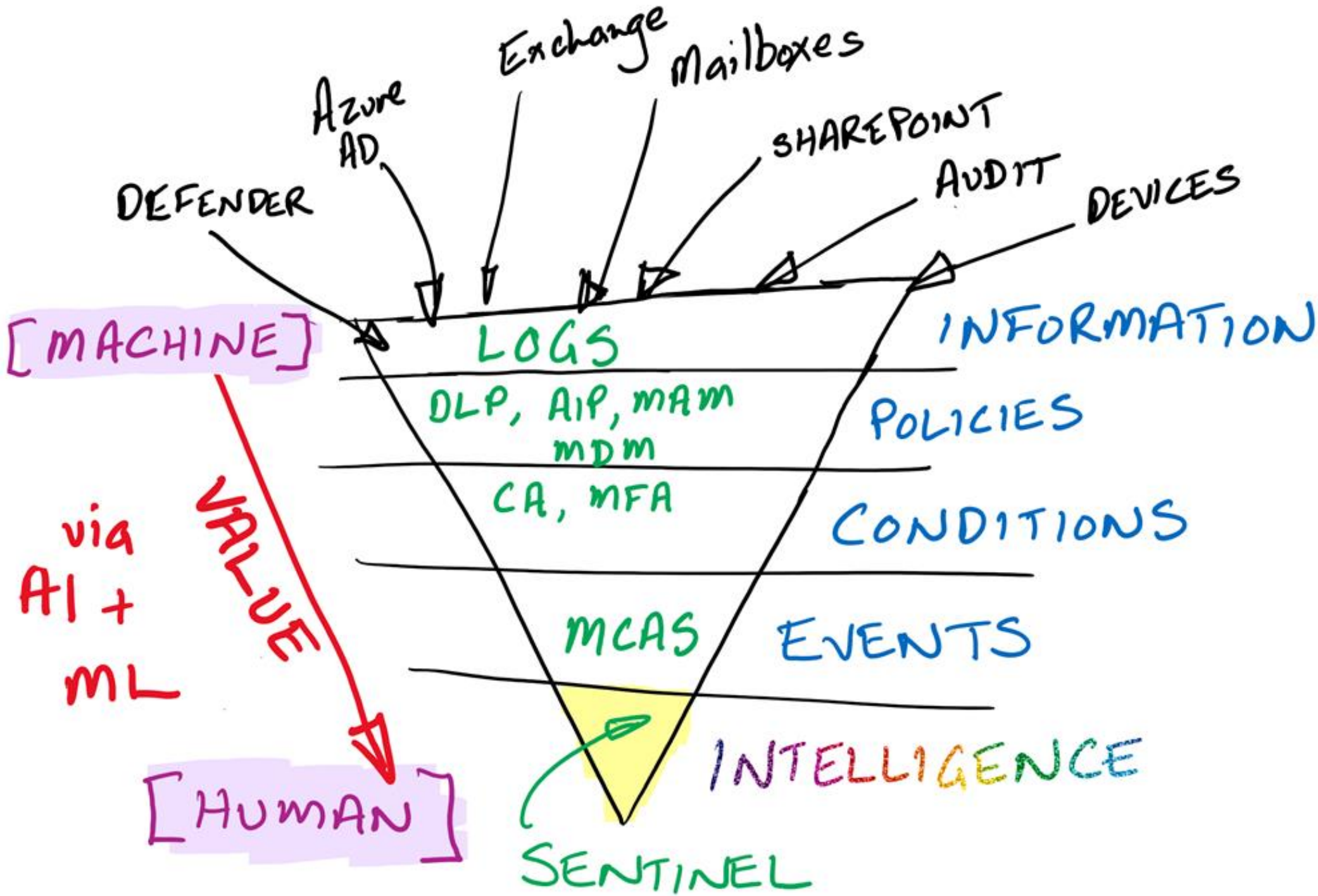
@directorcia

http://about.me/ciaops

Acronyms

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

Intelligence vs Information


Exchange
Mailboxes
Azure AD
SHAREPOINT
AUDIT
DEVICES
DEFENDER
[MACHINE]
LOGS
INFORMATION
DLP, AIP, MAM
MDM
POLICIES
CA, MFA
CONDITIONS
via AI + ML
VALUE
MCAS
EVENTS
[HUMAN]
INTELLIGENCE
SENTINEL

Introducing Microsoft Sentinel

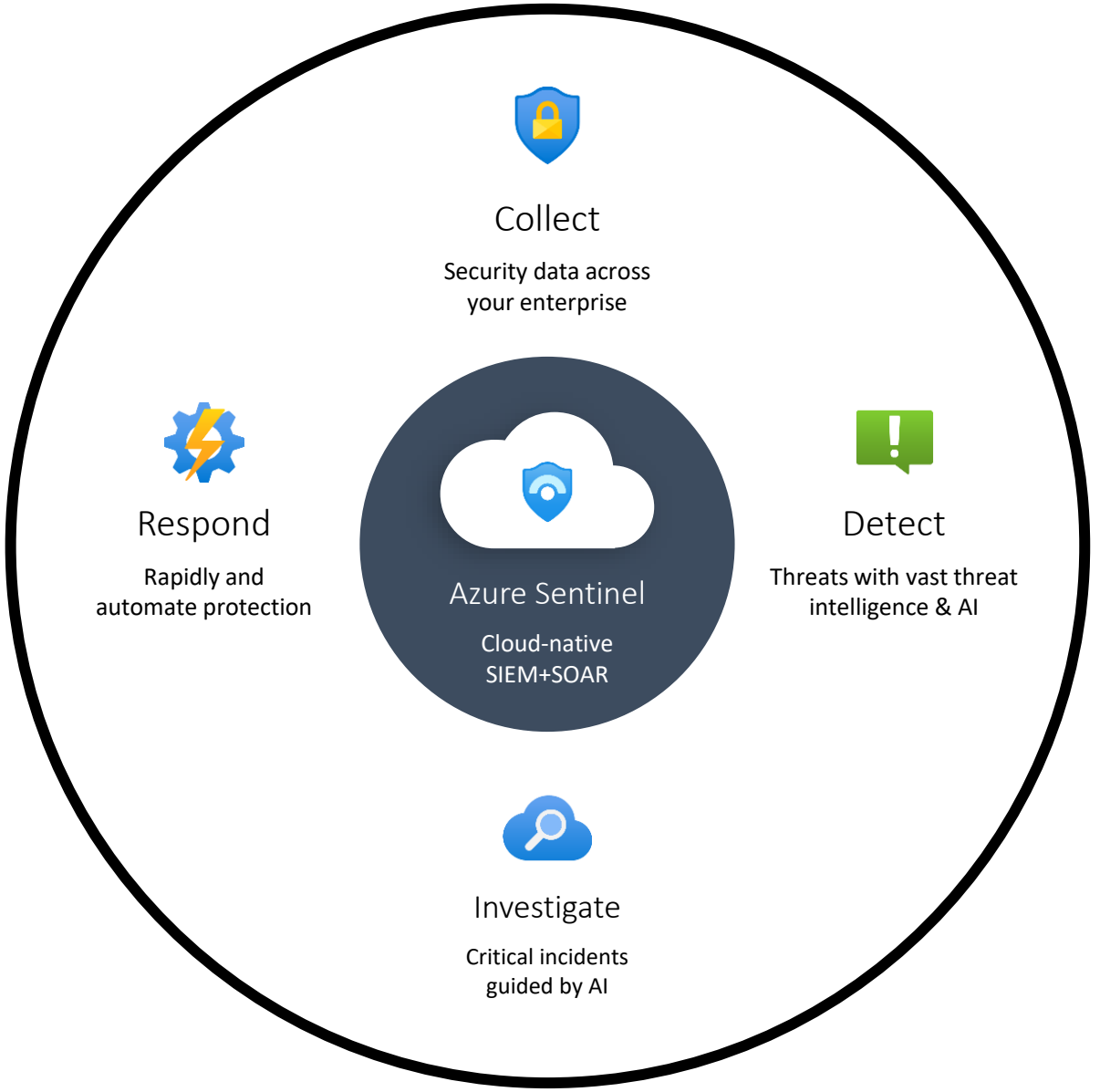
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your Office 365 + M365 Alerts for Free

Easy integration with your existing tools

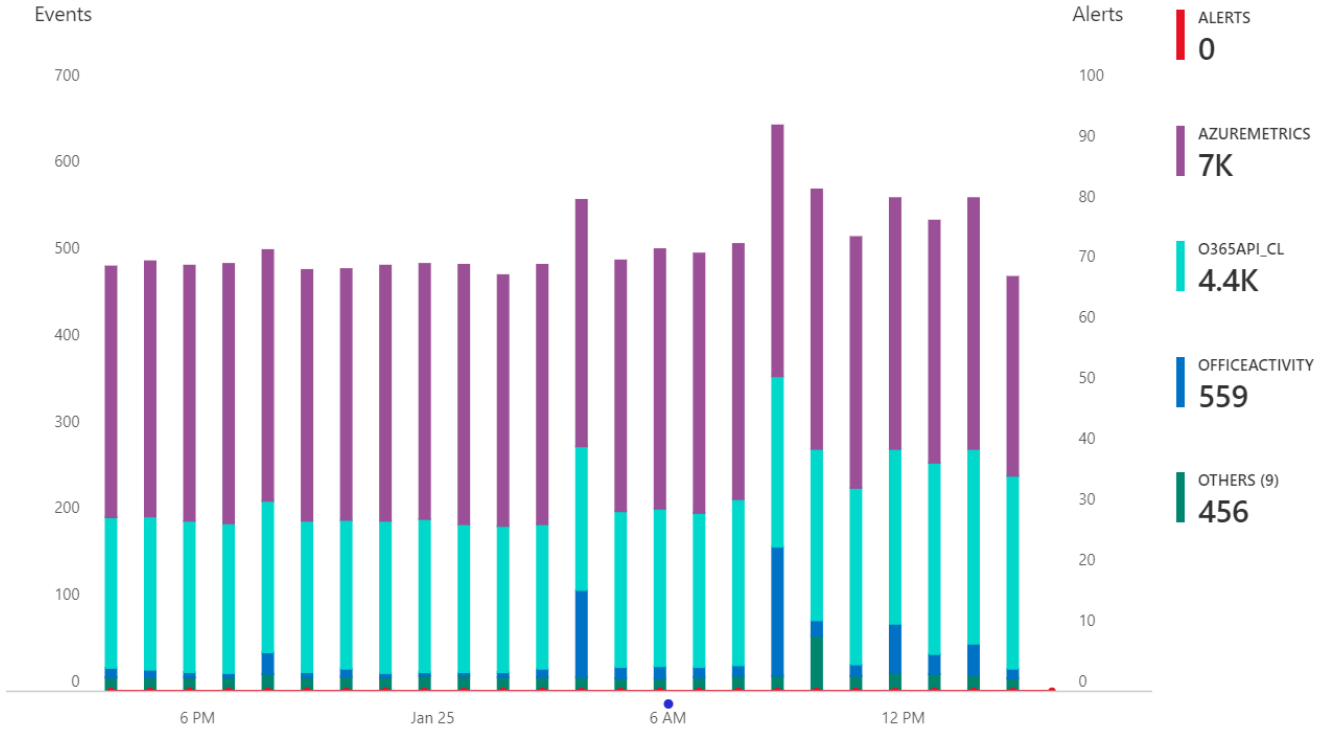
Faster threat protection with AI by your side



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



ALERTS 0
AZUREMETRICS 7K
O365API_CL 4.4K
OFFICEACTIVITY 559
OTHERS (9) 456

Potential malicious events

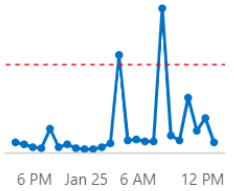
POTENTIAL MALICIOUS EVENTS 0
OUTBOUND 0
INBOUND AND UNKNOWN 0

Recent incidents

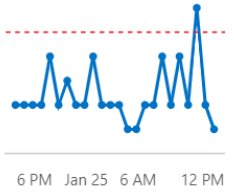
Medium Failed logins from external 1 Al

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.

Microsoft SENTINEL

Core capabilities

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security solutions

Analyze & detect threats

Machine learning, UEBA

Investigate & hunt suspicious activities

Interactive Attack Visualization, Azure Notebooks

Automate & orchestrate response

Playbooks

Enrichment with Intelligence (Geo location, IP Reputation)

Data Ingestion

Data Repository

Data Search

Azure Monitor (log analytics)

Integrate

ServiceNow

Other tools

Community

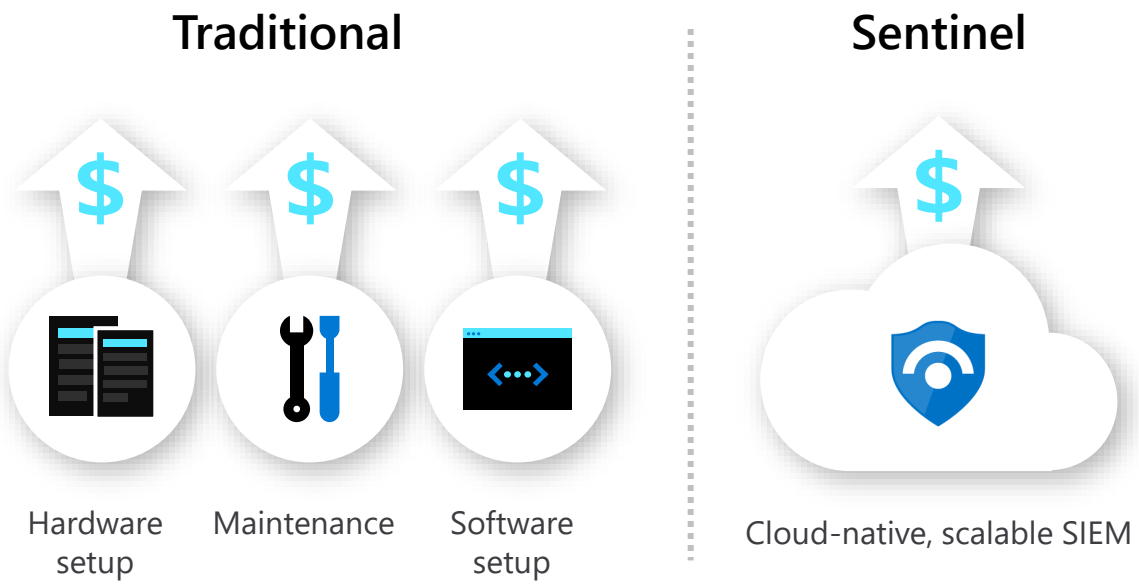
What is Microsoft Sentinel?

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



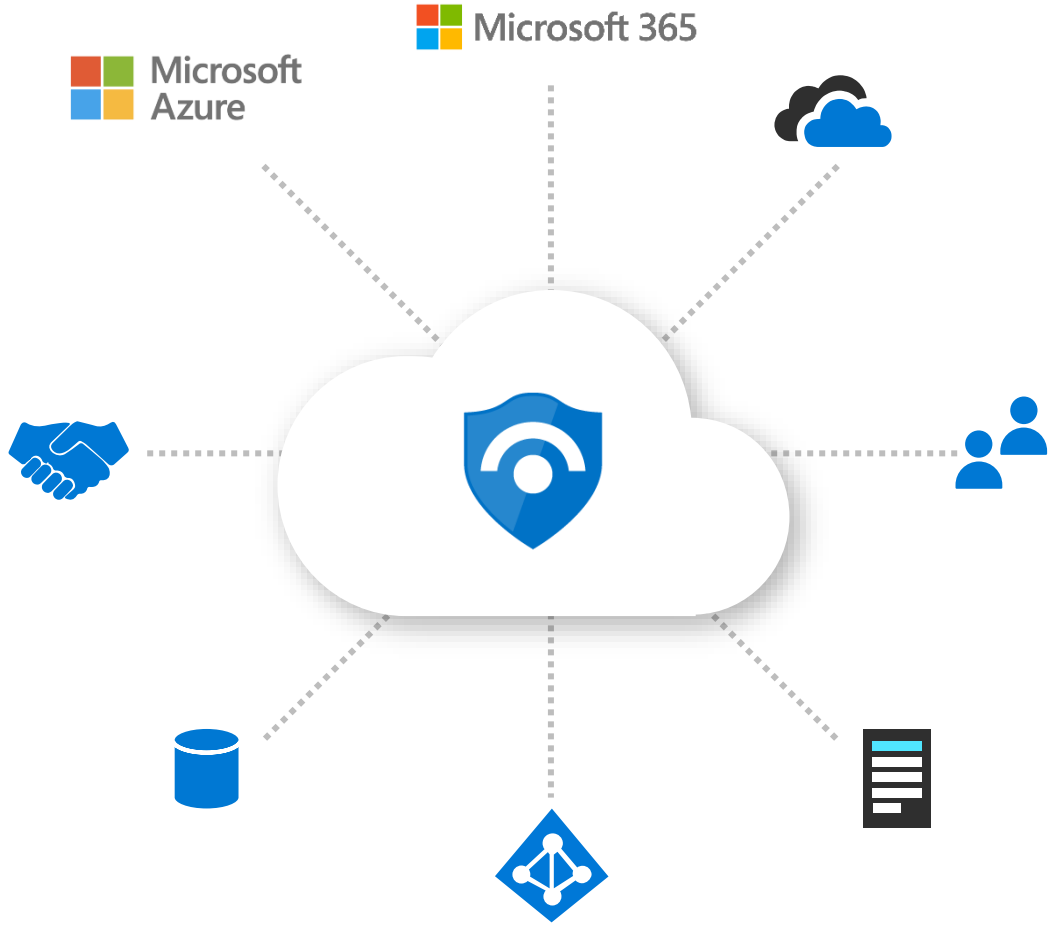
And how it plays into the larger story…

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



Azure Sentinel | Data connectors

Selected workspace: 'ciaops'

Search (Ctrl+/)

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

Guides & Feedback | Refresh

74 Connectors | 8 Connected | 0 Coming soon

Search by name or provider | Providers : All | Data Types : All | Status : All

Status	Connector name
	AI Vectra Detect (Preview) — Vectra AI
	Alcide kAudit (Preview) — Alcide
	Amazon Web Services — Amazon
	Azure Active Directory — Microsoft
	Azure Active Directory Identity Protection — Microsoft
	Azure Activity — Microsoft
	Azure DDoS Protection — Microsoft
	Azure Defender — Microsoft
	Azure Defender for IoT — Microsoft
	Azure Firewall — Microsoft

Azure Active Directory

Connected (Status) | Microsoft (Provider) | 2 hours ago (Last Log Received)

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

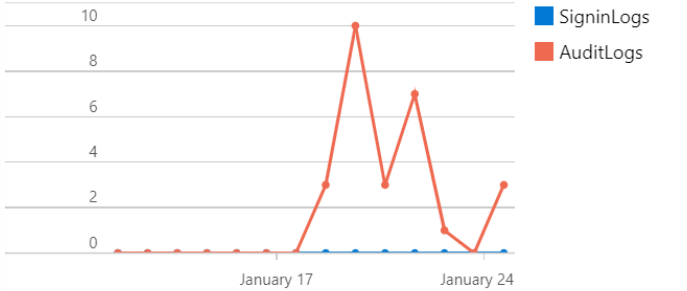
Last data received

01/25/21, 02:00 PM

Related content

6 Workbooks | 2 Queries | 36 Analytic rules templates

Data received — Go to log analytics



Total data received | Total data received

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
High	Known Strontium group domains	Scheduled	Enabled	Commar
High	Known IRIDIUM IP	Scheduled	Enabled	Commar
High	Known Phosphorus group domains/IP	Scheduled	Enabled	Commar
High	Create incidents based on Azure Security Center al...	Microsoft Secur...	Enabled	
High	Create incidents based on Azure Active Directory I...	Microsoft Secur...	Enabled	
High	Advanced Multistage Attack Detection	Fusion	Enabled	
High	Create incidents based on Azure Advanced Threat ...	Microsoft Secur...	Enabled	
High	Create incidents based on Microsoft Defender Adv...	Microsoft Secur...	Enabled	
High	Create incidents based on Microsoft Cloud App Se...	Microsoft Secur...	Enabled	
High	Known Manganese IP and UserAgent activity	Scheduled	Enabled	
High	Create incidents based on Office 365 Advanced Th...	Microsoft Secur...	Enabled	
High	Suspicious application consent similar to O365 Att...	Scheduled	Enabled	
High	First access credential added to Application or Ser...	Scheduled	Enabled	Credenti
Medium	Failed AzureAD logons but success logon to host	Scheduled	Enabled	
Medium	Malware in the recycle bin	Scheduled	Enabled	Defense
Medium	CIAOPS - URL detonation	Scheduled	Enabled	
Medium	Suspicious number of resource creation or deploy...	Scheduled	Enabled	Impact
Medium	SSH Potential Brute Force	Scheduled	Enabled	Credenti
Medium	Rare high NXDomain count	Scheduled	Enabled	Commar
Medium	SharePointFileOperation via devices with previousl...	Scheduled	Enabled	Exfiltratic
Medium	Process executed from binary hidden in Base64 en...	Scheduled	Enabled	
Medium	Brute force attack against Azure Portal	Scheduled	Enabled	Credenti
Medium	SSH newly internet-exposed endpoints	Scheduled	Enabled	Initial Ac
Medium	Multiple users email forwarded to same destination	Scheduled	Enabled	
Medium	User account created and deleted within 10 mins	Scheduled	Enabled	

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

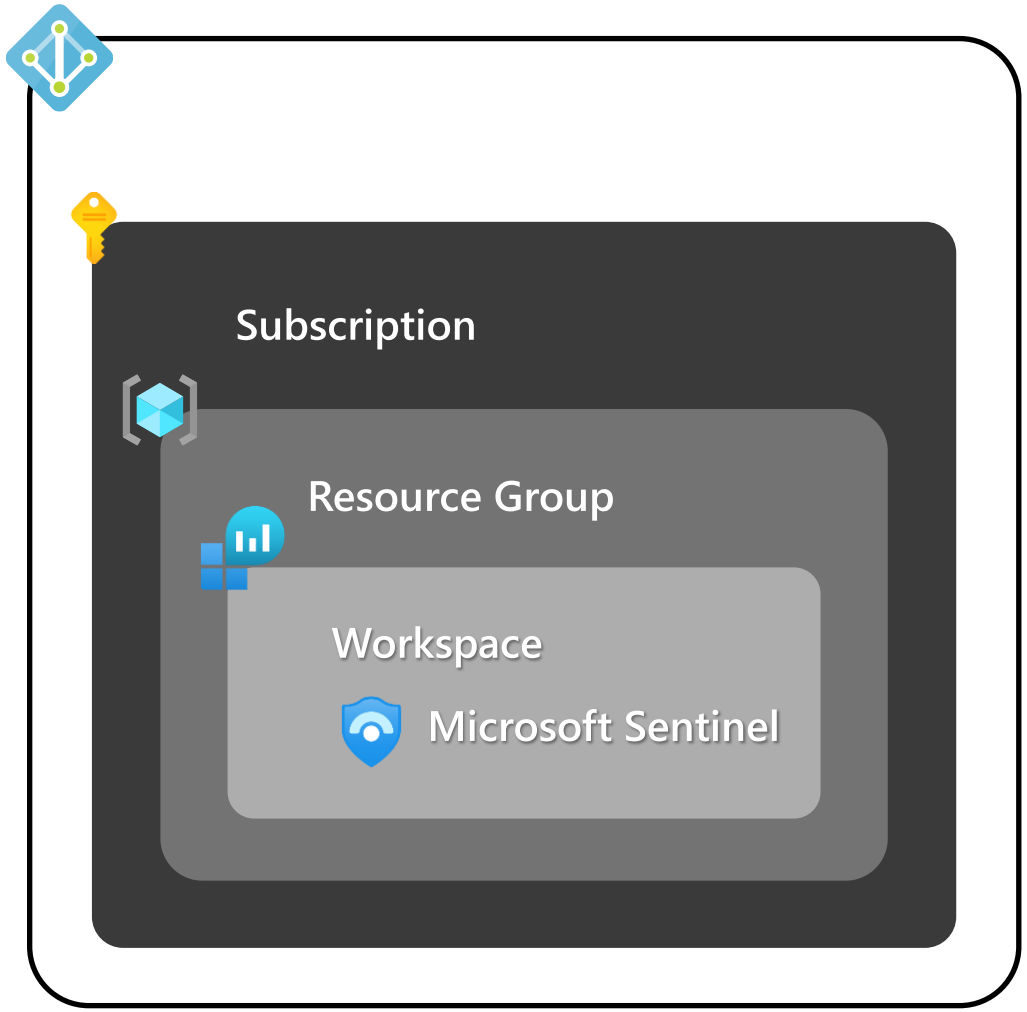
Event grouping
Group all events into a single alert

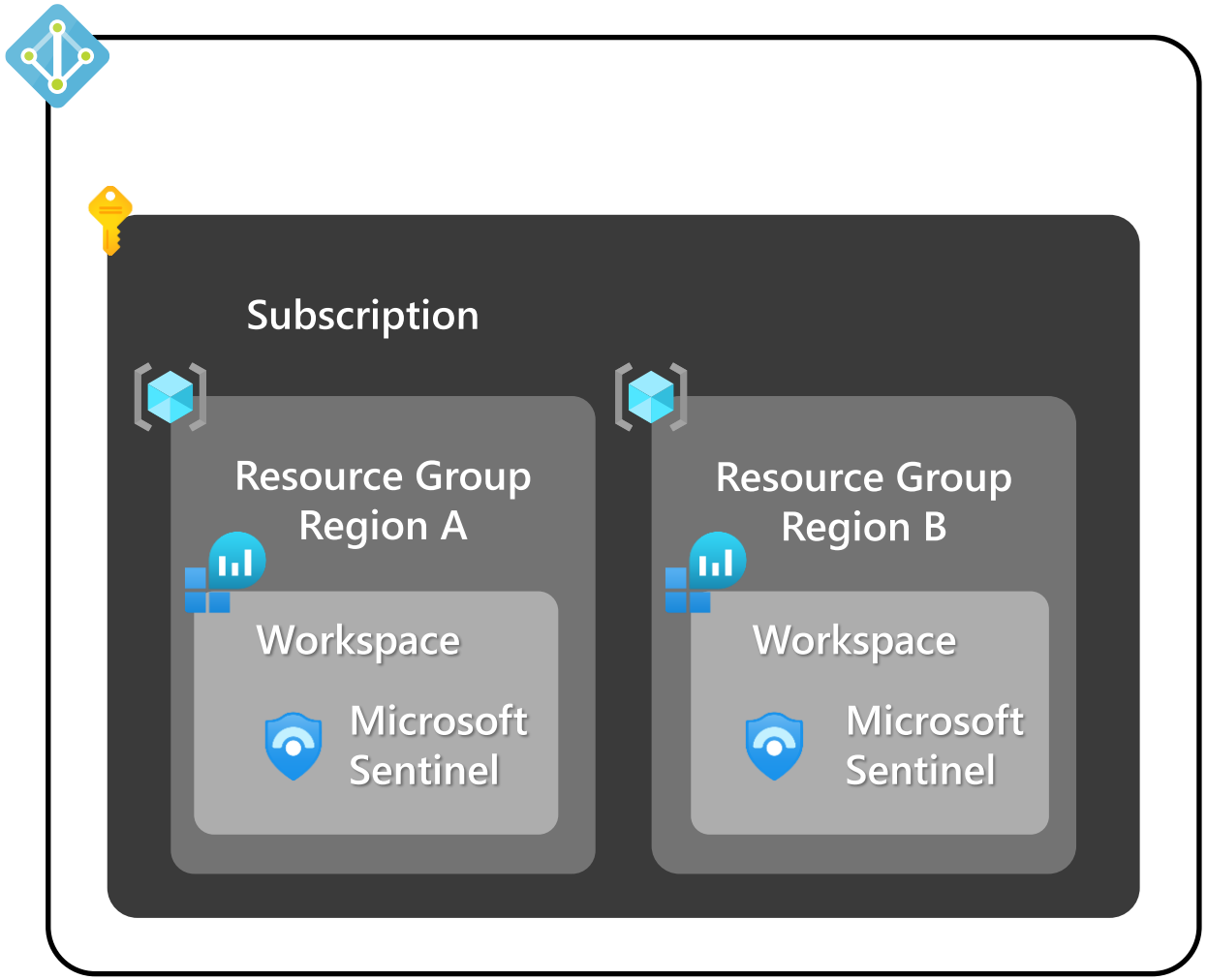
Suppression
Not configured

Create incidents from this rule
Enabled

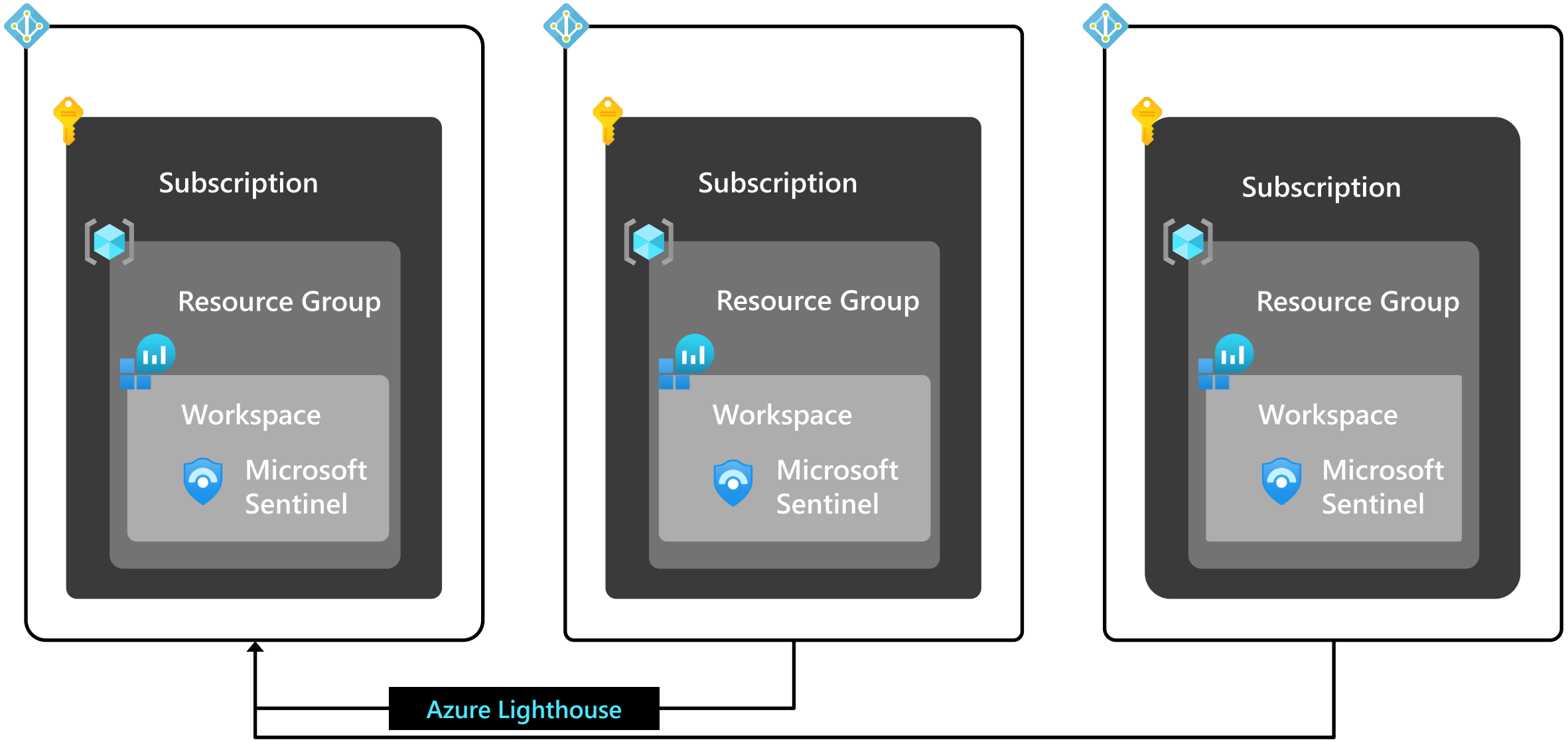
Alert grouping
Disabled

Workspace Design (Single Tenant)

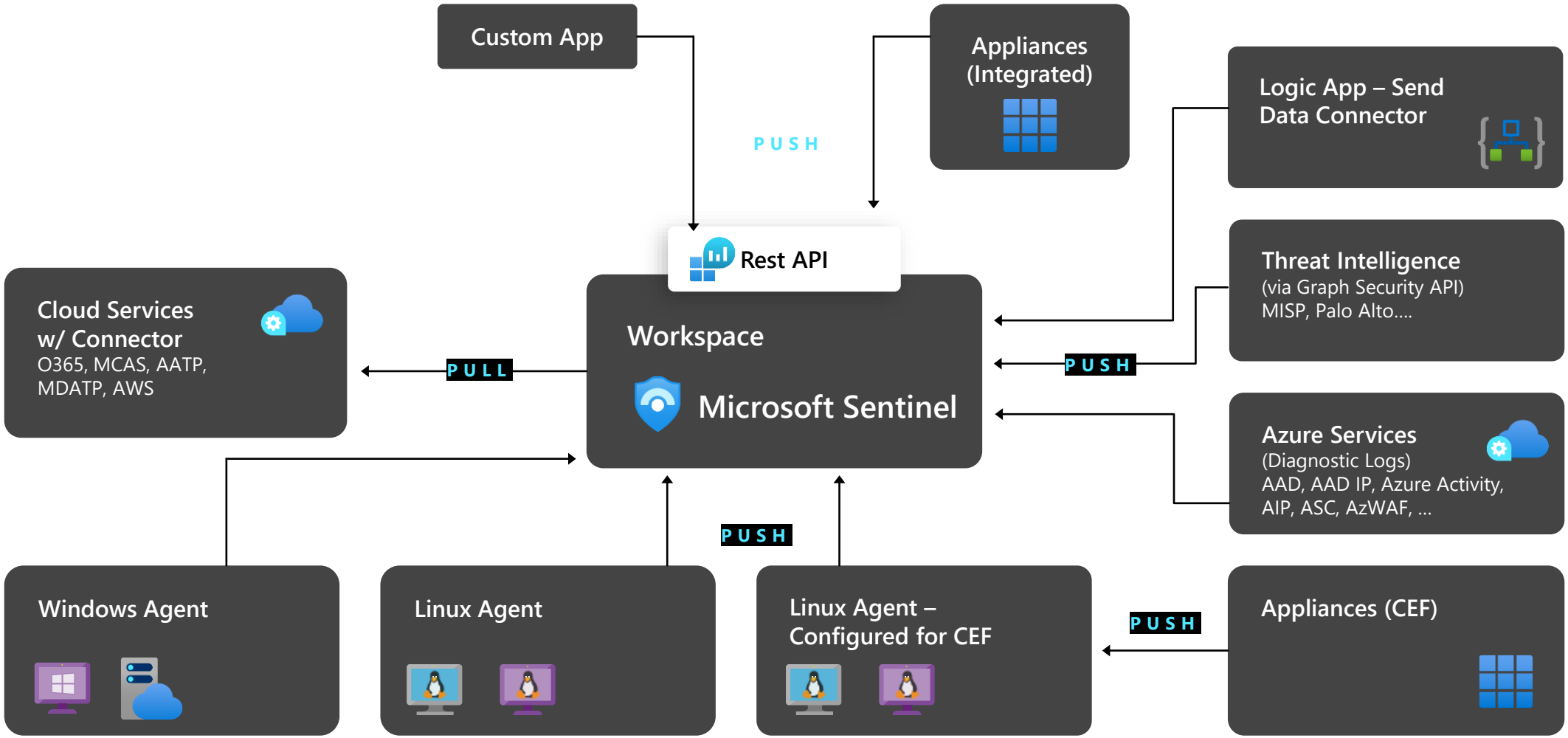




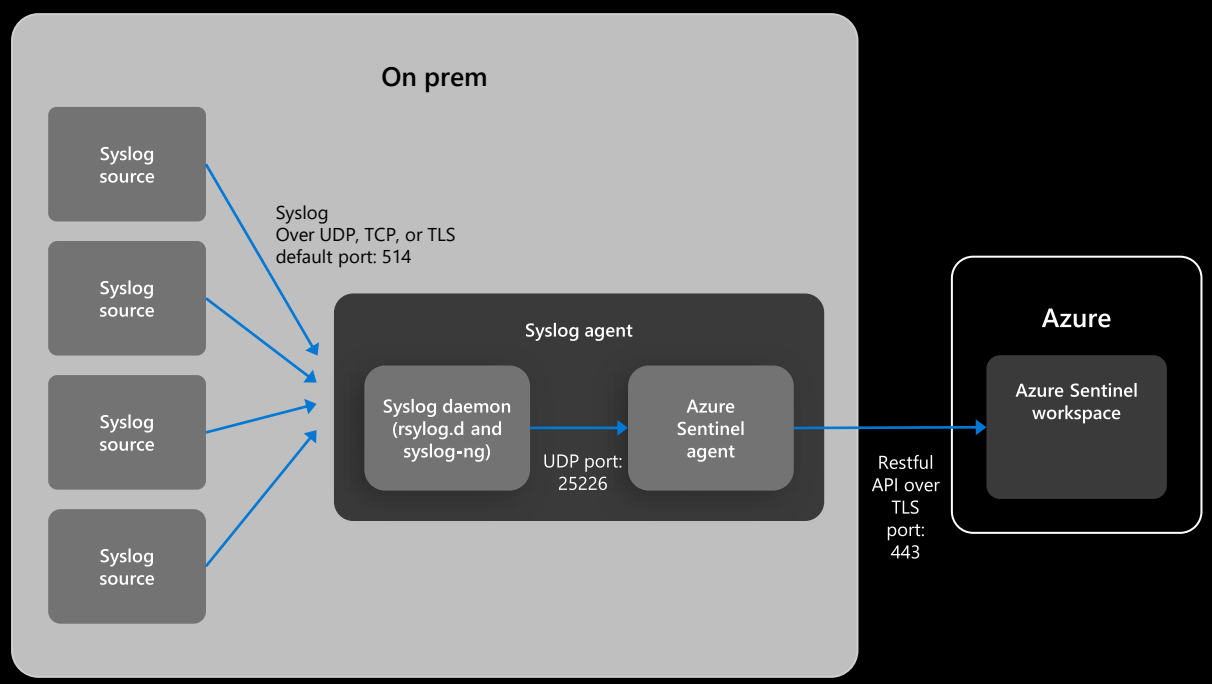
Workspace Design (Multi-Tenant)

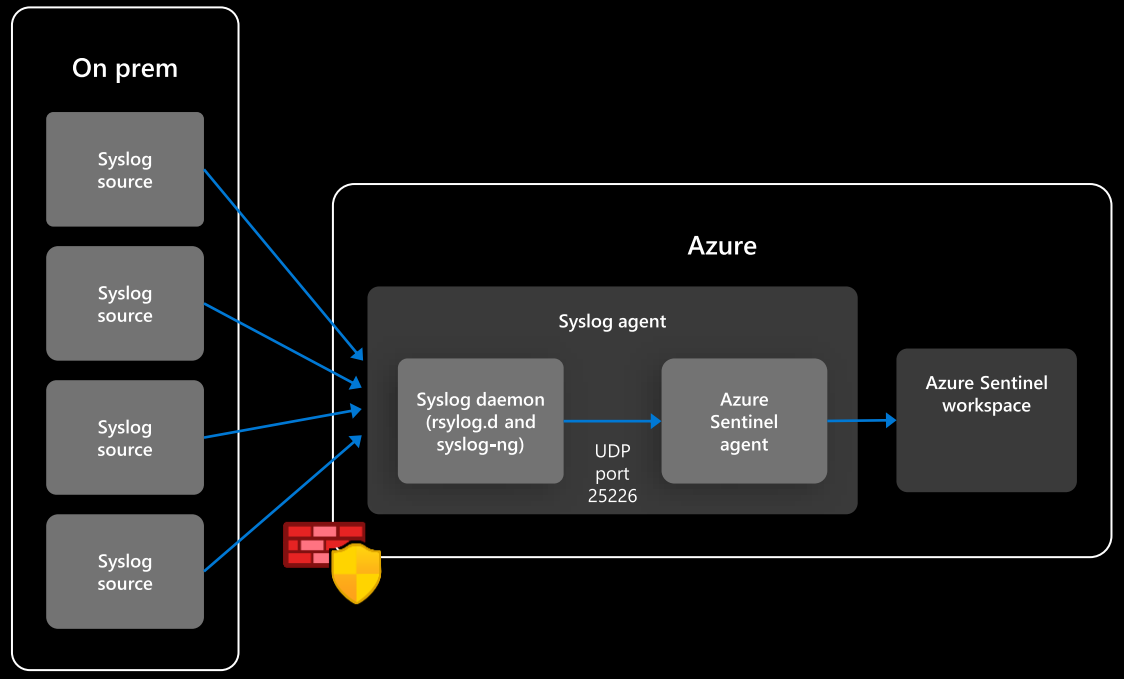


All the ways data gets in



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)

BEST PRACTICE

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

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

CIAOPS Resources

- Blog – http://blog.ciaops.com
- Github – http://github.com/directorcia
- Free Office 365, Azure Administration newsletter – http://bit.ly/cia-o365-tech
- Free Office 365, Azure video tutorials – http://www.youtube.com/directorciaops
- Free documents, presentations, eBooks – http://slideshare.net/directorcia
- Office 365, Azure, Cloud podcast – http://ciaops.podbean.com
- Office 365, Azure online training courses – http://www.ciaopsacademy.com
- Office 365 and Azure community – http://www.ciaopspatron.com

Twitter
@directorcia

Facebook
https://www.facebook.com/ciaops

Email
director@ciaops.com

Teams
admin@ciaops365.com