



Microsoft Sentinel

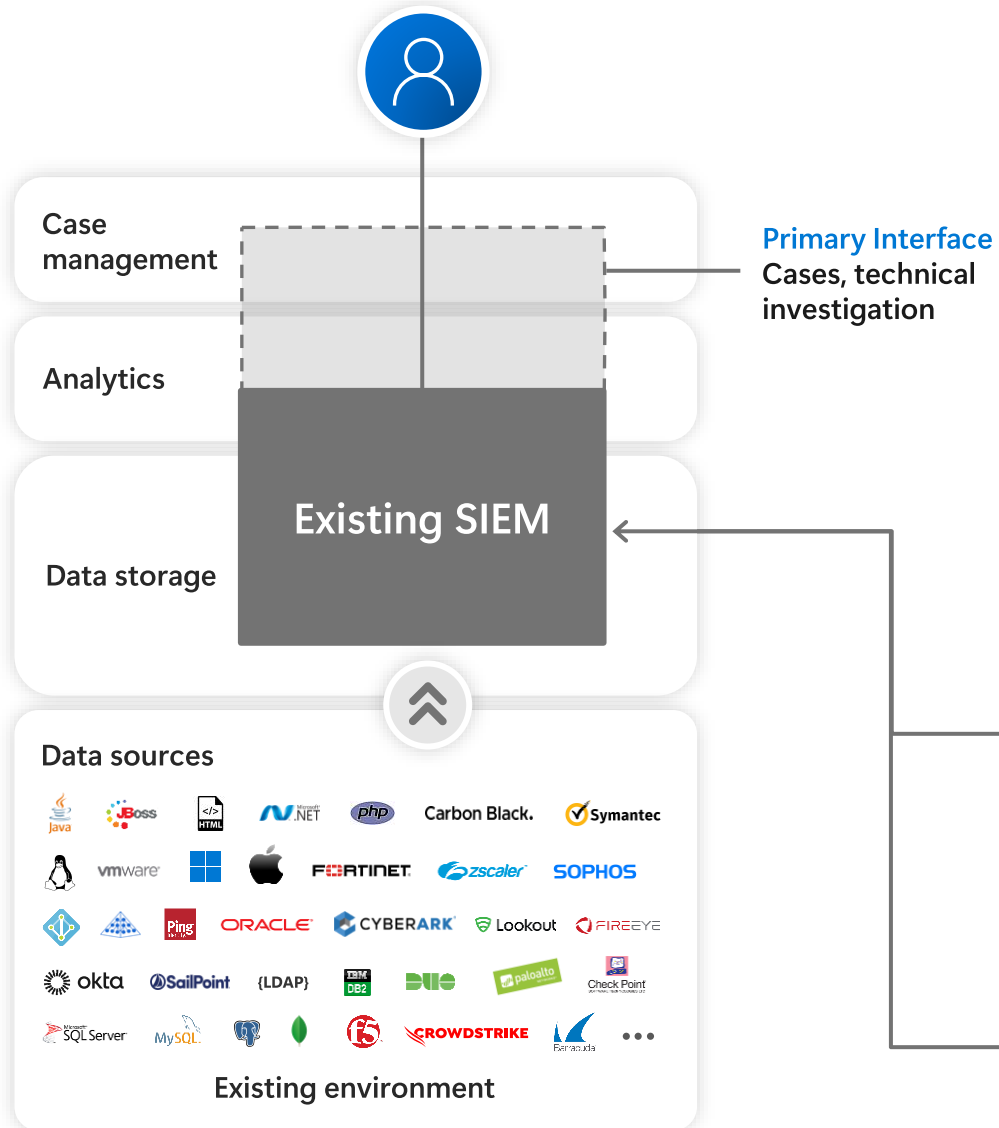
Architecture options
for MSSPs

System4u SecuRadar

Luděk Suk
Microsoft

Legacy SIEM architecture

with XDR

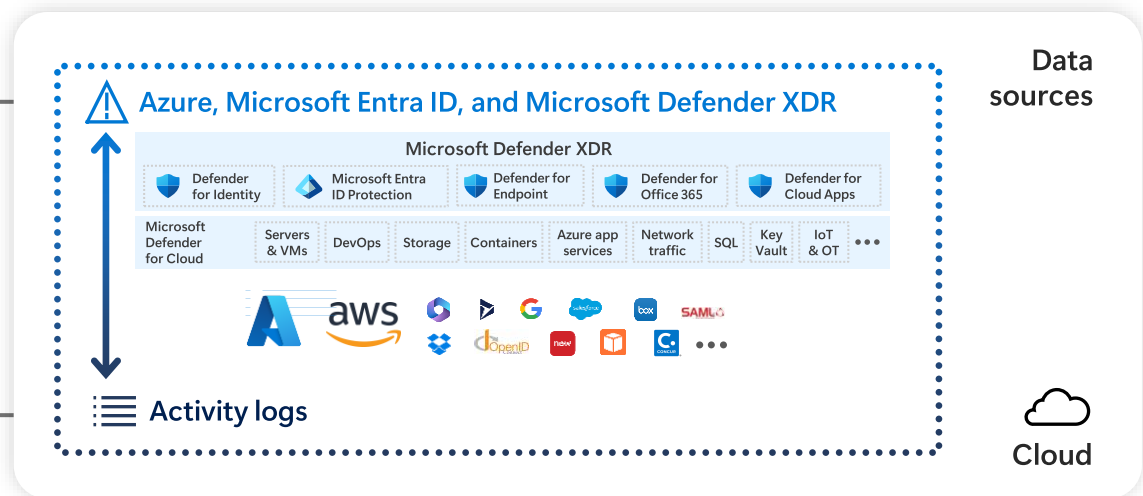


Advantages

✓ **Well-understood** – Classic/legacy SIEM architecture and skills for static queries have stayed relatively stable and consistent since early 2000s

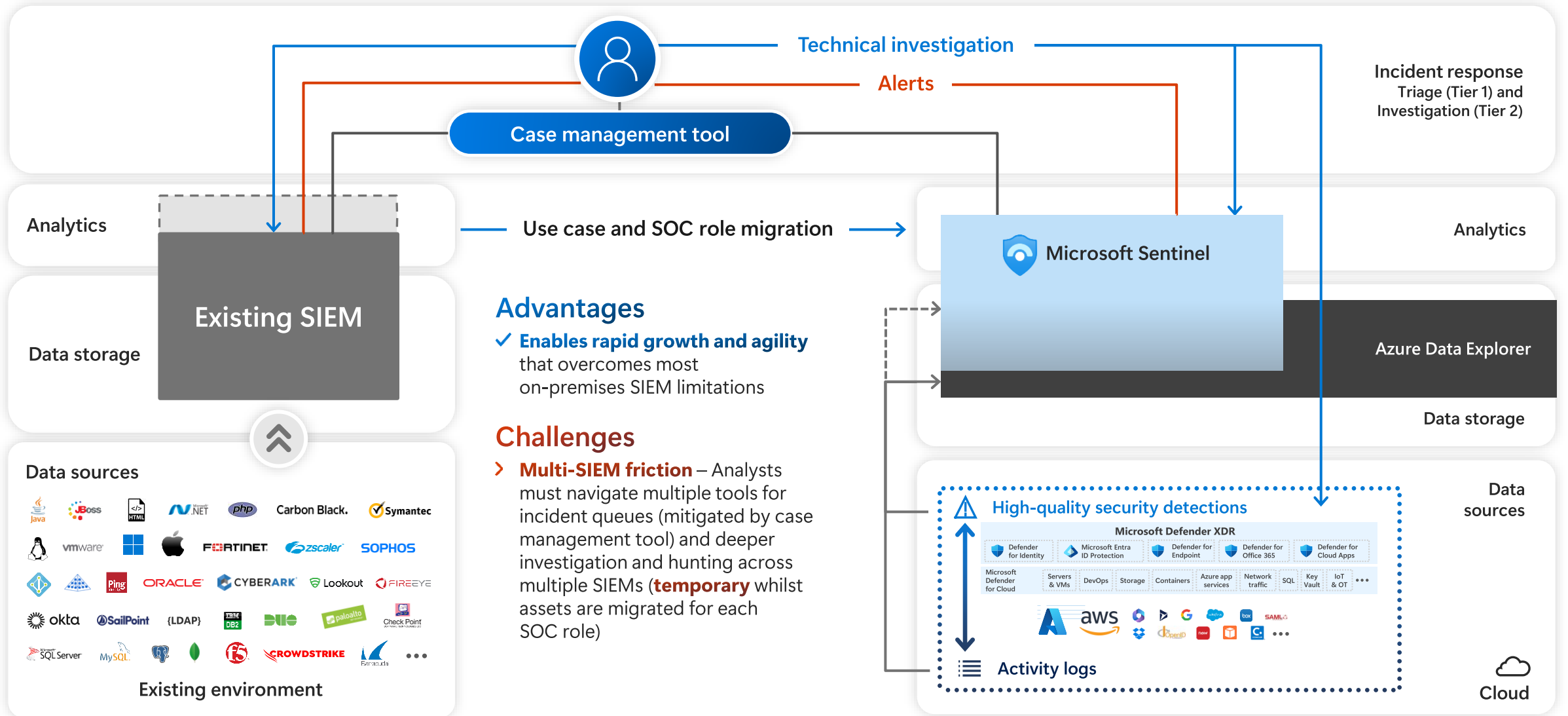
Challenges

- **False positive overload** – Analysts overloaded from false positives alerts (false alarms) because of difficulty of getting clean alerts from static queries and manual correlation
- **Poor investigation workflow** – Common analyst workflows (investigation, escalation, etc.) often require case management tooling and customization work
- **Limited analytics** – Legacy SIEMs often lack native support for machine learning, alert correlation and fusion across sources, SOAR automation and orchestration, and behavior analytics
- **Cost vs. visibility tradeoff** – High cost to increasing storage often forces organizations into choosing between complete visibility and cost control—constricting agility and scale while increasing organizational risk (of missed attackers causing damage)

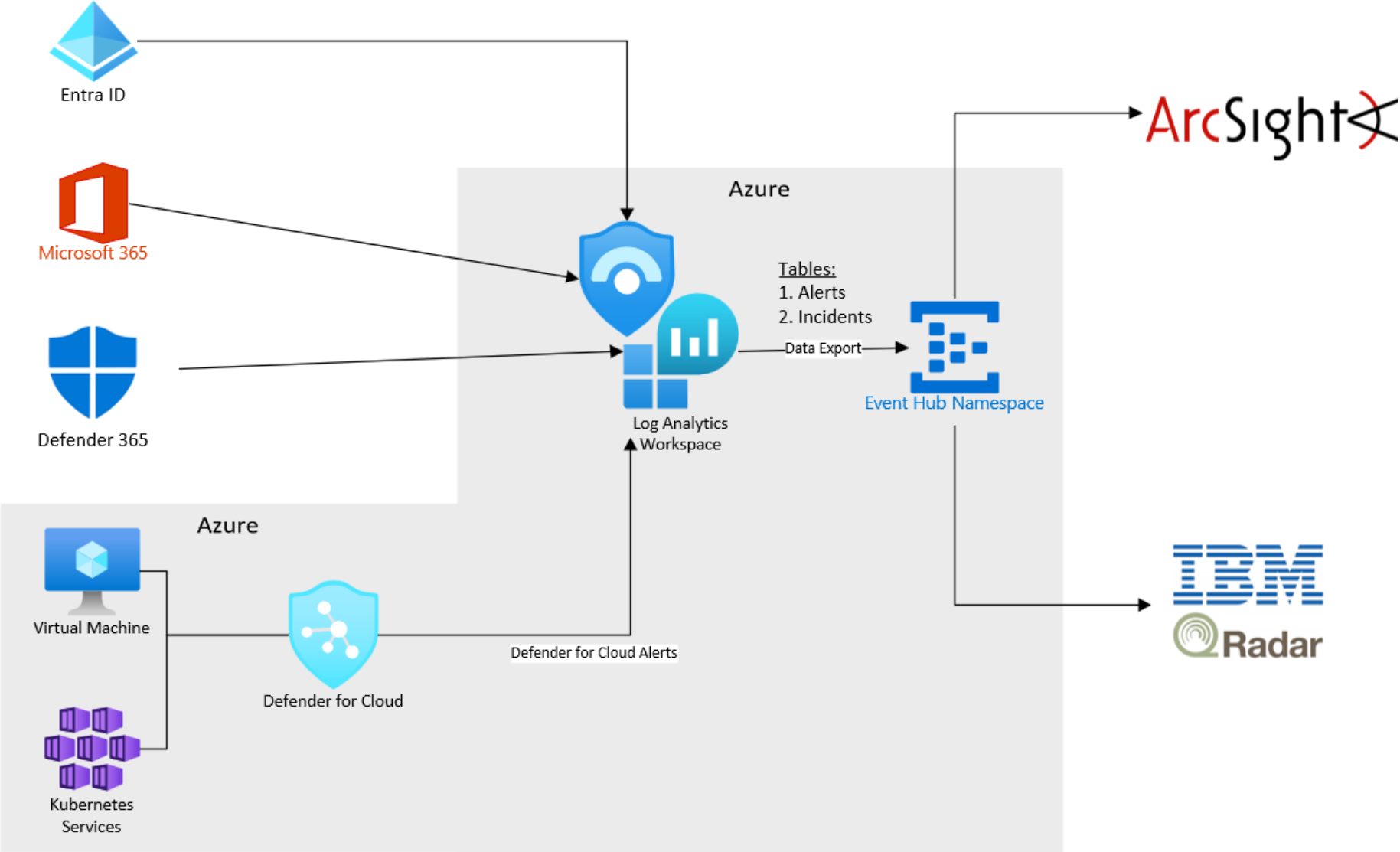


Side-by-side SIEM architecture

with XDR and Security Data Lake



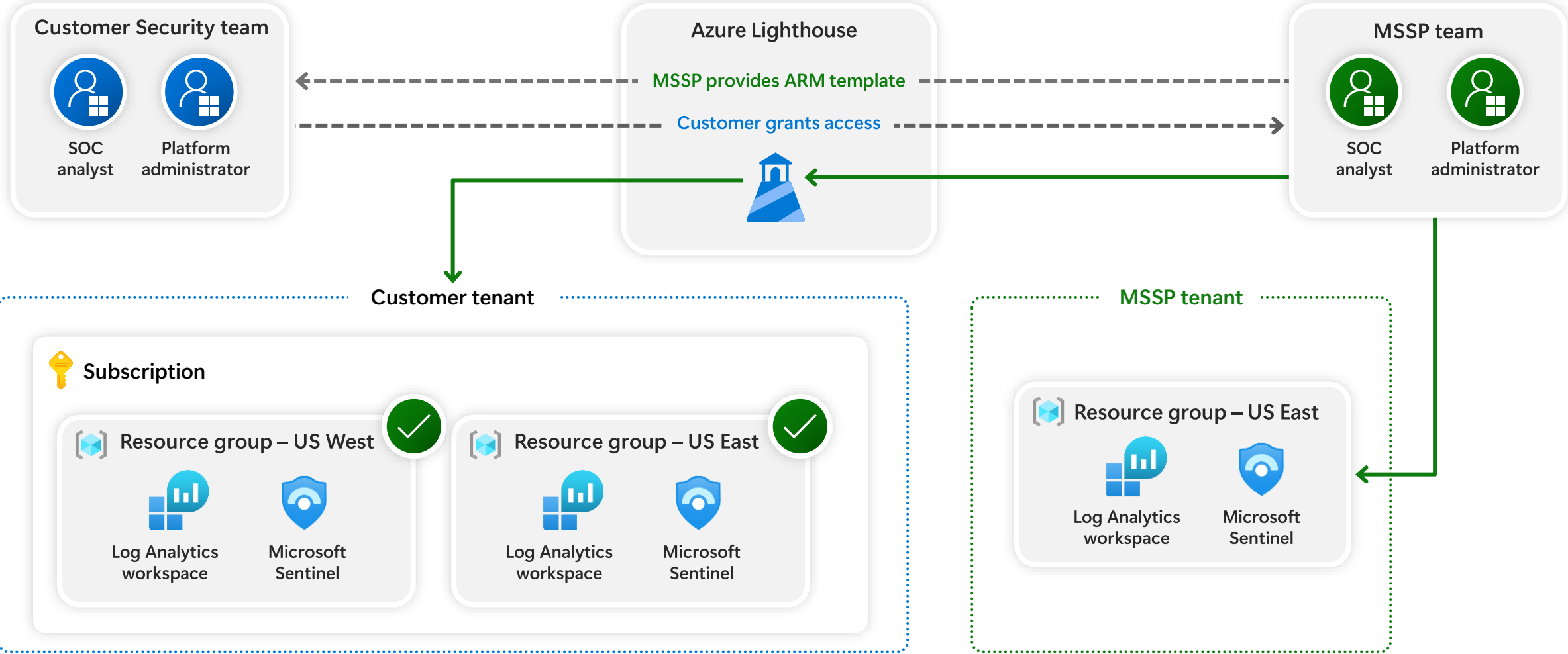
Sentinel side-by-side model architecture



MSSP architecture with Azure Lighthouse



MSSP scenario – MSSP allowed to managed subscription



View incident across multiple customer tenants (Azure Lighthouse)

[Home](#) >


Microsoft Sentinel ...


Microsoft

[+](#) Create [⚙️](#) Manage view [↻](#) Refresh [↓](#) Export to CSV [🔗](#) Open query [📁](#) View incidents [🗨️](#) Feedback

Filter for any field...

Subscription == **71 of 82 selected**


Resource group == **all** 


Location == **all** 

[+🔍](#) Add filter

Showing 1 to 4 of 4 records.

No grouping 

List view 

<input checked="" type="checkbox"/> Name 	Resource group 	Location 	Subscription 	Directory 
<input checked="" type="checkbox"/>  ContosoCorpSentinelWork Customer A tenant	demo_catalog	East US	Partner_Sandbox	Microsoft
<input checked="" type="checkbox"/>  CyberSecuritySOC Customer B tenant	soc	Central US	CyberSecSOC	contosohotels.com
<input checked="" type="checkbox"/>  Sentinel-Development Customer C tenant	demo_catalog	West Europe	Security - Common	Microsoft
<input checked="" type="checkbox"/>  temp-workspace Customer D tenant	demo_catalog	West Europe	Security - Common	Microsoft

< Previous

Page

1

of 1

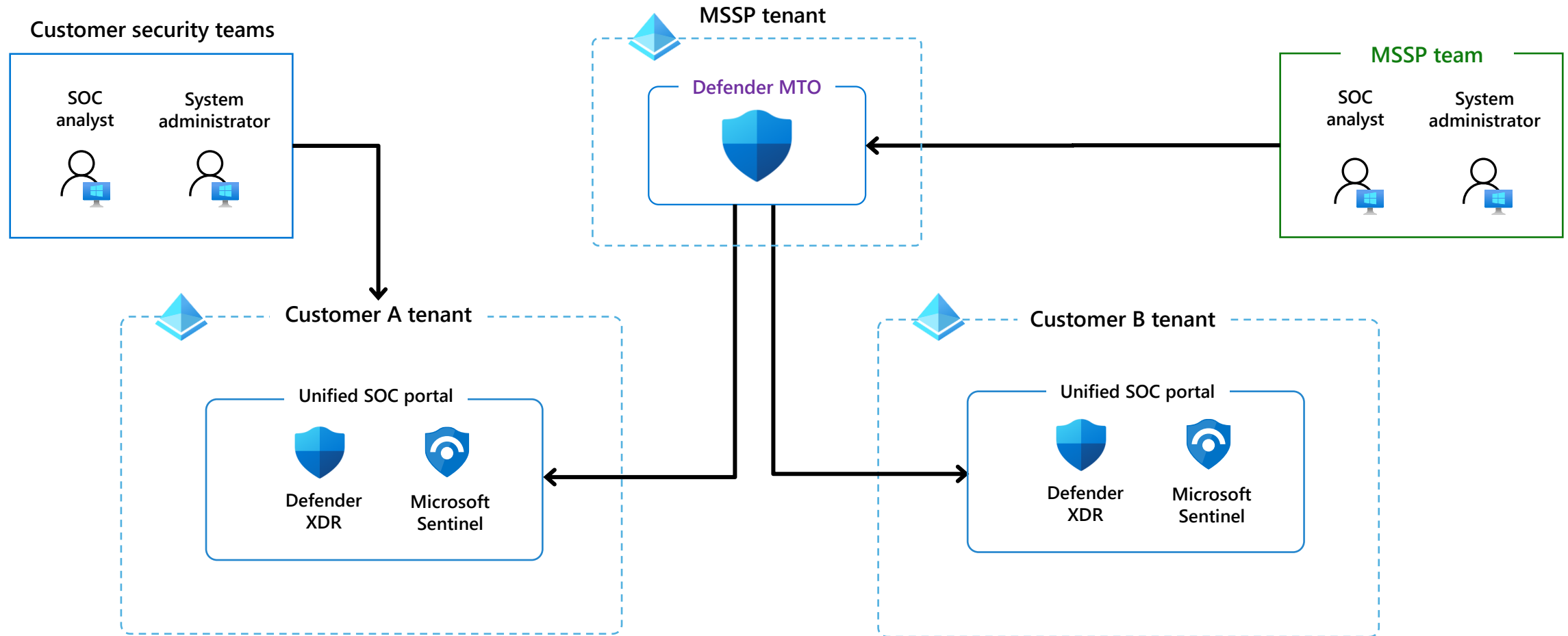
Next >

MSSP architecture with Defender MTO



Sentinel Architecture with Defender MTO (multi-tenant organization)

- A) Customer is using Defender XDR with integrated Sentinel
- B) Microsoft 365 E5 license may be required after preview ends





Sentinel can be accessed in Defender XDR console of each tenant

- Investigation & response
- Threat intelligence
- Assets
- Microsoft Sentinel**
 - Search
 - Threat management
 - Workbooks
 - Hunting
 - Notebooks
 - Threat intelligence
 - MITRE ATT&CK
 - Content management
 - Configuration
 - Data connectors
 - Analytics
 - Summary Rules
 - Watchlist
 - Automation

Incidents

Email notification

Most recent incidents and alerts

Export Copy list link

30 Incidents

Search for name or ID

1 Week

Customize columns

Filter set: Save

Status: Active, In Progress

Alert severity: High, Medium

Add filter

Reset all +4 more


<input type="checkbox"/>	<input type="checkbox"/>	Incident name	Incident Id	Tags	Severity	Investigator
<input type="checkbox"/>	>	DLP policy (U.S. Financial Data) matched for email...	2670	External user risk	High	
<input type="checkbox"/>	>	Exfiltration incident involving multiple users	2623	External user risk	Medium	
<input type="checkbox"/>	>	Multi-stage incident involving Execution & Lateral...	1788	Ransomware +10	High	2 investigatic
<input type="checkbox"/>	>	Multi-stage incident involving Initial access & Lat...	2219	Critical asset +4	High	3 investigatic
<input type="checkbox"/>	>	Multi-stage incident involving Initial access & Lat...	2563	Ransomware +7	High	5 investigatic
<input type="checkbox"/>	>	Attack using AiTM phishing (attack disruption)	2516	Ransomware +10	High	5 investigatic
<input type="checkbox"/>	>	DLP policy (U.S. Financial Data) matched for email...	2660	External user risk	High	
<input type="checkbox"/>	>	DLP policy (U.S. Financial Data) matched for email...	2655	External user risk	High	
<input type="checkbox"/>	>	Suspicious authentication activity on one endpoint	2653		Medium	

Add multiple tenants to Defender MTO

Microsoft 365 Defender | Multi-tenant

Search

Diagnostics



Welcome to the multi-tenant view in Microsoft 365 Defender

View and manage security data across all of your tenants.

Tenant selection

Select the tenants to unlock multi-tenant view (up to 50)

+ Add tenants - Remove tenants

4 items Search

<input type="checkbox"/>	Tenant name ↑	Added on	Status
<input type="checkbox"/>	Tenant A e444a514-da5a-4671-b33b-	Sep 15, 2023 2:03 PM	Active
<input type="checkbox"/>	Tenant B acbf9091-12d9-4d19-b769-	Sep 15, 2023 2:03 PM	Active
<input type="checkbox"/>	Tenant C 1fa99f2d-20af-4cff-b2fa-dc5	Sep 15, 2023 2:03 PM	Active
<input type="checkbox"/>	Tenant D f839b112-d9d7-4d27-9bf6-	Sep 15, 2023 2:03 PM	Active

View incident across multiple tenants in Defender MTO

Microsoft Defender | Multi-tenant

Search

Incidents

The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, [see incident queue details](#).

Export Search for name or ID 1 Week Customize columns

Filter set: Save

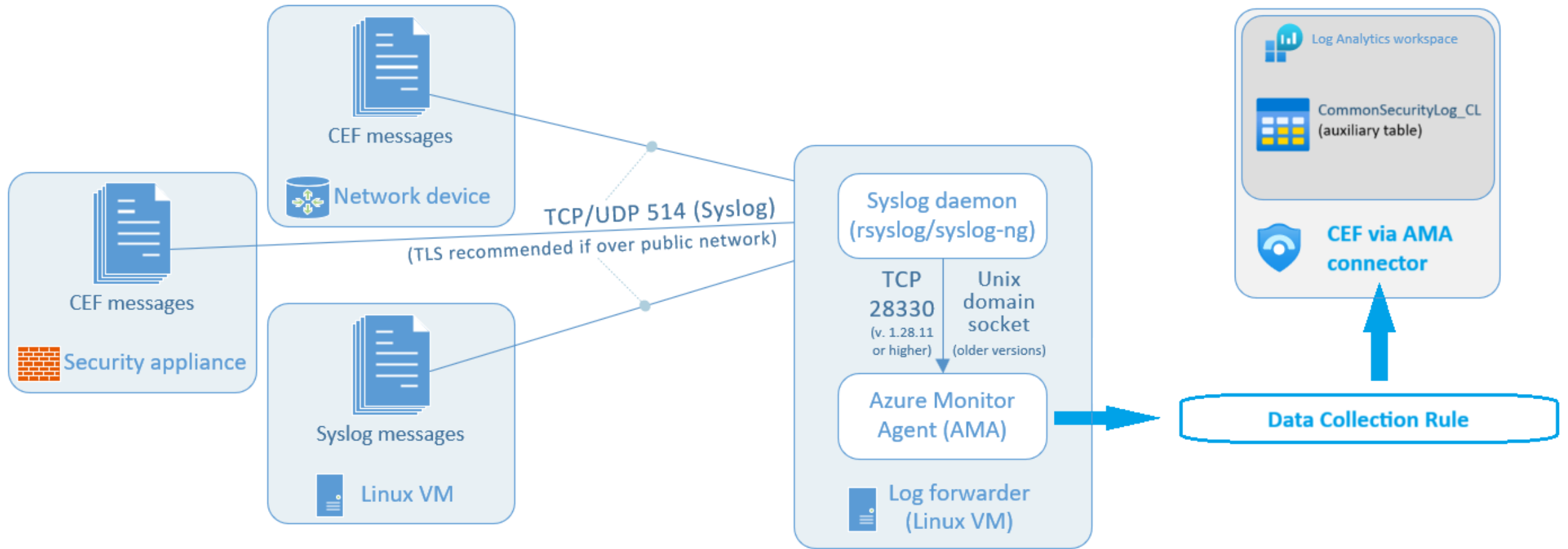
Status: Active, In Progress Alert severity: High, Medium, Low, +1 Incident severity: High, Medium, Low, +1 Add filter Reset all +3 more

Incident name	Tenant name	Severity	Investigation state	Categories	Active alerts	Service sources
Multi-stage incident involving Initial access & Exfi...	Tenant C	High	2 investigation states	Initial access, Execution, Pe...	14/15	Endpoint, Identity, Mic
Email messages containing malicious URL remove...	Tenant D	Informational	Terminated by system	Initial access	1/1	Office 365
Email messages containing malicious URL remove...	Tenant A	Informational	Terminated by system	Initial access	1/1	Office 365
Failed login attempts to Azure Portal involving m...	Tenant A	Low		Credential access	1/1	Microsoft Sentinel
Failed login attempts to Azure Portal involving m...	Tenant B	Low		Credential access	1/1	Microsoft Sentinel
Suspicious activity incident on multiple endpoints	Tenant B	Medium		Suspicious activity	3278/3278	Microsoft Sentinel
Failed login attempts to Azure Portal involving on...	Tenant C	Low		Credential access	1/1	Microsoft Sentinel
Multi-stage incident involving Initial access & Exfi...	Tenant A	High		Initial access, Exfiltration	27/27	Microsoft Sentinel
Failed login attempts to Azure Portal involving on...	Tenant C	Low		Credential access	1/1	Microsoft Sentinel
customized alert name	Tenant D	Medium		Lateral movement	6/6	Microsoft Sentinel

Ingestion architecture for auxiliary logs



CEF ingestion architecture for auxiliary logs



system4u



SecuRadar



Microsoft Security Partners portal

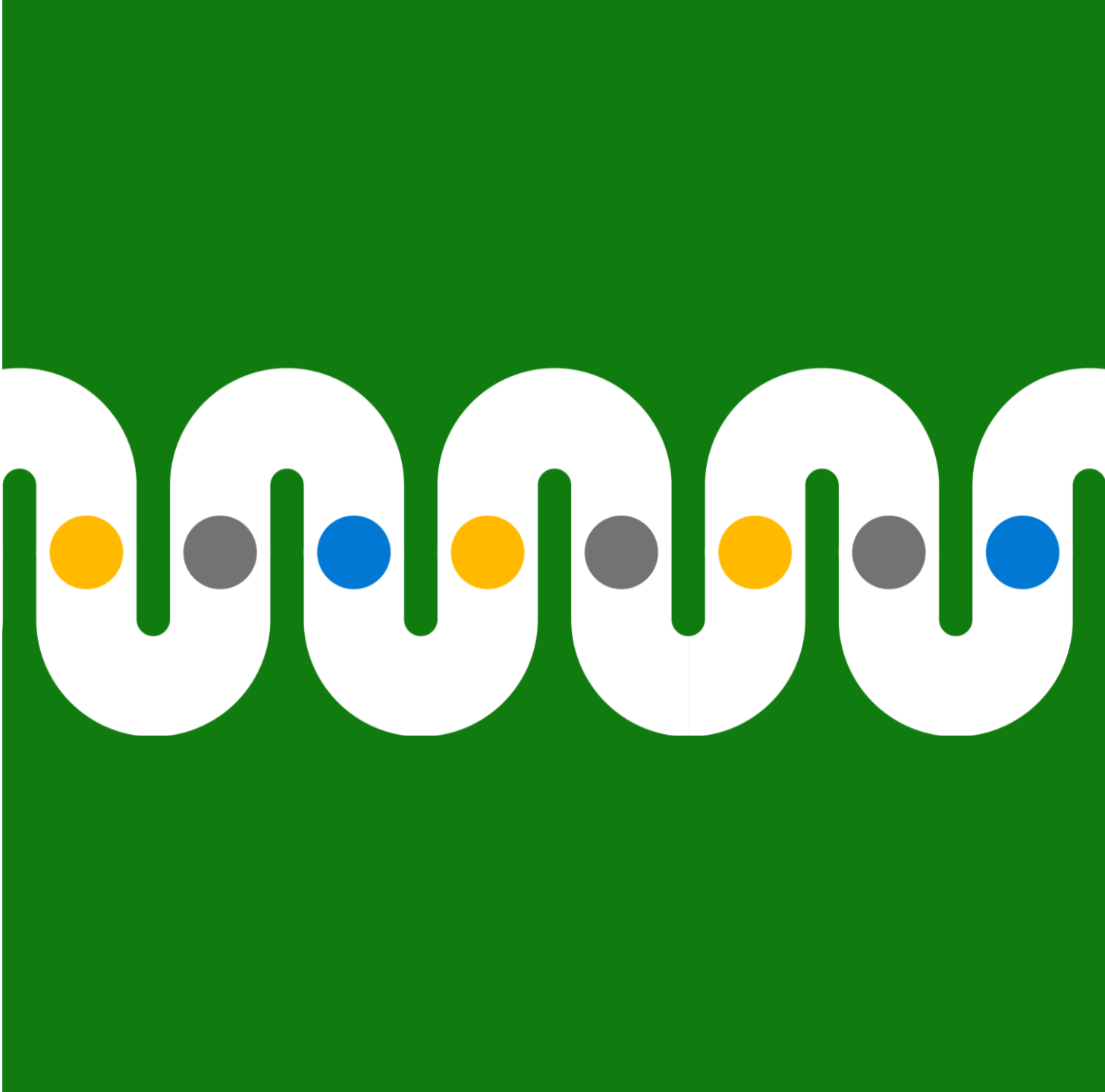
Product and solution presentations

- [Microsoft Sentinel Rapid Adoption Guide](#) 🔒
- [Modernize your SOC with Microsoft Sentinel Pitch Deck L100](#) 🔒
- [Modernize your SOC with Microsoft Sentinel Pitch Deck L200](#) 🔒
- [Microsoft Sentinel Reference Architecture](#) 🔒
- [Microsoft Sentinel Cost Optimization Guidance and Best Practices](#) 🔒
- [Microsoft Technical Playbook for MSSPs](#) 🔒



<https://securitypartners.transform.microsoft.com>

Q&A





Microsoft Partner Security Day

Praha, 11. 2. 2025

