Monitoring Microsoft 365 Security with Microsoft Sentinel

@jussiroine

@thomasvochten

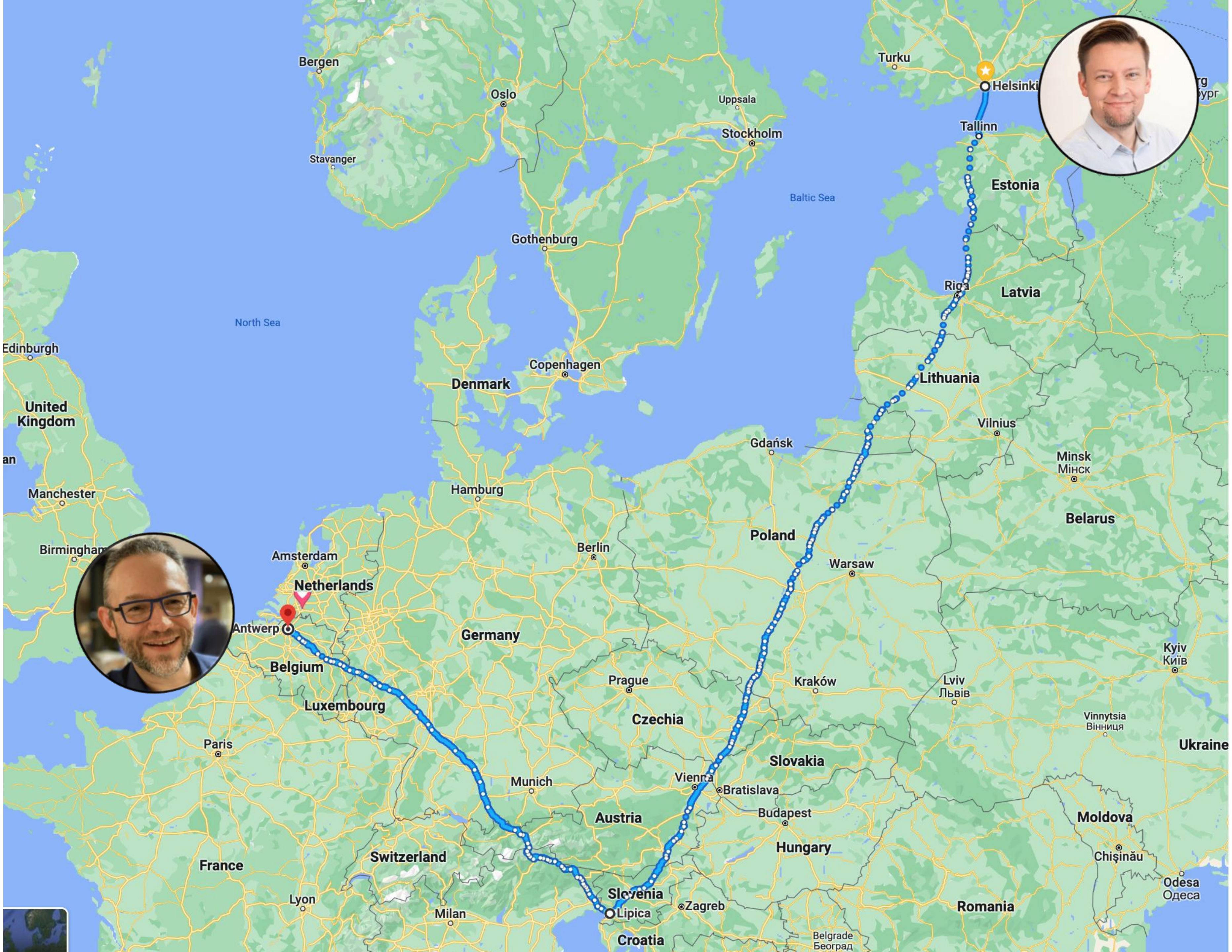
Monitoring Microsoft 365 Security with Microsoft Sentinel

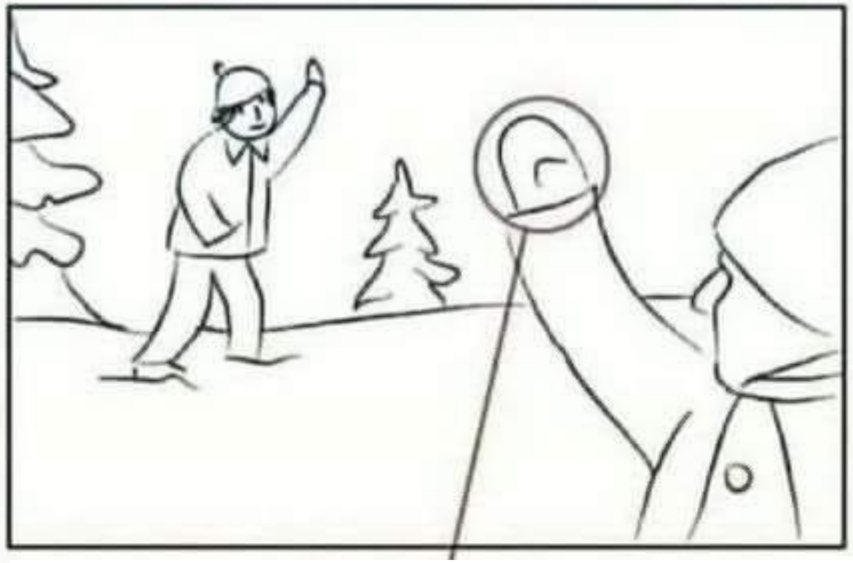
Jussi Roine

Microsoft MVP

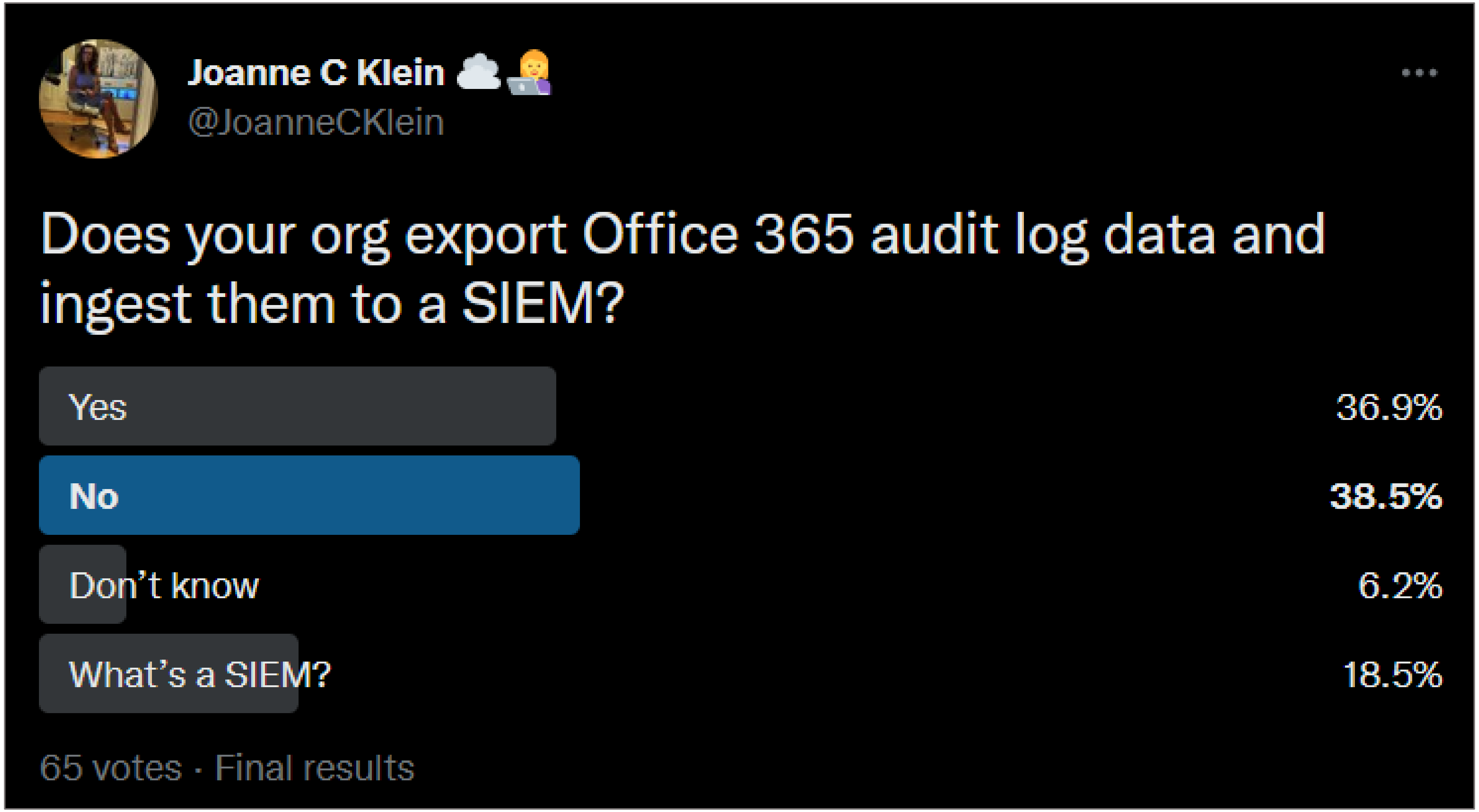
Thomas Vochten

Microsoft MVP


Bergen
Oslo
Turku
Helsinki
Uppsala
Stockholm
Stavanger
Tallinn
Estonia
Baltic Sea
Gothenburg
Riga
Latvia
North Sea
Edinburgh
Copenhagen
Denmark
Lithuania
United Kingdom
Vilnius
Gdańsk
Minsk
Мінск
Hamburg
Manchester
Belarus
Poland
Birmingham
Berlin
Amsterdam
Warsaw
Netherlands
Antwerp
Germany
Kyiv
Київ
Belgium
Prague
Kraków
Lviv
Львів
Luxembourg
Czechia
Vinnytsia
Вінниця
Paris
Ukraine
Slovakia
Vienna
Munich
Bratislava
Austria
Budapest
Moldova
Hungary
Switzerland
France
Chișinău
Odesa
Одеса
Slovenia
Lipica
Zagreb
Romania
Lyon
Milan
Croatia
Belgrade
Београд



- What exactly is Microsoft Sentinel?
- What are the risks and threats we face with Microsoft 365?
- What is a SIEM? What is SOAR? XDR? And why should I care?
- How do I get started with Microsoft Sentinel?
- What’s beyond the next-next-finish?
- This is all free, right?



Joanne C Klein ☁️👩‍💻

@JoanneCKlein

Does your org export Office 365 audit log data and ingest them to a SIEM?

Yes	36.9%
No	**38.5%**
Don’t know	6.2%
What’s a SIEM?	18.5%

65 votes · Final results

Acronym Soup 😵

SIEM: Security Information and Event Management

SOAR:

Security Orchestration, Automation and Response

EDR: Endpoint Detection and Response

XDR: Extended Detection and Response

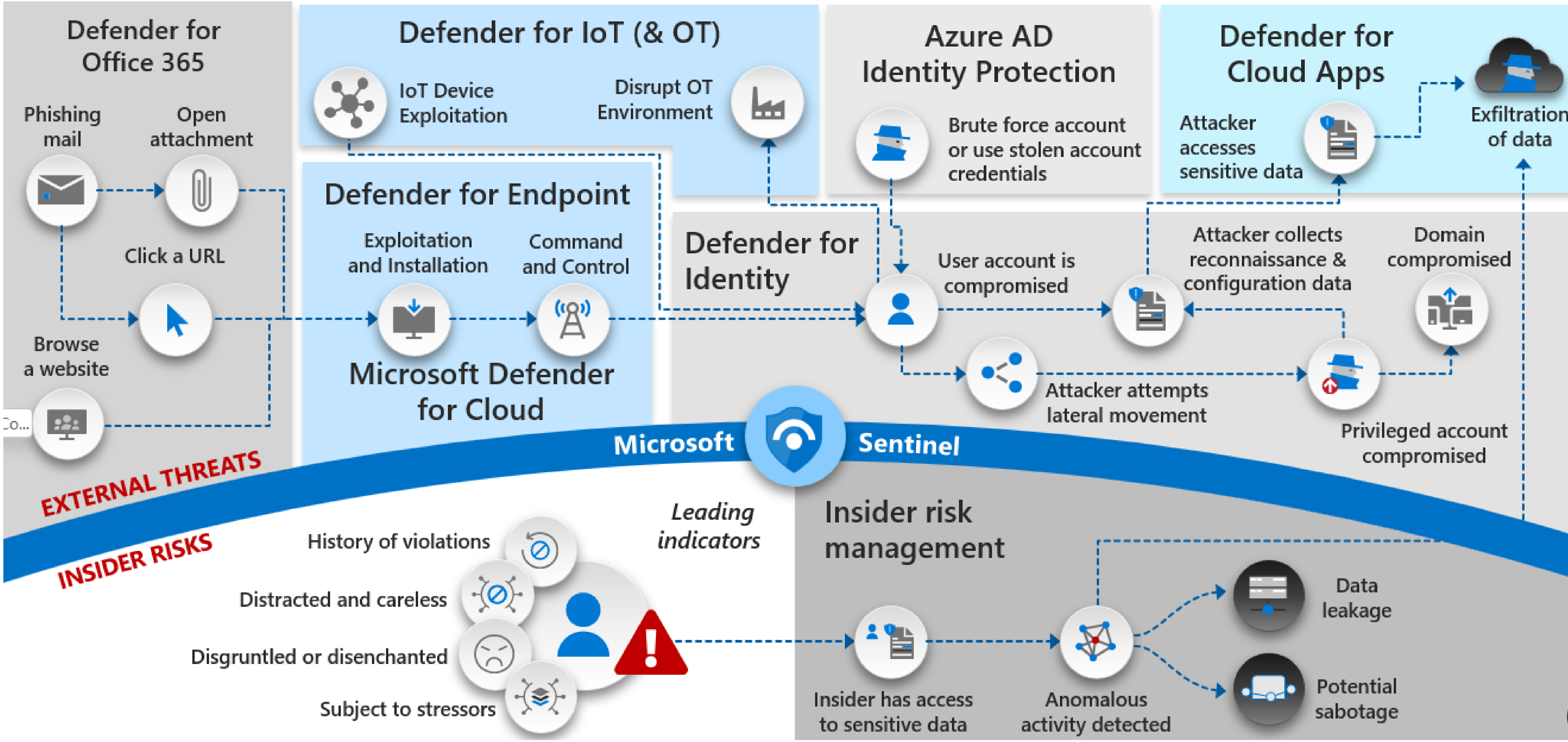
Microsoft 365 Threat landscape

- Compromised or malicious users/apps/endpoints
- Phishing, ransomware, malware
- Social engineering, confidential information leaks

Defend across attack chains

Insider and external threats

Microsoft December 2021 – https://aka.ms/MCRA



Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Co...

Defender for IoT (& OT)

IoT Device Exploitation

Disrupt OT Environment

Defender for Endpoint

Exploitation and Installation

Command and Control

Microsoft Defender for Cloud

Azure AD Identity Protection

Brute force account or use stolen account credentials

Defender for Identity

User account is compromised

Attacker attempts lateral movement

Attacker collects reconnaissance & configuration data

Domain compromised

Privileged account compromised

Defender for Cloud Apps

Attacker accesses sensitive data

Exfiltration of data

EXTERNAL THREATS

Microsoft Sentinel

INSIDER RISKS

Leading indicators

History of violations

Distracted and careless

Disgruntled or disenchanted

Subject to stressors

Insider risk management

Insider has access to sensitive data

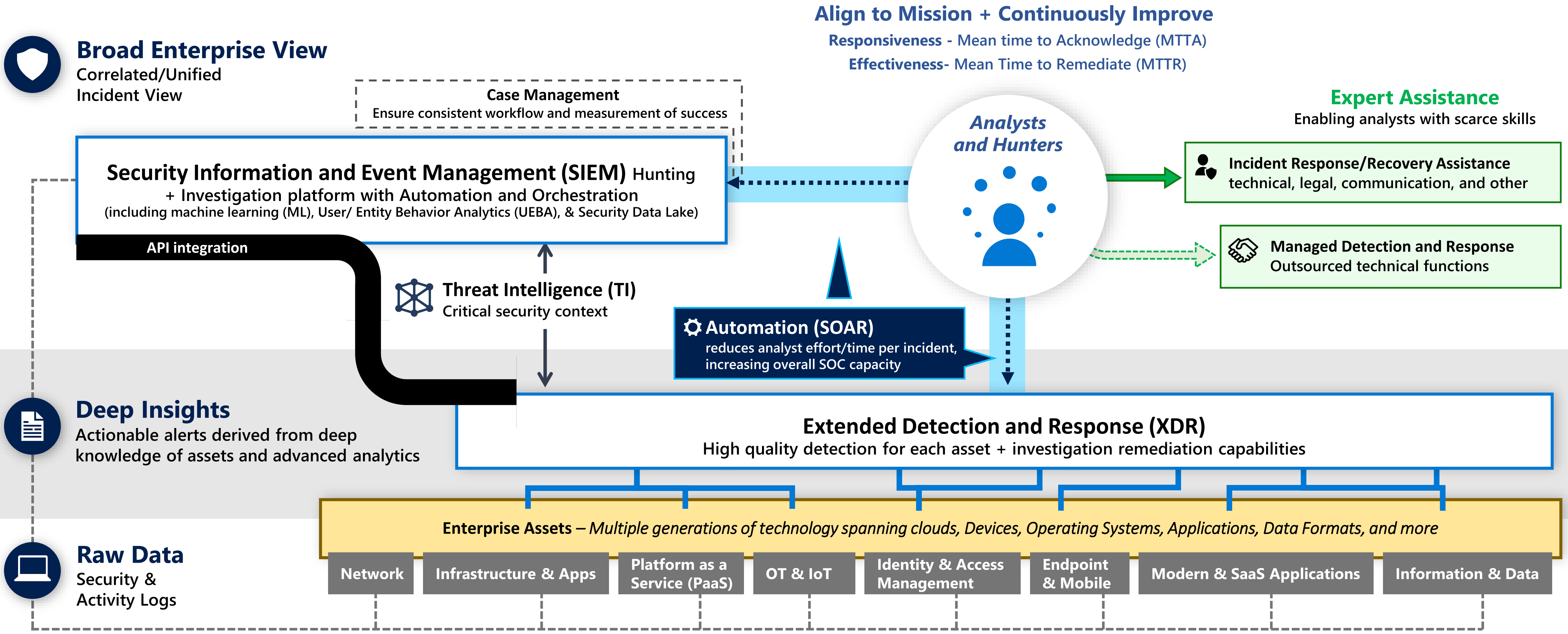
Anomalous activity detected

Data leakage

Potential sabotage

Modern Security Operations

People-Centric function focused on quality, responsiveness, and rapid remediation



Align to Mission + Continuously Improve

Responsiveness - Mean time to Acknowledge (MTTA)

Effectiveness- Mean Time to Remediate (MTTR)

Broad Enterprise View
Correlated/Unified
Incident View

Case Management
Ensure consistent workflow and measurement of success

Security Information and Event Management (SIEM) Hunting + Investigation platform with Automation and Orchestration (including machine learning (ML), User/ Entity Behavior Analytics (UEBA), & Security Data Lake)

API integration

Threat Intelligence (TI)
Critical security context

Analysts and Hunters

Expert Assistance
Enabling analysts with scarce skills

Incident Response/Recovery Assistance
technical, legal, communication, and other

Managed Detection and Response
Outsourced technical functions

Automation (SOAR)
reduces analyst effort/time per incident, increasing overall SOC capacity

Deep Insights
Actionable alerts derived from deep knowledge of assets and advanced analytics

Extended Detection and Response (XDR)
High quality detection for each asset + investigation remediation capabilities

Enterprise Assets – *Multiple generations of technology spanning clouds, Devices, Operating Systems, Applications, Data Formats, and more*

Raw Data
Security &
Activity Logs

Network

Infrastructure & Apps

Platform as a Service (PaaS)

OT & IoT

Identity & Access Management

Endpoint & Mobile

Modern & SaaS Applications

Information & Data

What is Microsoft Sentinel

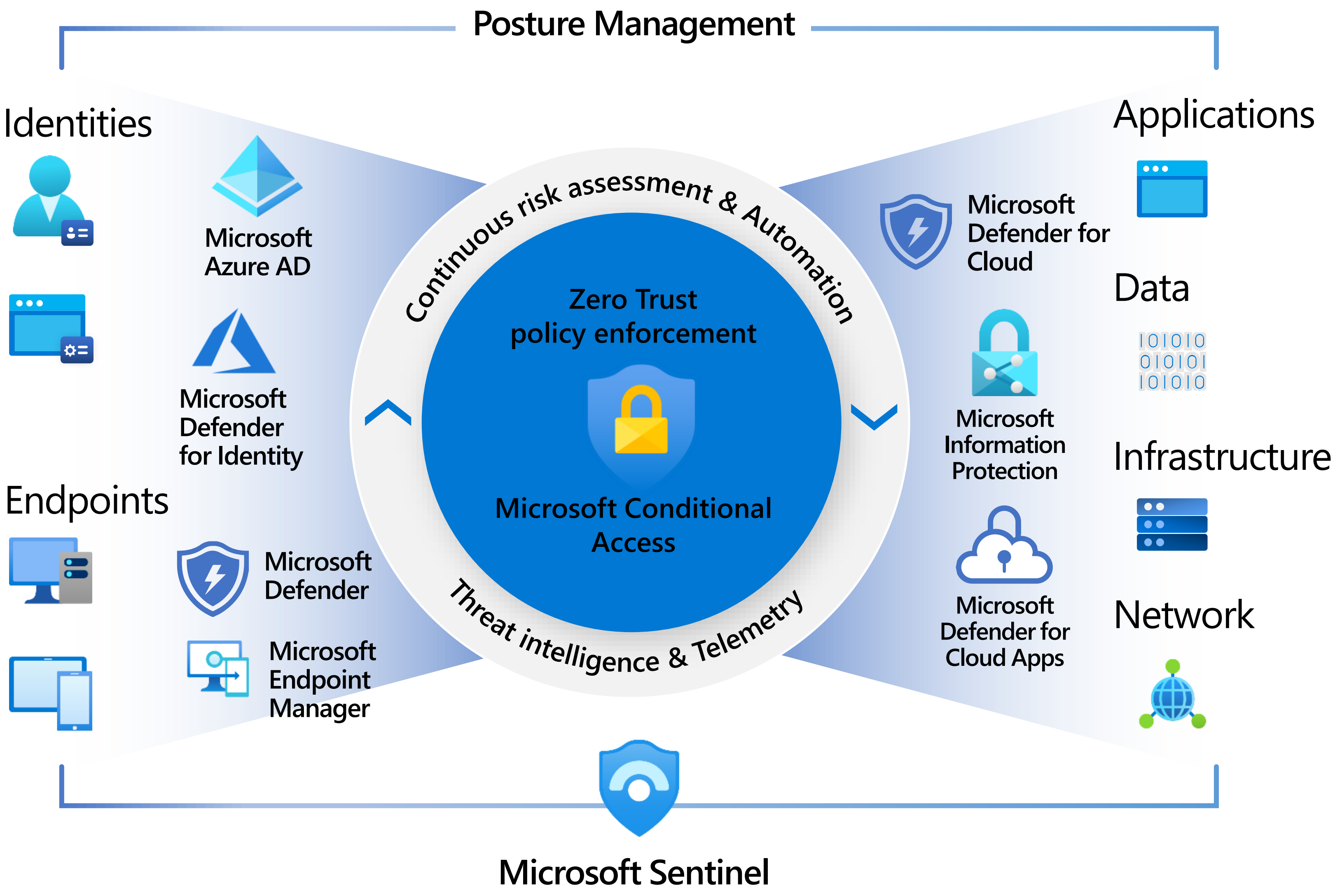
Single pane of glass for all security insights and response

Based on Log Analytics Workspace

Microsoft Sentinel components & capabilities

Data connectors

- Analytics rules
- Workbooks
- Incidents and alerts
- Threat hunting and intelligence
- Response automation



Posture Management

Identities

Microsoft Azure AD

Microsoft Defender for Identity

Endpoints

Microsoft Defender

Microsoft Endpoint Manager

Continuous risk assessment & Automation

Zero Trust policy enforcement

Microsoft Conditional Access

Threat intelligence & Telemetry

Microsoft Defender for Cloud

Microsoft Information Protection

Microsoft Defender for Cloud Apps

Applications

Data

Infrastructure

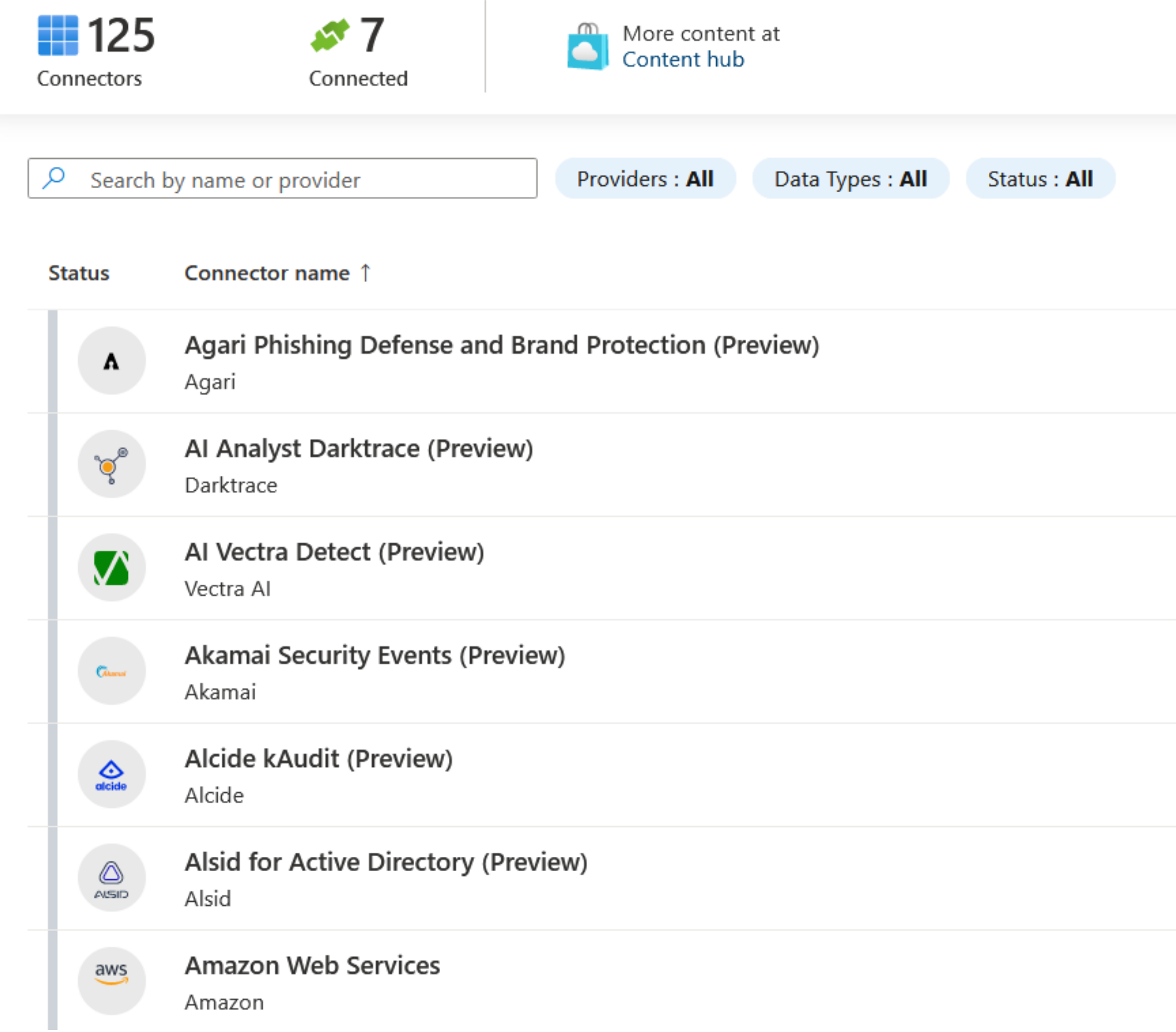
Network

Microsoft Sentinel

Data connectors

Gather logs from everywhere

- Analytics rules
- Hunting queries
- Parsers
- Workbooks
- Playbooks



125 Connectors

7 Connected

More content at Content hub

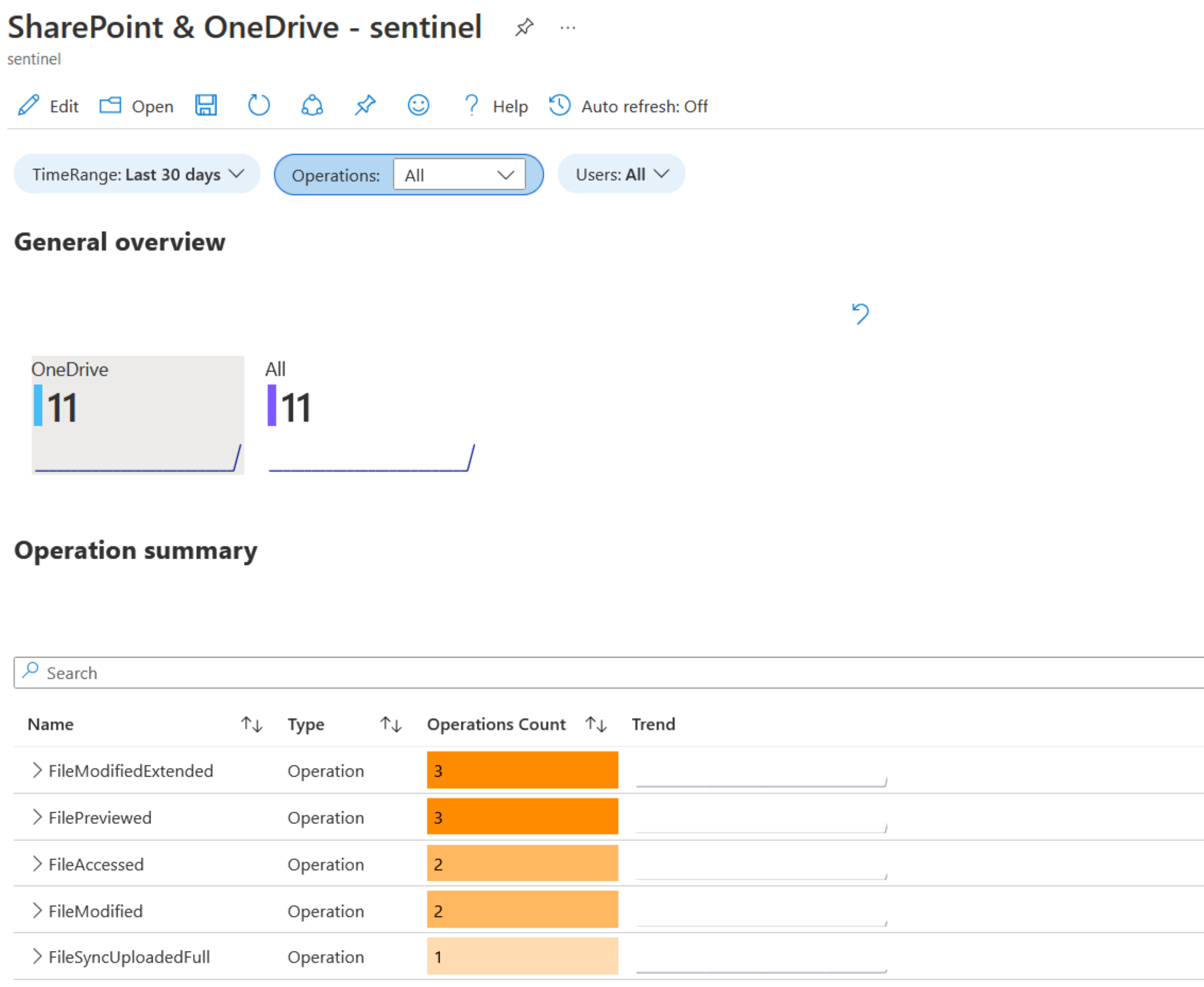
Search by name or provider

Providers : **All** Data Types : **All** Status : **All**

Status	Connector name ↑
	Agari Phishing Defense and Brand Protection (Preview) Agari
	AI Analyst Darktrace (Preview) Darktrace
	AI Vectra Detect (Preview) Vectra AI
	Akamai Security Events (Preview) Akamai
	Alcide kAudit (Preview) Alcide
	Alsid for Active Directory (Preview) Alsid
	Amazon Web Services Amazon

Workbooks

- Customizable reports & insights
- Templates or create your own
- Content hub (Preview)
- Based on KQL



SharePoint & OneDrive - sentinel

sentinel

TimeRange: Last 30 days

Operations: All

Users: All

General overview

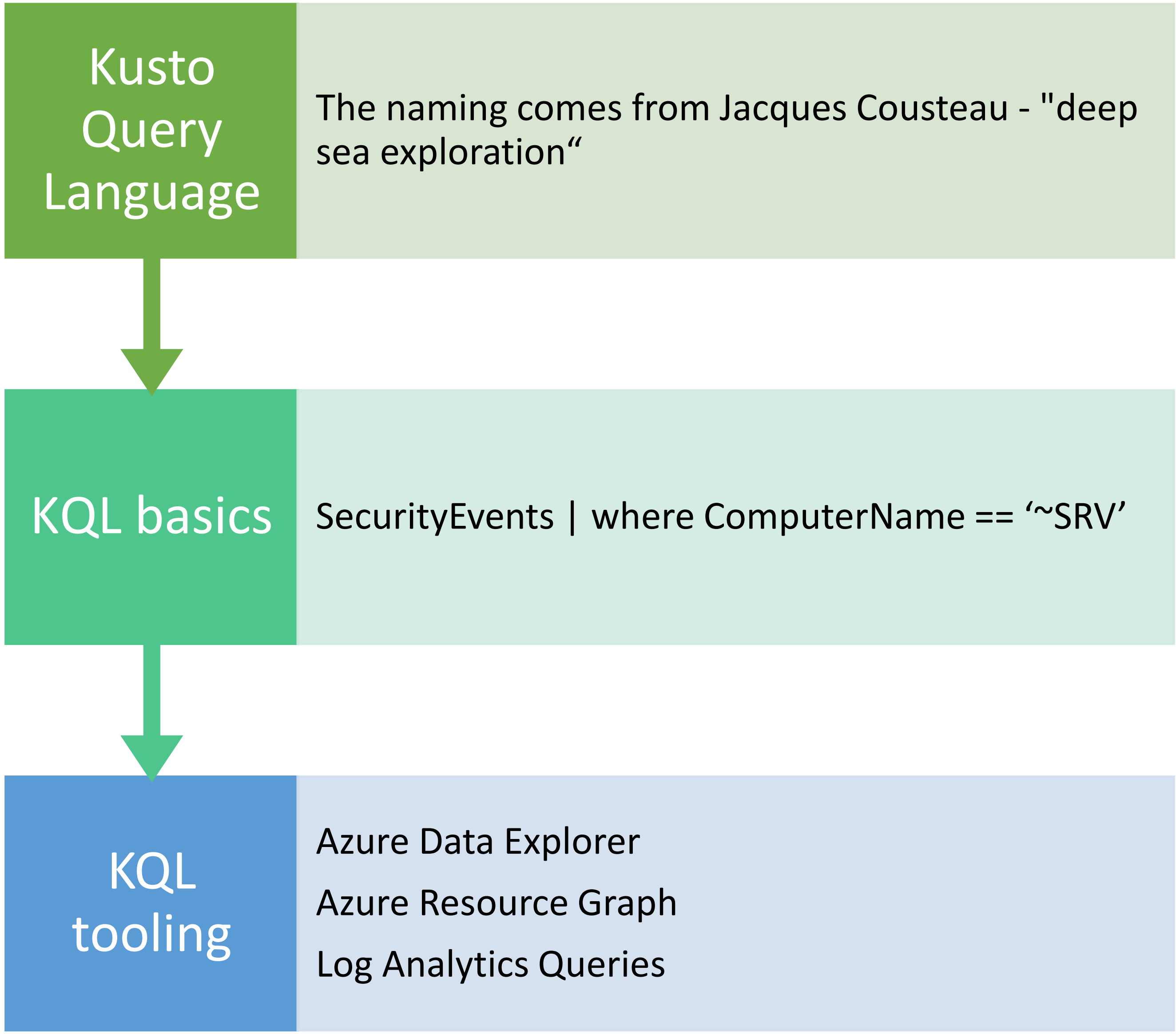
OneDrive 11

All 11

Operation summary

Name	Type	Operations Count	Trend
FileModifiedExtended	Operation	3	
FilePreviewed	Operation	3	
FileAccessed	Operation	2	
FileModified	Operation	2	
FileSyncUploadedFull	Operation	1	

KQL?



Kusto Query Language

The naming comes from Jacques Cousteau - "deep sea exploration“

KQL basics

SecurityEvents | where ComputerName == ‘~SRV’

KQL tooling

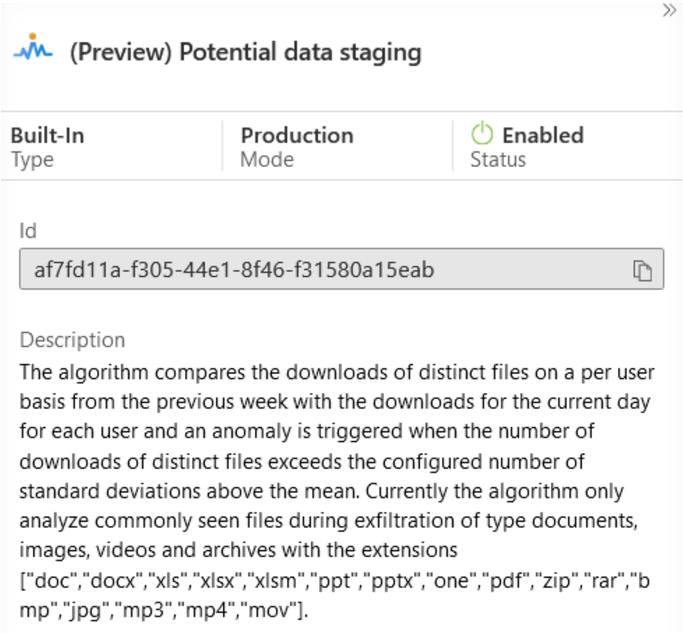
Azure Data Explorer

Azure Resource Graph

Log Analytics Queries

Analytics rules

- Threat detection
- Anomaly detection
- Incident creation



(Preview) Potential data staging

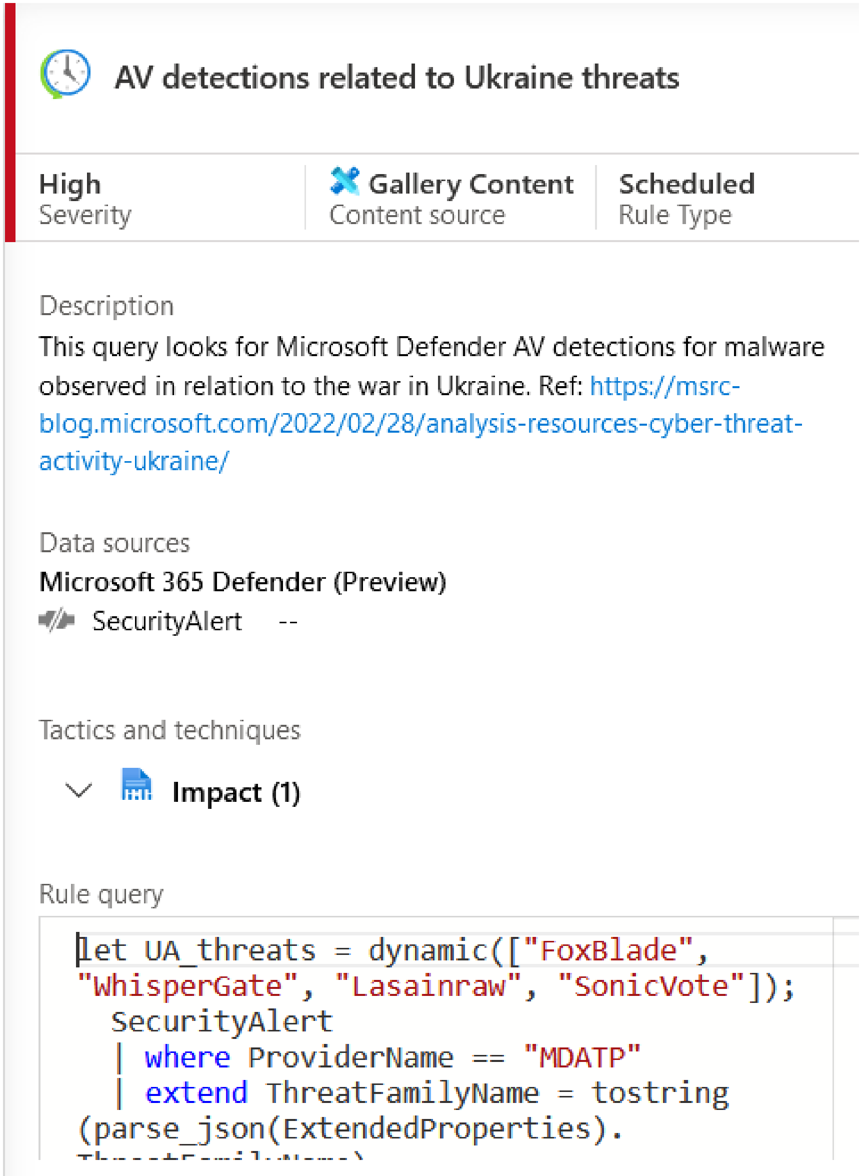
Built-In
Type

Production
Mode

Enabled
Status

Id
af7fd11a-f305-44e1-8f46-f31580a15eab

Description
The algorithm compares the downloads of distinct files on a per user basis from the previous week with the downloads for the current day for each user and an anomaly is triggered when the number of downloads of distinct files exceeds the configured number of standard deviations above the mean. Currently the algorithm only analyze commonly seen files during exfiltration of type documents, images, videos and archives with the extensions ["doc","docx","xls","xlsx","xlsm","ppt","pptx","one","pdf","zip","rar","bmp","jpg","mp3","mp4","mov"].



AV detections related to Ukraine threats

High
Severity

Gallery Content
Content source

Scheduled
Rule Type

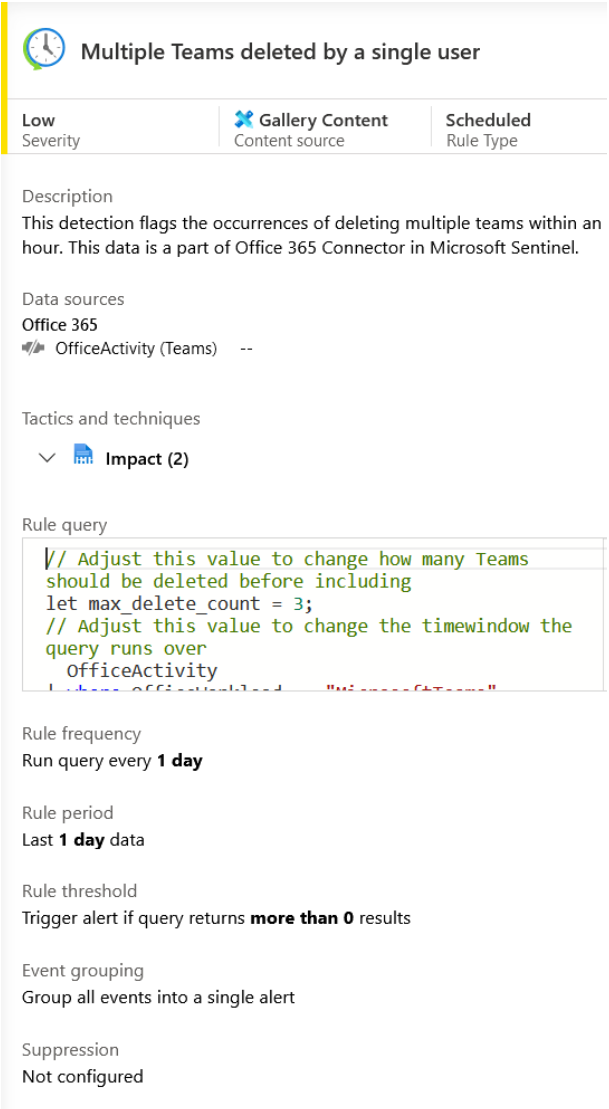
Description
This query looks for Microsoft Defender AV detections for malware observed in relation to the war in Ukraine. Ref: https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/

Data sources
Microsoft 365 Defender (Preview)
SecurityAlert --

Tactics and techniques
Impact (1)

Rule query

```
let UA_threats = dynamic(["FoxBlade",
"WhisperGate", "Lasainraw", "SonicVote"]);
  SecurityAlert
  | where ProviderName == "MDATP"
  | extend ThreatFamilyName = tostring
(parse_json(ExtendedProperties).
```



Multiple Teams deleted by a single user

Low
Severity

Gallery Content
Content source

Scheduled
Rule Type

Description
This detection flags the occurrences of deleting multiple teams within an hour. This data is a part of Office 365 Connector in Microsoft Sentinel.

Data sources
Office 365
OfficeActivity (Teams) --

Tactics and techniques
Impact (2)

Rule query

```
// Adjust this value to change how many Teams
should be deleted before including
let max_delete_count = 3;
// Adjust this value to change the timewindow the
query runs over
  OfficeActivity
```

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

Demo

Deploying and Configuring Microsoft Sentinel

Security Operations

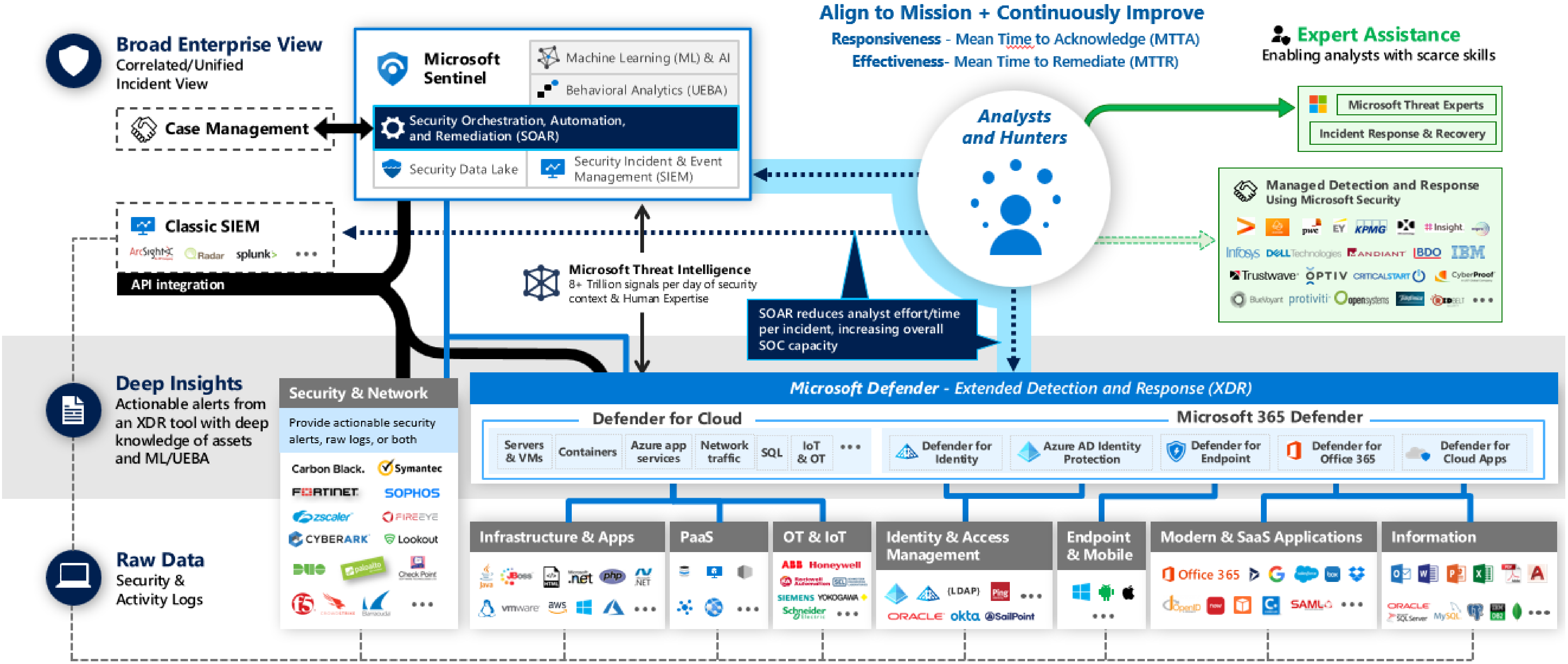
Microsoft Reference Architecture

Legend

- - - Event Log Based Monitoring
▪▪▪▪ Investigation & Proactive Hunting
⇢ Outsourcing
➡ Consulting and Escalation
▬ Native Resource Monitoring

Microsoft

December 2021 – https://aka.ms/MCRA



Broad Enterprise View
Correlated/Unified Incident View

Case Management

Microsoft Sentinel

- Machine Learning (ML) & AI
- Behavioral Analytics (UEBA)
- Security Orchestration, Automation, and Remediation (SOAR)
- Security Data Lake
- Security Incident & Event Management (SIEM)

Classic SIEM
ArcSight · QRadar · splunk> • • •

API integration

Microsoft Threat Intelligence
8+ Trillion signals per day of security context & Human Expertise

Align to Mission + Continuously Improve
Responsiveness - Mean Time to Acknowledge (MTTA)
Effectiveness- Mean Time to Remediate (MTTR)

Analysts and Hunters

SOAR reduces analyst effort/time per incident, increasing overall SOC capacity

Expert Assistance
Enabling analysts with scarce skills

- Microsoft Threat Experts
- Incident Response & Recovery

Managed Detection and Response Using Microsoft Security
pwc · EY · KPMG · Insight · Infosys · DELL Technologies · MANDIANT · BDO · IBM · Trustwave · OPTIV · CRITICALSTART · CyberProof · BlueVoyant · protiviti · opensystems • • •

Deep Insights
Actionable alerts from an XDR tool with deep knowledge of assets and ML/UEBA

Security & Network
Provide actionable security alerts, raw logs, or both
Carbon Black. · Symantec · FORTINET · SOPHOS · zscaler · FIREEYE · CYBERARK · Lookout · DUO · paloalto · Check Point · CrowdStrike · Barracuda • • •

Microsoft Defender - Extended Detection and Response (XDR)

Defender for Cloud: Servers & VMs · Containers · Azure app services · Network traffic · SQL · IoT & OT • • •

Microsoft 365 Defender: Defender for Identity · Azure AD Identity Protection · Defender for Endpoint · Defender for Office 365 · Defender for Cloud Apps

Raw Data
Security & Activity Logs

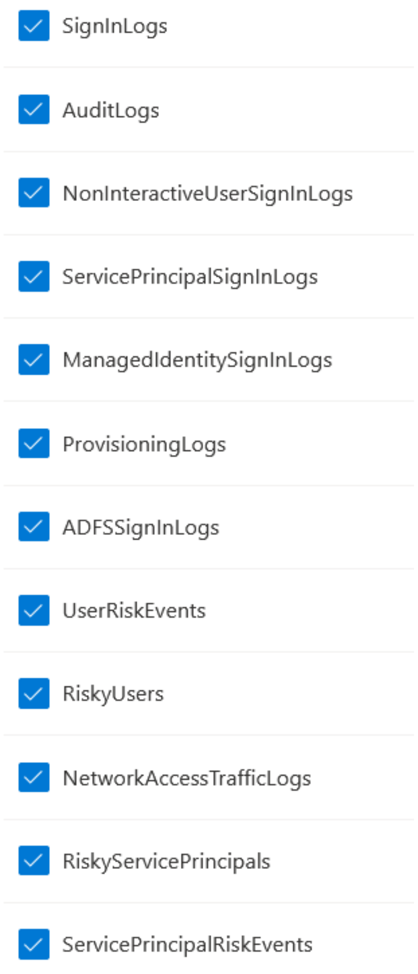
- Infrastructure & Apps: Java · JBoss · HTML · .net · php · .NET · vmware · aws • • •
- PaaS • • •
- OT & IoT: ABB · Honeywell · Rockwell Automation · SEL · SIEMENS · YOKOGAWA · Schneider Electric • • •
- Identity & Access Management: (LDAP) · Ping · ORACLE · okta · SailPoint • • •
- Endpoint & Mobile • • •
- Modern & SaaS Applications: Office 365 · salesforce · box · OpenID · SAML • • •
- Information: ORACLE · SQL Server · MySQL · DB2 • • •

Connecting to Microsoft 365

The bare minimum you need

Azure Active Directory
audit & sign-in logs

Office 365
user activities



☑ SignInLogs

☑ AuditLogs

☑ NonInteractiveUserSignInLogs

☑ ServicePrincipalSignInLogs

☑ ManagedIdentitySignInLogs

☑ ProvisioningLogs

☑ ADFSSignInLogs

☑ UserRiskEvents

☑ RiskyUsers

☑ NetworkAccessTrafficLogs

☑ RiskyServicePrincipals

☑ ServicePrincipalRiskEvents

Example: AAD SignInLog

Additional connectors

Microsoft 365 Defender

- MS Defender for Office 365
- MS Defender for Identity
- MS Defender for EndPoint
- MS Defender for Cloud Apps
- Azure Active Directory Identity Protection

Microsoft Defender for Cloud

MS Purview Insider Risk Management

MS Power BI

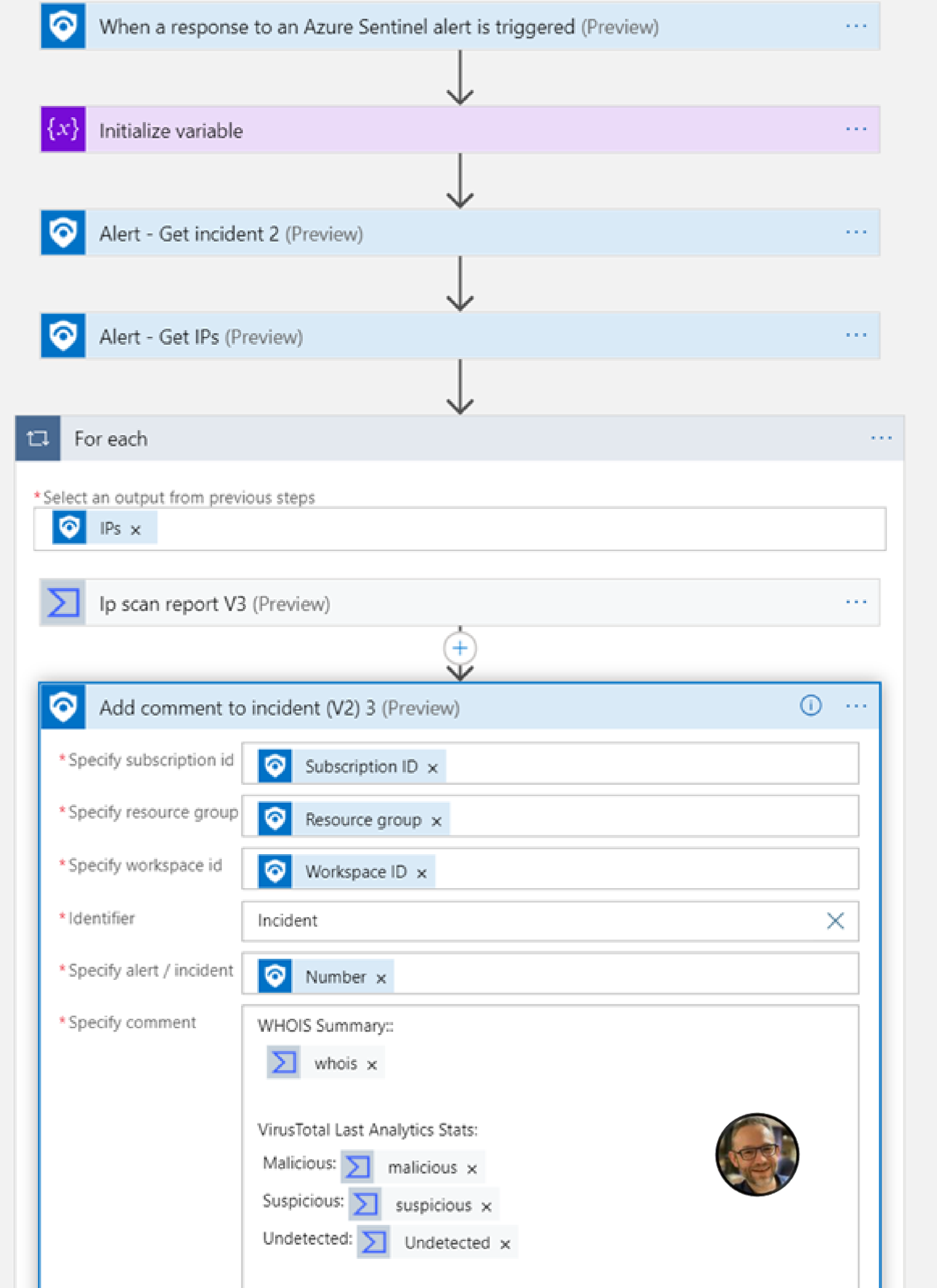
MS Project

Demo

Monitoring Microsoft 365 with Sentinel

Playbooks & Automation Rules

- Automate responses
- Azure Logic Apps
    - Connect with other services



When a response to an Azure Sentinel alert is triggered (Preview)

Initialize variable

Alert - Get incident 2 (Preview)

Alert - Get IPs (Preview)

For each

* Select an output from previous steps: IPs ×

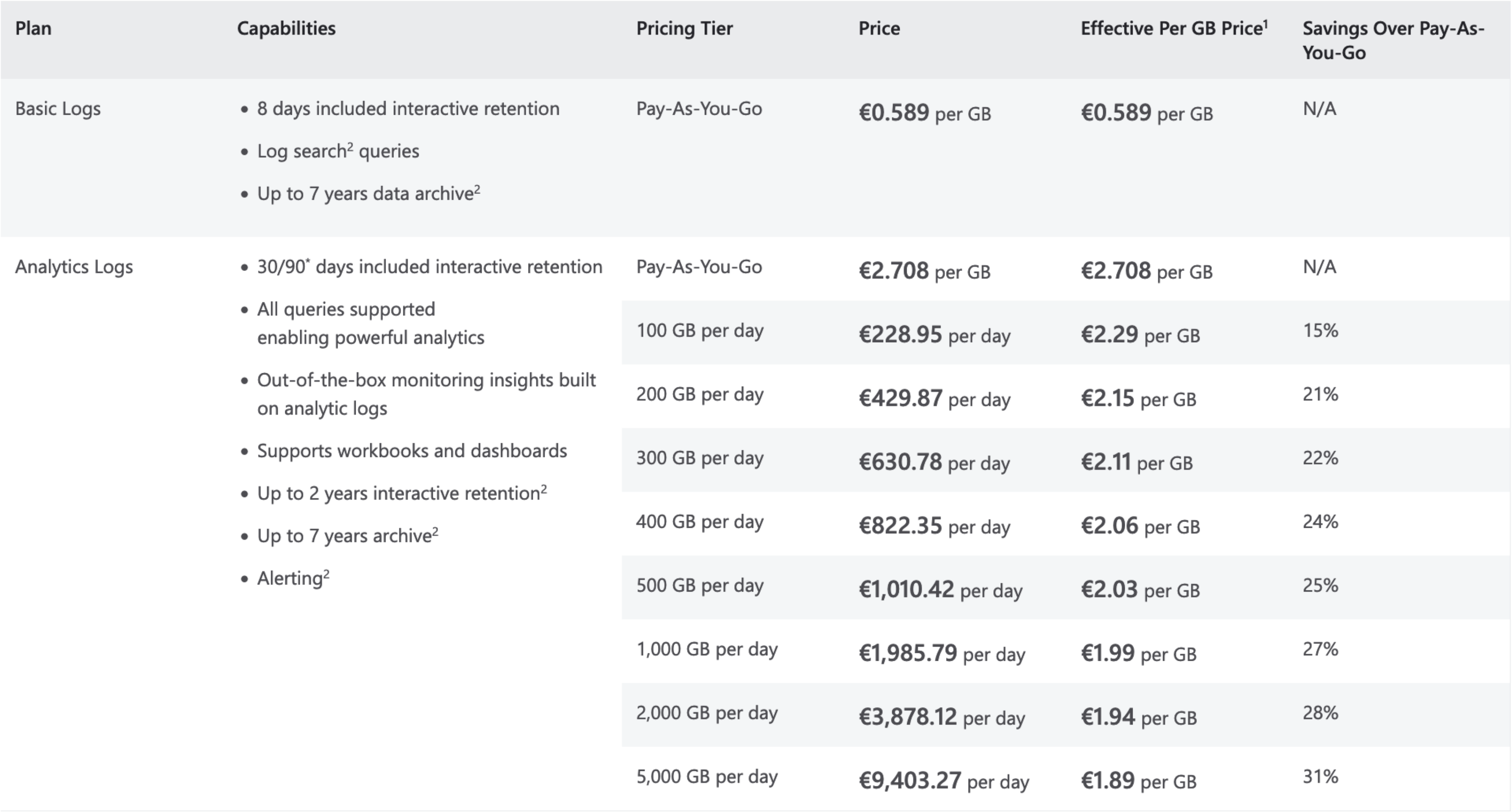
Ip scan report V3 (Preview)

Add comment to incident (V2) 3 (Preview)

* Specify subscription id	Subscription ID ×
* Specify resource group	Resource group ×
* Specify workspace id	Workspace ID ×
* Identifier	Incident
* Specify alert / incident	Number ×
* Specify comment	WHOIS Summary:: whois × VirusTotal Last Analytics Stats: Malicious: malicious × Suspicious: suspicious × Undetected: Undetected ×

Cost estimation and cost management

- Pricing based on Log Analytics Workspace (per GB) and Sentinel (per GB ingested)
  - 31-day trial is available with 10 GB/day of log data
- Costs are mainly dependent on data volume - Pay-As-You-Go or through a commitment tier



Plan	Capabilities	Pricing Tier	Price	Effective Per GB Price[1]	Savings Over Pay-As-You-Go
Basic Logs	• 8 days included interactive retention • Log search[2] queries • Up to 7 years data archive[2]	Pay-As-You-Go	**€0.589** per GB	**€0.589** per GB	N/A
Analytics Logs	• 30/90[*] days included interactive retention • All queries supported enabling powerful analytics • Out-of-the-box monitoring insights built on analytic logs • Supports workbooks and dashboards • Up to 2 years interactive retention[2] • Up to 7 years archive[2] • Alerting[2]	Pay-As-You-Go	**€2.708** per GB	**€2.708** per GB	N/A
		100 GB per day	**€228.95** per day	**€2.29** per GB	15%
		200 GB per day	**€429.87** per day	**€2.15** per GB	21%
		300 GB per day	**€630.78** per day	**€2.11** per GB	22%
		400 GB per day	**€822.35** per day	**€2.06** per GB	24%
		500 GB per day	**€1,010.42** per day	**€2.03** per GB	25%
		1,000 GB per day	**€1,985.79** per day	**€1.99** per GB	27%
		2,000 GB per day	**€3,878.12** per day	**€1.94** per GB	28%
		5,000 GB per day	**€9,403.27** per day	**€1.89** per GB	31%

Data retention

Office 365 audit log data:
90 days

Log analytics workspace:
configurable

Which logs should I get?

Analytics logs

- default, most expensive, 730 days retention

Basic logs

- cheaper, but limited to 8 days retention, doesn’t support all queries such as a join, billed per scanned GB

Archive logs

- cheaper, but cannot be queried through KQL

One or multiple Microsoft Sentinels?

Ideally, you'll have one Microsoft Sentinel → one Log Analytics Workspace

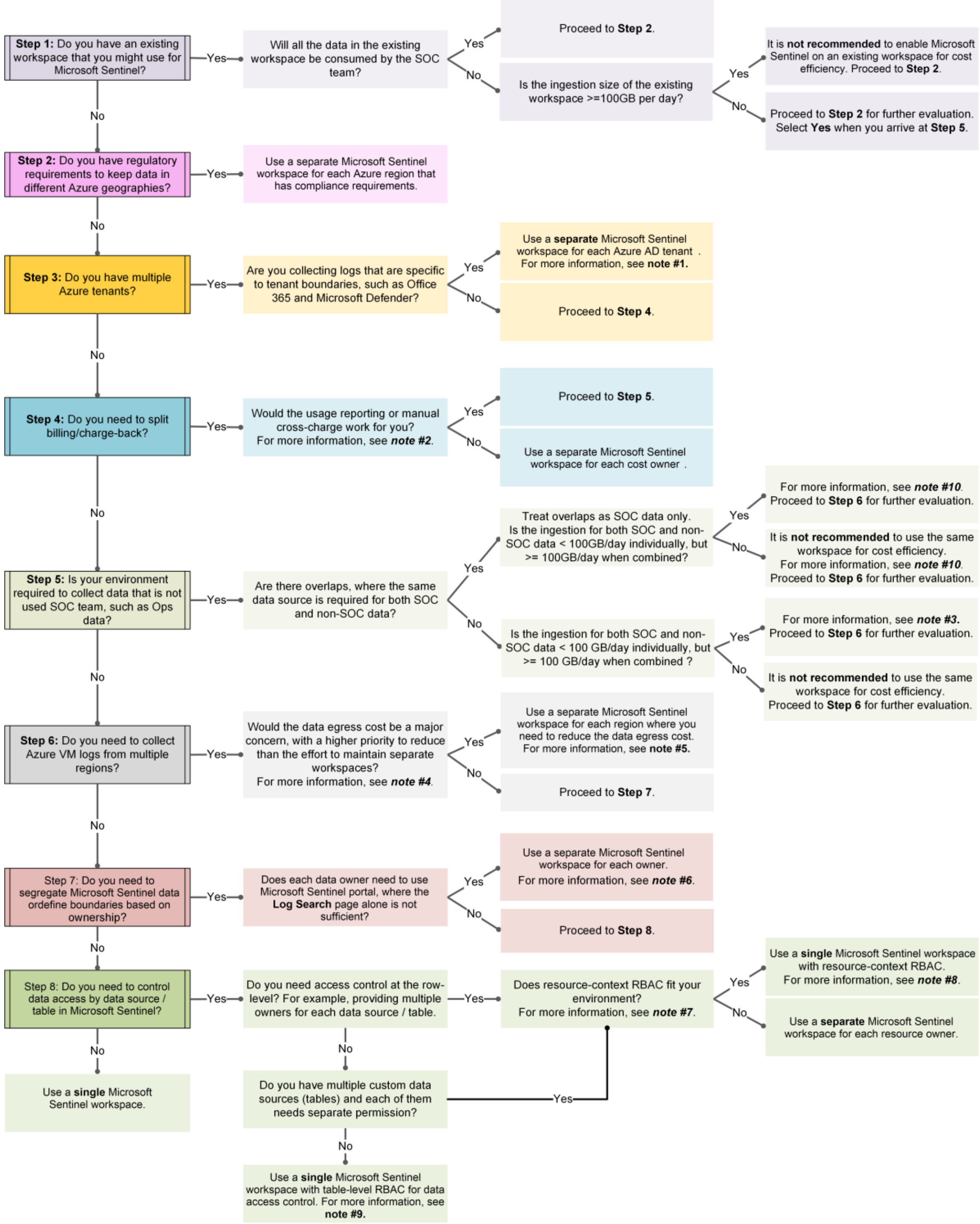
Obvious challenges with this approach in certain architectures

Multiple Sentinels

Regulatory compliance

Customer data

Split billing



Step 1: Do you have an existing workspace that you might use for Microsoft Sentinel?

Yes → Will all the data in the existing workspace be consumed by the SOC team?

- Yes → Proceed to **Step 2**.
- No → Is the ingestion size of the existing workspace >=100GB per day?
  - Yes → It is **not recommended** to enable Microsoft Sentinel on an existing workspace for cost efficiency. Proceed to **Step 2**.
  - No → Proceed to **Step 2** for further evaluation. Select **Yes** when you arrive at **Step 5**.

No ↓

Step 2: Do you have regulatory requirements to keep data in different Azure geographies?

Yes → Use a separate Microsoft Sentinel workspace for each Azure region that has compliance requirements.

No ↓

Step 3: Do you have multiple Azure tenants?

Yes → Are you collecting logs that are specific to tenant boundaries, such as Office 365 and Microsoft Defender?

- Yes → Use a **separate** Microsoft Sentinel workspace for each Azure AD tenant . For more information, see **note #1.**
- No → Proceed to **Step 4**.

No ↓

Step 4: Do you need to split billing/charge-back?

Yes → Would the usage reporting or manual cross-charge work for you? For more information, see ***note #2***.

- Yes → Proceed to **Step 5**.
- No → Use a separate Microsoft Sentinel workspace for each cost owner .

No ↓

Step 5: Is your environment required to collect data that is not used SOC team, such as Ops data?

Yes → Are there overlaps, where the same data source is required for both SOC and non-SOC data?

- Yes → Treat overlaps as SOC data only. Is the ingestion for both SOC and non-SOC data < 100GB/day individually, but >= 100GB/day when combined?
  - Yes → For more information, see ***note #10***. Proceed to **Step 6** for further evaluation.
  - No → It is **not recommended** to use the same workspace for cost efficiency. For more information, see ***note #10***. Proceed to **Step 6** for further evaluation.
- No → Is the ingestion for both SOC and non-SOC data < 100 GB/day individually, but >= 100 GB/day when combined ?
  - Yes → For more information, see ***note #3.*** Proceed to **Step 6** for further evaluation.
  - No → It is **not recommended** to use the same workspace for cost efficiency. Proceed to **Step 6** for further evaluation.

No ↓

Step 6: Do you need to collect Azure VM logs from multiple regions?

Yes → Would the data egress cost be a major concern, with a higher priority to reduce than the effort to maintain separate workspaces? For more information, see ***note #4***.

- Yes → Use a separate Microsoft Sentinel workspace for each region where you need to reduce the data egress cost. For more information, see **note #5.**
- No → Proceed to **Step 7**.

No ↓

Step 7: Do you need to segregate Microsoft Sentinel data ordefine boundaries based on ownership?

Yes → Does each data owner need to use Microsoft Sentinel portal, where the **Log Search** page alone is not sufficient?

- Yes → Use a separate Microsoft Sentinel workspace for each owner. For more information, see ***note #6***.
- No → Proceed to **Step 8**.

No ↓

Step 8: Do you need to control data access by data source / table in Microsoft Sentinel?

Yes → Do you need access control at the row-level? For example, providing multiple owners for each data source / table.

- Yes → Does resource-context RBAC fit your environment? For more information, see ***note #7***.
  - Yes → Use a **single** Microsoft Sentinel workspace with resource-context RBAC. For more information, see ***note #8***.
  - No → Use a **separate** Microsoft Sentinel workspace for each resource owner.
- No → Do you have multiple custom data sources (tables) and each of them needs separate permission?
  - Yes → Does resource-context RBAC fit your environment?
  - No → Use a **single** Microsoft Sentinel workspace with table-level RBAC for data access control. For more information, see **note #9.**

No → Use a **single** Microsoft Sentinel workspace.

What about Defender for Cloud?

Defender for Cloud is the old Azure Security Center

Alert synchronization

Bi-directional alert synchronization

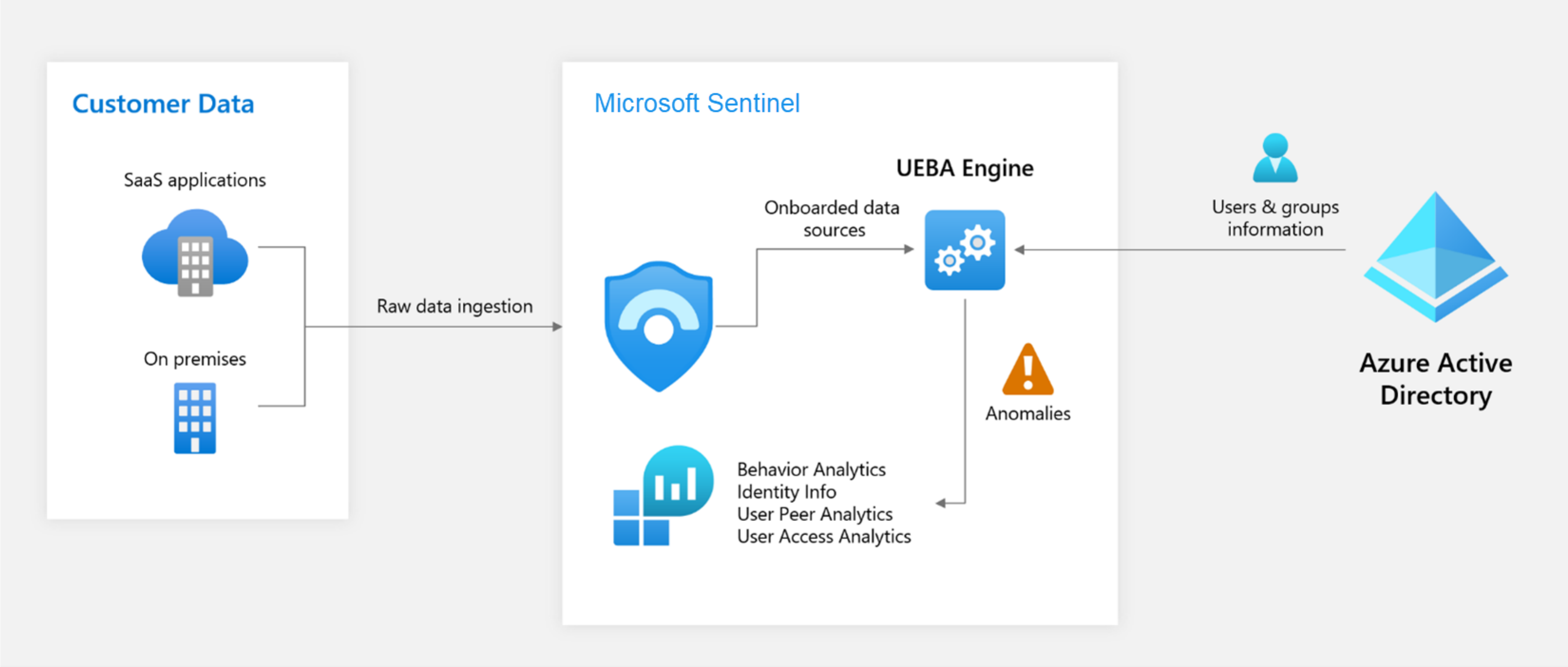
Do I need to use Data Collection Rules?

Filtering your logs before ingestion

Useful for optimizing cost – based on KQL

Creation via Azure Monitor

Can transform data also

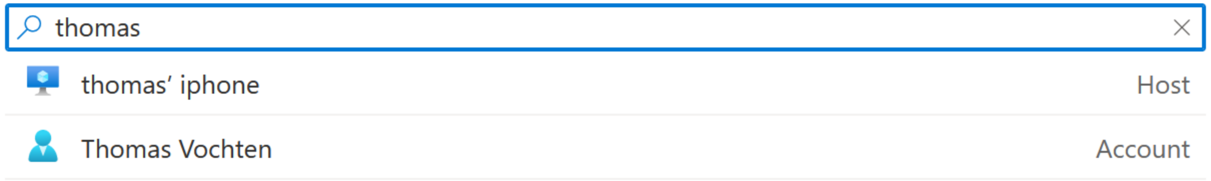


A few thoughts on UEBA

User Entity Behavior Analytics

Builds behavioral profiles of users, hosts, IP addresses and applications

A few thoughts on UEBA

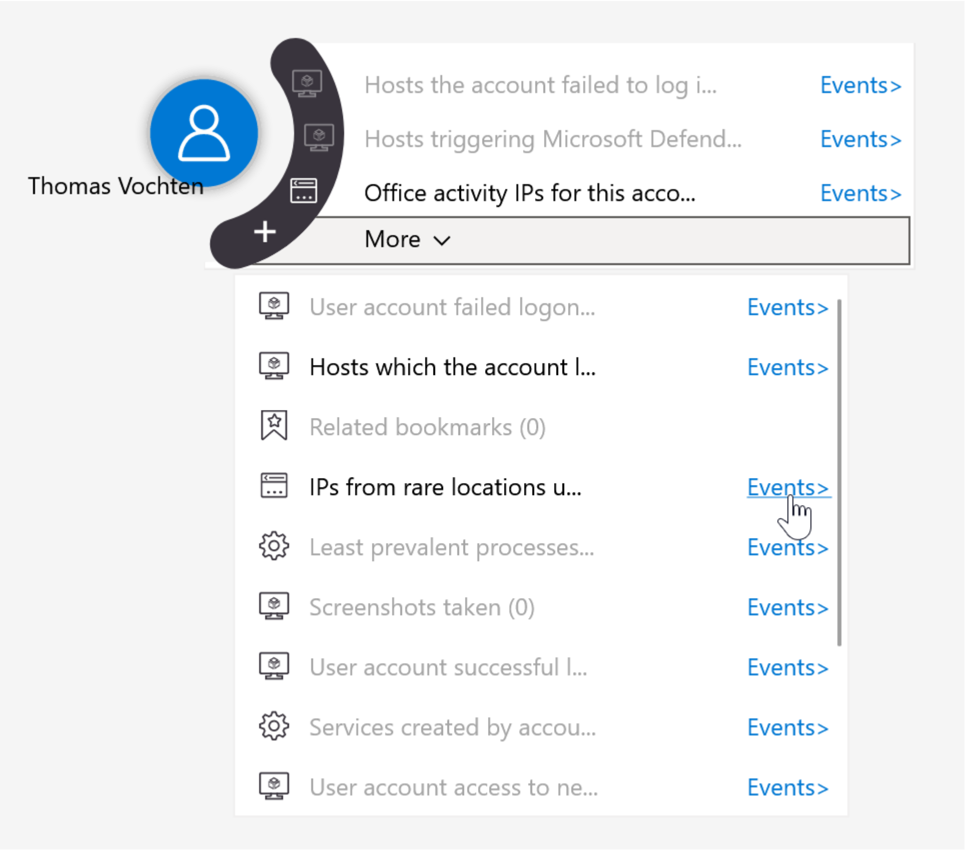


thomas

thomas' iphone Host

Thomas Vochten Account

A few thoughts on UEBA



Thomas Vochten

Hosts the account failed to log i... Events>

Hosts triggering Microsoft Defend... Events>

Office activity IPs for this acco... Events>

More

User account failed logon... Events>

Hosts which the account l... Events>

Related bookmarks (0)

IPs from rare locations u... Events>

Least prevalent processes... Events>

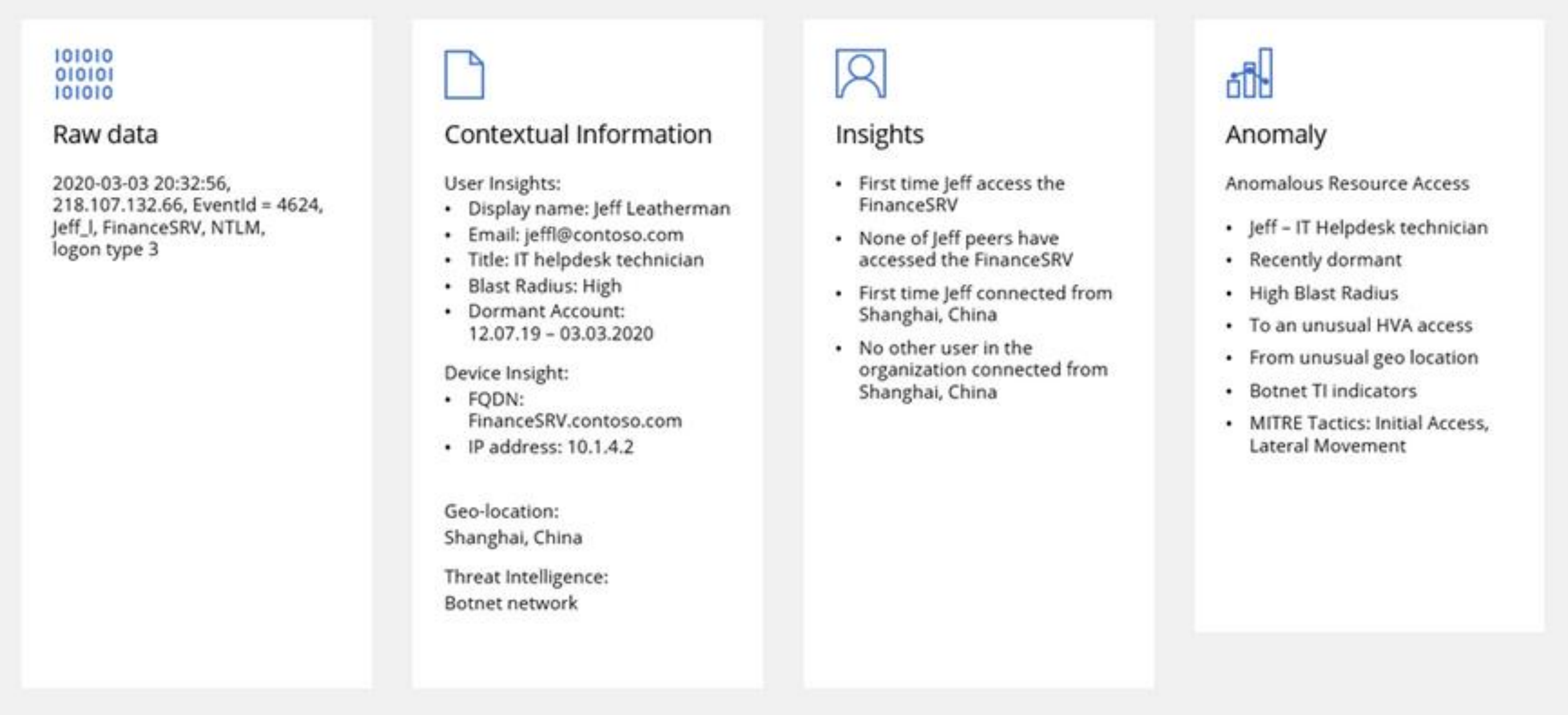
Screenshots taken (0) Events>

User account successful l... Events>

Services created by accou... Events>

User account access to ne... Events>

A few thoughts on UEBA



Raw data

2020-03-03 20:32:56, 218.107.132.66, EventId = 4624, Jeff_l, FinanceSRV, NTLM, logon type 3

Contextual Information

User Insights:

- Display name: Jeff Leatherman
- Email: jeffl@contoso.com
- Title: IT helpdesk technician
- Blast Radius: High
- Dormant Account: 12.07.19 – 03.03.2020

Device Insight:

- FQDN: FinanceSRV.contoso.com
- IP address: 10.1.4.2

Geo-location:
Shanghai, China

Threat Intelligence:
Botnet network

Insights

- First time Jeff access the FinanceSRV
- None of Jeff peers have accessed the FinanceSRV
- First time Jeff connected from Shanghai, China
- No other user in the organization connected from Shanghai, China

Anomaly

Anomalous Resource Access

- Jeff – IT Helpdesk technician
- Recently dormant
- High Blast Radius
- To an unusual HVA access
- From unusual geo location
- Botnet TI indicators
- MITRE Tactics: Initial Access, Lateral Movement

Demo

Log analytics configuration & Defender for Cloud incidents

Call to Action + resources

Plan & deploy Sentinel

Carefully configure connectors & analytics rules

Ingest only what needed – build over time

Thank You

@jussiroine
@thomasvochten