



Maximize Your Security with Sentinel and Security Copilot

Anders Kristiansen
Lead Security @ Devoteam M Cloud

Who am I



Father



Gamer



Disc golfer (Frisbee)



Working as consultant for 15 years



Microsoft Security User group organizer



Microsoft MVP Security



Anders Kristiansen

**Principal
Security Lead**



Microsoft®
Most Valuable
Professional

Sentinel and Security Copilot

Mission briefing:

This presentation will provide you **insight and tips** so you can start utilize and add value using Sentinel and Copilot for Security in your organization.



+



=



Major Incident =

**USD
4.88M**

The global average cost of a data breach in 2024—a 10% increase over last year and the highest total ever.



Microsoft Sentinel Landscape

Cloud-native security information and event management (SIEM)

Collect



Visibility

Detect



Analytics



Hunting



Intelligence

Investigate



Incidents

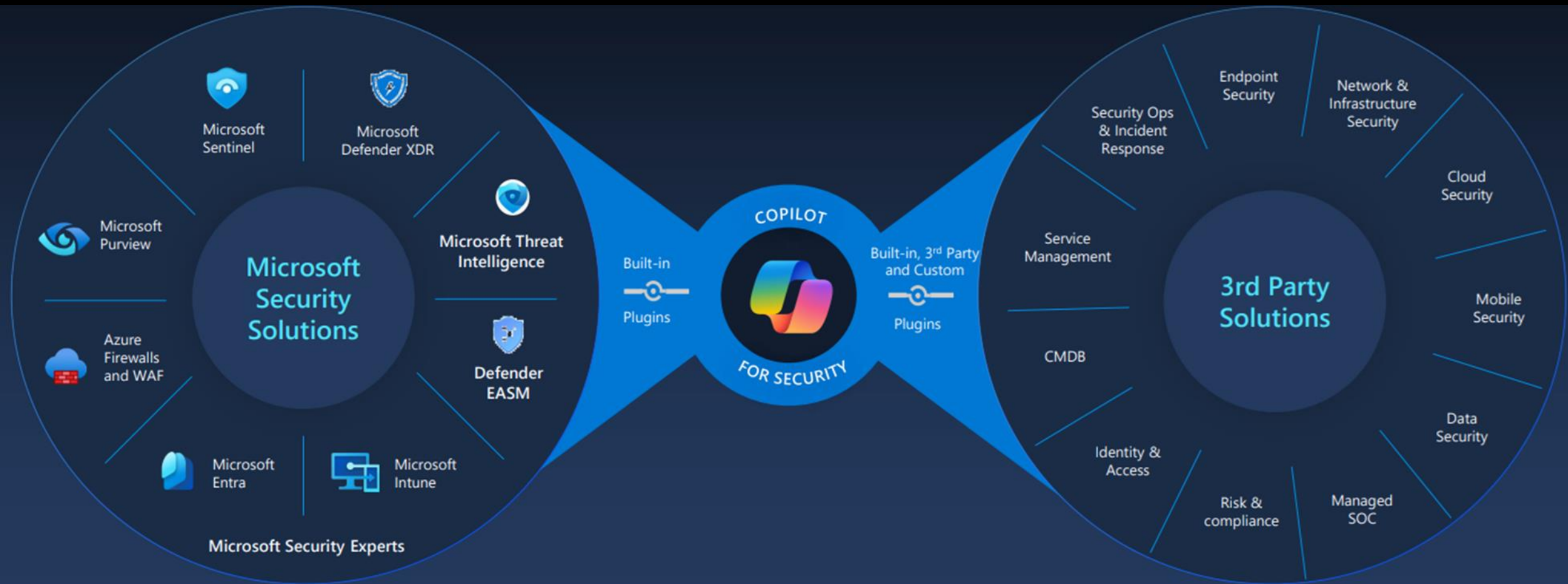
Respond









Automation

« 🔍 Microsoft Security Copilot »»

Copilot for security Landscape



Incident response



					
Governance Lead	Incident Controller	Investigation Lead	Infrastructure Lead	Communications Lead	Regulatory Lead
WHO: CISO/CIO	WHO: ITSM/Security Operations Lead	WHO: Senior IR/Senior IT Operations Rep.	WHO: Senior IT Operations Rep.	WHO: Communications Specialist	WHO: Internal Counsel/ GRC Rep.
WHAT: Operational Oversight	WHAT: Operational Management & Tasking	WHAT: Forensic Investigation	WHAT: Threat Containment	WHAT: Stakeholder Engagement	WHAT: Risk/impact assessment & management of regulatory/legal requirements
WHY: Maintain visibility and understand risk and impact to the wider business, communicate with senior stakeholders	WHY: Coordinate all operational workstreams to understand and contain the threat. Communicate risk to Governance lead	WHY: Understand the compromise overall and communicate the associated risk	WHY: Contain the threat, reduce risk presented by the compromise	WHY: Control messaging externally and internally	WHY: Maintain compliance

A study on cyber resiliency conducted by IBM determined that only 26% of organizations have an incident response plan which is consistently applied.

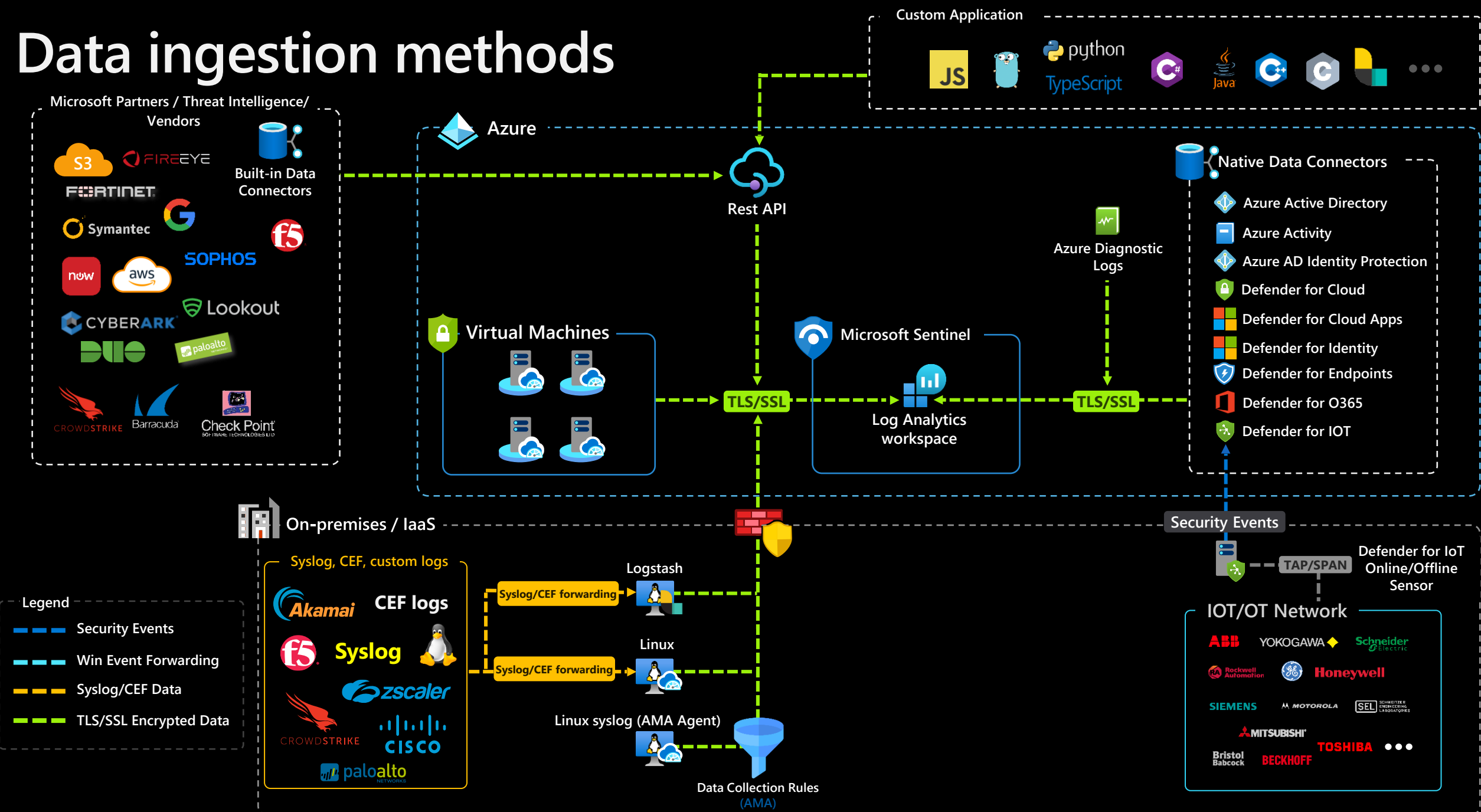
Objective #1

Understanding the capabilities of Microsoft Sentinel and how it can be used to enhance security in your organization

- Architecture is key to understand.
- Fast deployment
- How incidents is created.
- Start small and expand
- XDR portal integration give you a single pane of glass view

<input type="checkbox"/>		SecurityInsights(t-stacks-log)	Solution
<input type="checkbox"/>		t-stacks-log	Log Analytics workspace

Data ingestion methods



Objective #2

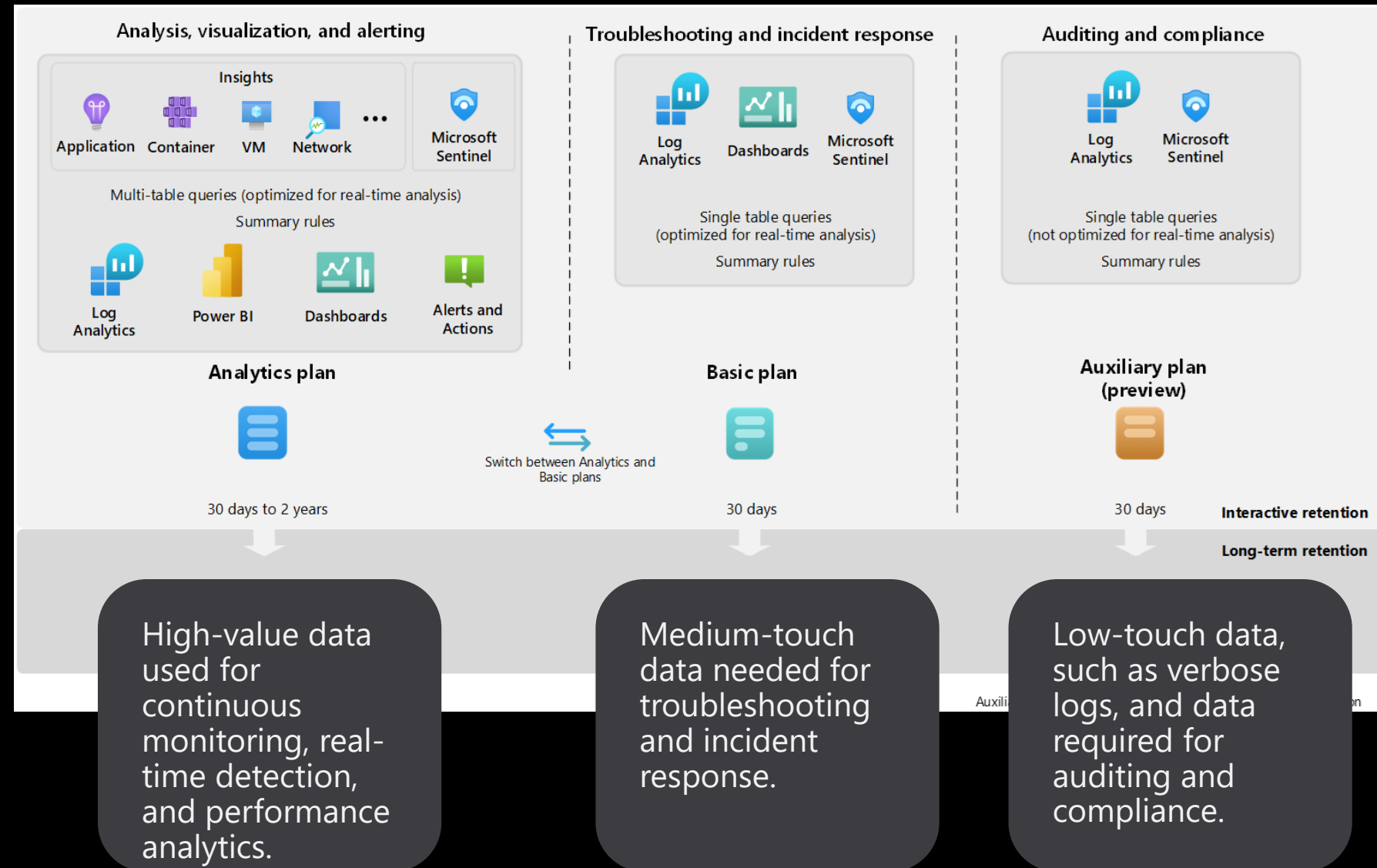
Learning from real-world examples and demos to see how Sentinel can be effectively implemented

- Logs is still essential for detection, categorize your logs
- Start with analyzing your most critical assets and scenarios
- Cost control



Log planning

- **Categorize logs:**
Primary Security
Secondary Security
- Filter logs before reaching target (DCR).



Objective #3

Maximizing value of your Sentinel deployment with Copilot for Security

Scale – Catch what others miss

Speed – Outpace adversaries

Skilling – Skilling and strengthen team expertise

Copilot access model

Deployment – What's needed to spin up copilot for security

Usage – What roles is needed to use? Defaults roles

Sentinel specifics – Microsoft Sentinel Reader required

Primary use cases in Copilot

Incident summary – Assistant in IR reporting and communication

Reverse Engineering – Speeds up investigation and complex scripts, etc

Guided assistance – Give hints and guide you towards similar incidents

Promptbooks - Work as a playbook for certain workflows

Example built in experience

Incidents > CA - Detect Conditional Access Changes After Hours

CA - Detect Conditional Access Changes After ...

Copilot

Medium

Resolved

Unassigned

Attack story

Alerts (6)

Assets (0)

Investigations (0)

Evidence and Response (0)

Summary

Similar incidents (0)

Alerts

Play attack story

Unpin all

Show all

Aug 7, 2024 10:17 PM

Resolved

CA - Detect Conditional Access Changes After Hours

Aug 7, 2024 10:22 PM

Resolved

CA - Detect Conditional Access Changes After Hours

Aug 7, 2024 10:32 PM

Resolved

CA - Detect Conditional Access Changes After Hours

Aug 7, 2024 10:52 PM

Resolved

CA - Detect Conditional Access Changes After Hours

Aug 7, 2024 10:57 PM

Resolved

CA - Detect Conditional Access Changes After Hours

Incident graph

Incident details

Assigned to

Unassigned

Incident ID

3503

Classification

True alert

Categories

Suspicious activity

Resolution (note)

User choice from Send Teams adaptive card on incident creation playbook.

First activity

Aug 7, 2024 10:17:58 PM

Last activity

Aug 7, 2024 11:07:58 PM

Active alerts in this incident (0/6)

Copilot

Incident summary

Aug 21, 2024 4:01 PM

The medium severity incident titled 'Detect Conditional Access Changes After Hours' occurred between 2024-08-07 20:17:58 UTC and 2024-08-07 21:07:58 UTC.

At 2024-08-07 20:17:58 UTC, the first alert was triggered indicating a change in Conditional Access settings after hours. The alert was identified by the ID 'snabc5b5f1-426e-43a1-857a-36af60ccc084'.

A similar alert was triggered at 2024-08-07 20:32:58 UTC, with the ID 'snc0928882-652f-

See more

AI-generated content may be incorrect. Check it for accuracy.

Guided response

No actions to recommend

Aug 21, 2024 4:01 PM

We're constantly improving Copilot, so leave feedback if you believe it missed something.

AI-generated content may be incorrect. Check it for accuracy.

Example guided response

Tampering with the Microsoft Defender for Endpoint sens...

Low | Active | Unassigned

Attack story Alerts (2) Assets (2) Investigations (0) Evidence and Response (5) Summary Similar incidents (0)

Guided response

Aug 26, 2024 9:12 AM

Completed recommendations 0/2

Status: All

Remediation

New

Disable the account s...
Aug 26, 2024 9:10 AM

Other organizations tend to take this action for similar incidents.

Disable user in AD

View user

AI-generated content may be incorrect. Check it for accuracy.

New

Reset password for s...
Aug 26, 2024 9:10 AM

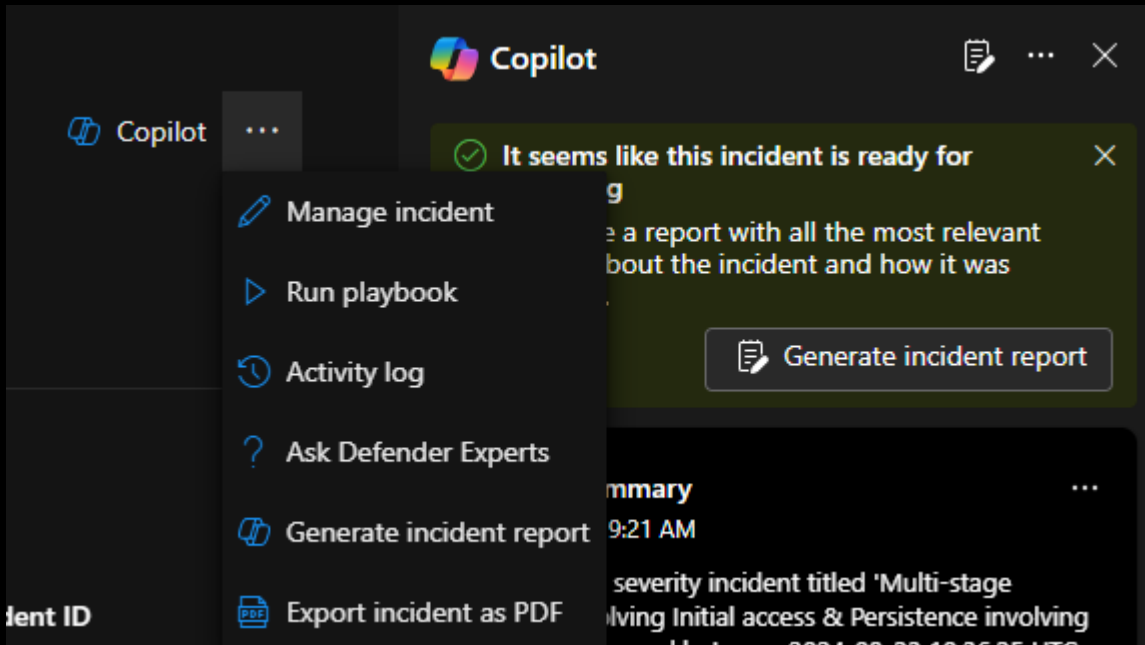
Other organizations tend to take this action for similar incidents.

Force password reset

View user

AI-generated content may be incorrect. Check it for accuracy.

Incident summary from copilot



Incident report

Aug 26, 2024 9:19 AM

Incident title

(Preview) GitHub - Repository was created involving one user

Incident details

Analysts	Incident closed after timeout .
Time created	08/23/2024 10:36:25
First log	08/25/2024 12:26:15
Last log	08/25/2024 12:26:15
Time closed	08/25/2024 12:26:15

Incident summary

The medium severity incident titled '(Preview) GitHub - Repository was created involving one user' occurred at 2024-08-23 10:36:25 UTC.

- InitialAccess: At 2024-08-23 10:36:25 UTC, a GitHub repository was created by the user 'climpr-mcloud-lz-managementbot'. This event marked the initial access stage of the incident.

Standalone experience

Can create an summarize incident 3503 readable for a communication lead for Incident response

>  **3 steps completed** 47 seconds

Aug 21, 4:07 PM

On August 7, 2024, between 20:17:58 and 21:07:58 UTC, a medium severity incident titled 'Detect Conditional Access Changes After Hours' was recorded. This incident is significant due to the multiple changes made to Conditional Access settings outside of regular business hours, which could potentially indicate unauthorized or suspicious activity.


Here are the key details of the alerts triggered during this incident:

- The first alert, identified by the ID 'snabc5b5f1-426e-43a1-857a-36af60ccc084', was triggered at 20:17:58 UTC.
- The second alert, identified by the ID 'snc0928882-652f-4ebc-9bb8-173304a2ce47', was triggered at 20:32:58 UTC.
- The third alert, identified by the ID 'sn1ff66f41-9917-41a6-a493-61be2833e83b', was triggered at 20:52:58 UTC.
- The final alert, identified by the ID 'sn88ef6dbf-7264-4c43-9804-1c30e5bec523', was triggered at 21:02:58 UTC.

Each of these alerts indicated a change in Conditional Access settings after hours, reinforcing the potential for unauthorized or suspicious activity. This information is crucial for understanding the nature of the incident and planning the appropriate response.

Cost model and optimization

Microsoft Copilot for Security compute capacity

<input type="checkbox"/> Name ↑↓	Type ↑↓
<input type="checkbox"/>  copilotscujstzszb75vrfs	Microsoft Copilot for Security compute capacity

Security compute units per hour *

1

Estimated monthly cost \$2880/month

✓ Copilot-for-Security

✓ .github\workflows

📄 deploy.yml

📄 destroy.yml

📄 LICENSE

📄 main.bicep

📄 main.bicepparam

📄 README.md



<https://github.com/Anders-Kristiansen/Copilot-for-Security>

DEMO



Thank you

