# How to monitor from the cloud

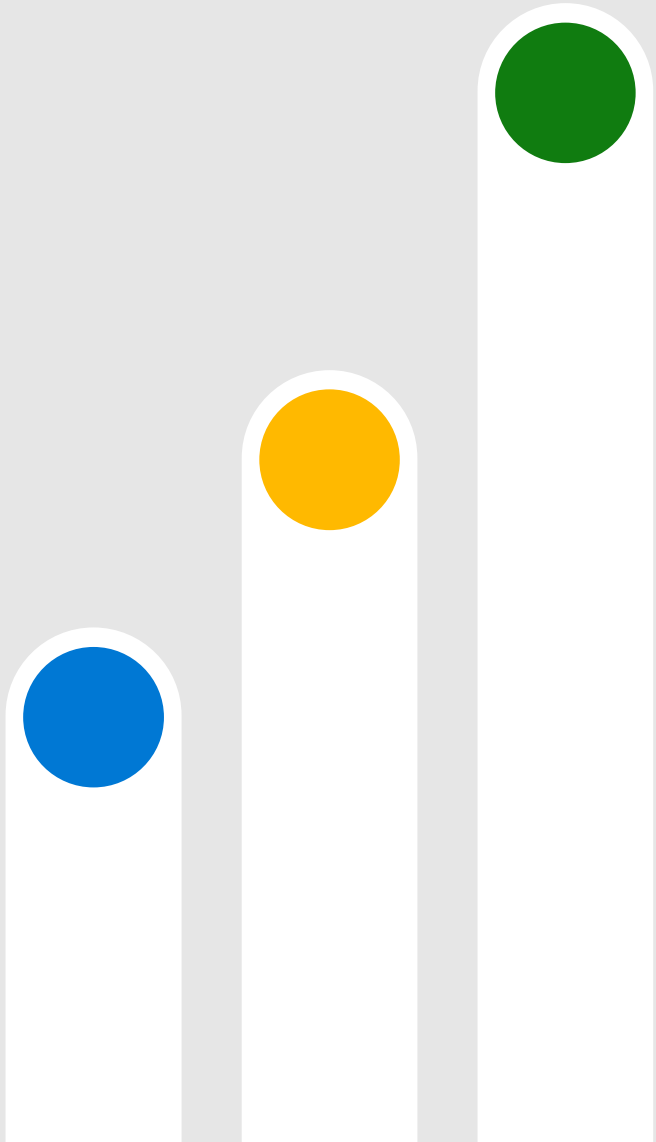
Kyle Krüsi
Senior MSM Customer Engineer

Pascal Wechsler
Infra Customer Engineer

Dominik Kessler
Identity & Security Customer Engineer

# Agenda

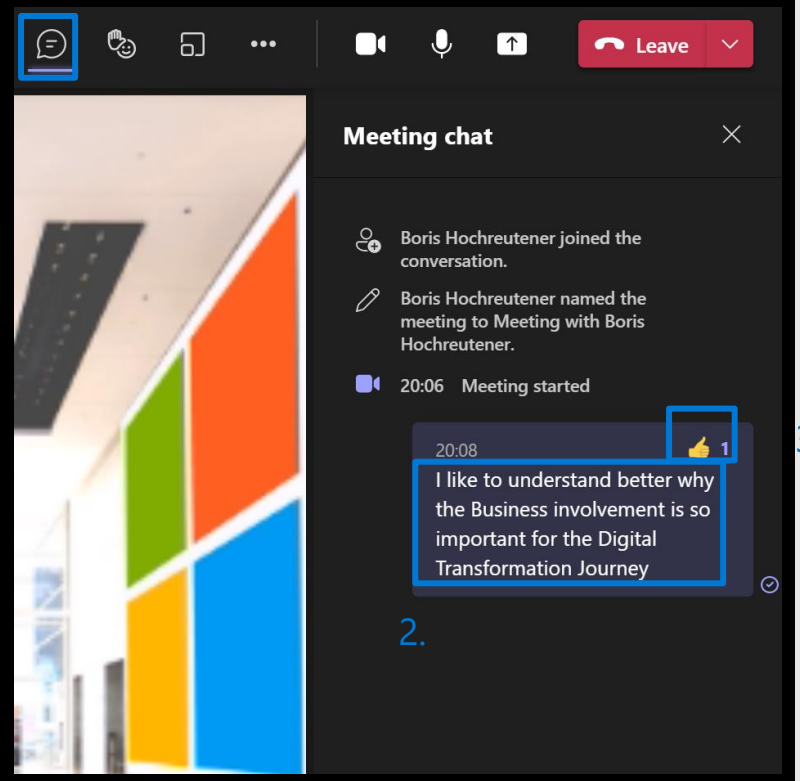
- Monitoring Plan & Challenges
- What can monitoring learn from Cyber Security
- Summary
- Roundtable Discussion



# Welcome to our #virtual Roundtable

We start with a Road to the Cloud to ensure a common End2End understanding and wording. This session will be followed by more interactive conversation based on your questions in the 2nd Roundtable Session.
Please continuously raise your questions and ideas in our Chat.

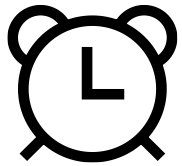
HOW




1. Press the "Chat" icon in Teams
2. Ongoing Ask your questions in the Chat
3. Continuously vote questions –then more thumbs up then higher the priority in the 2nd Roundtable Session

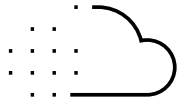
# How to monitor from the cloud

# Monitoring Challenges

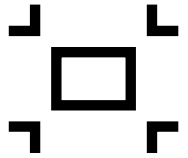


High numbers of alerts (Alert Fatigue)

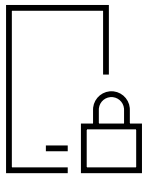
Complex service / application dependencies



Services and applications rapidly changing



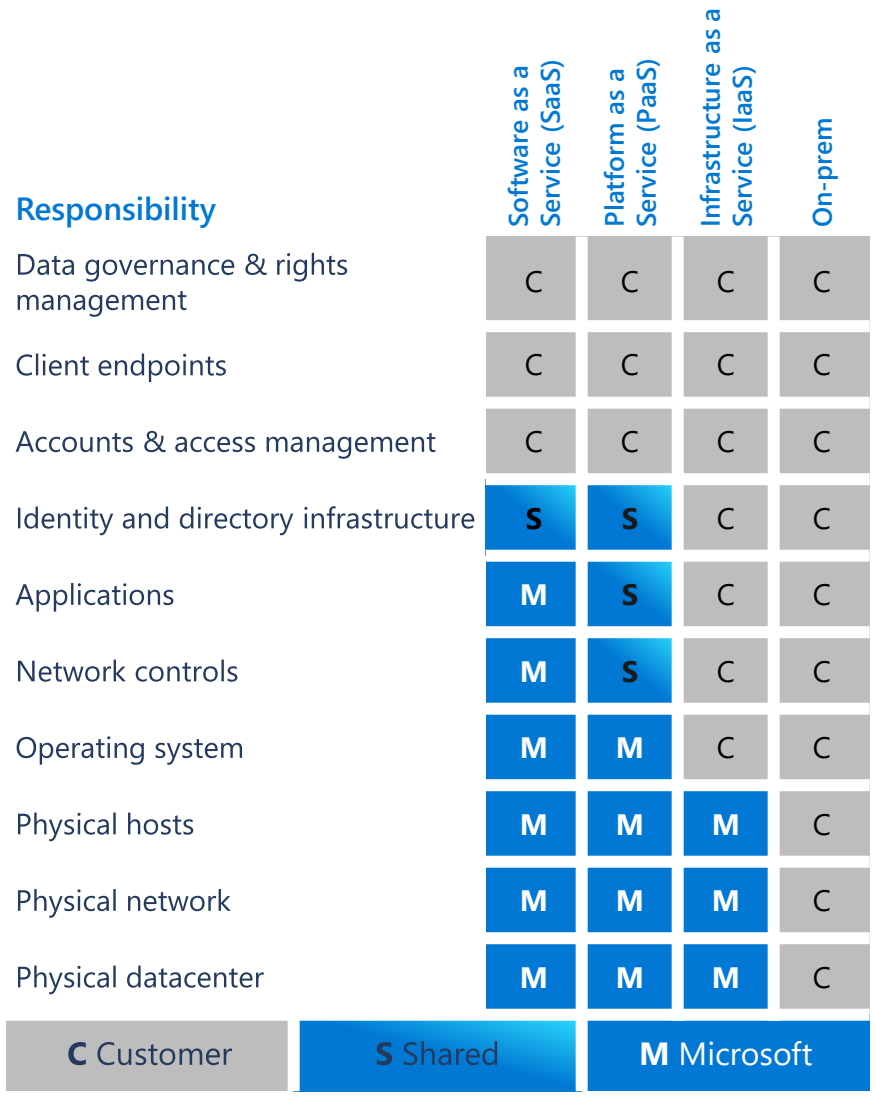
Lack of automated responses



Security and compliance requirements

# Cloud / Hybrid Monitoring Models

- Environments with different characteristics
- Different levels of responsibility
- Move toward SaaS services does not eliminate your monitoring responsibility



# How to move forward?

Based on Cloud Adoption Framework aka.ms/caf

# Monitoring Plan

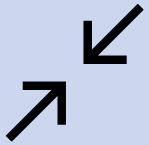
## What?

- Start early during strategy and planning phase of a project
- Include modern monitoring disciplines: Observe, measure, respond, learn, and improve
- Get agreement from relevant stakeholders incl. Business stakeholder

## How?

Describes goals and objectives, requirements and other important details

Defines the line of visibility between Service Provider and consumer



Describes how to develop and operate monitoring solutions

Based on Cloud Adoption Framework aka.ms/caf

# Monitoring Plan

## Business Perspective

- Business value streams and risks
- Stakeholders and consumers
- End-user perspective
- And more…

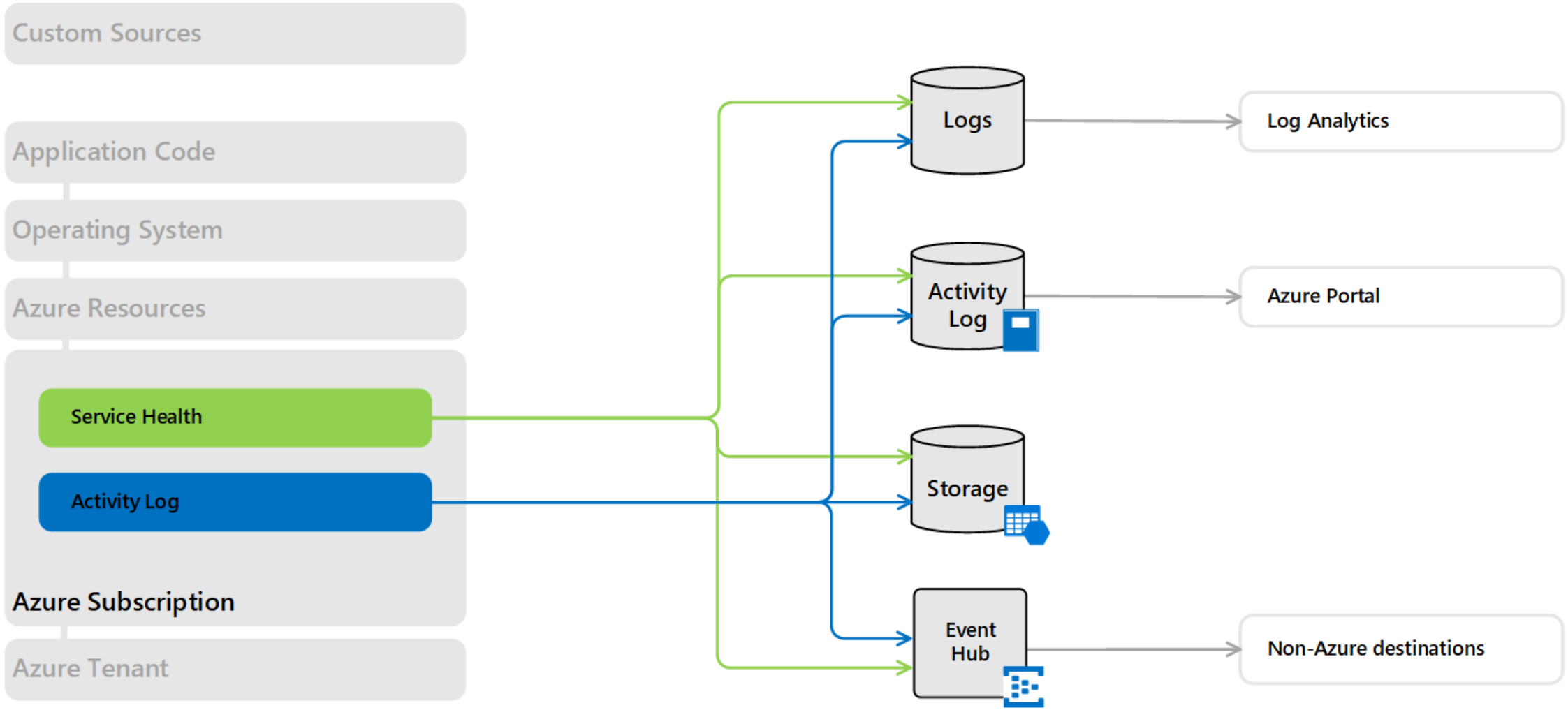
## Service Perspective

- Definition of Service
- Service Map
- Roles and accountabilities
- Service agreements (incl. Partner/Supplier)

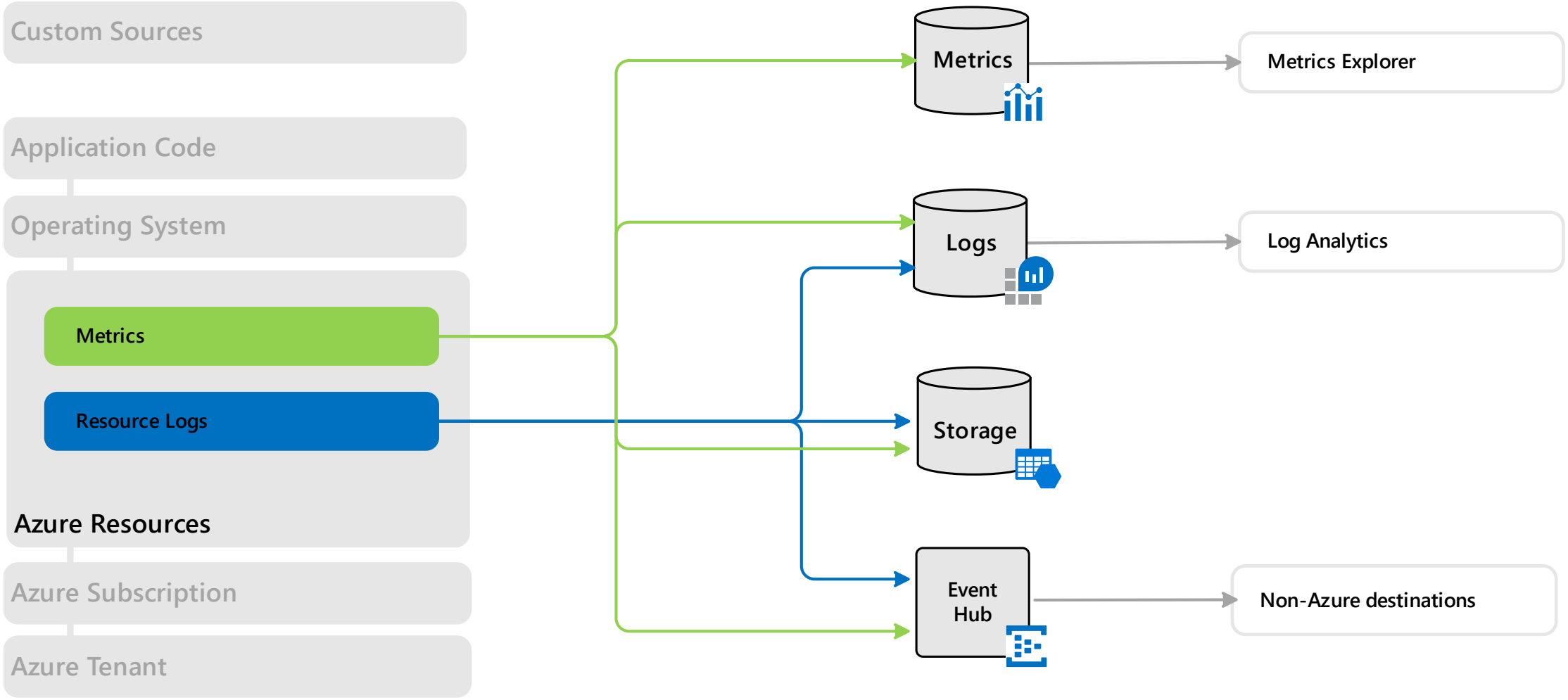
## Technology Perspective

- User stories and scenarios
- Component dependency map
- Technical targets
- And more…

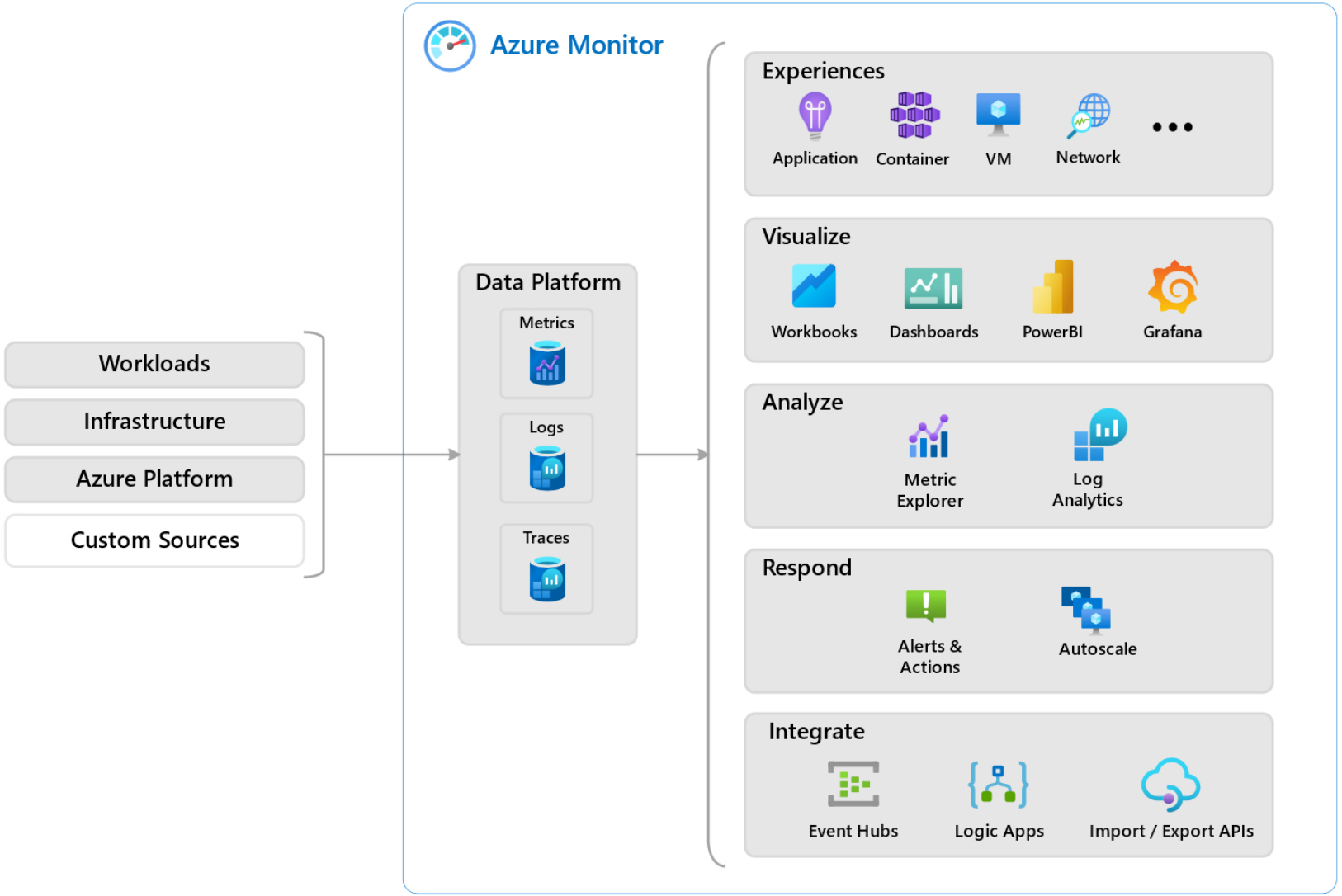
# Data sources – Example *Azure Subscription*



# Data sources – Example *Azure Resource*



# Azure Monitor - Overview



# Comparison with *System Center Operations Manager*

**Azure Monitor**

- Designed for the cloud but can monitor on-premises systems
- Modern APM capabilities (Application Insights)
- Natively integrates with Azure Platform (Diagnostic Settings)

**Operations Manager**

- Designed for on-premises and then extended to the cloud
- Well established for Server Workloads (existing Management Packs)
- Custom work required for Business Applications
- Lack of modern APM capabilities

Full comparison can be found here: [Cloud monitoring platforms overview - Cloud Adoption Framework | Microsoft Docs]

# Skills relevant for Monitoring

- Understand the fundamentals of Cloud Infrastructure / Cloud Applications
- Understand Azure Management tools & services
- Understand diagnostic settings of Azure Resource types
- Scripting languages
  - Kusto Query Language (KQL)
  - Azure PowerShell / CLI
  - JSON & XML

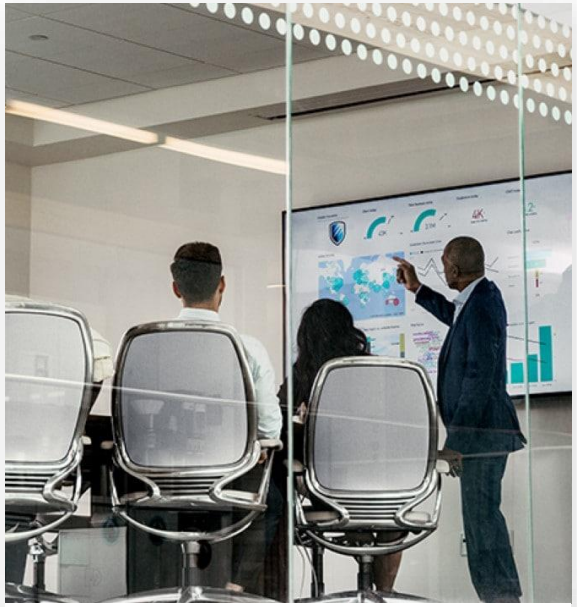
# What can monitoring learn from Cyber Security?

# What is Cyber Security?

- Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- The term applies in a variety of contexts, from business to mobile computing, and can be broken down into a few common categories.

## Identity and access management

Your universal platform for managing and securing identities.



## Threat protection

Stop attacks with built-in and automated security.

## Information protection

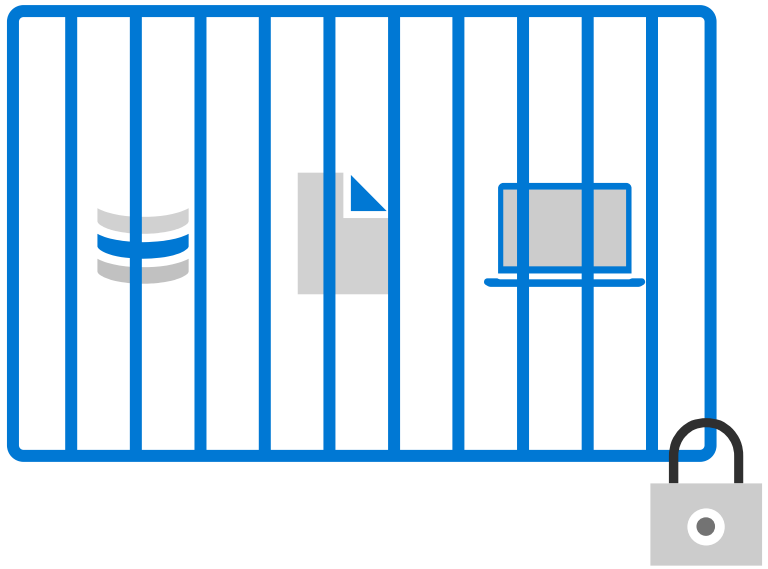
Protect your sensitive data – wherever it resides or travels.

## Cloud security (Security management)

Protect your cross-cloud resources.

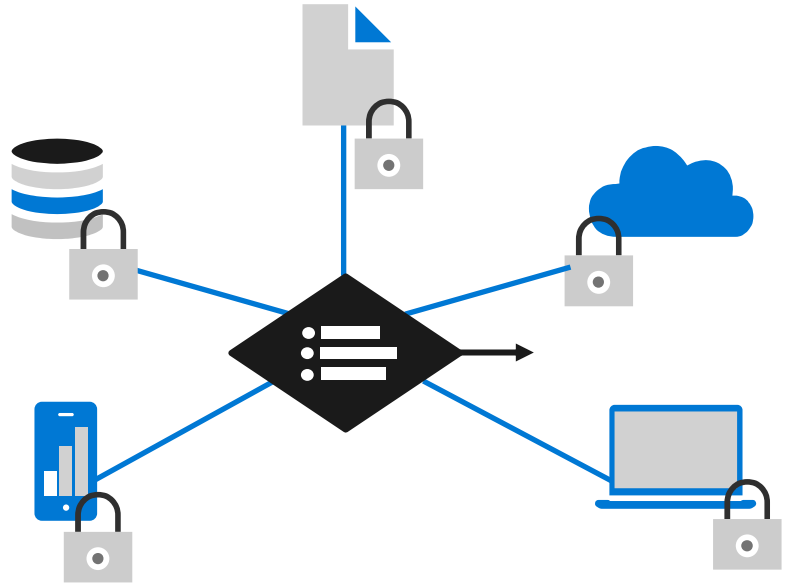
# Secure assets where they are with Zero Trust

Simplify security and make it more effective



**Classic Approach**

Restrict everything to a ‘secure’ network



**Zero Trust**

Protect assets anywhere with central policy

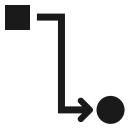
# Cyber Monitoring Challenges

About 70 security products from 35 different vendors

talent scarcity

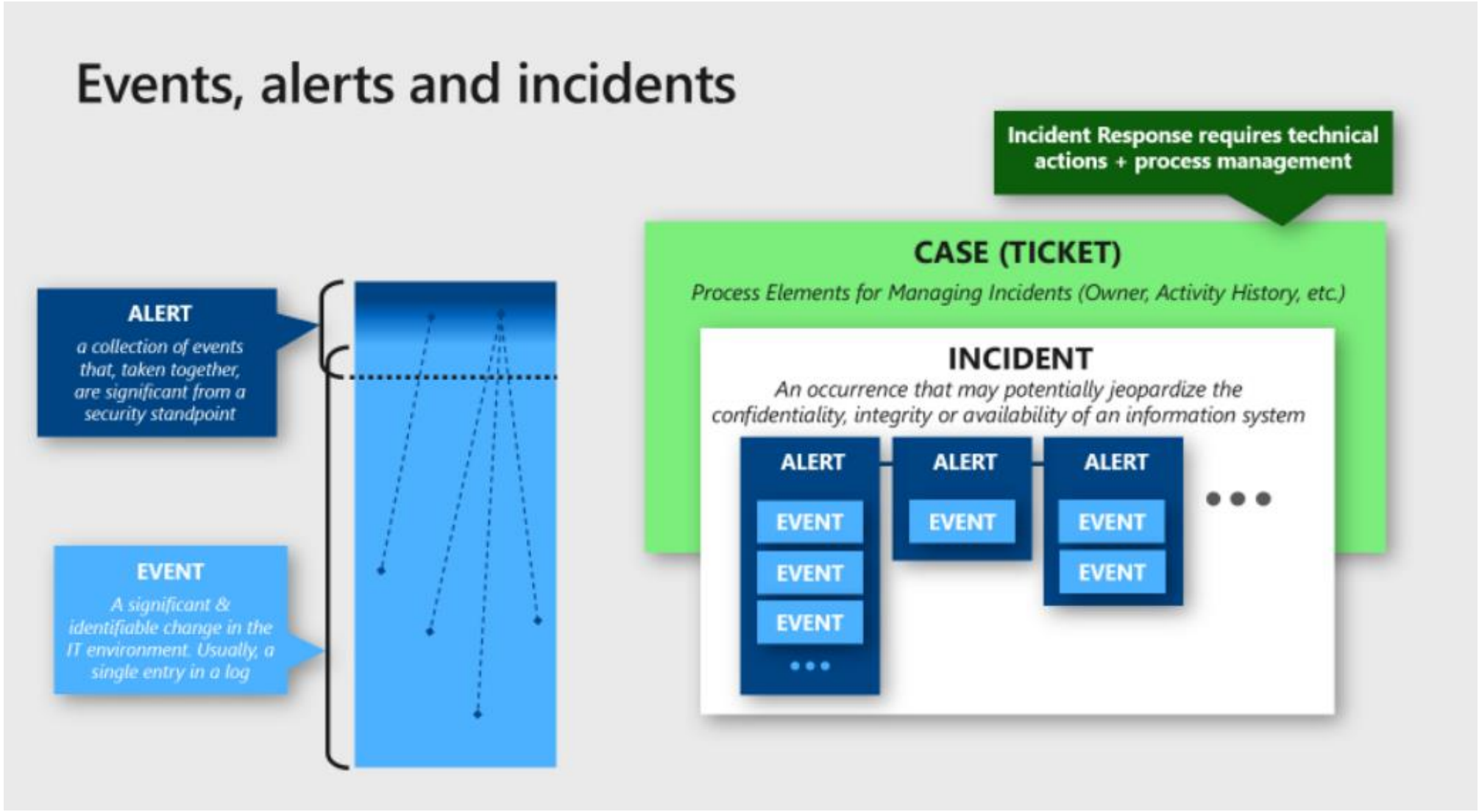
huge volume of alerts (Alert Fatigue)

44 % of these alerts go uninvestigated



Missing automation

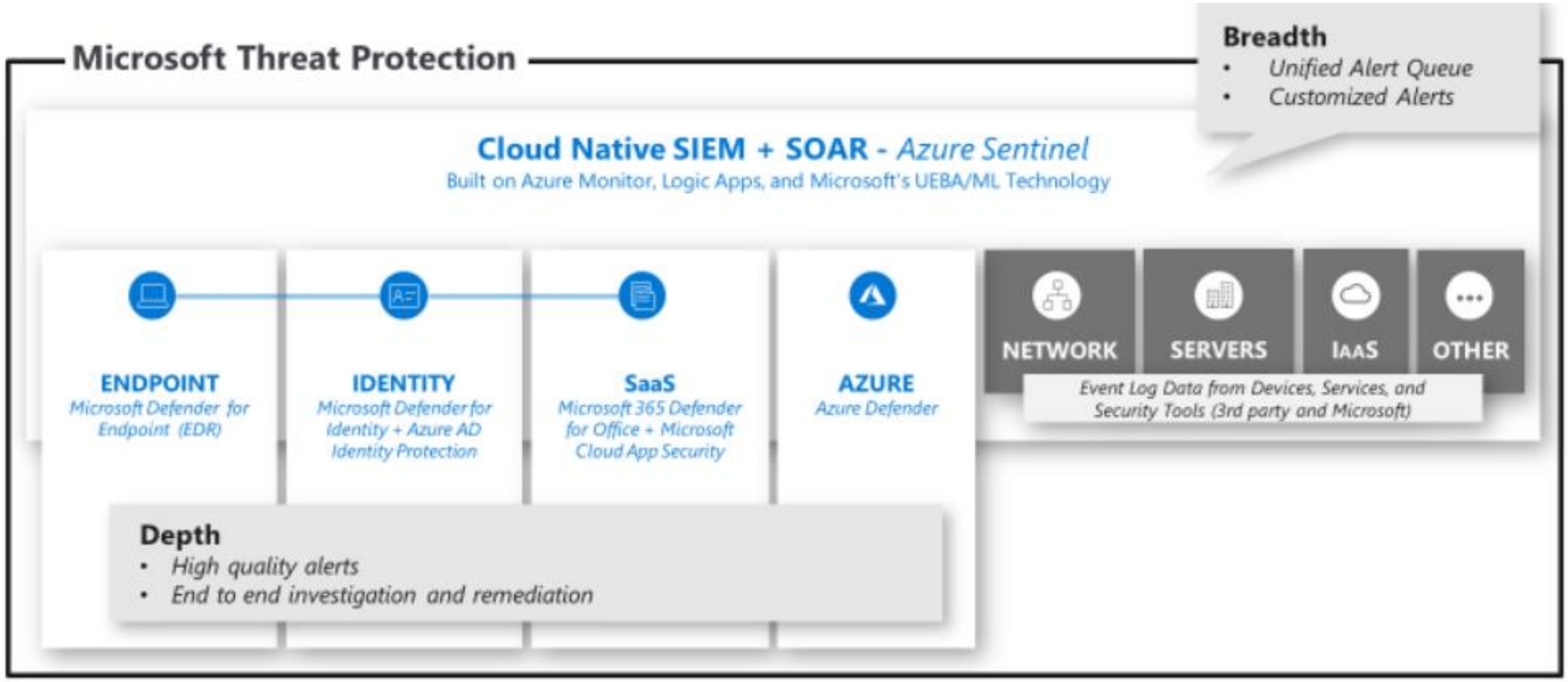
# Correlation



# Threat intelligence

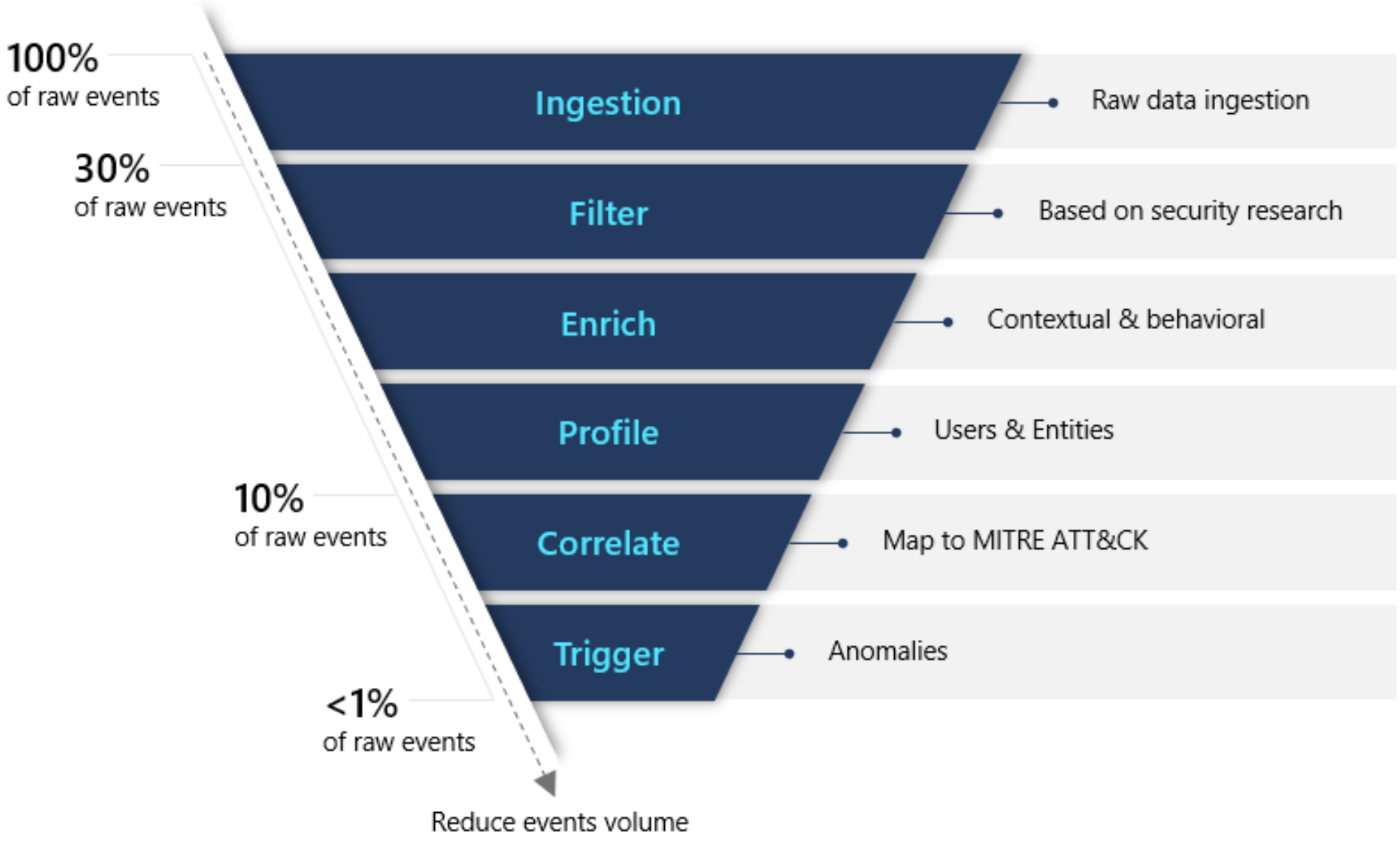
- Microsoft example
  - trillions of daily signals, across all clouds and all platforms
  - holistic view of the global security ecosystem
  - latest in machine learning and artificial intelligence techniques
  - taking automated actions
  - providing actionable intelligence to security teams for analysis

# Native Integration

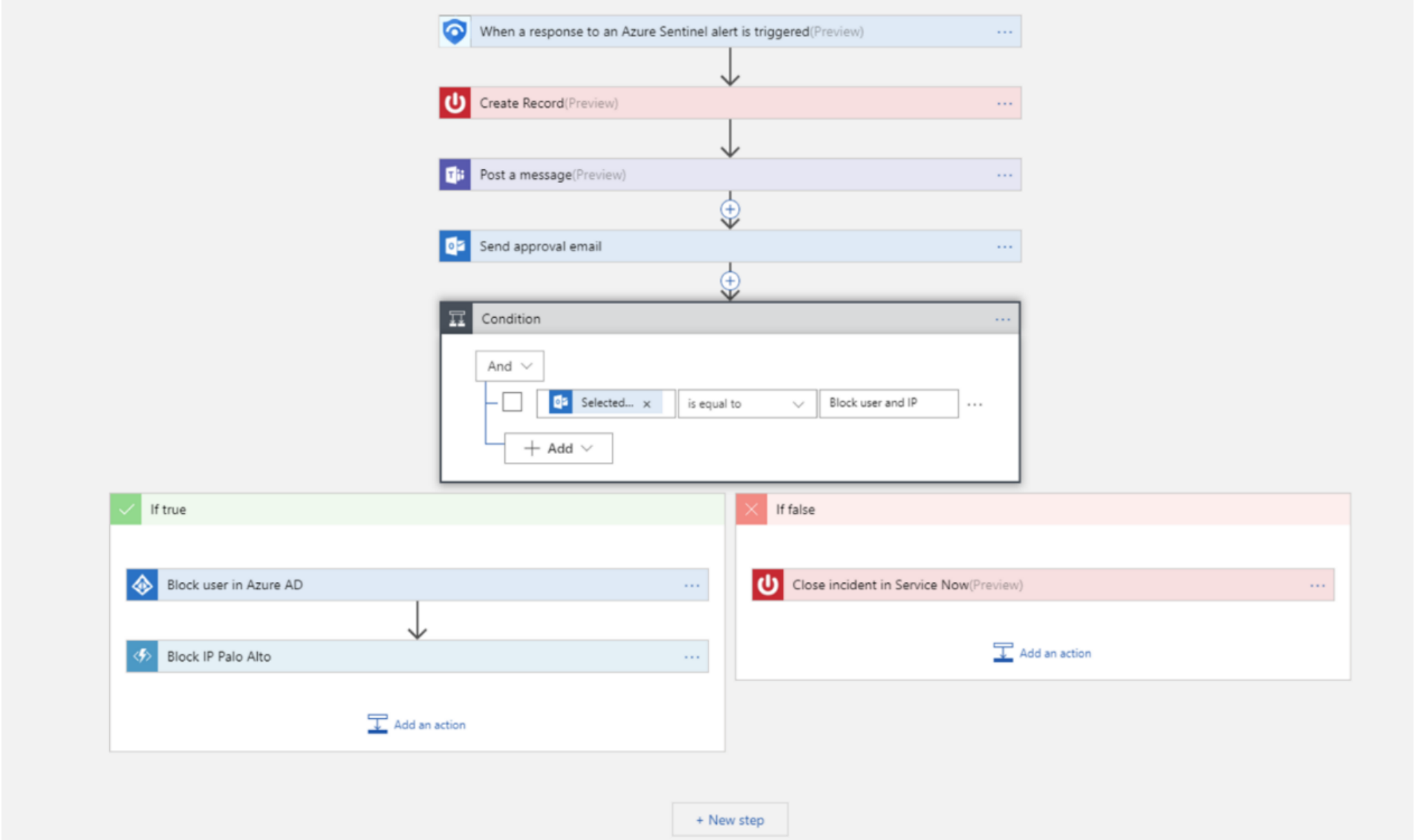


# Machine learning

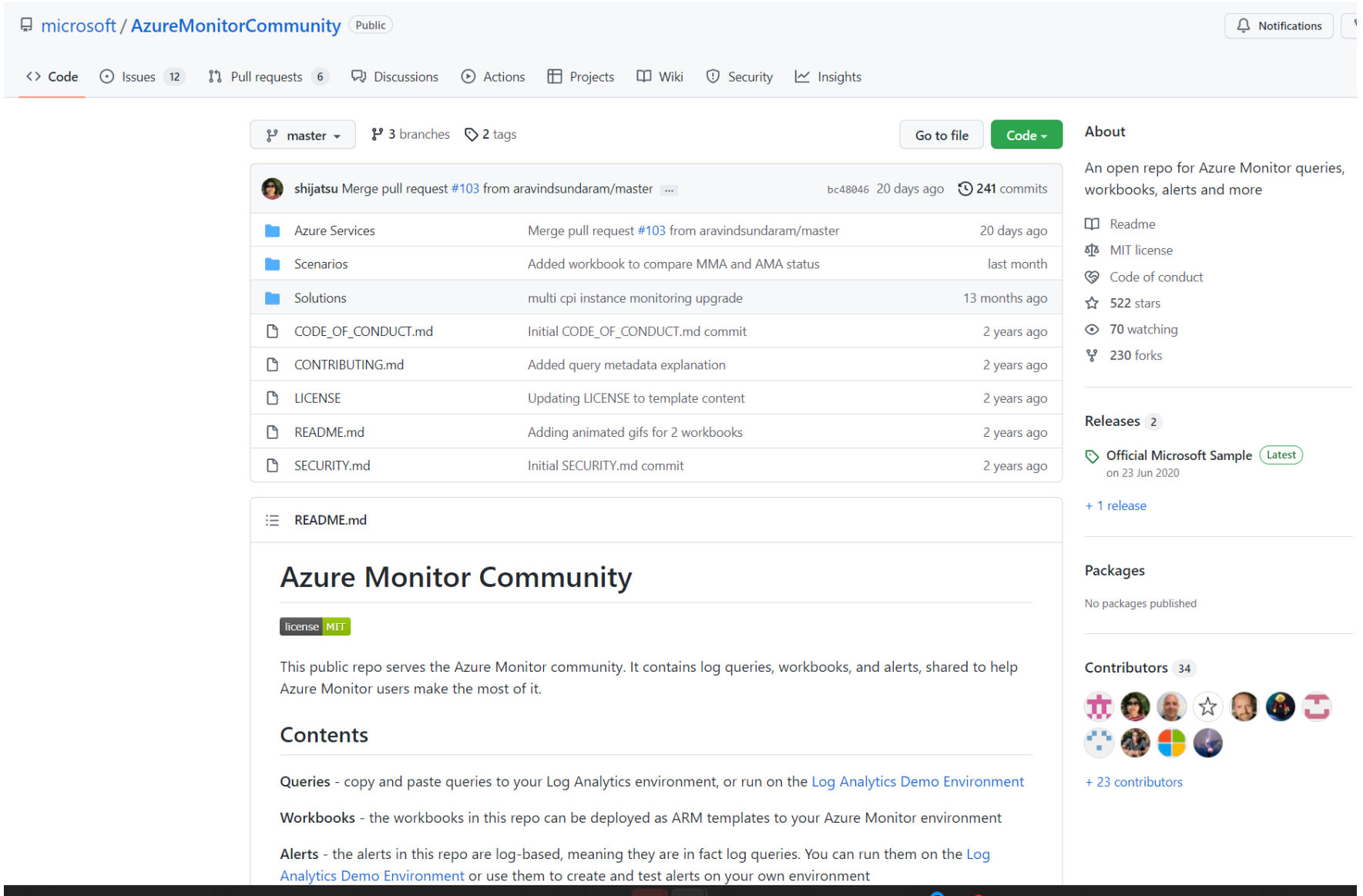
# User and entity behavior analytics (UEBA)



# Automation


When a response to an Azure Sentinel alert is triggered(Preview)
Create Record(Preview)
Post a message(Preview)
Send approval email
Condition
And
Selected...
is equal to
Block user and IP
Add
If true
Block user in Azure AD
Block IP Palo Alto
Add an action
If false
Close incident in Service Now(Preview)
Add an action
+ New step

# Community



microsoft / AzureMonitorCommunity Public

Notifications

Code | Issues 12 | Pull requests 6 | Discussions | Actions | Projects | Wiki | Security | Insights

master | 3 branches | 2 tags | Go to file | Code

shijatsu Merge pull request #103 from aravindsundaram/master ... bc48046 20 days ago 241 commits

| | | |
|---|---|---|
| Azure Services | Merge pull request #103 from aravindsundaram/master | 20 days ago |
| Scenarios | Added workbook to compare MMA and AMA status | last month |
| Solutions | multi cpi instance monitoring upgrade | 13 months ago |
| CODE_OF_CONDUCT.md | Initial CODE_OF_CONDUCT.md commit | 2 years ago |
| CONTRIBUTING.md | Added query metadata explanation | 2 years ago |
| LICENSE | Updating LICENSE to template content | 2 years ago |
| README.md | Adding animated gifs for 2 workbooks | 2 years ago |
| SECURITY.md | Initial SECURITY.md commit | 2 years ago |

README.md

## Azure Monitor Community

license MIT

This public repo serves the Azure Monitor community. It contains log queries, workbooks, and alerts, shared to help Azure Monitor users make the most of it.

### Contents

**Queries** - copy and paste queries to your Log Analytics environment, or run on the Log Analytics Demo Environment

**Workbooks** - the workbooks in this repo can be deployed as ARM templates to your Azure Monitor environment

**Alerts** - the alerts in this repo are log-based, meaning they are in fact log queries. You can run them on the Log Analytics Demo Environment or use them to create and test alerts on your own environment

About

An open repo for Azure Monitor queries, workbooks, alerts and more

Readme
MIT license
Code of conduct
522 stars
70 watching
230 forks

Releases 2

Official Microsoft Sample Latest
on 23 Jun 2020

+ 1 release

Packages

No packages published

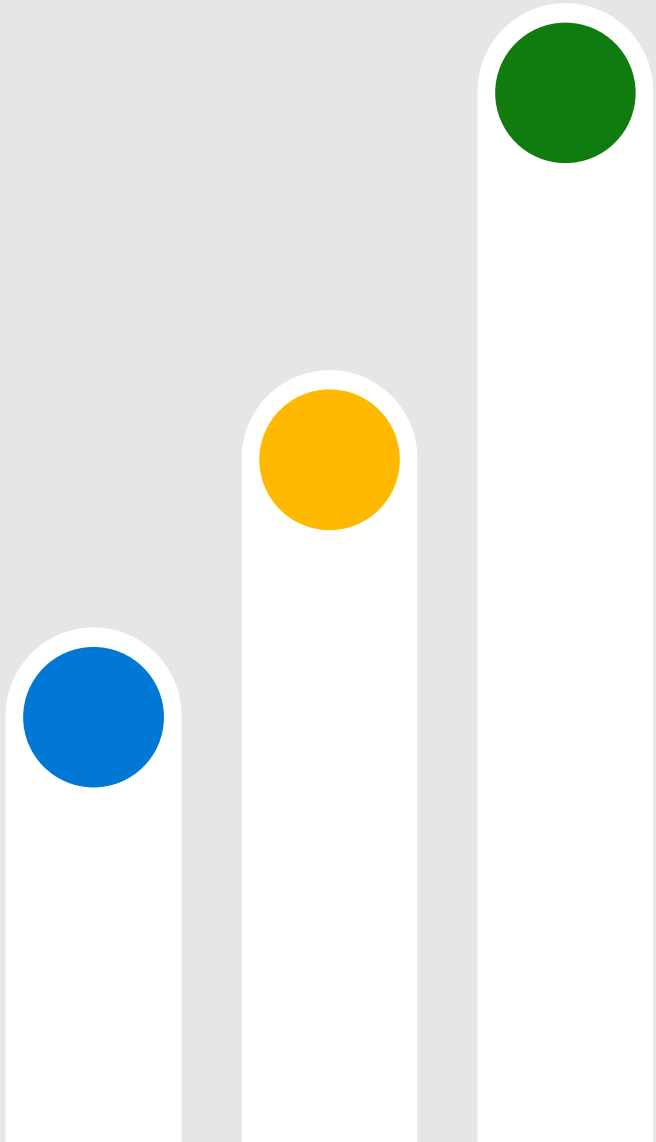
Contributors 34

+ 23 contributors

# Summary

# General Guidance

- Monitoring Strategy/Plan comes first, Monitoring tools second
- Create visibility across multiple layers
- Define the right log sources
- Reduce alert noise, leverage automation
- Kusto Query Language (KQL) is key
- Machine Learning reduces the amount of alerts



# Additional Resources

- Cloud monitoring guide - Cloud Adoption Framework | Microsoft Docs
- AZ-305: Design identity, governance, and monitor solutions - Learn | Microsoft Docs
- Monitor the usage, performance, and availability of resources with Azure Monitor - Learn | Microsoft Docs
- Cloud monitoring strategy - Cloud Adoption Framework | Microsoft Docs
- Health Endpoint Monitoring pattern - Azure Architecture Center | Microsoft Docs
- 6 strategies to reduce cybersecurity alert fatigue in your SOC - Microsoft Security Blog

Microsoft

# Thank you

The following slides contain preliminary information that may be changed substantially prior to final commercial release of the software described herein. The information contained represents the current view of Microsoft Corporation on the issues discussed as of the date of the presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of the presentation.

This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THE ROADMAP PORTION OF THIS PRESENTATION.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this presentation. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this information does not give you any license to these patents, trademarks, copyrights, or other intellectual property.