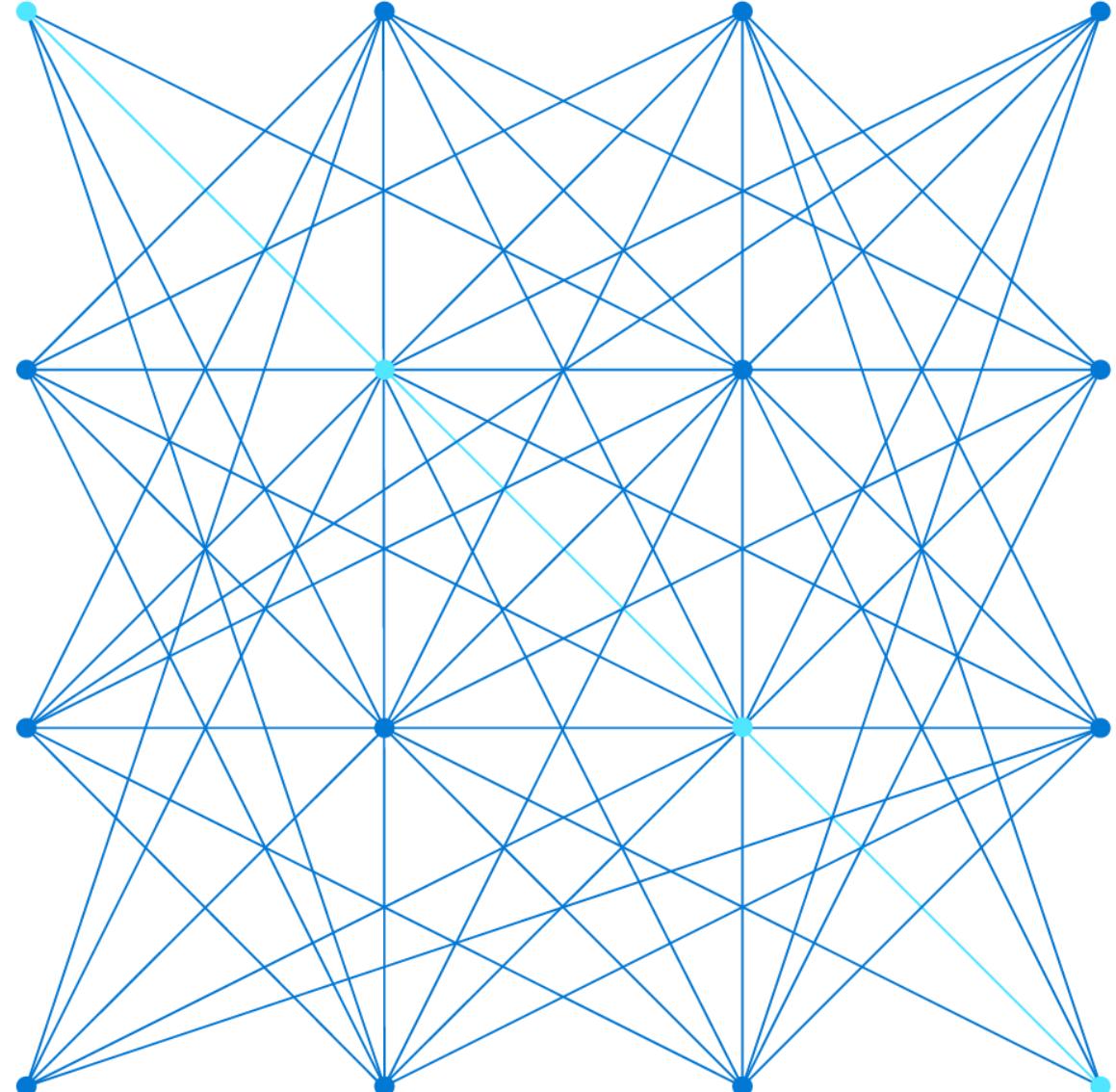
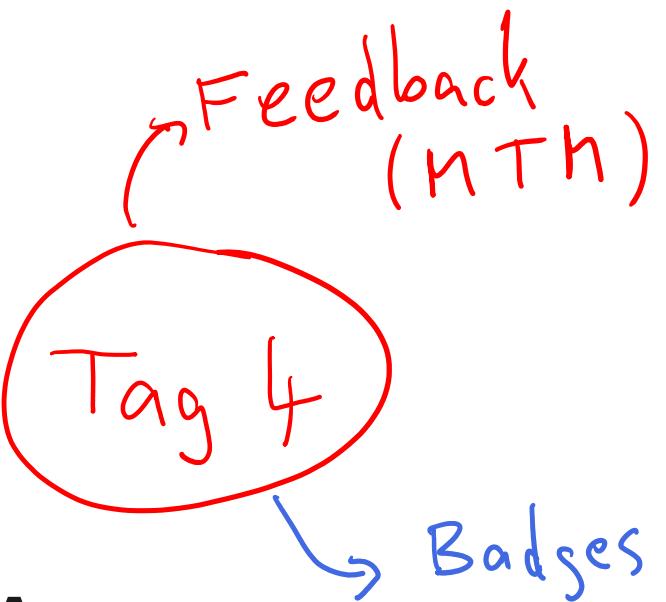


AZ-500

# Microsoft Azure Security Technologies

Guten Morgen!



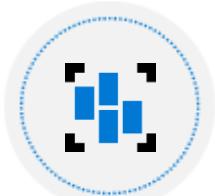
# AZ-500 Agenda



## Learning Path 1 Identity and Access



## Learning Path 2 Implement Platform Protection



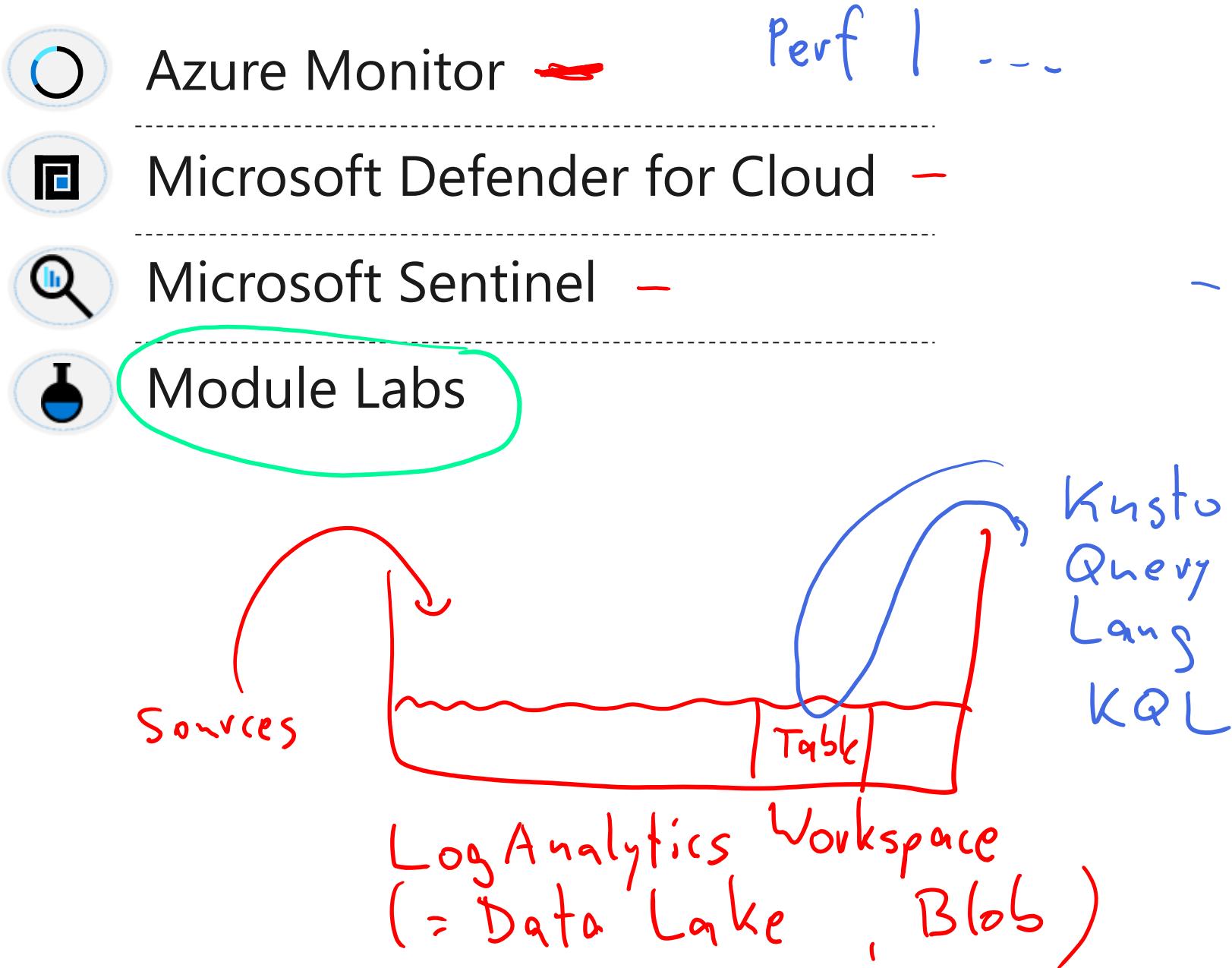
## Learning Path 3 Data and Application Security



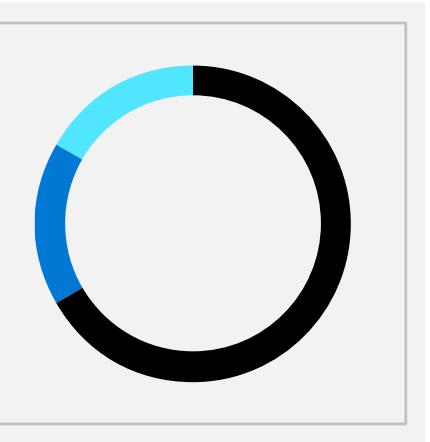
## Learning Path 4 Security Operations

SC-200

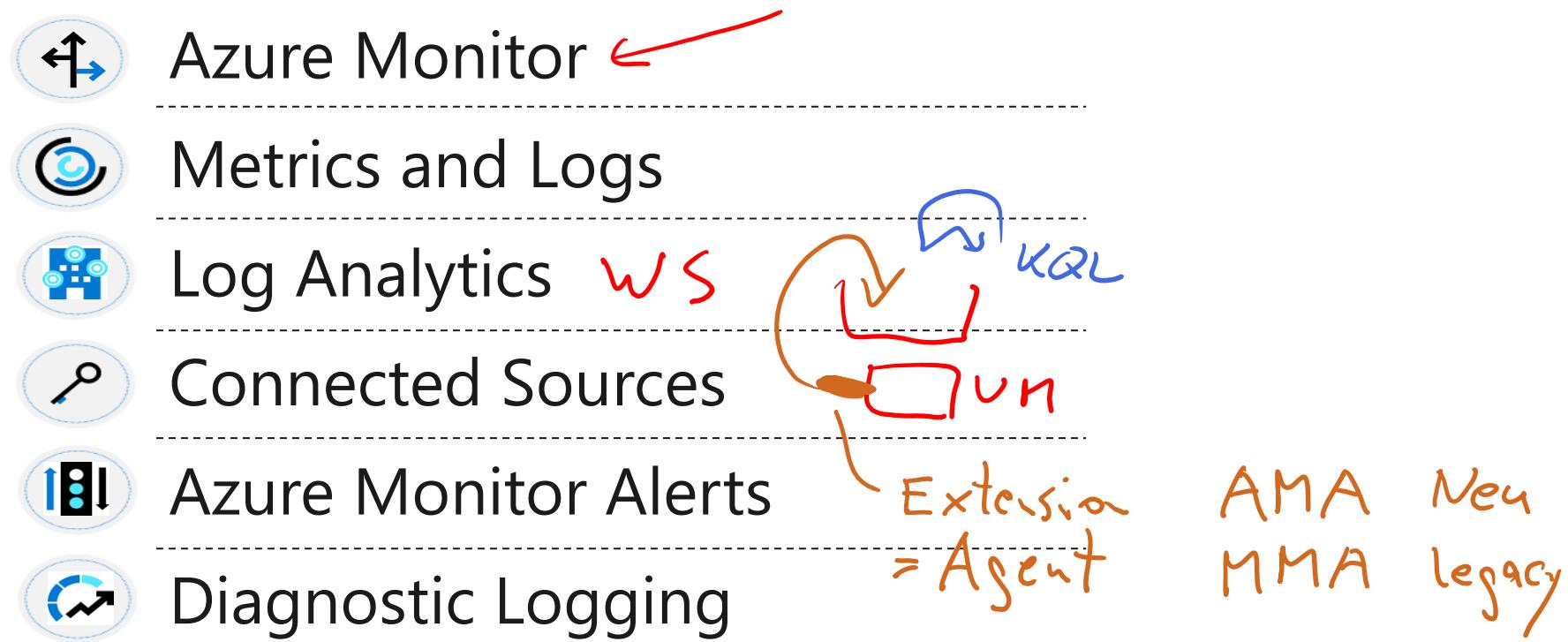
# Learning Path: Security Operations



# Azure Monitor



# Azure Monitor

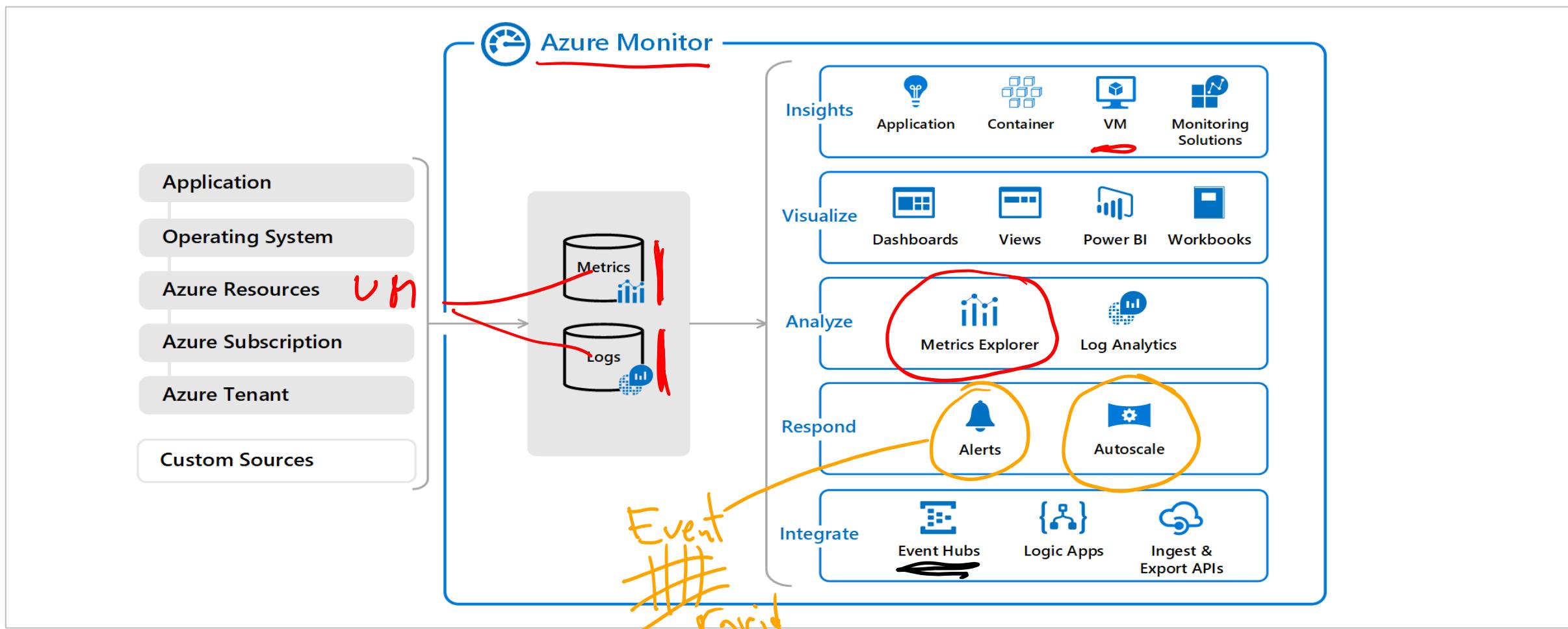


Cloud Native?

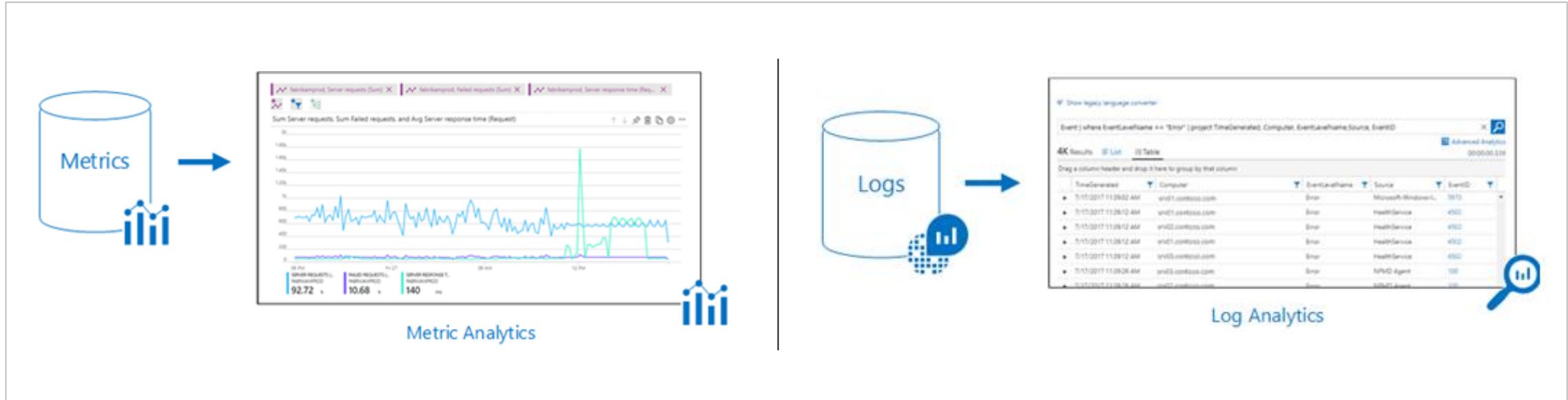
VM → App Service  
Container  
Functions  
Logic App

# Azure Monitor Architecture

Azure Monitor offers a consolidated pipeline for routing any of your monitoring data into a SIEM tool – Security Center



# Metrics and Logs



Metrics are numerical values that describe some aspect of a system at a point in time

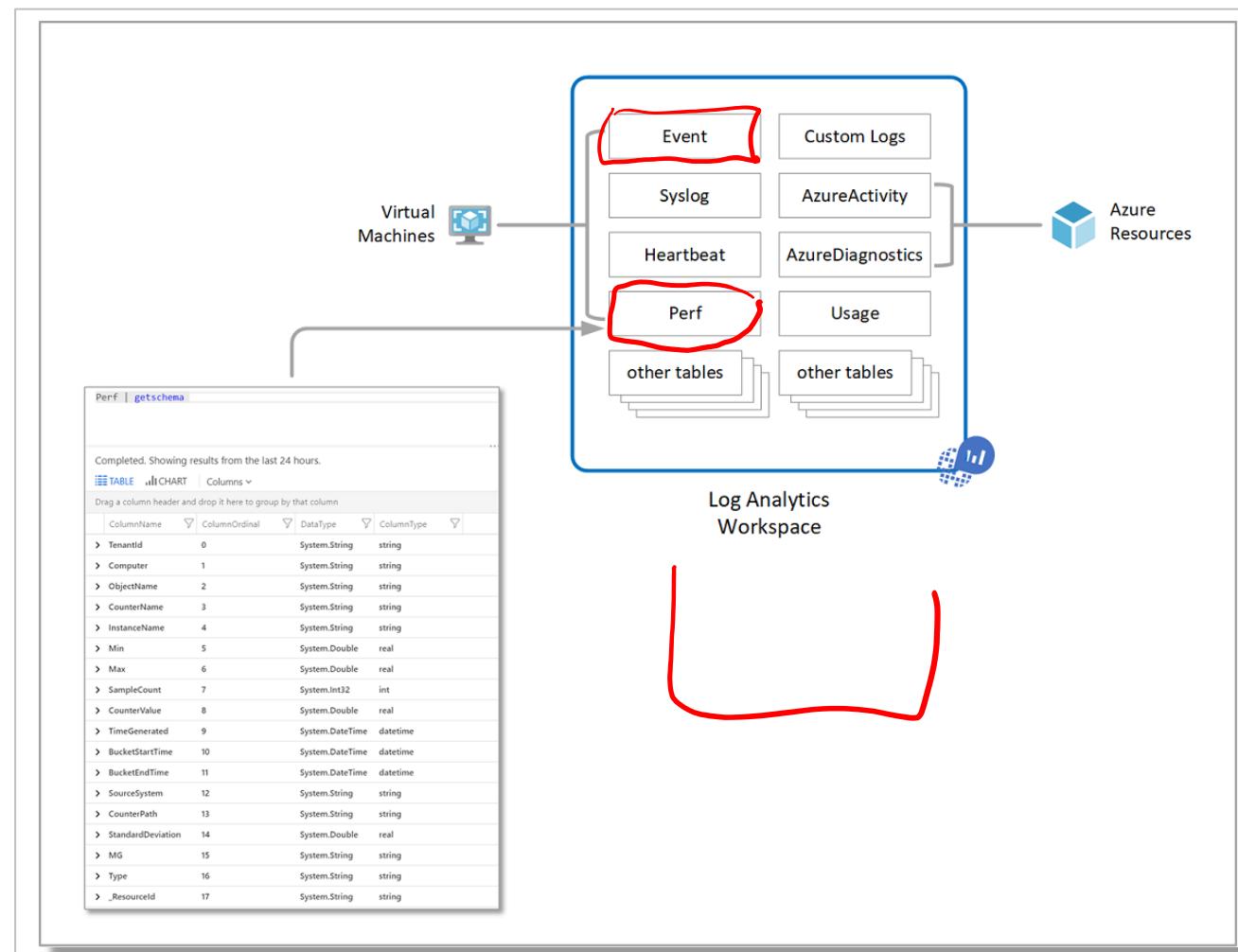
They are lightweight and capable of supporting near real-time scenarios

Logs contain different kinds of data organized into records with different sets of properties for each type

Telemetry (events, traces) and performance data can be combined for analysis

# Log Analytics

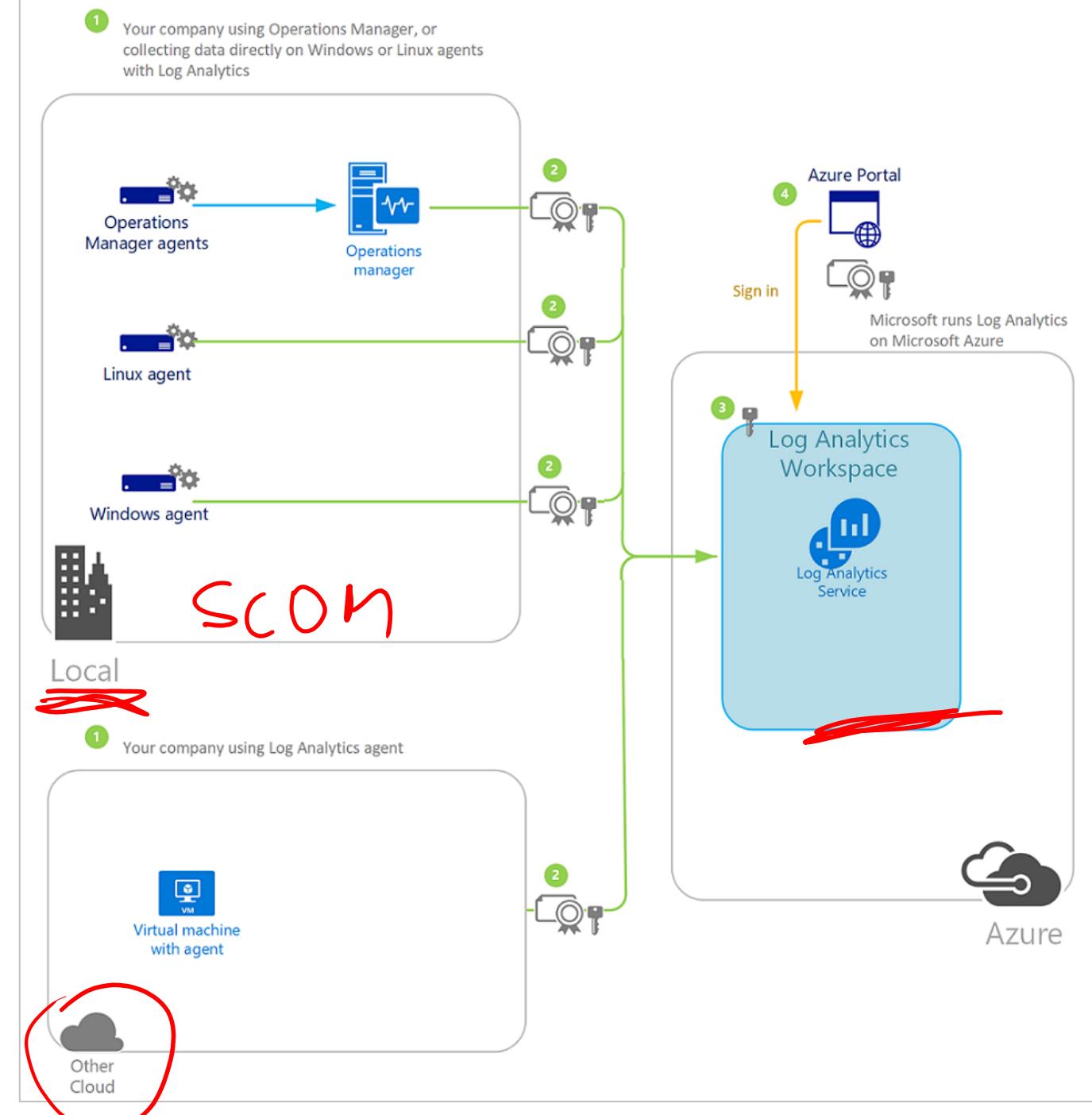
Collect and analyze resource data (cloud and on-premises) - write log queries and interactively analyze their results.



# Connected Sources

Connected Sources generate data

Data can be collected from Windows,  
Linux, SCOM and Azure Storage



# Azure Monitor Alerts

Select the target resource to monitor

Add a condition to select a signal and define the logic

Notify the team or automate follow-on actions

Display by severity (0 to 4)

Administer with New, Acknowledged, and Closed status

## Create alert rule

Create an alert rule to identify and address issues when important conditions are found in your monitoring data. [View tutorial + read more](#)

### Scope

Select the target resource you wish to monitor.

Resource

Hierarchy

No resource selected yet

[Select resource](#)

### Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name

No condition selected yet

[Add condition](#)

### Actions

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group. [Learn more](#)

Action group name

Contains actions

No action group selected yet

[Add action groups](#)

### Alert rule details

Provide details on your alert rule so that you can identify and manage it later.

Alert rule name \*  ⓘ

Specify the alert rule name

Description

Specify the alert rule description

Enable alert rule upon creation

[Create alert rule](#)

# Diagnostic Settings

Tenant Logs – logs from outside of the Azure Subscriptions

Resource Logs – Logs from services inside of the subscription

Configure Diagnostic Settings to send logged metrics to different destinations

Retention times are available for archiving to a storage account

The screenshot shows the 'Diagnostics settings' configuration page in the Azure portal. The URL in the top left corner is 'Home > Monitor | Diagnostics settings > Diagnostics settings'. The page title is 'Diagnostics settings'. There are four buttons at the top: 'Save' (with a disk icon), 'Discard' (with a crossed-out disk icon), 'Delete' (with a trash bin icon), and 'Provide feedback' (with a smiley face icon). Below these buttons is a descriptive text block: 'A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)'.

The main form has two sections: 'Category details' and 'Destination details'.

**Category details:**

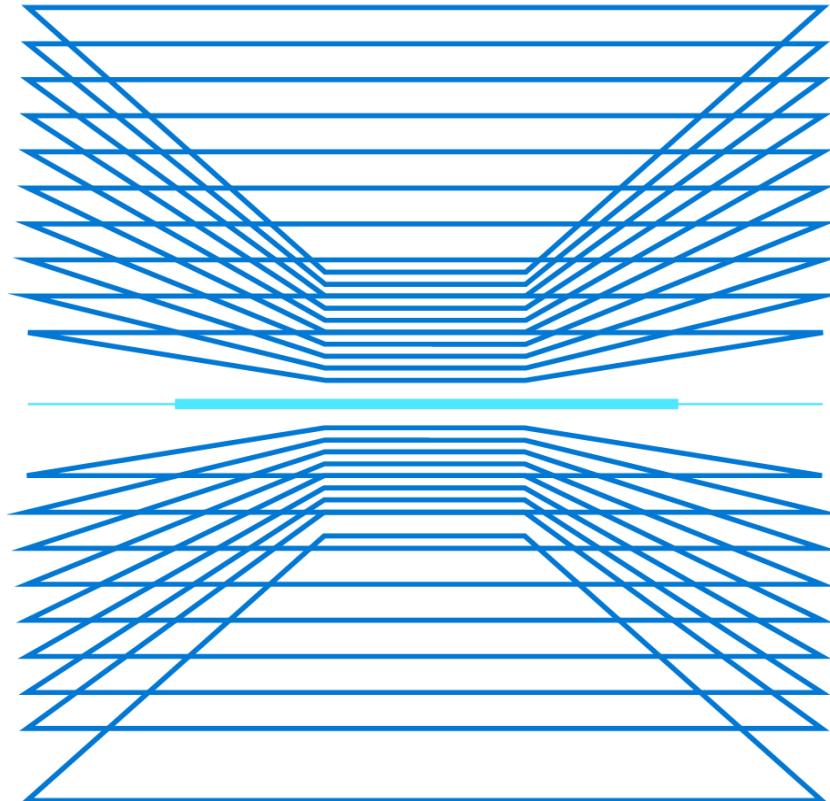
- log:** A list of checked checkboxes:
  - WorkflowRuntime
- metric:** A list of checked checkboxes:
  - AllMetrics

**Destination details:**

- Send to Log Analytics
- Archive to a storage account
- Stream to an event hub

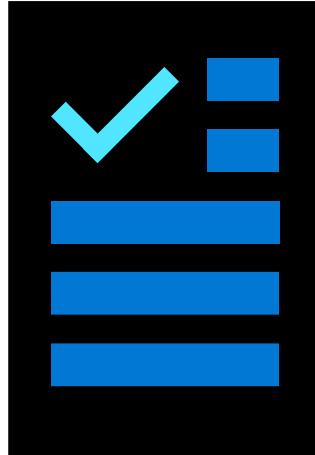
# Demonstration: Azure Monitor

- Activity logs and alerts
- Log analytics



# Additional Study – Azure Monitor

## Module Review Questions



## Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

Analyze your Azure infrastructure by using Azure Monitor logs (Exercise)

Design a holistic monitoring strategy on Azure Monitor and report on security events in Azure AD (Exercise)

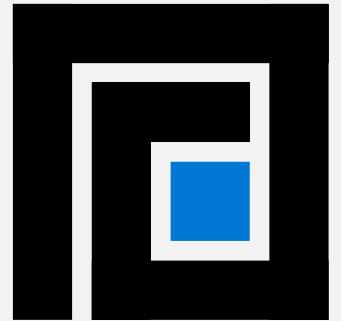
Improve incident response with alerting on Azure (Exercise)

Defender M365

- Cloud Apps
- Identity
- Endpoint
- Office

## Microsoft Defender for Cloud

ASC  
Subscription



# Microsoft Defender for Cloud



MITRE | ATT&CK®



Microsoft Defender for Cloud



Microsoft Defender for Cloud Features



Microsoft Defender for Cloud Security Policies



Microsoft Defender for Cloud Recommendations



Secure Score



Brute Force Attacks



Just in Time Virtual Machine Access

# MITRE | ATT&CK® matrix

The MITRE ATT&CK matrix is a **publicly accessible knowledge base** for understanding the various **tactics** and **techniques** used by attackers during a cyberattack.

The knowledge base is organized into several categories: **pre-attack**, **initial access**, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration, and command and control.

Defender for Cloud leverages the MITRE Attack matrix to **associate alerts** with their **perceived intent**, helping formalize security domain knowledge.

Home > Microsoft Defender for Cloud | Security alerts >

## Security alert

2517210707511130134\_c97105c5-13a7-45c1-b132-b30dfa7a96f6

 Suspected brute-force attack attempt Sample alert

High  
Severity

 Active  
Status

 04/11/23, 11:20 AM  
Activity time

### Alert description

 Copy alert JSON

THIS IS A SAMPLE ALERT: Someone is attempting to brute force credentials to your SQL server 'Sample-SQL'.

### Affected resource



## MITRE ATT&CK® tactics

- Pre-attack



Pre-  
attack

# MITRE | ATT&CK® matrix (continued)

**Pre-Attack** could be either an **attempt to access a certain resource** regardless of a malicious intent, or a failed attempt to gain access to a target system **to gather information prior to exploitation.**

This step is usually detected as an attempt, originating from outside the network, to scan the target system and identify an entry point.

## MITRE Tactic Example: Pre-attack

The screenshot shows a Microsoft Azure Defender interface for security alerts. A specific alert is highlighted with a red oval. The alert details are as follows:

- Title:** Security alert
- Description:** Attempted logon by a potentially harmful application
- Status:** High Severity, Active, 04/11/23, 11:20 AM
- Alert description:** THIS IS A SAMPLE ALERT: A potentially harmful application attempted to access SQL server 'Sample-SQL'.
- Affected resource:** Sample-DB, MCAPS-Hybrid-REQ-48118-2022-serlingdavis Subscription
- MITRE ATT&CK® tactics:** Pre-attack (highlighted with a red underline)

# MITRE | ATT&CK® matrix (continued)

**Initial Access** is the stage where an **attacker manages to get a foothold** on the attacked resource.

This stage is relevant for **compute hosts and resources** such as **user accounts, certificates etc.**

Threat actors will often be able to control the resource after this stage.

## MITRE Tactic Example: Initial Access

The screenshot shows a Microsoft Azure Defender for Cloud Security alerts interface. A specific alert is highlighted:

- Security alert**: 2517210708970817645\_a23dfa...  
Type: Access from a suspicious IP
- Severity**: High
- Status**: Active
- Activity time**: 04/11/23, 11:18 AM
- Alert description**: THIS IS A SAMPLE ALERT: Azure Cosmos DB account 'Sample-AzureCosmosDBAccount' was successfully accessed from an IP address that was identified as a threat by Microsoft Threat Intelligence. The threat actor's access was authenticated using Aad.
- Affected resource**: Sample-AzureCosmosDBAccount, MCAPS-Hybrid-REQ-48118-2022-serlingdavis Subscription
- MITRE ATT&CK® tactics**: Initial Access

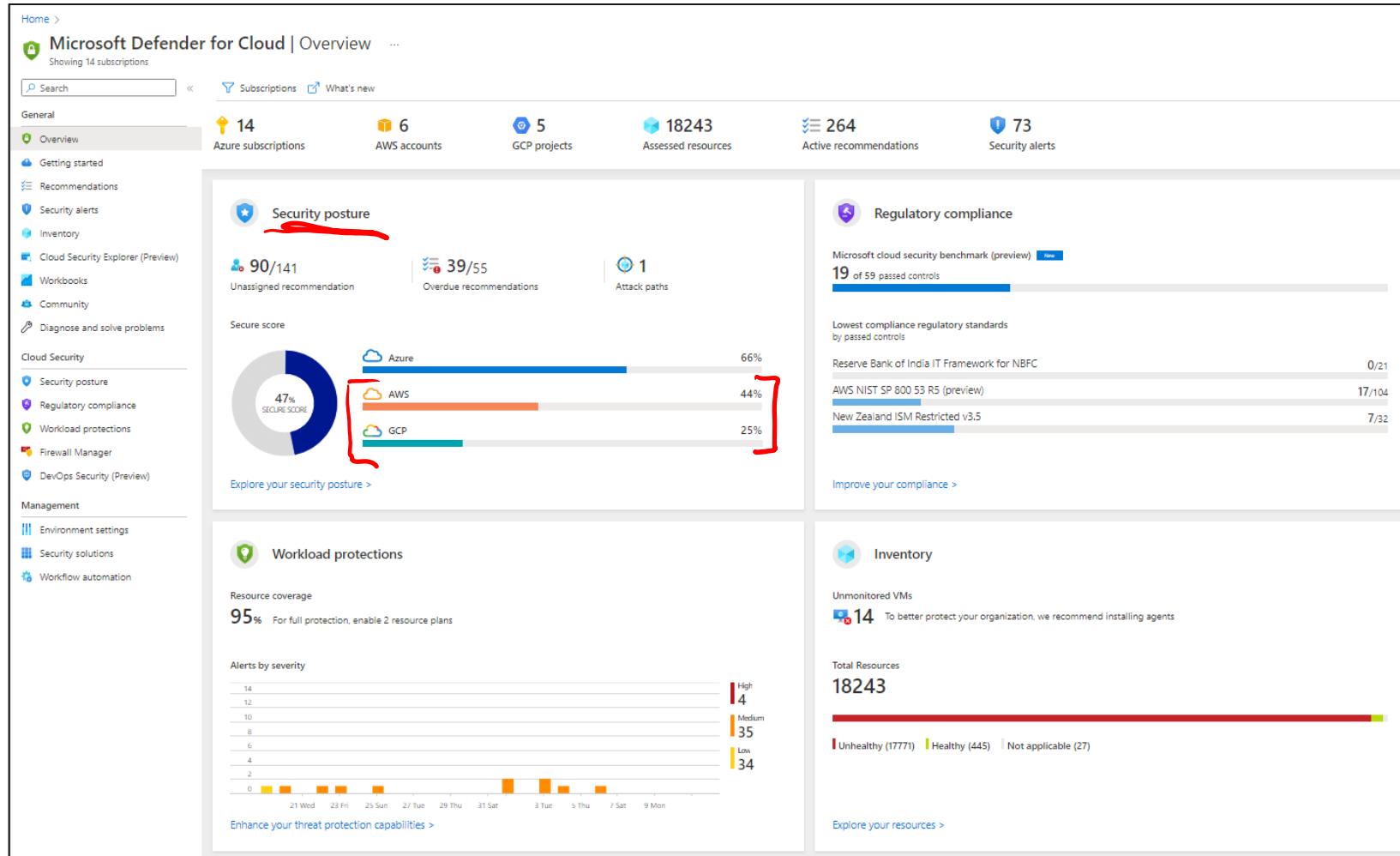
# Implement Microsoft Defender for Cloud

ARC

Microsoft Defender for Cloud is a Security Posture Management and Workload Protection Platform for Azure, on-premises, and multicloud (Amazon AWS and Google GCP) resources.

Microsoft Defender for Cloud's features covers the two broad pillars of cloud security:

1. Security Posture Management
2. Workload Protection



# Cloud security posture management (CSPM)

The cloud security posture management features provide the following:

- 1** Visibility - to help you understand your current security situation.
- 2** Hardening guidance - to help you efficiently and effectively improve your security.

Home > Microsoft Defender for Cloud

## Microsoft Defender for Cloud | Security posture

Secure score over time | Governance report | Guides & Feedback

**General**

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

**Azure environment**

**Secure score**

60% SECURE SCORE

**Environment**

- Management groups: 3
- Subscriptions: 1
- Unhealthy resources: 2/5
- Recommendations: 25

| Name  | Secure score | Unhealthy resources |
|---|--------------|---------------------|
| Tenant Root Group<br>Azure management group | 60%          | 2 of 5              |
| MCAPS-Root<br>Azure management group        | 60%          | 2 of 5              |

# Cloud workload protection (CWP)

1

Microsoft Defender  
for Cloud coverage

2

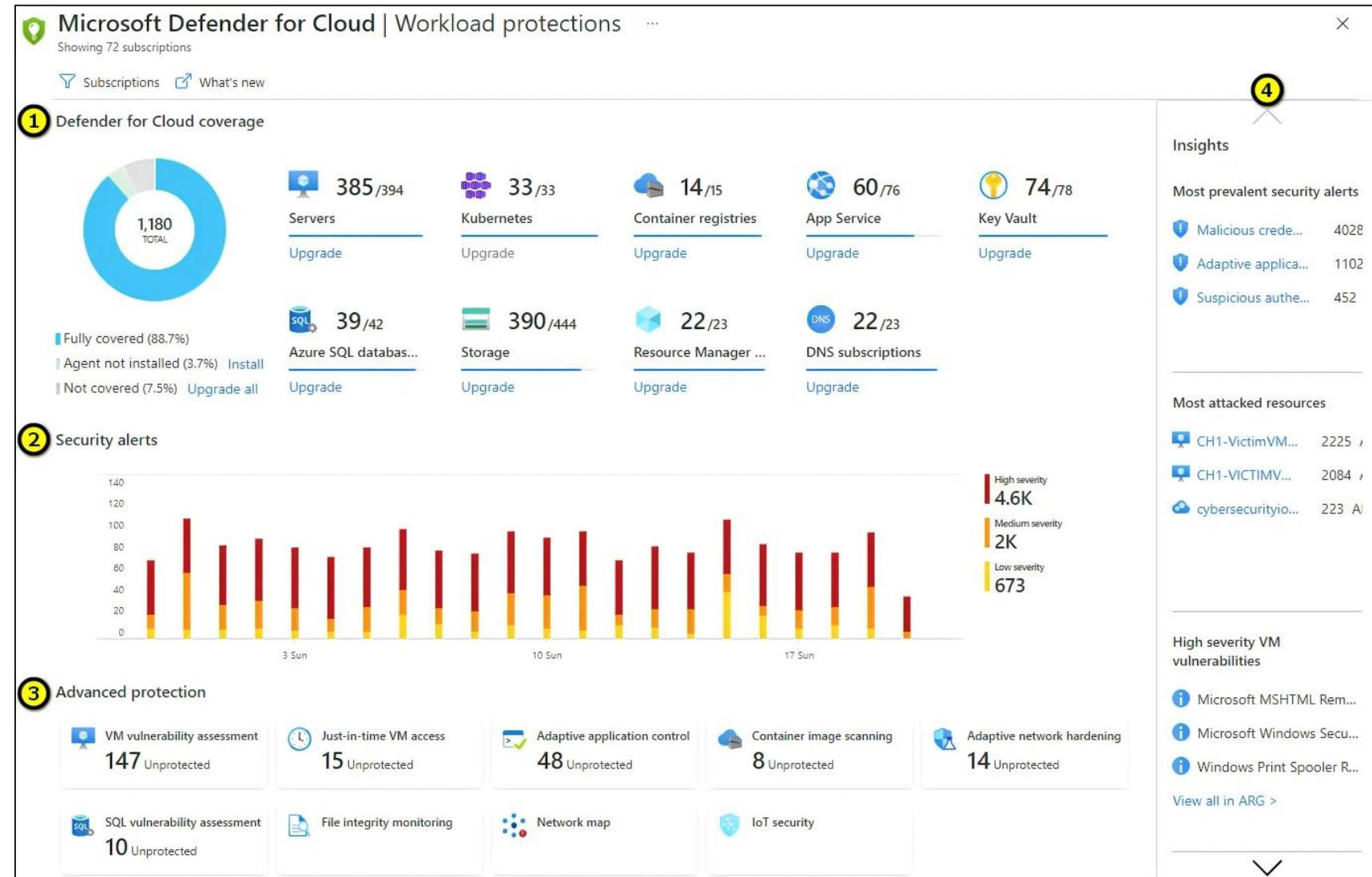
Security alerts

3

Advanced  
protection

4

Insights



# Basic security features

Defender for cloud offers **foundational** multicloud Cloud Security Posture Management (CSPM) capabilities for free and automatically enabled by default on any subscription or account that has onboarded to Defender for Cloud.

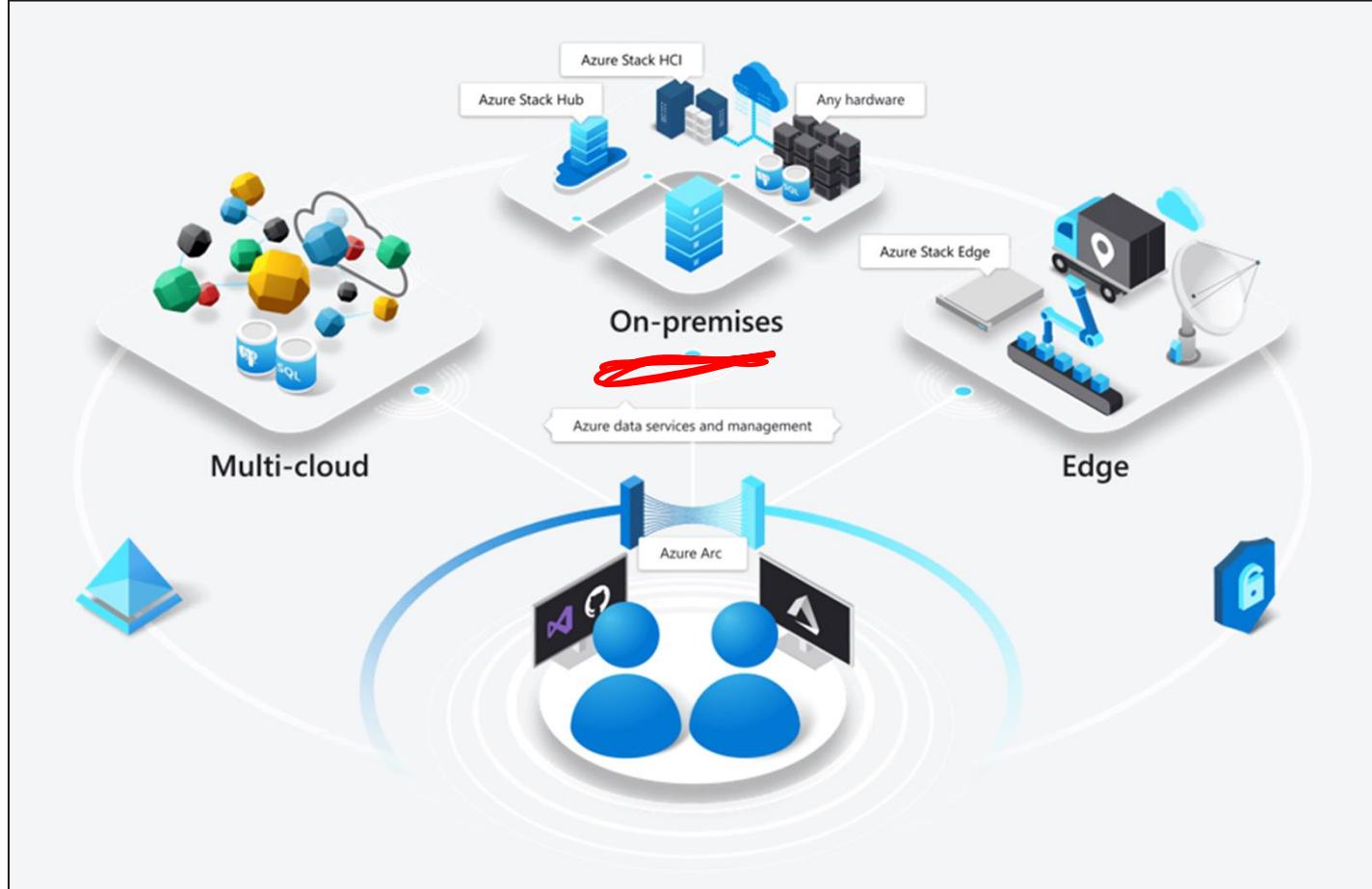
| Feature   | Foundational CSPM capabilities | Defender CSPM | Cloud availability           |
|---|--------------------------------|---------------|------------------------------|
| Continuous assessment of the security configuration of your cloud resources | ✓                              | ✓             | Azure, AWS, GCP, on-premises |
| Security recommendations to fix misconfigurations and weaknesses            | ✓                              | ✓             | Azure, AWS, GCP, on-premises |
| Secure score  | ✓                              | ✓             | Azure, AWS, GCP, on-premises |
| Governance  | —                              | ✓             | Azure, AWS, GCP, on-premises |
| Regulatory compliance   | —                              | ✓             | Azure, AWS, GCP, on-premises |
| Cloud security explorer   | —                              | ✓             | Azure, AWS                   |
| Attack path analysis  | —                              | ✓             | Azure, AWS                   |
| Agentless scanning for machines   | —                              | ✓             | Azure, AWS                   |

# Enhanced features

| Save  Settings & monitoring        |   |  |  |
|---|---|--|--|
|  Foundational CSPM                 | Free<br><a href="#">Details &gt;</a>  |  |  Full                                     |
|  Defender CSPM                     | Free (during preview)<br><a href="#">Details &gt;</a>   | N/A  |  Partial<br><a href="#">Settings &gt;</a> |
|  Servers                           | Plan 2 (\$15/Server/Month) <br><a href="#">Change plan &gt;</a>  | 1 servers                                  |  Partial<br><a href="#">Settings &gt;</a> |
|  App Service                       | \$15/Instance/Month <br><a href="#">Details &gt;</a>   | 0 instances                                |  Full                                     |
|  Databases                         | Selected: 4/4 <br><a href="#">Select types &gt;</a>  | Protected: 0/0 instances                   |  Full<br><a href="#">Settings &gt;</a>    |
|  Storage                           | \$0.02/10K transactions<br> <a href="#">New pricing plan available</a>  | 1 storage accounts                         |  Full                                     |
|  Containers                        | \$7/VM core/Month <br><a href="#">Details &gt;</a>   | 0 container registries; 0 kubernetes cores |  Partial<br><a href="#">Settings &gt;</a> |
|  Kubernetes (deprecated)           | \$2/VM core/Month    | 0 kubernetes cores                         |  Full                                     |
|  Container registries (deprecated) | \$0.29/Image  | 0 container registries                     |  Full                                     |
|  Key Vault                         | \$0.02/10k transactions<br><a href="#">Details &gt;</a>   | 1 key vaults                               |  Full                                     |
|  Resource Manager                | \$4/1M resource management operations <br><a href="#">Details &gt;</a>   |  |  Full                                   |
|  DNS                             | \$0.7/1M DNS queries <br><a href="#">Details &gt;</a>  |  |  Full                                   |

When you enable the **enhanced** security features (**paid**), Defender for Cloud can provide unified security management and threat protection across your cloud workloads.

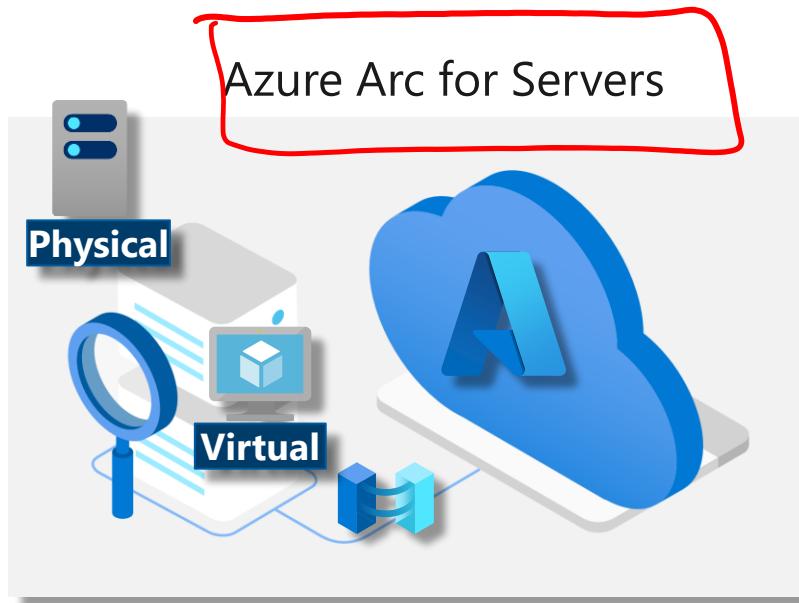
# Azure Arc



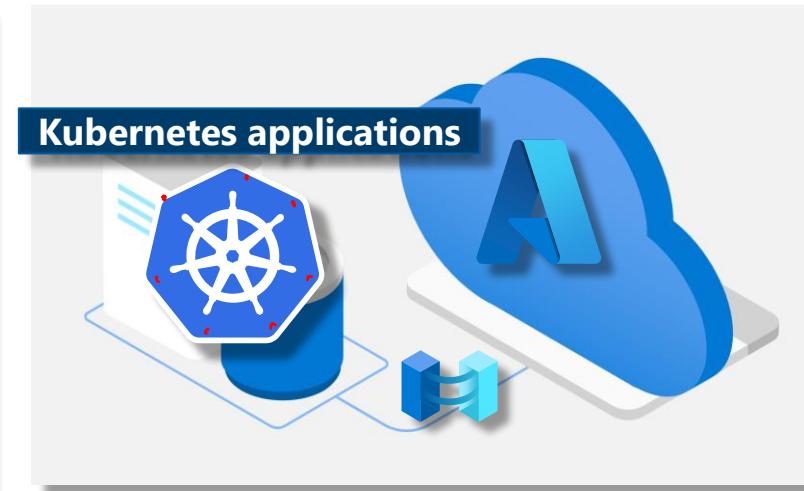
Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

# Azure Arc capabilities

Azure Arc for Servers



Azure Arc for Kubernetes



Azure data services on Azure Arc



Organize and govern servers across environments

Manage Kubernetes applications at-scale

Run data services anywhere



# Microsoft cloud security benchmark in Defender for Cloud

- The Microsoft cloud security benchmark (**MCSB**) provides best practices and recommendations, with input from a set of holistic Microsoft and industry security guidance that includes:



**Cloud Adoption Framework:** Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.



**Azure Well-Architected Framework:** Guidance on securing your workloads on Azure.



**The Chief Information Security Officer (CISO) Workshop:** Program guidance and reference strategies to accelerate security modernization using Zero Trust principles.



**Other industry and cloud service providers security best practice standards and framework:** Examples include the Amazon Web Services, Center for Internet Security Controls, National Institute of Standards and Technology, and the Payment Card Industry Data Security Standard.

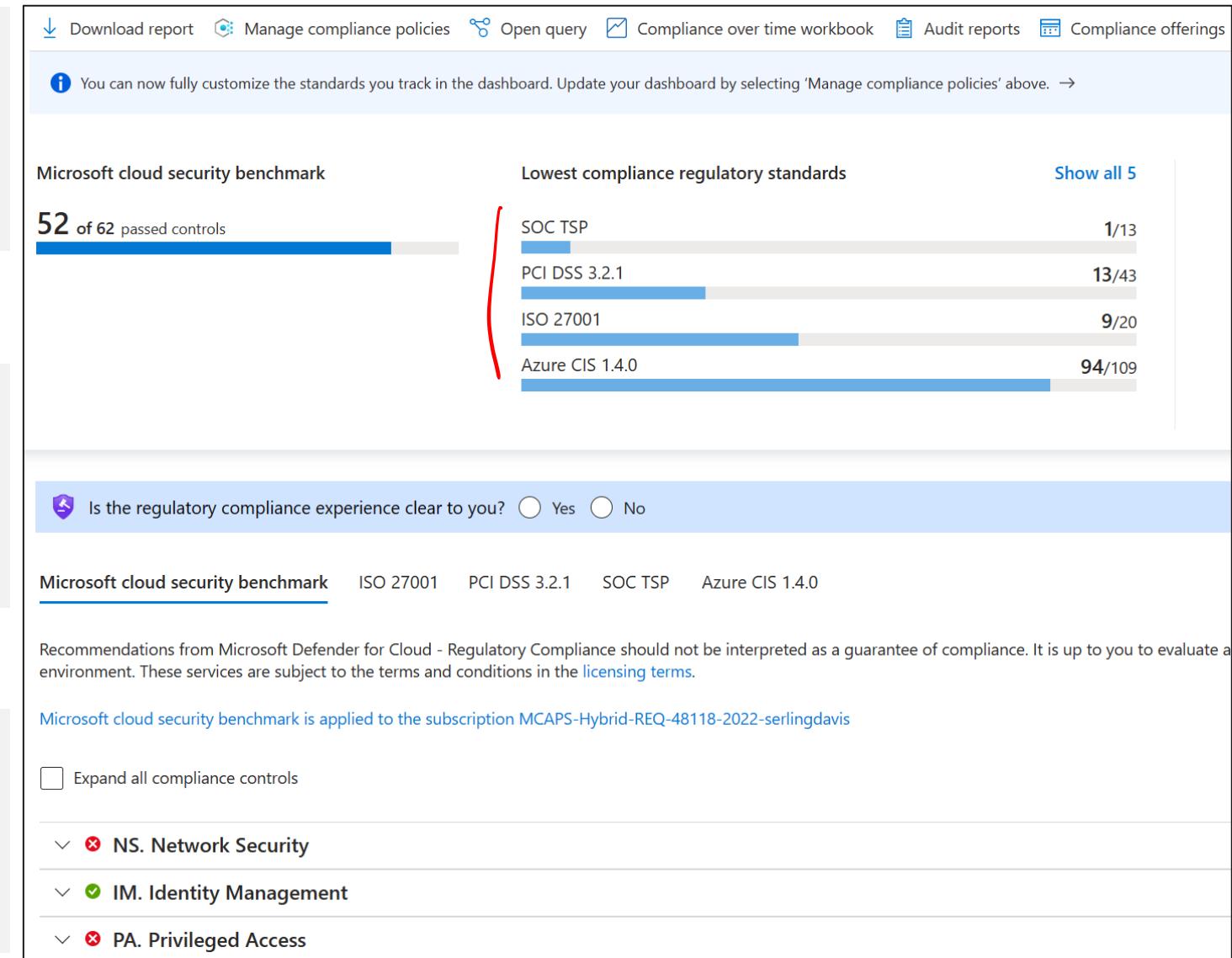
# Regulatory compliance dashboard

Microsoft Defender for Cloud streamlines the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard.

The compliance dashboard gives you a view of your overall compliance standing.

Security for non-Azure platforms follows the same cloud-neutral security principles as Azure.

Purview Portal

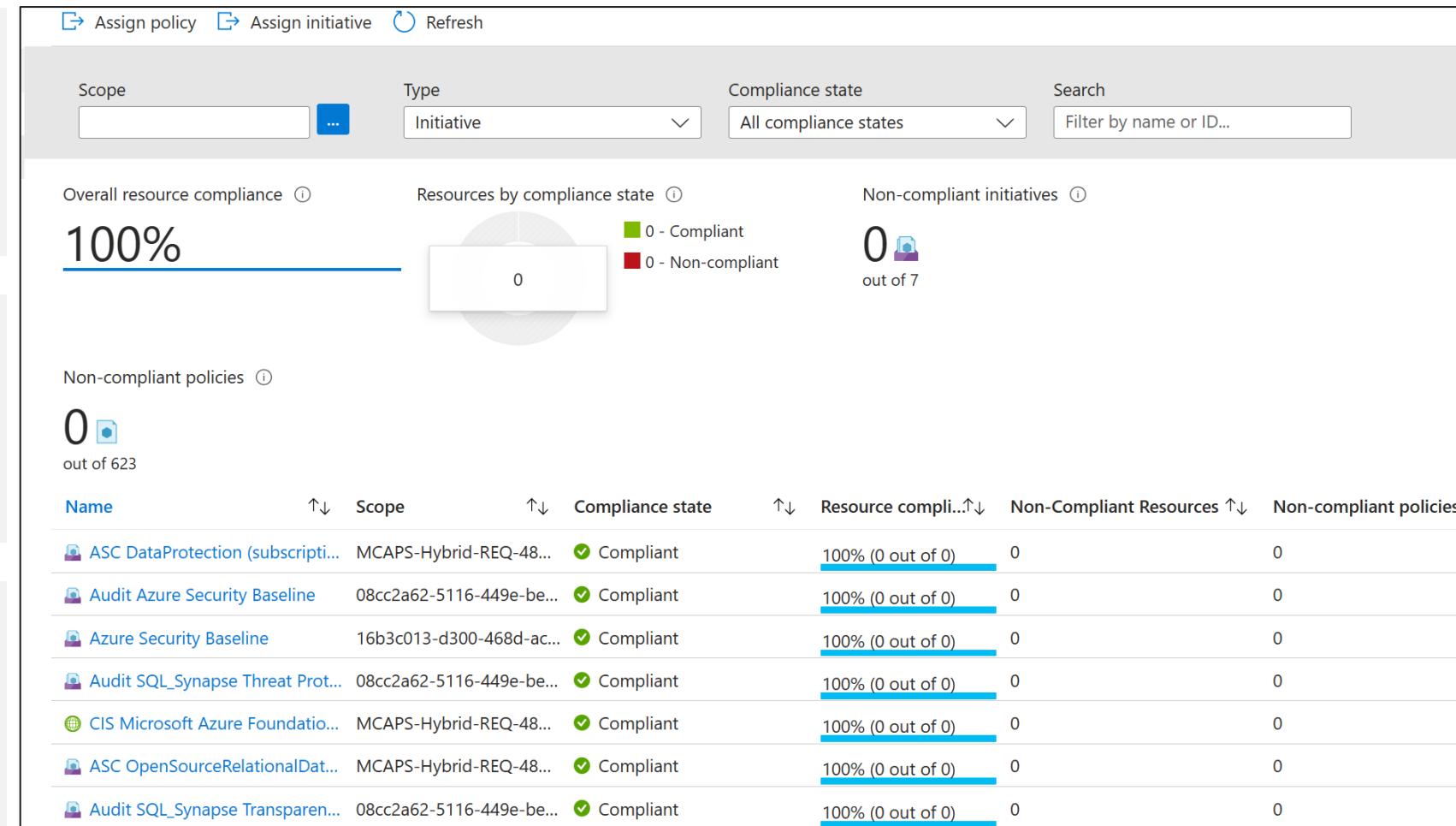


# What are security initiatives, and policies

Microsoft Defender for Cloud applies security initiatives to your subscriptions.

These initiatives contain one or more security policies.

Each of those policies results in a security recommendation for improving your security posture.



**Out of the box examples:** Microsoft Defender for Cloud > Environment settings > Subscription > Policy settings > Security policy

# What is a security initiative?

A Security initiative is a collection of Azure Policy definitions, or rules, that are grouped together towards a specific goal or purpose.

Security initiatives simplify management of your policies by grouping a set of policies together, logically, as a single item.

Home > Policy | Definitions >

## CIS Microsoft Azure Foundations Benchmark v1.1.0

Initiative Definition

[Assign](#) [Edit initiative](#) [Duplicate initiative](#) [Delete initiative](#)

[Essentials](#)

Name : CIS Microsoft Azure Foundations Benchmark v1.1.0  
Description : The Center for Internet Security (CIS) is a nonprofit entity whose mission is to 'identify, develop, validate, and publish consensus-based security benchmarks, methodologies, and tools to assist the information security community'.  
Category : Regulatory Compliance  
Version : 16.0.0

[Automated](#) [Definition](#) [Microsoft managed](#) [Assignments \(0\)](#) [Parameters](#)

Filter by reference ID, policy name... All effects All types

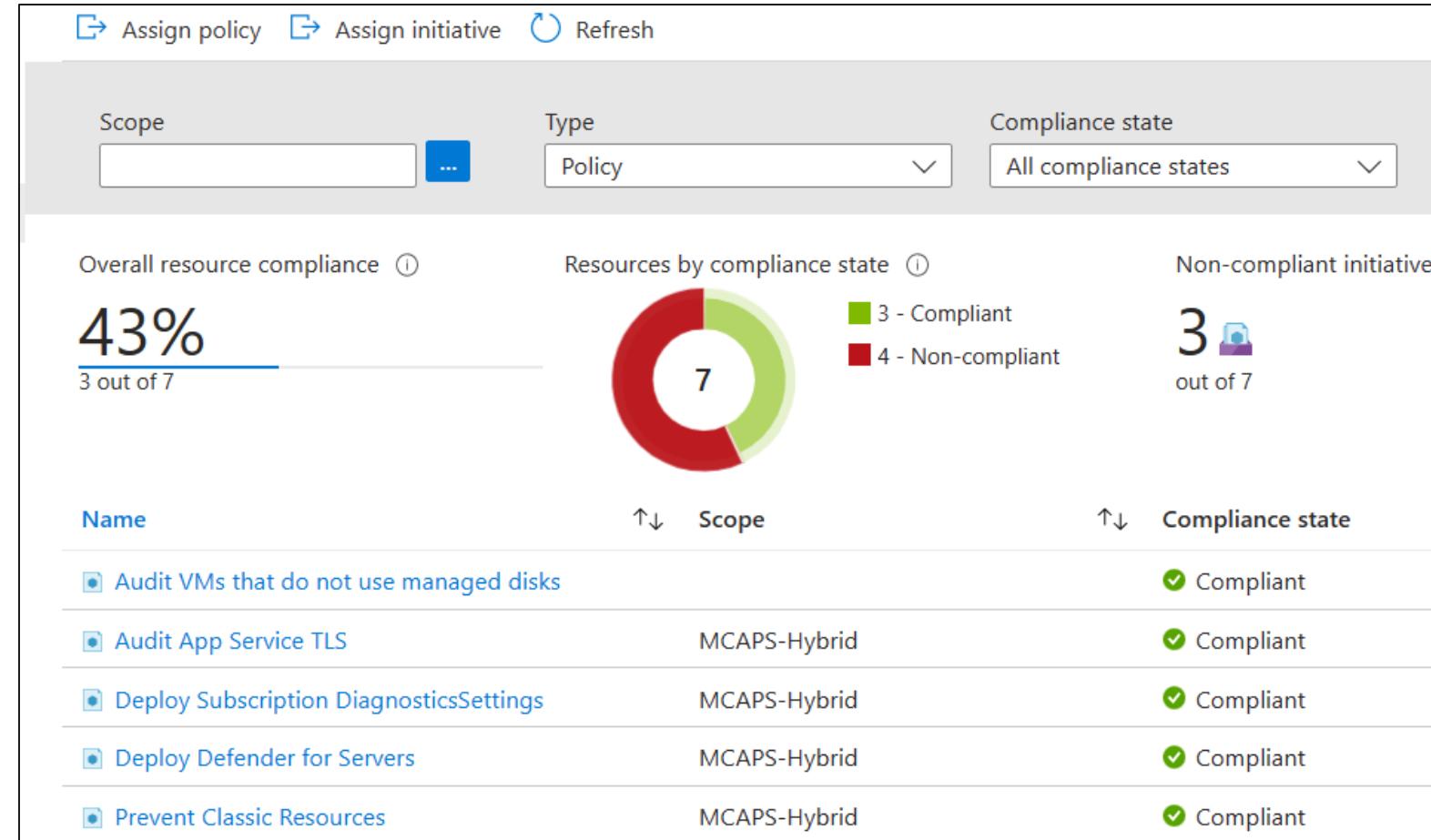
Policy ↑↓

- MFA should be enabled on accounts with owner permissions on your subscription
- MFA should be enabled for accounts with write permissions on your subscription
- MFA should be enabled on accounts with read permissions on your subscription
- External accounts with read permissions should be removed from your subscription
- External accounts with write permissions should be removed from your subscription
- External accounts with owner permissions should be removed from your subscription
- Azure Defender for servers should be enabled
- Azure Defender for Azure SQL Database servers should be enabled
- Azure Defender for Storage should be enabled
- Microsoft Defender for Containers should be enabled

# What is a security policy?

An Azure Policy definition, created in Azure Policy, is a rule about specific security conditions that you want controlled.

For example, controlling what type of resources can be deployed or enforcing the use of tags on all resources.



# Viewing and editing security policies

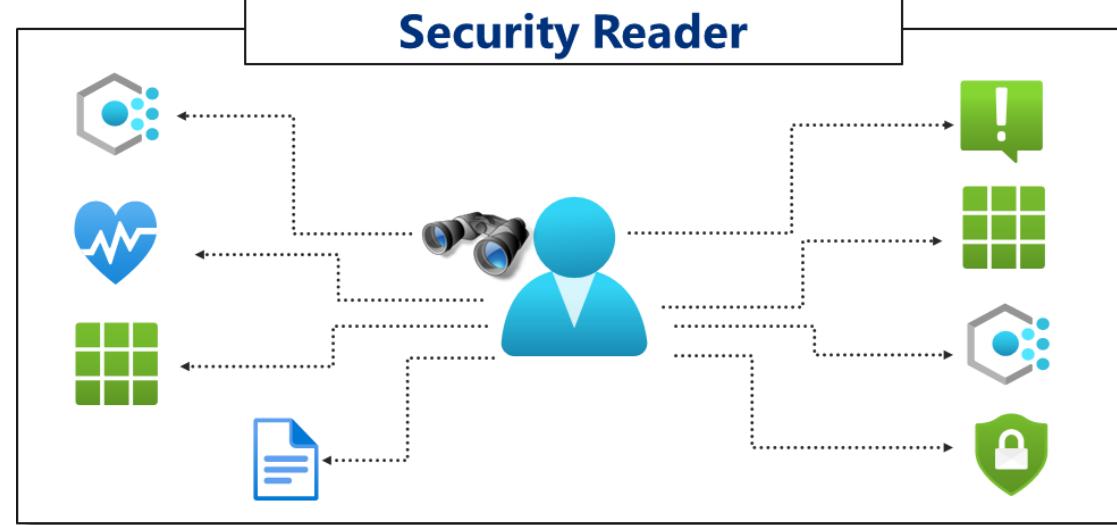
**View, Update, and Dismiss Alerts**

**Security Administrator**  
vs.  
**Security Reader**

**View Only**



**Security Reader**



# Recommendations

Using the policies, Defender for Cloud periodically analyzes the compliance status of your resources to identify potential security misconfigurations and weaknesses.

It then provides you with recommendations on how to remediate those issues.

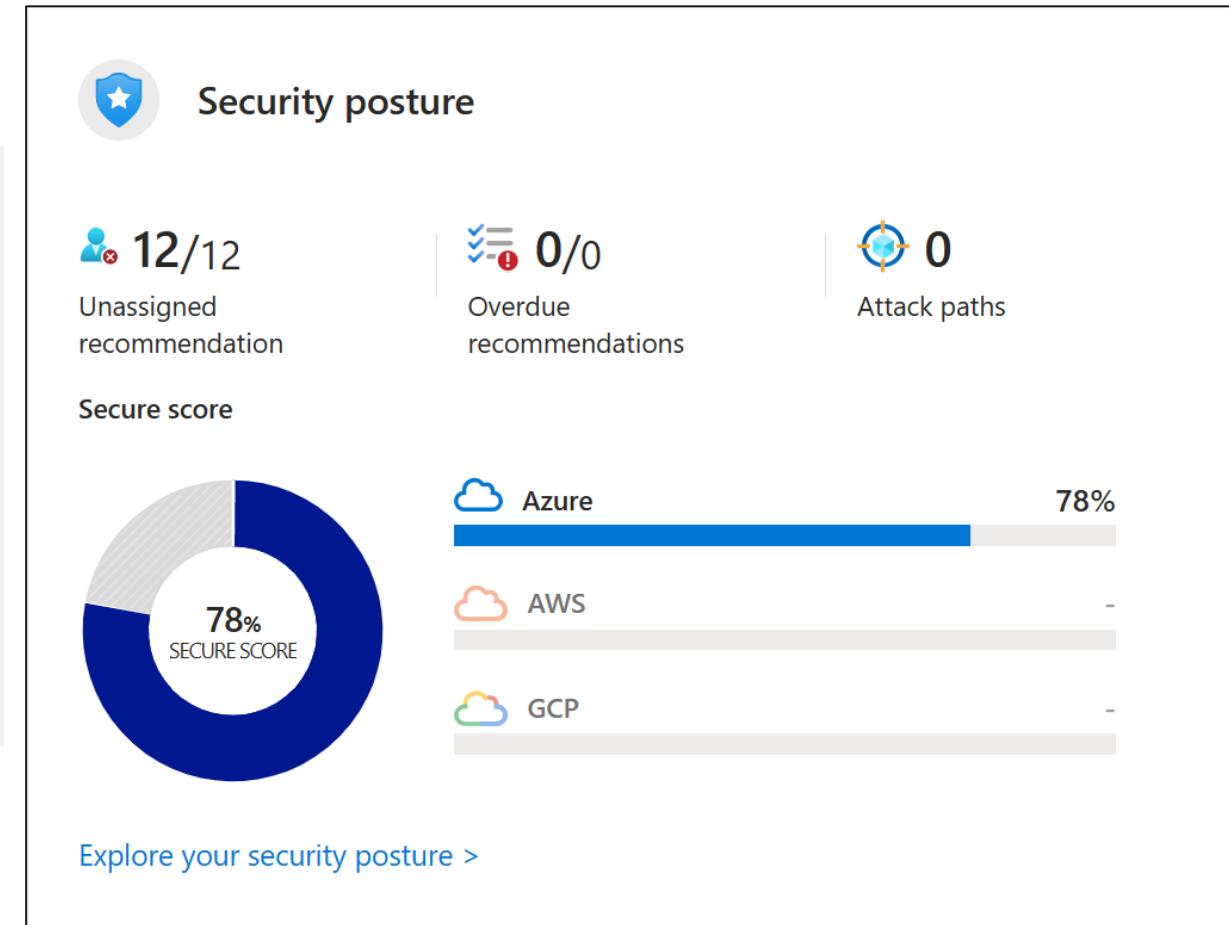
Recommendations result from assessing your resources against the relevant policies and identifying resources that aren't meeting your defined requirements.

| Secure score recommendations  |                | All recommendations  |
|---|----------------|--|
|  77% | Secure score ⓘ |  7/38<br>Active recommendations |
| <input type="text"/> Search recommendations   |                | Recommendation status == <b>None</b> <span>×</span>  |
| <span> ⓘ</span> Name ↑  |                | Max score ↓  |
| <span> &gt;</span> Enable MFA   |                | 10   |
| <span> &gt;</span> Secure management ports  |                | 8  |
| <span> &gt;</span> Remediate vulnerabilities  |                | 6  |
| <span> &gt;</span> Apply system updates   |                | 6  |
| <span> &gt;</span> Encrypt data in transit  |                | 4  |
| <span> &gt;</span> Manage access and permissions  |                | 4  |
| <span> &gt;</span> Enable encryption at rest  |                | 4  |
| <span> &gt;</span> Remediate security configurations                                    |                | 4  |
| <span> &gt;</span> Restrict unauthorized network access                                 |                | 4  |

# Secure Score

Microsoft Defender for Cloud has two main goals:

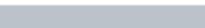
1. To help you understand your current security situation
2. To help you efficiently and effectively improve your security



# Improve your secure score

To improve your secure score, remediate security recommendations from your recommendations list.

You can remediate each recommendation manually for each resource or use the **Fix**  option (**when available**) to resolve an issue on multiple resources quickly.

| Unhealthy resources   | Insights  |
|---|---|
| 0 of 1 resources  |    |
| 0 of 1 resources  |    |
| 1 of 1 resources  |    |
|  1 of 1 virtual machines | <br>  |
|  0 of 1 virtual machines |    |
| 0 of 1 resources  |    |
| 0 of 1 resources  |    |
| 0 of 4 resources  |   |
| 1 of 1 resources  |    |

# Security controls

Recommendations are grouped into **security controls** and each control is a logical group of related security recommendations and reflects your vulnerable attack surfaces.

Your score only improves when you **remediate all of the recommendations** for a single resource within a control.

## Example: Security Controls

|  | Max score |
|--|-----------|
| ➤ Name ↑↓                              |           |
| ➤ Enable MFA                           | 10        |
| ➤ Secure management ports              | 8         |
| ➤ Remediate vulnerabilities            | 6         |
| ➤ Apply system updates                 | 6         |
| ➤ Encrypt data in transit              | 4         |
| ➤ Manage access and permissions        | 4         |
| ➤ Enable encryption at rest            | 4         |
| ➤ Remediate security configurations    | 4         |
| ➤ Restrict unauthorized network access | 4         |

# Define brute force attacks



Dea & Jit

vn1  
:3389 NSG  
:22 inbound

A Brute force attack is a type of **hacking technique** in which an attacker tries to gain access to a network or system by guessing the **username** and **password** combination through an automated process.



The attacker typically uses a **program** that generates a large number of login attempts in a short period of time to try every possible combination of characters until the correct one is discovered.



This type of attack can be very effective against **weak passwords** and security systems with no protection against brute force attacks, but it is time-consuming and can be detected by security measures such as account lockouts after a certain number of failed login attempts.

# Management services, ports, and protocols

- Typically, management services over **commonly used ports** are used when guessing passwords.

| Management Service  | Port and Protocol  |
|---|--|
| <b>SSH</b> (Secure Shell)   | 22 / TCP (Transmission Control Protocol)   |
| <b>Telnet</b> (Teletype Network)  | 23 / TCP (Transmission Control Protocol)   |
| <b>FTP</b> (File Transfer Protocol)   | 21 / TCP (Transmission Control Protocol)   |
| <b>NetBIOS</b> (Network Basic Input/Output System)/ <b>SMB</b> (Server Message Block)/ <b>Samba</b> | 139 and 445 / TCP (Transmission Control Protocol)                                      |
| <b>LDAP</b> (Lightweight Directory Access Protocol)   | 389 / TCP (Transmission Control Protocol)  |
| <b>Kerberos</b>   | 88 / TCP (Transmission Control Protocol)   |
| <b>RDP</b> (Remote Desktop Protocol)  | 3389 / TCP (Transmission Control Protocol)   |
| <b>HTTP/HTTP</b> (Hypertext Transfer Protocol) Management Services                                  | 80 and 443 / TCP (Transmission Control Protocol)                                       |
| <b>MSSQL</b> (Microsoft Structured Query Language)  | 1433 / TCP (Transmission Control Protocol)   |
| <b>Oracle</b>   | 1521 / TCP (Transmission Control Protocol)   |
| <b>MySQL</b> (My Structured Query Language)   | 3306 / TCP (Transmission Control Protocol)   |
| <b>VNC</b> (Virtual Network Computing)  | 5900 / TCP (Transmission Control Protocol)   |
| <b>SNMP</b> (Simple Network Management Protocol)  | 161 and 162 / UDP (User Datagram Protocol) / 162 / TCP (Transmission Control Protocol) |

# Brute force attack programs and use cases

- There are several types of brute force attack programs used by attackers, including:

| Types of Brute Force Attack Programs and Use Case |   |
|---|---|
| Password crackers                                 | used for guessing passwords and encryption keys.    |
| Port scanners                                     | used to identify open ports on a network or system. |
| Network mappers                                   | used to map the topology of a network.              |
| Web application servers                           | used to test web applications for vulnerabilities.  |
| SSH brute force tools                             | used to guess SSH login credentials.                |
| Remote desktop brute force tools                  | used to guess RDP login credentials.                |
| FTP brute force tools                             | used to guess FTP login credentials.                |
| SNMP brute force tools                            | used to guess SNMP community strings.               |

- These programs can be used individually or in combination to launch a successful brute force attack on a target network or system.

# Indications of an attack

Extreme counts of **failed sign-ins** from many unknown usernames.

Never previously “**successfully authenticated**” from multiple remote desktop protocol (RDP) connections or from new source IP addresses.

Potential SQL Brute Force attempt [Sample alert](#)

High Severity | Active Status | 10/25/22, 03:32 PM (UTC-5...) Activity time

[Copy alert JSON](#)

**Alert description**  
THIS IS A SAMPLE ALERT: Someone is attempting to brute force credentials to your SQL server 'Sample-SQL'.

**Affected resource**

Sample-DB **Example: Alert**

Visual Studio Enterprise Subscription Subscription

**MITRE ATT&CK® tactics** ⓘ

- Pre-attack

[View full details](#) [Take action](#)

# Practices to blunt a Brute Force Attacks

To counteract brute-force attacks, you can take multiple measures such as:

1. Disable the public IP address and use one of these connection methods:
  - a. Use a **point-to-site** virtual private network (VPN)
  - b. Create a **site-to-site** VPN
  - c. Use **Azure ExpressRoute** to create secure links from your on-premises network to Azure
2. Require two-factor authentication
3. Increase password length and complexity. (i.e., **Ztyn%9\*qvB**)
4. Limit login attempts
5. Implement Completely Automated Public Turing test "**CAPTCHA**"
6. Limit the amount of time that the ports are open.

# Understanding just-in-time (JIT) VM access (example)

Home > Microsoft Defender for Cloud | Workload protections >

## Just-in-time VM access

Last week

Some of your subscriptions don't have Defender for Cloud's full protections enabled. To upgrade those subscriptions, click here. →

- > What is just-in-time VM access?
- > How does it work?

### Virtual machines

Configured   Not Configured   Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

1 VMs

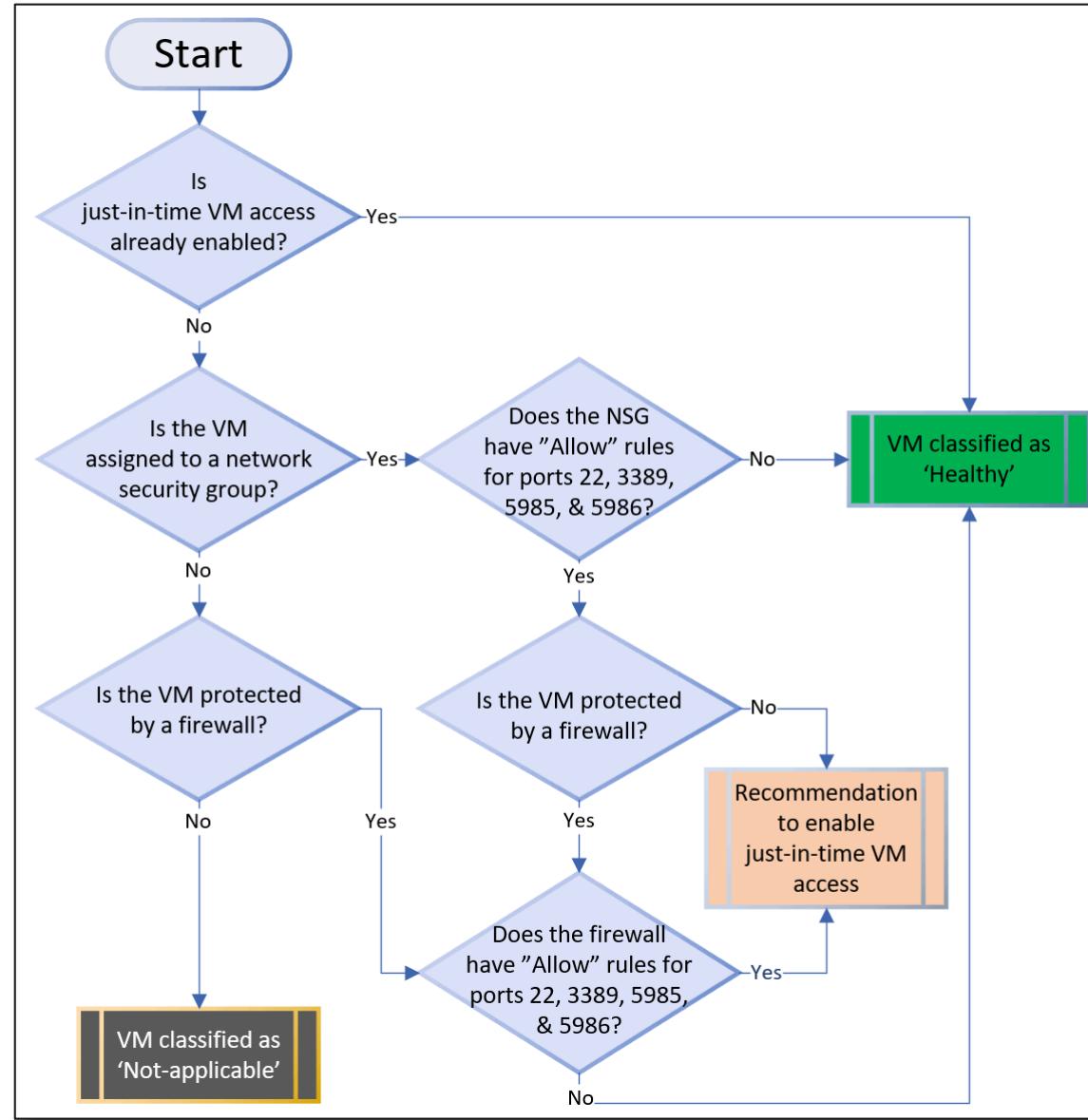
Request access

Search to filter items...

| Virtual machine ↑↓   | Approved ↑↓ | Last access ↑↓ | Connection details  | Last user ↑↓ | ... |
|--|-------------|----------------|---|--------------|-----|
| <input type="checkbox"/>  romebuild | 0 Requests  | N/A            |  - | N/A          | ... |

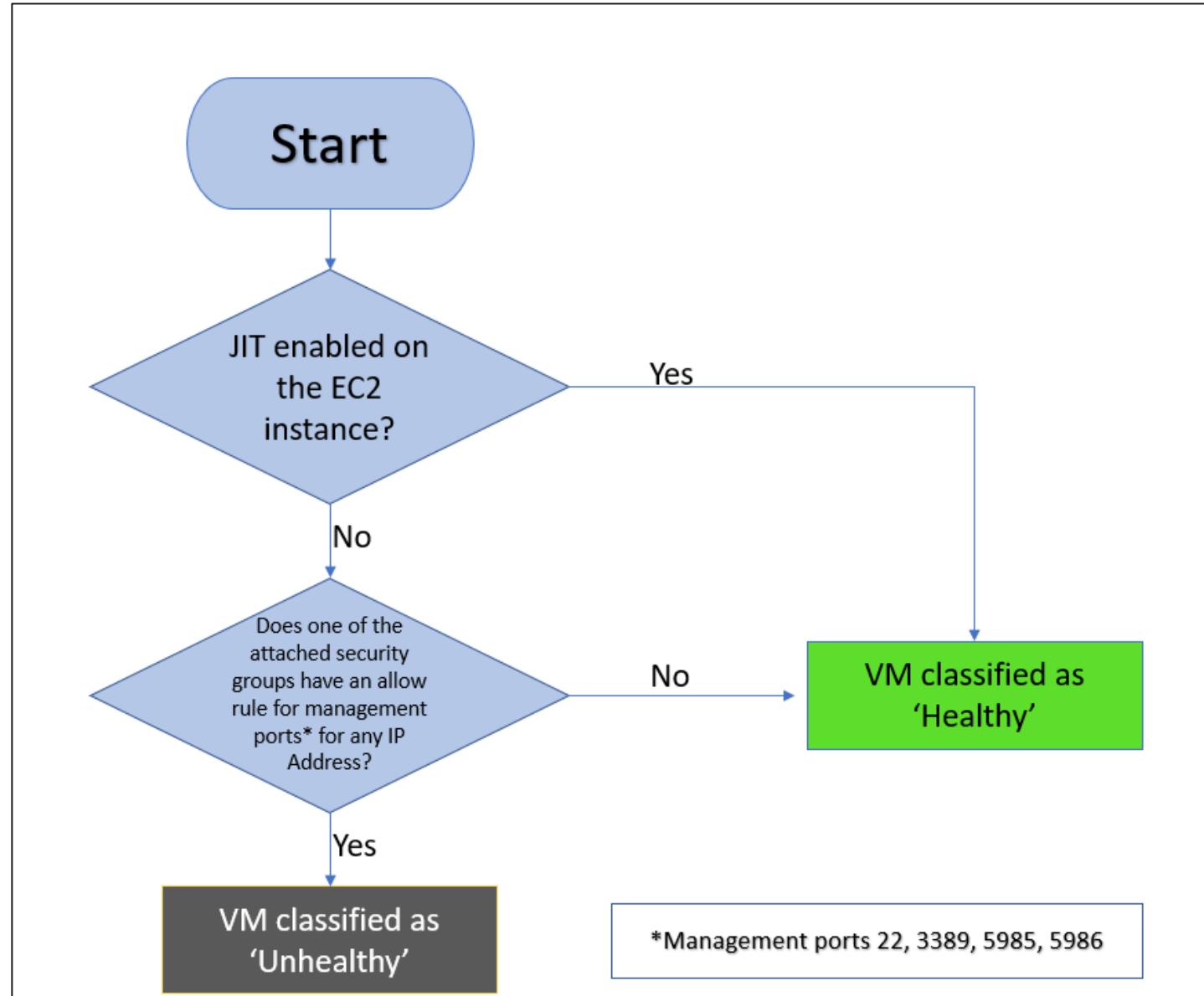
# Just-in-time VM is enabled an Azure Virtual Machine

Example: Azure Virtual Machine



# Just-in-time VM is enabled on the AWS EC2 Instance

**Example: AWC EC2 Instance**



# Added to the recommendation's Unhealthy resources tab

When Defender for Cloud finds a machine that can benefit from JIT, it adds that machine to the recommendation's Unhealthy resources tab.

Dashboard > Microsoft Defender for Cloud | Recommendations >

## Management ports of virtual machines should be protected with just-in-time network access control

**Description**  
Microsoft Defender for Cloud has identified some overly-permissive inbound rules for management ports in your Network Security Group. Enable just-in-time access control to protect your VM from internet-based brute-force attacks. [Learn more](#).

**Remediation steps**

**Affected resources**

**Example: Affected resources**

Unhealthy resources (78)    Healthy resources (112)    Not applicable resources (66)

| Name           | Subscription      |
|----------------|-------------------|
| ContosoWeb2    | Contoso IT - demo |
| ContosoWeb1    | Contoso IT - demo |
| ContosoSQLSrv3 | Contoso IT - demo |
| ContosoSQLSrv3 | Contoso IT - demo |
| ContosoSQLSrv2 | Contoso IT - demo |

# Implement Just-in-time VM access

- Just-in-time (JIT) virtual machine (VM) access is used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

A

To use Just-in-Time VM access, you must **enable** Microsoft Defender for Cloud.



After you enable Defender, you can view which virtual machines have JIT configured.

The screenshot shows the Microsoft Defender for Cloud Overview page. A red circle labeled '1' highlights the top navigation bar. A red circle labeled '2' highlights the 'Workload protections' section. A red circle labeled '3' highlights the 'Just-in-time VM access' section, which displays '2 Unprotected' VMs.

The screenshot shows the 'Virtual machines' page under the 'Not Configured' tab. It lists two VMs: SGVM1 and SGMME, both of which are protected by NSGs allowing access to management ports. A red circle labeled '4' highlights a button labeled 'Enable JIT on 2 VMs' with a hand cursor icon.

| Virtual machine | Resource group | Subscription Name                     | Severity | Reason   |
|-----------------|----------------|---------------------------------------|----------|--|
| SGVM1           | DALLASVDC1A    | Visual Studio Enterprise Subscription | High     | This VM is protected by an NSG that allows access to management ports. |
| SGMME           | DALLASVDC1A    | Visual Studio Enterprise Subscription | High     | This VM is protected by an NSG that allows access to management ports. |

# Implement Just-in-time VM access (continued)



For each virtual machine, you are provided with a list of recommended specific ports and access.



You can save the recommendations or Add other ports of your choosing.

Home > Microsoft Defender for Cloud > Just-in-time VM access >

## JIT VM access configuration

5GVM1, 5GMME

5

+ Add Save Discard

Configure the ports for which the just-in-time VM access will be applicable

| Port               | Protocol | Allowed source IPs | IP range | Time range (hours) | ... |
|--------------------|----------|--------------------|----------|--------------------|-----|
| 22 (Recommended)   | Any      | Per request        | N/A      | 3 hours            | ... |
| 3389 (Recommended) | Any      | Per request        | N/A      | 3 hours            | ... |
| 5985 (Recommended) | Any      | Per request        | N/A      | 3 hours            | ... |
| 5986 (Recommended) | Any      | Per request        | N/A      | 3 hours            | ... |

## Add port configuration

Port \*

Protocol  Any  TCP  UDP

Allowed source IPs  Per request  CIDR block

IP addresses

Max request time

3 (hours)

Discard OK

# Implement Just-in-time VM access (continued)

E

Once everything is in place, users must request access to the virtual machine.



You can also monitor the usage of each virtual machine.

**Virtual machines**

Configured   Not Configured   Unsupported

VMs for which the just-in-time VM access control is already in place. Presented data is for the last week.

**2 VMs**

Search to filter items...

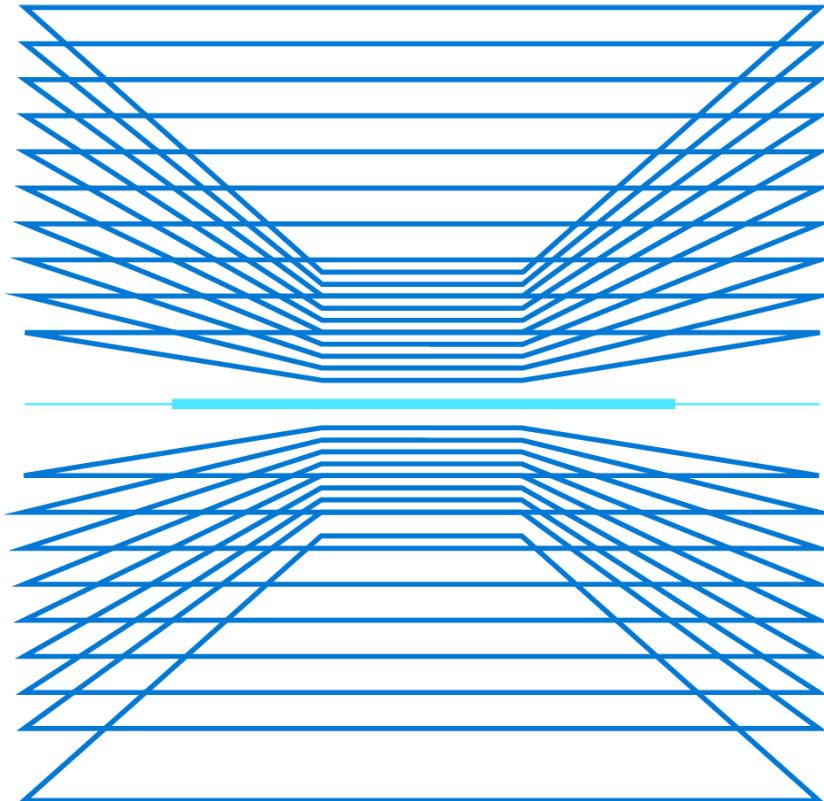
| Virtual machine ↑↓ | Approved ↑↓ | Last access ↑↓ | Connection details | Last user ↑↓ |
|--------------------|-------------|----------------|--------------------|--------------|
| 5GVM1              | 0 Requests  | N/A            | -                  | N/A          |
| 5GMME              | 0 Requests  | N/A            | -                  | N/A          |

**Request access**

6

# Demonstration: Microsoft Defender for Cloud

- Review Microsoft Defender for Cloud recommendations
- Review Microsoft Defender for Cloud security policies
- Review Microsoft Defender for Cloud regulatory compliance



# Additional Study – Microsoft Defender for Cloud

## Module Review Questions



## Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

Resolve security threats with Microsoft Defender for Cloud (Exercise)

Protect your servers and VMs from brute-force and malware attacks with Microsoft Defender for Cloud (Exercise)

Identify security threats with Microsoft Defender for Cloud

Top 5 security items to consider before pushing to production

# Microsoft Sentinel



# Microsoft Sentinel



Microsoft Sentinel

---



Data Connections

---



Workbooks

---



Incidents

---



Playbooks

---



Hunting

Splunk

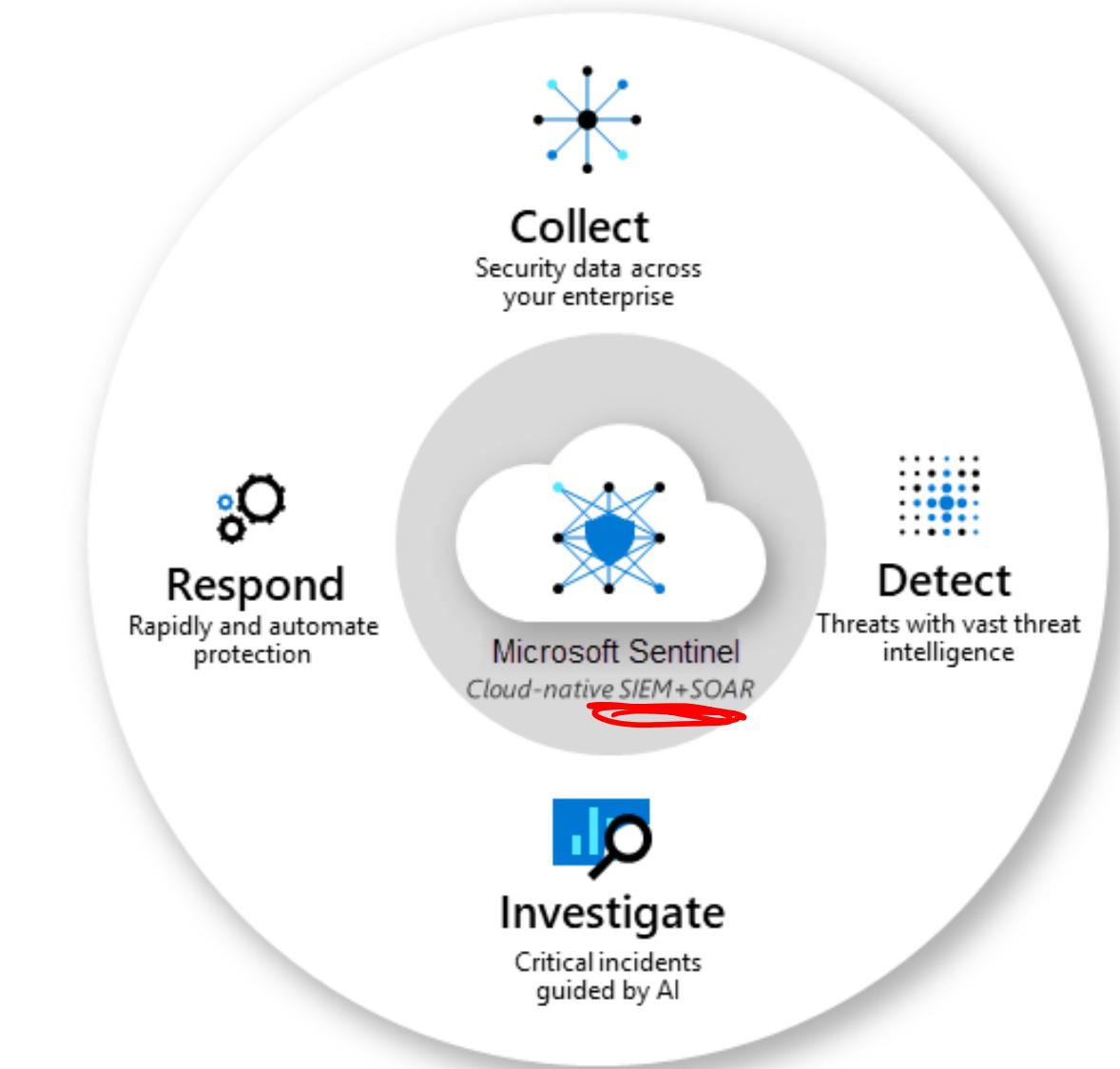
# Microsoft Sentinel

Collect data at cloud scale across all users, devices, applications, and infrastructure

Detect threats, and minimize false positives

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale

Respond to incidents rapidly with built-in orchestration and automation of common tasks



# Data Connections

Microsoft Sentinel comes with many connectors for Microsoft solutions that are available out of the box and provide real-time integration.

Microsoft sources like Microsoft 365 Defender, Microsoft Defender for Cloud, Office 365, Microsoft Defender for IoT.

Azure service sources like Azure Active Directory, Azure Activity, Azure Storage, Azure Key Vault, Azure Kubernetes service, and more.

The screenshot shows the Microsoft Sentinel Data connectors page. At the top, it displays 'Selected workspace: 'msftwrkspc1a''. Below this is a search bar and a sidebar with navigation links: General (Overview (Preview), Logs, News & guides, Search), Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview)), Content management (Content hub (Preview), Repositories (Preview), Community), and Configuration. On the right, the main area shows a summary: '126 Connectors' with '0 Connected' (circled in red). A 'Search by name or provider' bar is at the top, and filters for 'Providers : All', 'Data Types : All', and 'Status : All' are below. A 'More content at Content hub' link is also present. The list of connectors includes:

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

# Workbooks

After you onboard to Microsoft Sentinel, monitor your data by using the integration with Azure Monitor workbooks.

Microsoft Sentinel allows you to create custom workbooks across your data.

Microsoft Sentinel also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source.

The screenshot shows the Microsoft Sentinel Workbooks interface. At the top, there's a navigation bar with 'Home > Microsoft Sentinel > Microsoft Sentinel' and a search bar. Below the navigation is a header with 'Microsoft Sentinel | Workbooks' and 'Selected workspace: "cybersoc-demo"'. It features three summary cards: '1 Saved workbooks', '90 Templates', and '0 Updates'. On the left, a sidebar has sections for 'General' (Overview, Logs, News & guides), 'Threat management' (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence (Preview)), and 'Configuration' (Data connectors, Analytics, Watchlist (Preview), Automation, Community, Settings). The main area is titled 'My workbooks' and 'Templates'. It lists several templates with icons and names: 'AI Analyst Darktrace Model Breach Summary' (DARKTRACE), 'AI Vectra Detect' (VECTRA AI), 'Alsid for AD | Indicators of Exposure' (ALSID), 'Analytics Efficiency' (MICROSOFT), 'ASC Compliance and Protection' (MICROSOFT SENTINEL COMMUNITY), 'AWS Network Activities' (MICROSOFT), 'AWS User Activities' (MICROSOFT), and 'Azure Activity'. A callout box highlights 'Required data types: SecurityAlert, SecurityIncident'. To the right, a panel titled 'Analytics Efficiency' (MICROSOFT) provides insights into analytics rule efficacy. At the bottom right are 'View template' and 'Save' buttons.

# Incidents

To help you reduce noise and minimize the number of alerts you have to review and investigate, Microsoft Sentinel uses analytics to correlate alerts into incidents.

Incidents are groups of related alerts that together indicate an actionable possible-threat that you can investigate and resolve.

Use the built-in correlation rules as-is, or use them as a starting point to build your own.

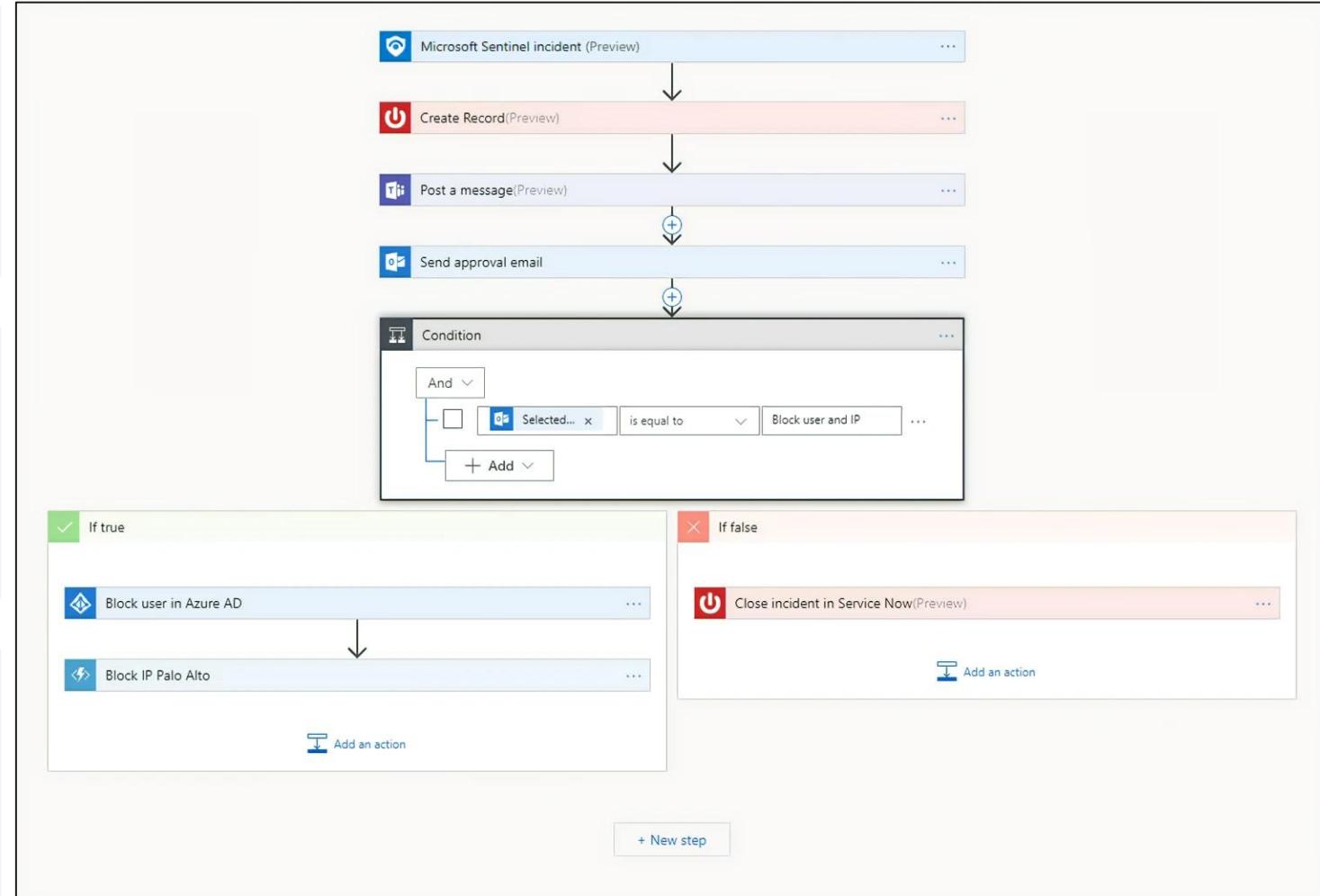
The screenshot shows the Microsoft Sentinel Incidents page. At the top, it displays summary counts: 403 Open incidents, 400 New incidents, and 3 Active incidents. Below this is a chart titled "Open incidents by severity" showing the distribution across High (82), Medium (95), Low (207), and Informational (19) levels. The main area is a table of incidents with columns for Severity, Status, Incident ID, Title, Alerts, Product names, and Created time. One specific incident is highlighted with a red border: "Authentication Methods Changed for Privileged Acc..." (Incident ID: 203443). The details pane on the right shows the incident's properties: Unassigned Owner, New Status, and High Severity. It also includes sections for Description (identifying authentication methods being changed for a privileged account), Alert product names (Microsoft Sentinel), Evidence (1 Events, 1 Alerts, 0 Bookmarks), Last update time (05/11/22, 12:50 PM), Creation time (05/11/22, 12:49 PM), Entities (2), Tactics and techniques, and links to View full details and Actions.

# Playbooks

Automate your common tasks and simplify security orchestration with playbooks that integrate with Azure services and your existing tools.

Playbooks automate and simplify tasks, including data ingestion, enrichment, investigation, and remediation.

Playbooks work best with single, repeatable tasks, and don't require coding knowledge.



# Hunting

Microsoft Sentinel's search-and-query tool, is based on the MITRE framework, which enables you to hunt for security threats across your organization's data sources, before an alert is triggered.

Create custom detection rules based on your hunting query.

Surface insights as alerts to your security incident responders.

The screenshot displays the Microsoft Sentinel - Hunting interface within the Microsoft Azure portal. The left sidebar shows navigation options like Overview, Logs, Threat management, Cases, Dashboards, User profiles (Coming soon), and Hunting (which is selected). The main area shows a summary of 19 Total Queries and 106 Total Results. Below this, a table lists various hunting queries with columns for QUERY, DESCRIPTION, PROVIDER, DATA SOURCE, RELEVANCE, and TACTICS. Each row includes a star icon and a detailed description. To the right, there are sections for 'New processes observed in last 24 hours' (provider: Microsoft, 103 results, SecurityEvent Data Source) and 'Query Information' (with a code snippet for a specific query). At the bottom, there are 'Entities' and 'Tactics Execution' sections, and a 'Run Query' button.

Microsoft Azure

Home - Microsoft Sentinel - Hunting  
Selected workspace: 'CyberSecurityDemo' - PREVIEW

Search (Ctrl+)

General

Overview

Logs

Threat management

Cases

Dashboards

User profiles (Coming soon)

Hunting

Configuration

Getting started

Data collection

Security analytics

Playbooks

Community

Workspace Settings

19 Total Queries

106 Total Results

Queries

| QUERY  | DESCRIPTION  | PROVIDER  | DATA SOURCE    | RELEVANCE | TACTICS          |
|--|--|-----------|----------------|-----------|------------------|
| New processes observed in last 24 hours            | Shows new processes observed in the last 24 hours.                             | Microsoft | SecurityEvent  | 103       | ... (with icons) |
| Azure AD signins from new locations                | New AzureAD signin locations today versus previous 24 hours.                   | Microsoft | SignInLogs     | 3         | ... (with icons) |
| Processes executed from binaries hidden in base64  | Process executed from binary hidden in Base64 encoded PE files header section. | Microsoft | SecurityEvent  | 0         | ... (with icons) |
| Processes executed from base-encoded binaries      | Finding base64 encoded PE files header section.                                | Microsoft | SecurityEvent  | 0         | ... (with icons) |
| Anomalous Azure AD apps based on activity          | This query over Azure AD sign-in activity highlights anomalous apps.           | Microsoft | SignInLogs     | 0         | ... (with icons) |
| Summary of users creating new user accounts        | New user accounts may be an attacker profile.                                  | Microsoft | OfficeActivity | ...       | ... (with icons) |
| User and Group enumeration                         | The query finds attempts to list users or groups.                              | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Summary of failed user logons by reason            | A summary of failed logons can be used to identify potential attacks.          | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Hosts with new logons                              | Shows new accounts that have logged onto the host.                             | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Malware in the recycle bin                         | Finding attackers hiding malware in the recycle bin.                           | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Masquerading files                                 | Malware writers often use windows system files.                                | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Accounts and User Agents associated with a user    | Summary of users/user agents associated with a specific user account.          | Microsoft | OfficeActivity | ...       | ... (with icons) |
| Office365 authentications                          | Shows authentication volume by user agent.                                     | Microsoft | OfficeActivity | ...       | ... (with icons) |
| Summary of users created using uncommon file paths | Summarizes users of uncommon & undocumented file paths.                        | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Powershell downloads                               | Finds PowerShell execution events that could indicate malicious activity.      | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Script usage summary (cscript.exe)                 | Daily summary of vbs scripts run across the organization.                      | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Sharepoint downloads                               | Shows volume of documents uploaded to SharePoint.                              | Microsoft | OfficeActivity | ...       | ... (with icons) |
| Uncommon processes/files - bottom 1%               | Shows the rarest processes seen running on the host.                           | Microsoft | SecurityEvent  | ...       | ... (with icons) |
| Summary of user logons by logon type               | Comparing successful and nonsuccessful logons.                                 | Microsoft | SecurityEvent  | ...       | ... (with icons) |

New processes observed in last 24 hours

Microsoft provider 103 results SecurityEvent Data Source

Description

Show new processes observed in the last 24 hours versus the previous 30 days. These new processes could be benign new programs installed on hosts; however, especially in normally stable environments, these new processes could provide an indication of an unauthorized/malicious binary that has been installed and run. Reviewing the wider context of the logon sessions in which these binaries ran can provide a good starting point for identifying possible attacks.

Query Information

```
let start=datetime("2019-02-23T10:41:10.127Z");
let end=datetime("2019-02-24T10:41:10.127Z";
let processEvents=SecurityEvent
| where TimeGenerated > start and TimeGenerated < end
| where EventId==4688
| project TimeGenerated, ComputerName=Computer, Acco
```

View query result >

Entities

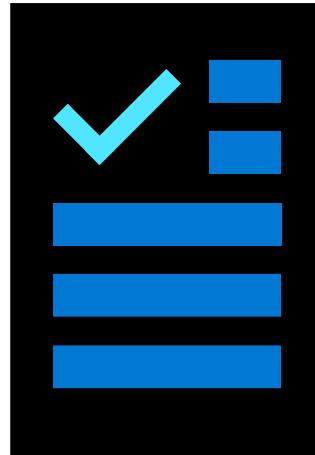
Tactics Execution

The execution tactic represents techniques that result in the execution of adversary-controlled code on a local or remote system.  
read more...

Run Query

# Additional Study – Microsoft Sentinel

Module Review Questions



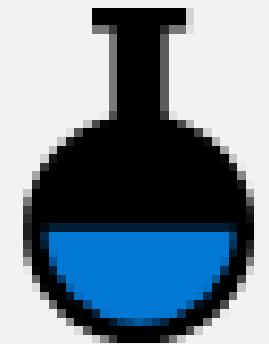
Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

Introduction to threat modeling

Use a framework to identify threats and find ways to reduce or eliminate risk

Create a threat model using data-flow diagram elements

# Module Labs



# Lab 13 – Azure Monitor

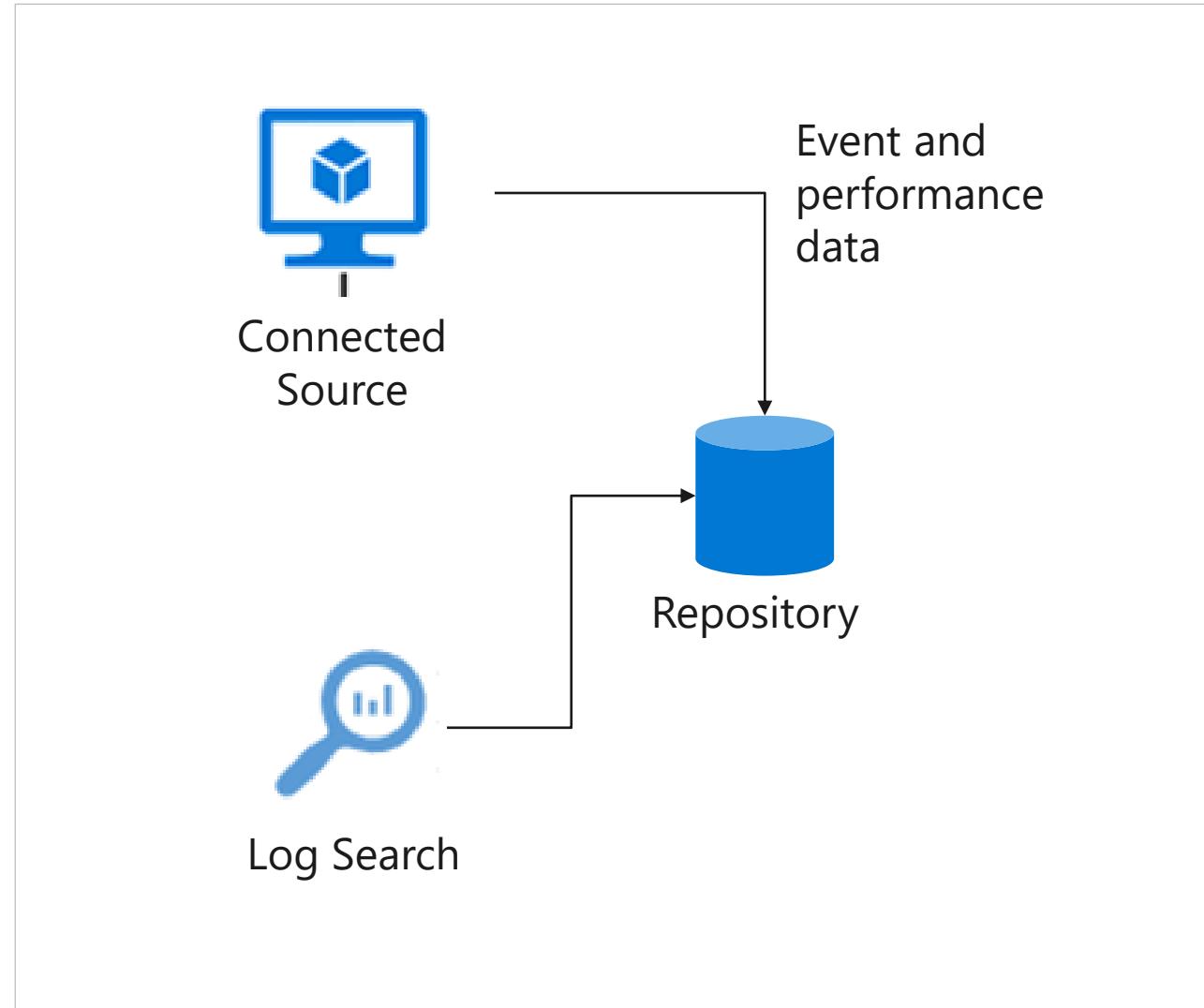
Deploy an Azure virtual machine

Create a Log Analytics workspace

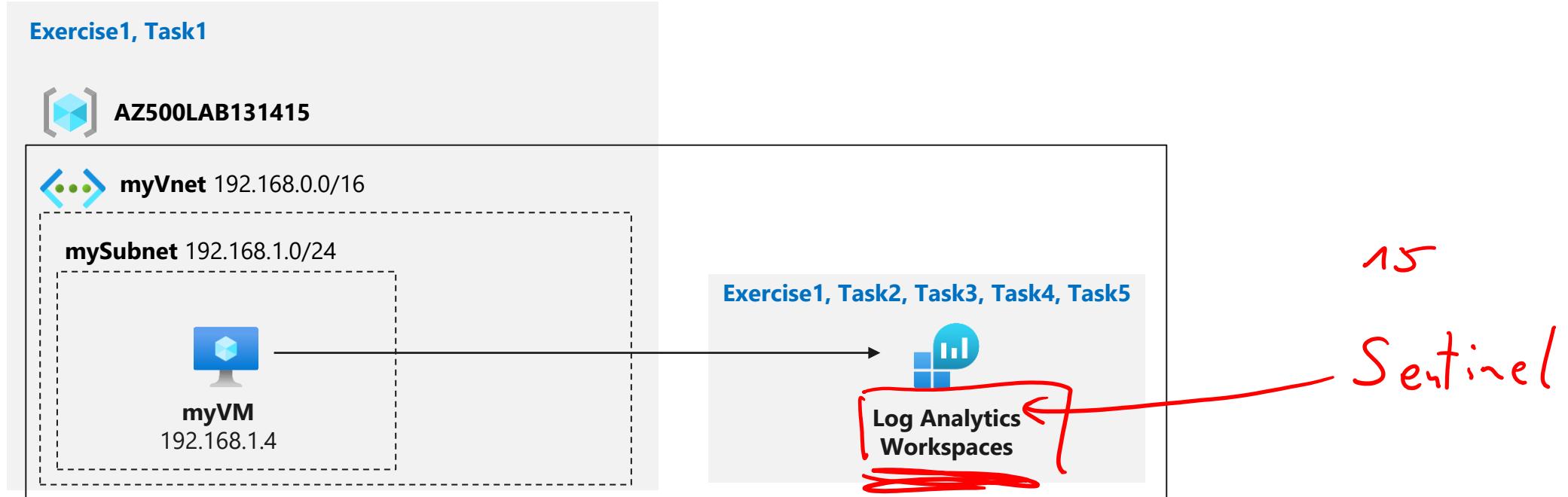
Enable the Log Analytics virtual machine extension

Collect virtual machine event and performance data

View and query collected data



# Lab 13 – Azure Monitor



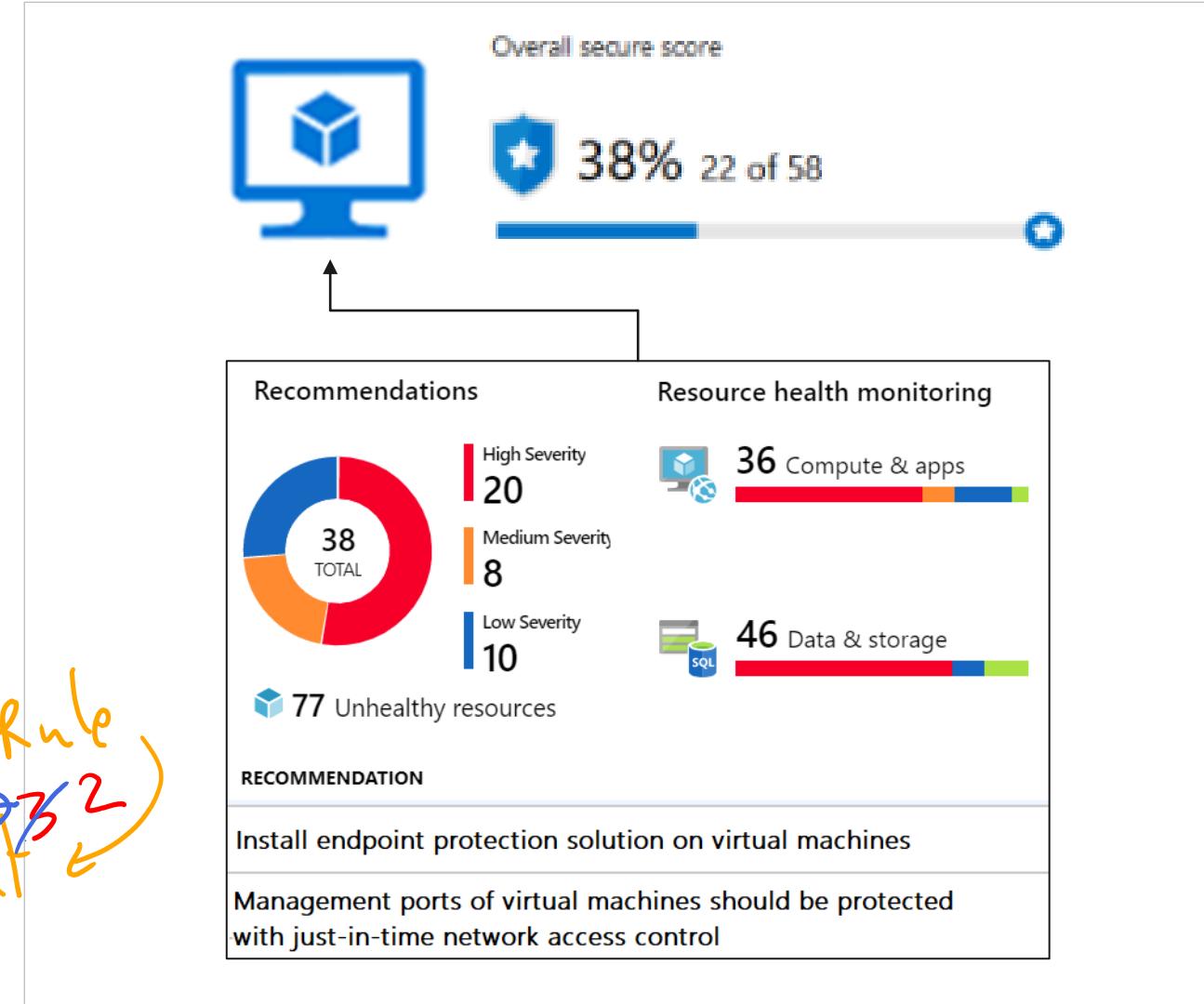
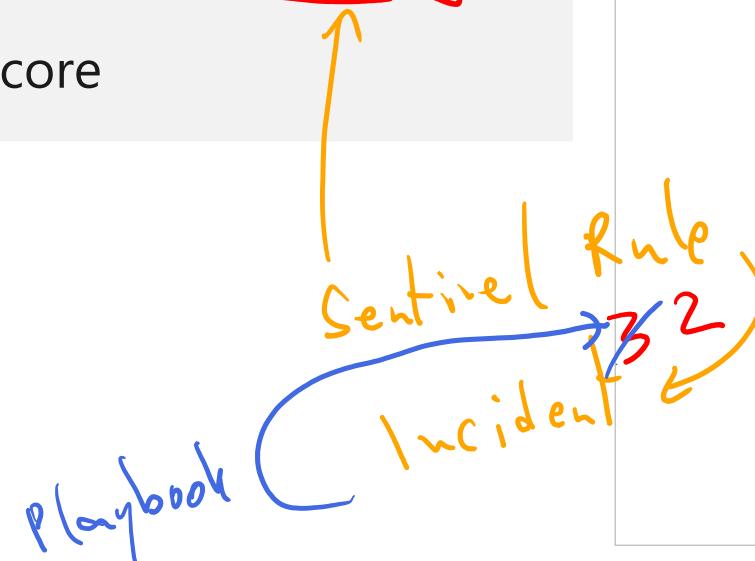
# Lab 14 – Microsoft Defender for Cloud

Configure Microsoft Defender for Cloud to monitor a virtual machine

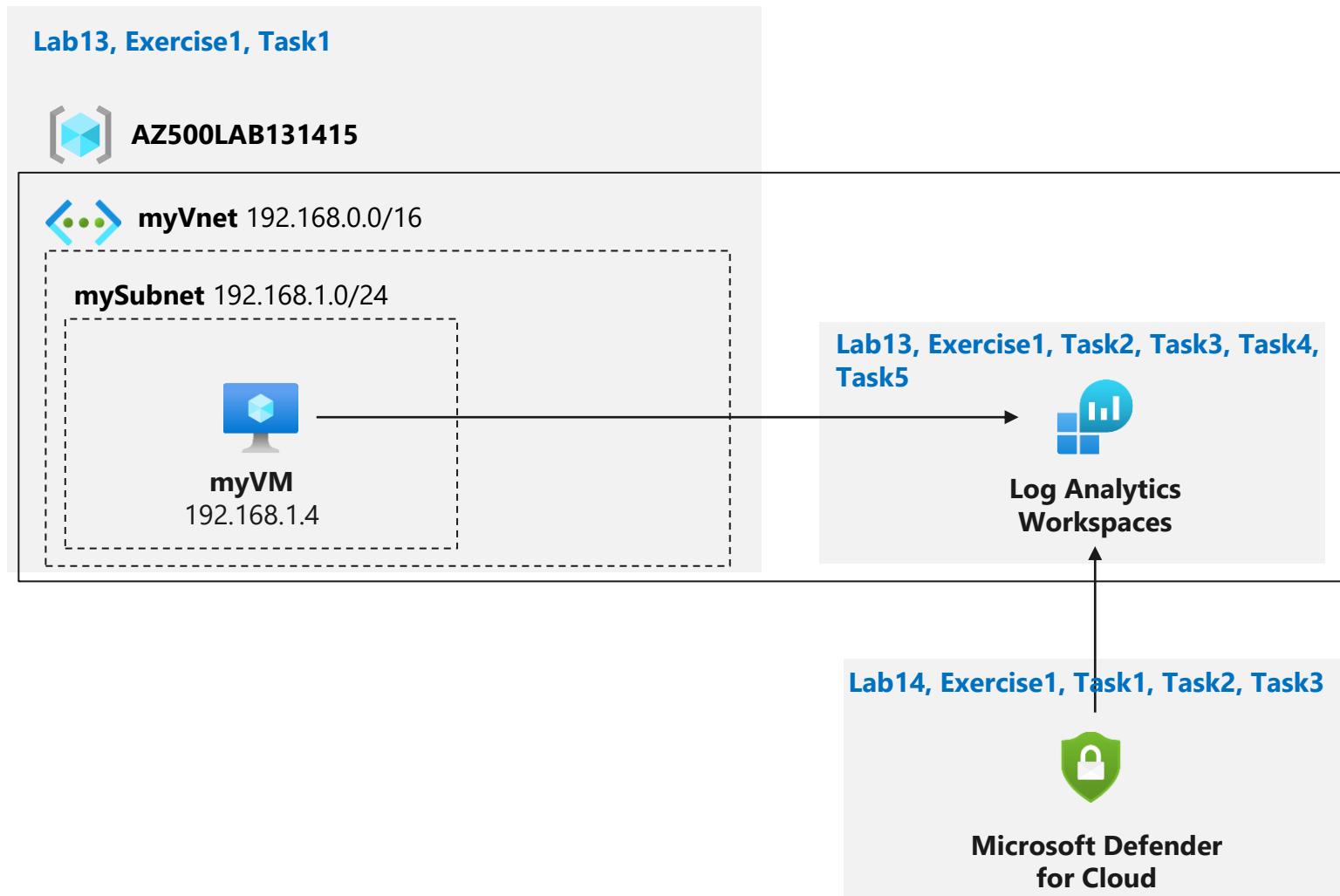
Review Microsoft Defender for Cloud recommendations for the virtual machine

Implement recommendations for endpoint protection and Just in time VM access

Review the Secure Score



# Lab 14 – Microsoft Defender for Cloud



# Lab 15 – Microsoft Sentinel

On-board Microsoft Sentinel

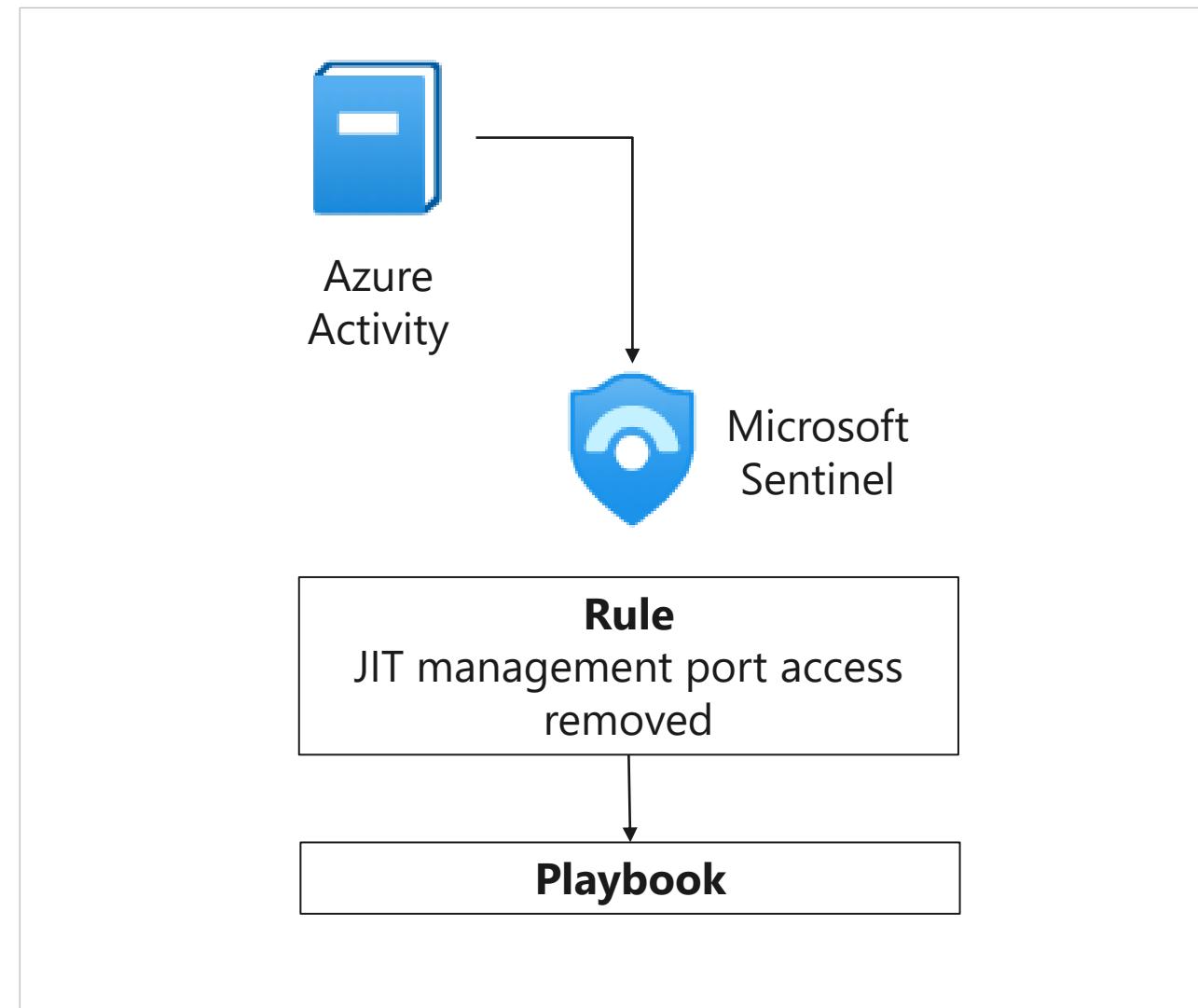
Connect Azure Activity to Sentinel

Review and create a rule that uses the Azure Activity data connector

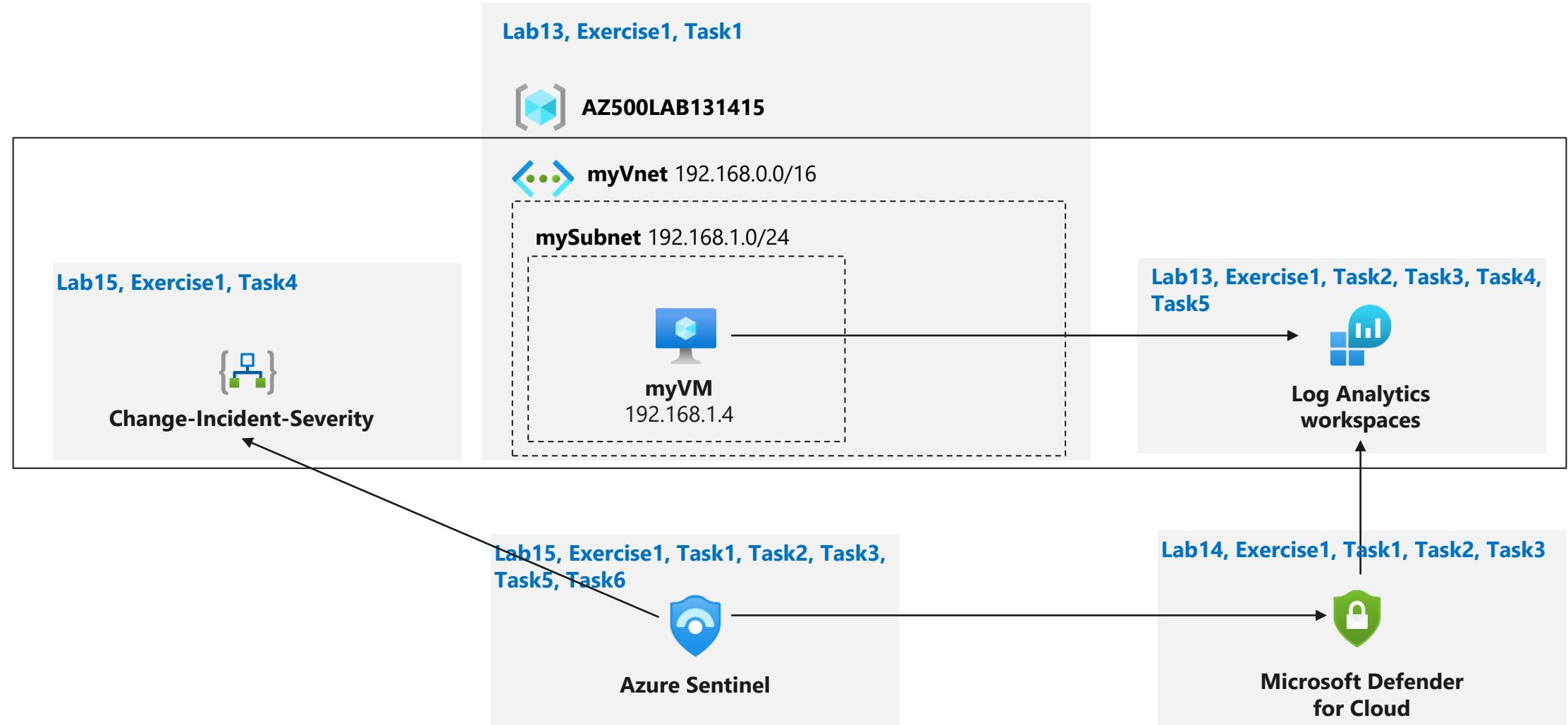
Create a playbook

Create a custom alert and configure the playbook as an automated response

Invoke an incident and review the associated actions



# Lab 15 – Microsoft Sentinel





**End of presentation**