Microsoft Azure

Feedback (MTH)

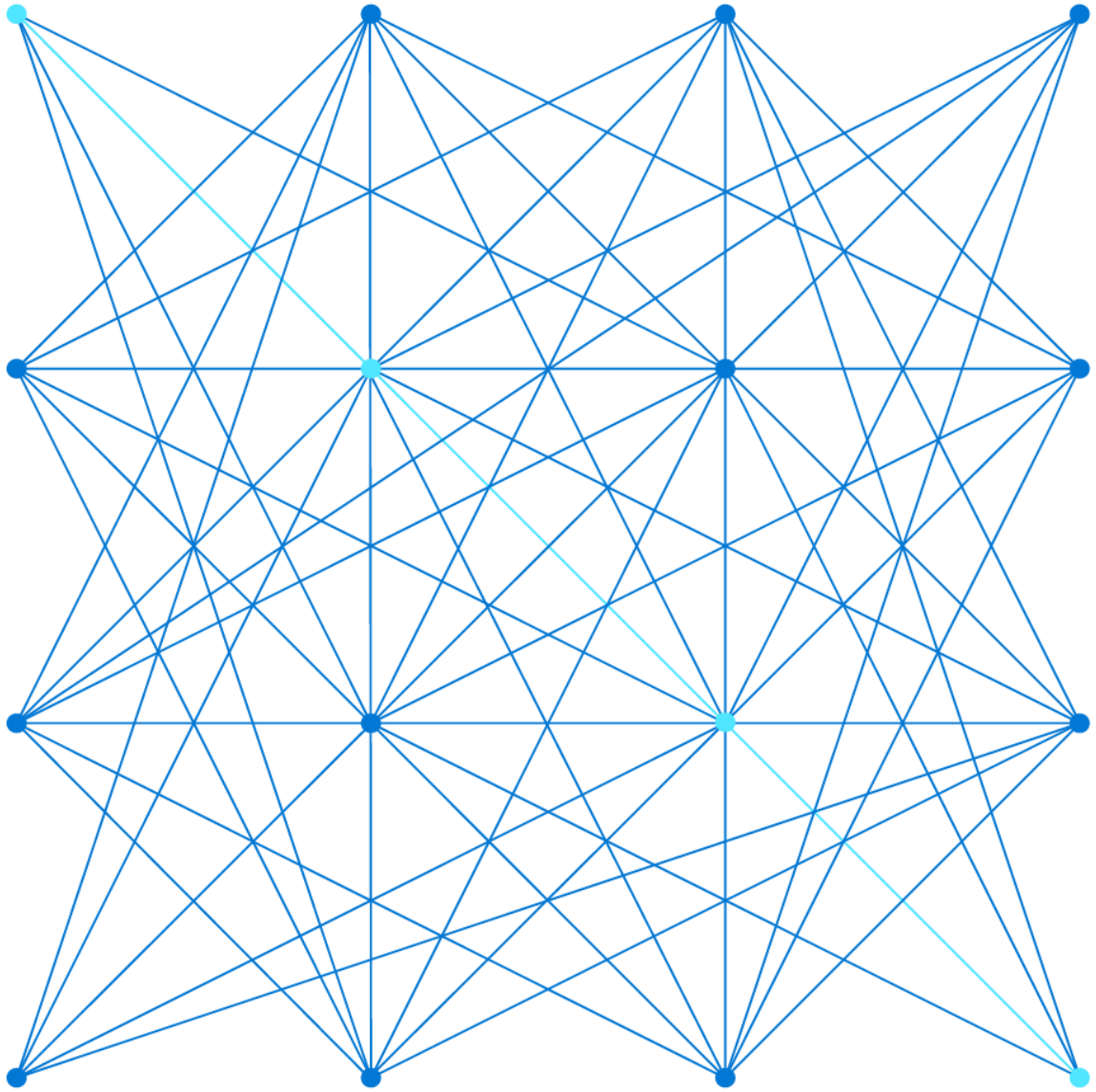
Tag 4

Badges
LP
+ notule

AZ-500

Microsoft Azure Security Technologies

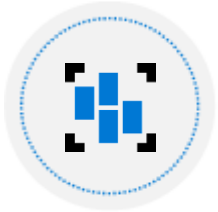
Guten Morgen!



AZ-500 Agenda

Learning Path 1 **Identity and Access**

Learning Path 2 **Implement Platform Protection**



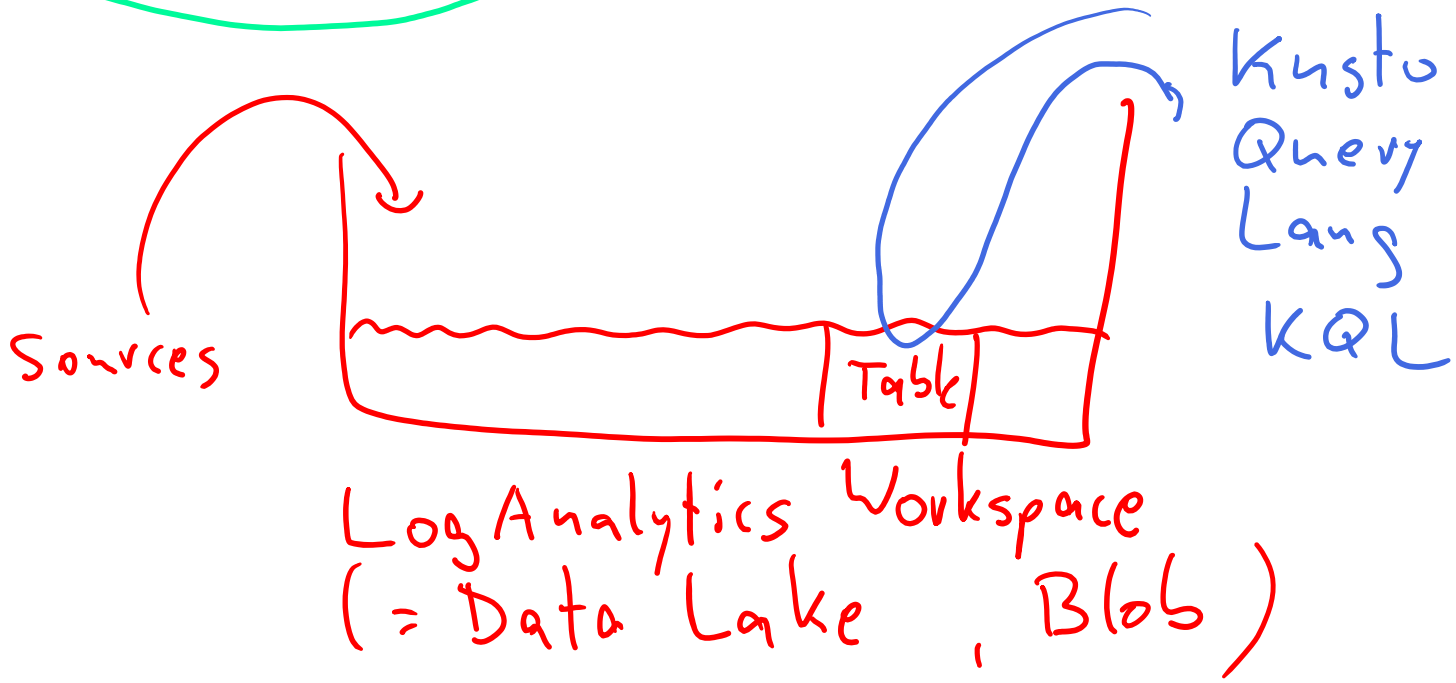
Learning Path 3 **Data and Application Security**

Learning Path 4 **Security Operations**

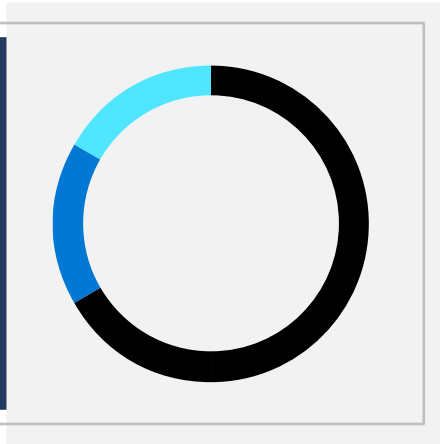
SC-200

Learning Path: Security Operations

- Azure Monitor
- Microsoft Defender for Cloud
- Microsoft Sentinel
- Module Labs



Azure Monitor



Azure Monitor

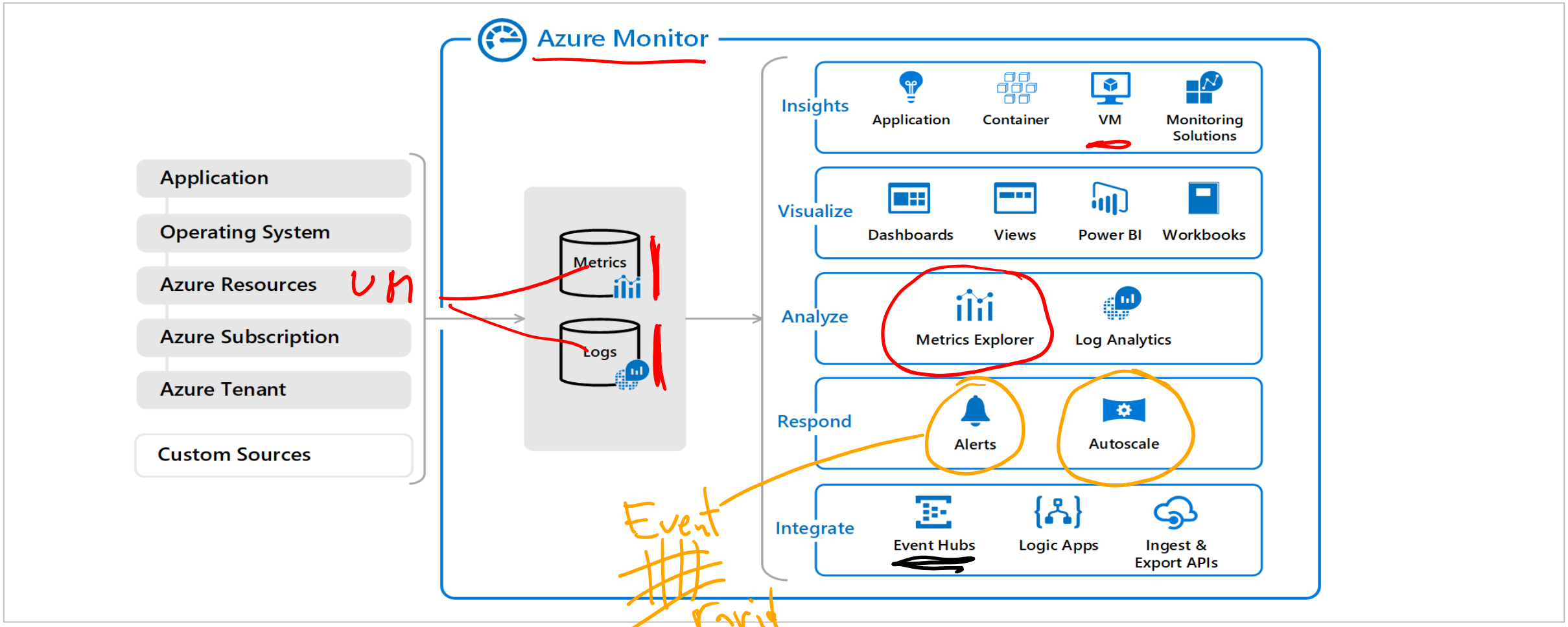
- Azure Monitor
- Metrics and Logs
- Log Analytics
- Connected Sources
- Azure Monitor Alerts
- Diagnostic Logging

Cloud Native ?

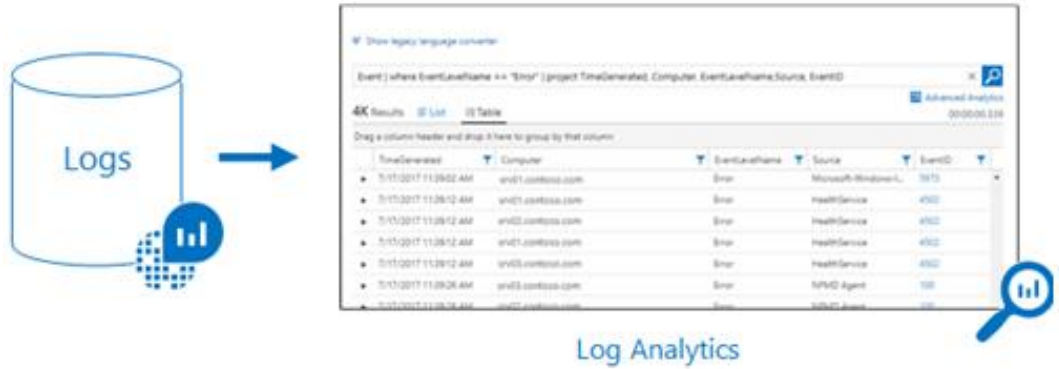
VM → App Service
Container
Functions λ
json - Logic App

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

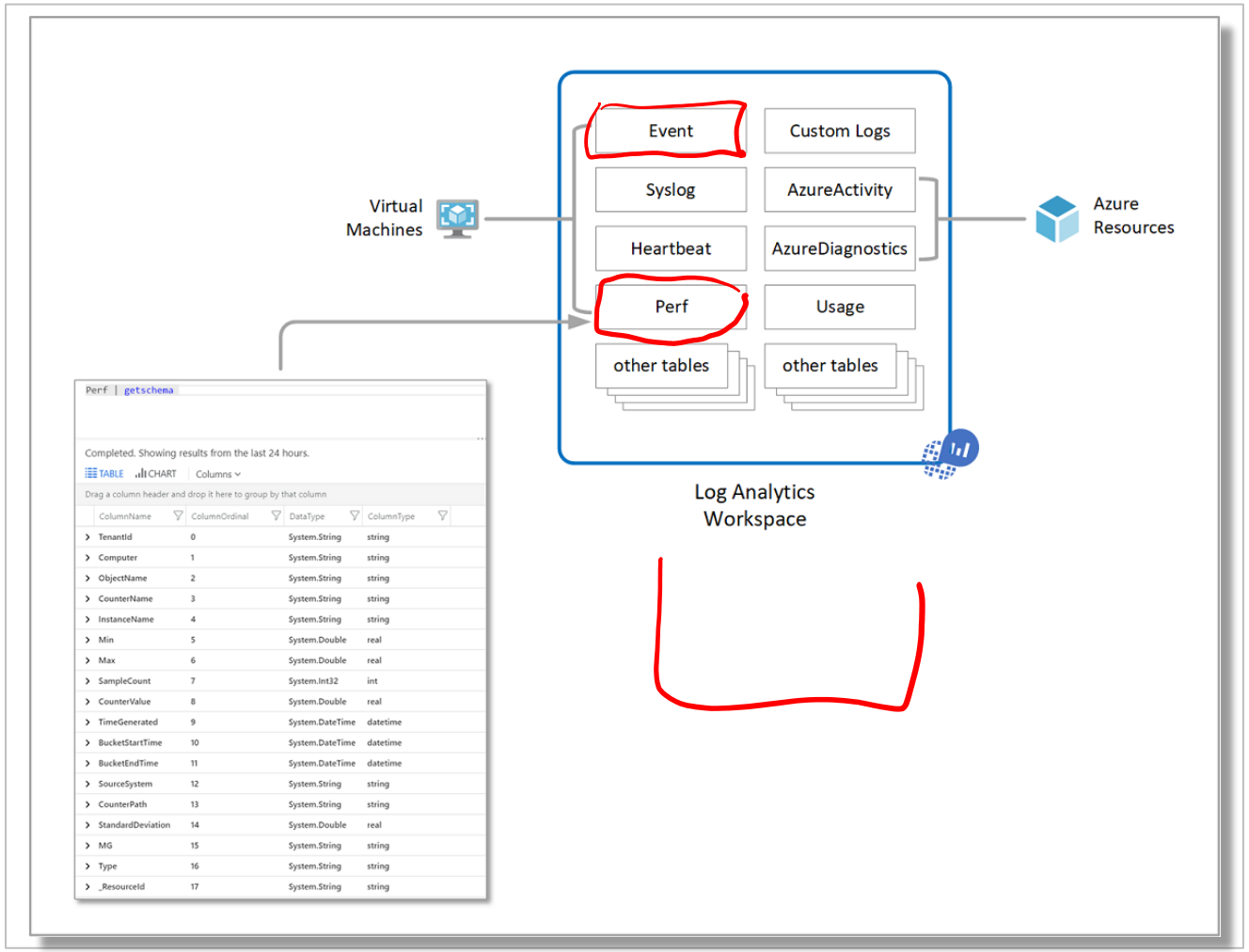
They are lightweight and capable of supporting near real-time scenarios

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

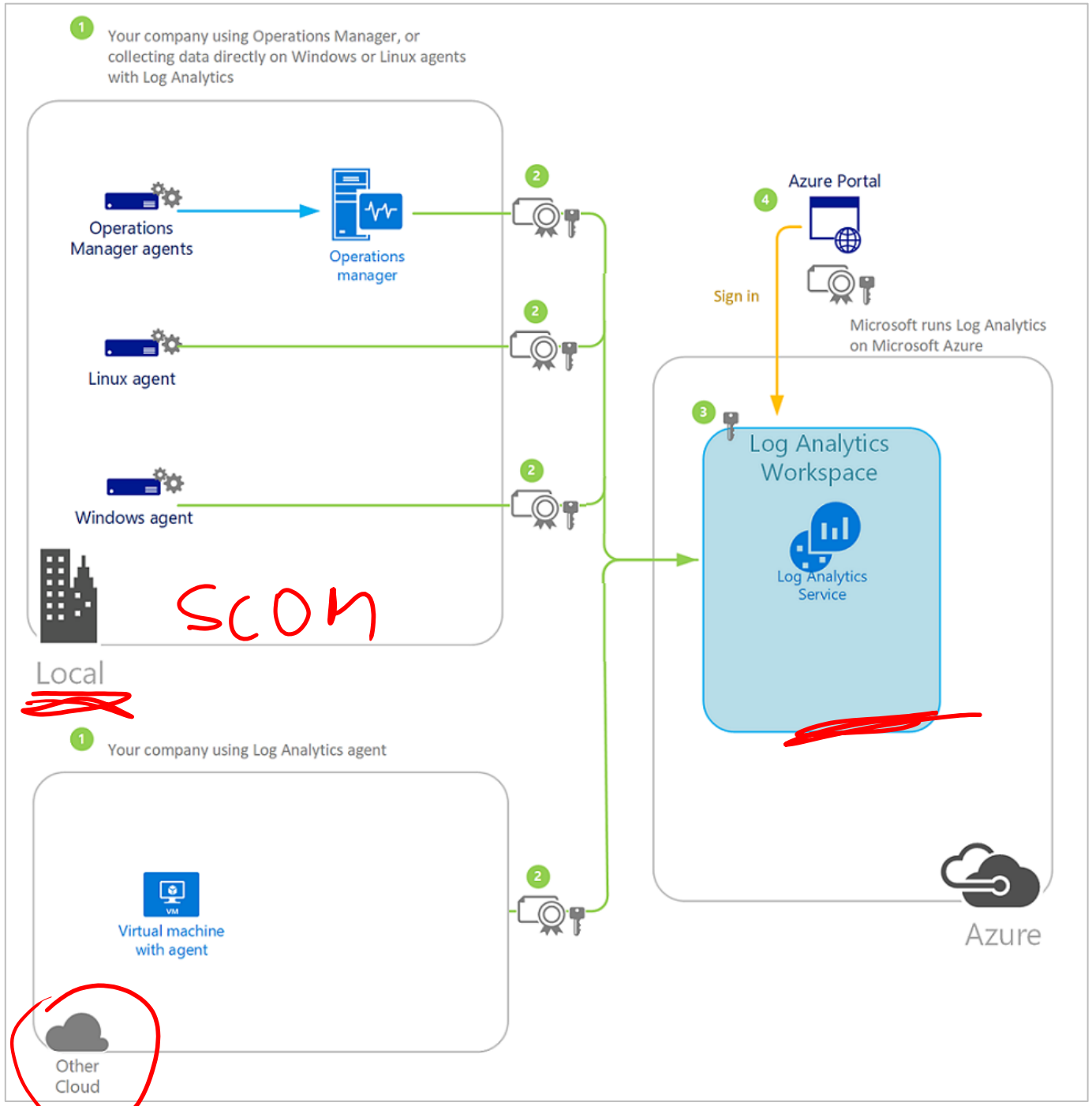
Collect and analyze resource data (cloud and on-premises) - write log queries and interactively analyze their results.



Connected Sources

Connected Sources generate data

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



Azure Monitor Alerts

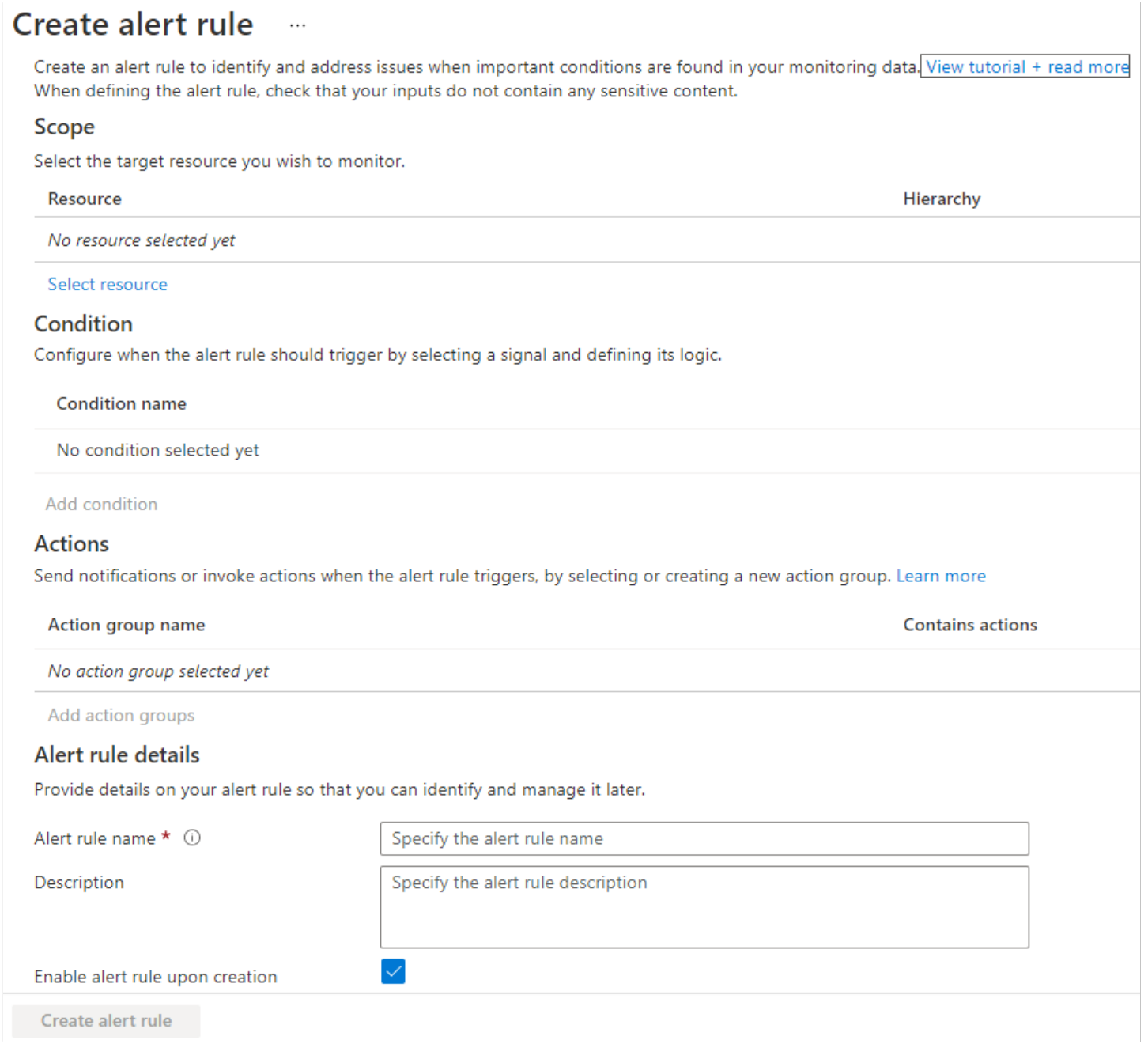
Select the target resource to monitor

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



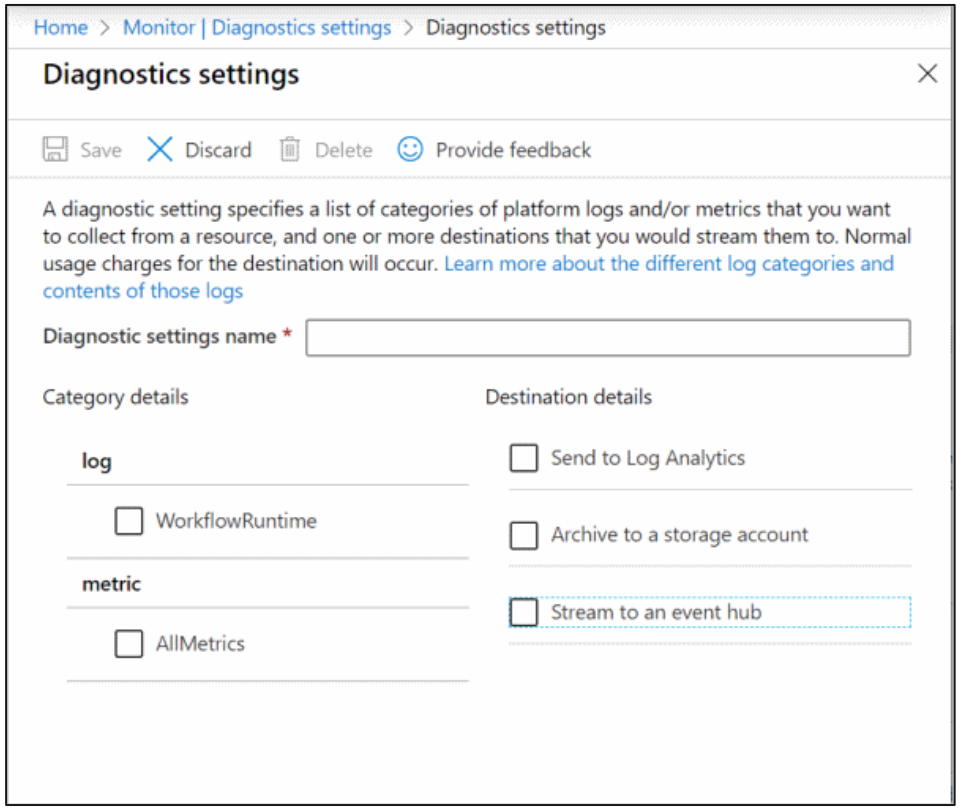
Diagnostic Settings

Tenant Logs – logs from outside of the Azure Subscriptions

Resource Logs – Logs from services inside of the subscription

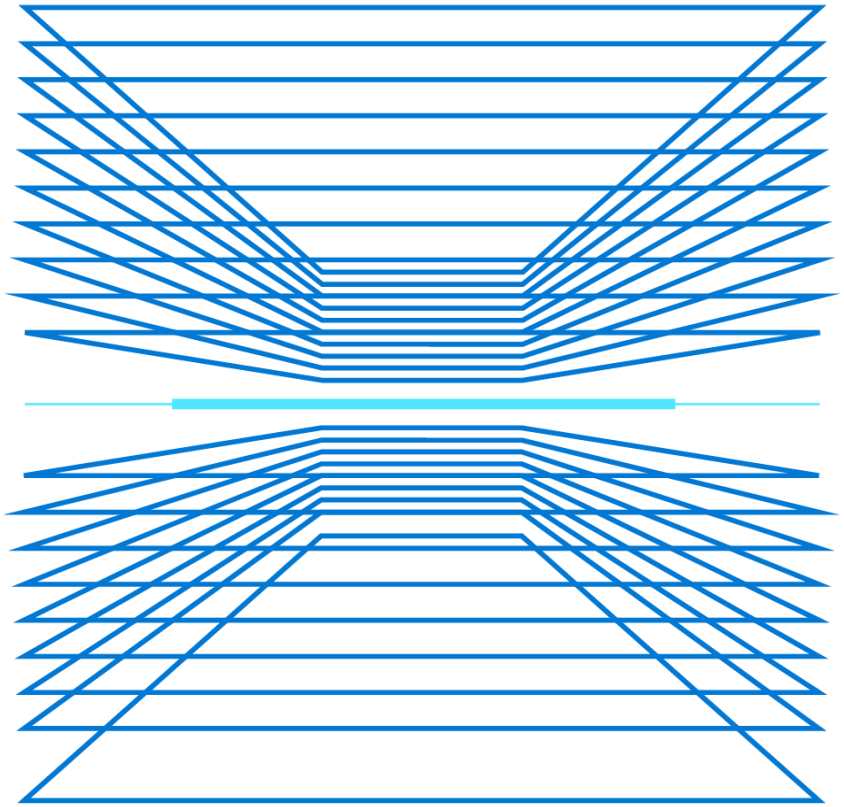
Configure Diagnostic Settings to send logged metrics to different destinations

Retention times are available for archiving to a storage account



Demonstration: Azure Monitor

- Activity logs and alerts
- Log analytics



Additional Study – Azure Monitor

Module Review Questions	Microsoft Learn Modules (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)

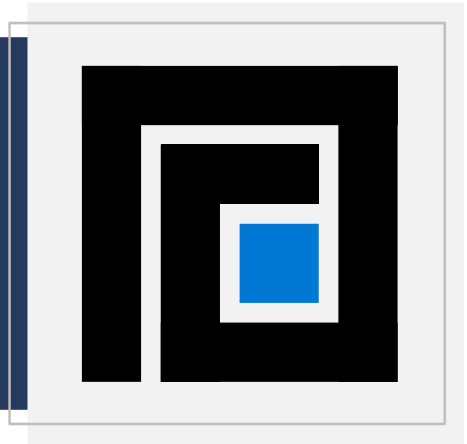
Defender M365

- Cloud Apps
- Identity
- Endpoint
- Office

Microsoft Defender for Cloud

ASC

Subscription



Microsoft Defender for Cloud


MITRE | ATT&CK®

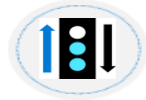

Microsoft Defender for Cloud


Microsoft Defender for Cloud Features


Microsoft Defender for Cloud Security Policies


Microsoft Defender for Cloud Recommendations


Secure Score


Brute Force Attacks

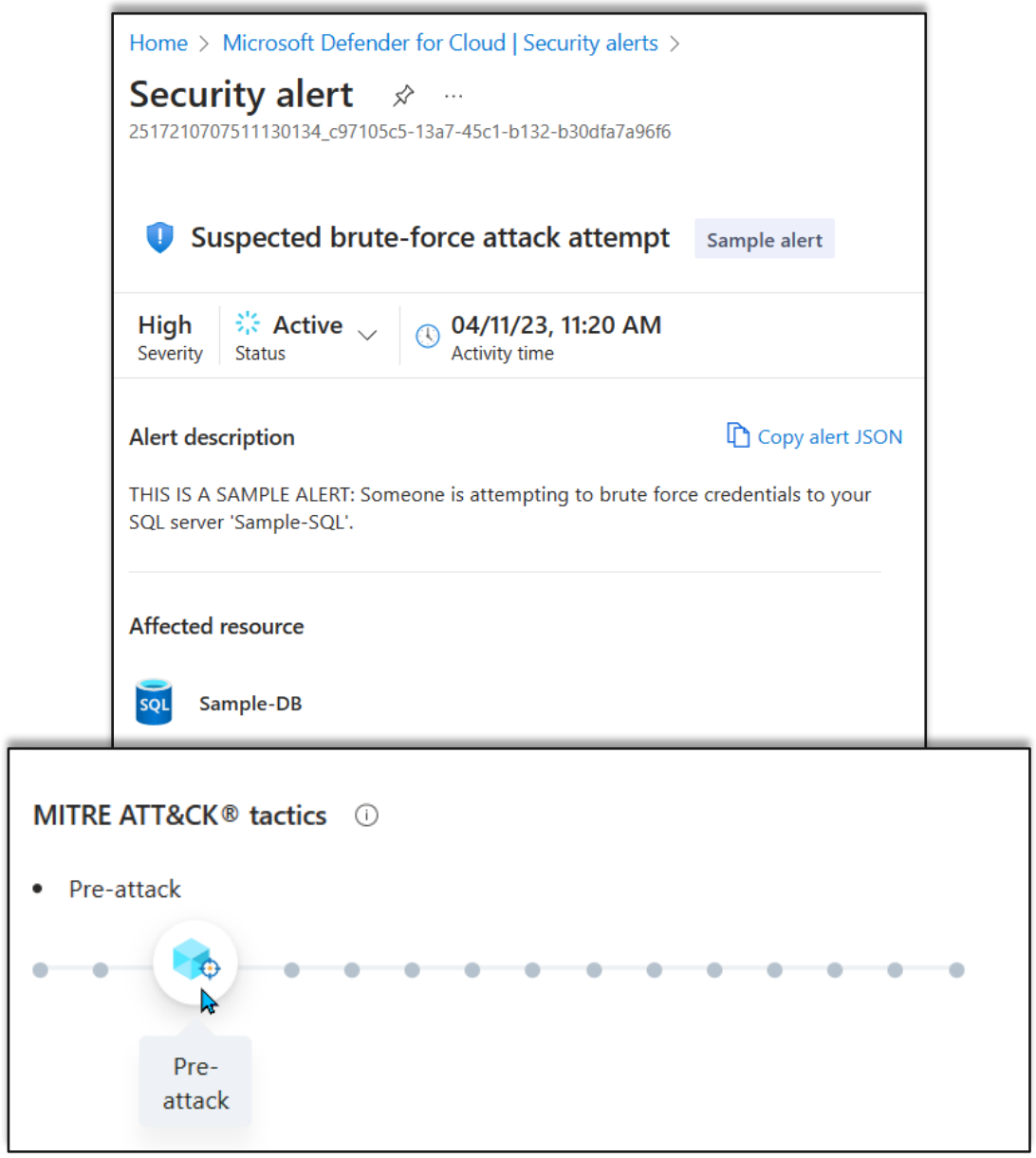

Just in Time Virtual Machine Access

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.

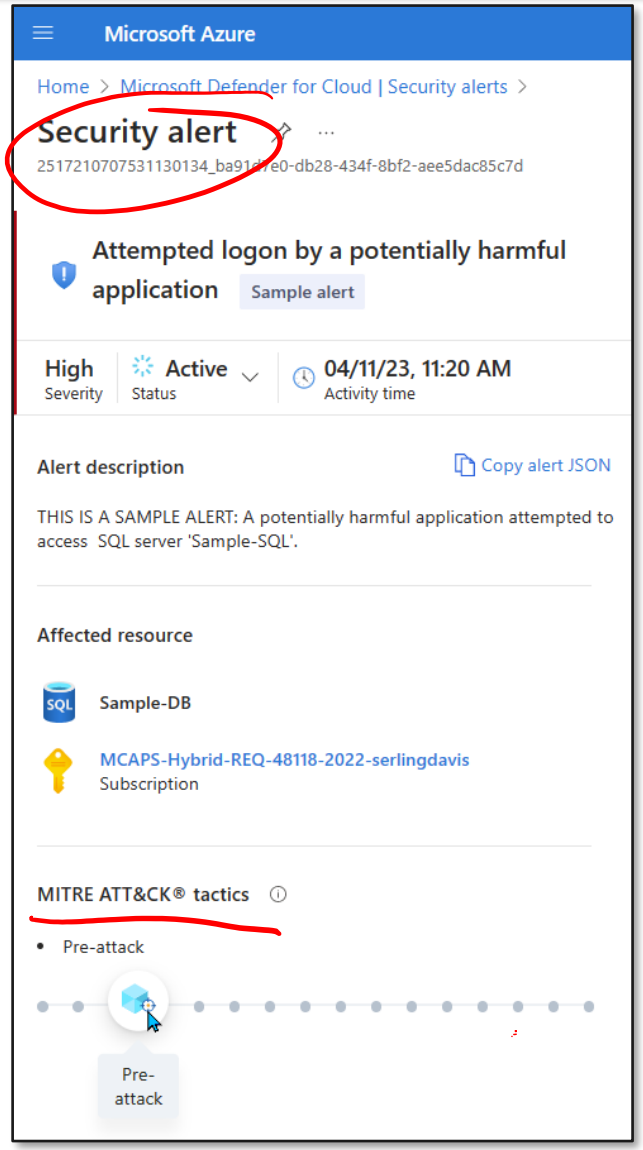


MITRE | ATT&CK® matrix (continued)

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



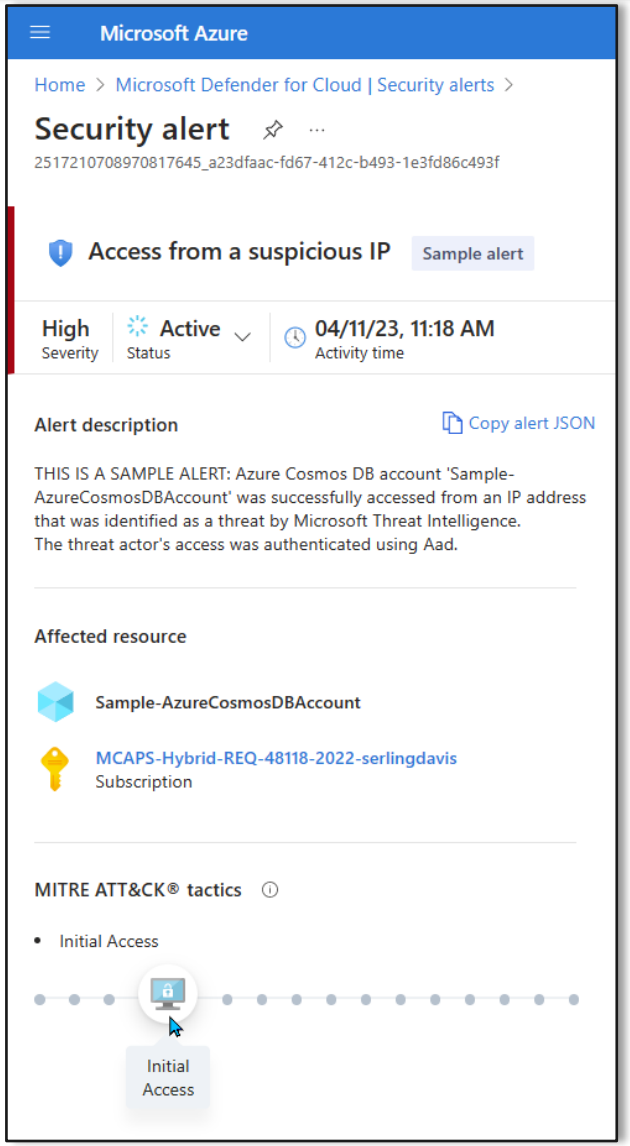
MITRE | ATT&CK® matrix (continued)

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



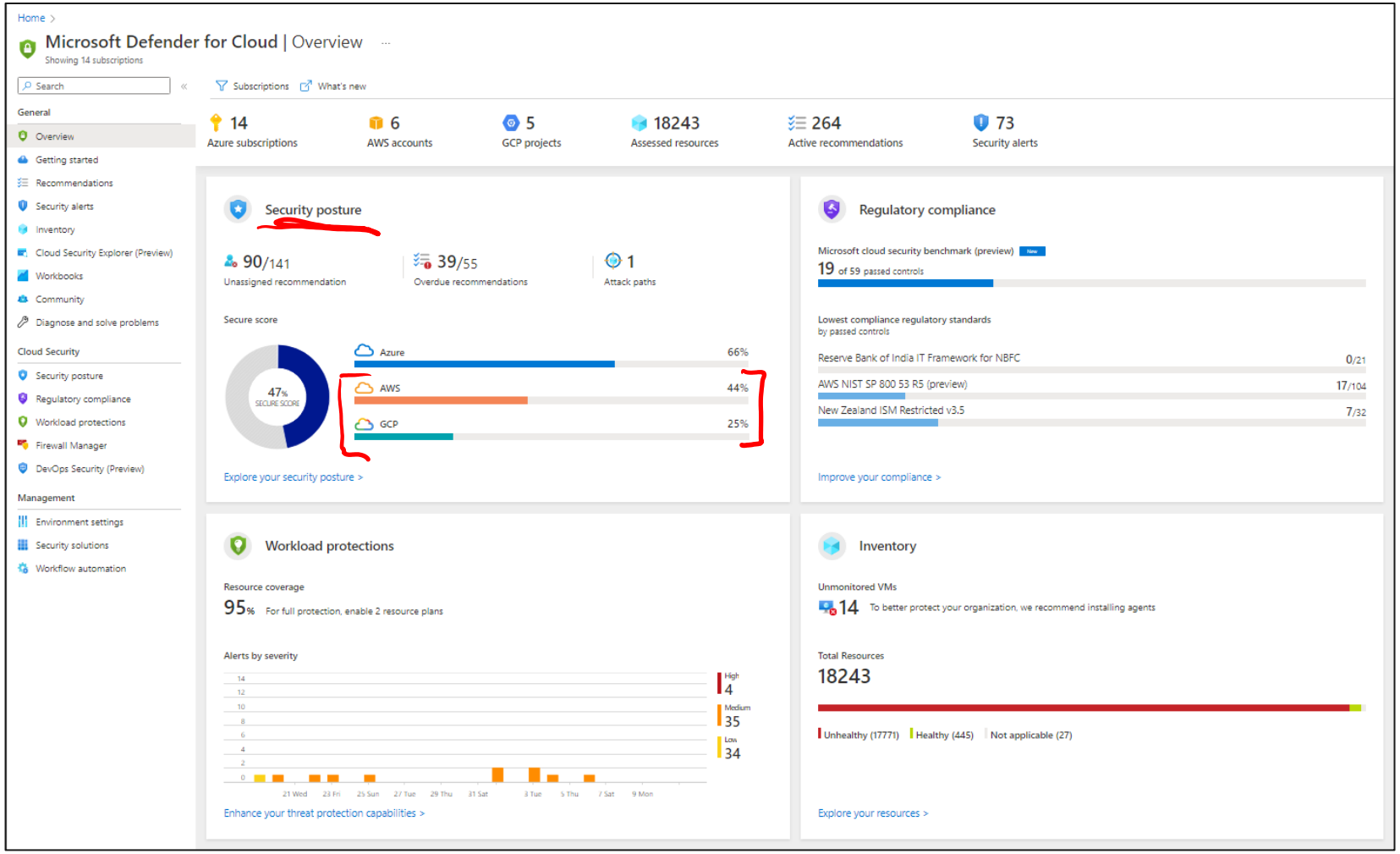
Implement Microsoft Defender for Cloud

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

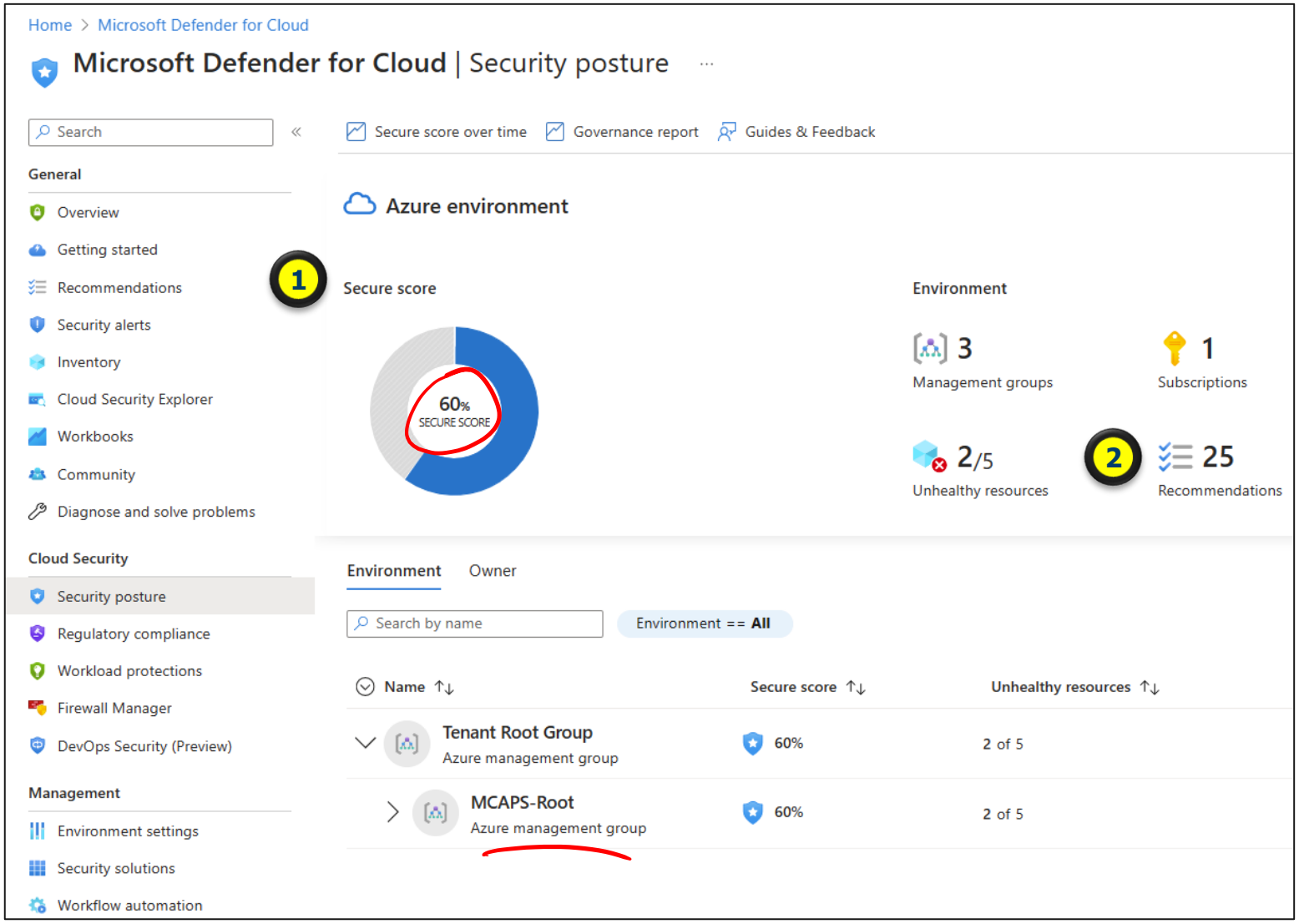


Cloud security posture management (CSPM)

The cloud security posture management features provide the following:

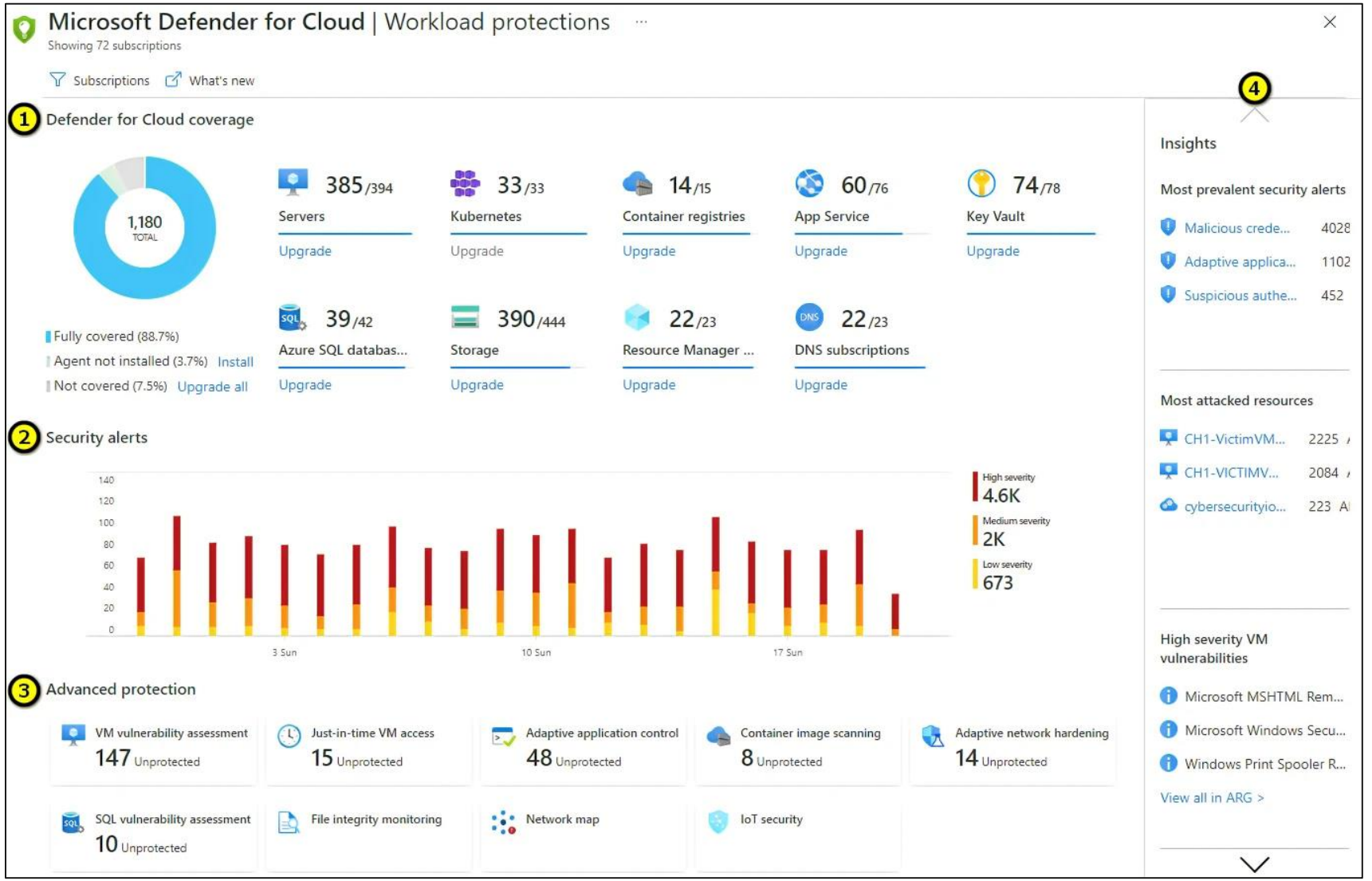
1. Visibility - to help you understand your current security situation.

2. Hardening guidance - to help you efficiently and effectively improve your security.



Cloud workload protection (CWP)

1. Microsoft Defender for Cloud coverage
2. Security alerts
3. Advanced protection
4. Insights

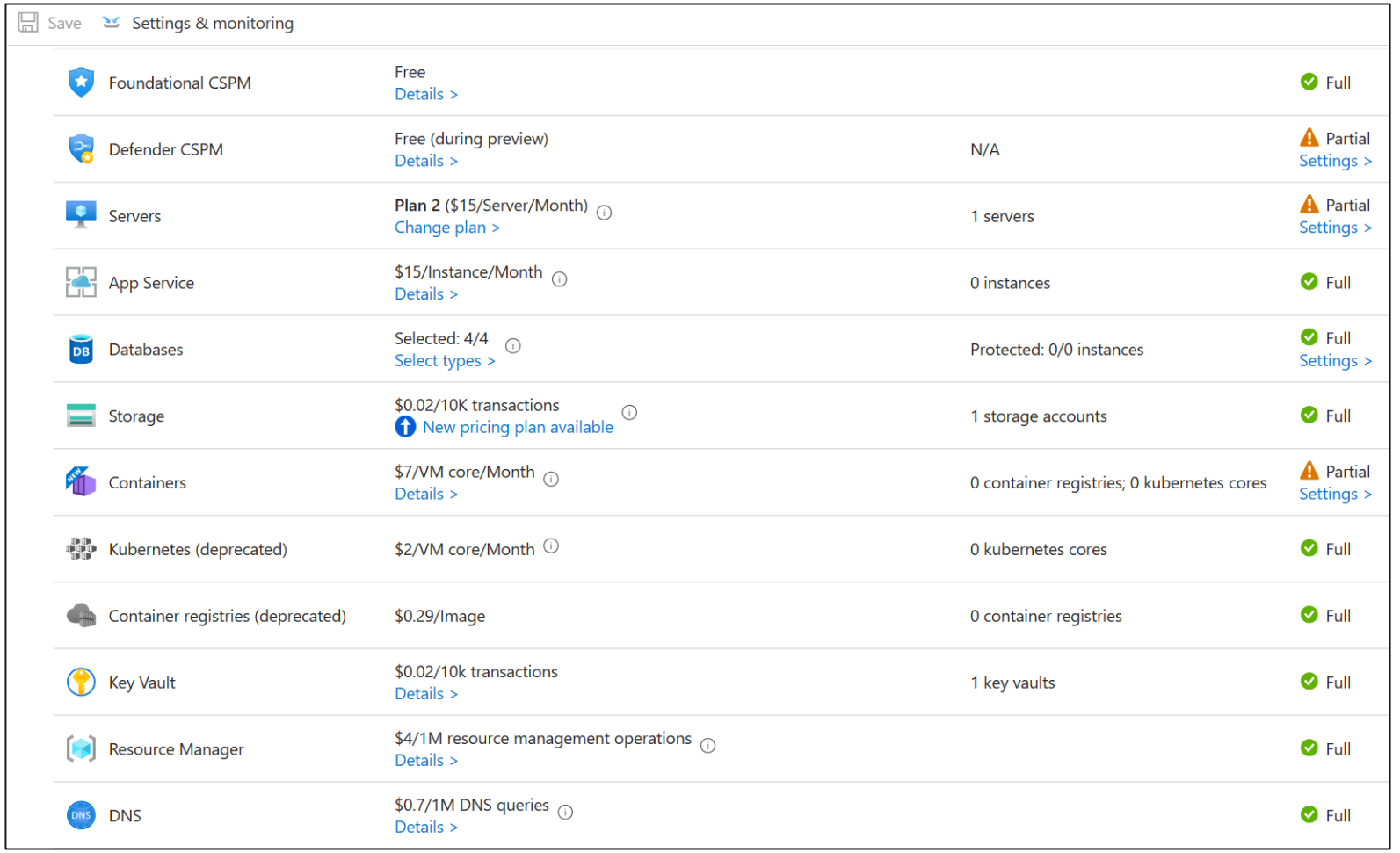


Basic security features

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.

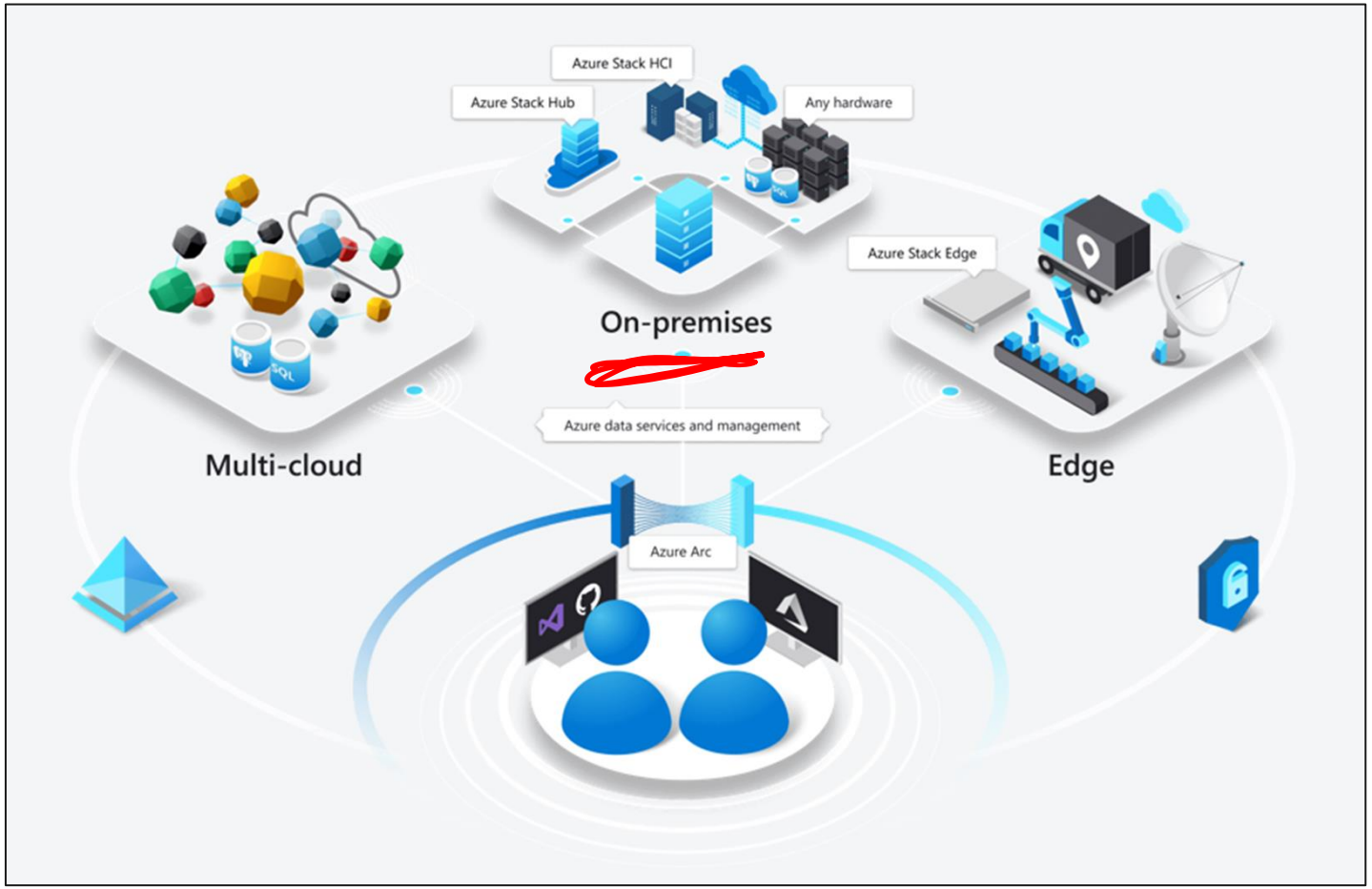
Feature	Foundational CSPM capabilities	Defender CSPM	Cloud availability
Continuous assessment of the security configuration of your cloud resources	✓	✓	Azure, AWS, GCP, on-premises
Security recommendations to fix misconfigurations and weaknesses	✓	✓	Azure, AWS, GCP, on-premises
Secure score	✓	✓	Azure, 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



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



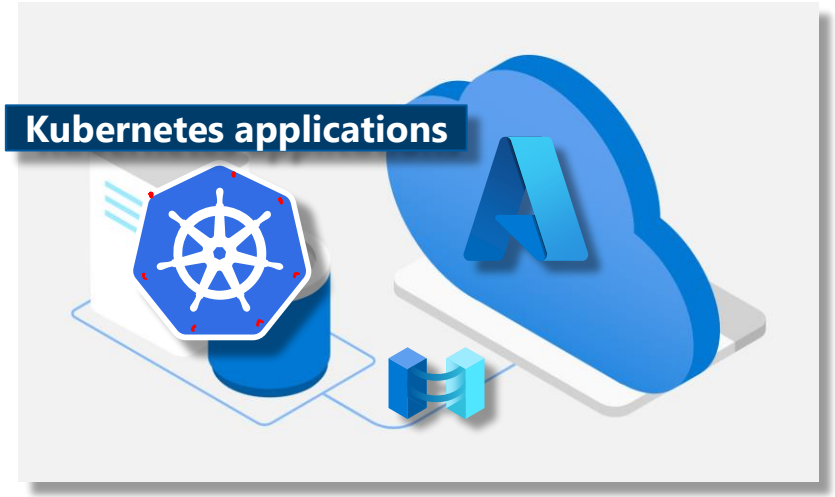
Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

Azure Arc capabilities

Azure Arc for Servers

Organize and govern servers across environments

Azure Arc for Kubernetes



Manage Kubernetes applications at-scale

Azure data services on Azure Arc

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.

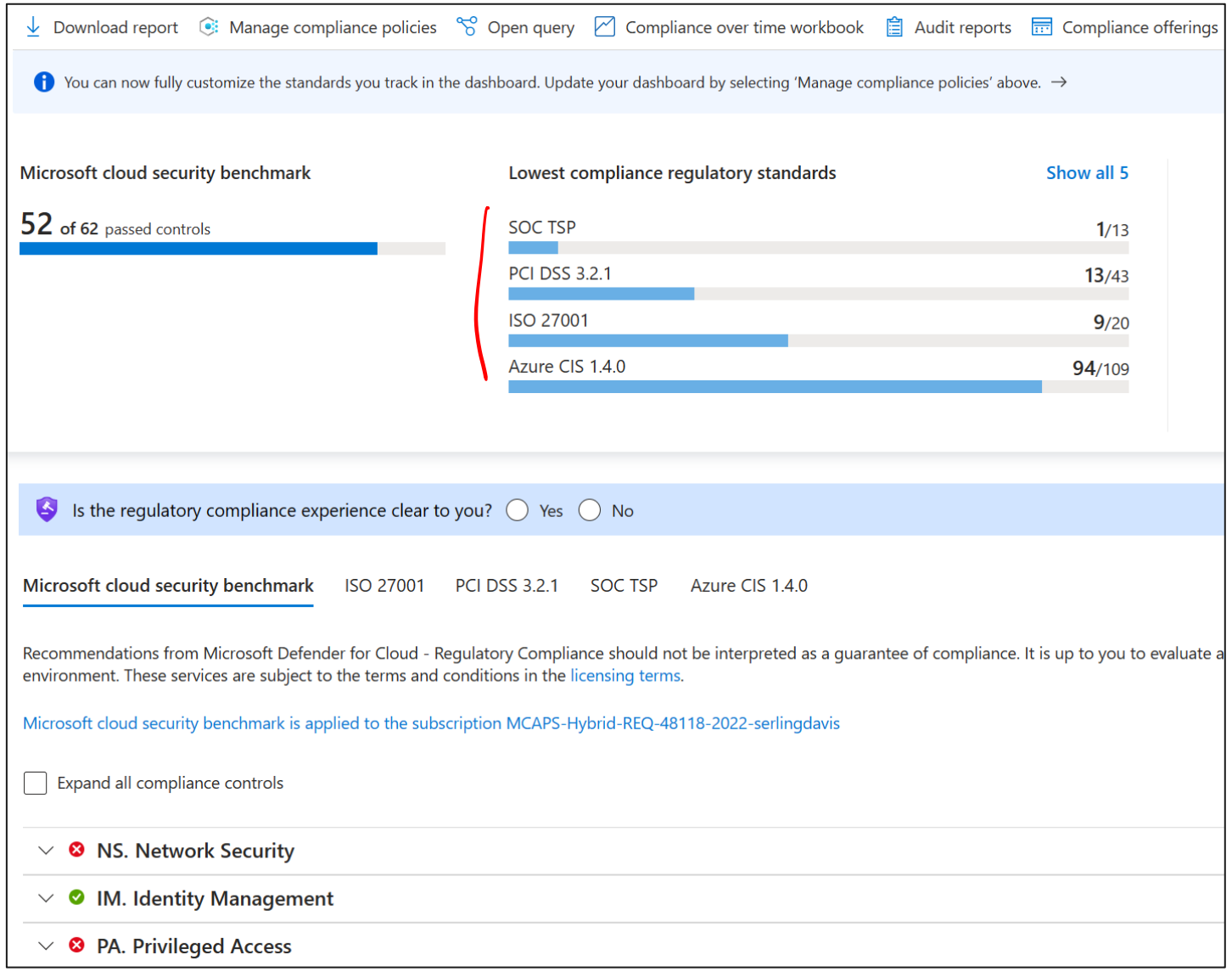
Regulatory compliance dashboard

Purview Portal

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.

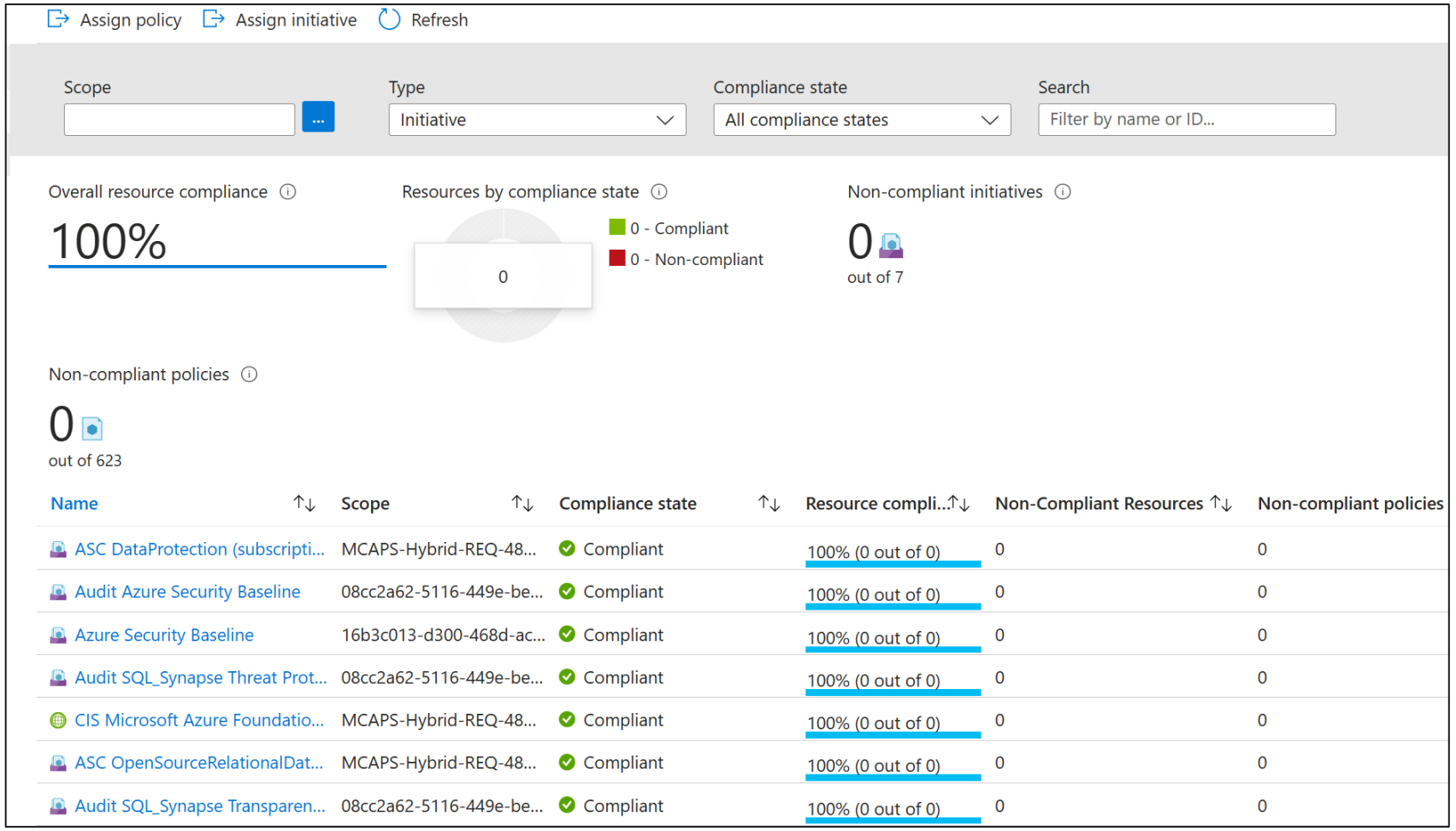


What are security initiatives, and policies

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.

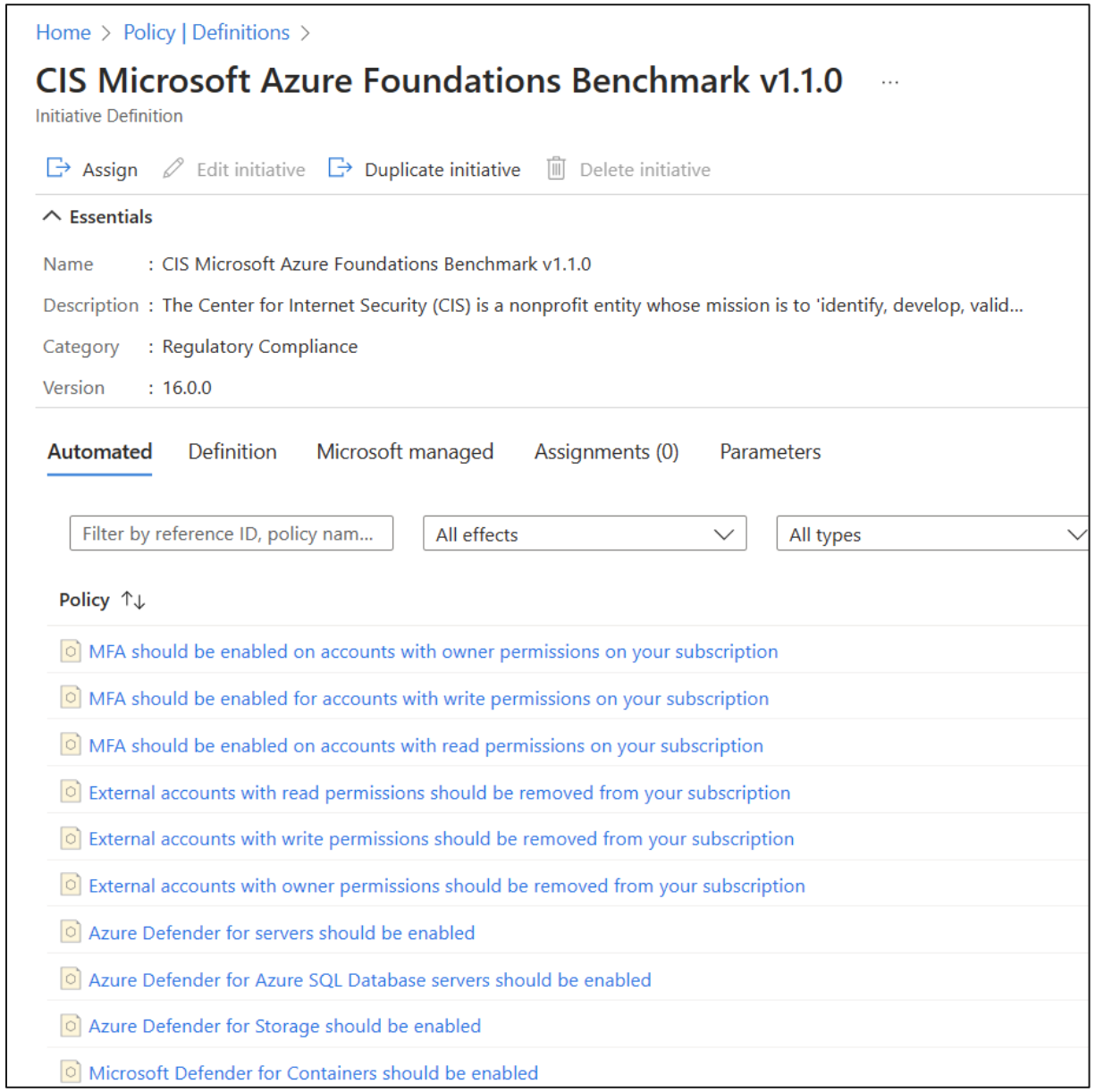


Out of the box examples: Microsoft Defender for Cloud > Environment settings > Subscription > Policy settings > Security policy

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.

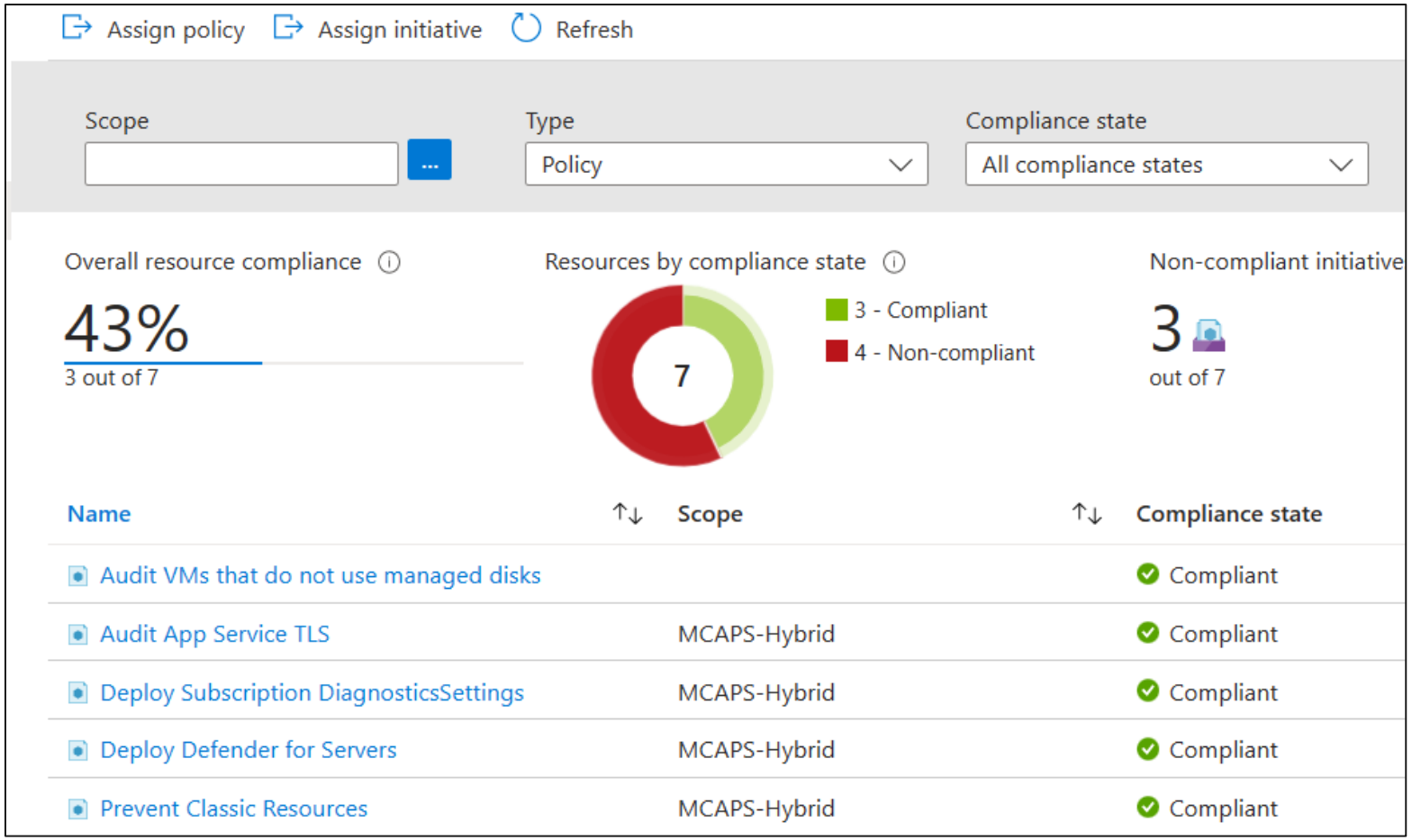
Security initiatives simplify management of your policies by grouping a set of policies together, logically, as a single item.



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.

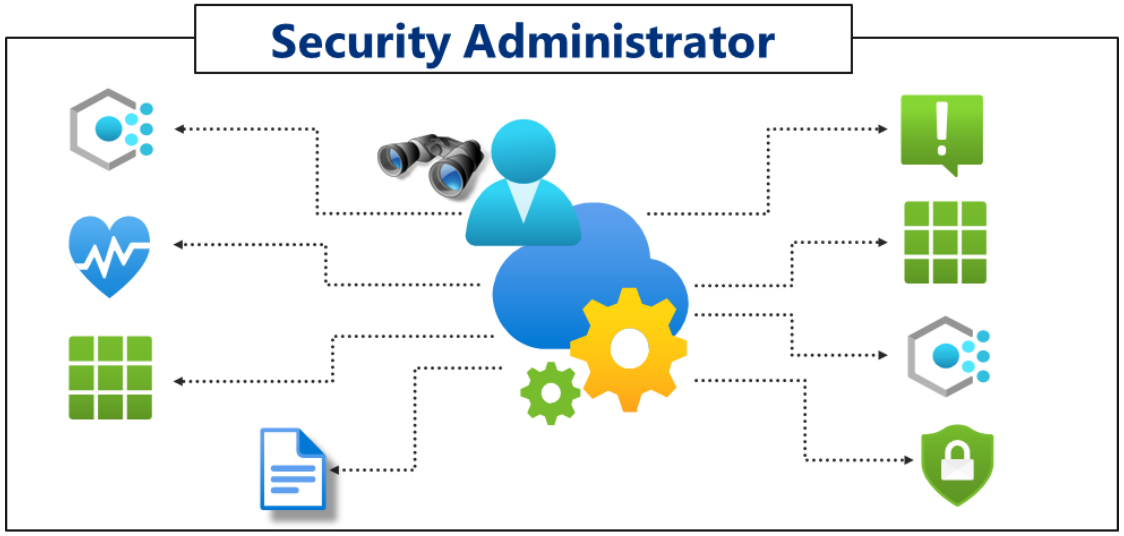


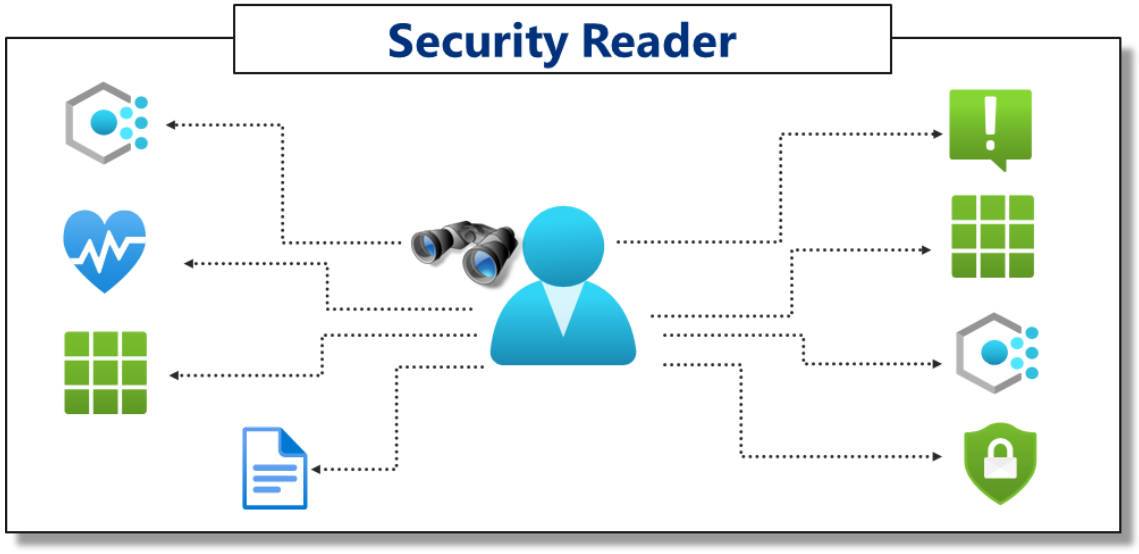
Viewing and editing security policies

View, Update, and Dismiss Alerts

Security Administrator
vs.
Security Reader

View Only



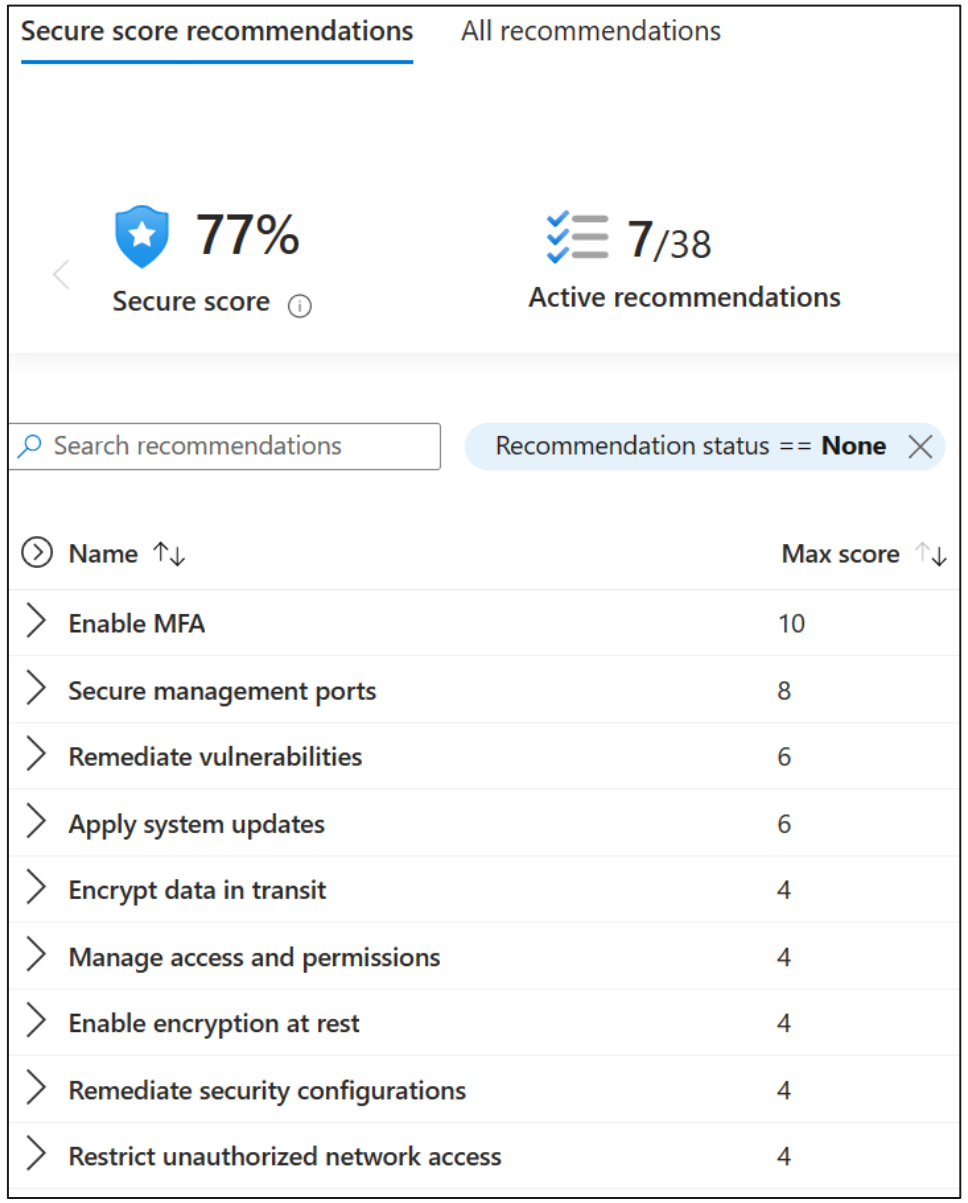


Recommendations

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.

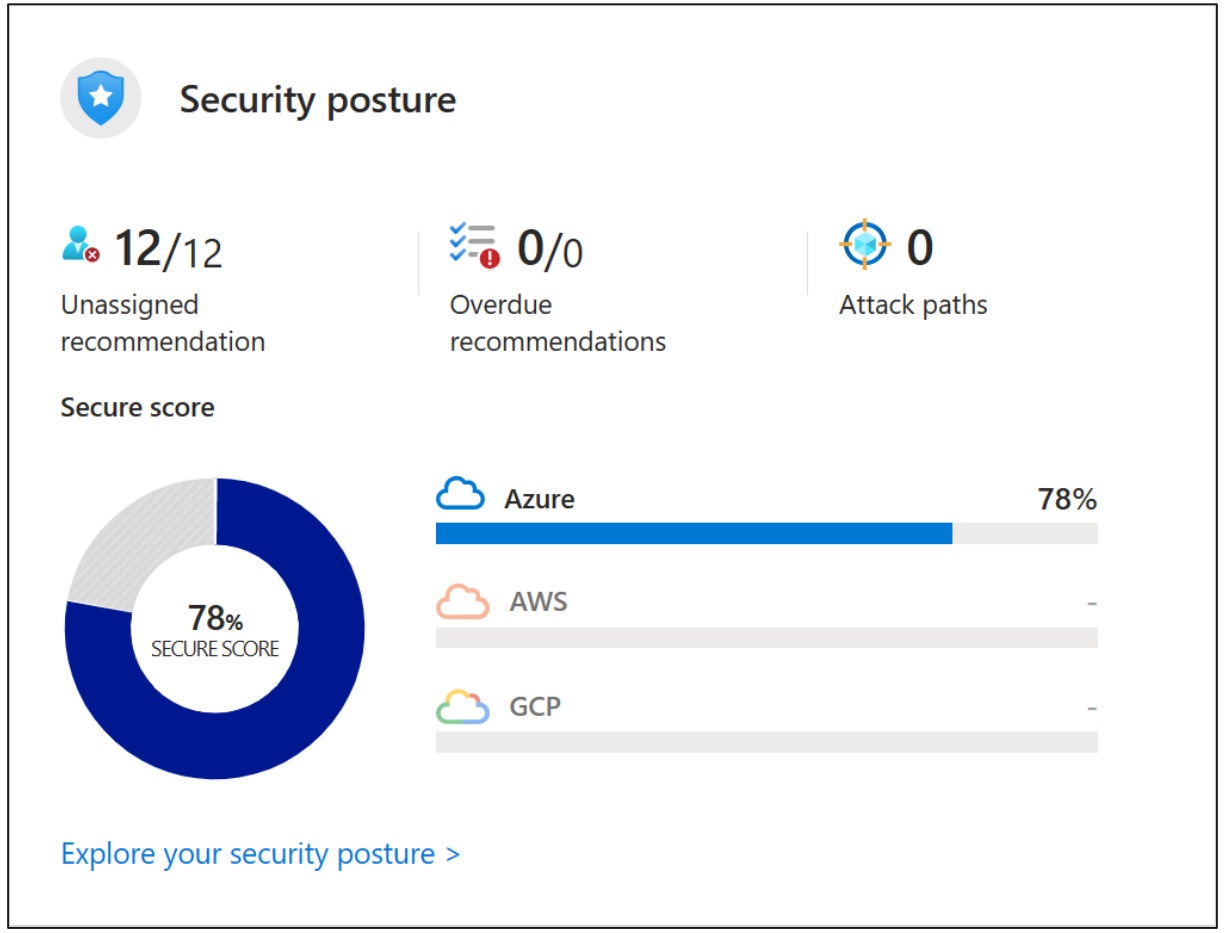


Secure Score

Microsoft Defender for Cloud has two main goals:

1. To help you understand your current security situation

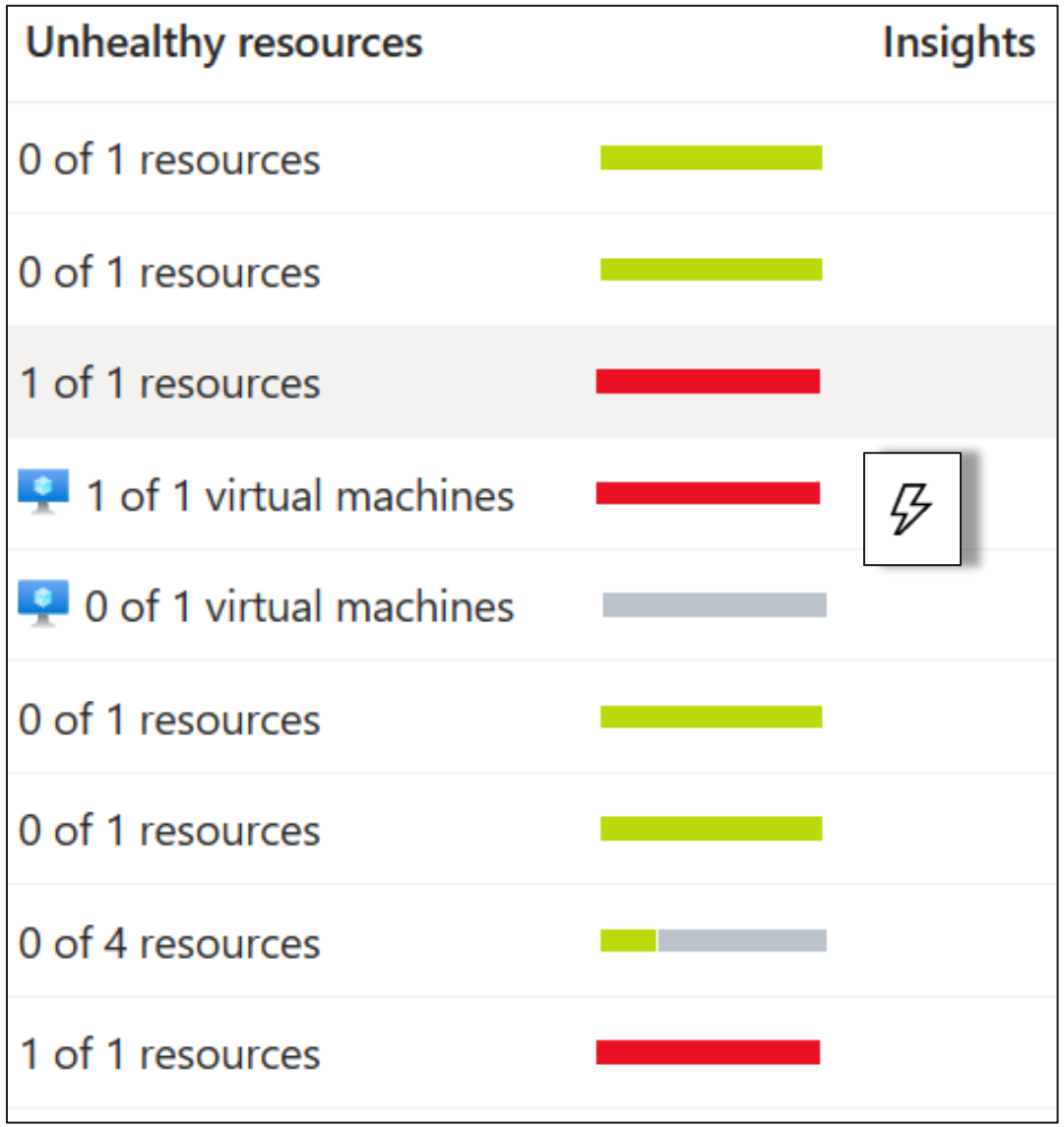
2. To help you efficiently and effectively improve your security



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.



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

Name	Max score
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

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
SSH (Secure Shell)	22 / TCP (Transmission Control Protocol)
Telnet (Teletype Network)	23 / TCP (Transmission Control Protocol)
FTP (File Transfer Protocol)	21 / TCP (Transmission Control Protocol)
NetBIOS (Network Basic Input/Output System)/**SMB** (Server Message Block)/**Samba**	139 and 445 / TCP (Transmission Control Protocol)
LDAP (Lightweight Directory Access Protocol)	389 / TCP (Transmission Control Protocol)
Kerberos	88 / TCP (Transmission Control Protocol)
RDP (Remote Desktop Protocol)	3389 / TCP (Transmission Control Protocol)
HTTP/HTTP (Hypertext Transfer Protocol) Management Services	80 and 443 / TCP (Transmission Control Protocol)
MSSQL (Microsoft Structured Query Language)	1433 / TCP (Transmission Control Protocol)
Oracle	1521 / TCP (Transmission Control Protocol)
My SQL (My Structured Query Language)	3306 / TCP (Transmission Control Protocol)
VNC (Virtual Network Computing)	5900 / TCP (Transmission Control Protocol)
SNMP (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:

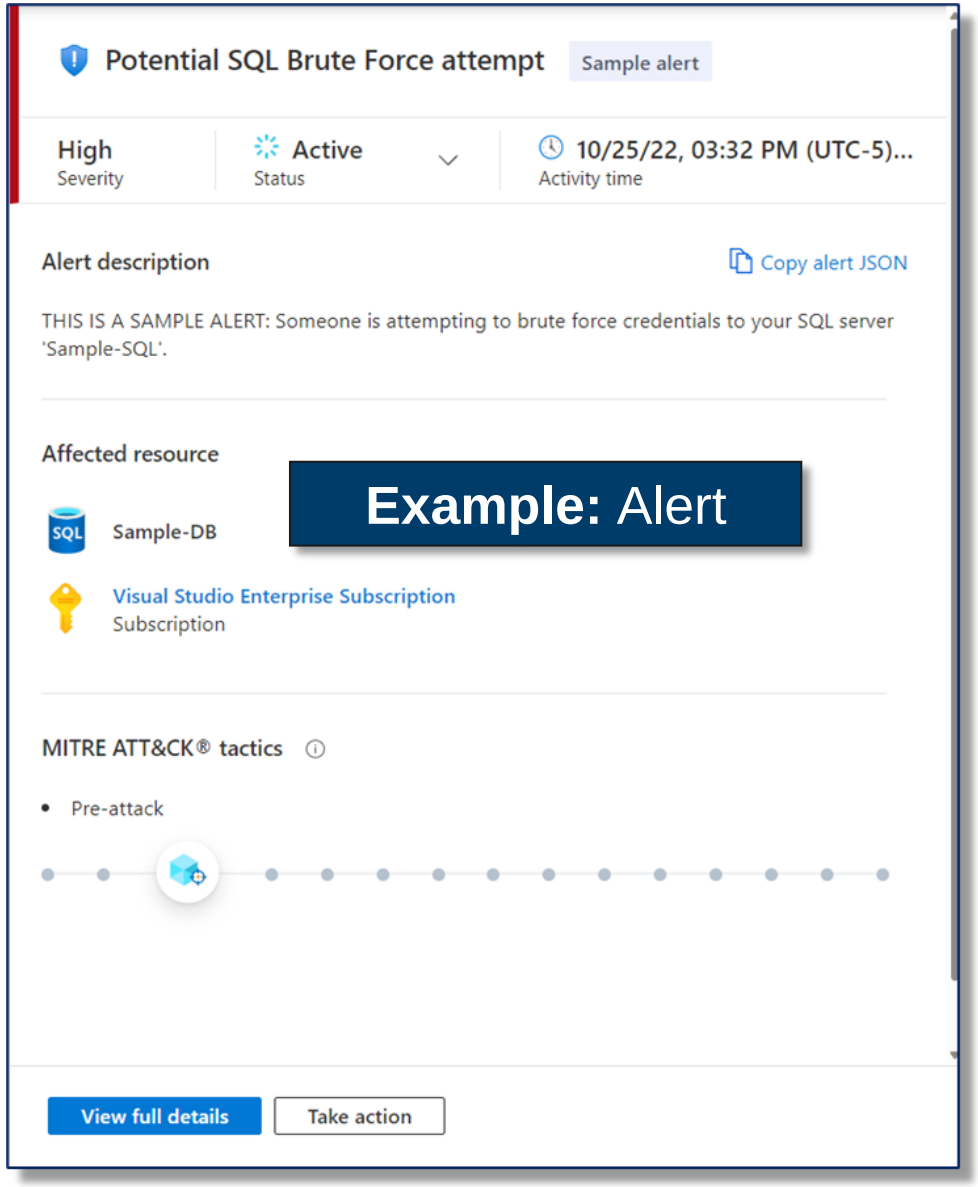
Types of Brute Force Attack Programs and Use Case	
Password crackers	used for guessing passwords and encryption keys.
Port scanners	used to identify open ports on a network or system.
Network mappers	used to map the topology of a network.
Web application servers	used to test web applications for vulnerabilities.
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.



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

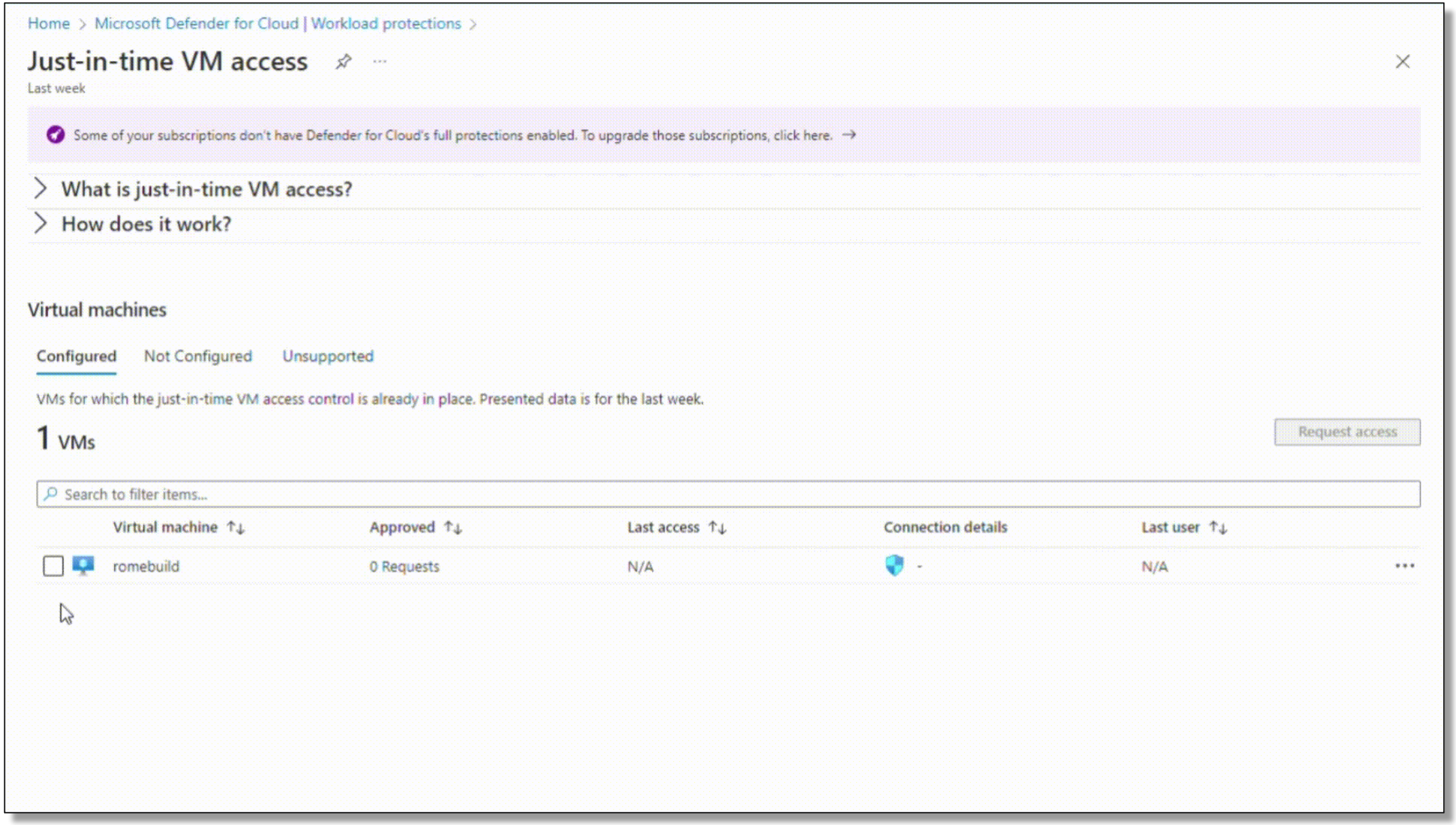
3. Increase password length and complexity. (i.e., **Ztyn%9*qvB**)

4. Limit login attempts

5. Implement Completely Automated Public Turing test "CAPTCHA"

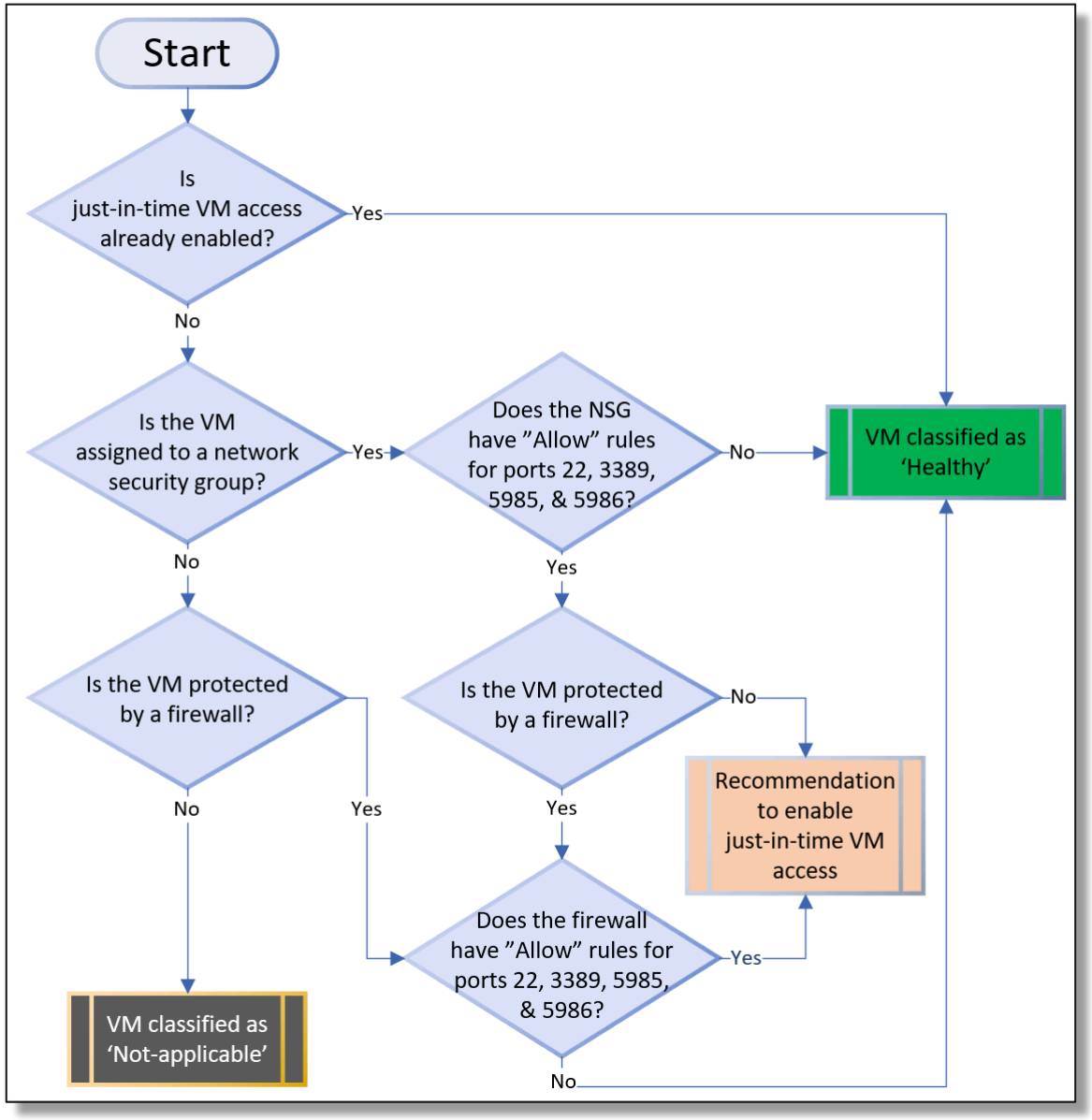
6. Limit the amount of time that the ports are open.

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



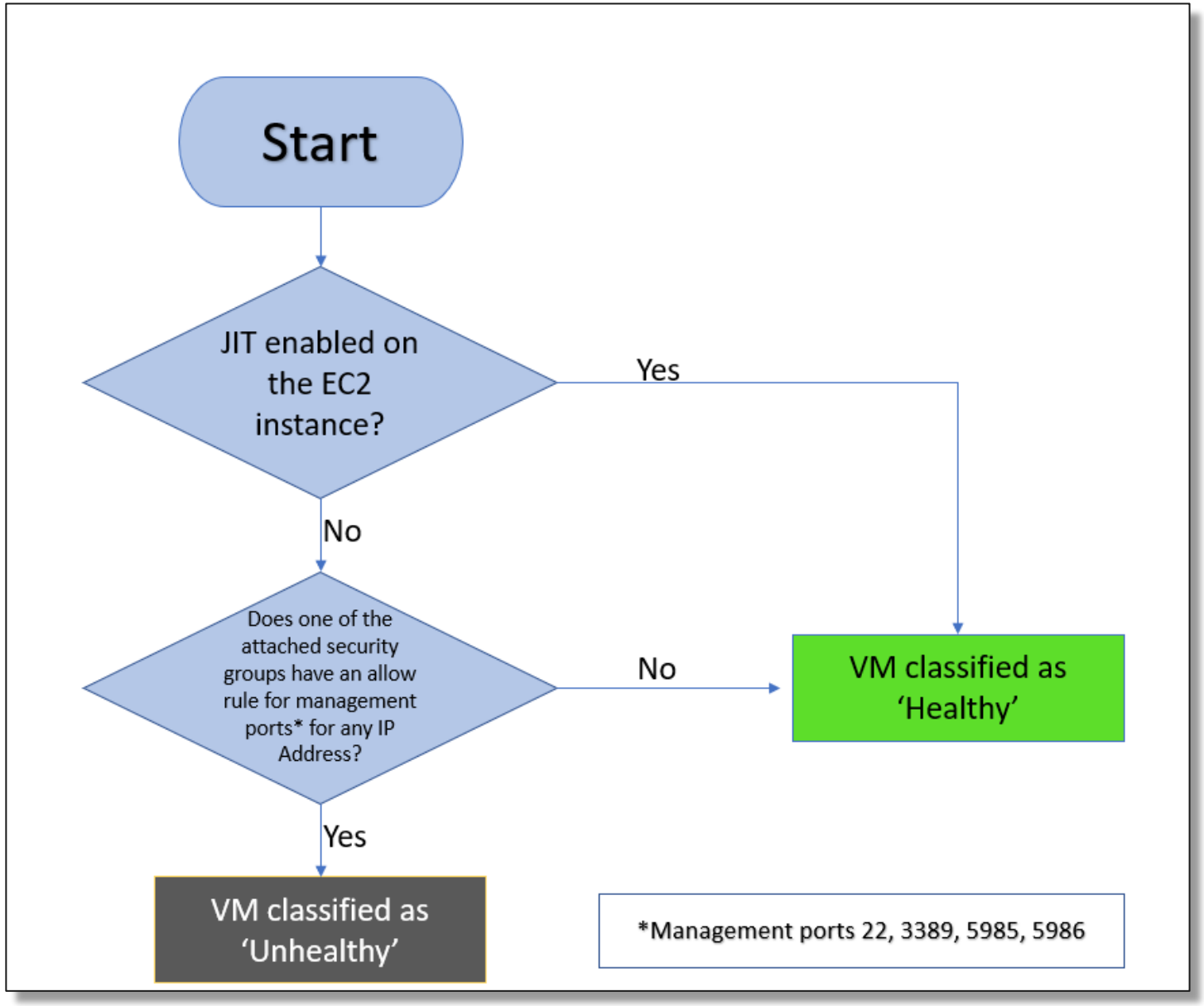
Just-in-time VM is enabled an Azure Virtual Machine

Example: Azure Virtual Machine



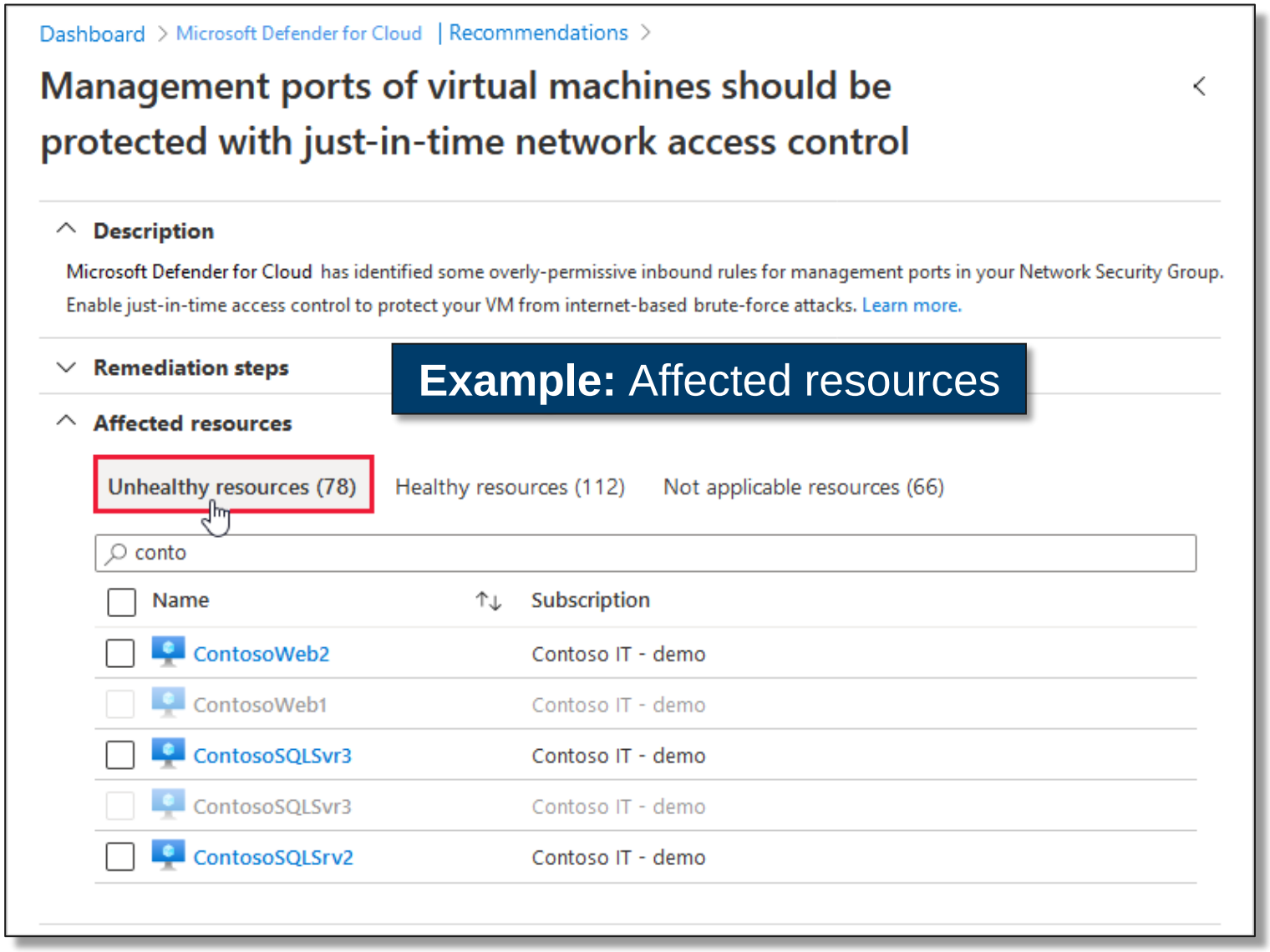
Just-in-time VM is enabled on the AWS EC2 Instance

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.

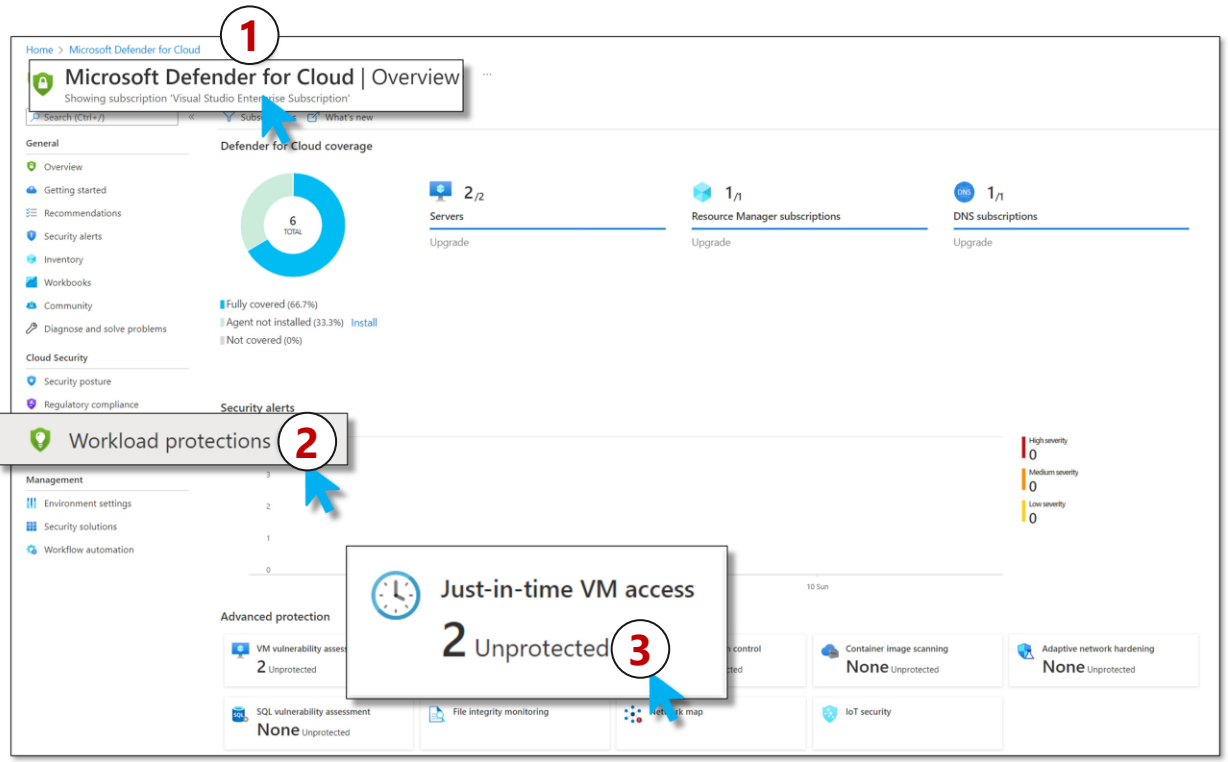


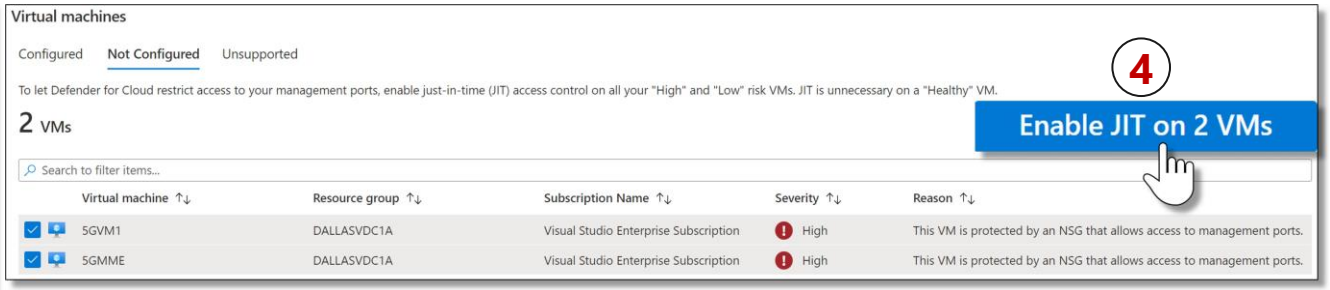
Implement Just-in-time VM access

- 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.

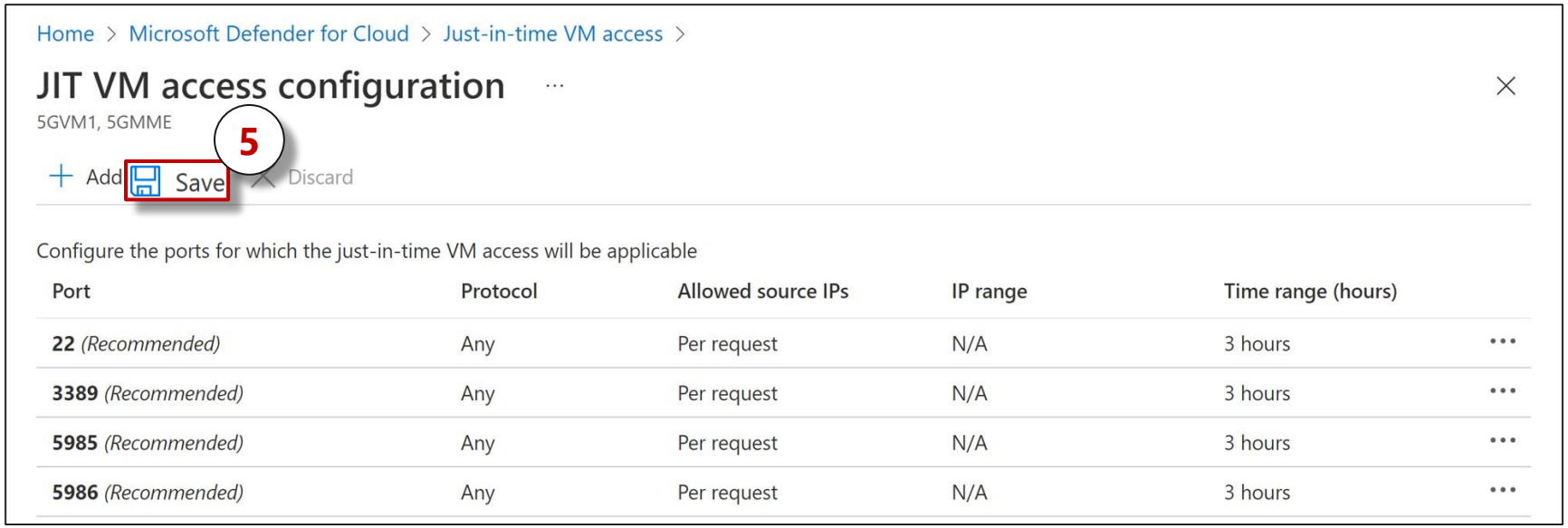


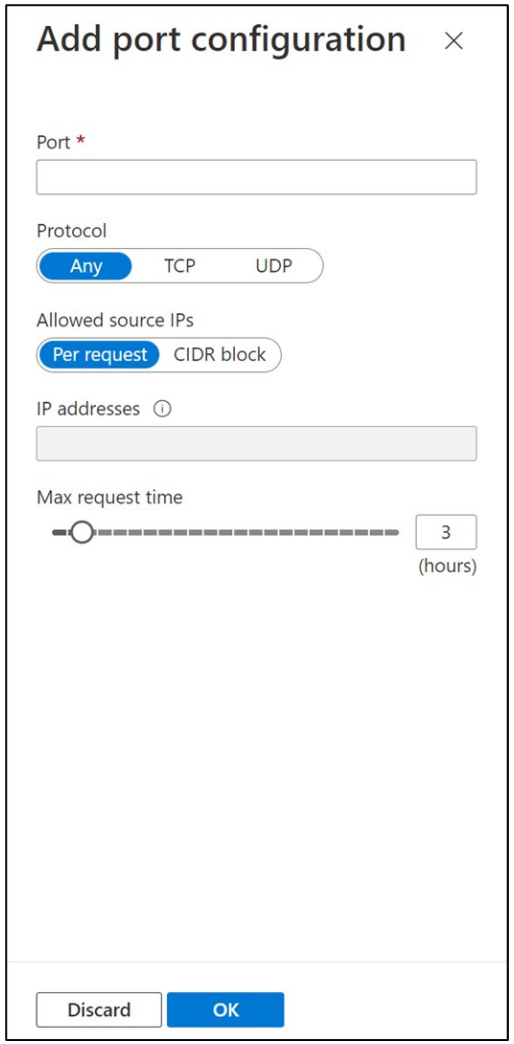


Implement Just-in-time VM access (continued)

C 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.

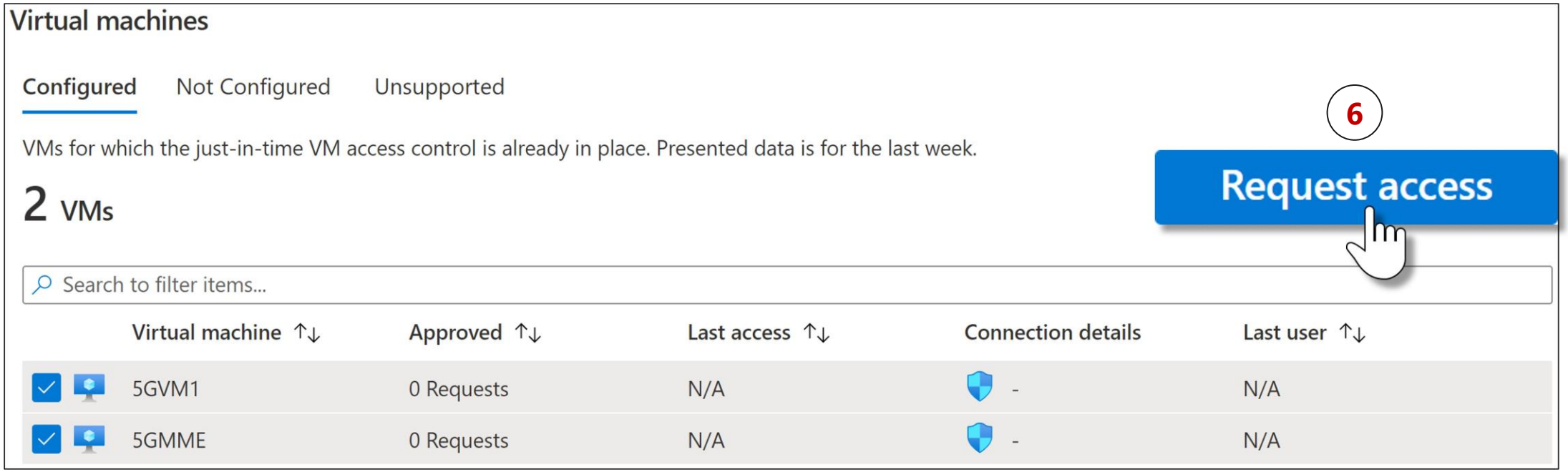




Implement Just-in-time VM access (continued)

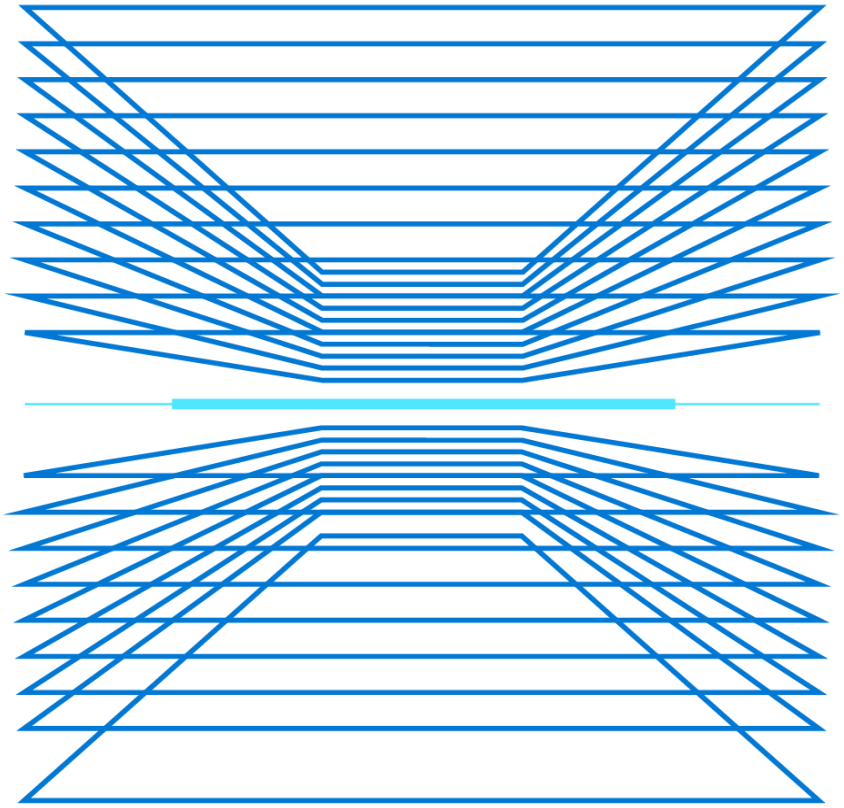
E Once everything is in place, users must request access to the virtual machine.

You can also monitor the usage of each virtual machine.



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)
	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

Microsoft Sentinel

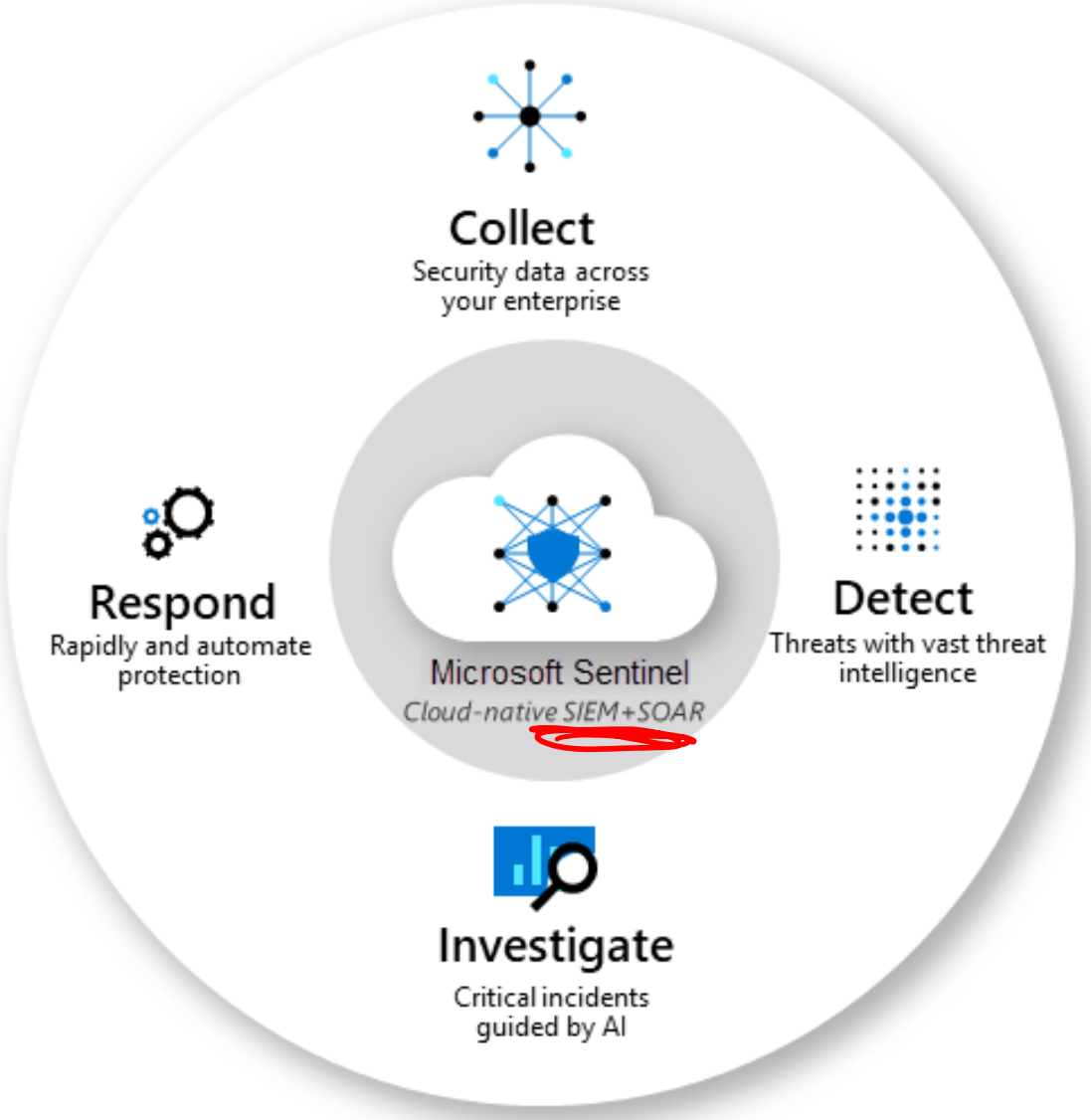
Splunk

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

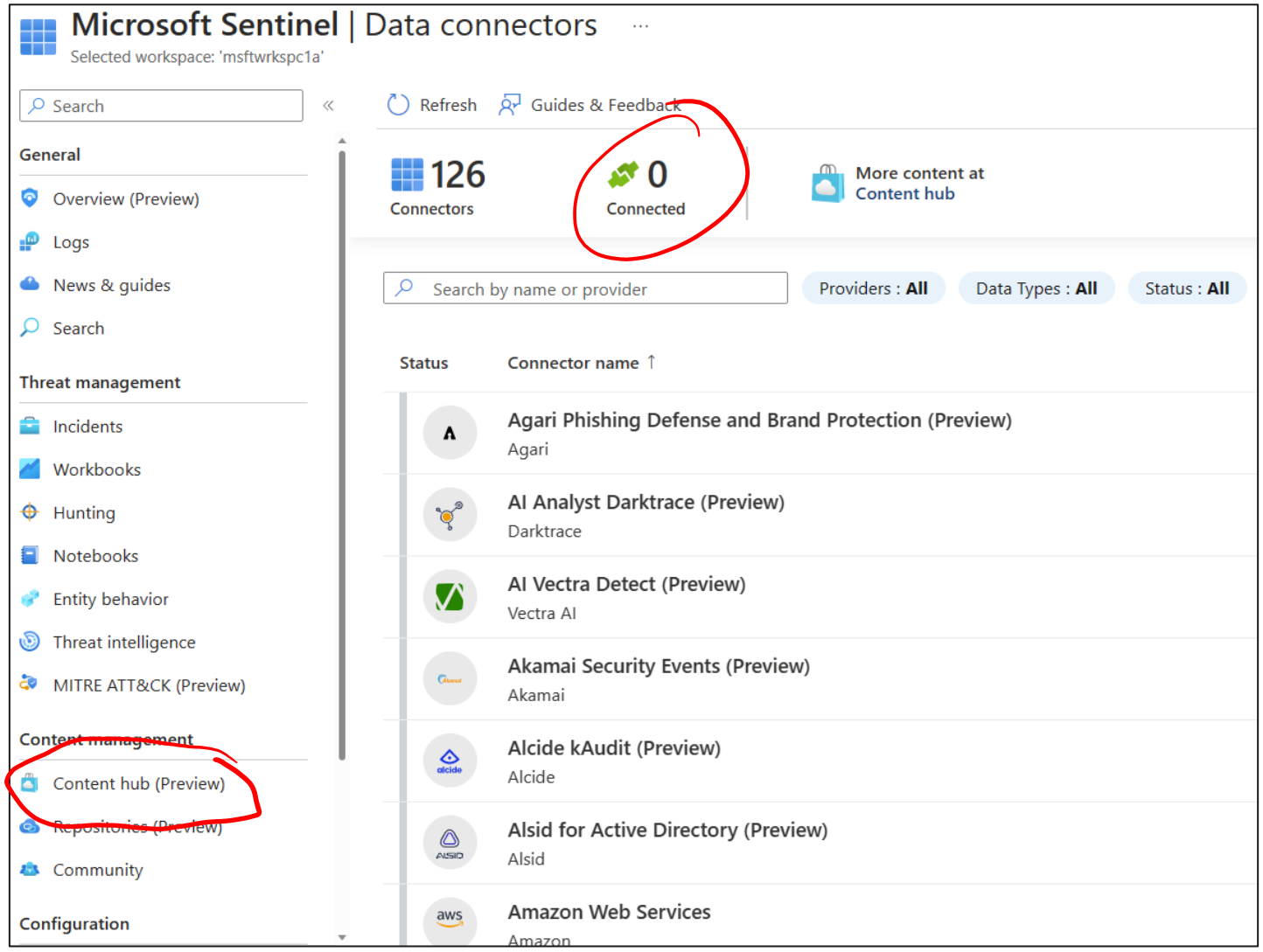


Data Connections

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.

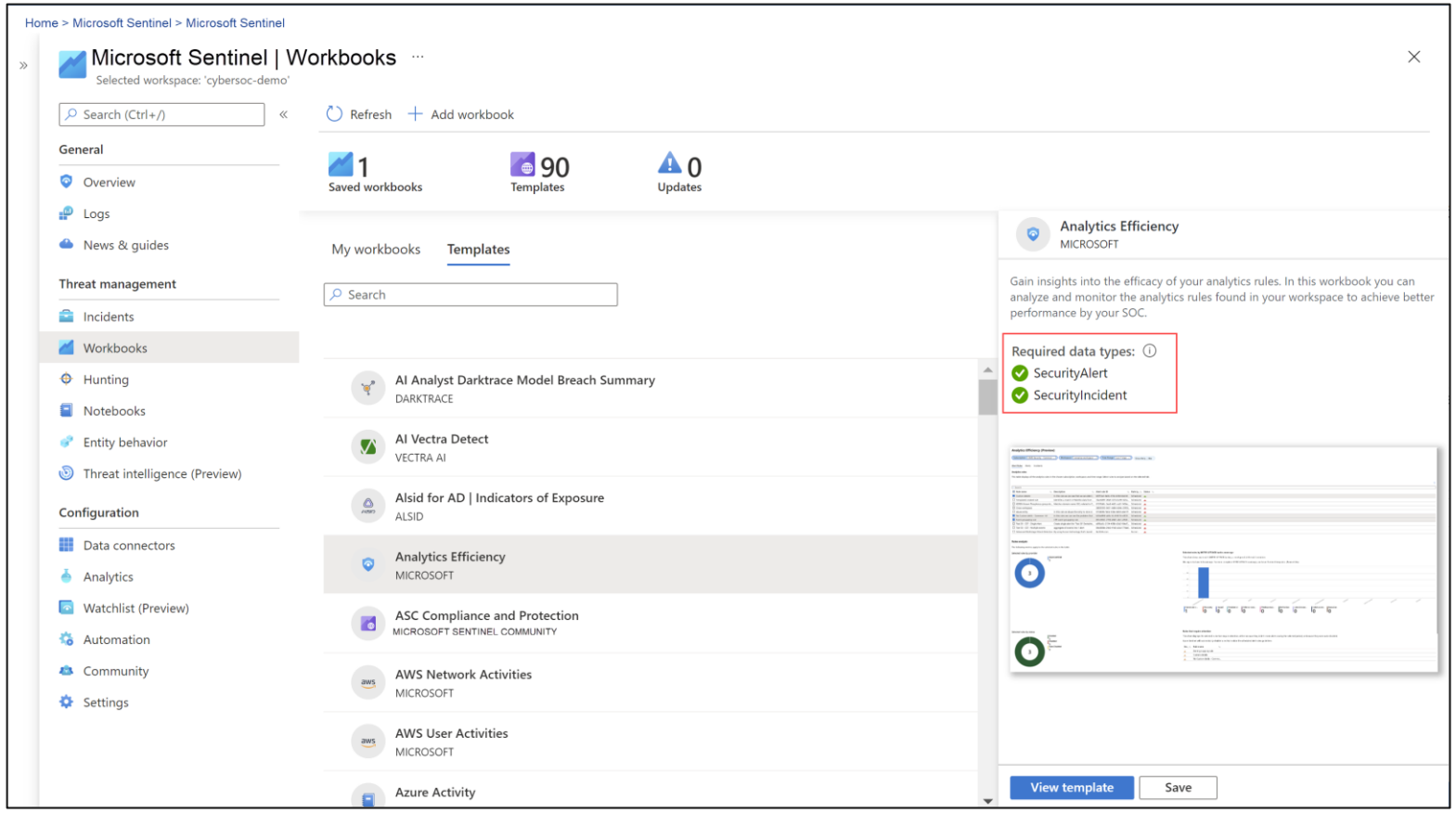


Workbooks

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.

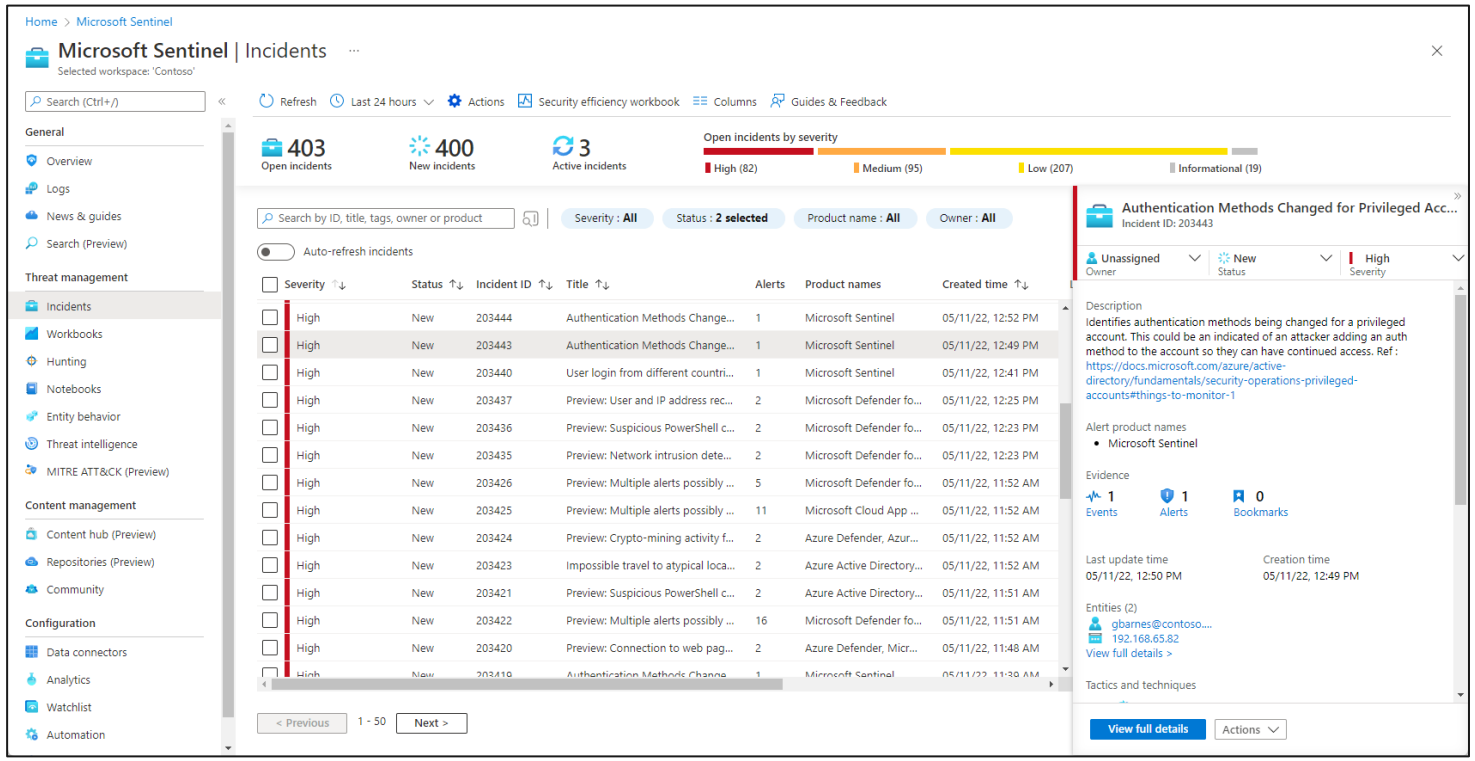


Incidents

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.

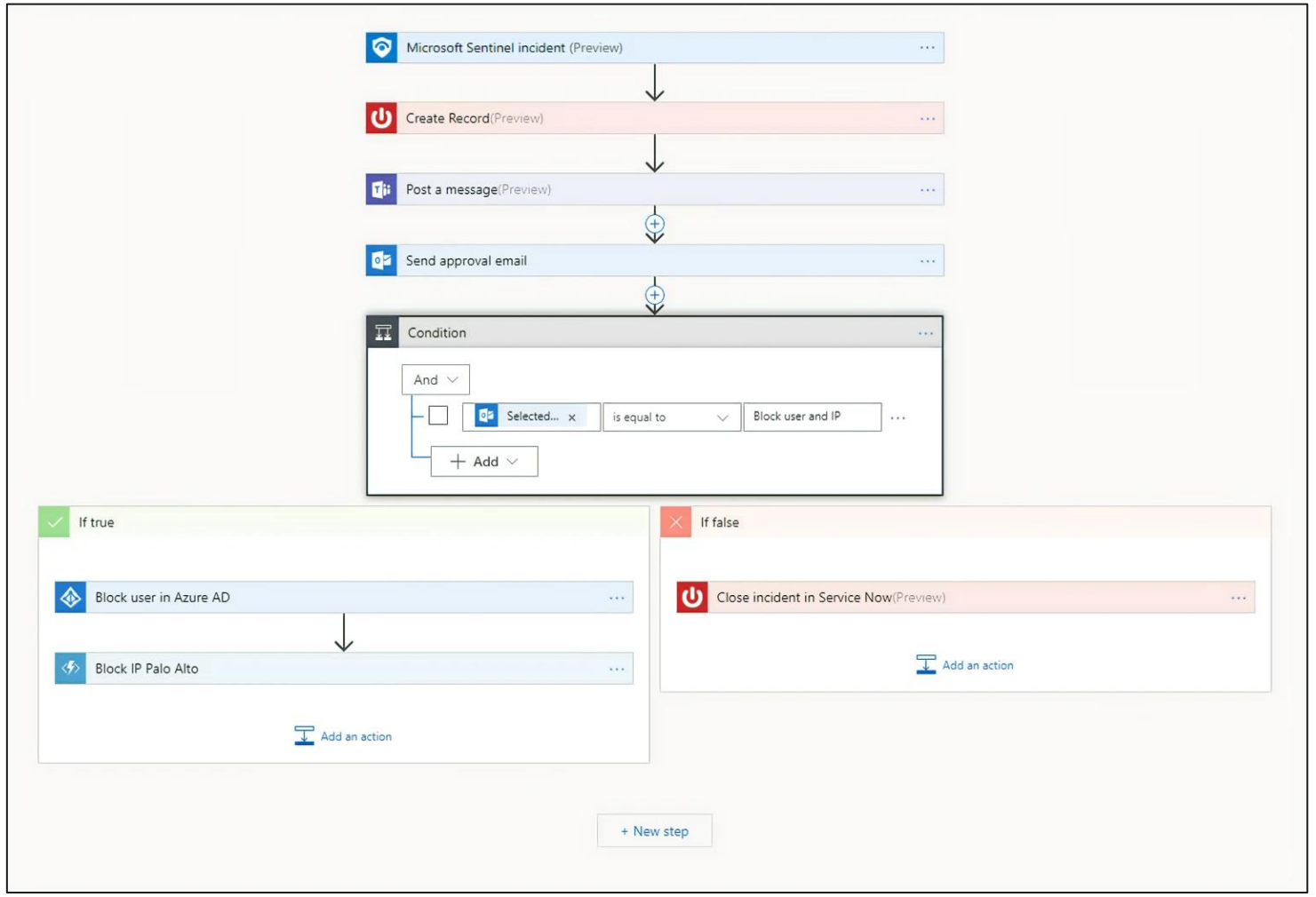


Playbooks

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.

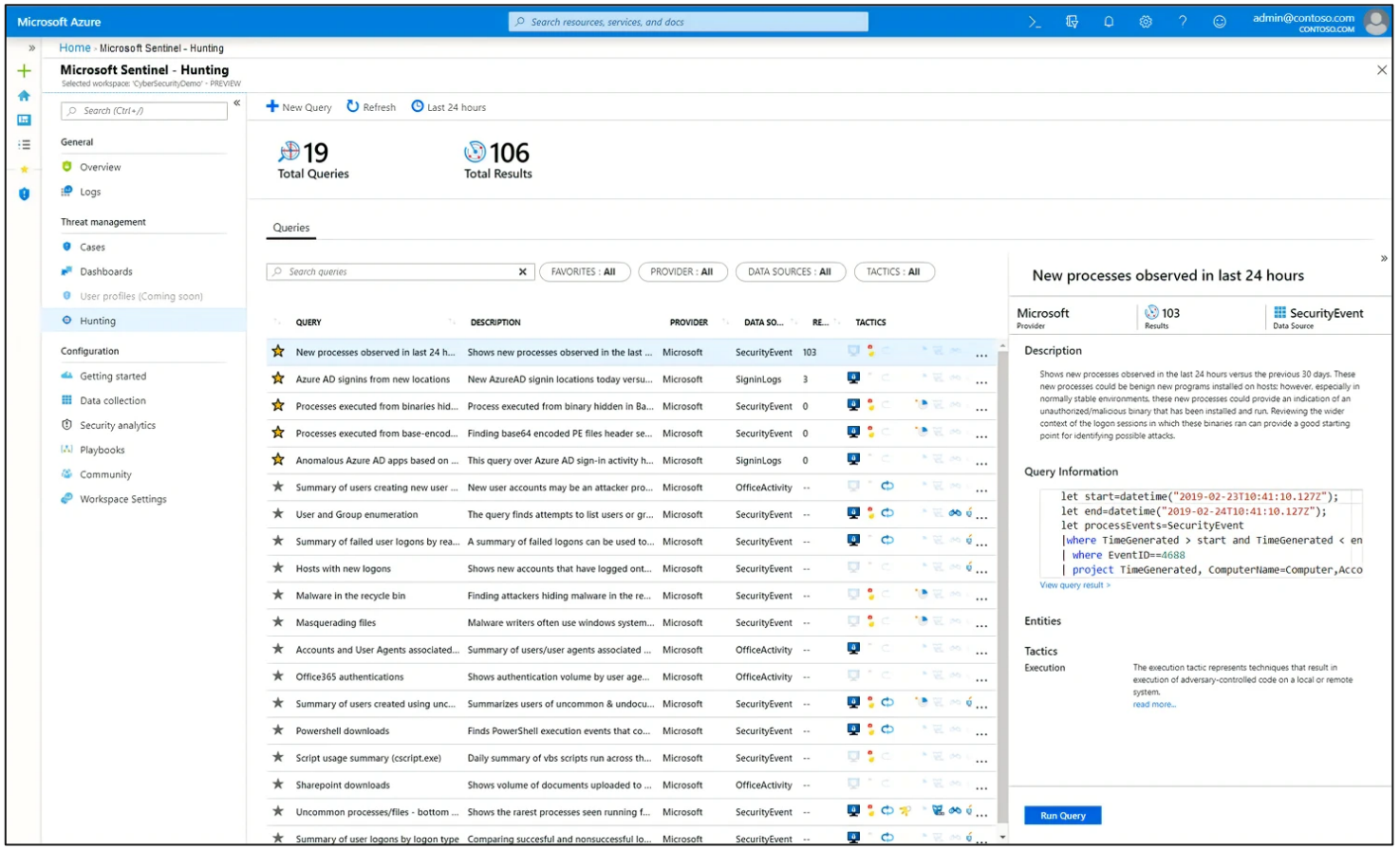


Hunting

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.



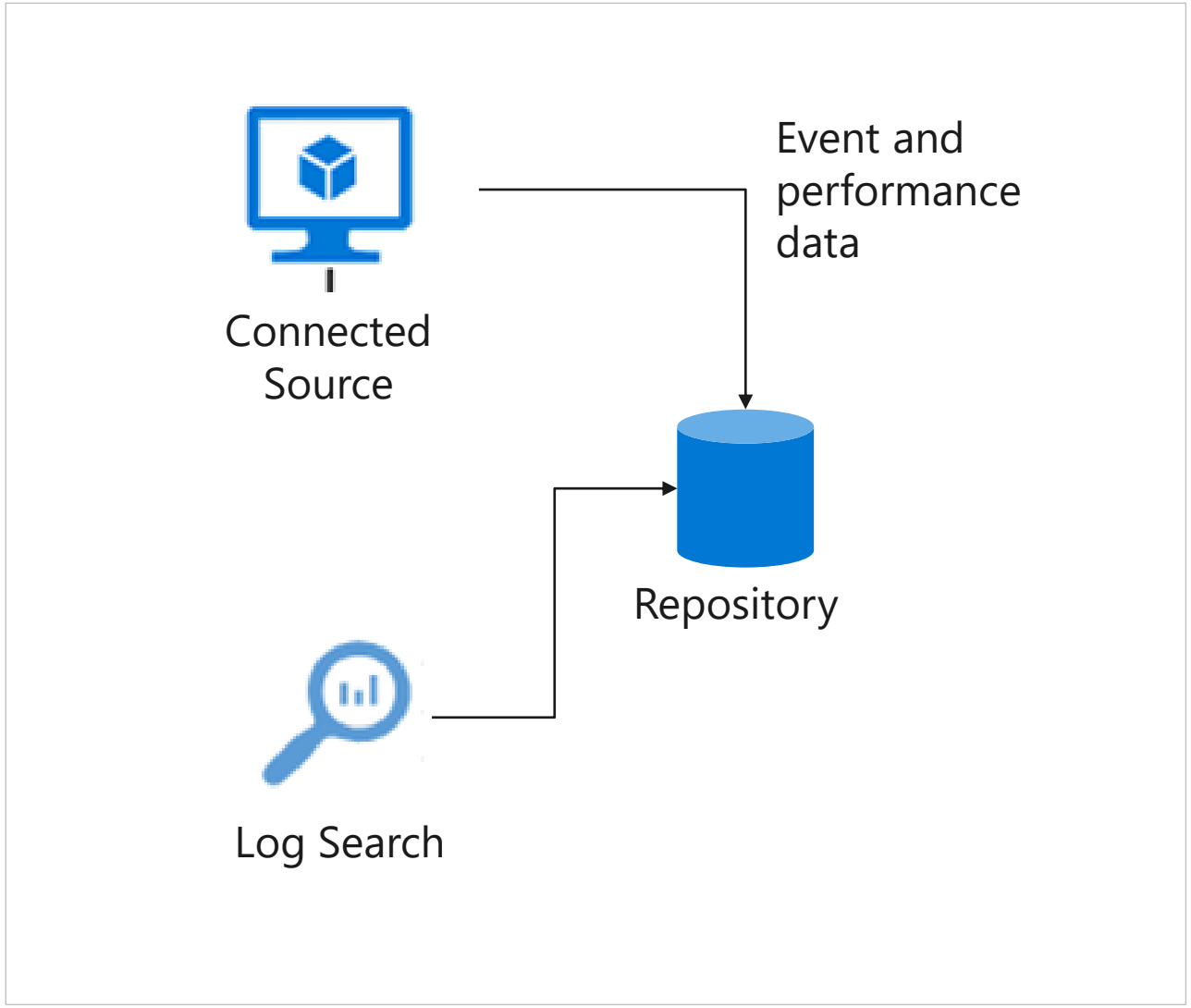
Additional Study – Microsoft Sentinel

Module Review Questions	Microsoft Learn Modules (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

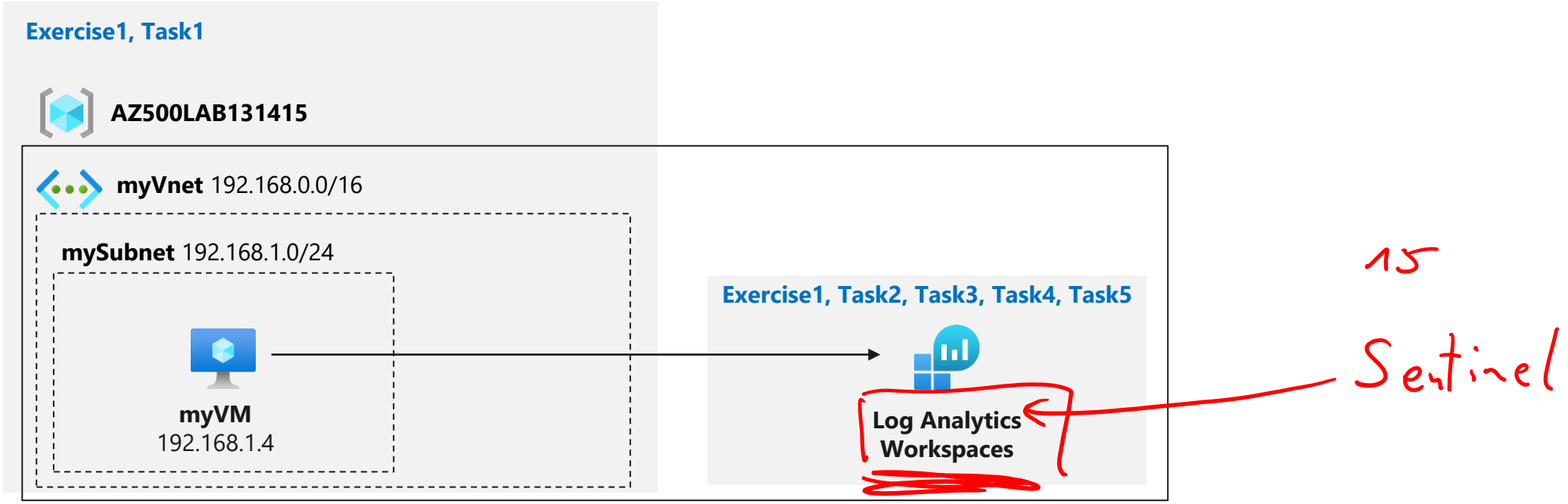
Module Labs

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

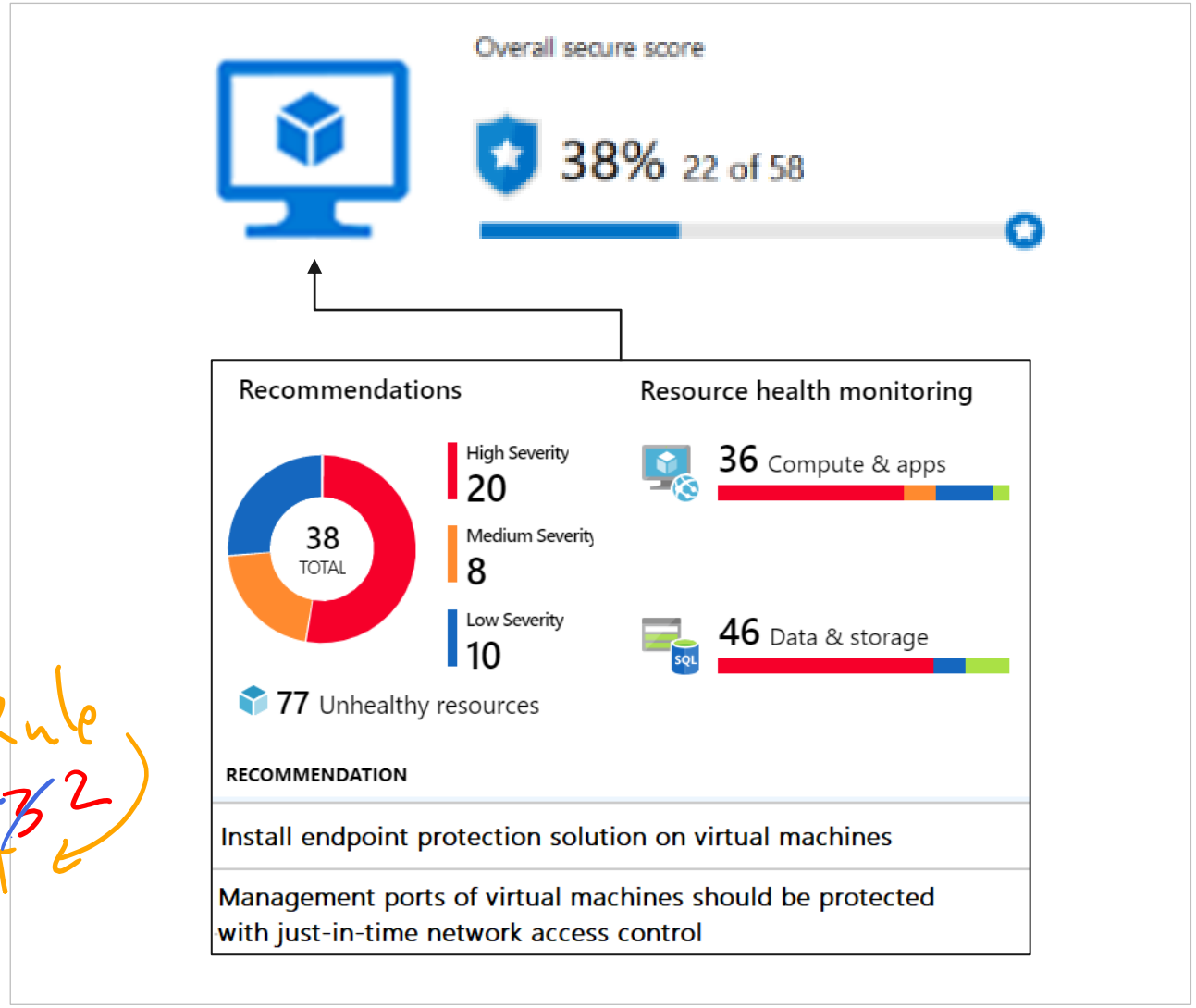


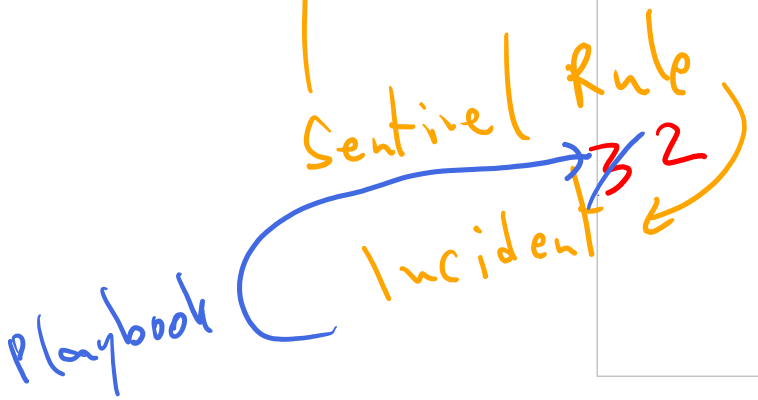
Lab 13 – Azure Monitor



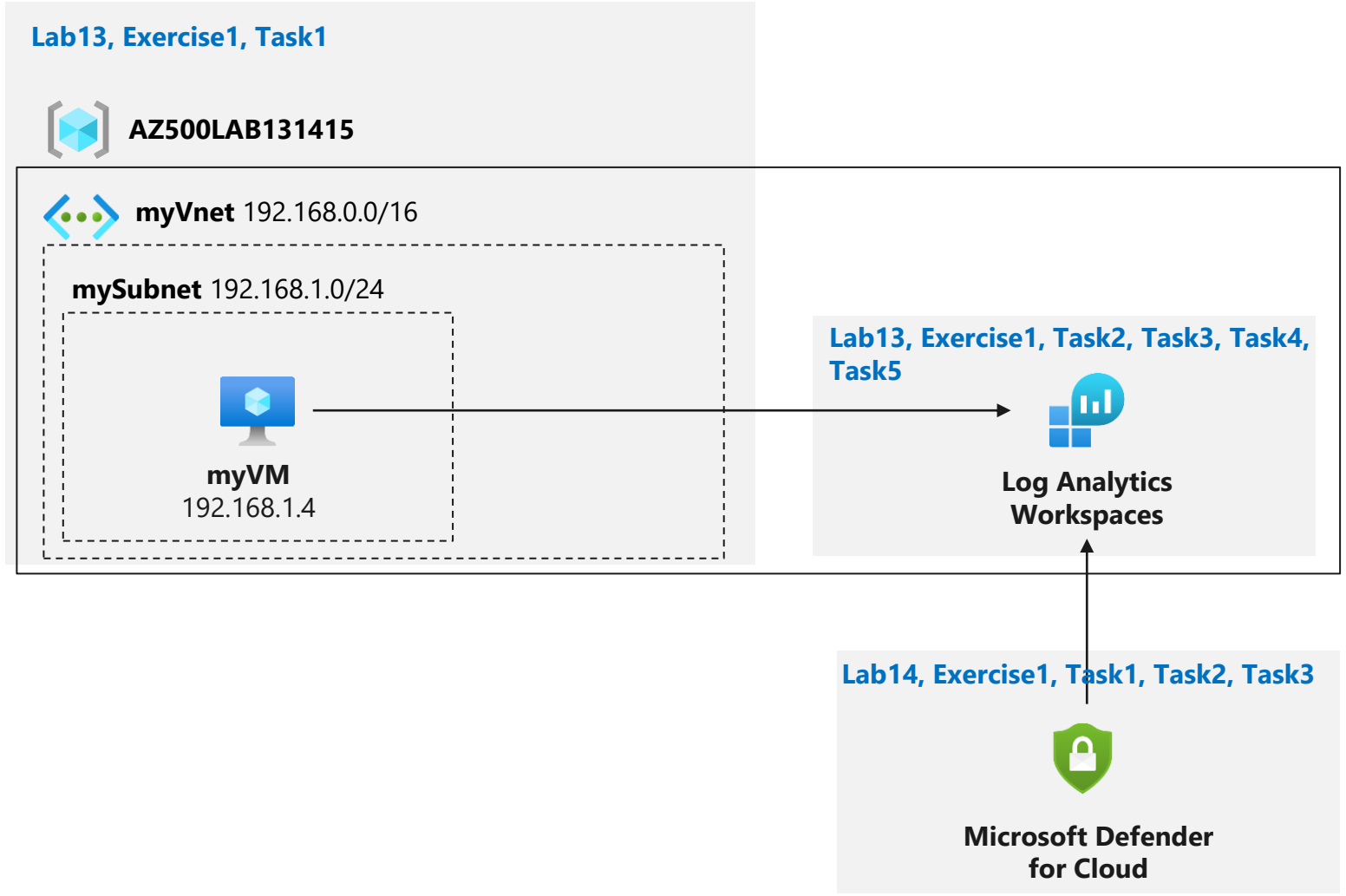
Lab 14 – Microsoft Defender for Cloud

- 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

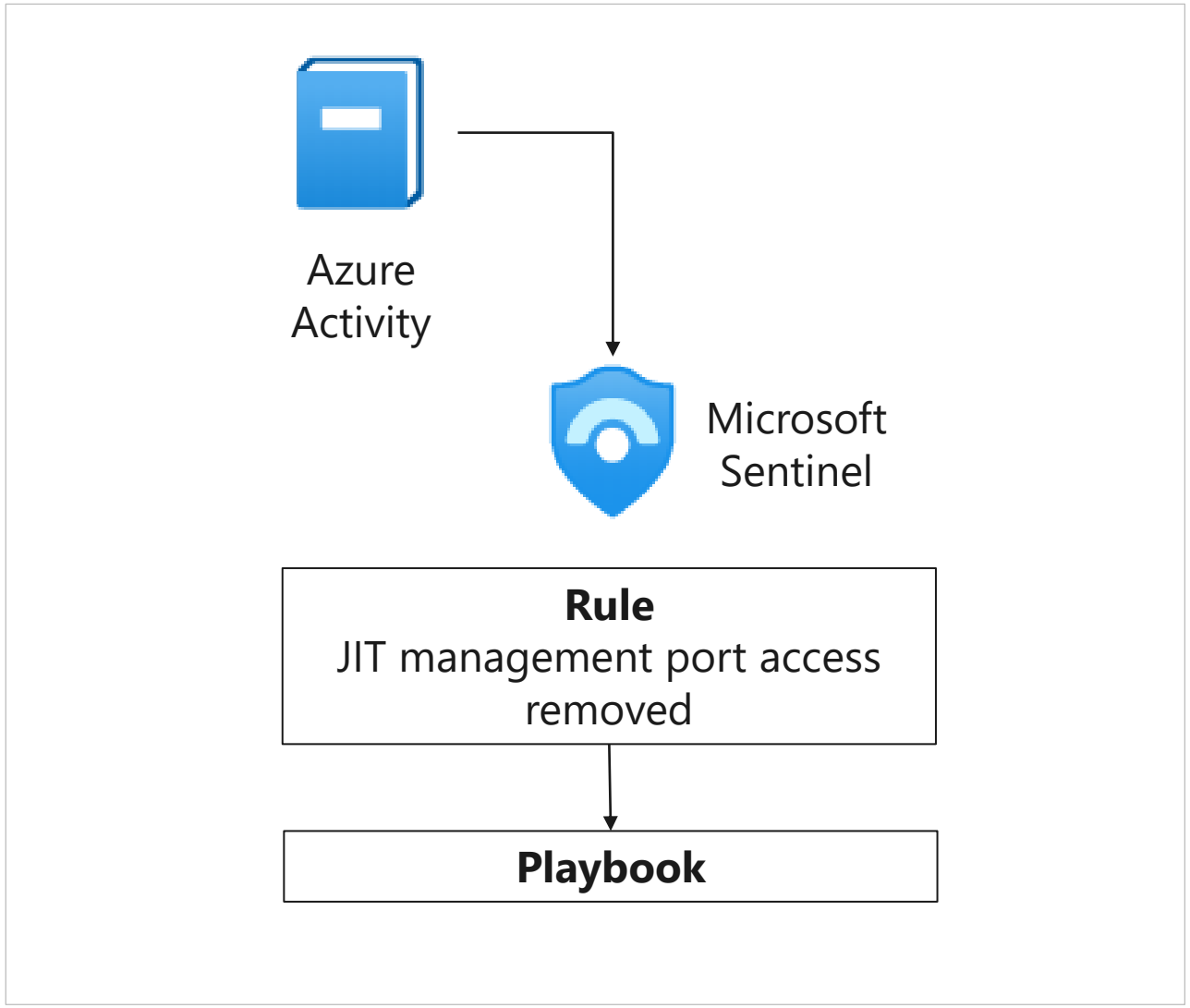
Connect Azure Activity to Sentinel

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

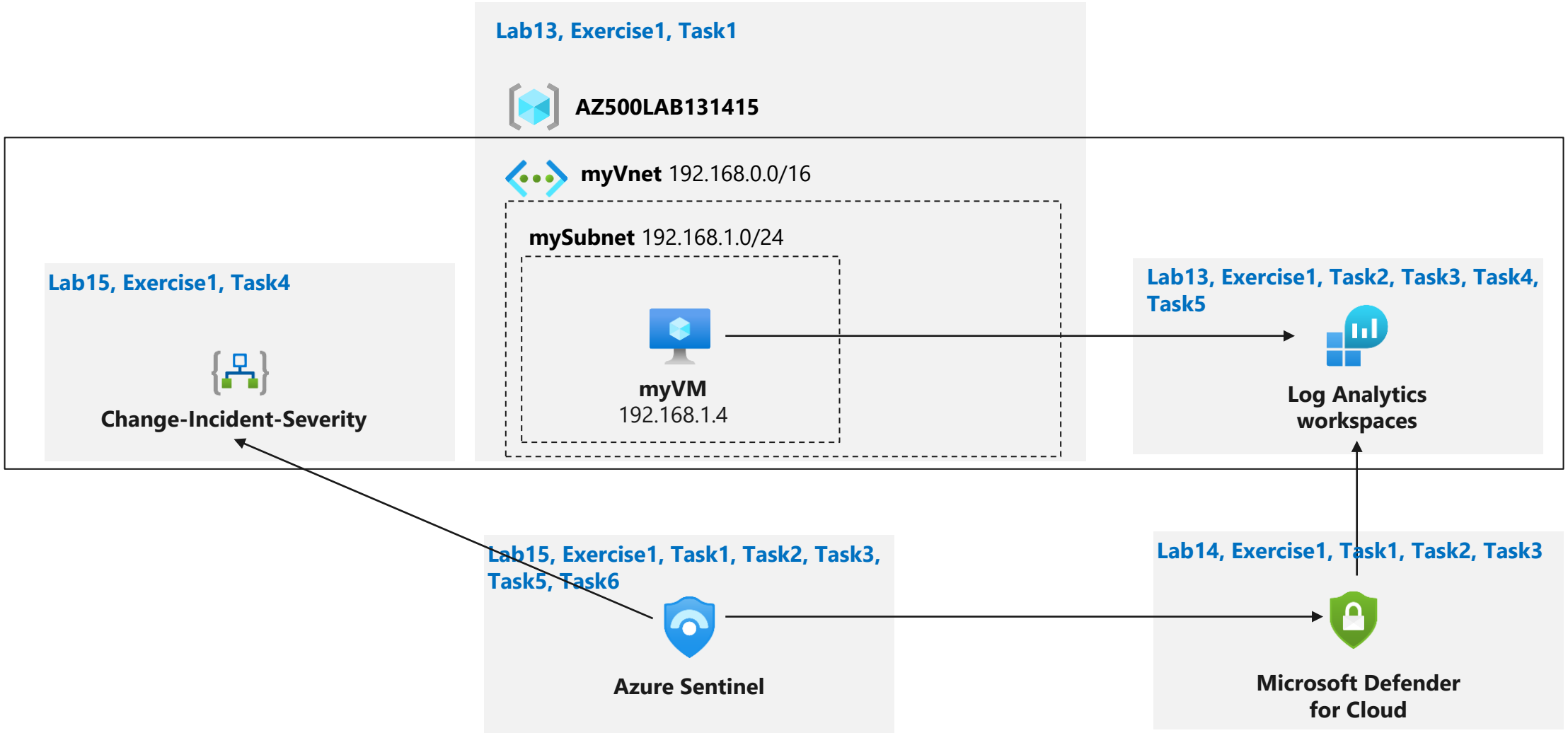
Create a playbook

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