Microsoft

Code
Learn

Feedback
MTM
5
++

Tag 4

AZ-500

Microsoft Azure Security Technologies

Guten Morgen!

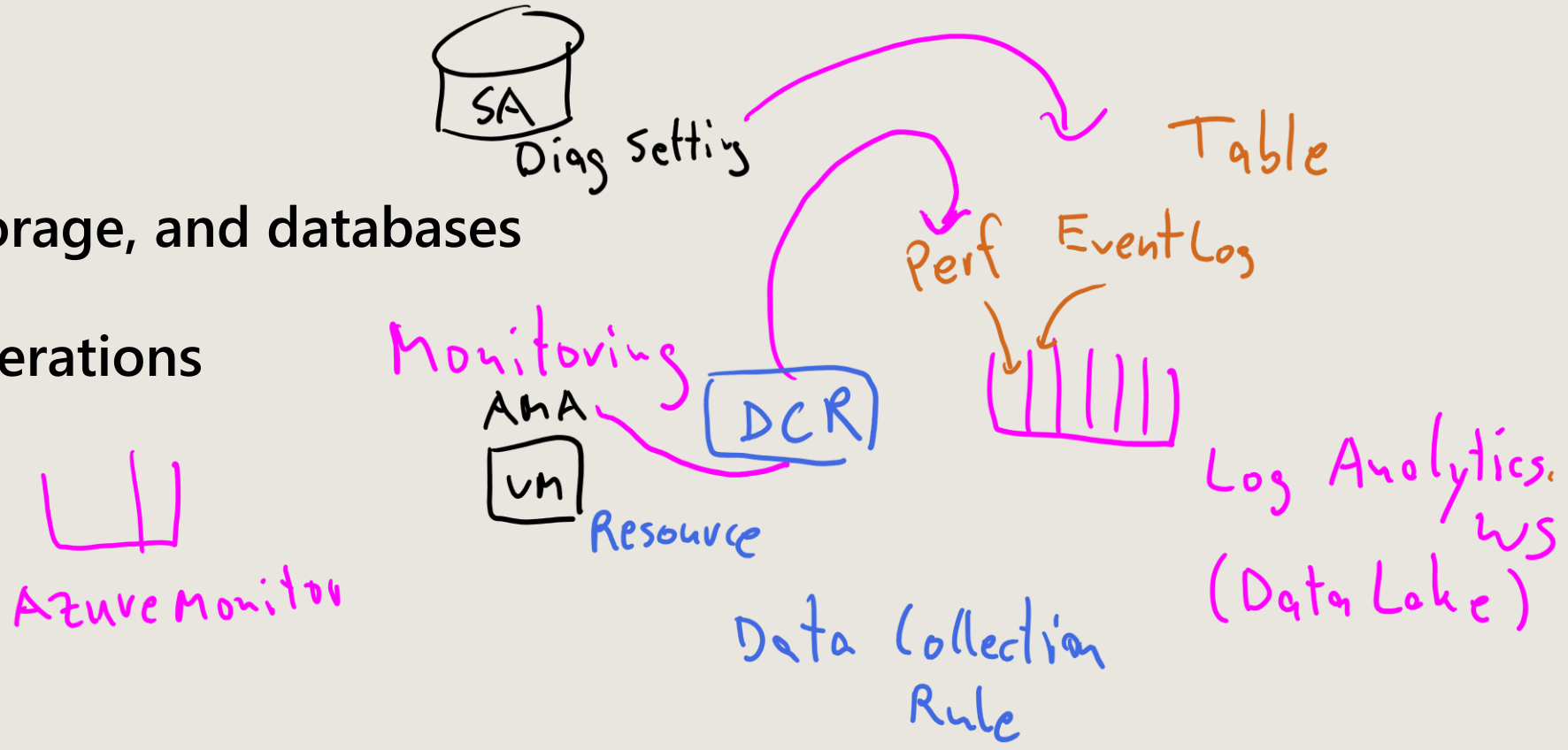
Agenda

1 Manage identity and access

2 Secure networking

3 Secure compute, storage, and databases

4 Manage security operations



Learning Path: Manage security operations

Plan, implement, and manage governance for security

Manage security posture by using Microsoft Defender for Cloud

Configure and manage threat protection by using Microsoft Defender for Cloud

Configure and manage security monitoring and automation solutions

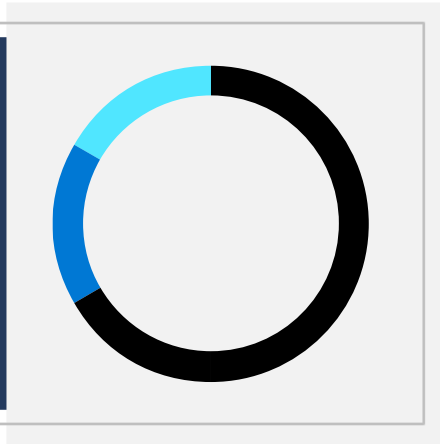
Module Labs

Learning Objectives

After completing this learning path, you will be able to:

1. Implement security operations, establish governance, and deploy Azure policies, infrastructures, while securing keys and certificates.
2. Enhance Defender's security posture, ensure compliance, and monitor external threats.
3. Set up Defender for diverse threats, manage alerts, and leverage Sentinel for advanced security strategies.

Azure Monitor

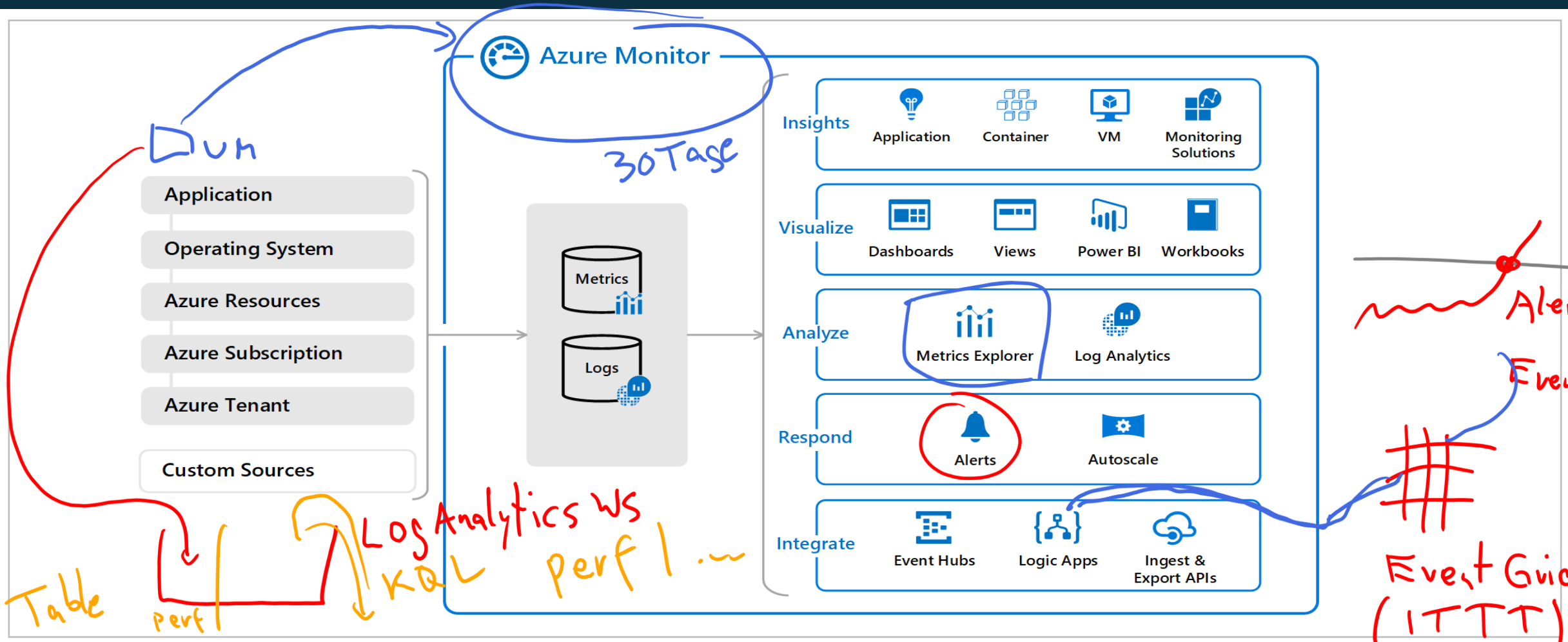


Azure Monitor Architecture

Kusto Query Lang
KQL

Data Lake

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

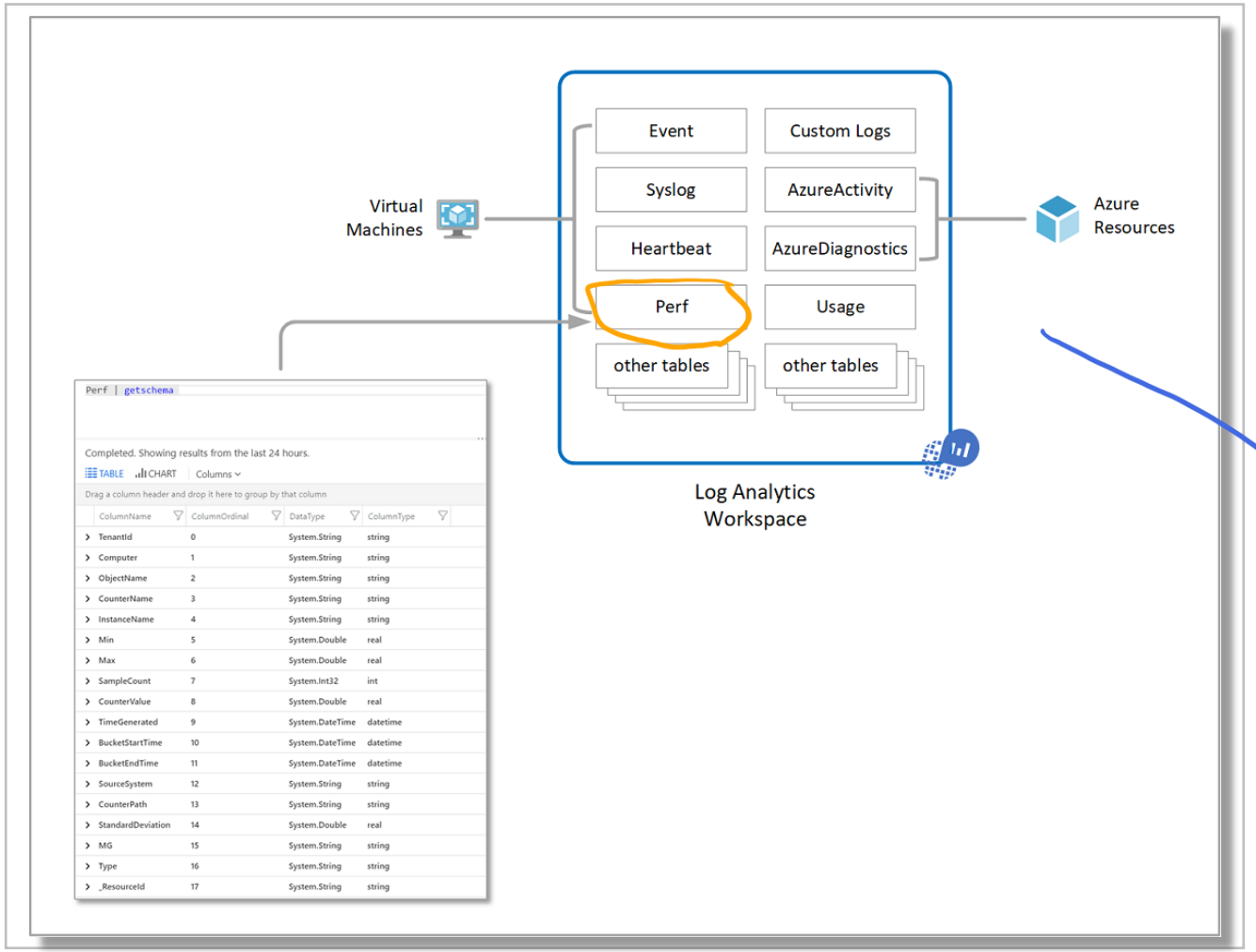
They are lightweight and capable of supporting near real-time scenarios

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.



SIEM
SOAR

Connector

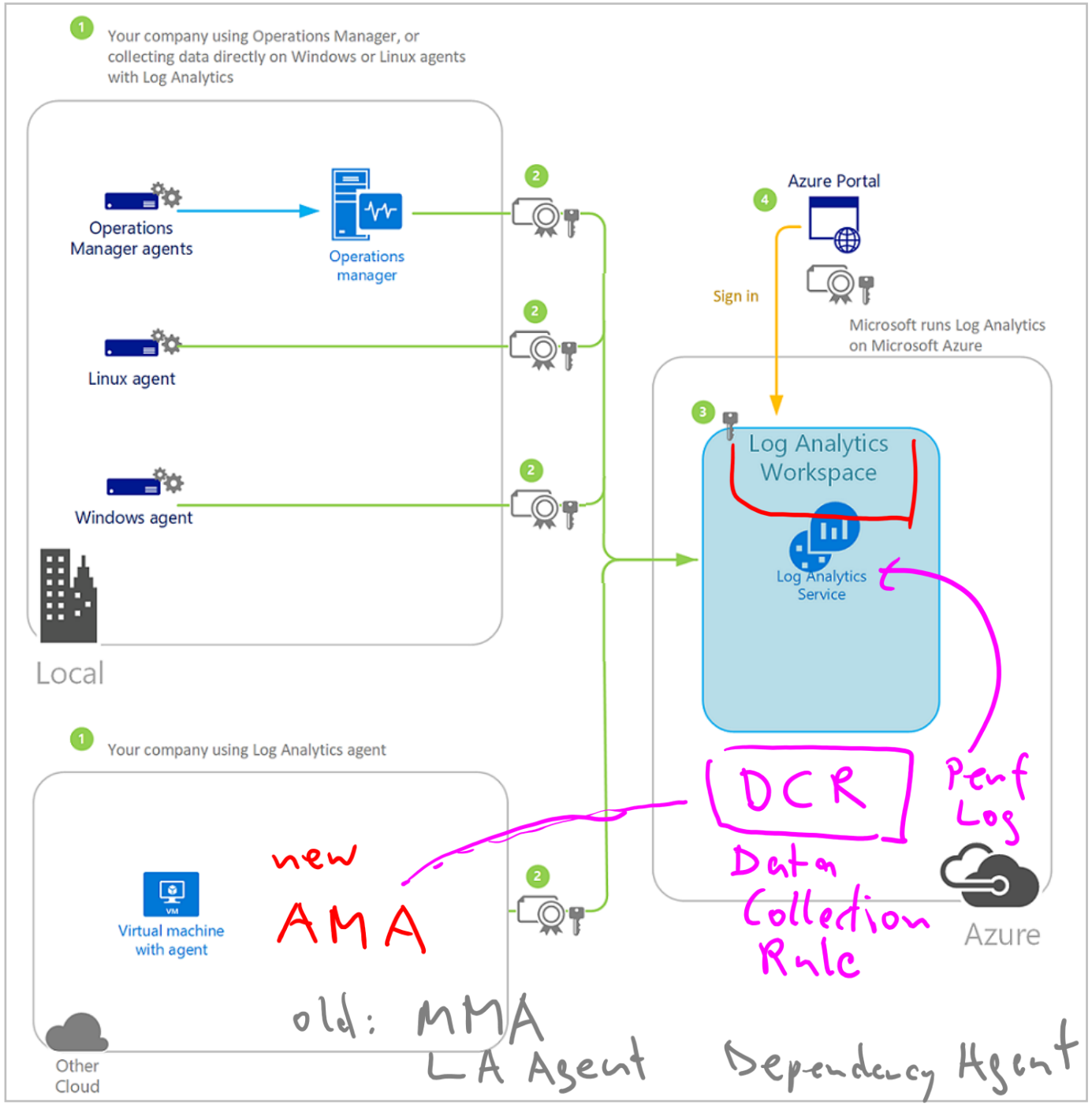
Sentinel
KQL

LA
workspace

Connected Sources

Connected Sources generate data

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



Azure Monitor Alerts

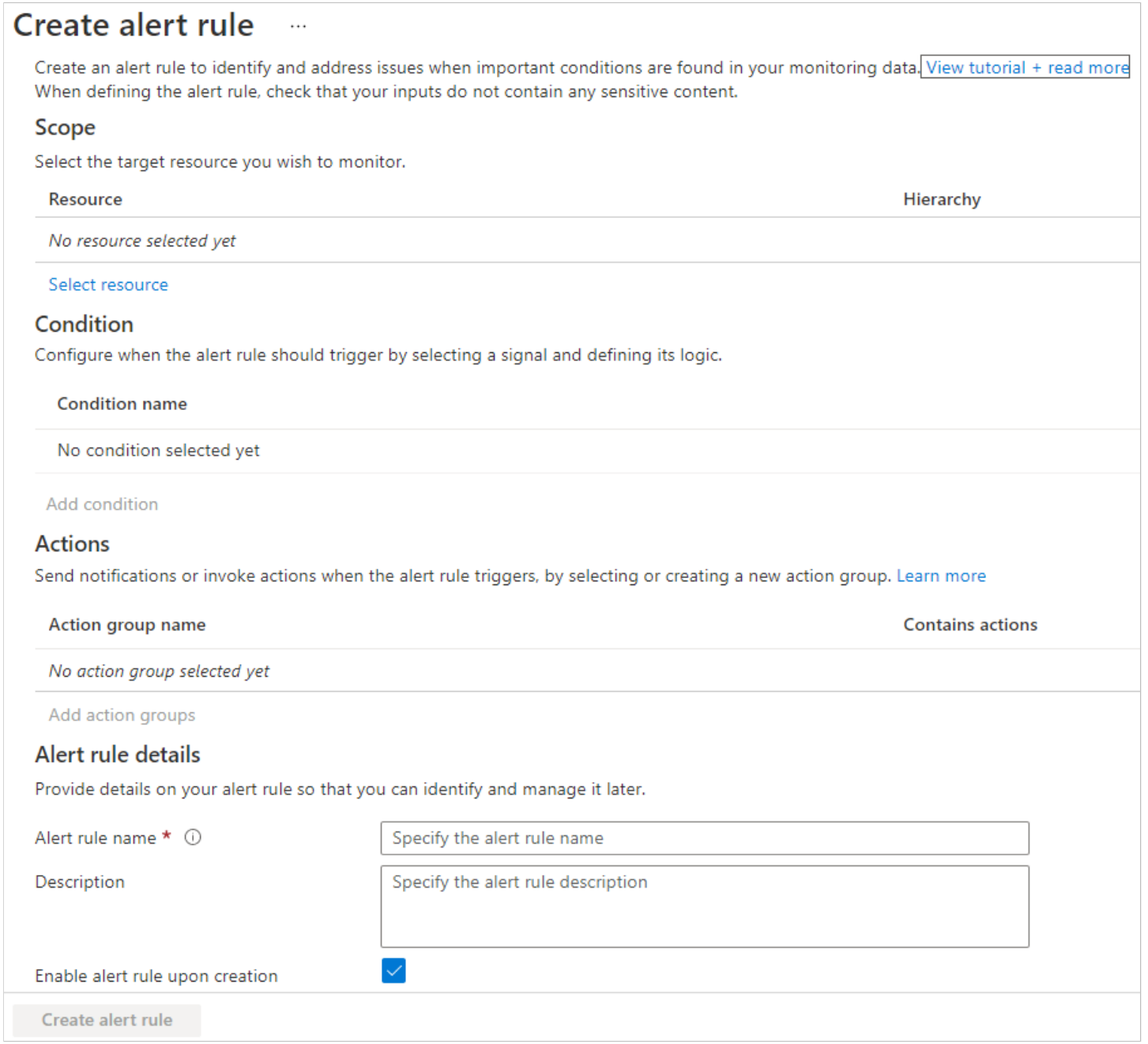
Select the target resource to monitor

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



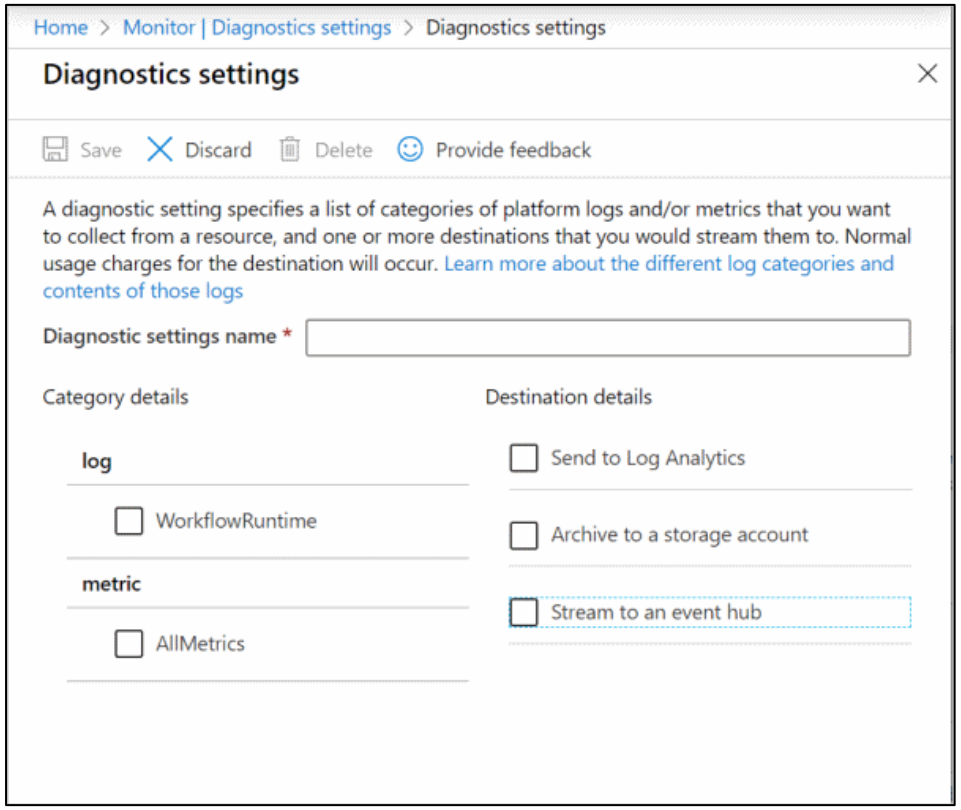
Diagnostic Settings

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

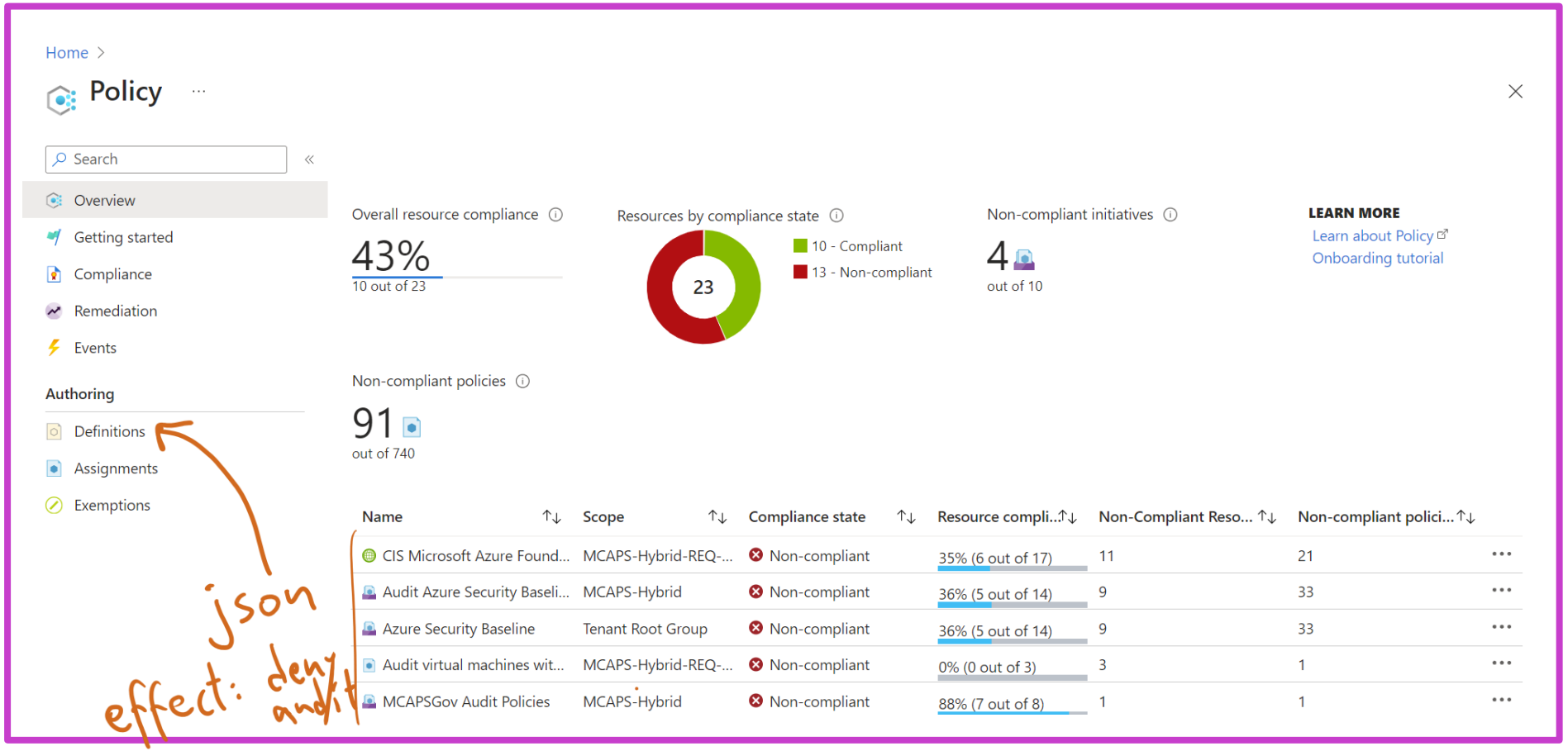
Retention times are available for archiving to a storage account



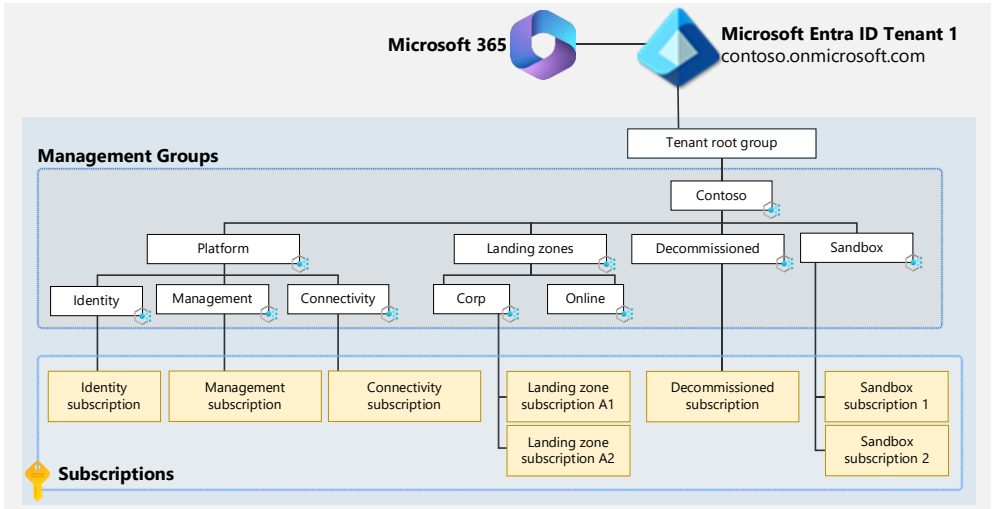
Plan, implement, and manage governance for security

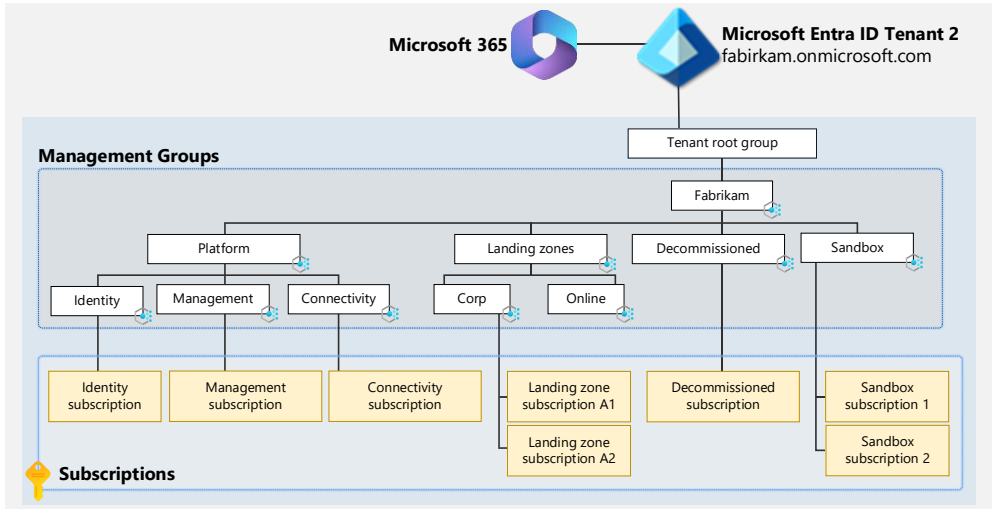
Create, assign, and interpret security policies and initiatives in Azure Policy

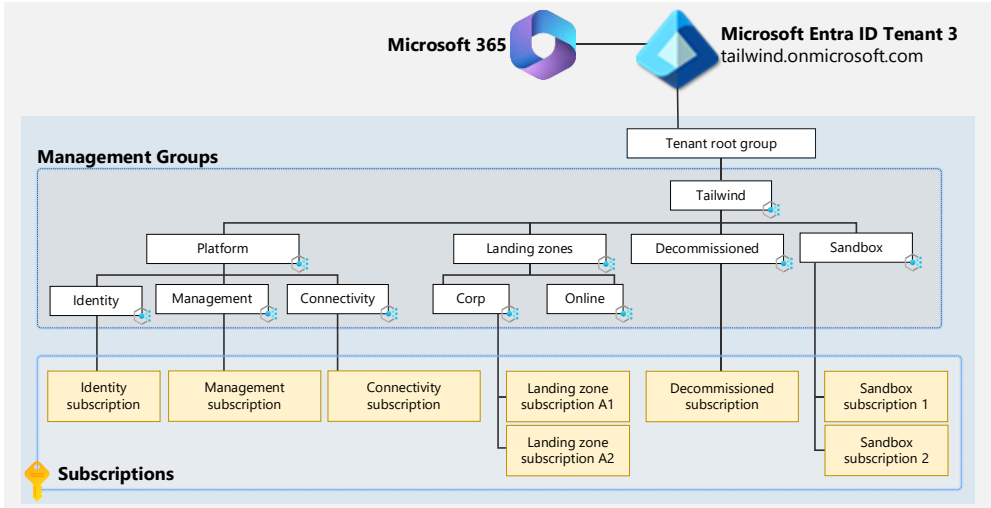
- Use Azure Policy for compliance with standards and SLAs.
- Assign policies and initiatives for future resources and compliance tracking.
- Resolve non-compliance and implement new policies organization-wide.

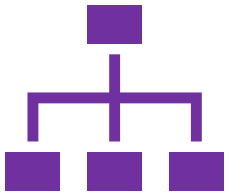


Deploy secure infrastructures by using a landing zone





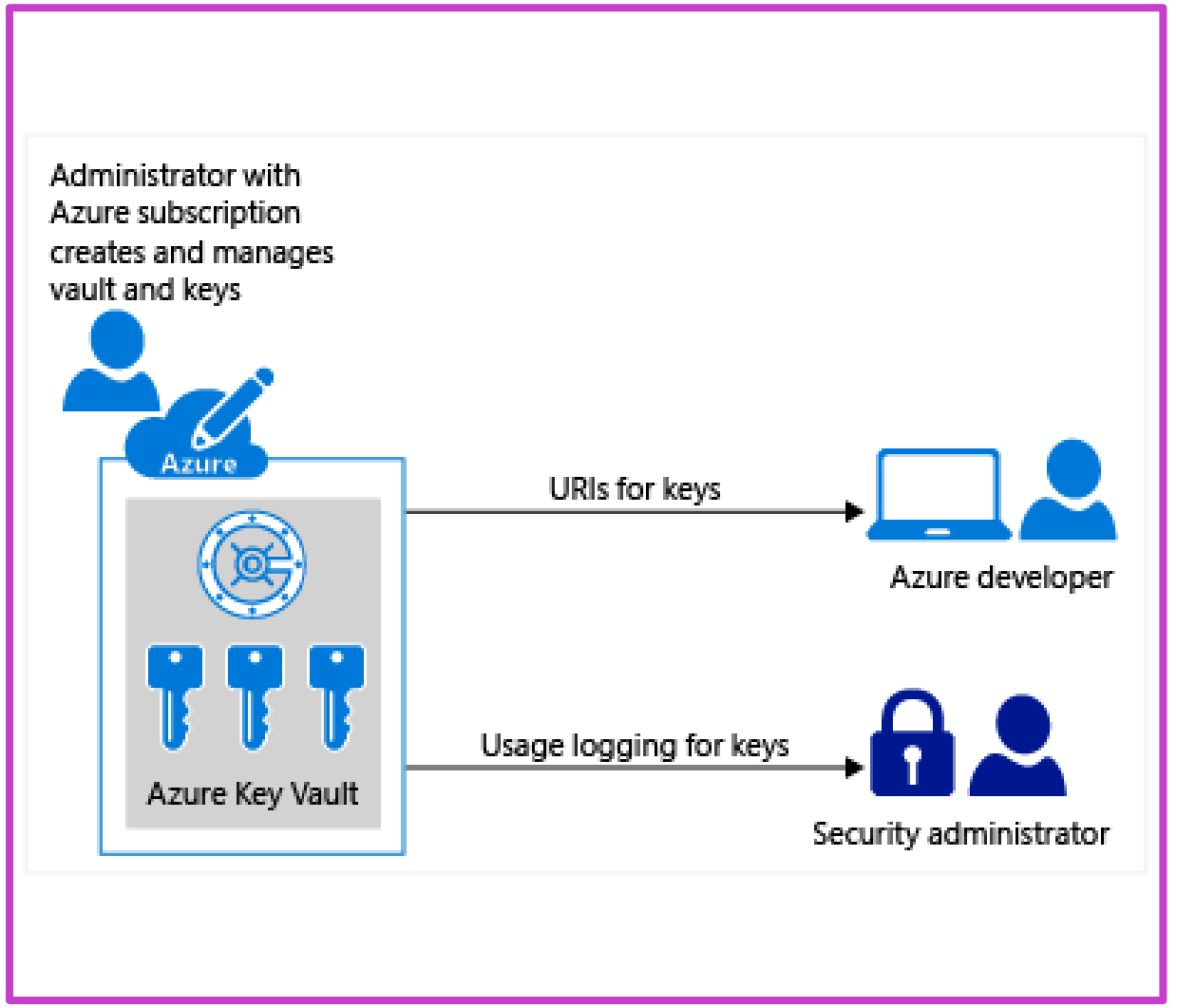




Contoso Corporation's Microsoft Entra ID Tenants

Azure Key Vault

- Azure Key Vault securely stores API keys, passwords, certificates, and cryptographic keys.
- Supports vaults for software/HSM-backed keys and managed HSM pools for HSM-backed keys only.
- Offers managed identities for secure authentication and enforces TLS for data-in-transit protection.



Azure Key Vault security

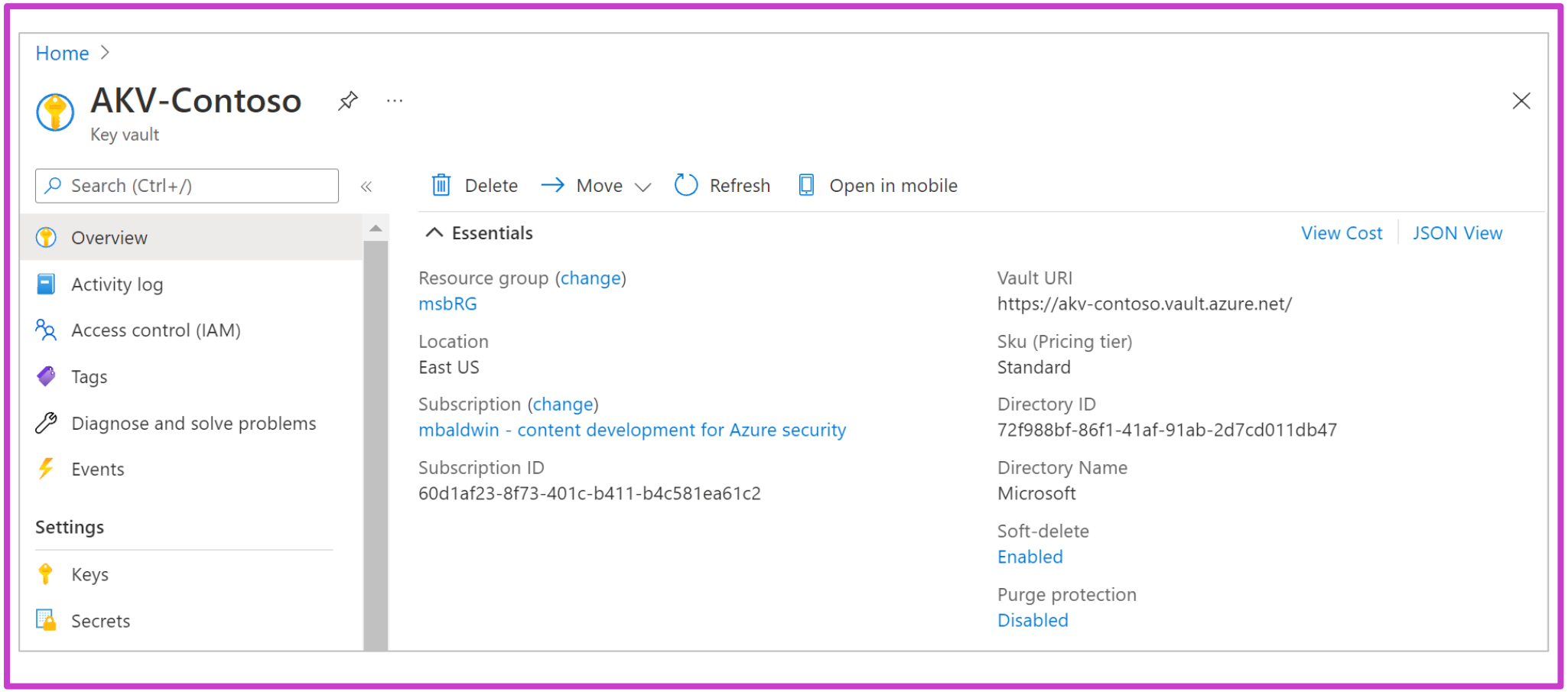
- Azure Key Vault securely stores API keys, passwords, certificates, and cryptographic keys.
- Supports vaults for software/HSM-backed keys and managed HSM pools for HSM-backed keys only.
- Offers managed identities for secure authentication and enforces TLS for data-in-transit protection.

Azure Key Vault authentication

- Authentication with Key Vault is integrated with Microsoft Entra ID to authenticate security principals.
- Security principals can be users, groups, or service principals with unique IDs for Azure resource access.
- Key Vault authentication flow involves token retrieval, firewall checks, and permission validation for operations.

Create and configure an Azure Key Vault

1. On the Azure portal, select **Create a resource**.
2. Search for "**Key Vault**", select the relevant result and select **Create**.
3. Specify a name, subscription, and location, and complete the process



Recommend when to use a Dedicated HSM

Use Azure Dedicated HSM when you need:

- FIPS 140-2 Level-3 compliance
- Single tenancy of the cryptographic storage device
- Full administrative control and sole access to the device for administrative purposes
- High application performance
- Unique cloud-based offerings

Best fit for "**lift-and-shift**" scenarios that require direct and sole access to HSM devices.

Unfit for scenarios such as: Microsoft cloud services that support encryption with customer-managed keys that are not integrated with Azure Dedicated HSM.

Configure access to Key Vault

Data – Key / Secrets / Cert

Configure vault access policies

You can use these options:

- Azure Portal: Under the **Principal** selection pane, configure the options.
- Azure CLI: Assign the access policy using the `az keyvault set-policy` command
- Azure PowerShell: Assign the access policy using the `Set-AzKeyVaultAccessPolicy` cmdlet

Configure Azure RBAC

With Azure RBAC, you can have

- One place to manage all permissions across all key vaults
- The ability to set permissions on different scope levels: management group, subscription, resource group, or individual resources
- Separate permissions on individual keys, secrets, and certificates with Azure RBAC for key vault

Manage certificates, secrets, and keys

Manage certificates

- Azure Key Vault assists in handling X.509 certificates.
- Ensures secure storage, management, and policy formulation.
- Users can input contact details for alerts.

Manage secrets

- Granularly isolate secrets for enhanced application security.
- Store credentials in secret values; rotate bi-monthly.
- Oversee access using Key Vault logging.

Manage keys

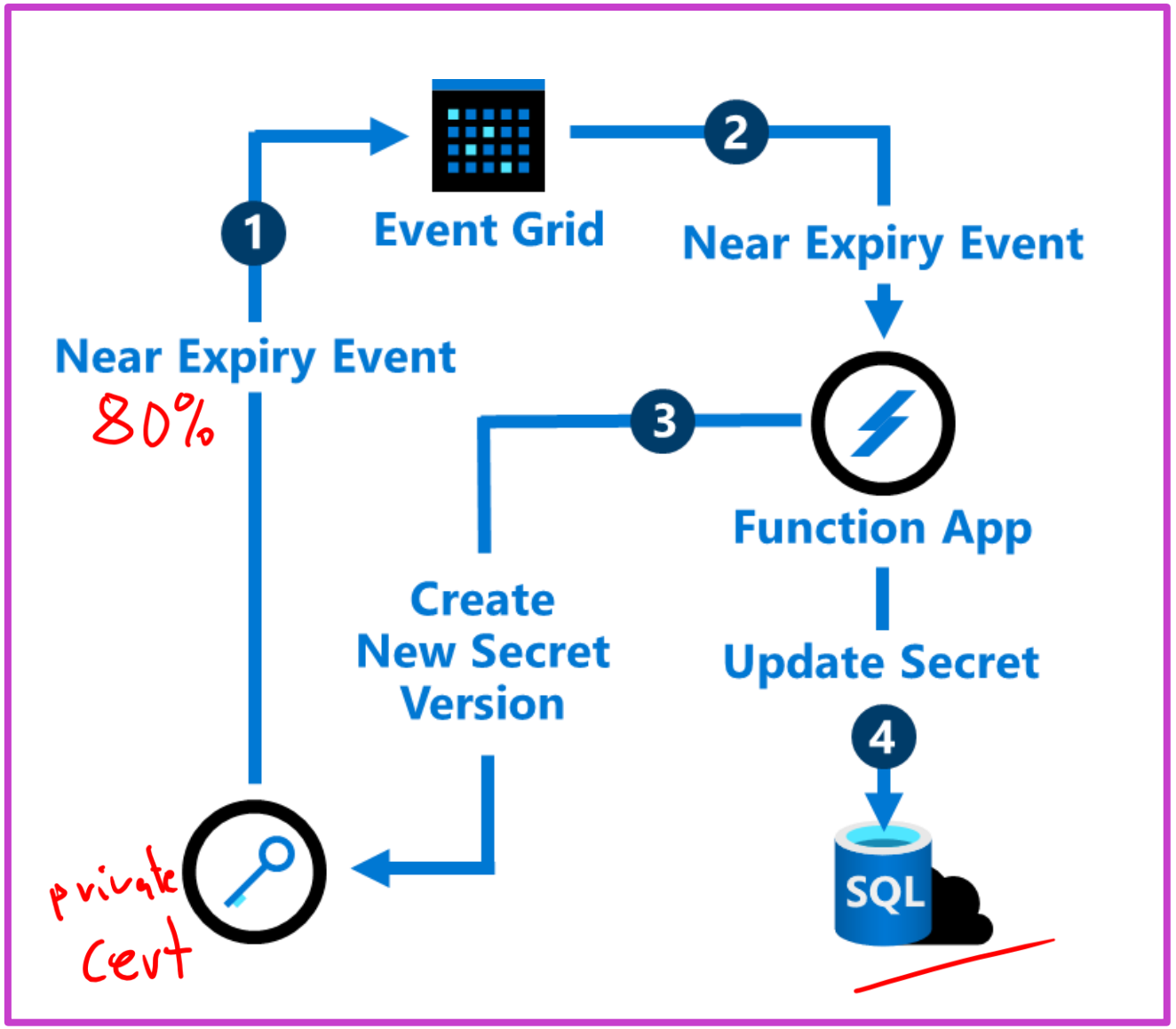
- Encryption keys: platform-managed or customer-managed.
- Storage options include Azure Key Vault and Dedicated HSM.
- Options vary by FIPS compliance, management overhead, and application suitability.

Configure key rotation

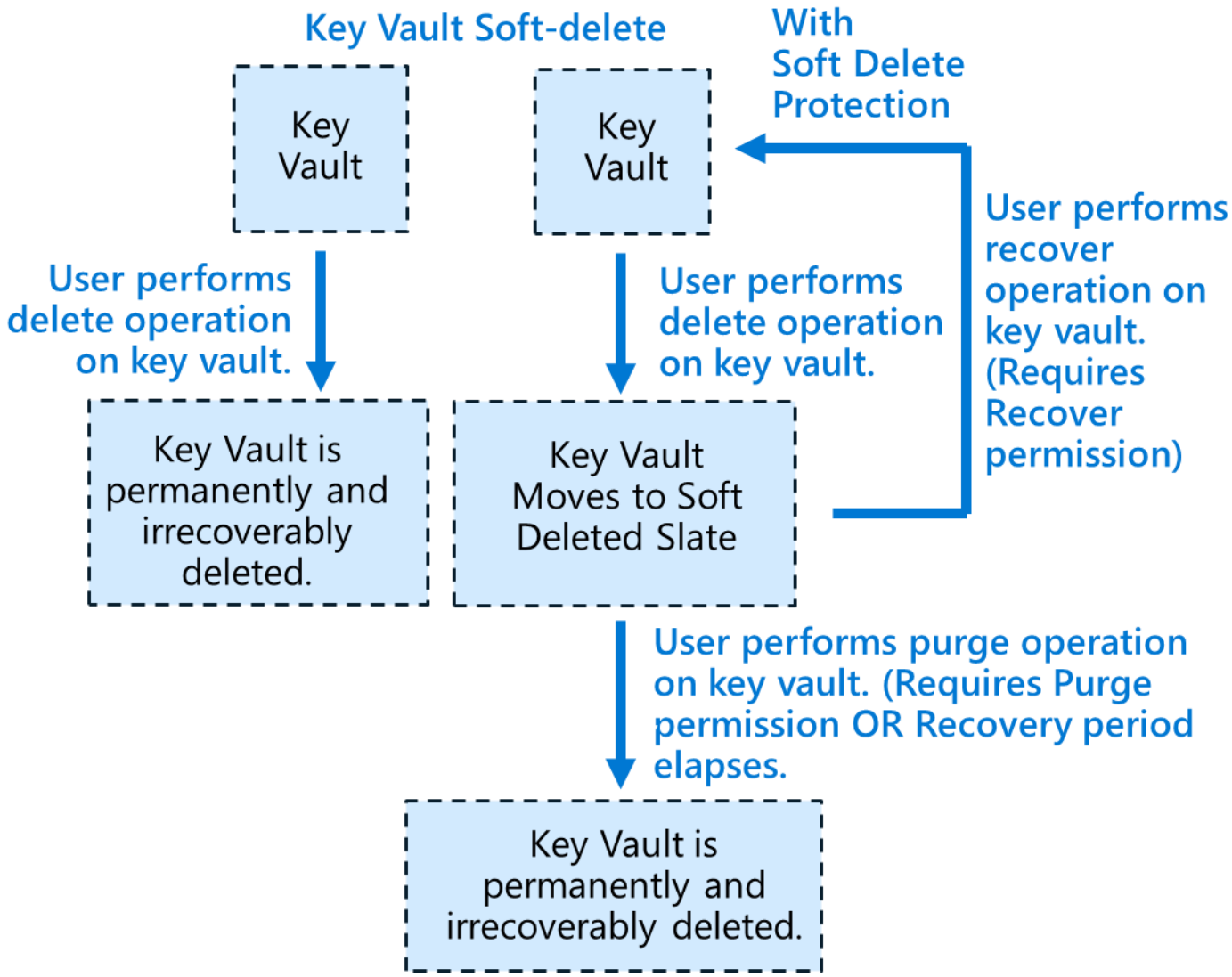
Update keys and secrets without affecting your application

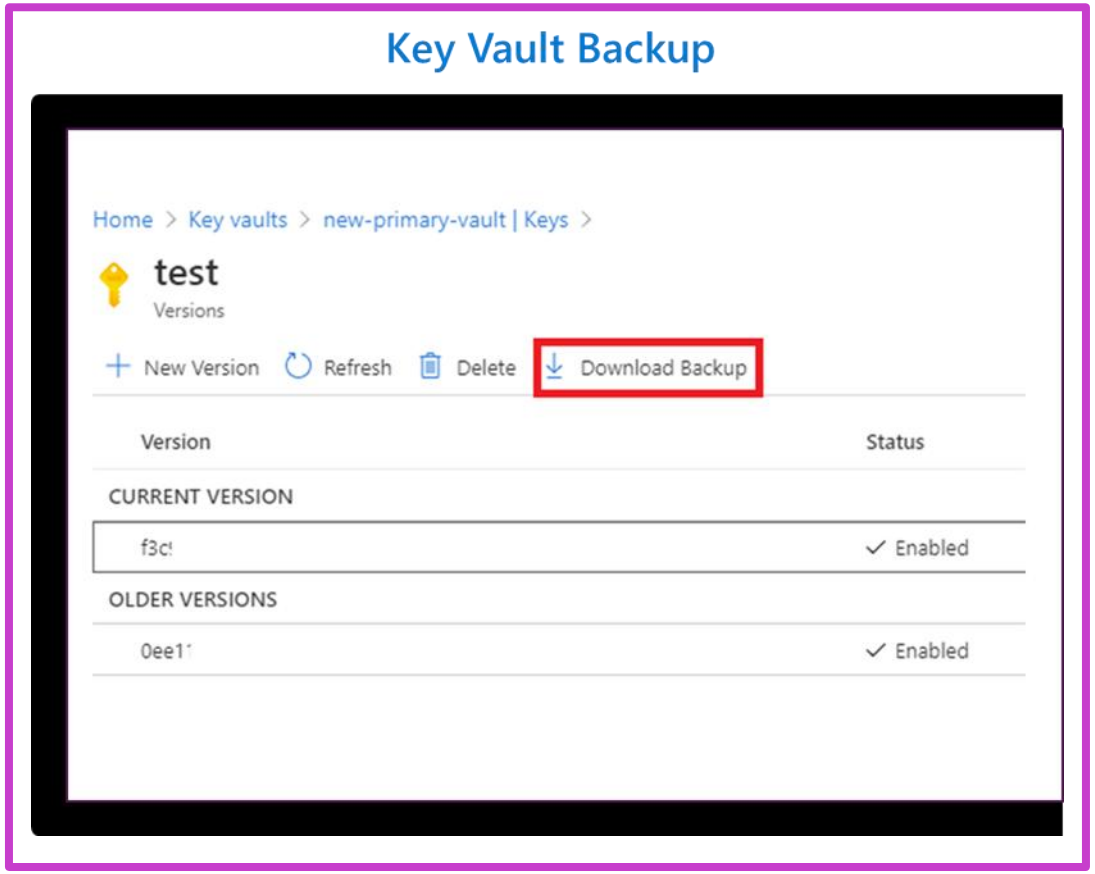
Rotate keys and secrets in several ways:

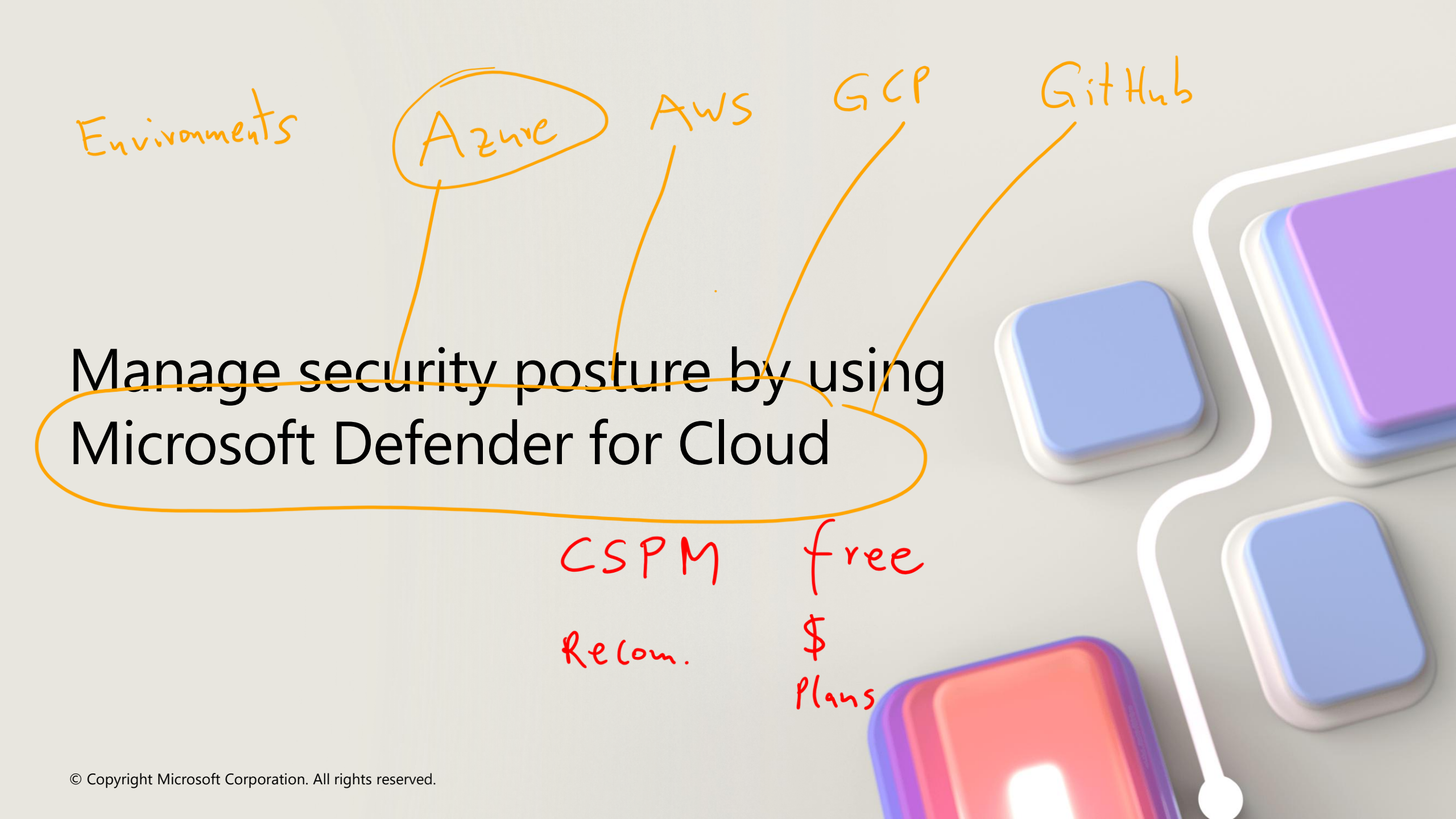
- As part of a manual process
- Programmatically with the REST API
- With an Azure Automation script



Configure backup and recovery of secrets, certificates, and keys







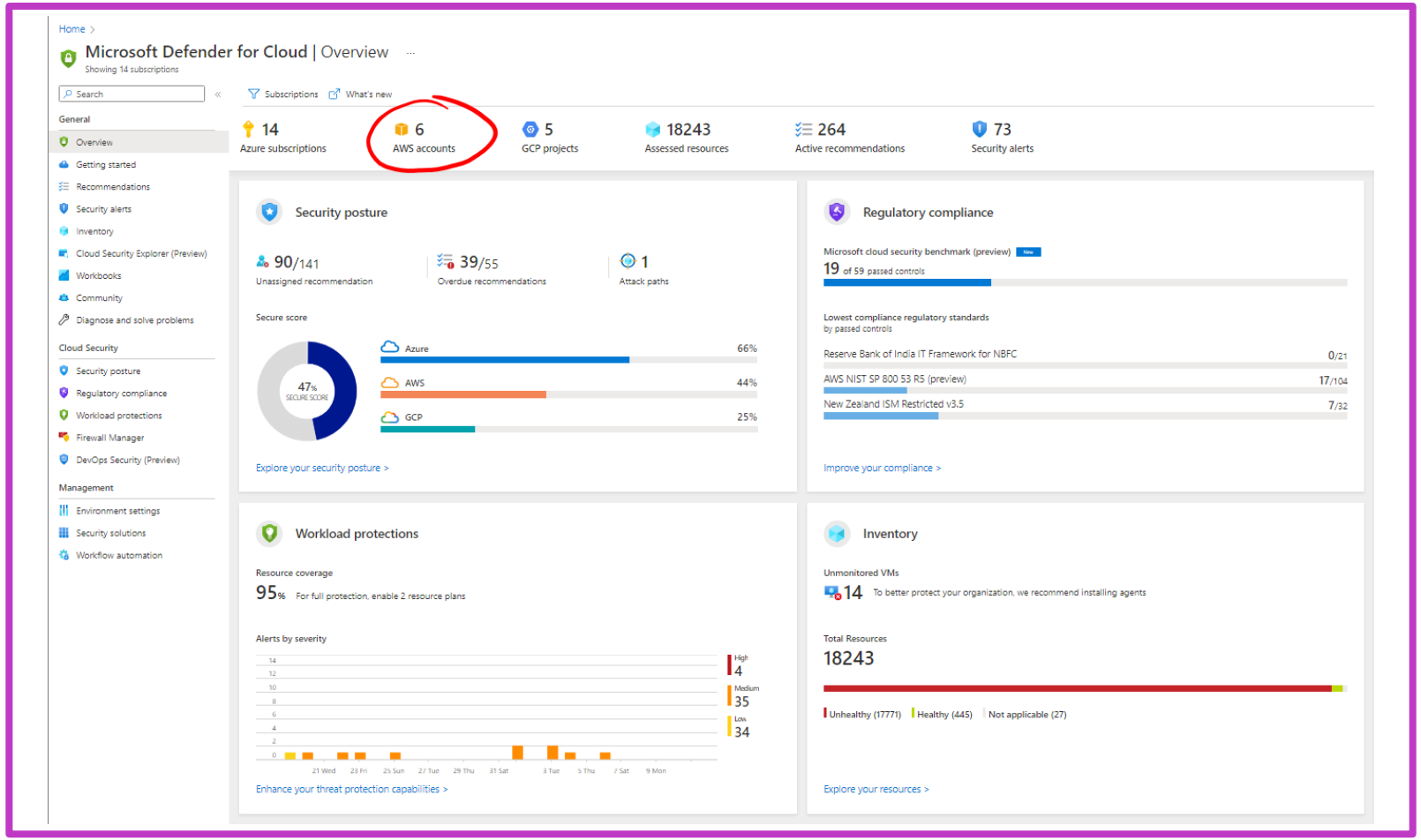
Manage security posture by using Microsoft Defender for Cloud

Implement Microsoft Defender for Cloud

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.

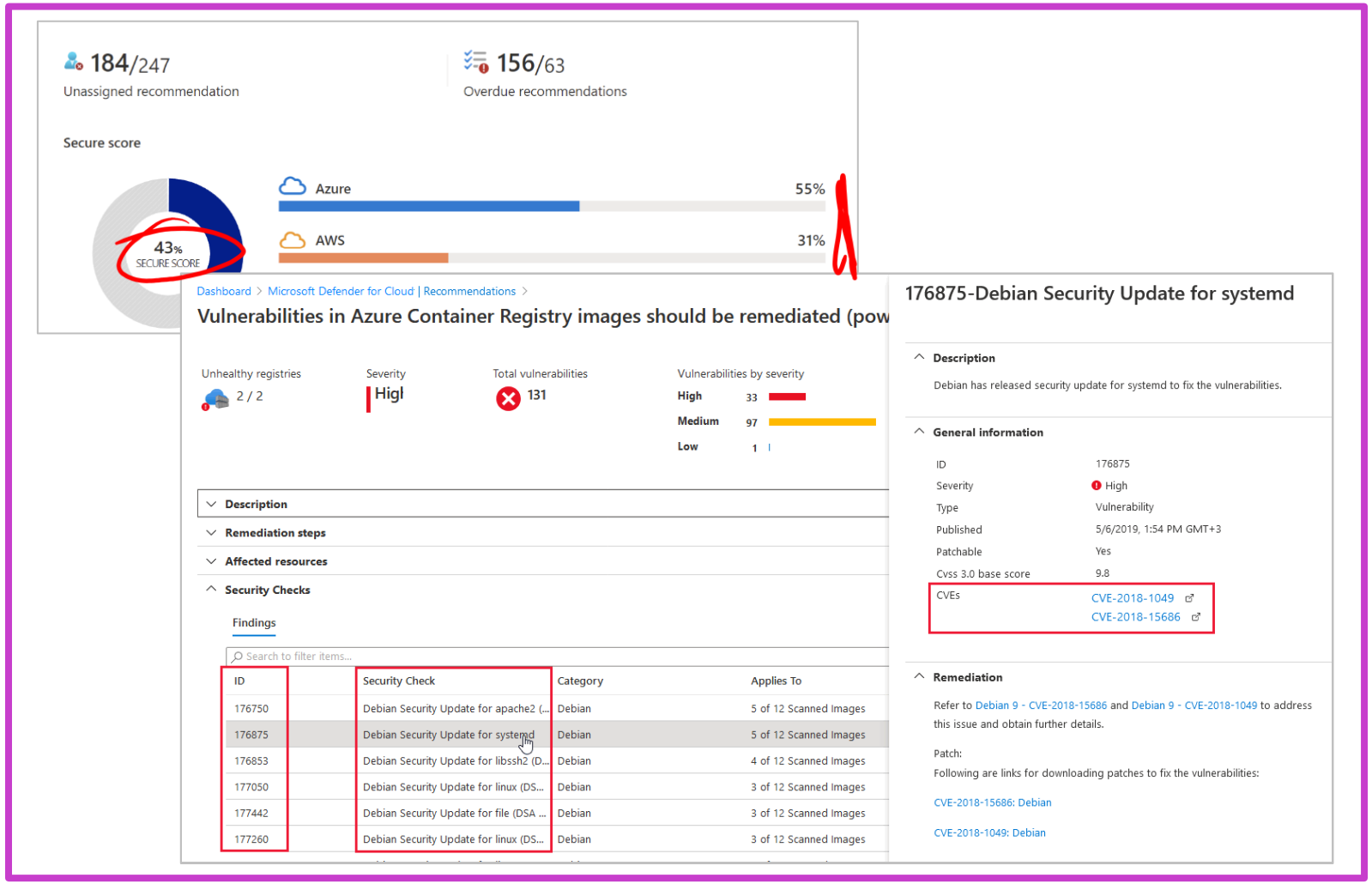
Microsoft Defender for Cloud's features covers the two broad pillars of cloud security:

1. Security Posture Management
2. Workload Protection



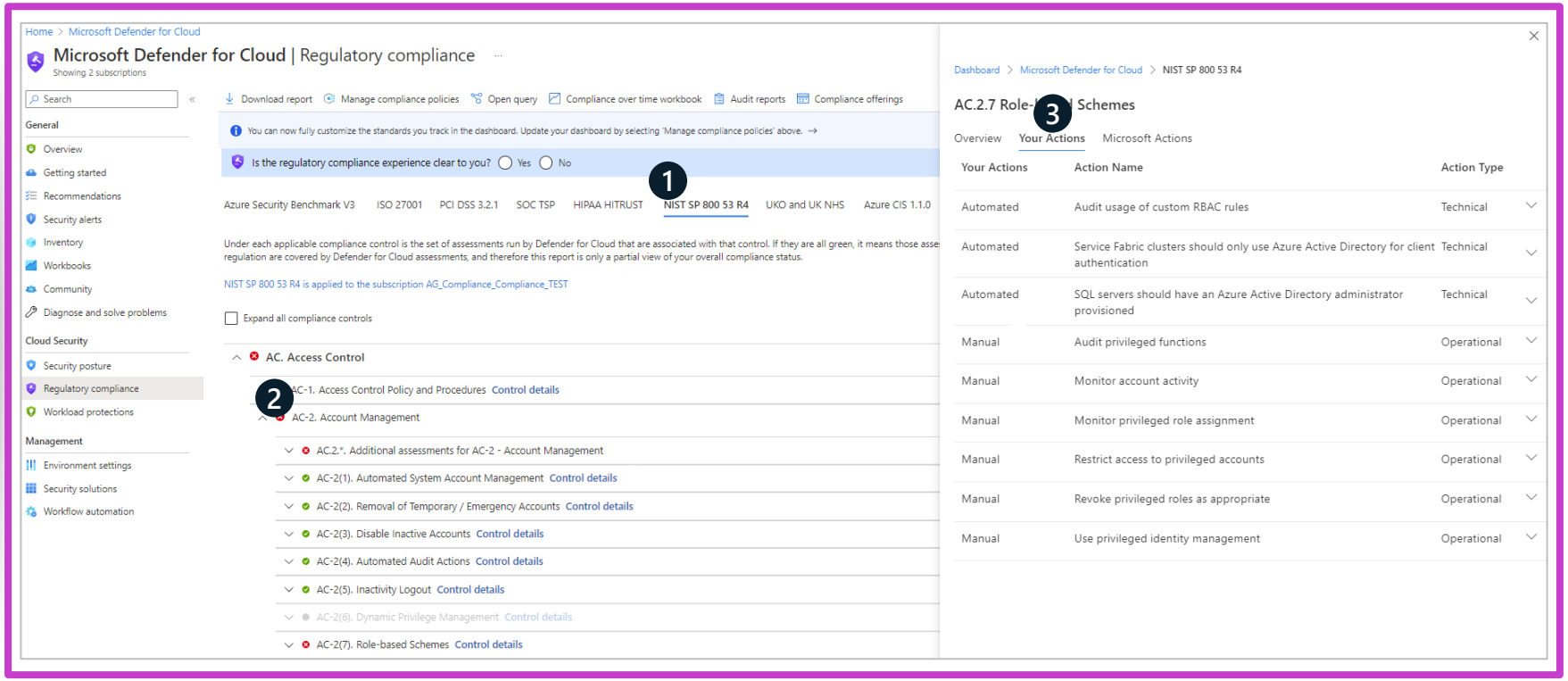
Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory

- Defender for Cloud evaluates cross-cloud resources for security threats.
- Secure Score aggregates findings to indicate the overall security status.
- Enhance security by following Defender's recommendations and using the Inventory page's filter for specific vulnerabilities.



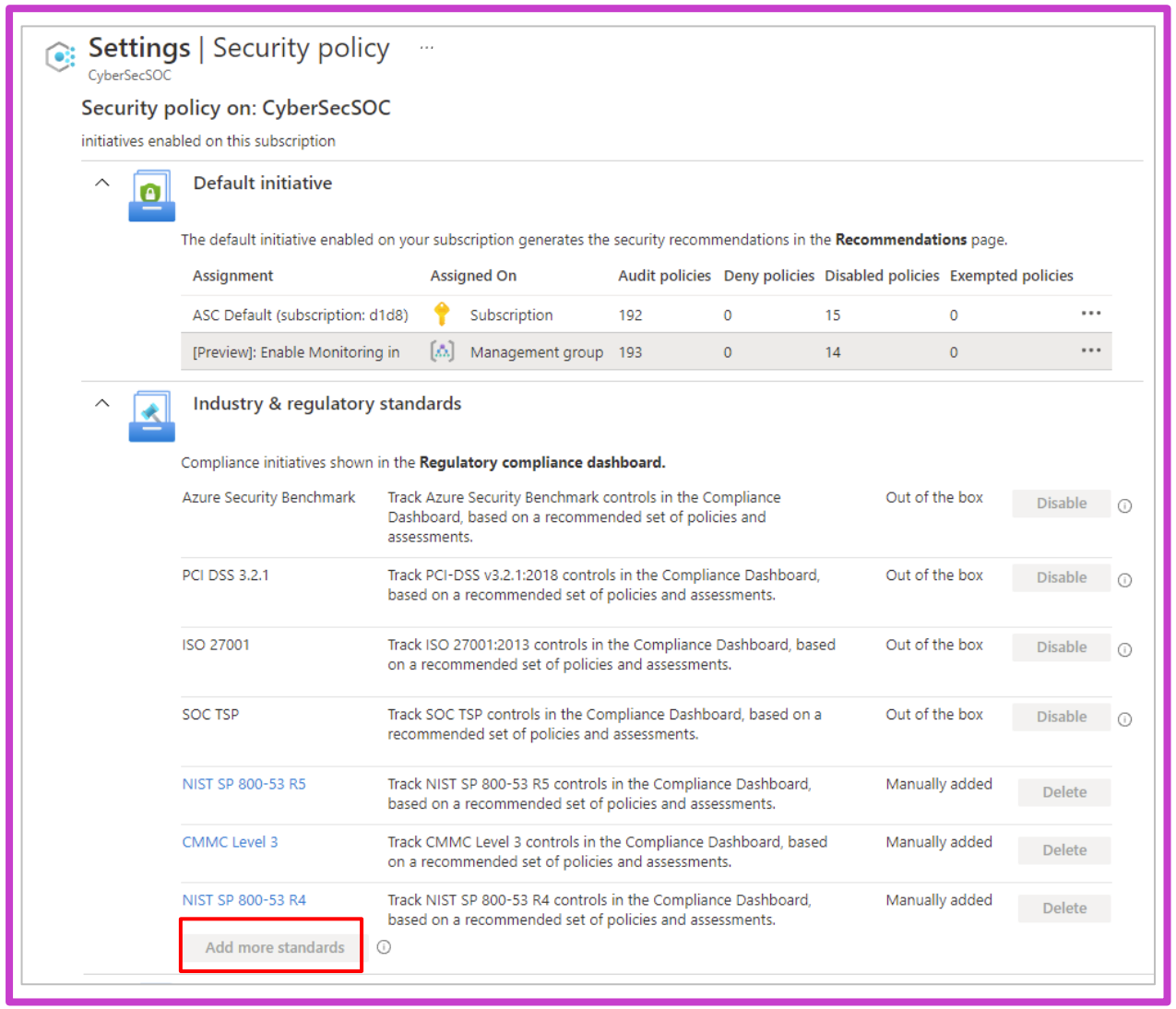
Assess compliance against security frameworks and Microsoft Defender for Cloud

- Visit the regulatory compliance dashboard for overall scores and assessment results.
- View controls, associated assessments, and their status.
- Check both automated and manual assessments under the "**Your Actions**" tab.



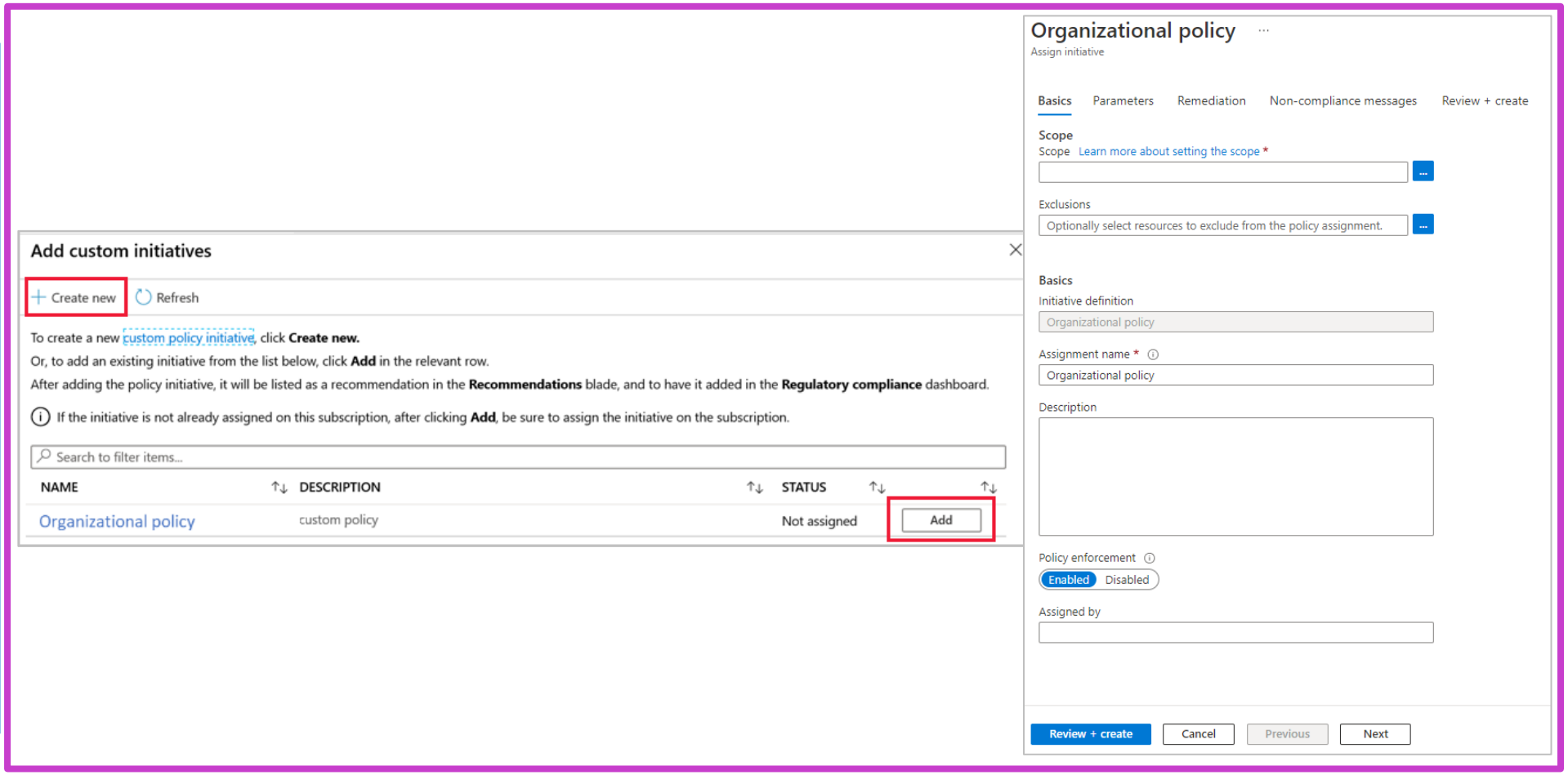
Add industry and regulatory standards to Microsoft Defender for Cloud

- Open the **Security policy** page and select **Add more standards** to add industry standards.
- You can add industry standards such as:
  - Regulatory standards
  - AWS regulatory standards
  - GCP regulatory standards



Add custom initiatives to Microsoft Defender for Cloud

- Open the **Security policy** page and select **Add a custom initiative.**
- Create a new custom initiative by selecting **Create new** and configure the policies and parameters



Connect hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud

Connect hybrid cloud environments

You can connect your non-Azure computers in the following ways:

- Using Azure Arc-enabled servers (recommended)
- From Defender for Cloud's pages in the Azure portal

Connect multi-cloud environments

You can connect multi-cloud environments through:

- Native cloud connector (recommended)
- Classic connector

Identify and monitor external-facing assets

With Microsoft Defender External Attack Surface Management, you can monitor internet-exposed assets with a global network that graphs online relationships.

It provides:

Continuous visibility beyond the firewall by:

- Discovering unmanaged resources
- Providing multicloud visibility
- Identifying exposed weaknesses

Capabilities such as:

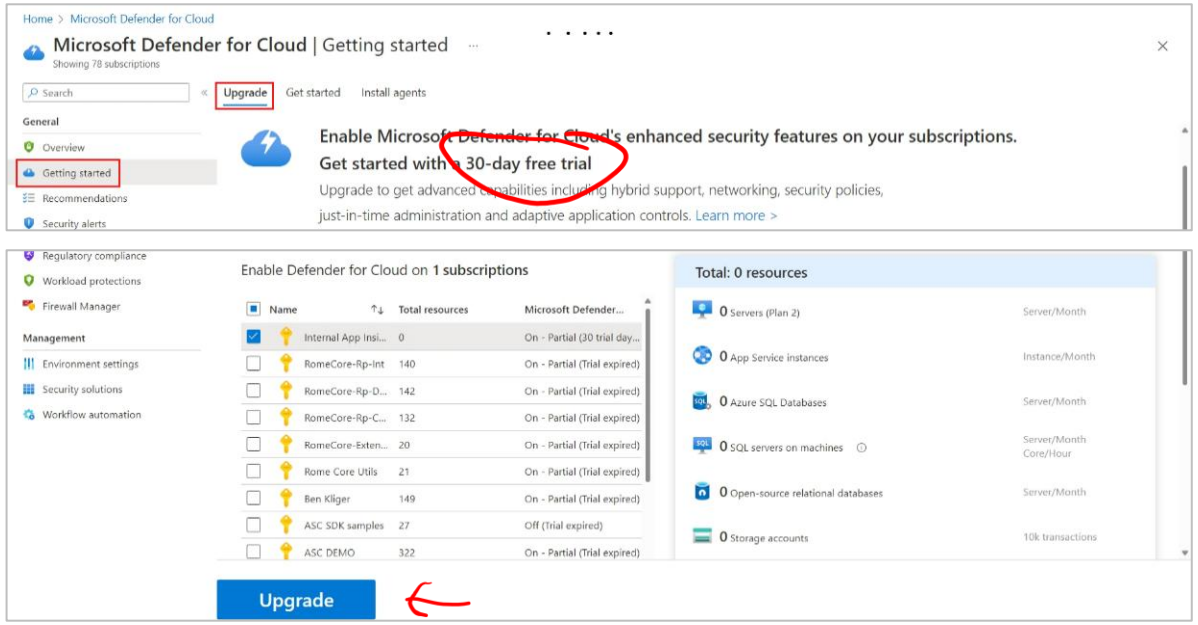
- Real-time inventory
- Attack surface visibility
- Exposure detection and prioritization
- Integrated threat protection

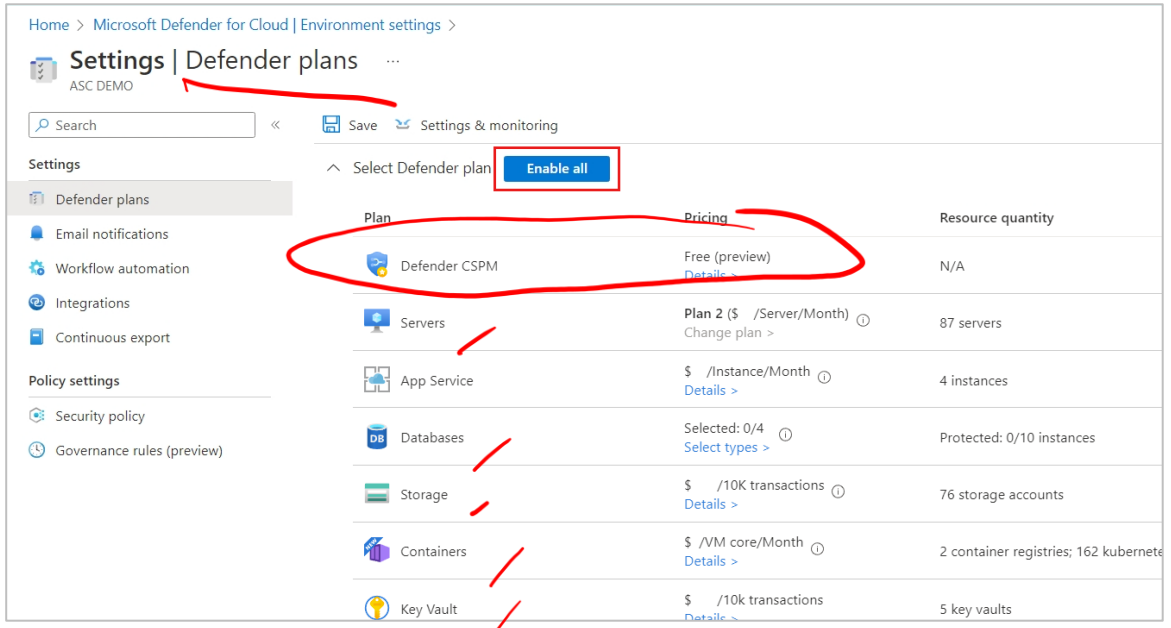
Configure and manage threat protection by using Microsoft Defender for Cloud

Enable workload protection services in Microsoft Defender for Cloud

- To enhance security on multiple subscriptions in Defender for Cloud, select "**Getting started**."
- Choose subscriptions and workspaces on the "**Upgrade**" tab. Click "**Upgrade**."

- Activate enhanced security in Defender for Cloud via Environment settings.
- Choose the desired subscription or workspace.
- Select "**Enable all**" for comprehensive Defender for Cloud plans.

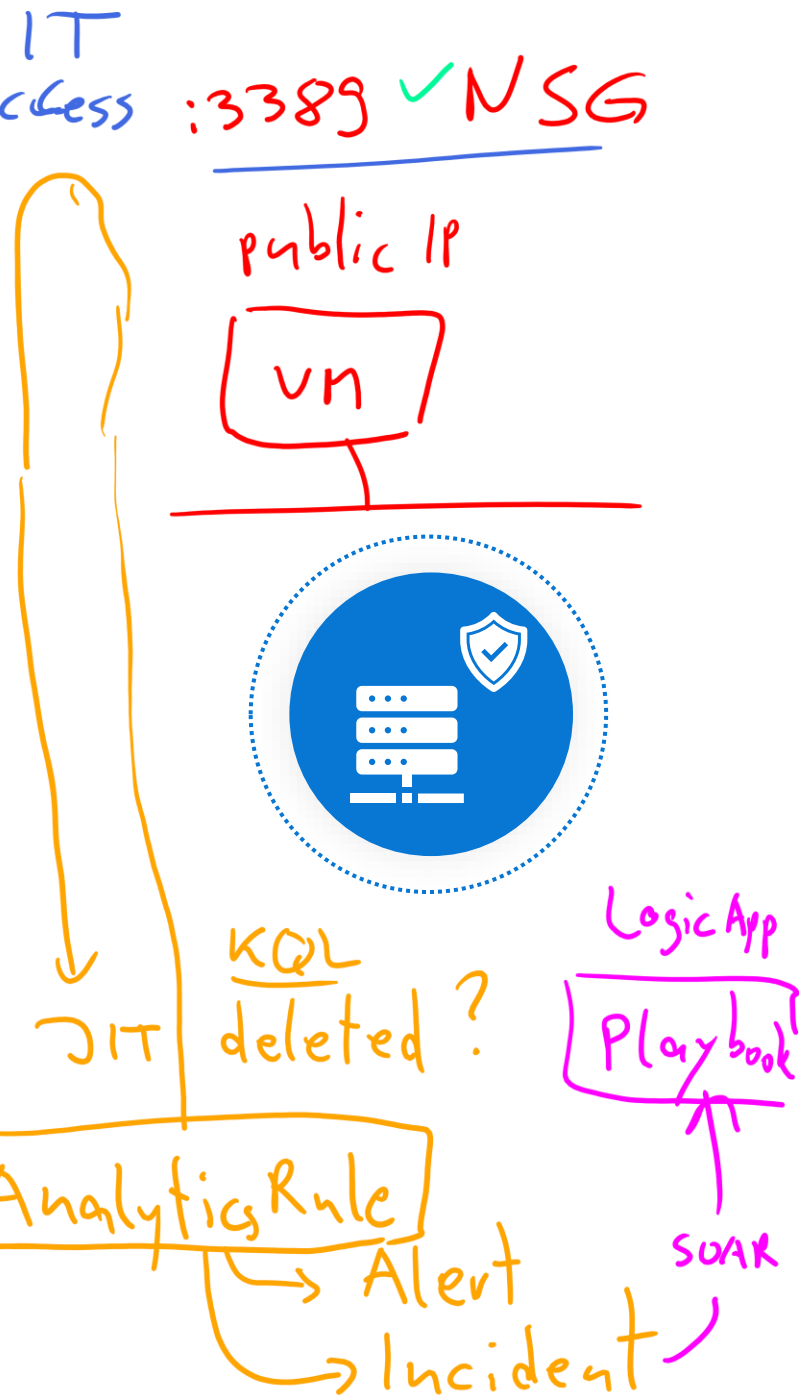




Configure Microsoft Defender for Servers

Remember the following while configuring Microsoft Defender for Servers:

- This product includes automatic, native integration with Microsoft Defender for Endpoint.
- You can enable Defender for Servers and then enable Defender for Endpoint unified integration to provision the Defender for Endpoint agent on all supported machines in the subscription.
- To configure Defender for Servers, you can choose from:
  - Plan 1: Includes Microsoft Defender for Endpoint (MDE) integration, automatic provisioning, and lower licensing cost.
  - Plan 2: Includes everything in Defender for Servers Plan 1 + All other enhanced security features.

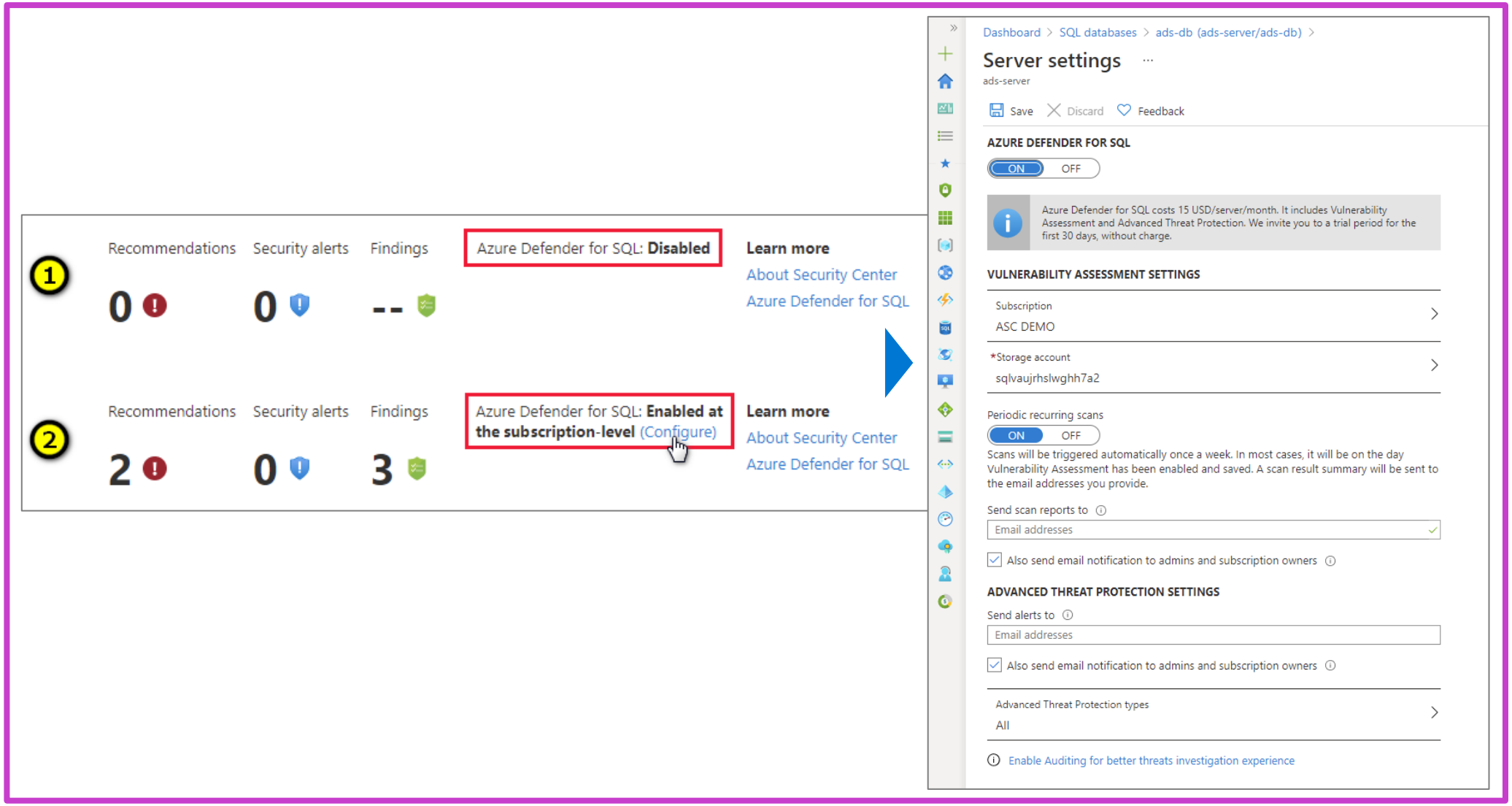


Configure Microsoft Defender for Azure SQL Database

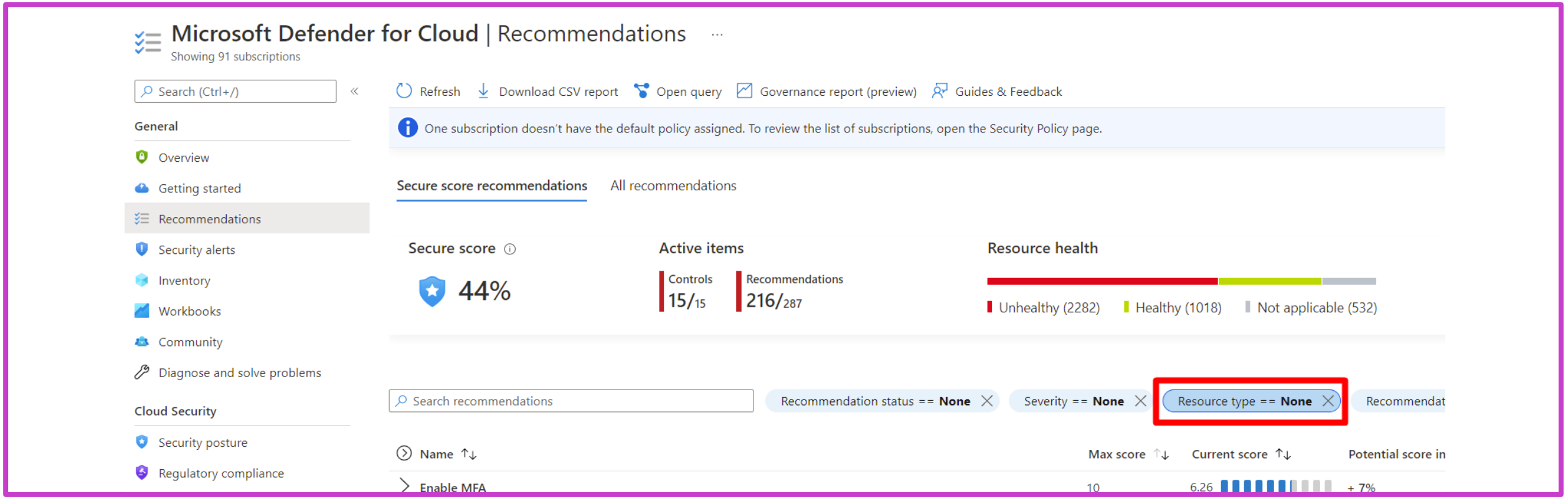
Enable Microsoft Defender for Azure SQL Database at subscription or resource level.

Access Defender for Cloud in the server's Security area.

If enabled, choose "**Configure**" to modify **Defender for SQL** settings.

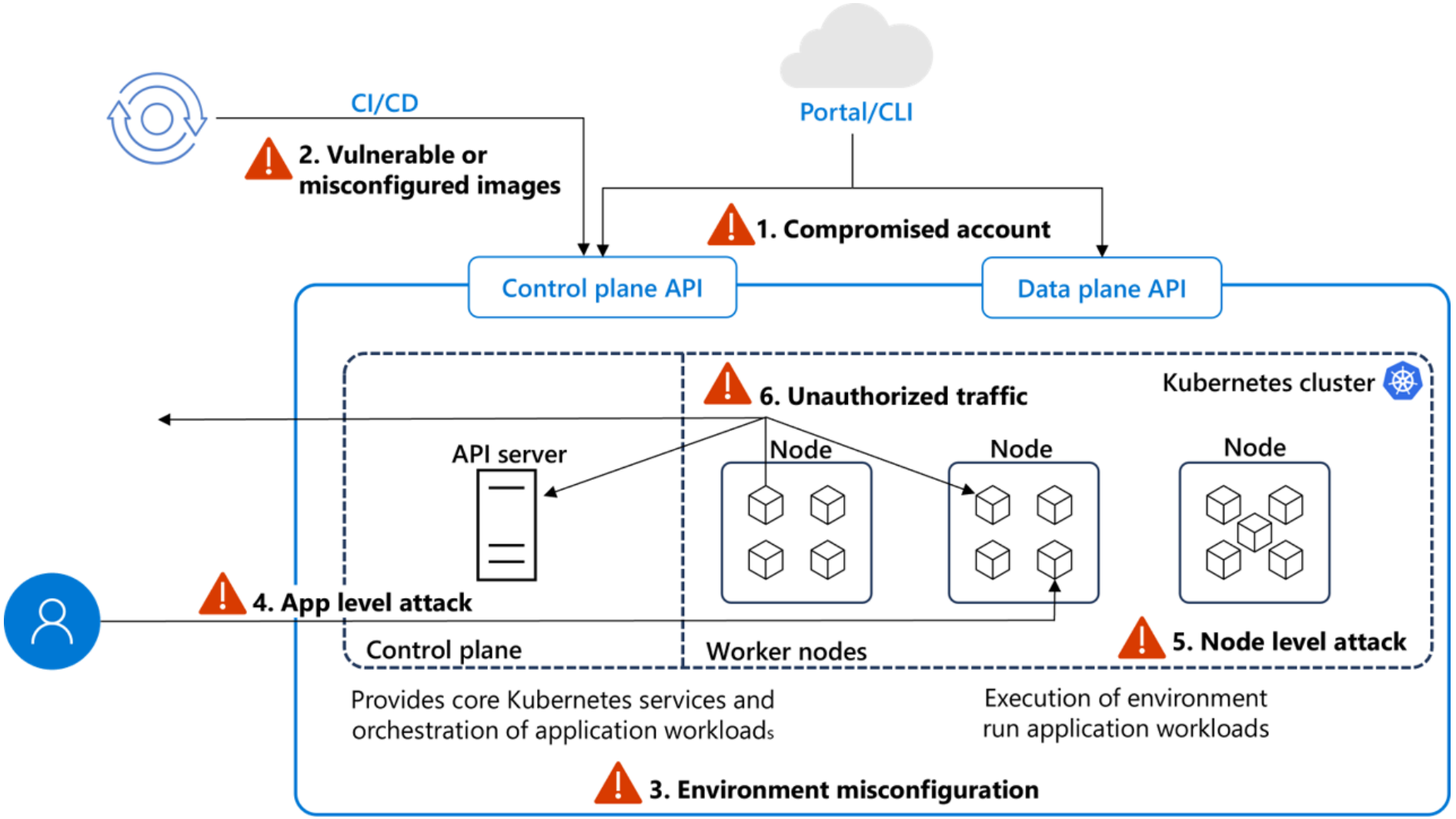


Container security in Microsoft Defender for Containers

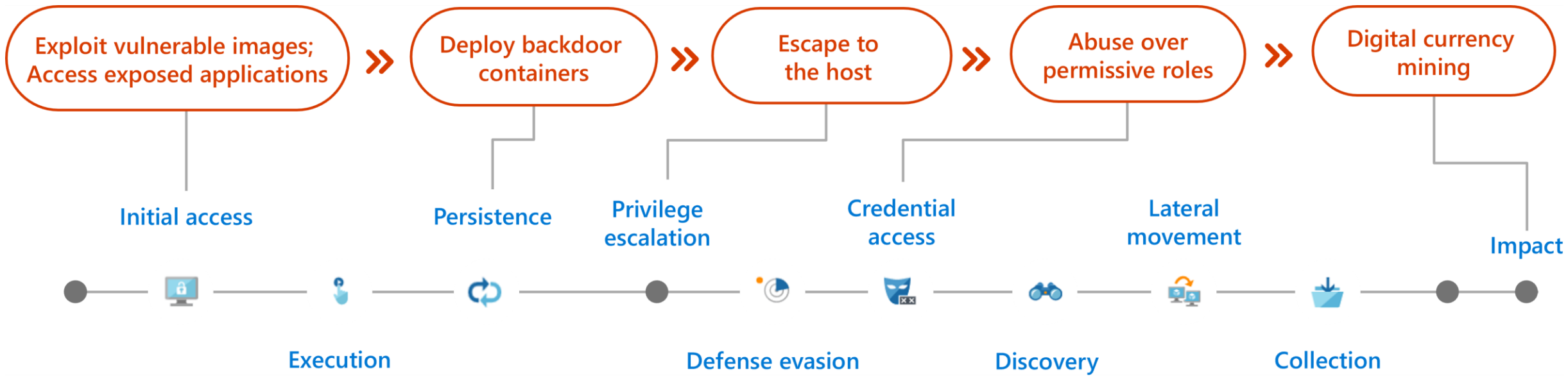


- Microsoft Defender for Containers: Cloud-native solution for container security across multicloud and on-premises environments.
- Four core domains: Security posture management, vulnerability assessment, run-time threat protection, deployment & monitoring.
- Features: Agentless capabilities, agent-based capabilities, vulnerability assessment, run-time protection with MITRE ATT&CK framework.

Managed Kubernetes threat factors

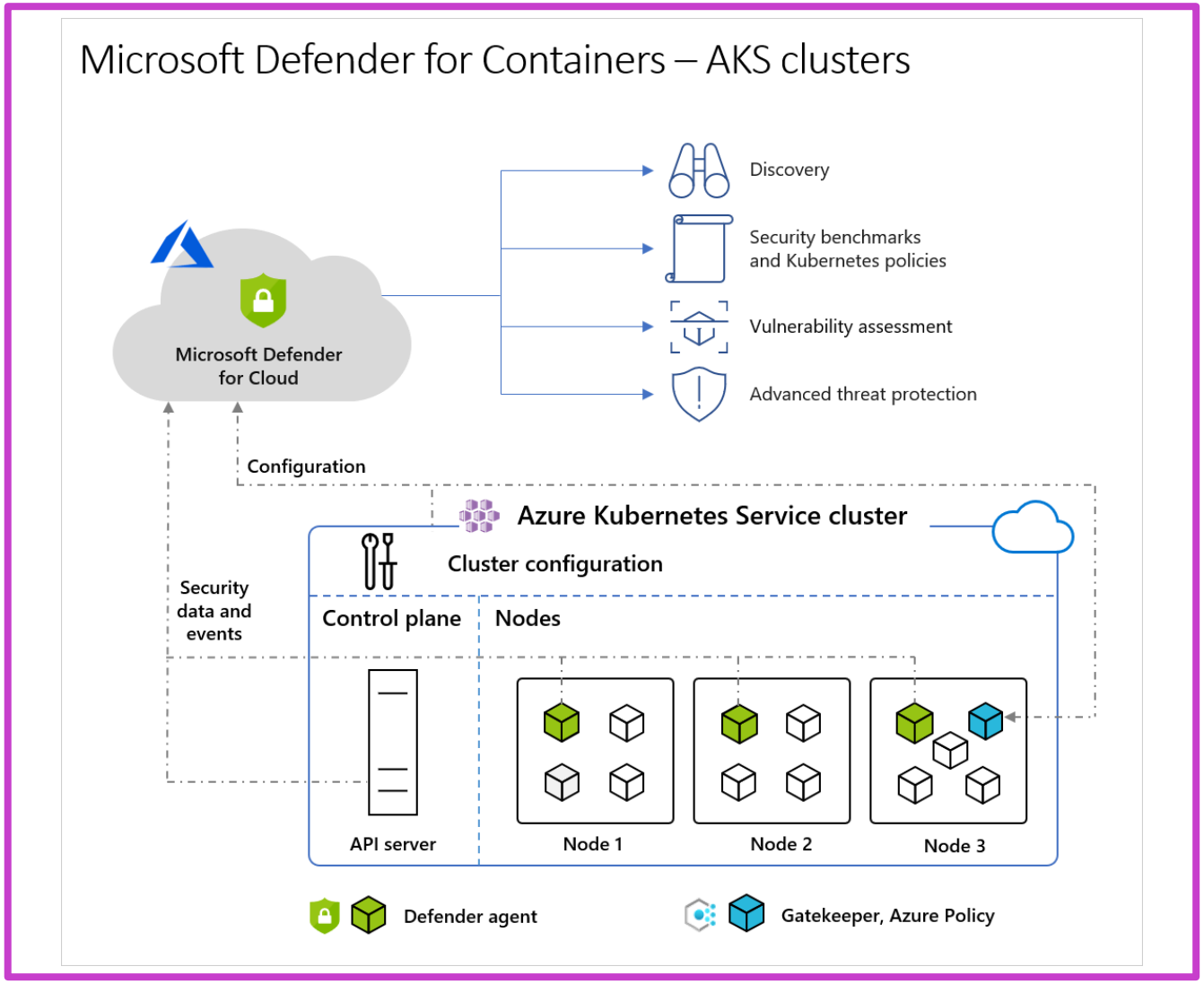


Common attack techniques



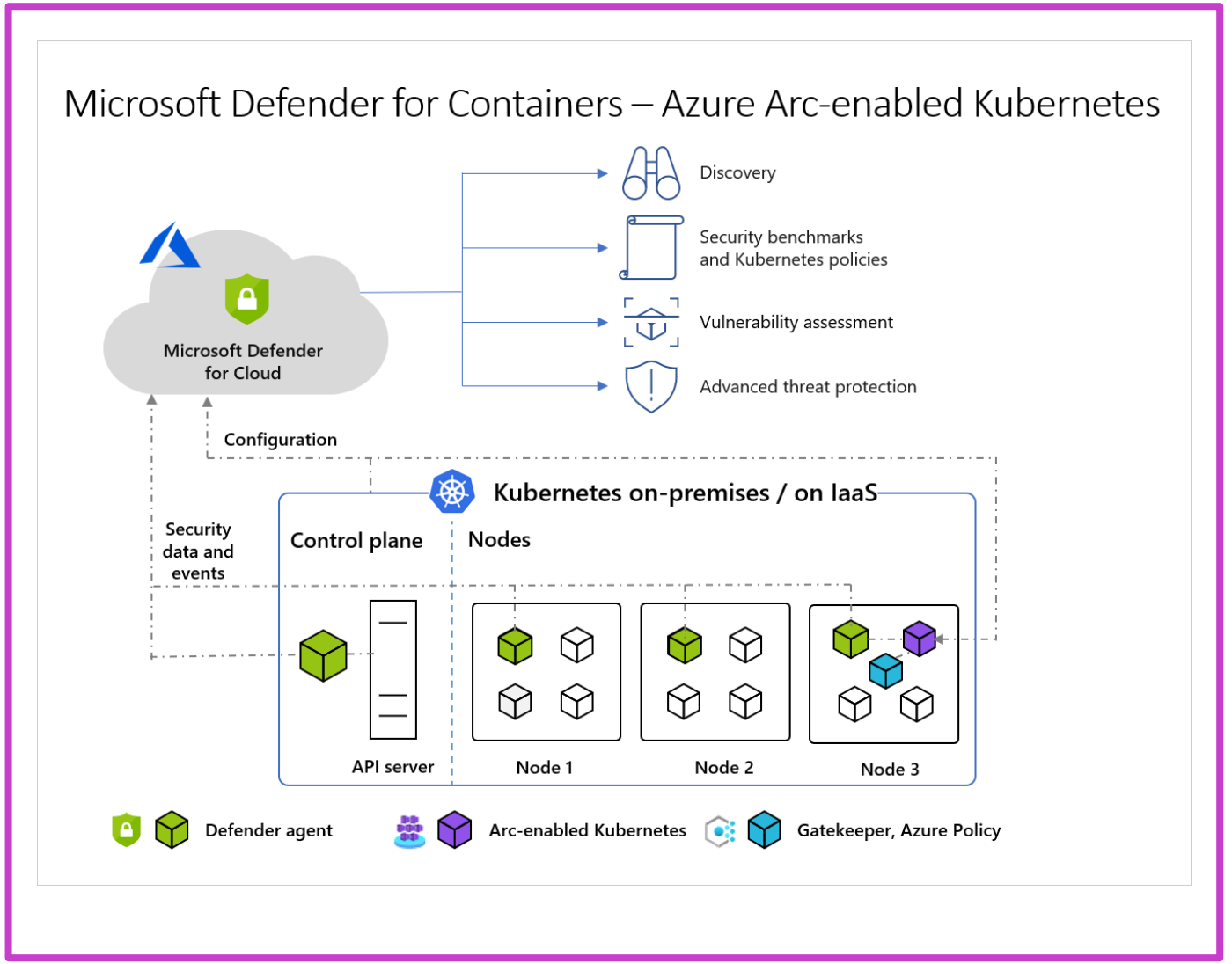
Architecture diagram of Defender for Cloud and AKS clusters

- Agentless audit log collection in AKS; automatic, no extra cost or setup.
- Defender agent for runtime protection, Azure Policy for Kubernetes for enforcement.
- Agentless discovery creates, assigns roles, discovers, and binds to AKS clusters.



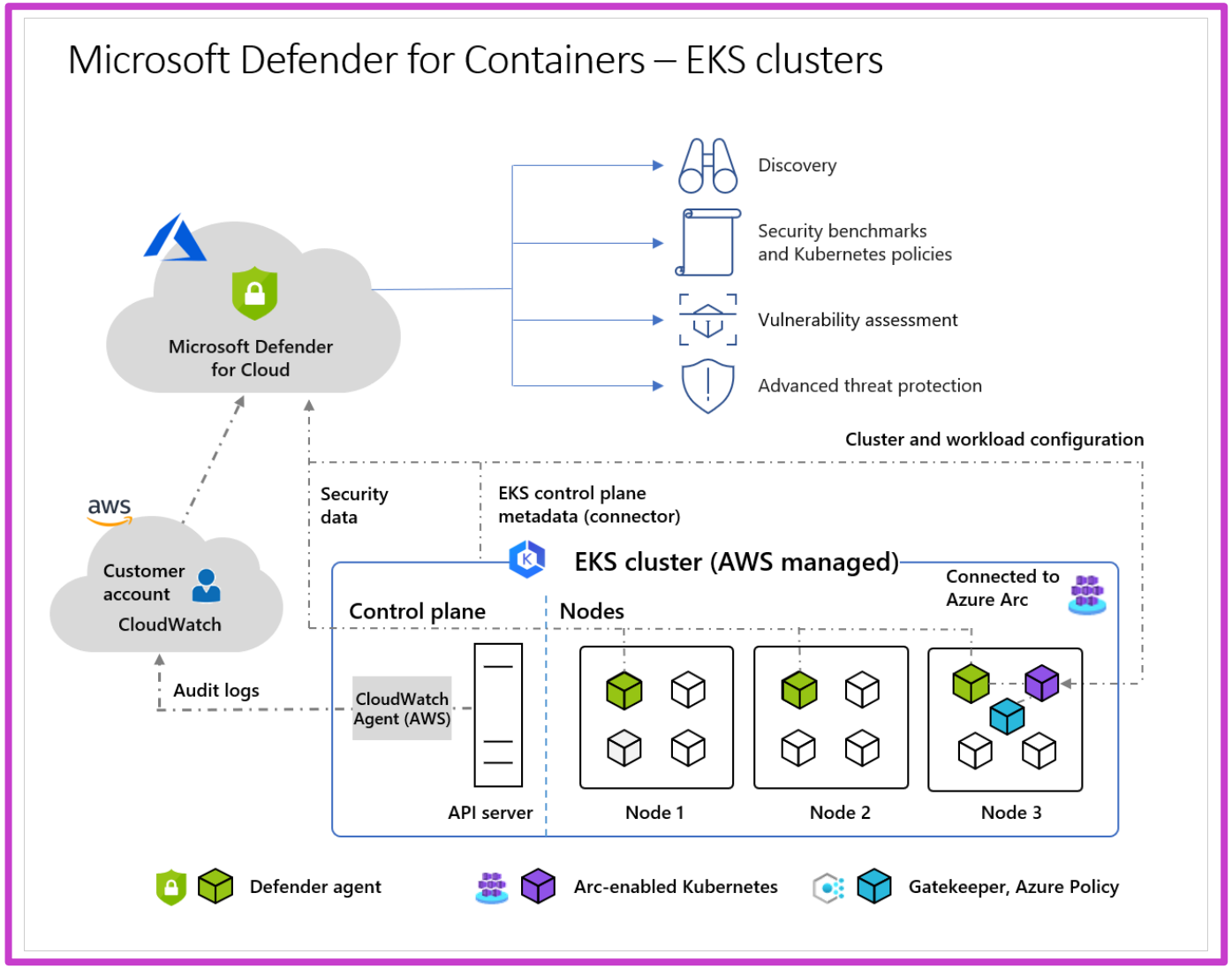
Architecture diagram of Defender for Cloud and Arc-enabled Kubernetes clusters

- Azure Arc connects clusters to Defender for Cloud; requires one node installation.
- Defender agent provides runtime protection, collects signals and audit logs as Arc extension.
- Azure Policy for Kubernetes enforces policies centrally as an Arc-enabled extension, one node required.



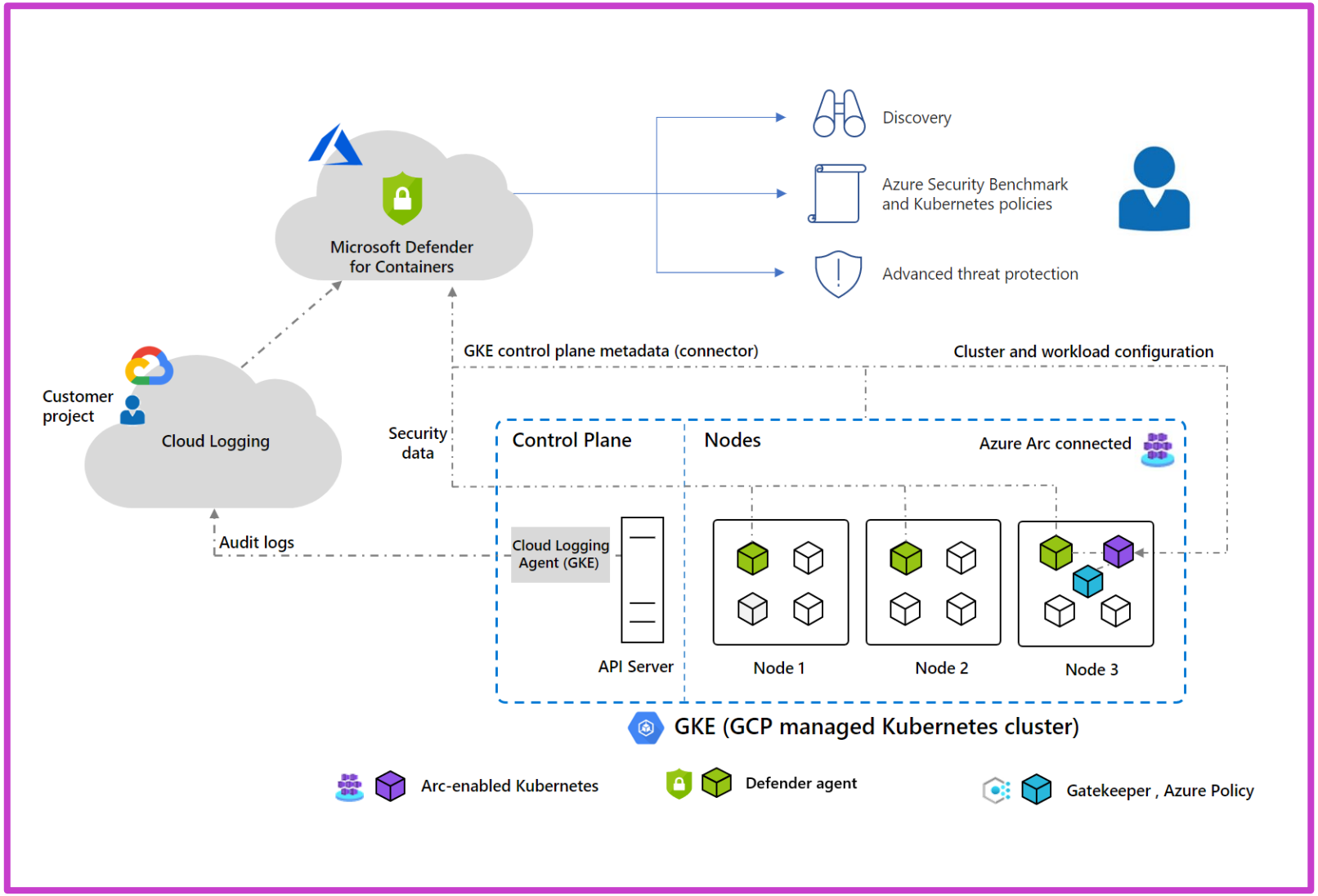
Architecture diagram of Defender for Cloud and EKS clusters

- Defender for Cloud and EKS: Audit logs collected agentlessly, Arc-enabled Kubernetes with Defender agent, Azure Policy.
- AWS discovery snapshots: Role assignment, API-based cluster discovery by Defender for Cloud.
- Components include CloudWatch, Arc-enabled Kubernetes, Defender agent, and Azure Policy.

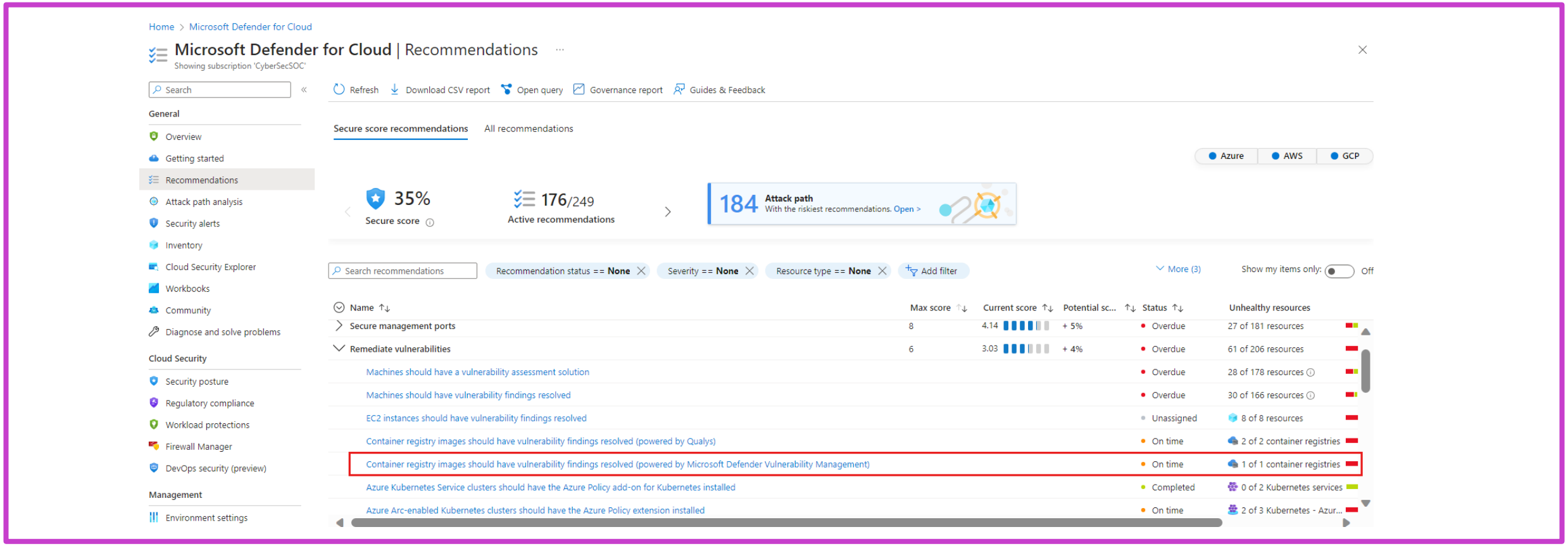


Architecture diagram of Defender for Cloud and GKE clusters

- Agentless audit log collection in GKE via GCP Cloud Logging.
- Azure Arc connects clusters to Defender for Cloud, enabling extensions.
- Extensions include Defender agent for runtime protection and Azure Policy for Kubernetes enforcement.



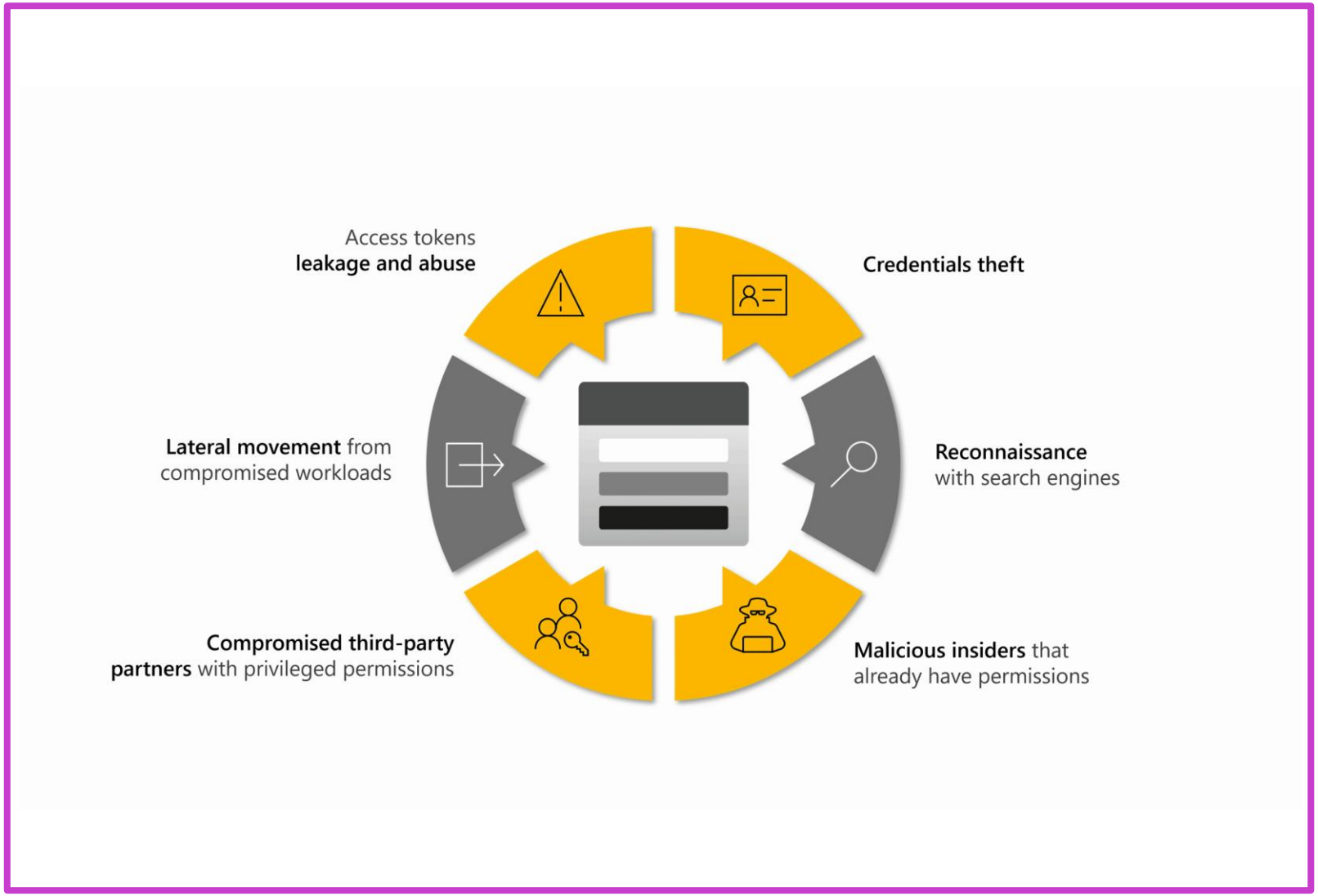
Vulnerability assessments for Azure



- Azure Vulnerability Assessment: Easy discovery and remediation for container vulnerabilities across Azure Container Registry.
- Continuous scanning triggers for newly pushed images and those running in AKS clusters.
- Detailed scan process includes inventory creation, vulnerability reports, and continuous rescans.

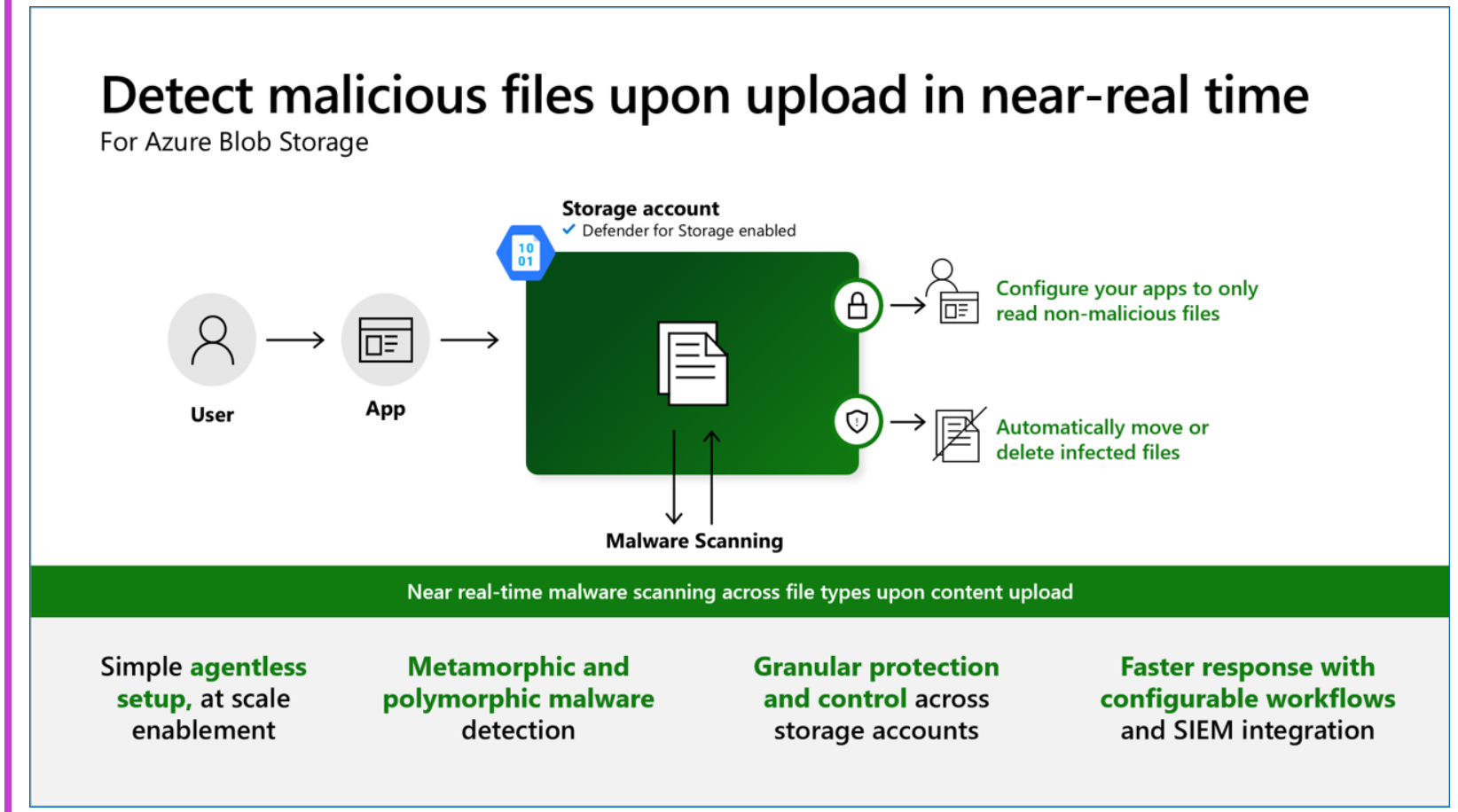
Microsoft Defender for Storage

- Detects threats, prevents malicious uploads, data exfiltration, and corruption.
- Uses Microsoft Threat Intelligence, Defender Antivirus, Sensitive Data Discovery.
- Agentless, scales easily, protects Azure Blob, Files, Data Lake Storage.



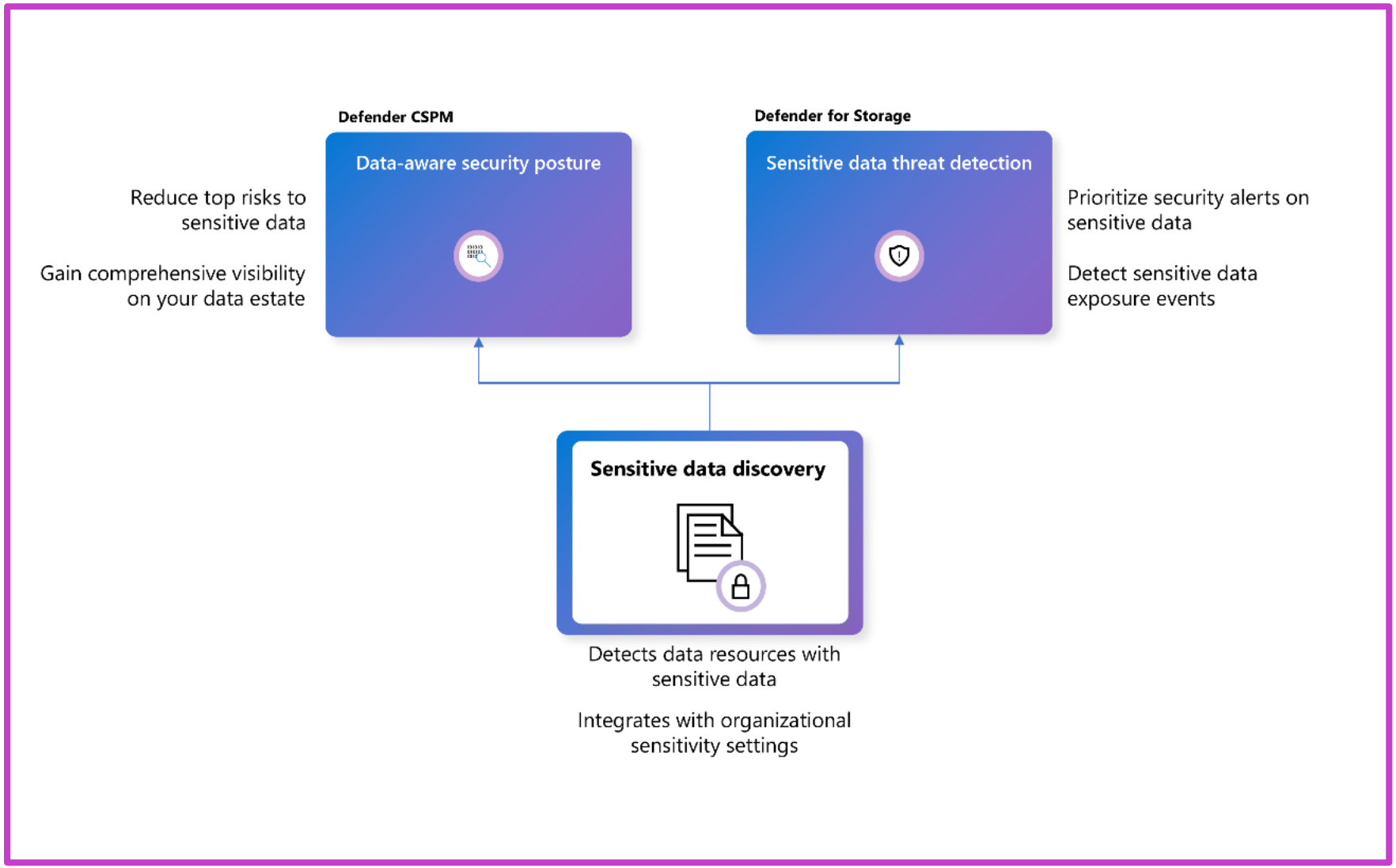
Malware scanning in Defender for Storage

- Scans uploads in real-time for malware, supports all file types.
- Detects sensitive data threats, enhances data protection.
- Agentless, scalable setup; provides comprehensive security analytics.



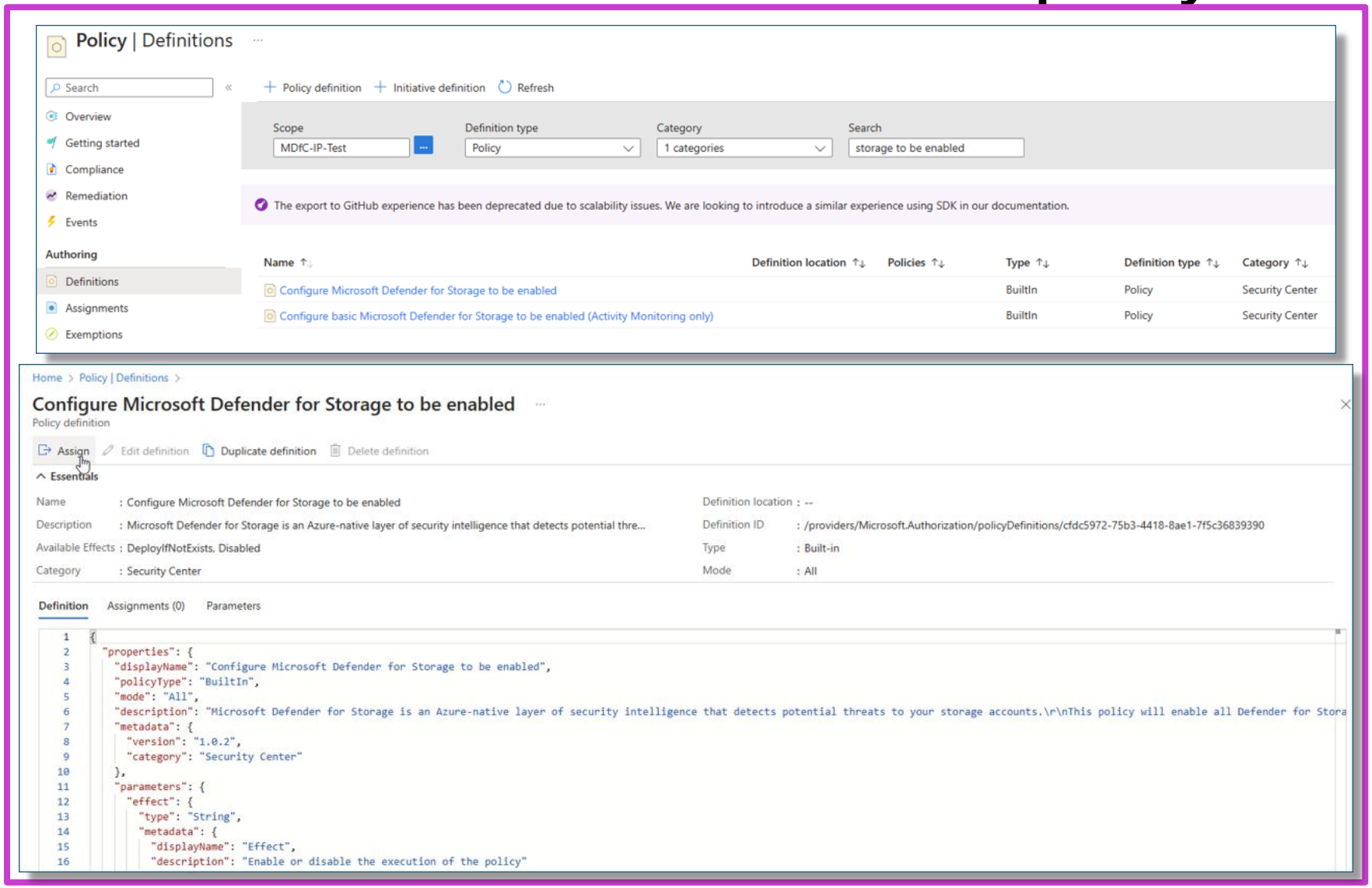
Detect threats to sensitive data

- Prioritizes alerts by data sensitivity, enhancing breach detection and prevention.
- Agentless scanning integrated with Microsoft Purview for policy alignment.
- Configurable without extra cost, automatic scans for new and existing storage.

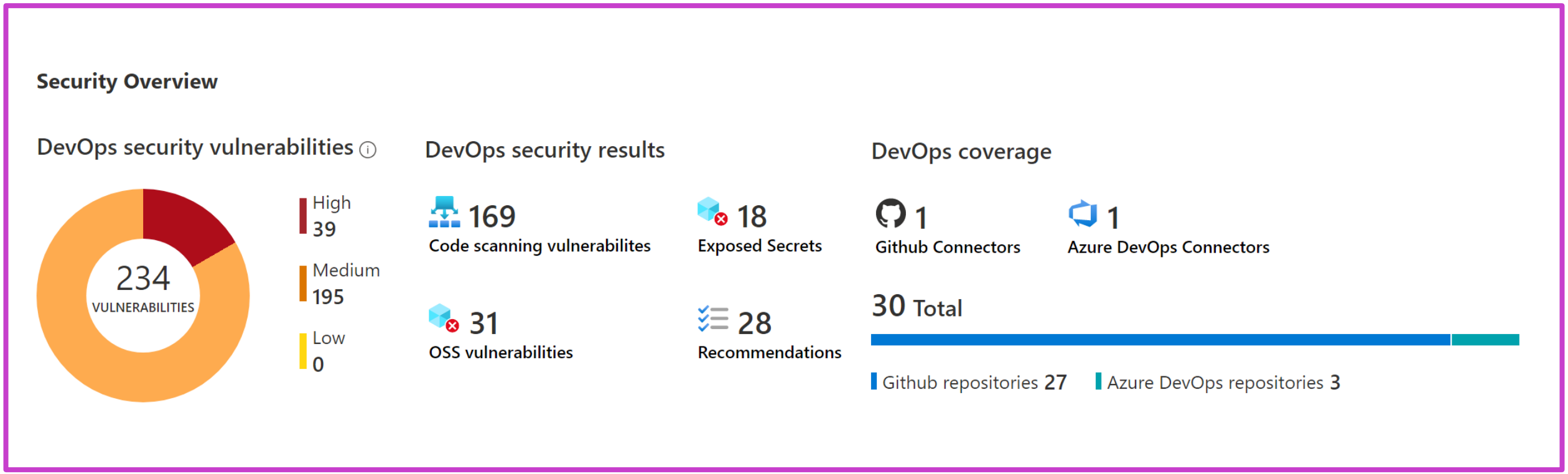


Enable and configure at scale with an Azure built-in policy

- Facilitates scalable, consistent security across all storage accounts via policy.
- Utilize Azure Policy dashboard to enable and configure Defender for Storage features.
- Assign policy for comprehensive or basic Defender for Storage capabilities, including customization.



Defender for Cloud DevOps Security



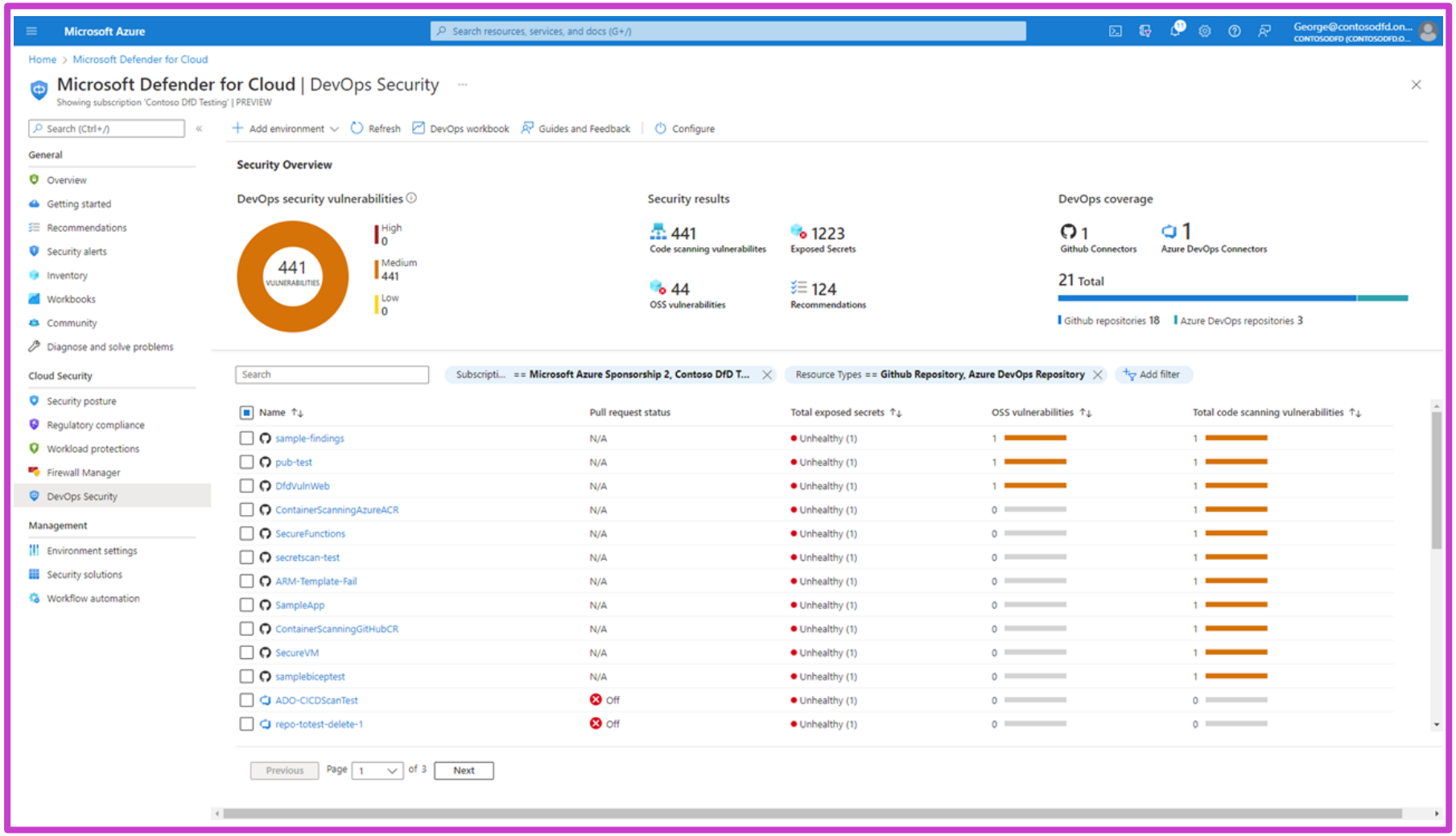
- Provides visibility, posture management, threat protection across Azure, AWS, GCP, on-premises.
- Centralizes DevOps security, integrates with Azure DevOps, GitHub, GitLab for application protection.
- Prioritizes code remediation with contextual insights, secures IaC templates, container images.

Defender for Cloud DevOps Security required permissions

Feature	Permissions
Connect DevOps environments to Defender for Cloud	• **Azure**: Subscription Contributor or Security Admin • Azure DevOps: Project Collection Administrator on target Organization • **GitHub**: Organization Owner • **GitLab**: Group Owner on target Group
Review security insights and findings	Security Reader
Configure pull request annotations	Subscription Contributor or Owner
Install the Microsoft Security DevOps extension in Azure DevOps	Azure DevOps Project Collection Administrator
Install the Microsoft Security DevOps action in GitHub	GitHub Write

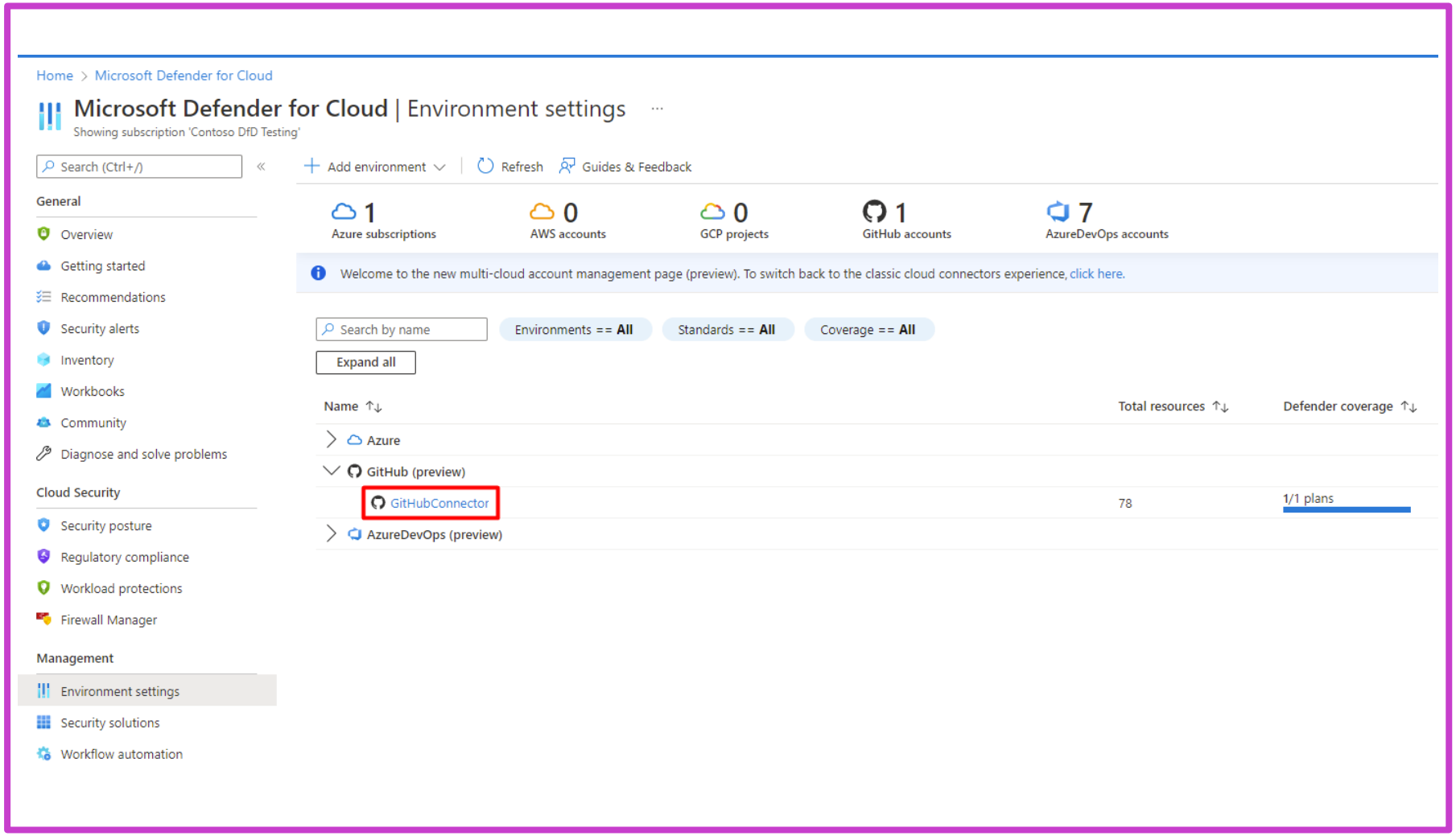
DevOps environment security posture

- Enhances security across DevOps lifecycle, identifies risks in CI/CD pipelines and source code management.
- Uses scanners for Azure DevOps, GitHub; auto-scans every 24 hours for vulnerabilities, misconfigurations.
- Offers actionable recommendations to reduce attack surface, prioritize fixes, integrate real-time alerts for compliance.



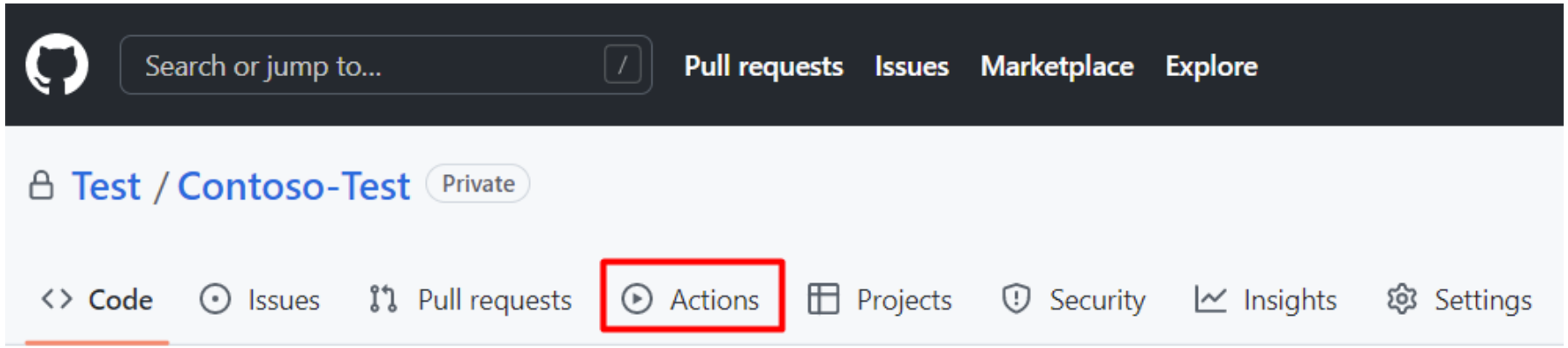
Connect your GitHub Environment to Defender for Cloud

- Connect GitHub organizations in Defender for Cloud for autodiscovery and enhanced security.
- Extends security with CSPM features and contextualized risk assessments for GitHub resources.
- Requires Azure account, GitHub Enterprise with Advanced Security, and authorization steps.



Configure the Microsoft Security DevOps GitHub action

- Integrates static analysis tools into development with Security DevOps command line application.
- Requires Azure subscription, GitHub repositories connection, and GitHub Advanced Security setup.
- Set up GitHub action for workflow, commit, and view scan results in Defender for Cloud.



Manage and respond to security alerts in Microsoft Defender for Cloud

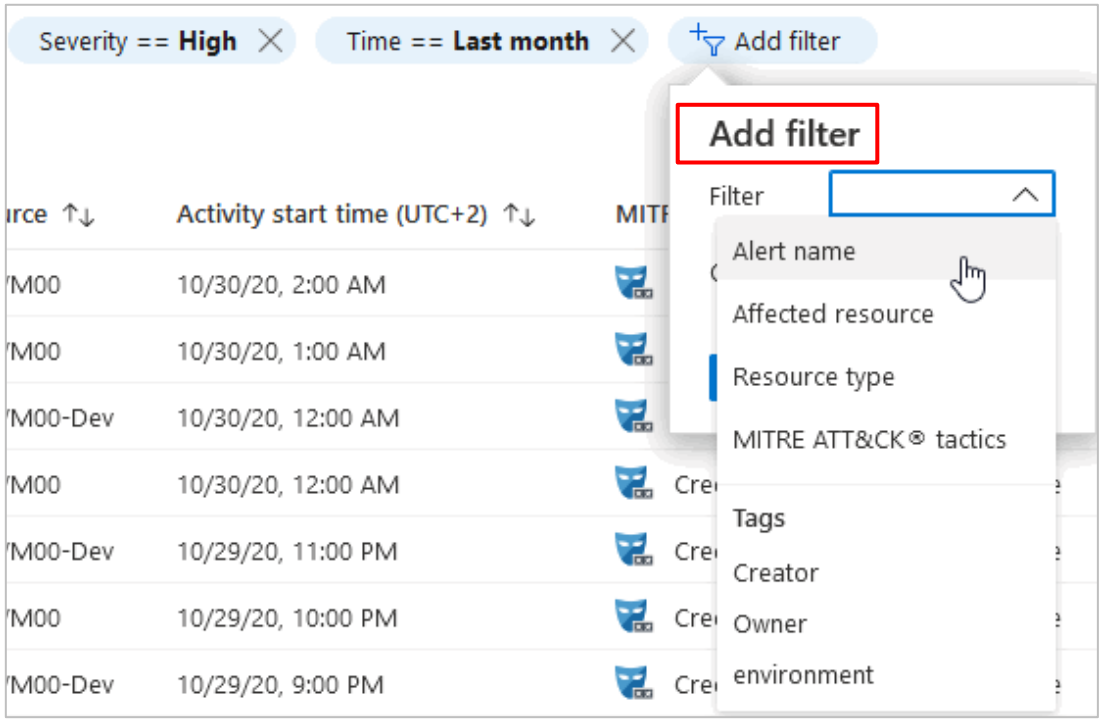
Manage security alerts

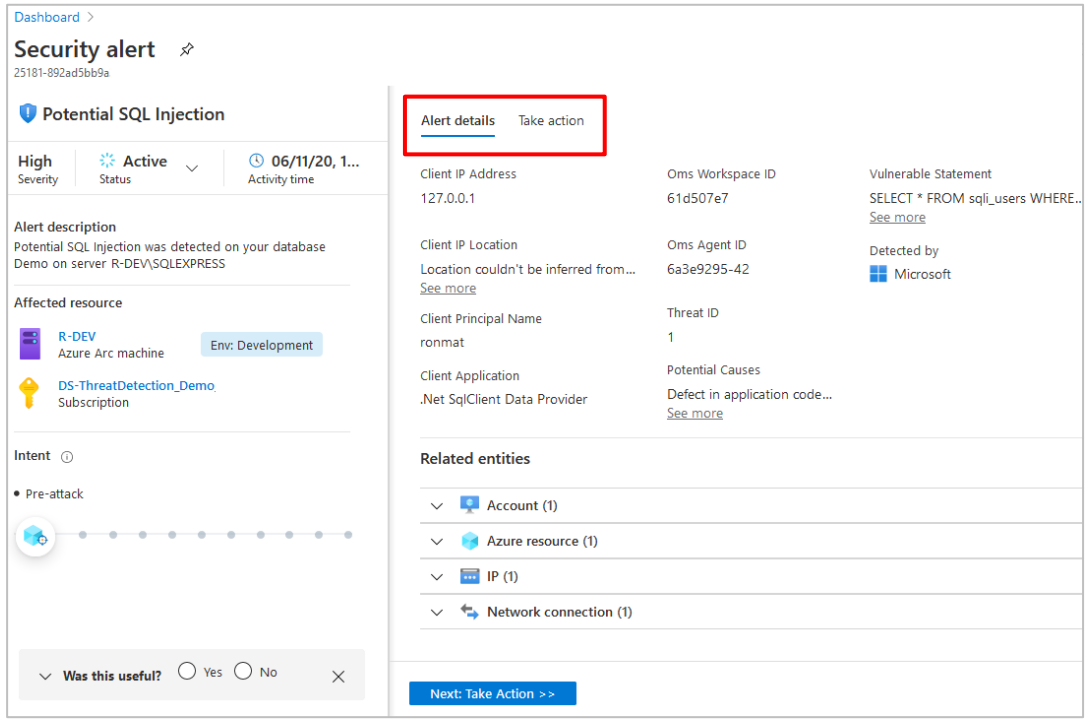
- From Defender for Cloud's overview, choose "**Security alerts**."
- Use and add filters to refine alert display.

Respond to security alerts

Choose an alert and click "**View full details**."

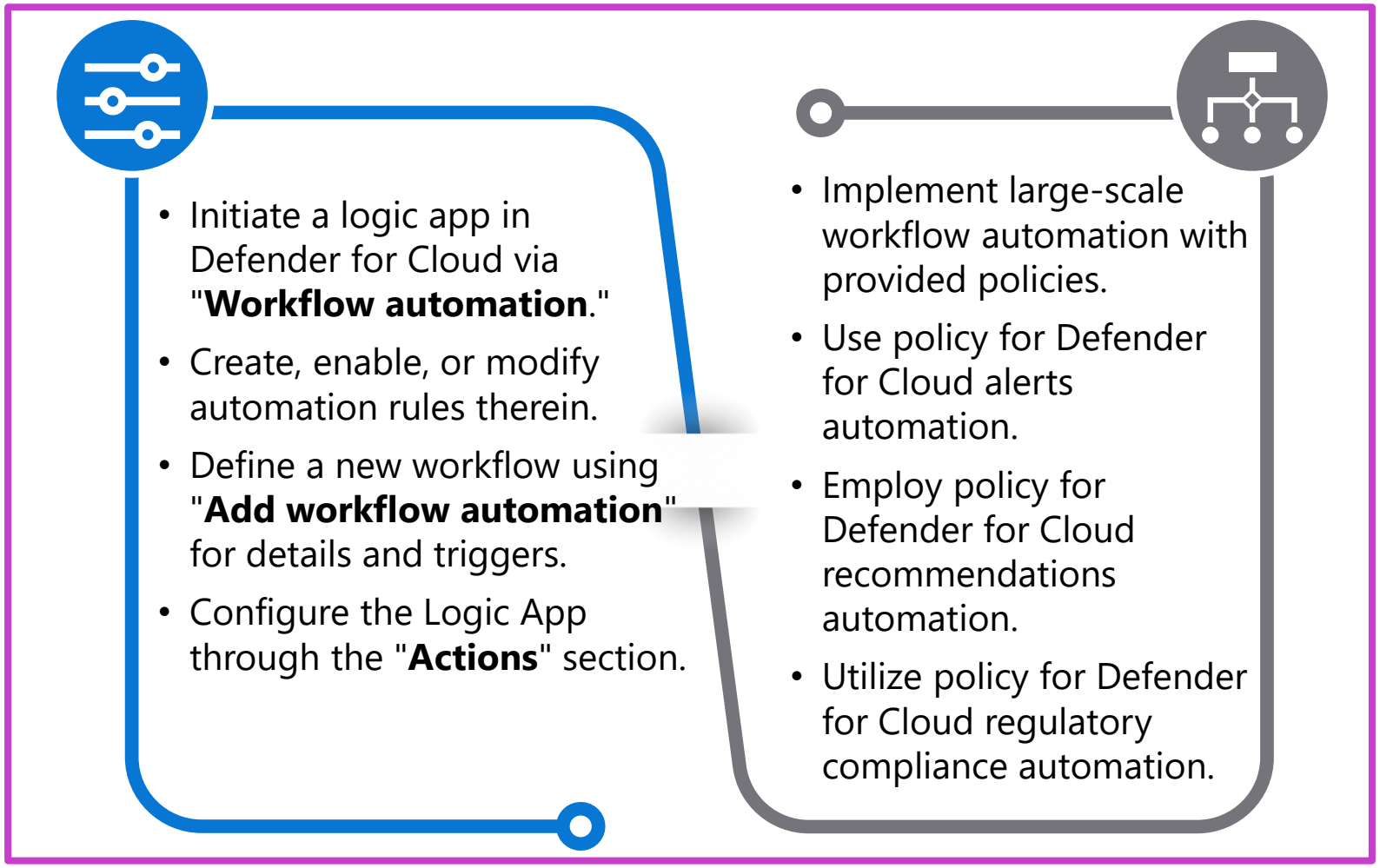
- Investigate and mitigate threats using "Alert details" and "Take action" tabs.





Configure workflow automation by using Microsoft Defender for Cloud

To configure workflow automation, you can:



Evaluate vulnerability scans from Microsoft Defender for Server

The following vulnerability assessment options are available in Defender for Servers:

Microsoft Defender Vulnerability Management

- Offered in both Defender for Servers Plan 1 and 2.
- Auto-enabled for machines with Defender for Endpoint's Vulnerability Management.
- Shares prerequisites with Defender for Endpoint across Windows, Linux, and networks.
- Requires no extra software installation.

Qualys vulnerability scanner

- Exclusive to Defender for Servers Plan 2.
- Ideal for **third-party EDR** or **Fanotify-based setups** without Defender for Endpoint.
- Defender for Cloud's integrated Qualys doesn't support proxy or connect to existing Qualys.
- Vulnerability findings limited to Defender for Cloud.

Configure and manage security monitoring and automation solutions

Monitor security events by using Azure Monitor

You can enable Azure Monitor in Azure and non-Azure virtual machines by installing an agent.

To monitor security events with Azure Monitor:

- Use Log Analytics Workspace to review logs and perform queries on log data
- Collect platform logs and metrics
- Collect Azure Virtual Machine internal host logs
- Perform custom queries

Azure security baseline for Azure Monitor covers areas such as:

- Network Security
- Identity Management
- Privileged Access
- Data Protection
- Asset Management
- Logging and Threat Detection
- Posture and Vulnerability Management
- Backup and Recovery

Configure data connectors in Microsoft Sentinel

Enable a data connector

- Select the connector and then select the **Open connector** page.
- Refer to the connector page to understand how to ingest the data.
- Review a summary of the data and the connectivity status.
- Go to the **Next steps** tab for more content for the specific data type.

Remember integrations for data connectors

- REST API integration
- Agent-based integration
- Service-to-service integration

Deploy data connectors as part of a solution

Deploy a solution with a data connector to get it together with the related content, in the same deployment.

Create and customize analytics rules in Microsoft Sentinel

Create a custom analytics rule with a scheduled query

- From the Microsoft Sentinel navigation menu, select **Analytics**.
- Select **+Create** and select **Scheduled query rule**.
- Configure the settings in the Analytics rule wizard's **General** tab.

Define the rule query logic and configure settings

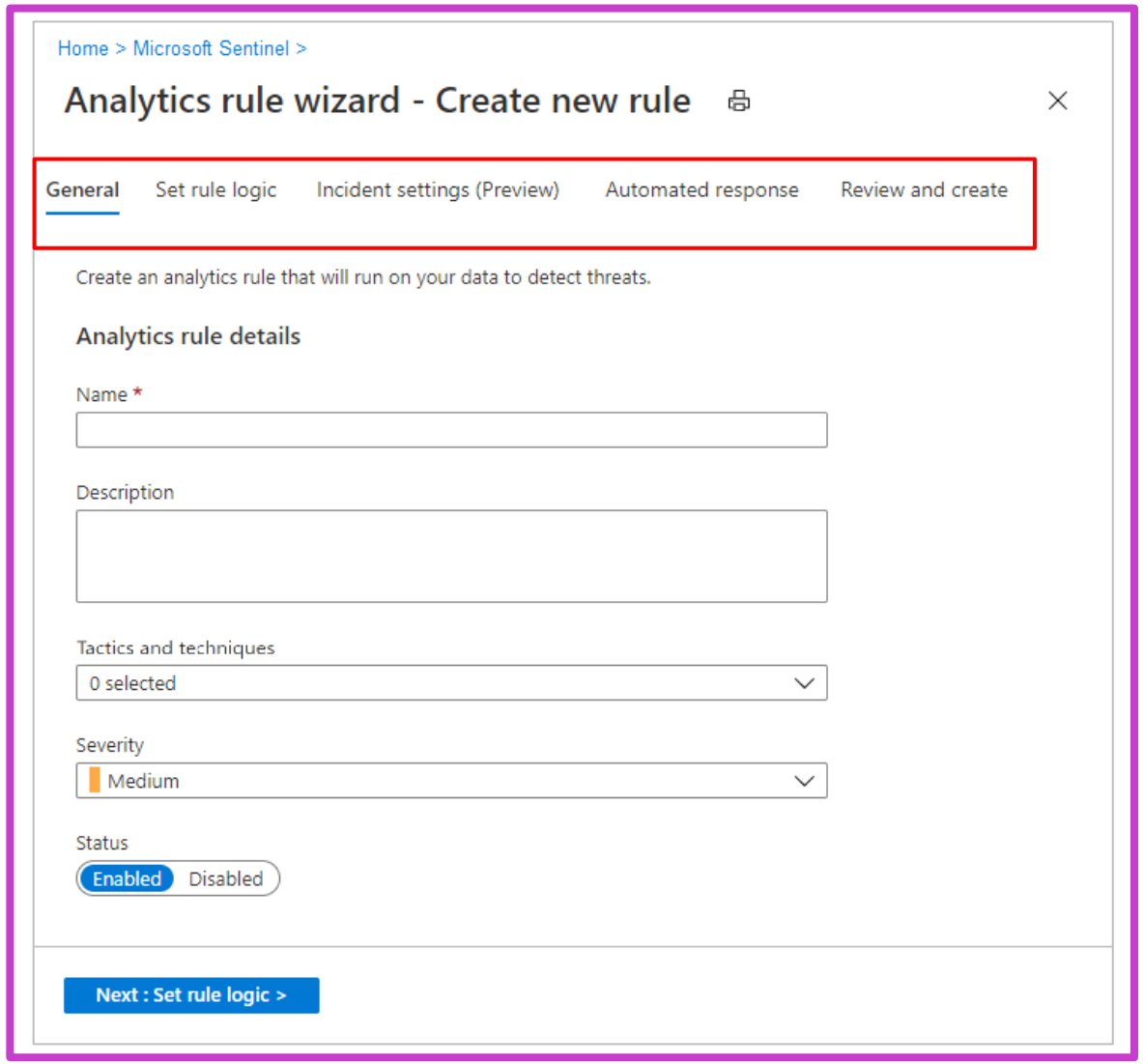
- Configure settings such as **Rule query**, **Alert enrichment**, **Query scheduling, Alert threshold,** and **Event grouping.**

Configure the incident creation settings

- Choose whether and how Microsoft Sentinel turns alerts into actionable incidents using **Incident settings** and **Alert grouping** sections.

Set automated responses and create the rule

- Set automation based on the alert generated by this analytics rule or on the incident created by the alerts.
- Review and create the rule.



Configure automation in Microsoft Sentinel

Configure automation rules

By configuring automation rules, you can:

- Centrally manage the automation of incident handling
- Assign playbooks to incidents and alerts
- Automate responses for multiple analytics rules at once
- Tag, assign, or close incidents automatically without using playbooks
- Create lists of tasks for your analysts to perform
- Control the order of actions that are executed
- Apply automations when an incident is updated (now in Preview), as well as when it's created

Automate using playbooks

Using a playbook, you can:

- Automate and orchestrate your threat response
- Integrate with other systems, both internal and external
- Set playbooks to run automatically in response to specific alerts or incidents
- Benefit from the power and customization
  offered by Logic Apps in the form of:
  - Its integration and orchestration capabilities
  - Easy-to-use design tools
  - Scalability, reliability, and service level of a Tier 1 Azure service

Module Labs

Lab 07 – Key Vault

Create a Key Vault and configure permissions

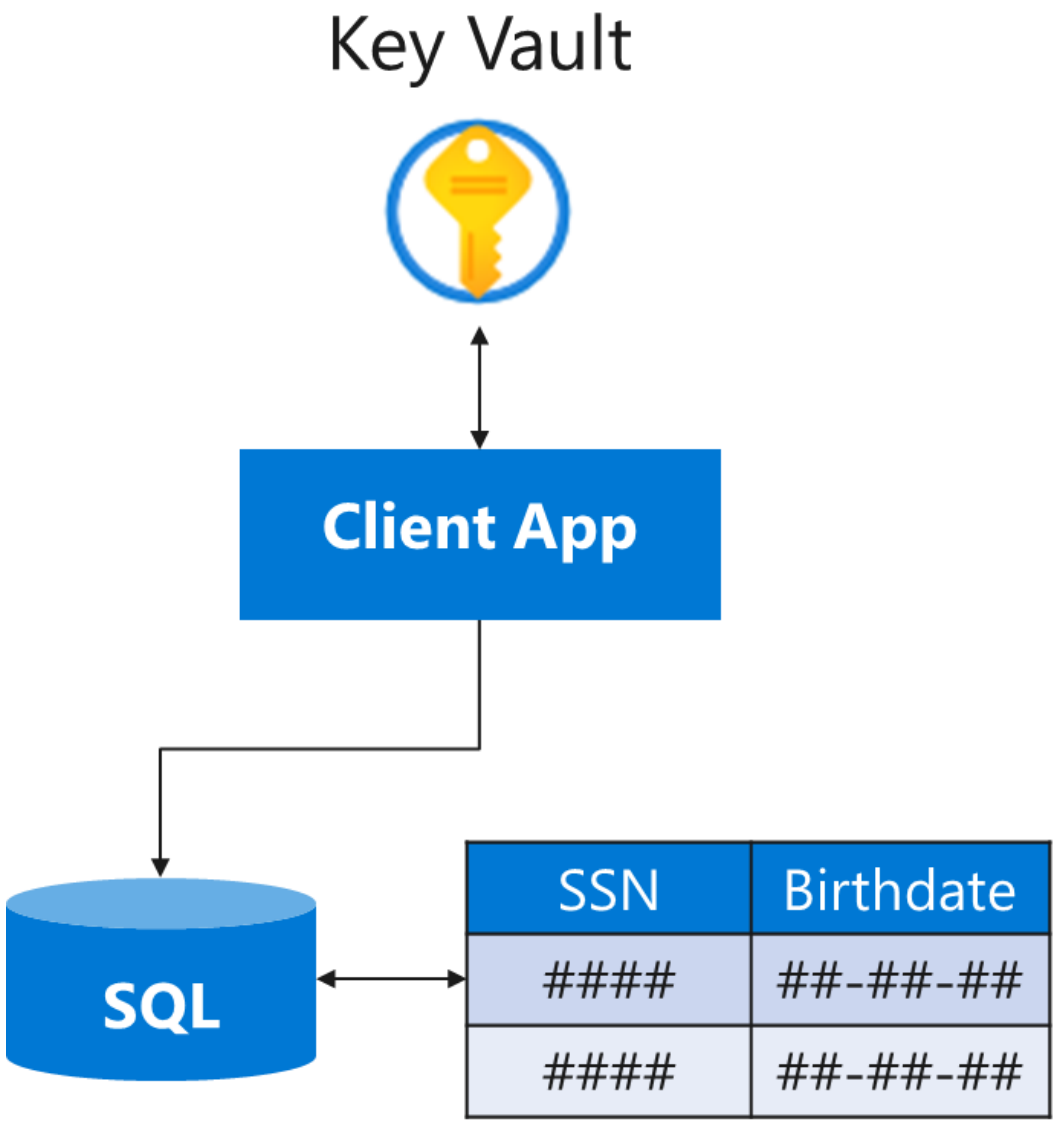
Add a key and a secret to the vault

Register a client app that uses the key

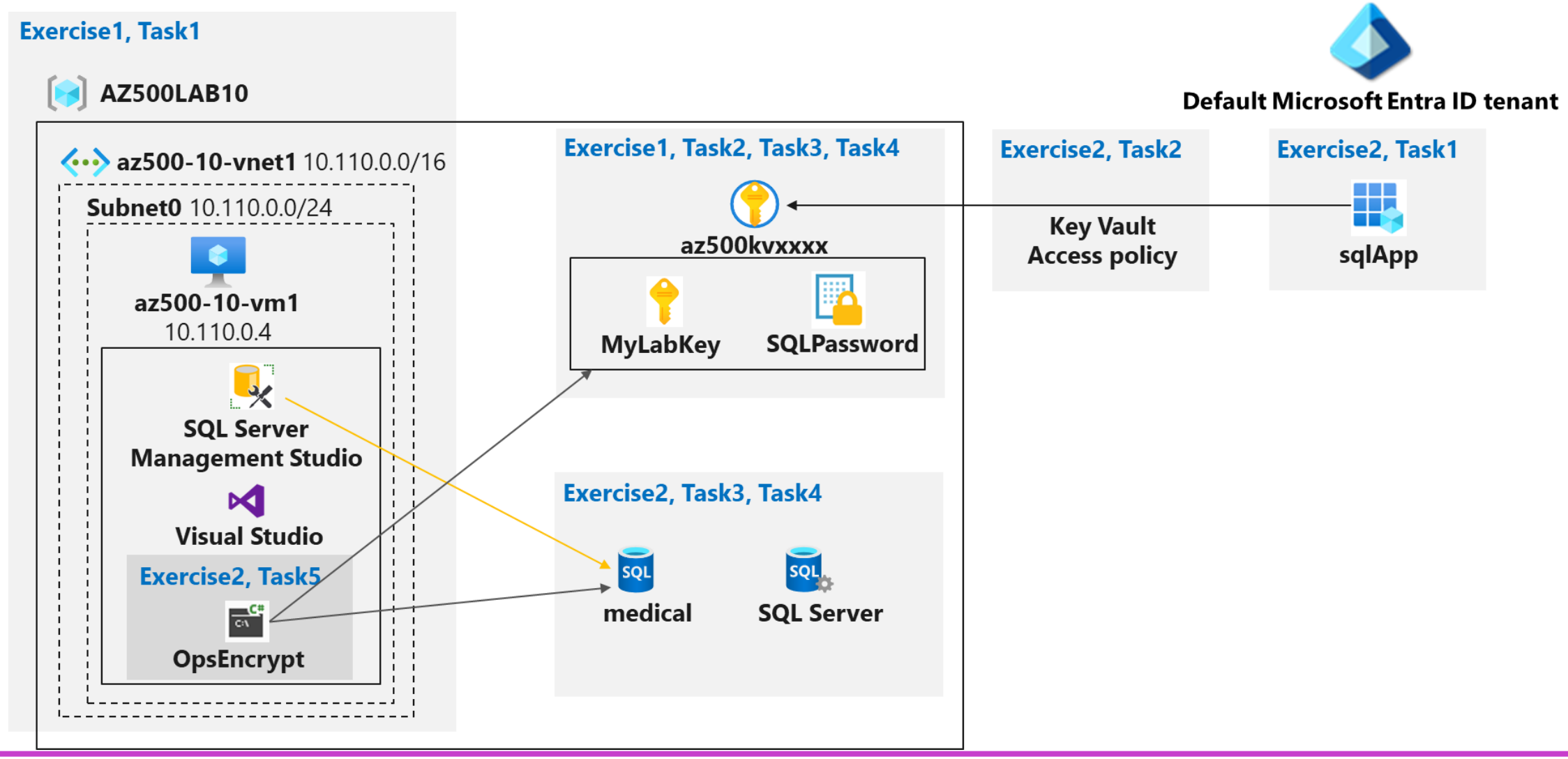
Create a SQL database

Encrypt columns in a table

Build a console app to test the encryption



Lab 07 - Key Vault



Lab 08 – Azure Monitor

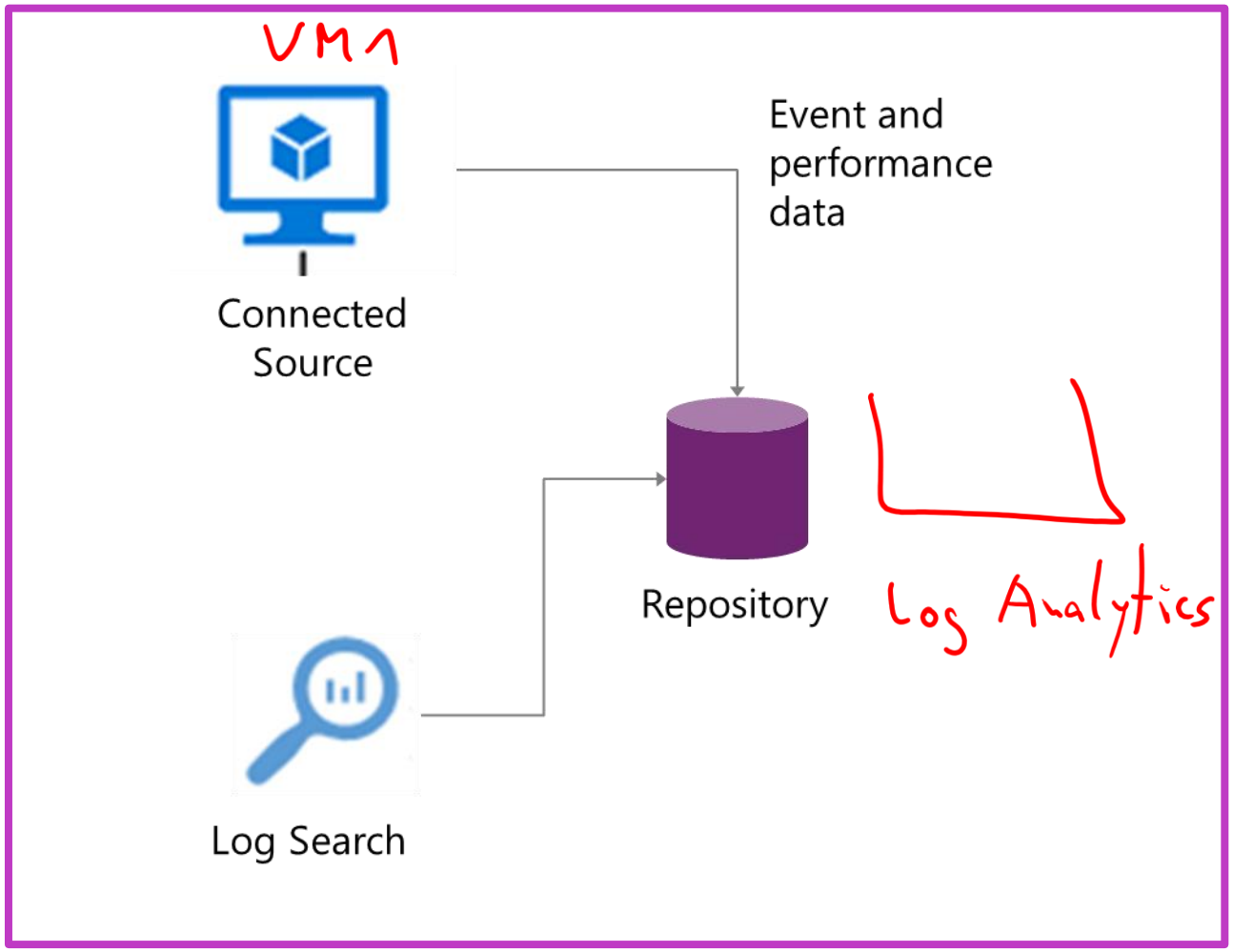
Deploy an Azure virtual machine

Create a Log Analytics workspace

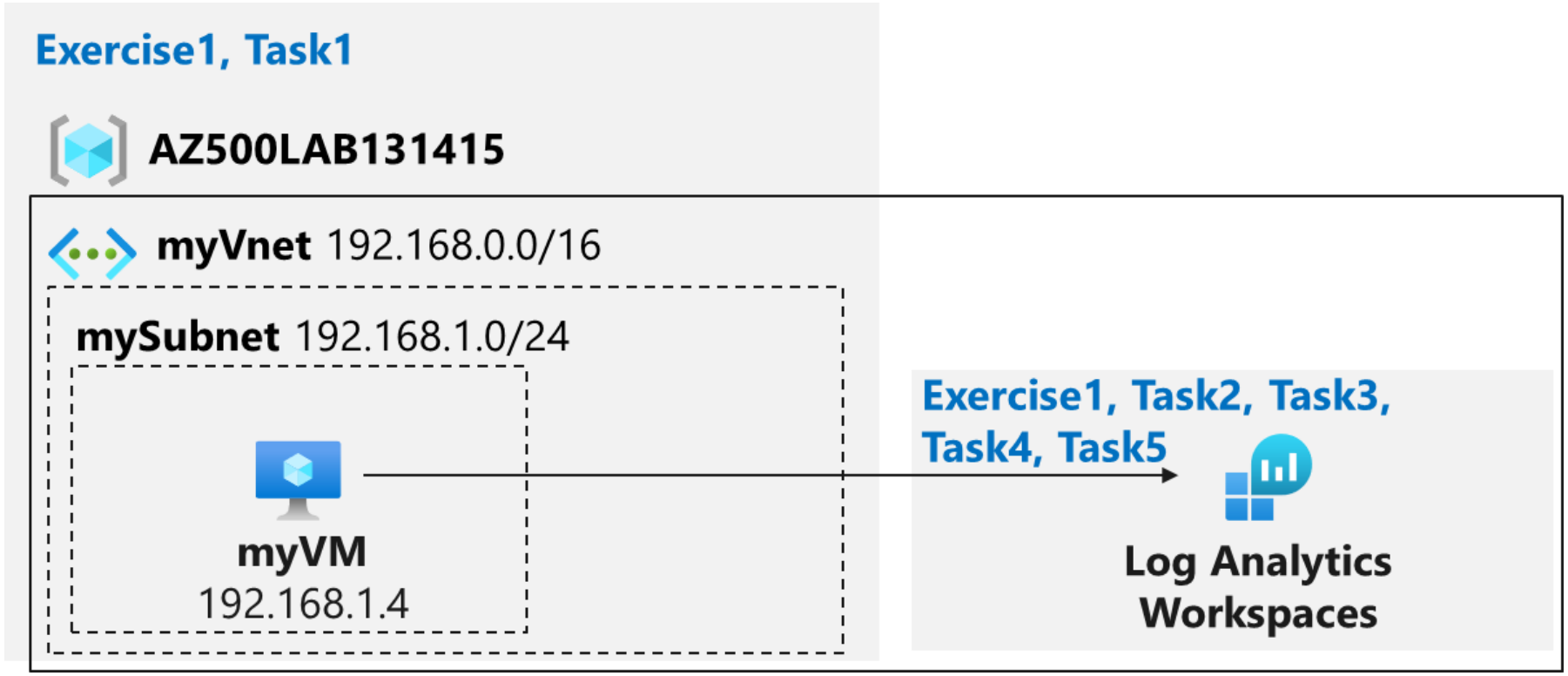
Enable the Log Analytics virtual machine extension

Collect virtual machine event and performance data

View and query collected data



Lab 08 – Azure Monitor



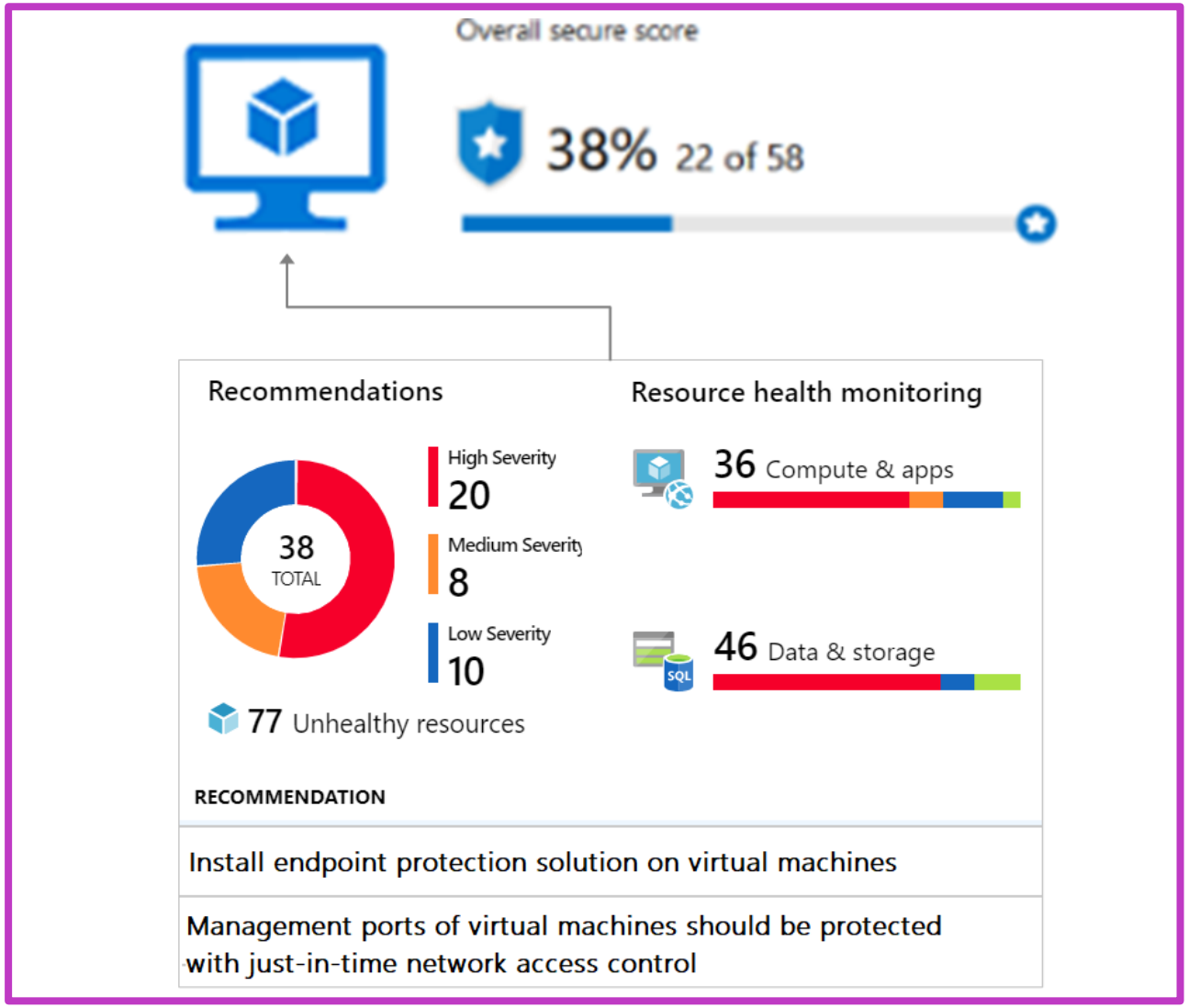
Lab 09 – Microsoft Defender for Cloud

Configure Microsoft Defender for Cloud to monitor a virtual machine

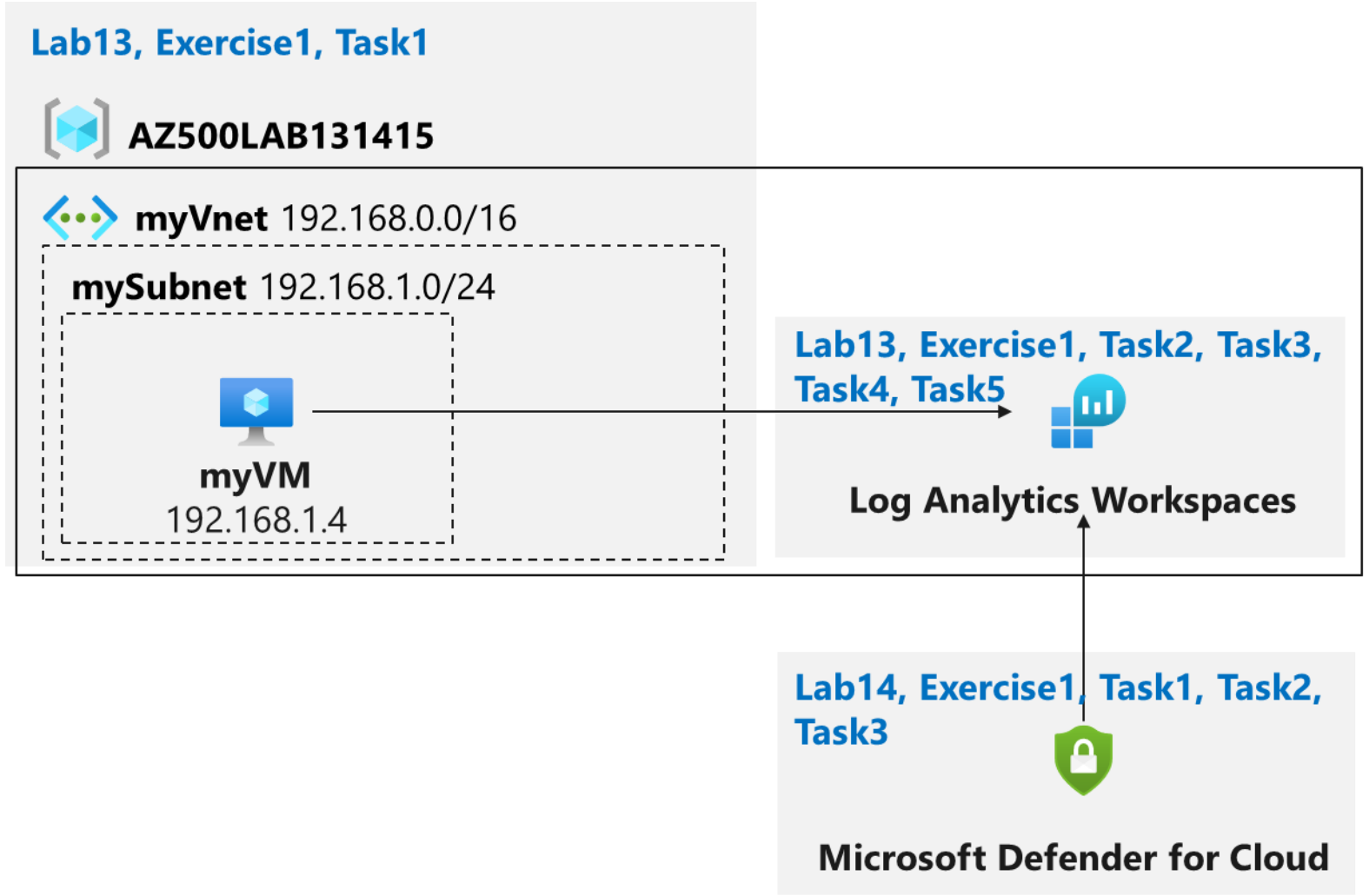
Review Microsoft Defender for Cloud recommendations for the virtual machine

Implement recommendations for endpoint protection and Just in time VM access

Review the Secure Score



Lab 09 – Microsoft Defender for Cloud



Lab 10 – Microsoft Sentinel

On-board Microsoft Sentinel

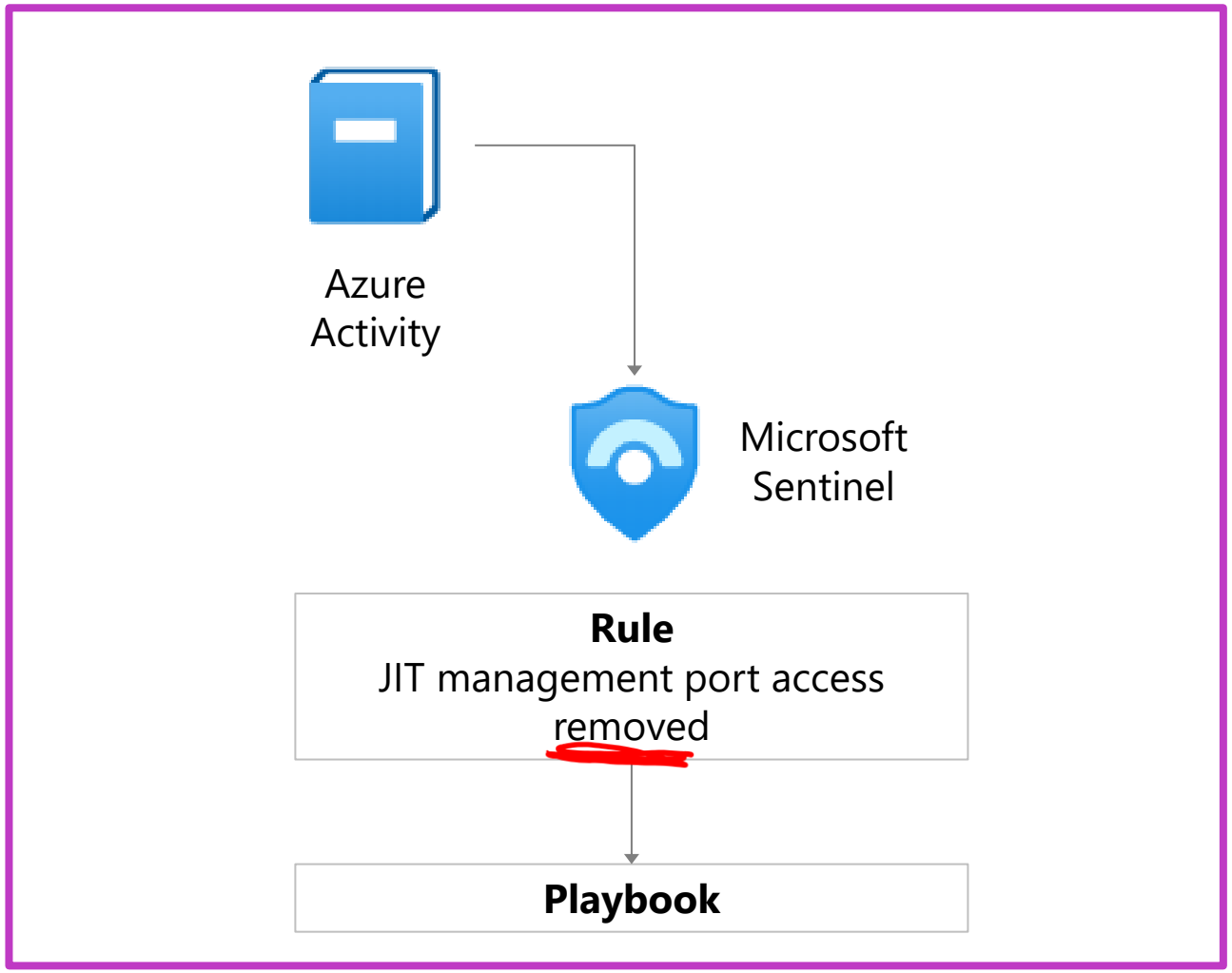
Connect Azure Activity to Sentinel

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

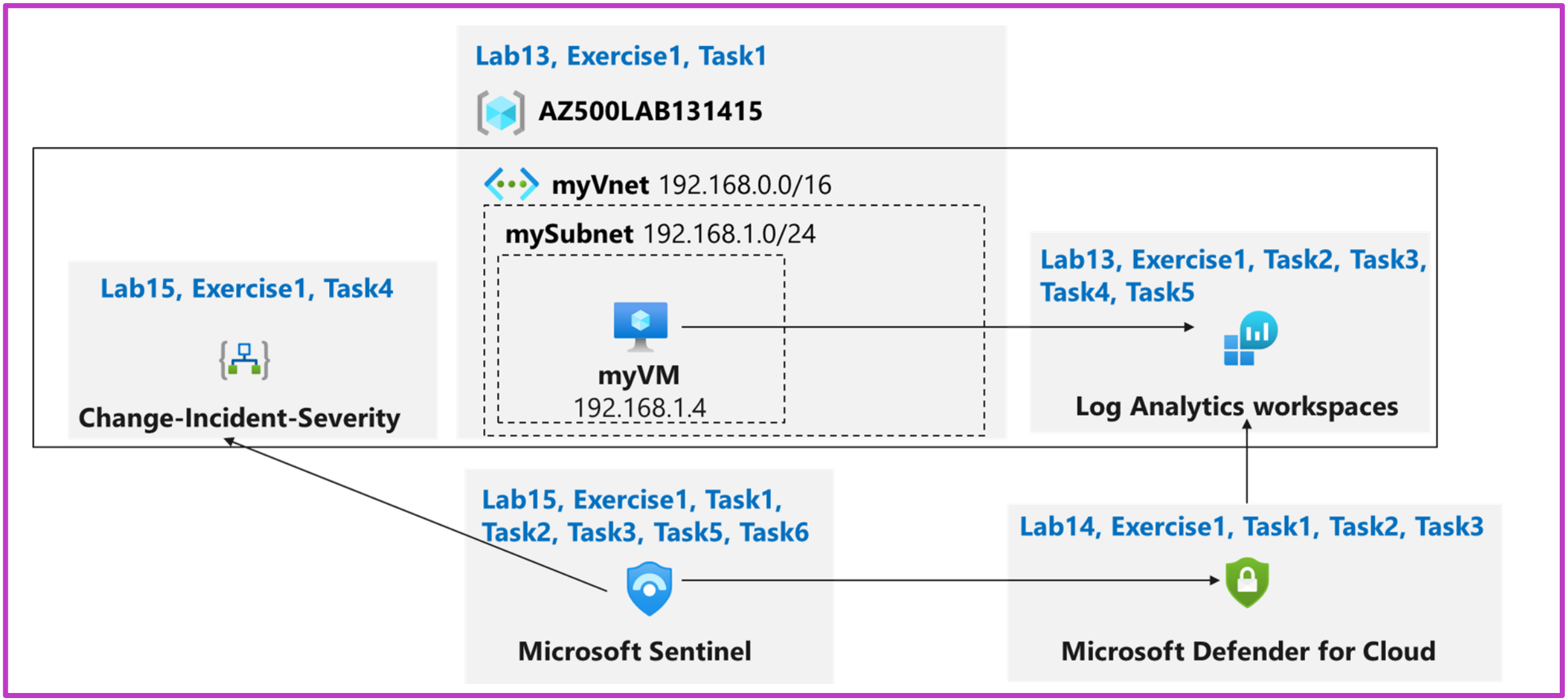
Create a playbook

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

Invoke an incident and review the associated actions



Lab 10 – Microsoft Sentinel



Knowledge check

1 **What is the primary function of Data Collection Rules (DCRs) in Azure Monitor?**

- ☑ To specify what data should be collected, how to transform that data, and where to send it
- ☐ To define the visual themes of Azure Monitor dashboards
- ☐ To manage user permissions in Azure Monitor

2 **What is the purpose of Microsoft Defender for Cloud?**

- ☐ To manage cloud billing and usage
- ☑ To protect cloud resources from threats
- ☐ To create virtual networks in Azure

3 **How can you customize detection rules in Microsoft Sentinel?**

- ☐ By predicting stock market trends
- ☑ By identifying potential security incidents
- ☐ By automating virtual machine deployments

Learning Path Recap

In this learning path, we:

Enabled effective performance tracking and real-time analytics through Azure Monitor configuration and management.

Fortified cloud security by enabling and managing Microsoft Defender for Cloud to counter various threats.

Set up and oversaw Microsoft Sentinel for centralized security data analysis and threat detection.

End of presentation