Microsoft Security

SC-200 Microsoft Security Operations Analyst

Author name

Date

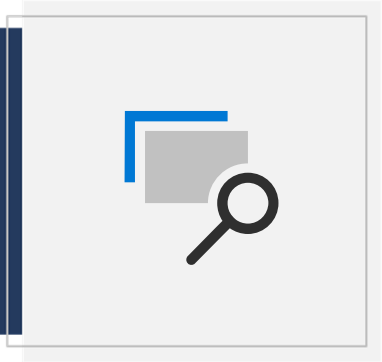
Microsoft Security

Module 3: Mitigate threats using Microsoft Defender for Cloud

Module agenda

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Workload protections in Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

Lesson 1: Plan for cloud workload protections using Microsoft Defender for Cloud



Lesson introduction

After this lesson, you will be able to:

- Describe Microsoft Defender for Cloud features
- Explain Microsoft Defender for Cloud workload protections
- Enable Microsoft Defender for Cloud

Explain Microsoft Defender for Cloud

- Strengthen security posture
- Manage organization security policy and compliance
- Continuous assessments
- Optimize and improve security by configuring recommended controls
- Network map
- Automatically discover and onboard Azure resources with automatic provisioning

Guided demonstration – Microsoft Defender for Cloud

Scenario:
You are the security operations analyst and must protect your hybrid cloud with Microsoft Defender for Cloud.

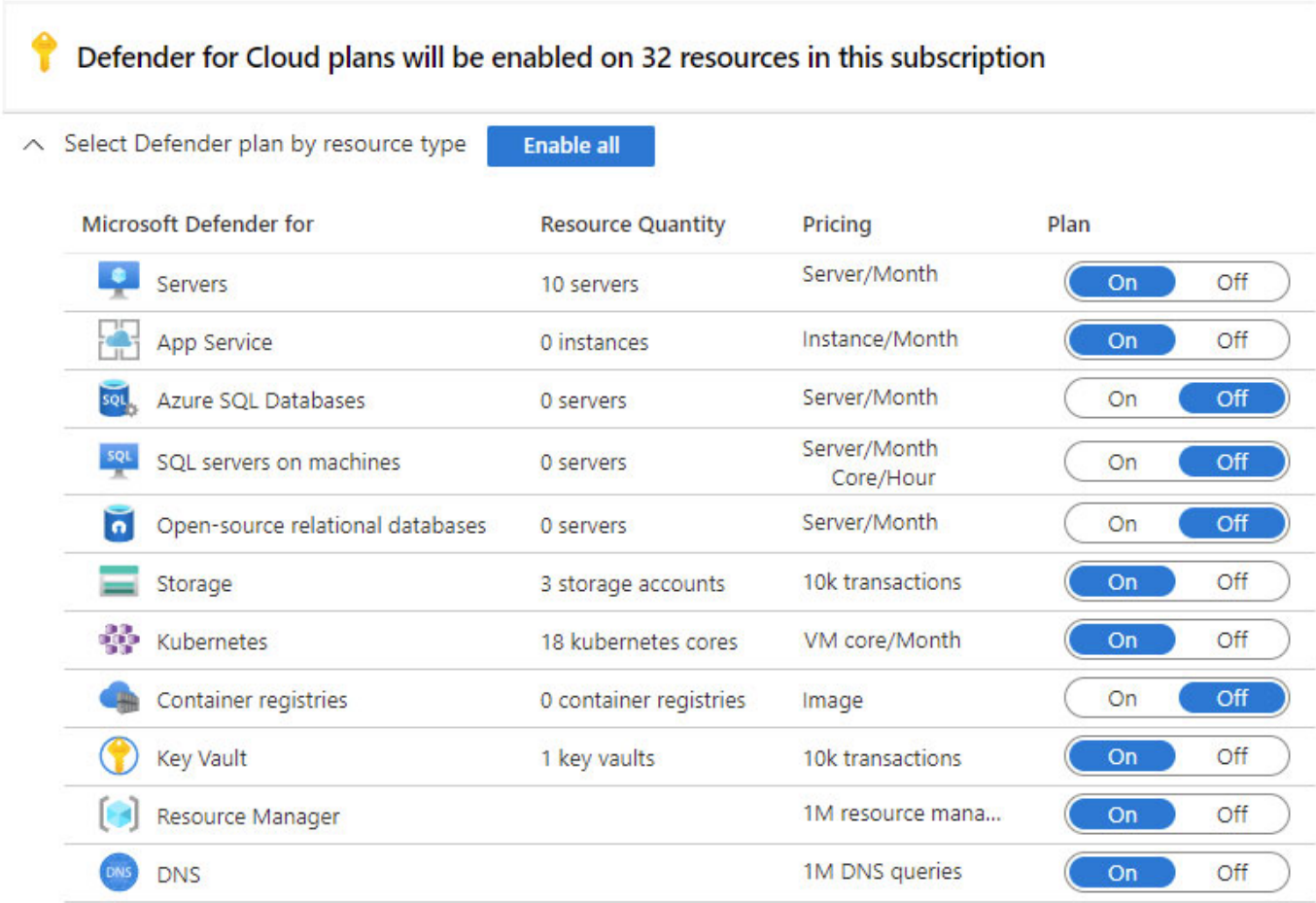
Task 1 Manage cloud security posture

Task 2 Protect against threats

Task 3 Get advanced insights

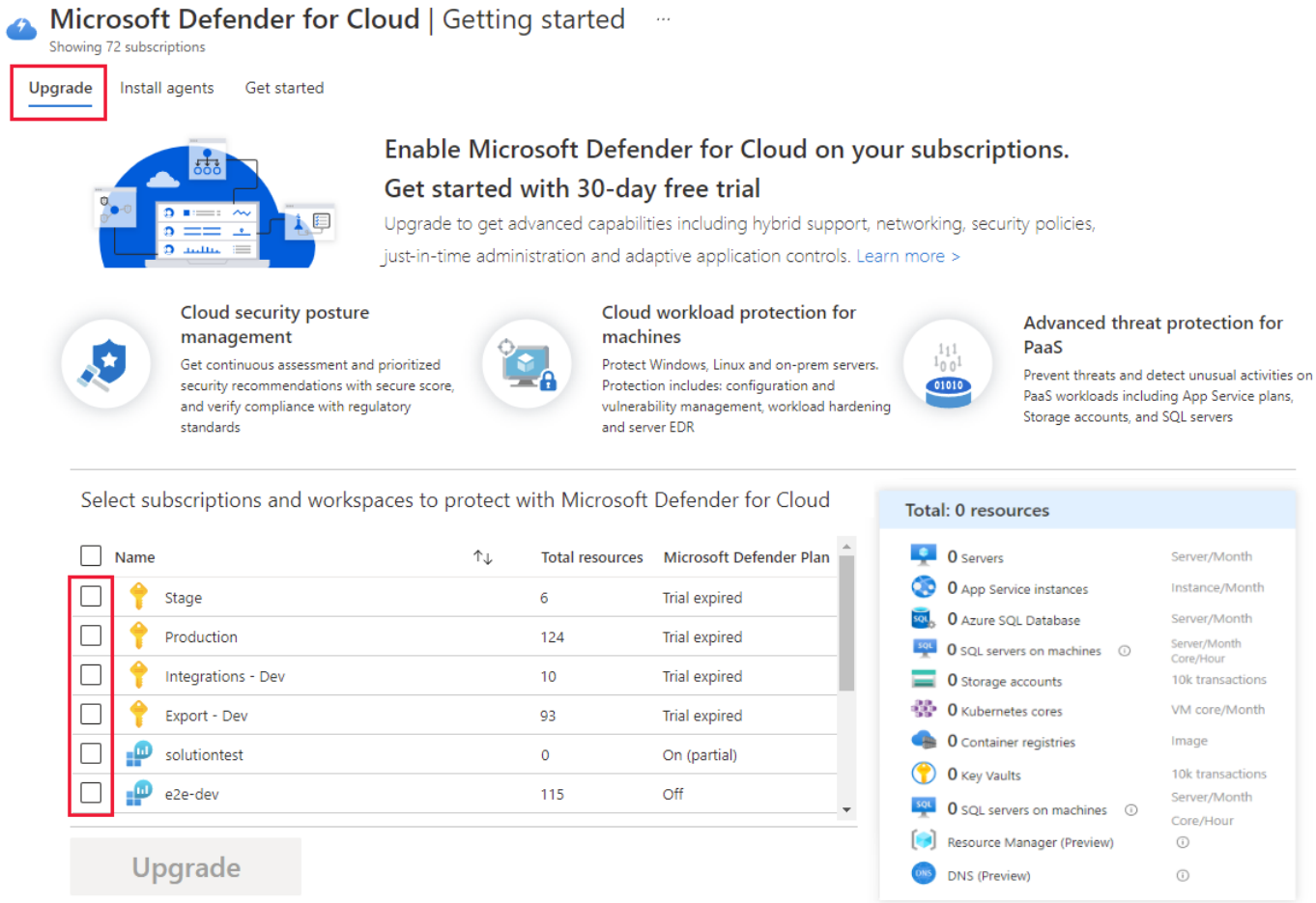
Microsoft Defender for Cloud workload protections

Microsoft Defender for Cloud, brings advanced, intelligent protection to your Azure and hybrid resources and workloads.



Enable Microsoft Defender for Cloud

To enable all Defender for Cloud features including threat protection capabilities, you must enable enhanced security features on the subscription containing the applicable workloads.



Lesson 2: Workload protections in Microsoft Defender for Cloud

Lesson introduction

After this lesson, you will be able to:

- Explain which workloads are protected by Microsoft Defender for Cloud
- Describe the benefits of the protections offered by Microsoft Defender for Cloud
- Explain how Microsoft Defender for Cloud protection's function

Microsoft Defender for servers

- Microsoft Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.

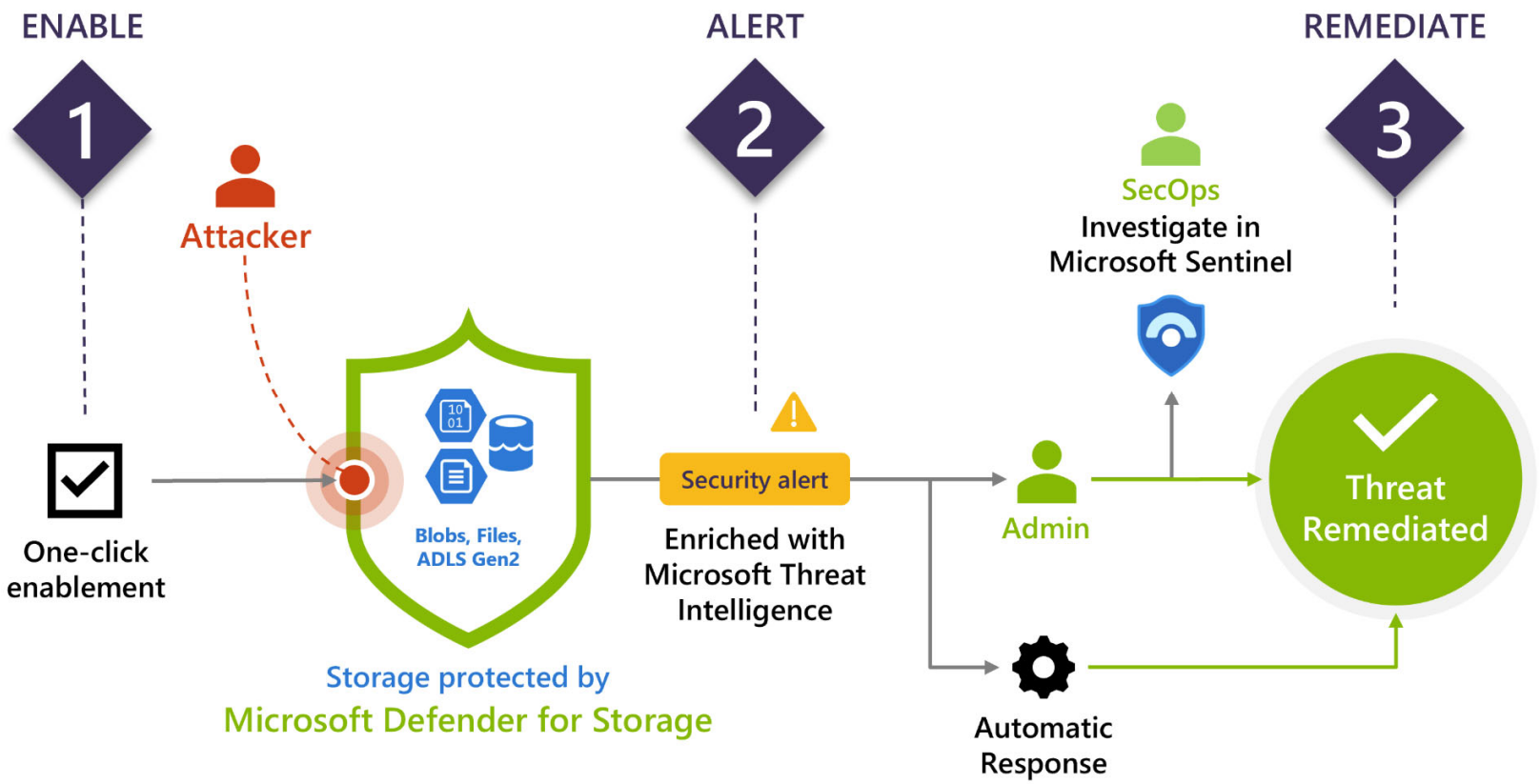
- For Windows, Microsoft Defender for Cloud integrates with Azure services to monitor and protect your Windows-based machines. Microsoft Defender for Cloud presents the alerts and remediation suggestions from all these services in an easy-to-use format.

- For Linux, Microsoft Defender for Cloud collects audit records from Linux machines by using auditd, one of the most common Linux auditing frameworks. auditd lives in the mainline kernel.

Microsoft Defender for App Service

- Microsoft Defender for App Service uses the scale of the cloud to identify attacks targeting applications running over App Service.
- Attackers probe web applications to find and exploit weaknesses. Before being routed to specific environments, requests to applications running in Azure go through several gateways, where they're inspected and logged.
- This data is then used to identify exploits and attackers and learn new patterns that will be used later.

Microsoft Defender for Storage



Microsoft Defender for SQL

Microsoft Defender for SQL comprises two separate Microsoft Defender plans:

Microsoft Defender for Azure SQL database servers protects:

- Azure SQL Database
- Azure SQL Managed Instance
- Dedicated SQL pool in Azure Synapse

Microsoft Defender for SQL servers on machines extends the protections for your Azure-native SQL Servers to fully support hybrid environments and protect SQL servers (all supported version) hosted in Azure, other cloud environments, and even on-premises machines:

- SQL Server on Virtual Machines
- On-premises SQL servers:
  - Azure Arc enabled SQL Server
  - SQL Server running on Windows machines without Azure Arc

Microsoft Defender for open-source relational databases

protections for the following open-source relational databases are available for:

- Azure Database for PostgreSQL
- Azure Database for MySQL
- Azure Database for MariaDB

Microsoft Defender for Key Vault

Microsoft Defender detects unusual and potentially harmful attempts to access or exploit Key Vault accounts. This layer of protection allows you to:

- Address threats without being a security expert.
- Address threats without the need to manage third-party security monitoring systems.

When anomalous activities occur, Microsoft Defender shows alerts and optionally sends them via email to relevant members of your organization. These alerts include the details of the suspicious activity and recommendations on how to investigate and remediate threats.

Microsoft Defender for Resource Manager

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through:

- Azure portal
- Azure REST APIs
- Azure CLI
- other Azure programmatic clients

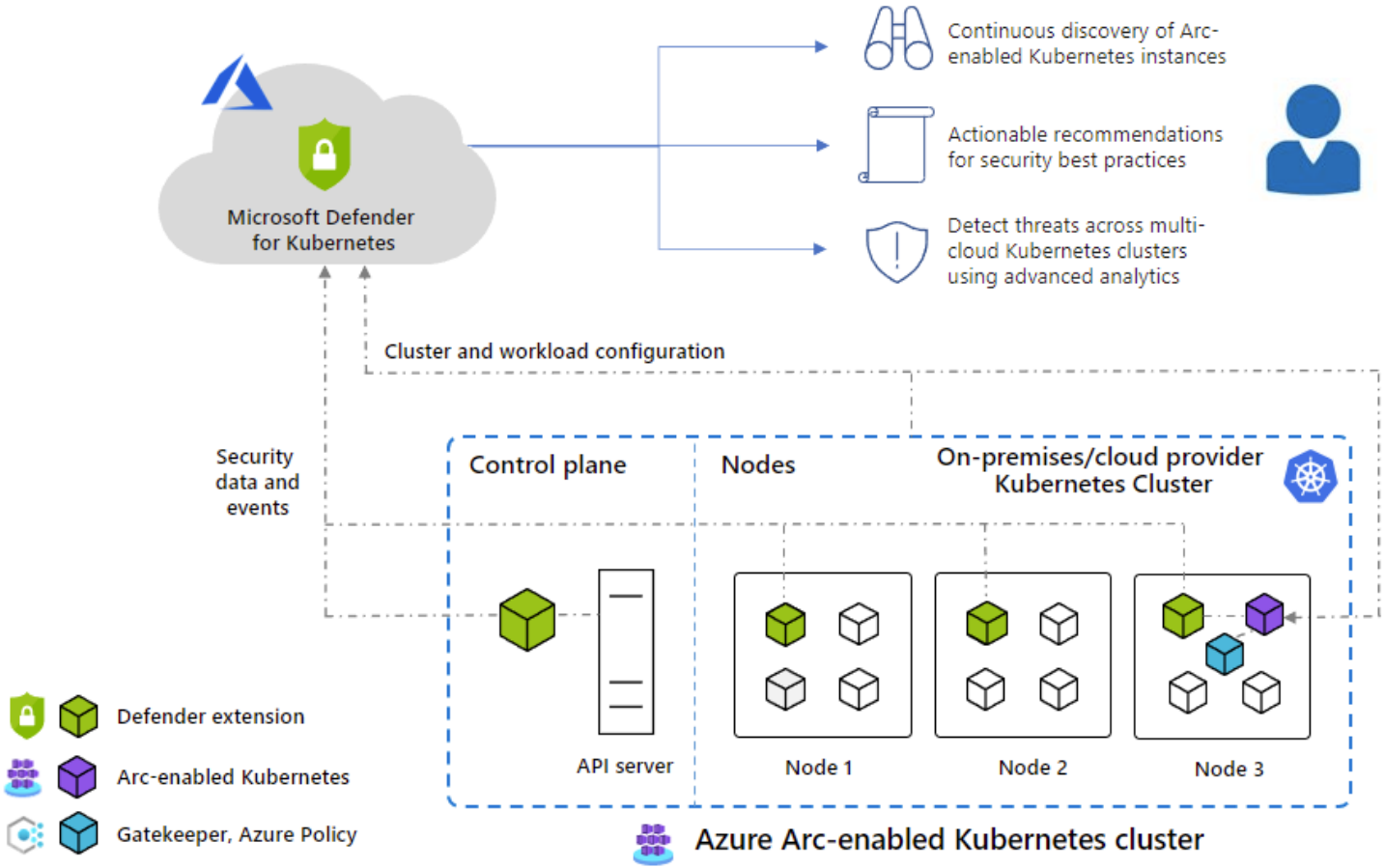
Microsoft Defender runs advanced security analytics to detect threats and alert you about suspicious activity.

Microsoft Defender for DNS

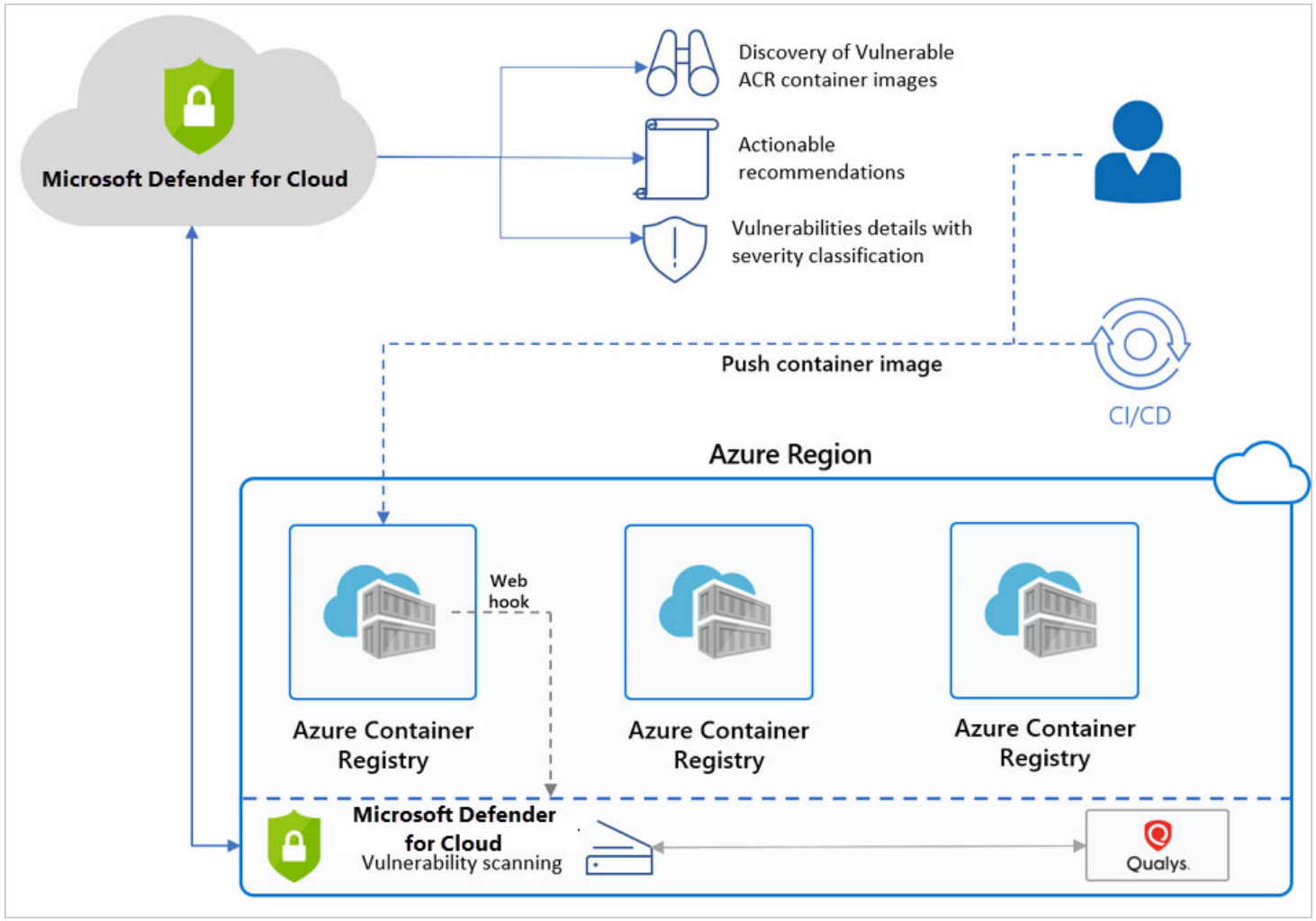
Microsoft Defender for DNS provides an extra layer of protection for your cloud resources by:

- Continuously monitoring all DNS queries from your Azure resources
- Running advanced security analytics to alert you about suspicious activity

Microsoft Defender for Kubernetes



Microsoft Defender for container registries



Microsoft Defender for Cloud more protections

Microsoft Defender for Cloud also offers the following threat protection capabilities:

- Threat protection for Azure network layer
- Threat protection for Azure Cosmos DB (Preview)
- Display Azure WAF alerts in Microsoft Defender for Cloud
- Display Azure DDoS Protection alerts in Microsoft Defender for Cloud
- Display Microsoft Defender for Cloud recommendations in Defender for Cloud Apps

Lesson 3: Connect Azure assets to Microsoft Defender for Cloud

Lesson introduction

After this lesson, you will be able to:

- Explore Azure assets
- Configure auto-provisioning in Microsoft Defender for Cloud
- Describe manual provisioning in Microsoft Defender for Cloud

Explore and manage your resources with asset inventory

Inventory Summary

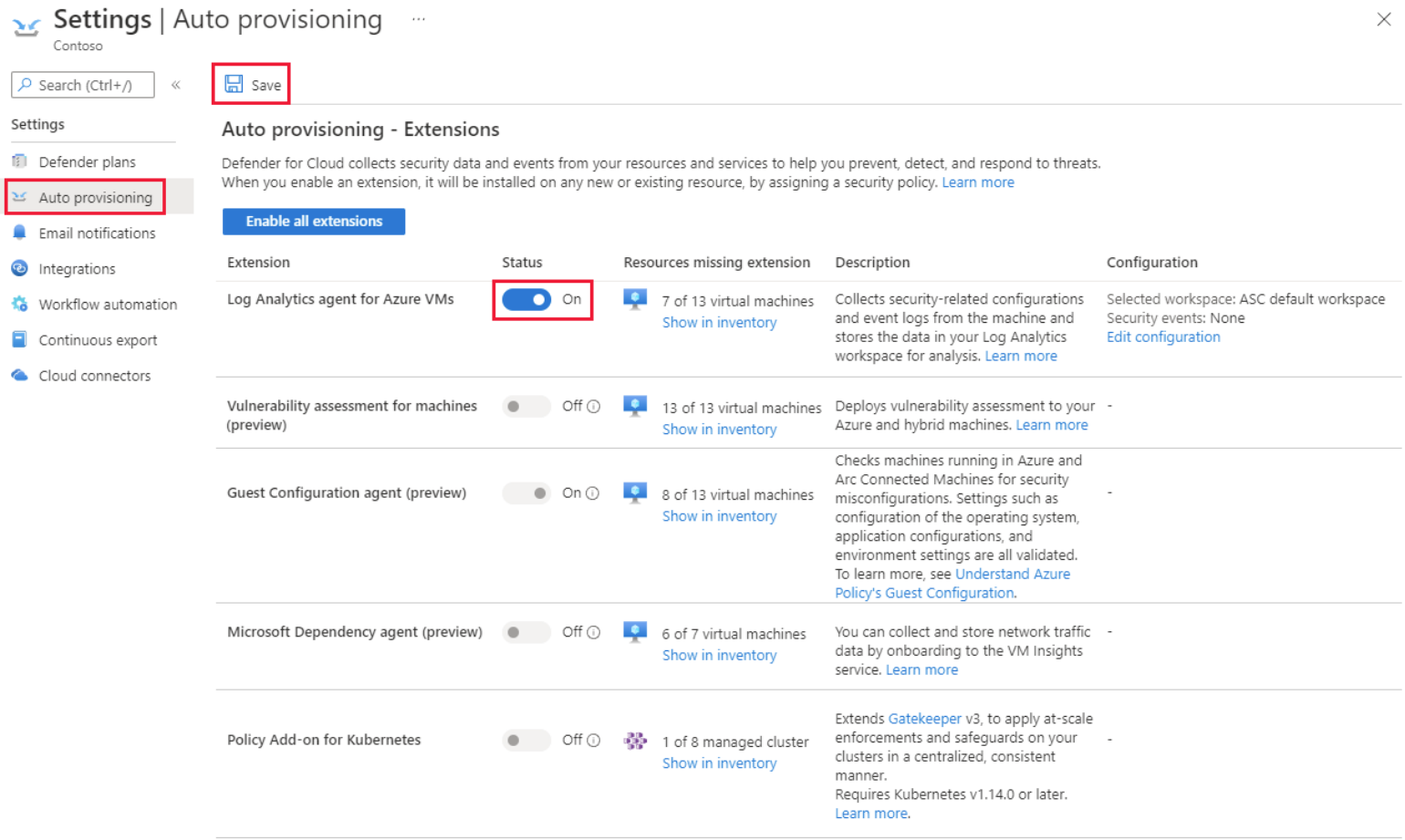
- Total Resources
- Unhealthy Resources
- Unmonitored Resources
- Unregistered Subscriptions

Status For each Resource

- Agent monitoring
- Microsoft Defender for Cloud
- Body Recommendations

Configure auto provisioning

Microsoft Defender for Cloud collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.



Manual log analytics agent provisioning

To manually install the Log Analytics agent on Azure VMs:

1. Disable auto provisioning.
2. Optionally, create a workspace.
3. Enable Microsoft Defender for Cloud on the workspace on which you're installing the Log Analytics agent.
4. Deploy agents on new VMs using a Resource Manager template, install the Log Analytics agent.
5. Deploy agents on your existing VMs.

Lesson 4: Connect non-Azure resources to Microsoft Defender for Cloud

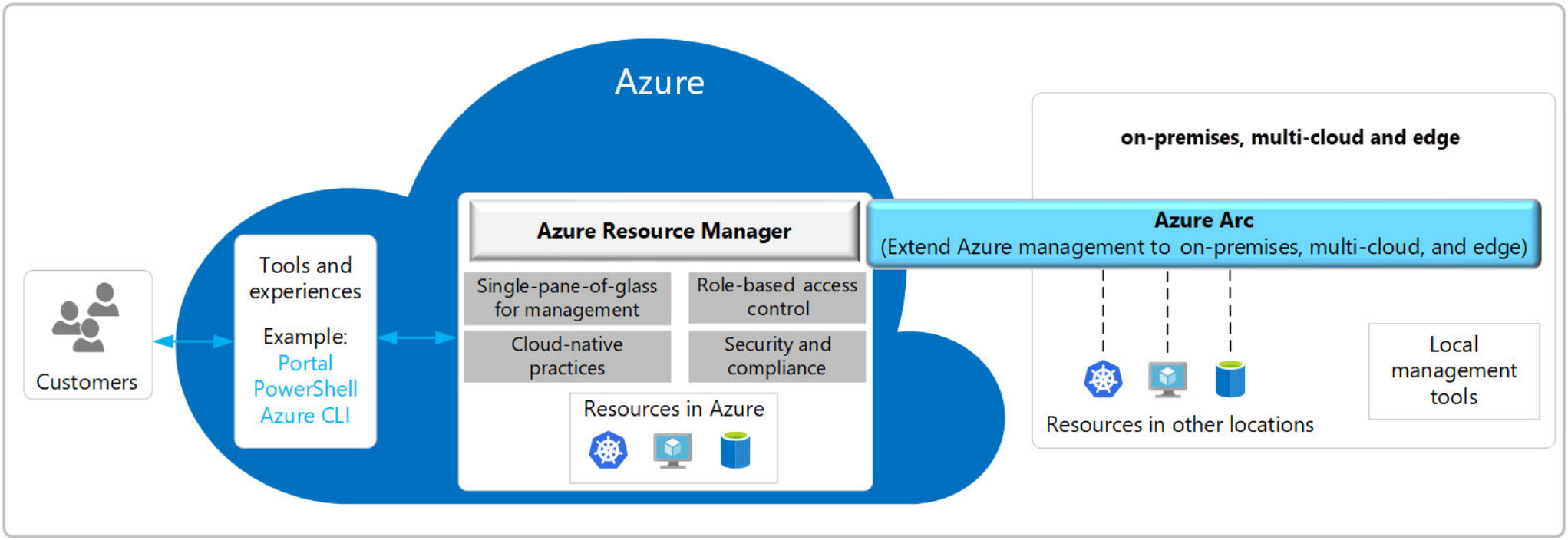
Lesson introduction

After this lesson, you will be able to:

- Connect non-Azure machines to Microsoft Defender for Cloud
- Connect AWS accounts to Microsoft Defender for Cloud
- Connect GCP accounts to Microsoft Defender for Cloud

Protect non-Azure resources

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

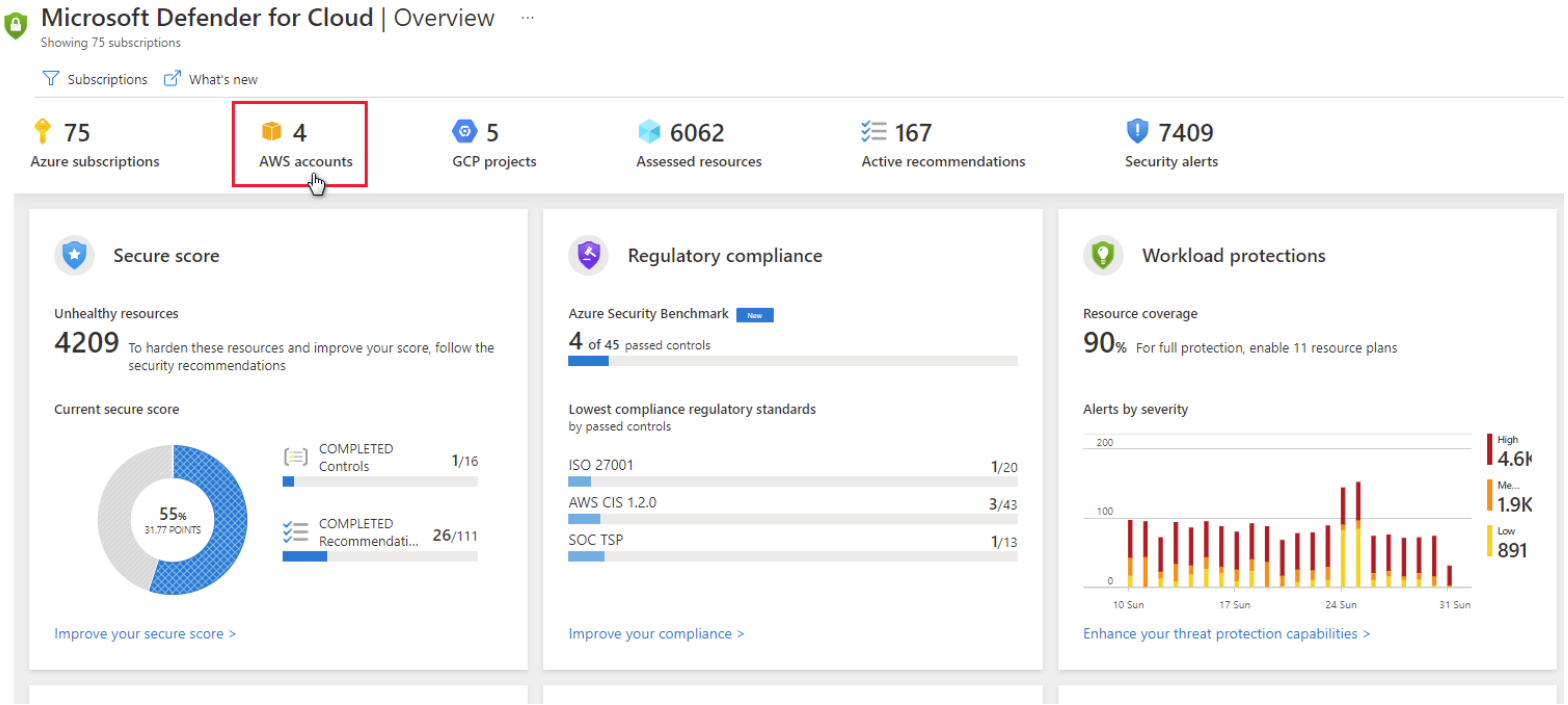


Connect non-Azure machines

Azure Arc Enabled	Without Azure Arc
Install Azure Arc agent on Host	Manually deploy Log Analytics agent to Windows Host
In the Azure Portal, Connect the host.	Manually deploy Log Analytics agent to Linux Host
	Manually deploy Log Analytics agent to Azure Stack VMs

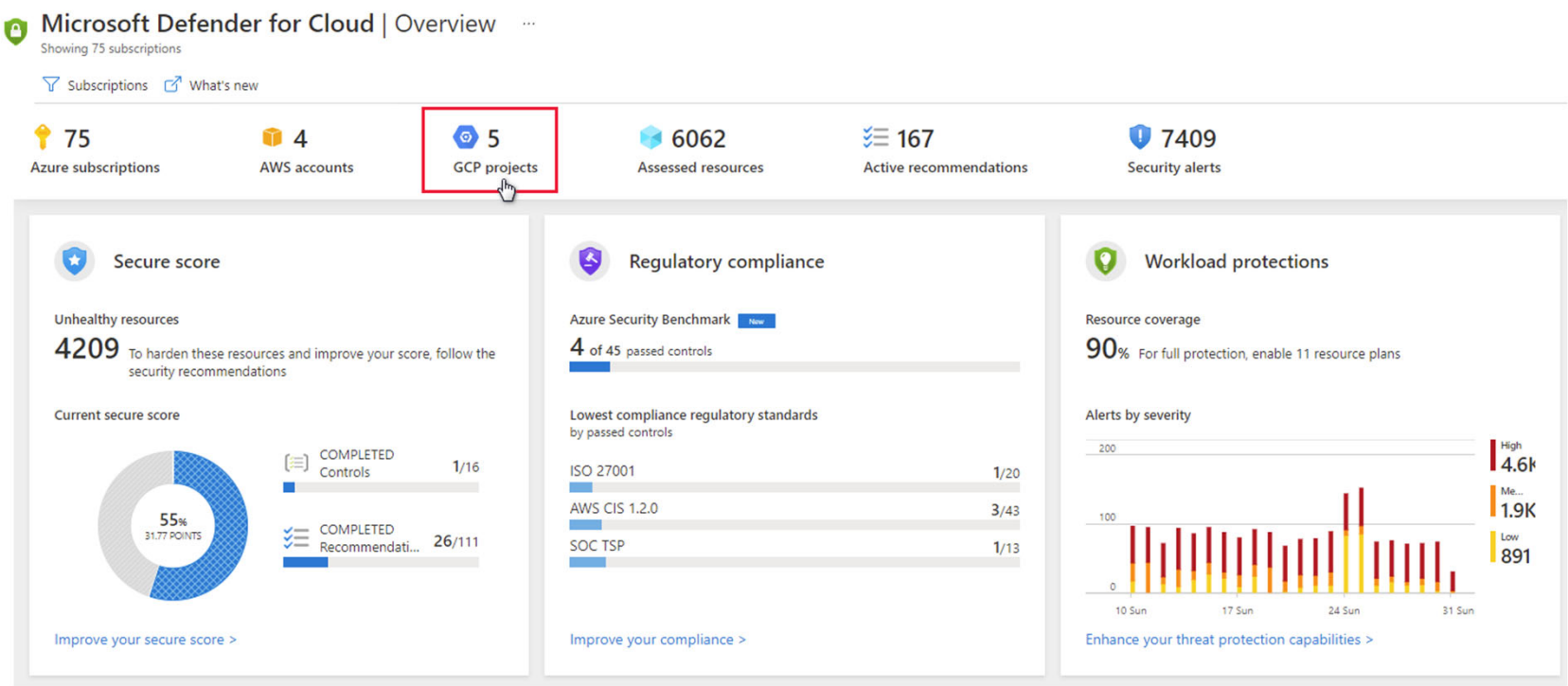
Connect AWS accounts

Onboarding your AWS account into Microsoft Defender for Cloud, integrates AWS Security Hub. Microsoft Defender for Cloud thus provides visibility and protection across both cloud environments.



Connect your GCP accounts

Onboarding your GCP account into Microsoft Defender for Cloud, integrates GCP Security Commands. Microsoft Defender for Cloud thus provides visibility and protection across both cloud environments.



Lesson 5: Remediate security alerts using Microsoft Defender for Cloud

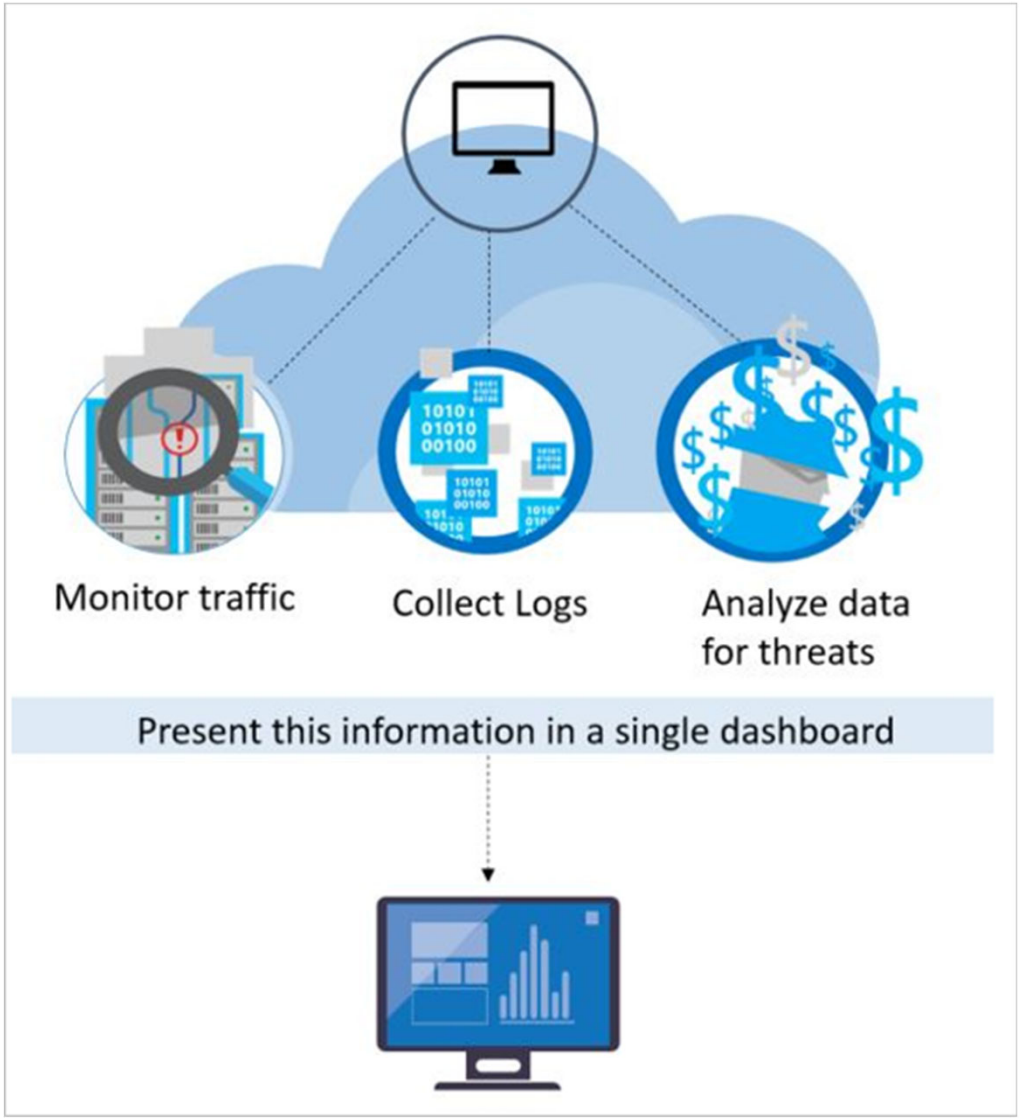
Lesson introduction

After this lesson, you will be able to:

- Describe alerts in Microsoft Defender for Cloud
- Remediate alerts in Microsoft Defender for Cloud
- Automate responses in Microsoft Defender for Cloud

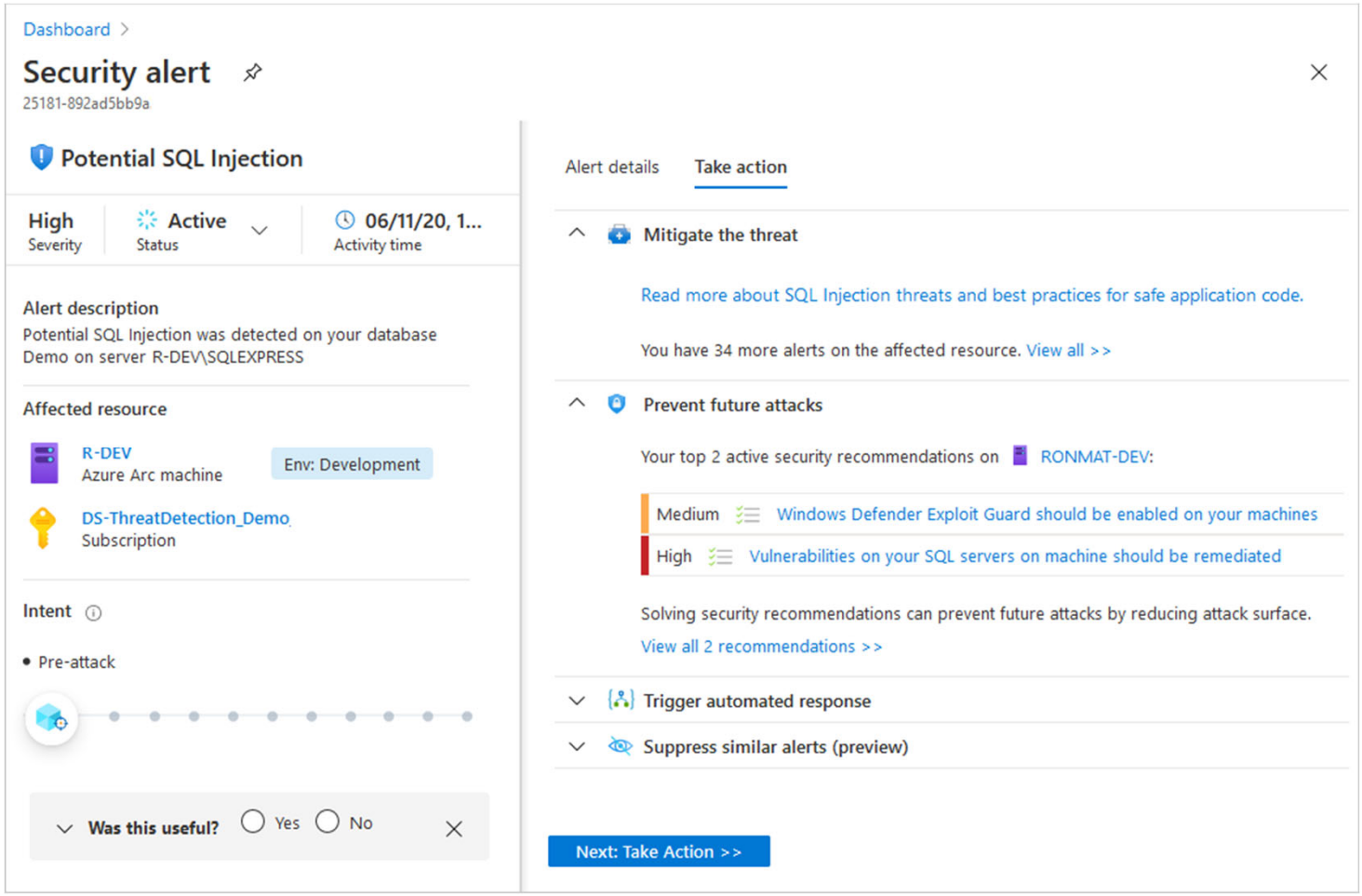
Explain security alerts

- Security alerts and incidents
- Detecting Threats
- Alert classification
- Continuous monitoring and assessments
- Alert types



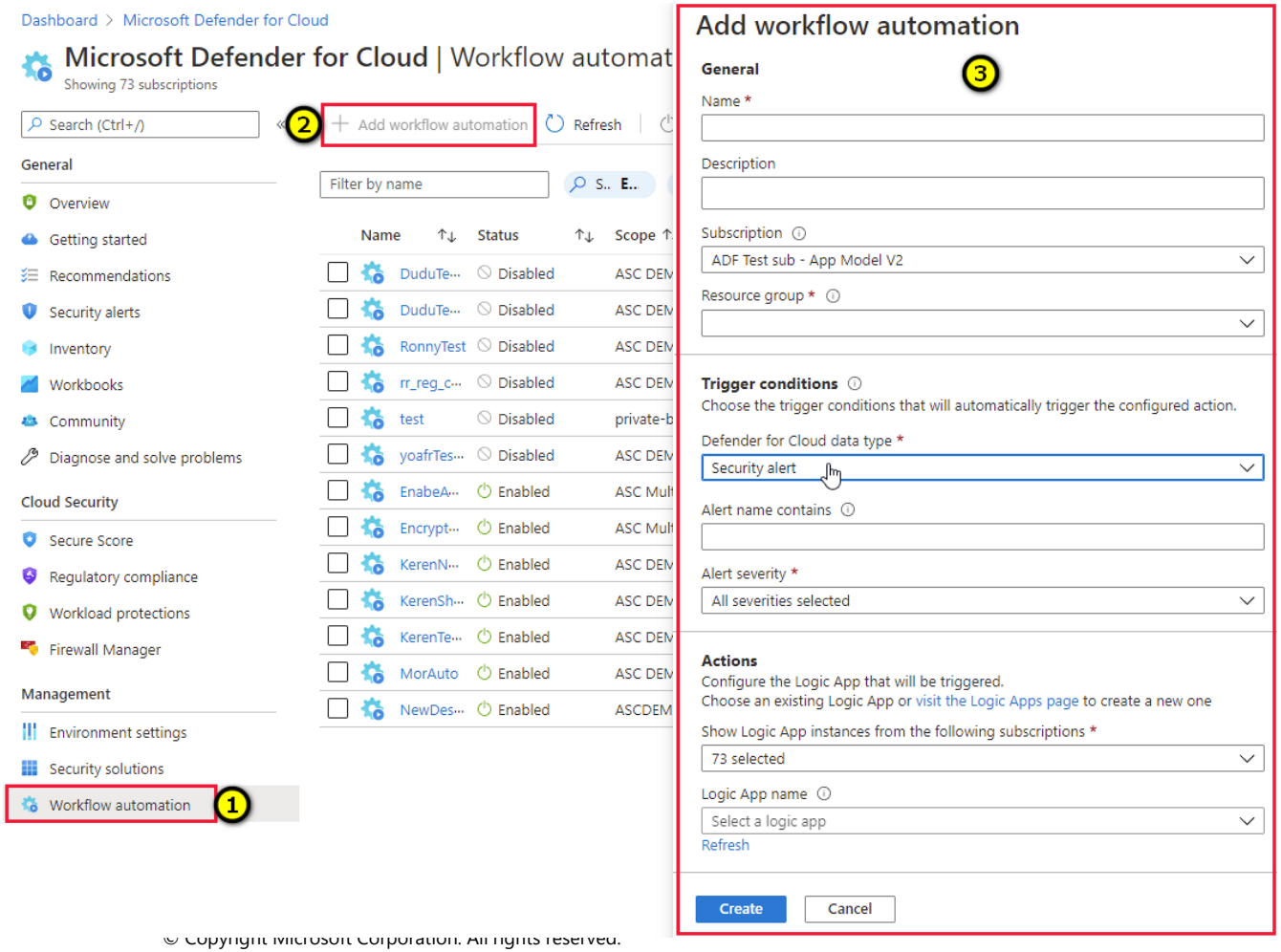
Remediate alerts

Microsoft Defender for Cloud provides actionable tasks to mitigate the threat, prevent future attacks, trigger automated response, suppress similar alerts.



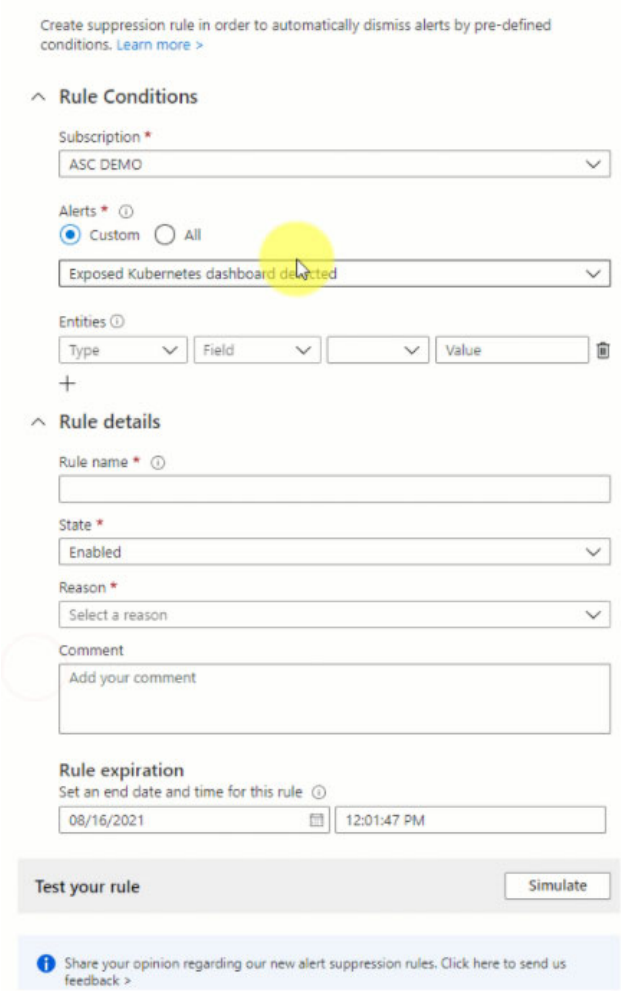
Remediate alerts (continued)

Create a logic app and define when it should automatically run.



Suppress alerts from Microsoft Defender for Cloud

A suppression rule can be useful to suppress alerts that you've identified as false positives or alerts that are being triggered too often to be useful.



Manage threat intelligence reports

Reports include: Activity Group, Campaign, Threat Summary

- Attacker's identity or associations (if this information is available)
- Attackers' objectives
- Current and historical attack campaigns (if this information is available)
- Attackers' tactics, tools, and procedures
- Associated indicators of compromise (IoC) such as URLs and file hashes
- Victimology, which is the industry and geographic prevalence to assist you in determining if your Azure resources are at risk
- Mitigation and remediation information

Respond to alerts from Azure resources

Respond to Microsoft Defender for Key Vault alerts

Respond to Microsoft Defender for DNS alerts

Respond to Microsoft Defender for Resource Manager alerts

Knowledge check

Check your knowledge with the module quiz in your course viewer

Module 3, Lab 01 – Mitigate threats using Microsoft Defender for Cloud

Lab Exercises for module 3

1. Enable Microsoft Defender for Cloud
2. Mitigate threats using Microsoft Defender for Cloud

Microsoft 365