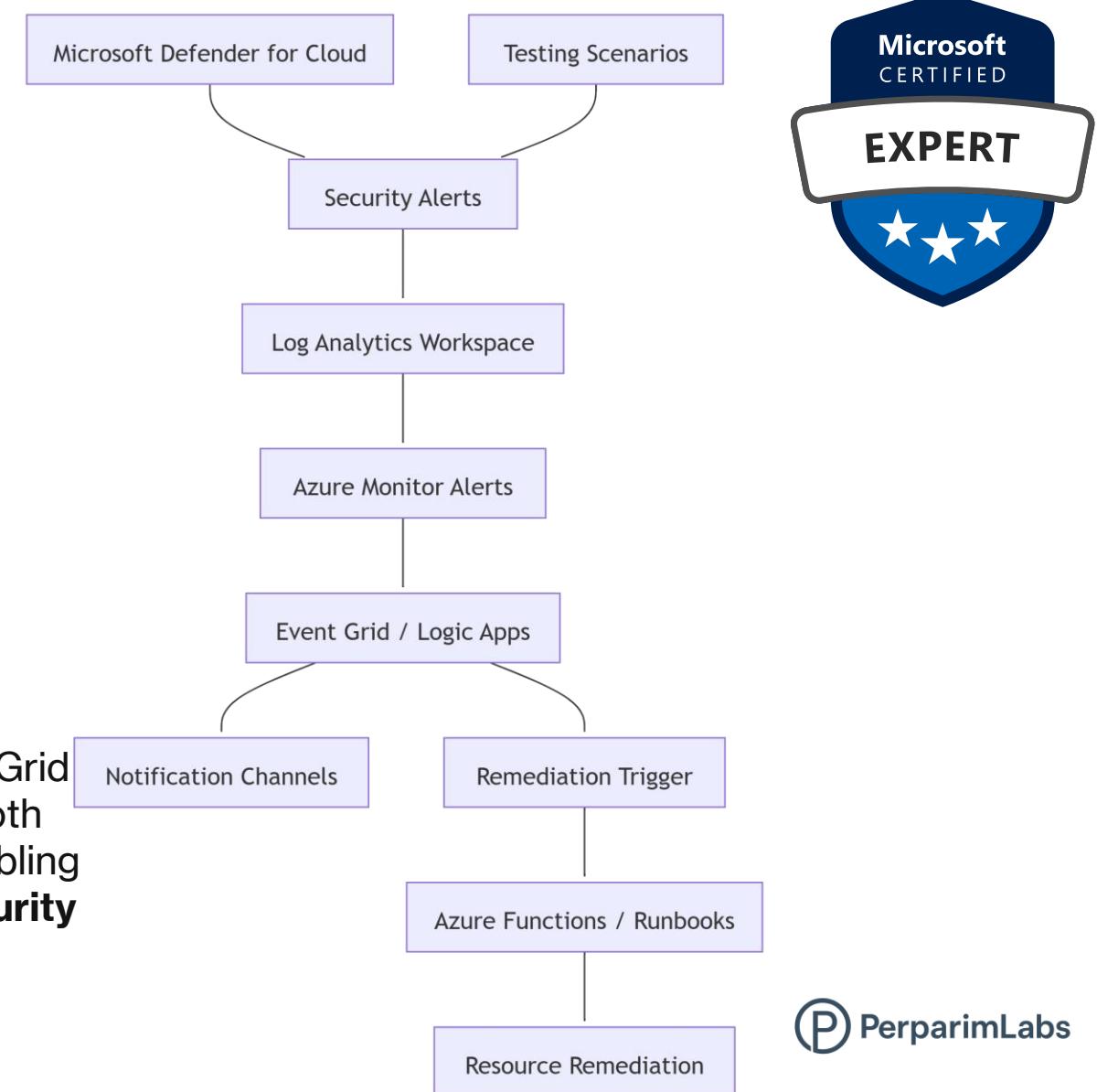


Defender for Cloud Notifications & Testing

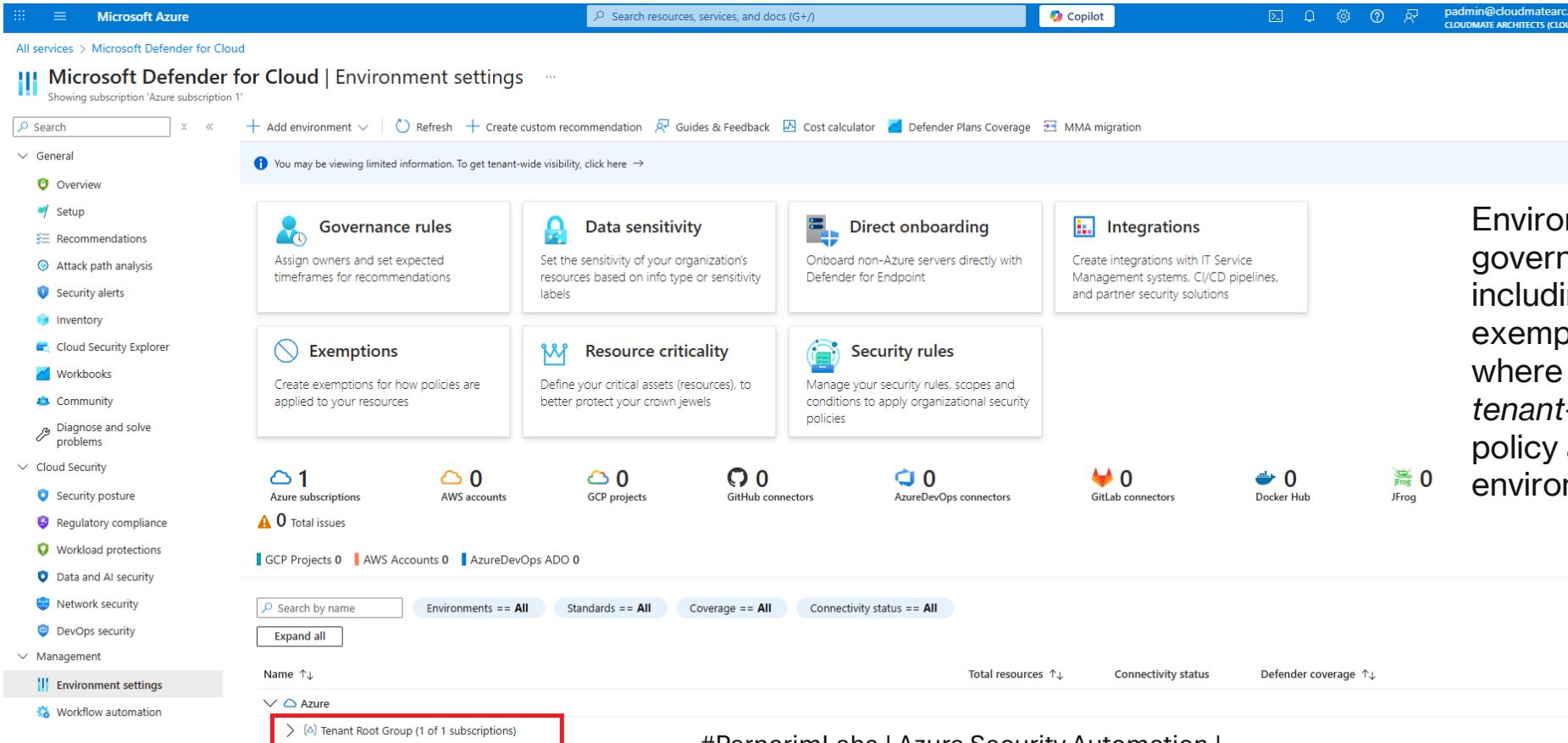
This architecture shows how Microsoft Defender for Cloud integrates with Logic Apps and Azure Monitor to automate alert notifications and remediation actions. Security alerts flow through Log Analytics and Event Grid to trigger Logic Apps, sending notifications or initiating remediation via Azure Functions and runbooks.

Defender for Cloud integrates with Logic Apps via Event Grid events to automate alert handling. This setup supports both *notification-driven* and *remediation-driven* workflows, enabling scalable security operations aligned with the **SOAR (Security Orchestration, Automation, and Response)** model.



Accessing Environment Settings

- Opened the Environment Settings to configure Defender for Cloud management options, including email alerts and automation integrations.



Microsoft Azure

Search resources, services, and docs (G+)

Copilot

padmin@cloudmatearch...

All services > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Environment settings

Showing subscription 'Azure subscription 1'

General

- Overview
- Setup
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Data and AI security
- Network security
- DevOps security

Management

- Environment settings
- Workflow automation

Governance rules
Assign owners and set expected timeframes for recommendations

Data sensitivity
Set the sensitivity of your organization's resources based on info type or sensitivity labels

Direct onboarding
Onboard non-Azure servers directly with Defender for Endpoint

Integrations
Create integrations with IT Service Management systems, CI/CD pipelines, and partner security solutions

Exemptions
Create exemptions for how policies are applied to your resources

Resource criticality
Define your critical assets (resources), to better protect your crown jewels

Security rules
Manage your security rules, scopes and conditions to apply organizational security policies

Azure subscriptions: 1 | AWS accounts: 0 | GCP projects: 0 | GitHub connectors: 0 | AzureDevOps connectors: 0 | GitLab connectors: 0 | Docker Hub: 0 | JFrog: 0

0 Total issues

GCP Projects 0 | AWS Accounts 0 | AzureDevOps ADO 0

Search by name Environments == All Standards == All Coverage == All Connectivity status == All

Expand all

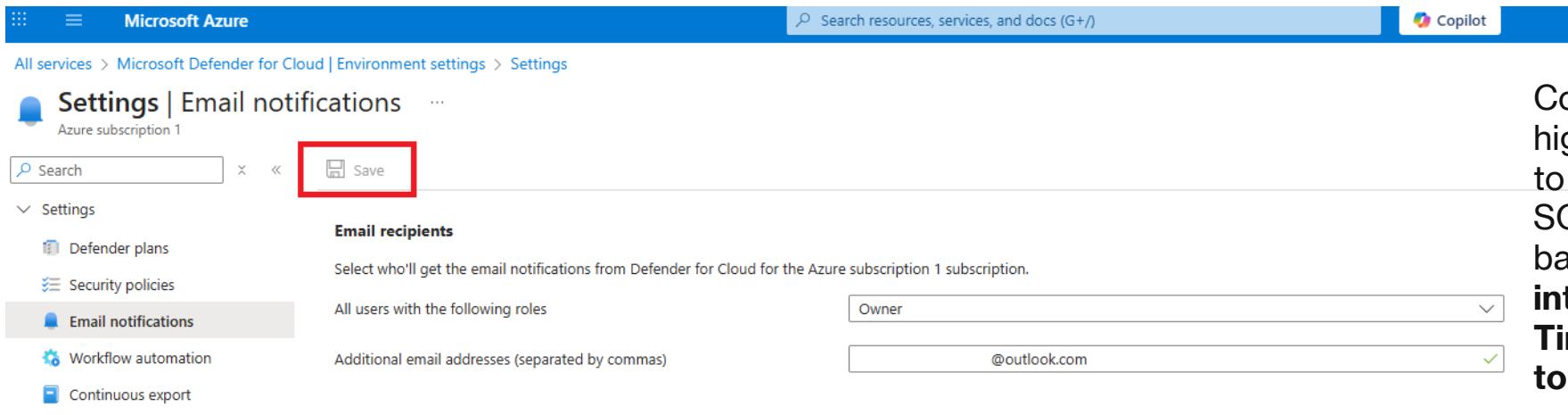
Name ↑ Total resources ↑ Connectivity status ↑ Defender coverage ↑

Cloud Azure Tenant Root Group (1 of 1 subscriptions)

Environment settings centralize governance for Defender for Cloud – including integrations, data sensitivity, exemptions, and security rules. This is where enterprise SOC teams configure *tenant-wide visibility* and ensure consistent policy application across multi-cloud environments.

Configuring Email Notifications

- Enabled email alerts for high-severity and critical attack path notifications to ensure immediate response visibility.



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

All services > Microsoft Defender for Cloud | Environment settings > Settings

Settings | Email notifications

Save

Settings

- Defender plans
- Security policies
- Email notifications**
- Workflow automation
- Continuous export

Email recipients

Select who'll get the email notifications from Defender for Cloud for the Azure subscription 1 subscription.

All users with the following roles

Owner

Additional email addresses (separated by commas)

@outlook.com

Notification types

Use the settings below to select the type of email notifications to be sent by Defender for Cloud.

Notify about alerts with the following severity (or higher):

High

ⓘ You'll receive a maximum of one email per 6 hours for high-severity alerts, one email per 12 hours for medium-severity alerts, and one email per 24 hours for low-severity alerts. [Learn more >](#)

Notify about attack paths with the following risk level (or higher):

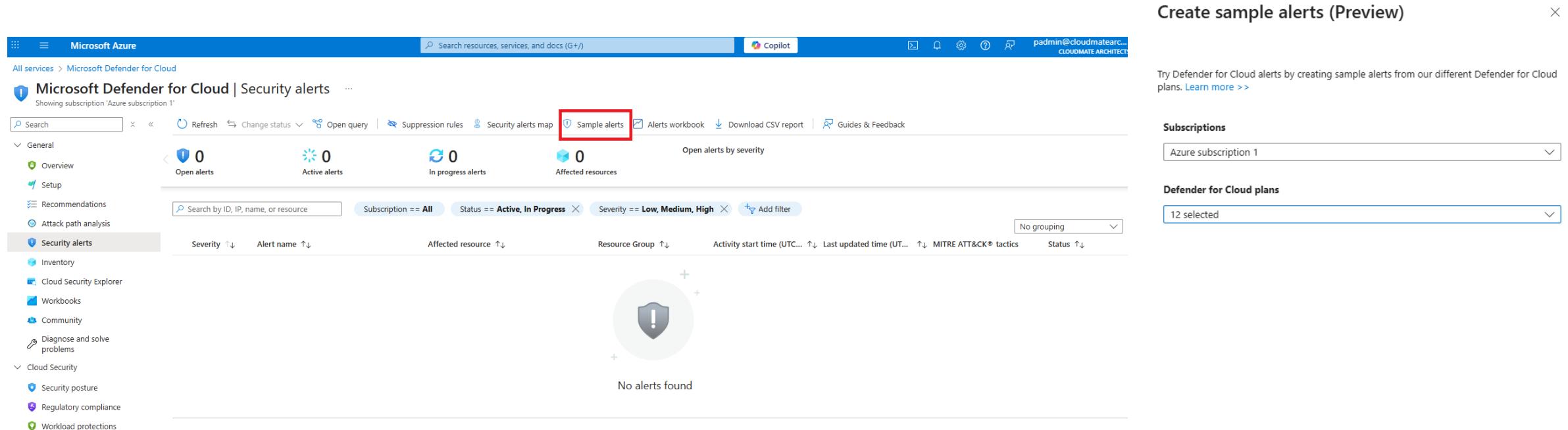
Critical

ⓘ You'll receive a maximum of one email per 30 minutes for attack paths with critical risk-level, one email per 1 hour for attack paths with high risk-level, one email per 2 hours for attack paths with medium risk-level, and 1 email per 3 hours for attack paths with low risk-level

Configuring notifications ensures that high-severity alerts are routed instantly to operational teams. This mirrors real SOC workflows, where email or ticket-based alerting bridges **SIEM + ITSM integration**, improving **MTTD (Mean Time to Detect)** and **MTTR (Mean Time to Respond)**.

Generating Sample Alerts

- Used Defender for Cloud's built-in simulation tool to create sample alerts across Defender plans for testing workflow automation.

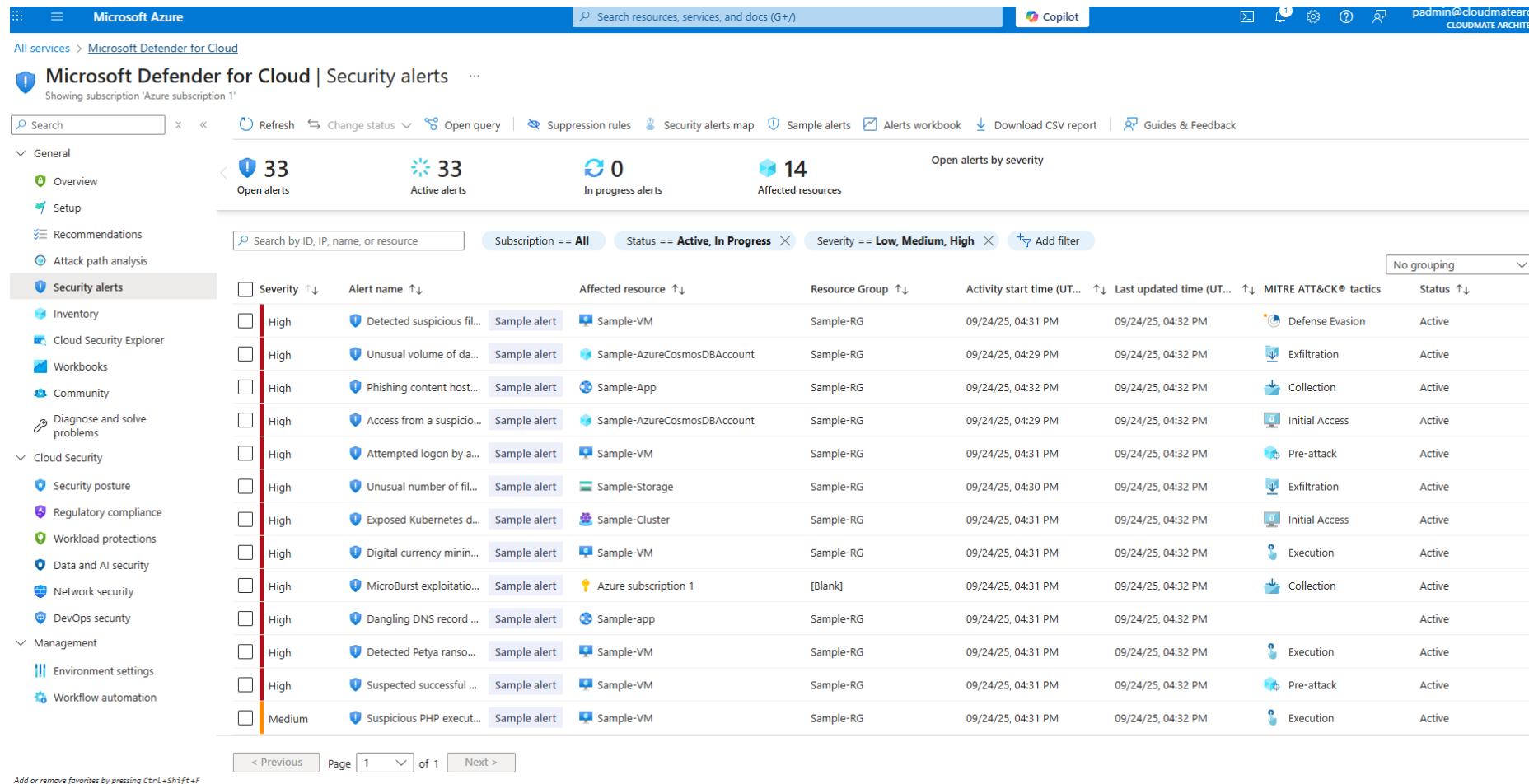


The screenshot shows the Microsoft Defender for Cloud Security alerts interface. The 'Sample alerts' button in the top navigation bar is highlighted with a red box. The main area displays metrics for Open alerts (0), Active alerts (0), In progress alerts (0), and Affected resources (0). Below these are search and filter options, including 'Subscription == All', 'Status == Active, In Progress', 'Severity == Low, Medium, High', and 'Add filter'. The 'Security alerts' section is selected in the sidebar. To the right, a modal titled 'Create sample alerts (Preview)' is open, showing 'Azure subscription 1' in the 'Subscriptions' dropdown and '12 selected' in the 'Defender for Cloud plans' dropdown.

Sample alerts simulate real-world attack vectors such as data exfiltration or suspicious sign-ins. Testing workflows before production ensures your Logic Apps handle real Defender alerts accurately – without impacting actual workloads.

Validating Alerts in Defender for Cloud

- Confirmed sample alerts were generated successfully across multiple Defender plans, covering scenarios like suspicious logons and data exfiltration.



The screenshot shows the Microsoft Defender for Cloud Security alerts page. The left sidebar is collapsed, and the main area displays a table of alerts. The table has the following columns: Severity, Alert name, Affected resource, Resource Group, Activity start time, Last updated time, MITRE ATT&CK® tactics, and Status. The table lists 14 sample alerts, all of which are High severity and Active. The alerts are categorized by tactic: Defense Evasion, Exfiltration, Collection, Initial Access, Pre-attack, and Execution. The affected resources include Sample-VM, Sample-AzureCosmosDBAccount, Sample-App, Sample-AzureCosmosDBAccount, Sample-VM, Sample-Storage, Sample-Cluster, Sample-VM, Azure subscription 1, Sample-app, Sample-RG, Sample-RG, Sample-RG, and Sample-RG. The activity start time and last updated time are all 09/24/25, 04:31 PM or 04:32 PM. The MITRE ATT&CK® tactics are Defense Evasion, Exfiltration, Collection, Initial Access, Pre-attack, and Execution respectively. The status for all alerts is Active.

Severity	Alert name	Affected resource	Resource Group	Activity start time (UT...)	Last updated time (UT...)	MITRE ATT&CK® tactics	Status
High	Detected suspicious fil...	Sample alert Sample-VM	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Defense Evasion	Active
High	Unusual volume of da...	Sample alert Sample-AzureCosmosDBAccount	Sample-RG	09/24/25, 04:29 PM	09/24/25, 04:32 PM	Exfiltration	Active
High	Phishing content host...	Sample alert Sample-App	Sample-RG	09/24/25, 04:32 PM	09/24/25, 04:32 PM	Collection	Active
High	Access from a suspicio...	Sample alert Sample-AzureCosmosDBAccount	Sample-RG	09/24/25, 04:29 PM	09/24/25, 04:32 PM	Initial Access	Active
High	Attempted logon by a...	Sample alert Sample-VM	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Pre-attack	Active
High	Unusual number of fil...	Sample alert Sample-Storage	Sample-RG	09/24/25, 04:30 PM	09/24/25, 04:32 PM	Exfiltration	Active
High	Exposed Kubernetes d...	Sample alert Sample-Cluster	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Initial Access	Active
High	Digital currency minin...	Sample alert Sample-VM	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Execution	Active
High	MicroBurst exploitatio...	Sample alert Azure subscription 1	[Blank]	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Collection	Active
High	Dangling DNS record ...	Sample alert Sample-app	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM		Active
High	Detected Petya ranso...	Sample alert Sample-VM	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Execution	Active
High	Suspected successfu...	Sample alert Sample-VM	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Pre-attack	Active
Medium	Suspicious PHP execut...	Sample alert Sample-VM	Sample-RG	09/24/25, 04:31 PM	09/24/25, 04:32 PM	Execution	Active

Each sample alert maps to the **MITRE ATT&CK** framework (e.g., Initial Access, Exfiltration, Defense Evasion). This helps correlate automated responses with the attack kill chain, strengthening incident response maturity.

Email Notification Confirmation

- Received confirmation that Azure Logic Apps connected successfully with Microsoft 365 – validating automation end-to-end.

New app(s) connected to your Microsoft account

Microsoft account team < .microsoft.com >
To: You
MT

Getting too much email?

Microsoft account

New app(s) have access to your data

Azure Logic Apps (Canada Central) connected to the Microsoft account [@outlook.com](#).

If you didn't grant this access, please remove the app(s) from your account.

[Manage your apps](#)

You can also [opt out](#) or change where you receive security notifications.

Thanks,
The Microsoft account team

[Privacy Statement](#)

Microsoft Corporation,

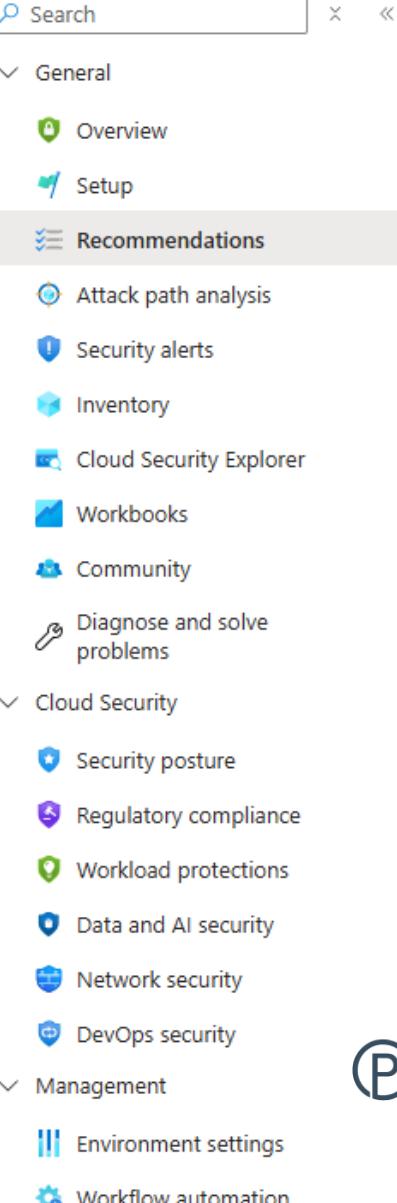
[Reply](#) [Forward](#)

Logic Apps rely on Microsoft Graph API and OAuth connections to send automated emails through Outlook. This validates secure, delegated access using **least privilege** principles for automation accounts.

Reviewing Security Recommendations

- Opened active recommendations under Defender for Cloud to examine detected misconfigurations and risk areas.

Defender for Cloud's *Recommendations* blade prioritizes risks using a Secure Score model. Reviewing these helps architects balance compliance and security posture improvement across hybrid environments.

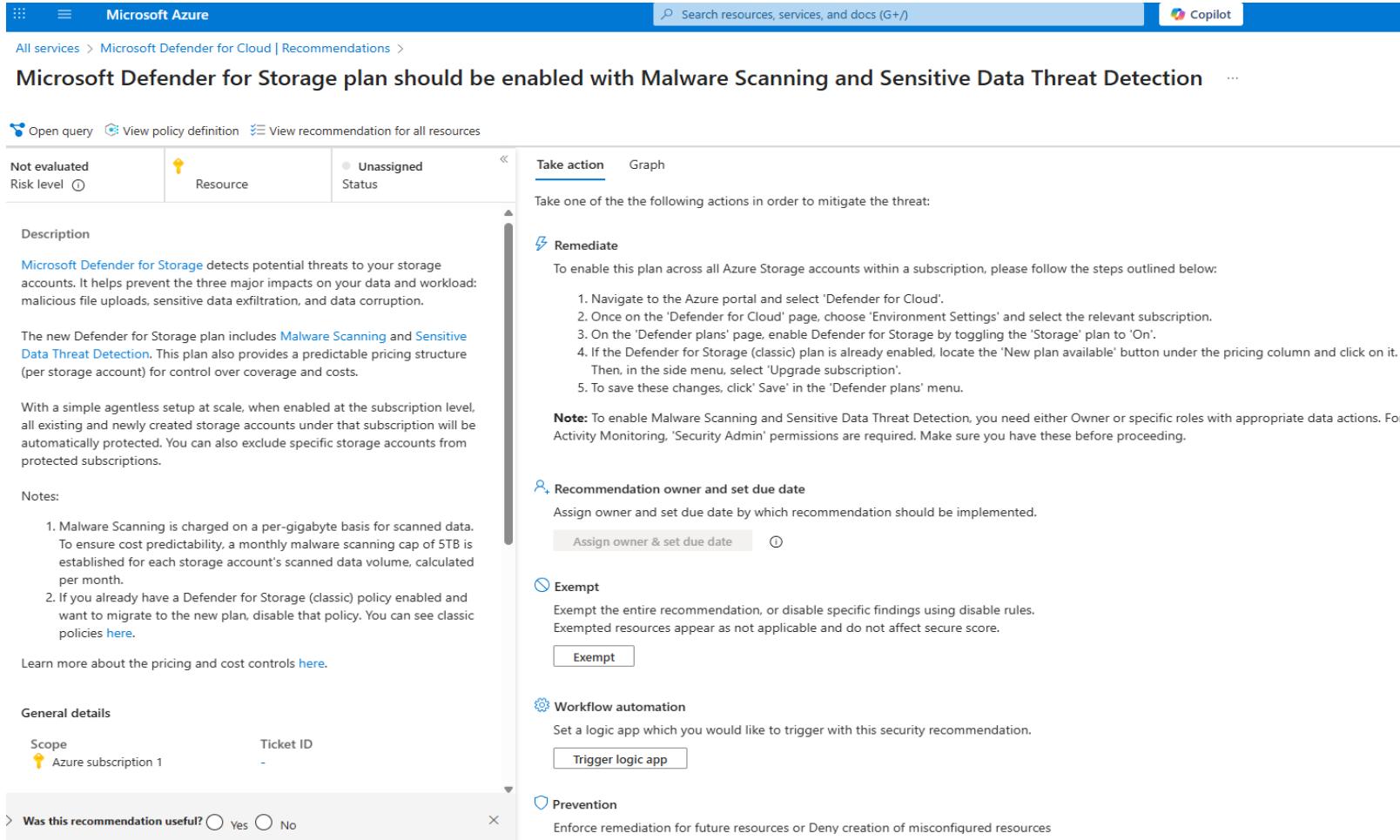


The screenshot shows the Microsoft Defender for Cloud interface with the 'Recommendations' blade selected. The left sidebar includes sections for General, Cloud Security, and Management, each with sub-options like Overview, Setup, and specific security categories. The 'Recommendations' section is highlighted with a gray background.

- General
 - Overview
 - Setup
 - Recommendations (selected)
 - Attack path analysis
 - Security alerts
 - Inventory
 - Cloud Security Explorer
 - Workbooks
 - Community
 - Diagnose and solve problems
- Cloud Security
 - Security posture
 - Regulatory compliance
 - Workload protections
 - Data and AI security
 - Network security
 - DevOps security
- Management
 - Environment settings
 - Workflow automation

Remediation Guidance

- Reviewed Defender's remediation guidance to resolve detected risks – like enabling Malware Scanning and Sensitive Data Threat Detection.



The screenshot shows a Microsoft Azure page for 'Microsoft Defender for Storage plan should be enabled with Malware Scanning and Sensitive Data Threat Detection'. The page includes a navigation bar with 'Microsoft Azure', a search bar, and a Copilot button. The main content area has a title 'Microsoft Defender for Storage plan should be enabled with Malware Scanning and Sensitive Data Threat Detection' with a '... more' link. Below the title are buttons for 'Open query', 'View policy definition', and 'View recommendation for all resources'. A table shows 'Not evaluated' status for a 'Resource' with 'Unassigned Status'. The 'Description' section details the threat of potential threats to storage accounts and the benefits of the new Defender for Storage plan. It also notes that the plan includes Malware Scanning and Sensitive Data Threat Detection. The 'Notes' section provides information about cost predictability and migration from classic policies. The 'Take action' tab is selected, showing steps to remediate the issue, a note about required permissions, and sections for 'Recommendation owner and set due date', 'Exempt', 'Workflow automation', and 'Prevention'. A footer at the bottom asks if the recommendation was useful, with 'Yes' and 'No' options. The 'General details' section shows 'Scope: Azure subscription 1' and 'Ticket ID: -'. A feedback section at the bottom asks if the recommendation was useful, with 'Yes' and 'No' options.

Automated remediation guidance bridges visibility and action – ensuring identified misconfigurations (like disabled malware scanning or missing threat detection) are resolved through scripted playbooks or policies.

Result & Cleanup

Automation loops like this form the foundation for **continuous cloud hardening**. They reduce manual investigation, eliminate repetitive alert handling, and align with the **Zero Trust principle: Assume Breach**.



Successfully verified automation loop (alert → email → remediation).
Cleaned up Logic App, sample alerts, and test resources.



Microsoft Defender for Cloud's automation with Logic Apps enables proactive detection, instant alerting, and guided remediation. This integration builds a foundation for intelligent, automated incident response across hybrid environments.