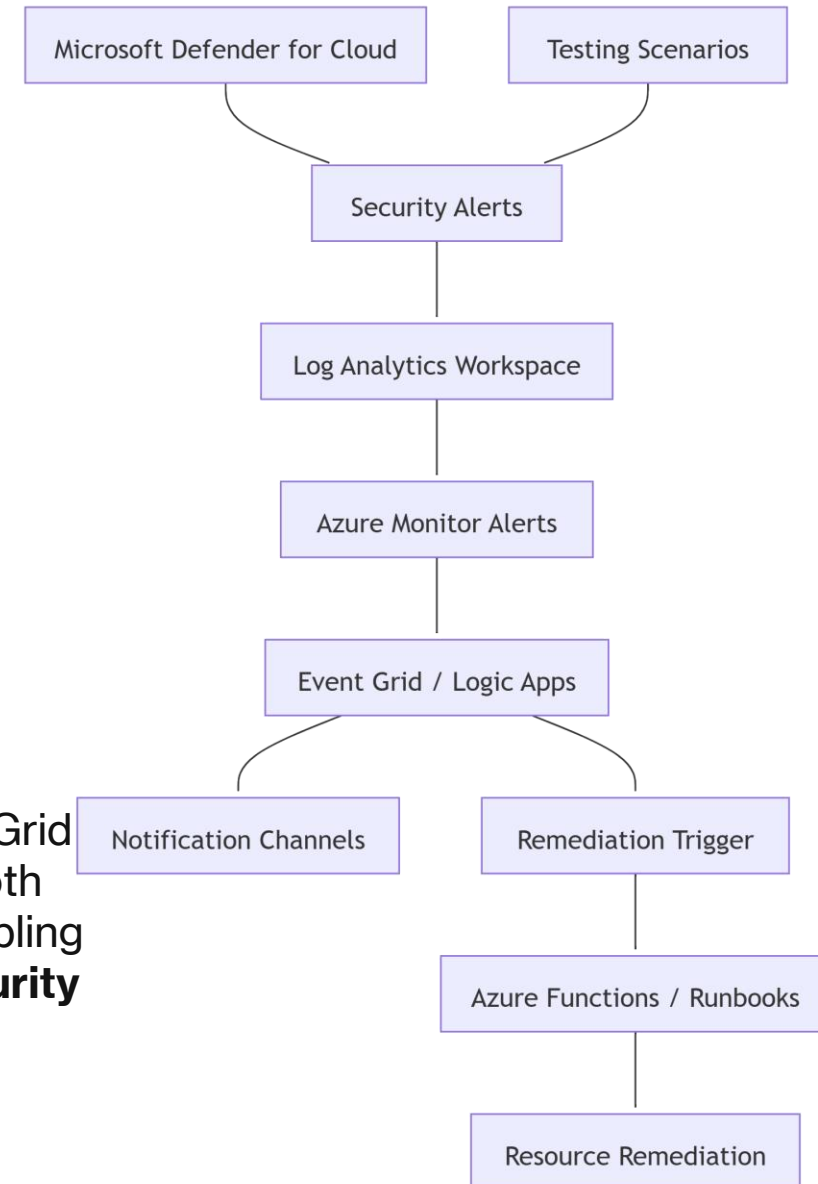


# Defender for Cloud Notifications & Testing

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.

The screenshot shows the Microsoft Defender for Cloud 'Environment settings' page. The left sidebar contains a navigation menu with categories like General, Cloud Security, and Management. The main area displays various configuration tiles such as Governance rules, Data sensitivity, Direct onboarding, Integrations, Exemptions, Resource criticality, and Security rules. Below these tiles is a summary section showing counts for Azure subscriptions (1), AWS accounts (0), GCP projects (0), and other connectors. At the bottom, a table lists environments, with the 'Tenant Root Group (1 of 1 subscriptions)' highlighted by a red box.

Microsoft Azure

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

Copilot

admin@cloudmatearc...  
CLOUDMATE ARCHITECTS (CLOU)

All services > Microsoft Defender for Cloud

## Microsoft Defender for Cloud | Environment settings

Showing subscription 'Azure subscription 1'

Search

+ Add environment | Refresh | + Create custom recommendation | Guides & Feedback | Cost calculator | Defender Plans Coverage | MMA migration

**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

**Summary:**

- 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

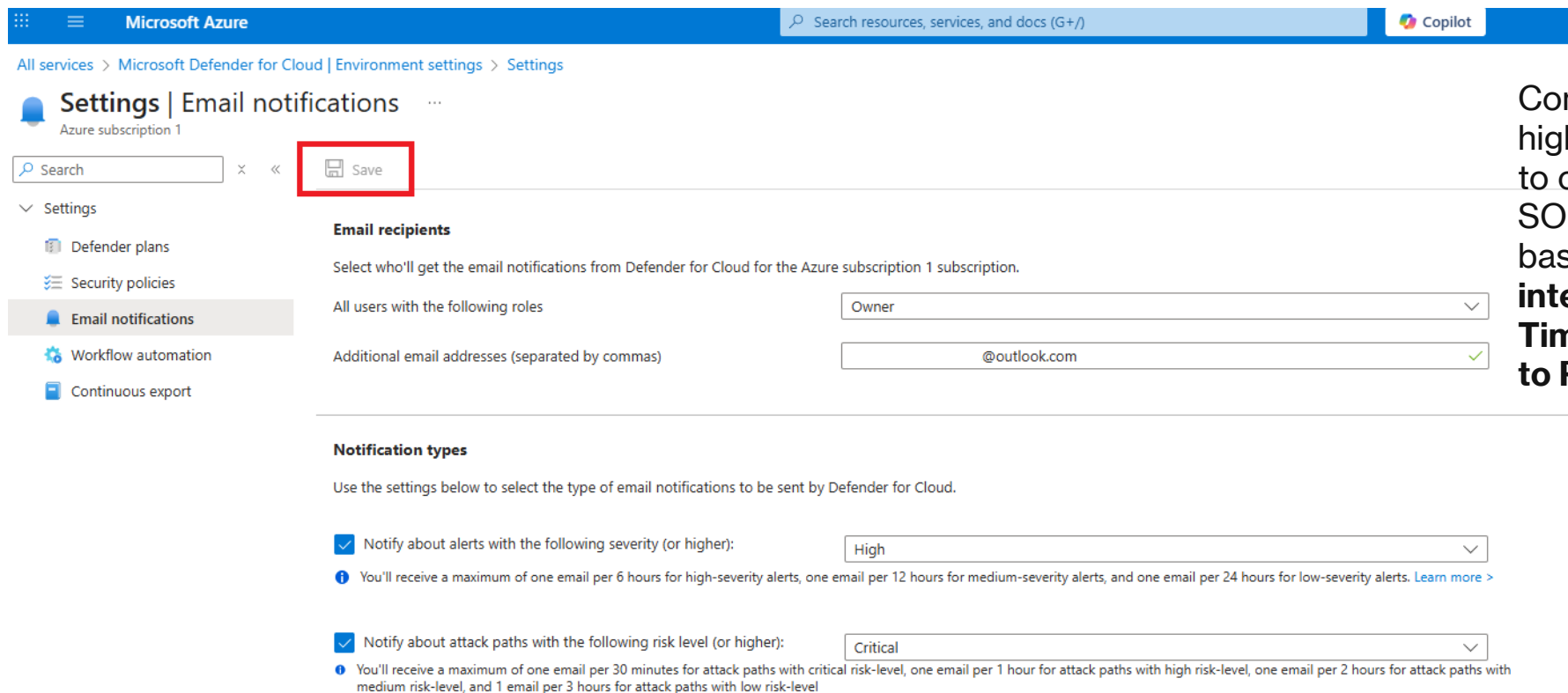
Expand all

Name ↑↓	Total resources ↑↓	Connectivity status	Defender coverage ↑↓
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.

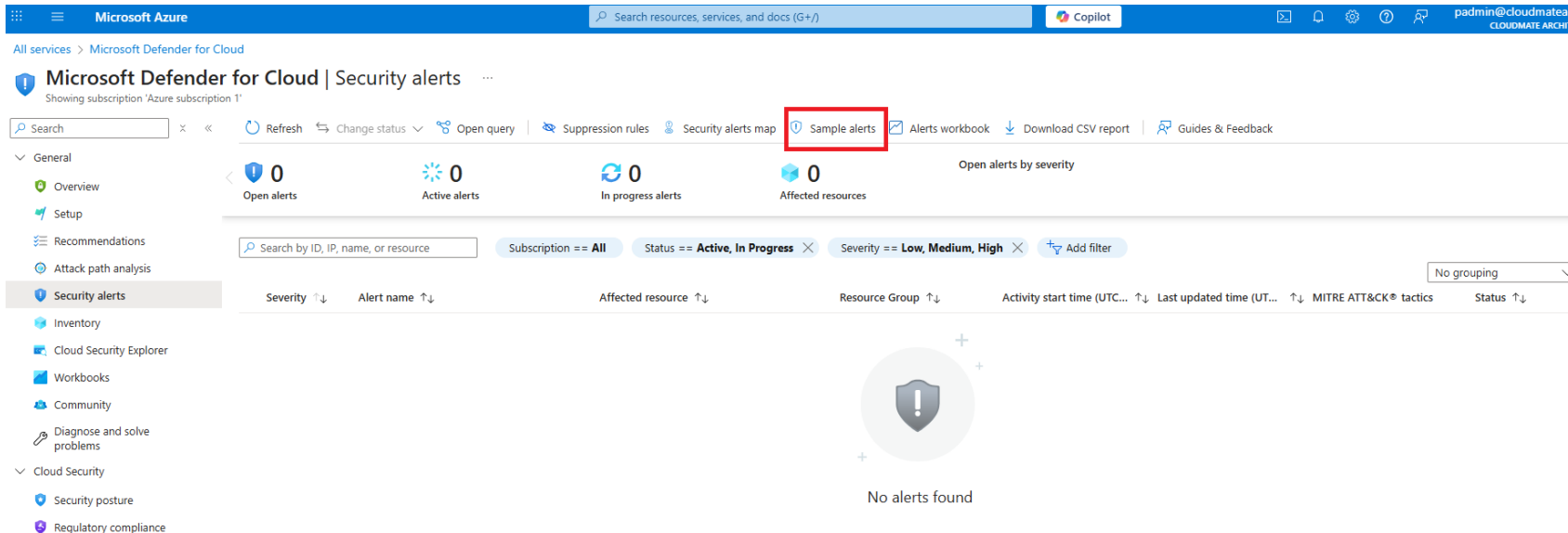


The screenshot shows the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. Below the navigation bar, the breadcrumb trail reads: All services > Microsoft Defender for Cloud | Environment settings > Settings. The main heading is 'Settings | Email notifications' for 'Azure subscription 1'. A search bar is present, and a 'Save' button is highlighted with a red box. The left sidebar shows a list of settings: Settings (expanded), Defender plans, Security policies, Email notifications (selected), Workflow automation, and Continuous export. The main content area is divided into two sections: 'Email recipients' and 'Notification types'. In the 'Email recipients' section, there is a description: 'Select who'll get the email notifications from Defender for Cloud for the Azure subscription 1 subscription.' Below this, there are two fields: 'All users with the following roles' with a dropdown menu set to 'Owner', and 'Additional email addresses (separated by commas)' with a text input field containing '@outlook.com' and a green checkmark. The 'Notification types' section has a description: 'Use the settings below to select the type of email notifications to be sent by Defender for Cloud.' It contains two checked checkboxes. The first checkbox is 'Notify about alerts with the following severity (or higher):' with a dropdown menu set to 'High'. Below it is a blue information icon followed by the text: '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 >](#)'. The second checkbox is 'Notify about attack paths with the following risk level (or higher):' with a dropdown menu set to 'Critical'. Below it is a blue information icon followed by the text: '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.



Microsoft Azure

Search resources, services, and docs (G+)

Copilot

admin@cloudmatearc...  
CLOUDMATE ARCHITECT

All services > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Security alerts

Showing subscription 'Azure subscription 1'

Search

Refresh Change status Open query Suppression rules Security alerts map **Sample alerts** Alerts workbook Download CSV report Guides & Feedback

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

Open alerts 0 Active alerts 0 In progress alerts 0 Affected resources 0

Open alerts by severity

Search by ID, IP, name, or resource

Subscription == All Status == Active, In Progress Severity == Low, Medium, High Add filter

No grouping

Severity Alert name Affected resource Resource Group Activity start time (UTC... Last updated time (UTC... MITRE ATT&CK® tactics Status

No alerts found

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.

## Create sample alerts (Preview)

Try Defender for Cloud alerts by creating sample alerts from our different Defender for Cloud plans. [Learn more >>](#)

### Subscriptions

Azure subscription 1

### Defender for Cloud plans

12 selected

Create sample alerts

# Validating Alerts in Defender for Cloud

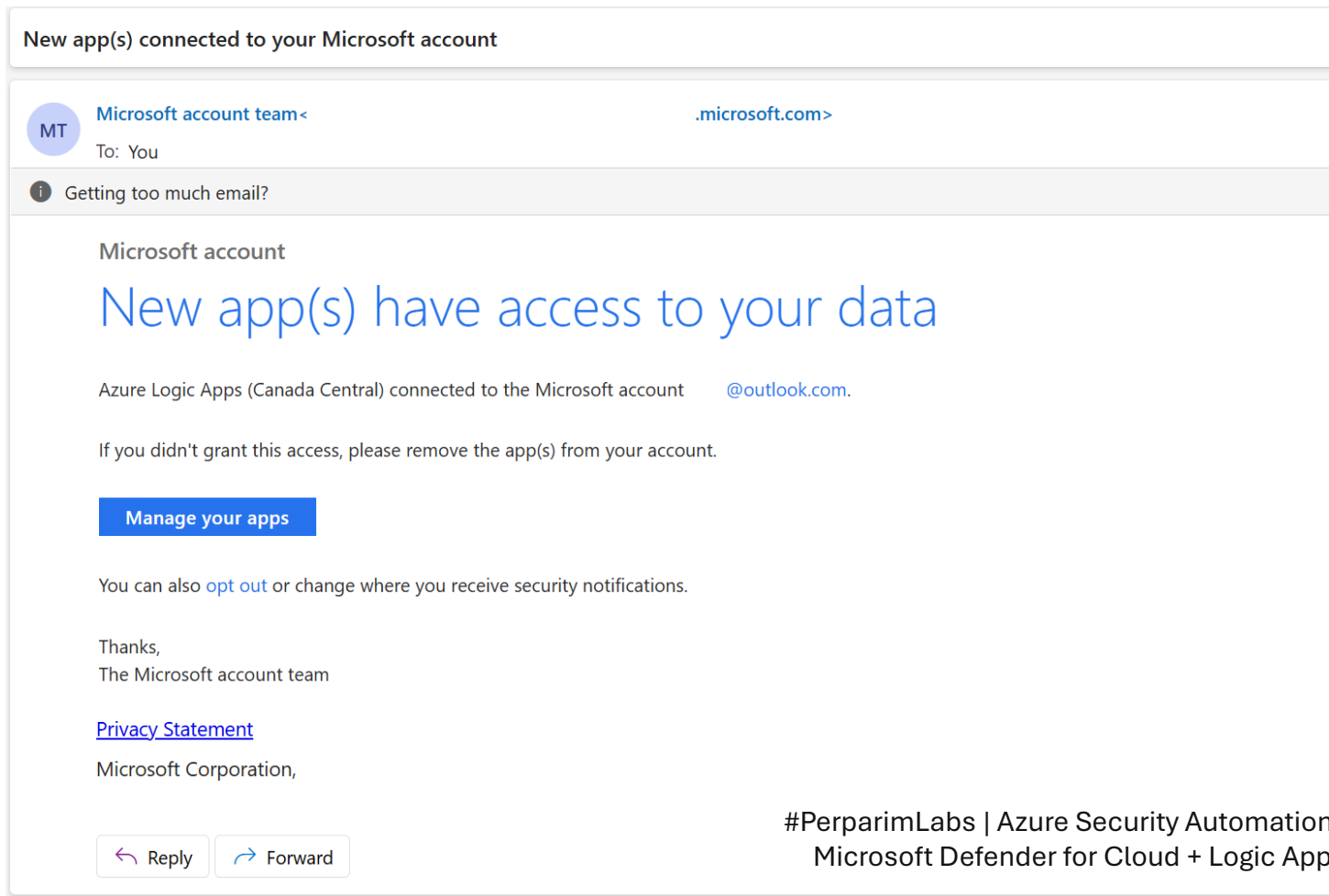
- Confirmed sample alerts were generated successfully across multiple Defender plans, covering scenarios like suspicious logons and data exfiltration.

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 successful ...	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.

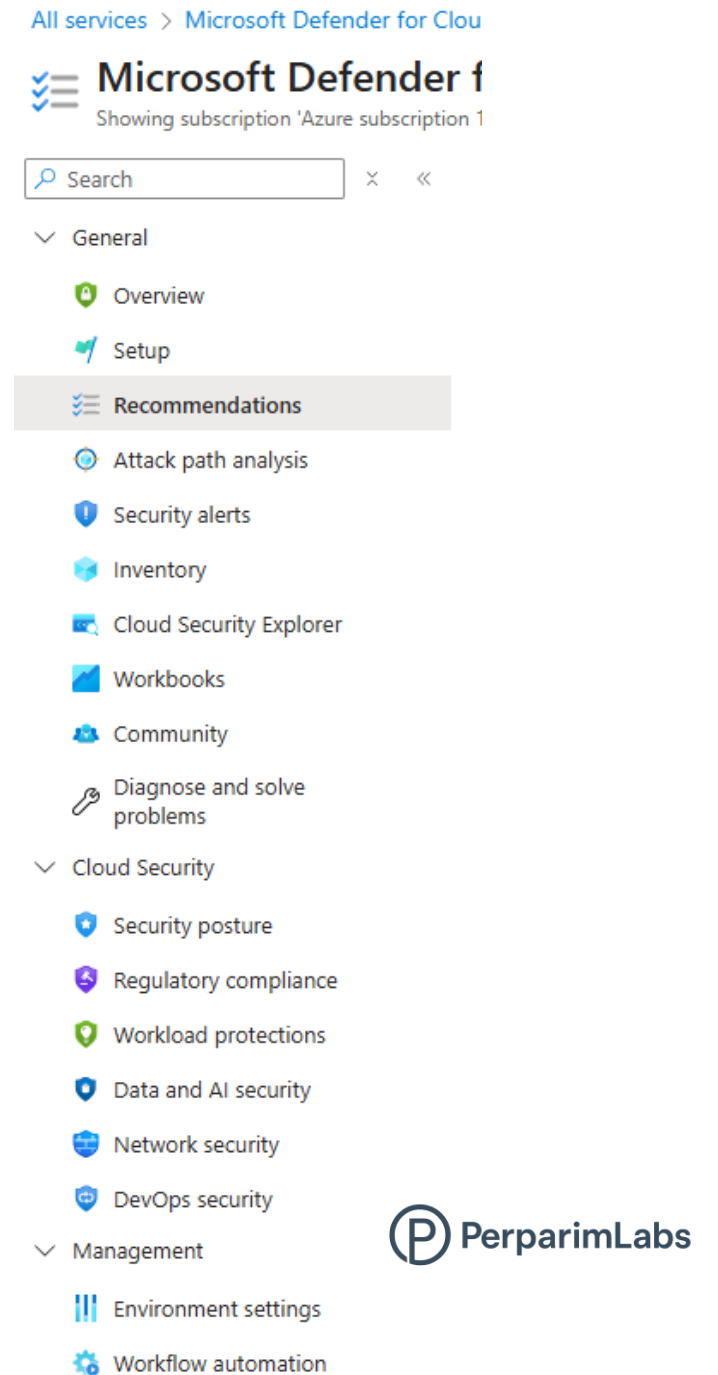


Logic Apps rely on Microsoft Graph API and OAuth connections to send automated emails through Outlook. This validates secure, delegated access using **least privilege** principles for automation accounts.

# 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.



# Remediation Guidance

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

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. Below the navigation bar, the breadcrumb trail reads: All services > Microsoft Defender for Cloud | Recommendations >. The main heading is "Microsoft Defender for Storage plan should be enabled with Malware Scanning and Sensitive Data Threat Detection". Below this, there are three tabs: "Open query", "View policy definition", and "View recommendation for all resources". The left sidebar shows a table with columns for "Not evaluated", "Risk level", "Resource", and "Unassigned Status". The main content area is divided into two sections: "Description" and "Take action". The "Description" section explains that Microsoft Defender for Storage detects potential threats to storage accounts and helps prevent malicious file uploads, sensitive data exfiltration, and data corruption. It also mentions that the new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. The "Take action" section provides a "Remediate" button and a list of steps to follow to enable the plan across all Azure Storage accounts within a subscription. The steps include navigating to the Azure portal, selecting 'Defender for Cloud', choosing 'Environment Settings', enabling the 'Storage' plan, and saving the changes. A note indicates that to enable Malware Scanning and Sensitive Data Threat Detection, you need either Owner or specific roles with appropriate data actions. Below the "Remediate" section, there are options to "Recommendation owner and set due date", "Exempt", "Workflow automation", and "Prevention".

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

All services > Microsoft Defender for Cloud | Recommendations >

Microsoft Defender for Storage plan should be enabled with Malware Scanning and Sensitive Data Threat Detection

Open query View policy definition View recommendation for all resources

Not evaluated  
Risk level

Resource

Unassigned  
Status

Description

Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption.

The new Defender for Storage plan includes [Malware Scanning](#) and [Sensitive Data Threat Detection](#). This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.

With a simple agentless setup at scale, when enabled at the subscription level, all existing and newly created storage accounts under that subscription will be automatically protected. You can also exclude specific storage accounts from protected subscriptions.

Notes:

1. Malware Scanning is charged on a per-gigabyte basis for scanned data. To ensure cost predictability, a monthly malware scanning cap of 5TB is established for each storage account's scanned data volume, calculated per month.
2. If you already have a Defender for Storage (classic) policy enabled and want to migrate to the new plan, disable that policy. You can see classic policies [here](#).

Learn more about the pricing and cost controls [here](#).

General details

Scope  
Azure subscription 1

Ticket ID  
-

Was this recommendation useful? ☐ Yes ☐ No

Take action Graph

Take one of the the following actions in order to mitigate the threat:

Remediate

To enable this plan across all Azure Storage accounts within a subscription, please follow the steps outlined below:

1. Navigate to the Azure portal and select 'Defender for Cloud'.
2. Once on the 'Defender for Cloud' page, choose 'Environment Settings' and select the relevant subscription.
3. On the 'Defender plans' page, enable Defender for Storage by toggling the 'Storage' plan to 'On'.
4. If the Defender for Storage (classic) plan is already enabled, locate the 'New plan available' button under the pricing column and click on it. Then, in the side menu, select 'Upgrade subscription'.
5. To save these changes, click 'Save' in the 'Defender plans' menu.

**Note:** To enable Malware Scanning and Sensitive Data Threat Detection, you need either Owner or specific roles with appropriate data actions. For Activity Monitoring, 'Security Admin' permissions are required. Make sure you have these before proceeding.

Recommendation owner and set due date

Assign owner and set due date by which recommendation should be implemented.

Assign owner & set due date

Exempt

Exempt the entire recommendation, or disable specific findings using disable rules. Exempted resources appear as not applicable and do not affect secure score.

Exempt

Workflow automation

Set a logic app which you would like to trigger with this security recommendation.

Trigger logic app

Prevention

Enforce remediation for future resources or Deny creation of misconfigured resources

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.