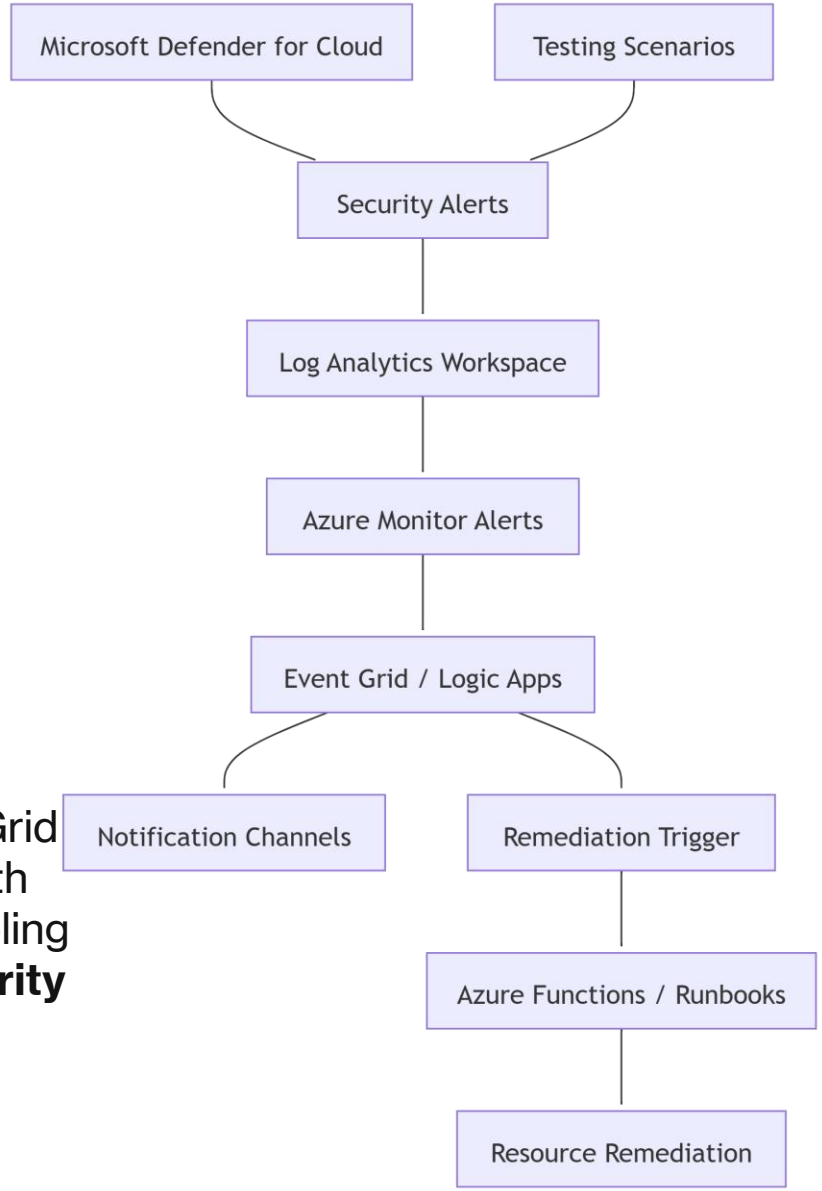
Defender for Cloud Notifications & Testing

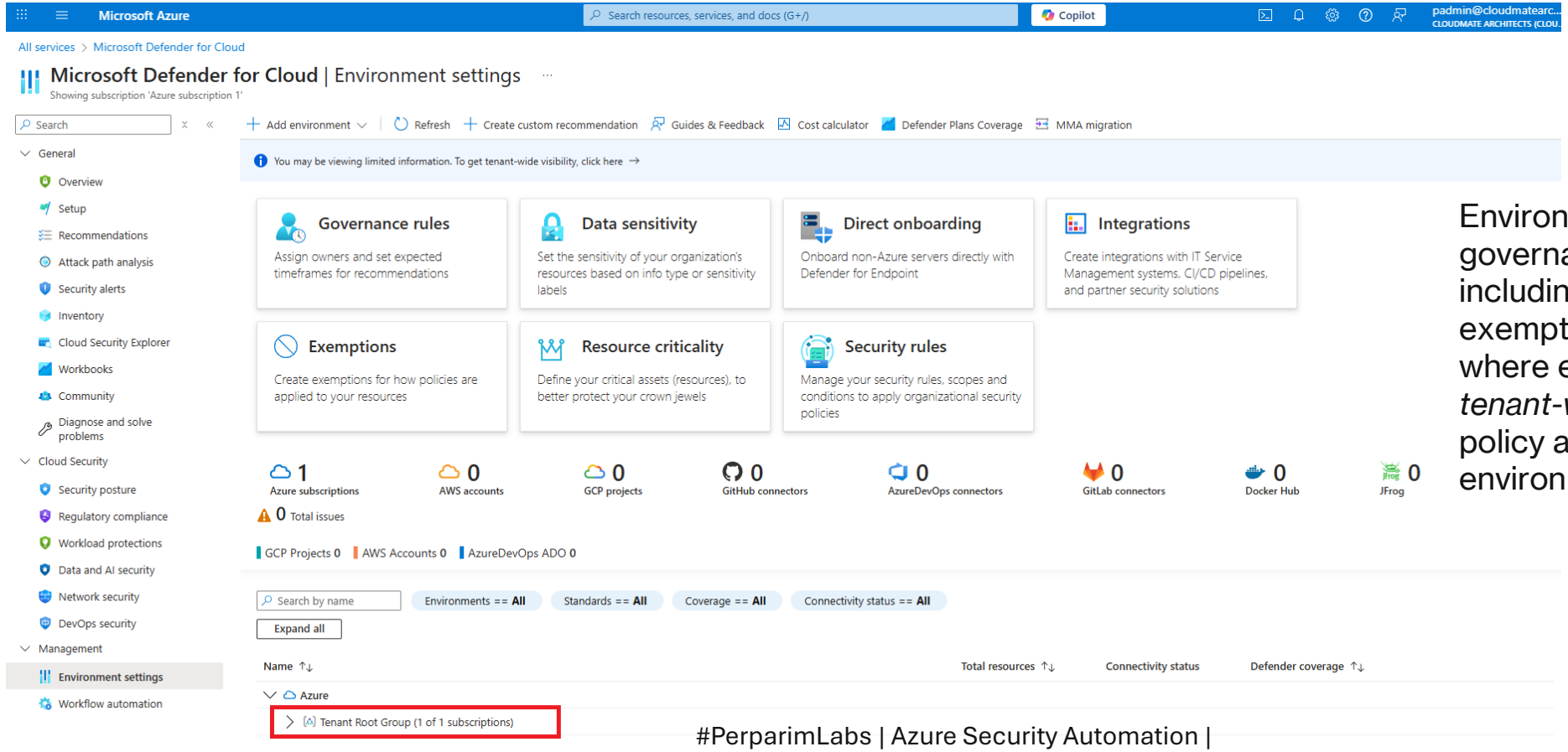


This architecture shows how Microsoft Defender for Cloud integrates with Logic Apps and Azure Monitor to automate alert notifications and remediation actions. Security alerts flow through Log Analytics and Event Grid to trigger Logic Apps, sending notifications or initiating remediation via Azure Functions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

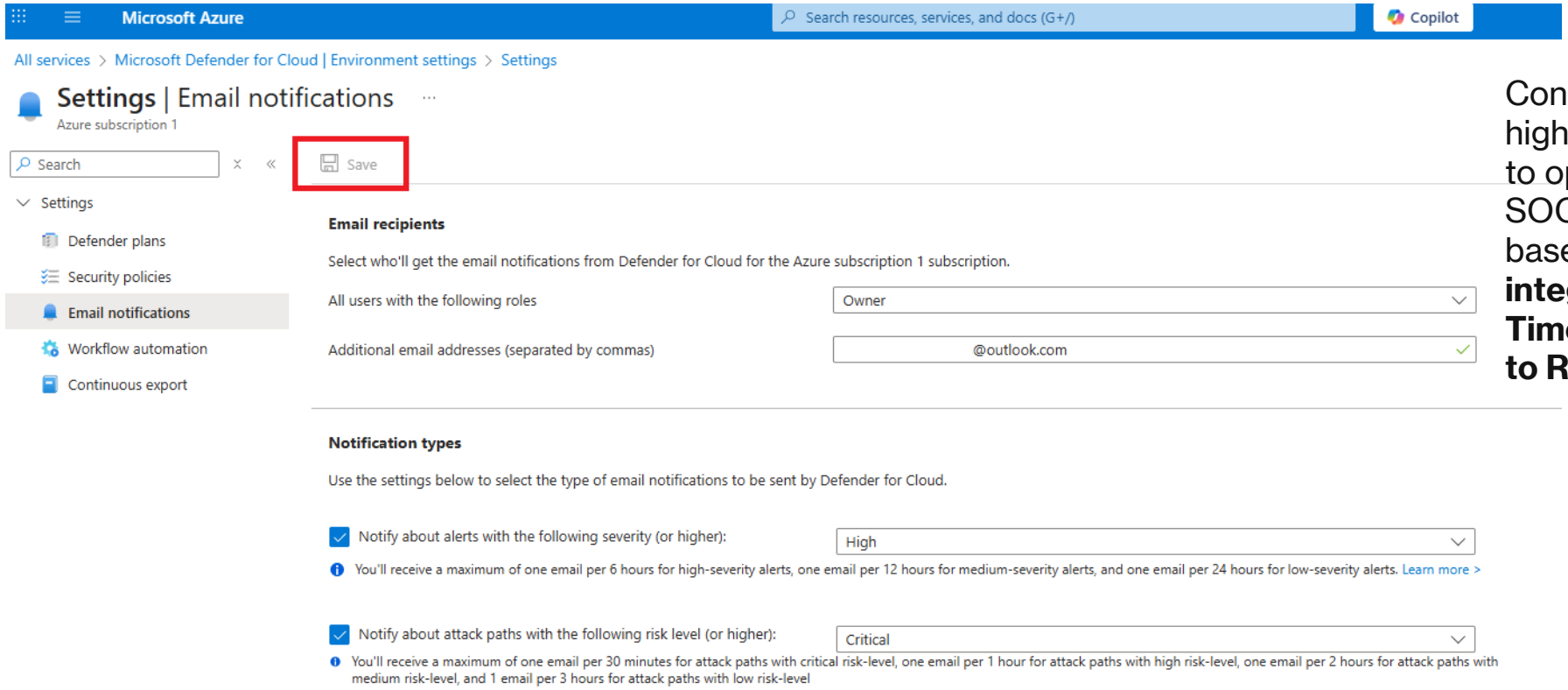


Environment settings centralize governance for Defender for Cloud – including integrations, data sensitivity, exemptions, and security rules. This is where enterprise SOC teams configure *tenant-wide visibility* and ensure consistent policy application across multi-cloud environments.

PerparimLabs

Configuring Email Notifications

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

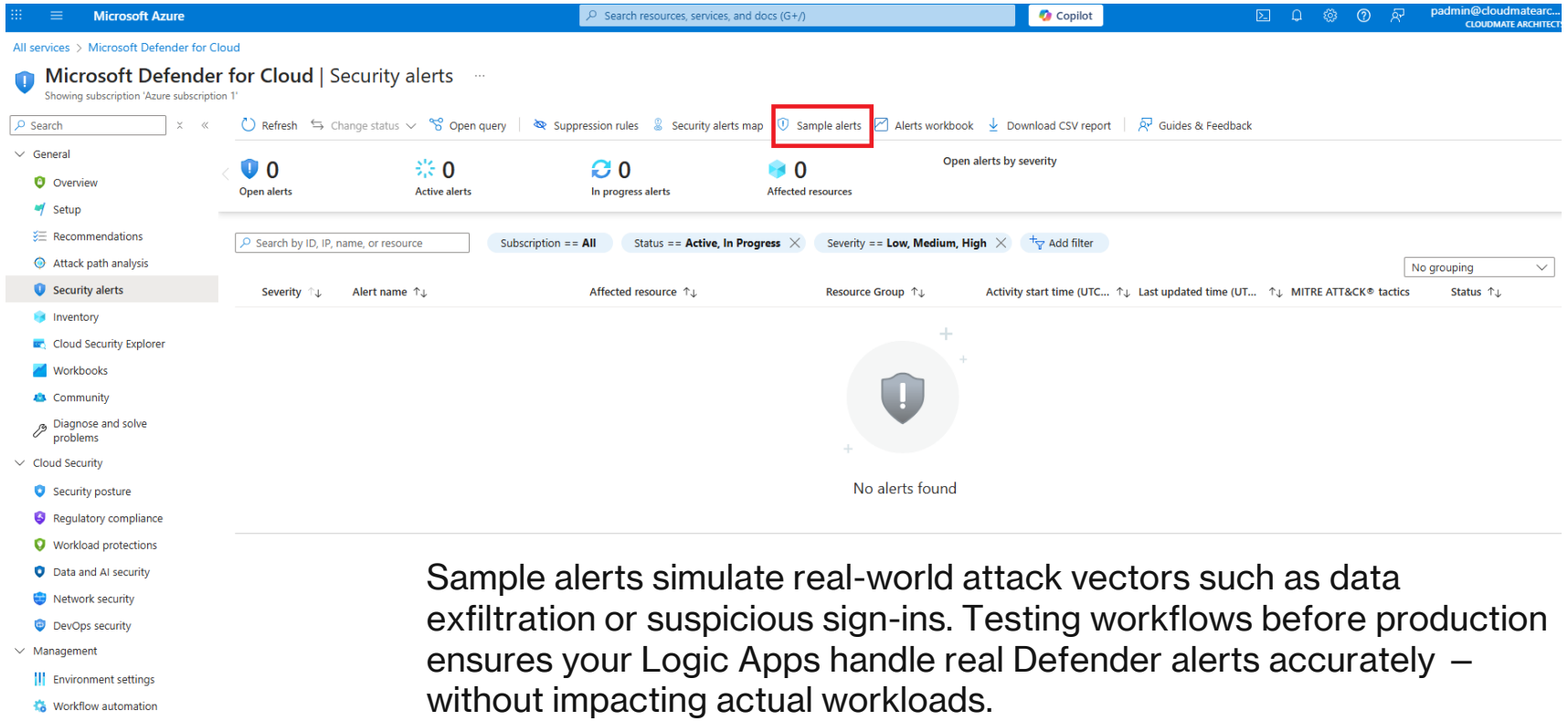


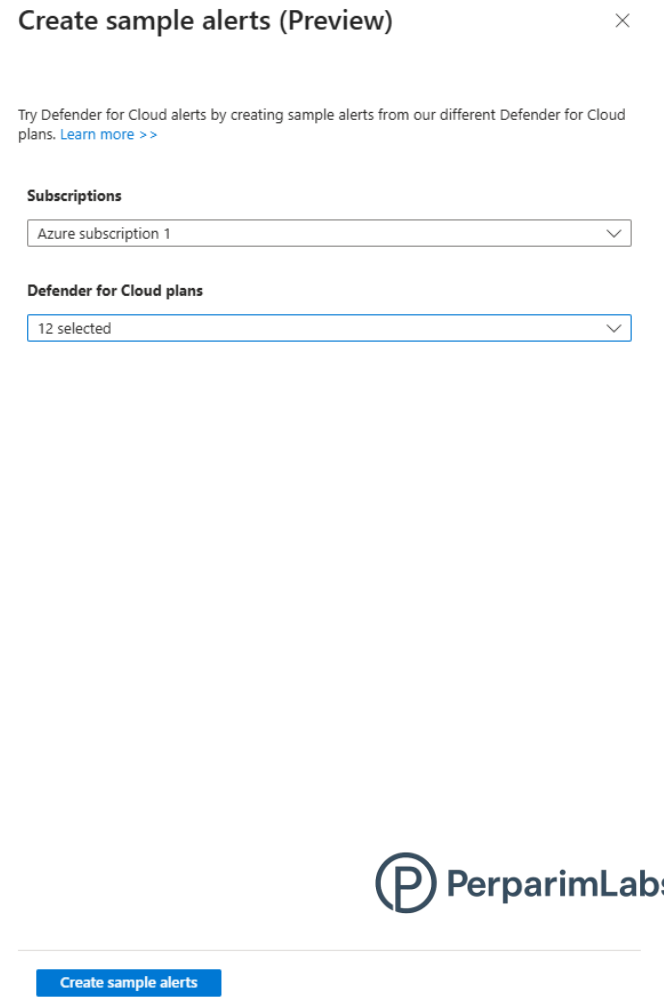
Configuring notifications ensures that high-severity alerts are routed instantly to operational teams. This mirrors real SOC workflows, where email or ticket-based alerting bridges **SIEM + ITSM integration**, improving **MTTD (Mean Time to Detect)** and **MTTR (Mean Time to Respond)**.

PerparimLabs

Generating Sample Alerts

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



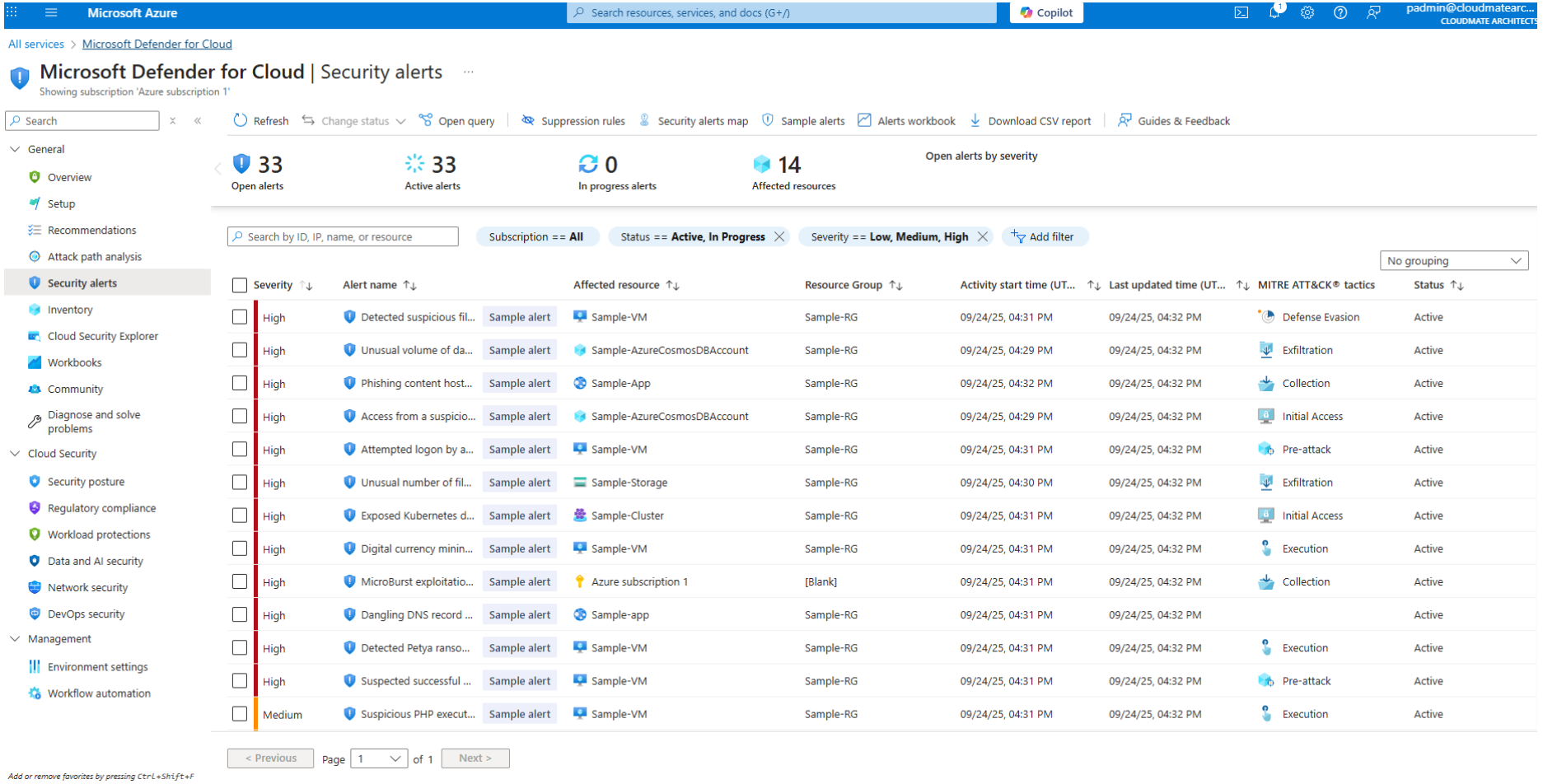


Sample alerts simulate real-world attack vectors such as data exfiltration or suspicious sign-ins. Testing workflows before production ensures your Logic Apps handle real Defender alerts accurately – without impacting actual workloads.

PerparimLabs

Validating Alerts in Defender for Cloud

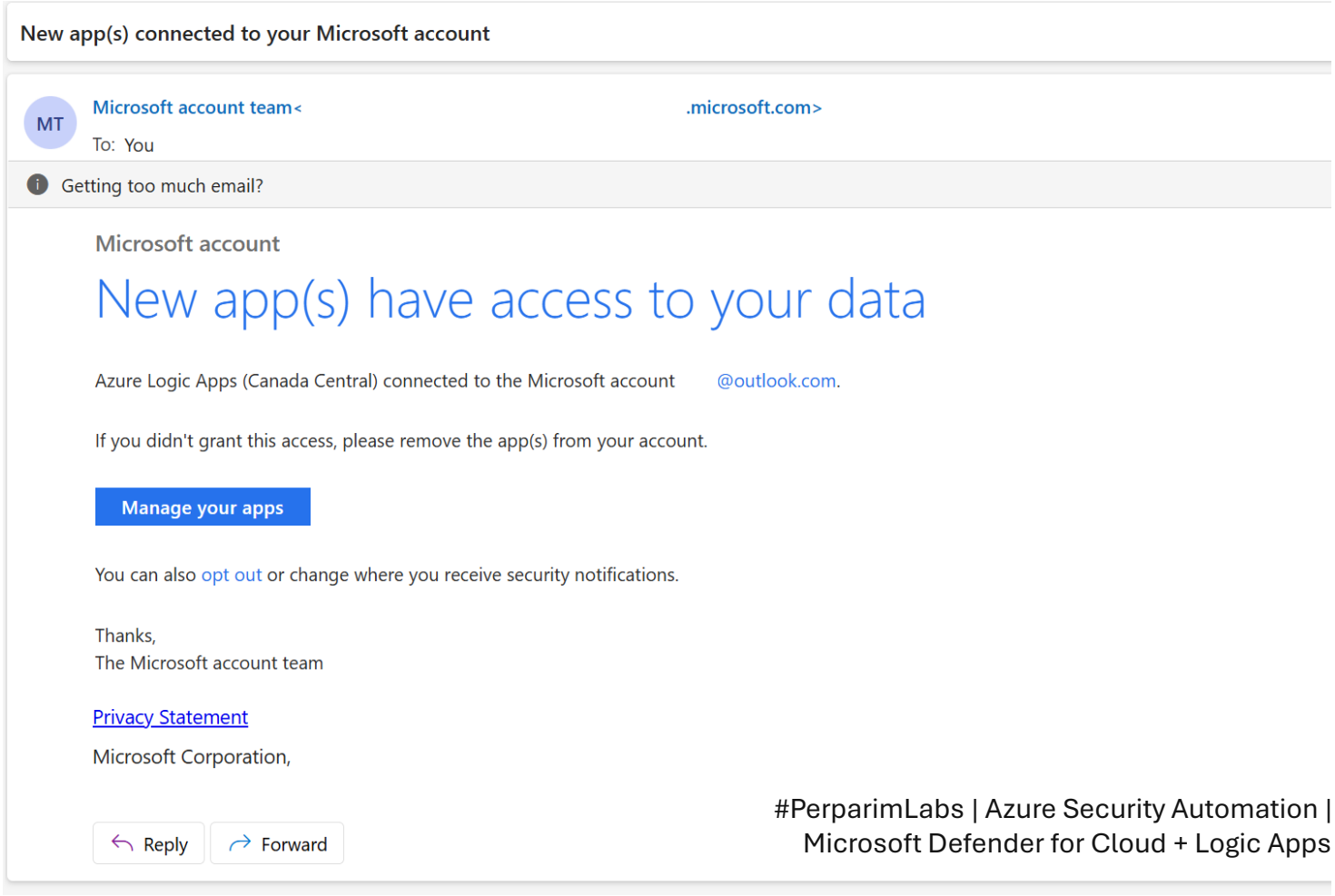
- Confirmed sample alerts were generated successfully across multiple Defender plans, covering scenarios like suspicious logons and data exfiltration.



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

MT Microsoft account team< .microsoft.com>

To: You

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,

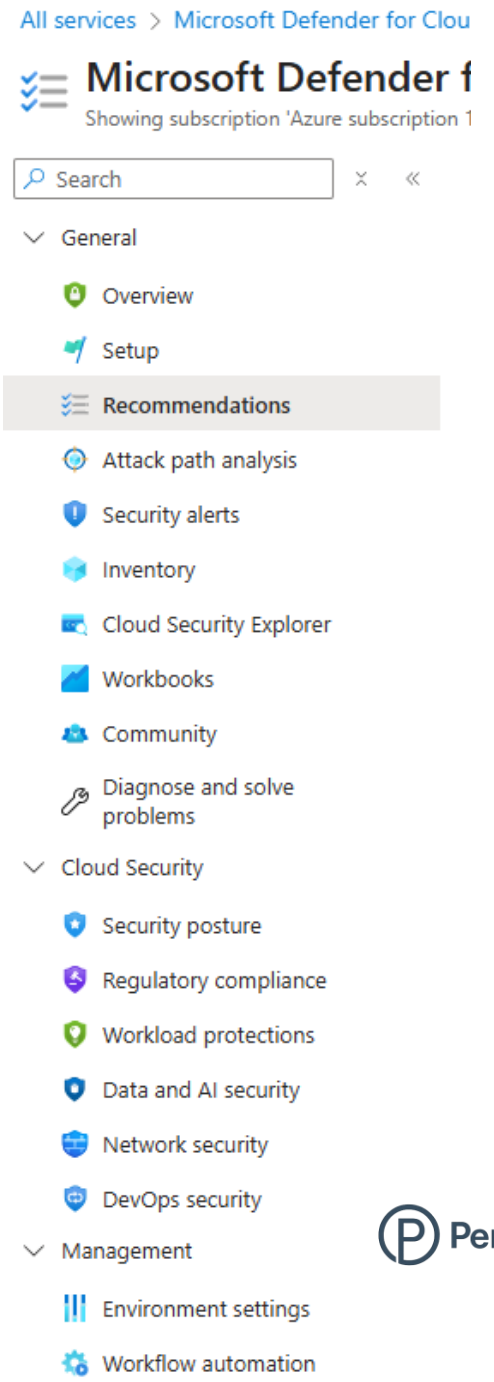
Reply Forward

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.

PerparimLabs

Reviewing Security Recommendations

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

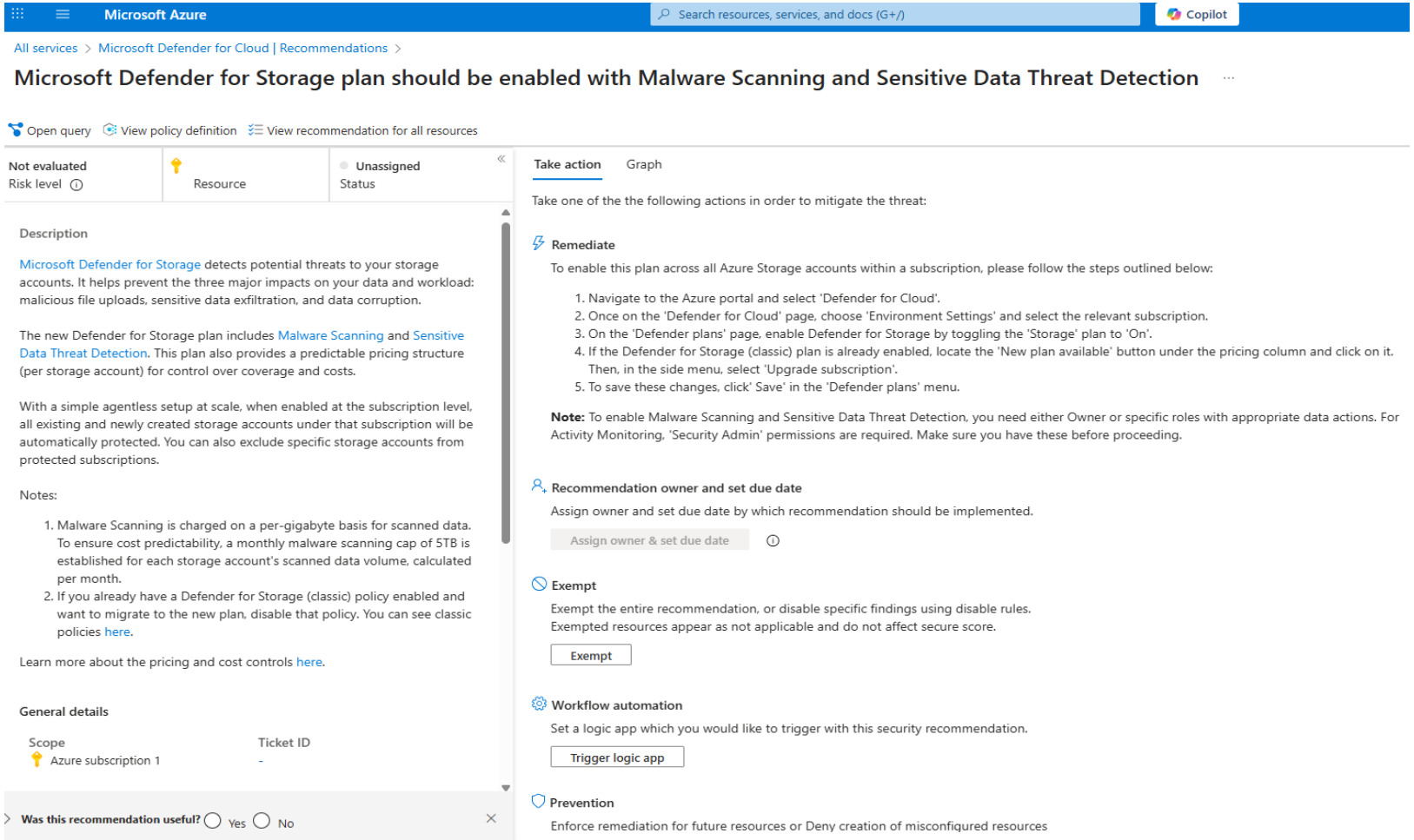


Defender for Cloud's *Recommendations* blade prioritizes risks using a Secure Score model. Reviewing these helps architects balance compliance and security posture improvement across hybrid environments.

PerparimLabs

Remediation Guidance

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



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.

PerparimLabs

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.

PerparimLabs