Automate Microsoft Defender for Cloud Alerts using Logic Apps

This project demonstrates how to automate security recommendations from Microsoft Defender for Cloud using Logic Apps (Standard), the modern approach to security orchestration in Azure.

Modern Portal Walkthrough – 2025 Edition (Workflow Standard Plan)

📍 #PerparimLabs | Azure Security Automation

PerparimLabs

Objective

Goal: Set up a Logic App to automatically send email notifications when new **Defender for Cloud recommendations** are triggered — demonstrating automation in modern Azure environments.

Logic Apps enable security teams to respond automatically when new risks are detected, reducing mean time to respond (MTTR) and ensuring consistent alert handling.

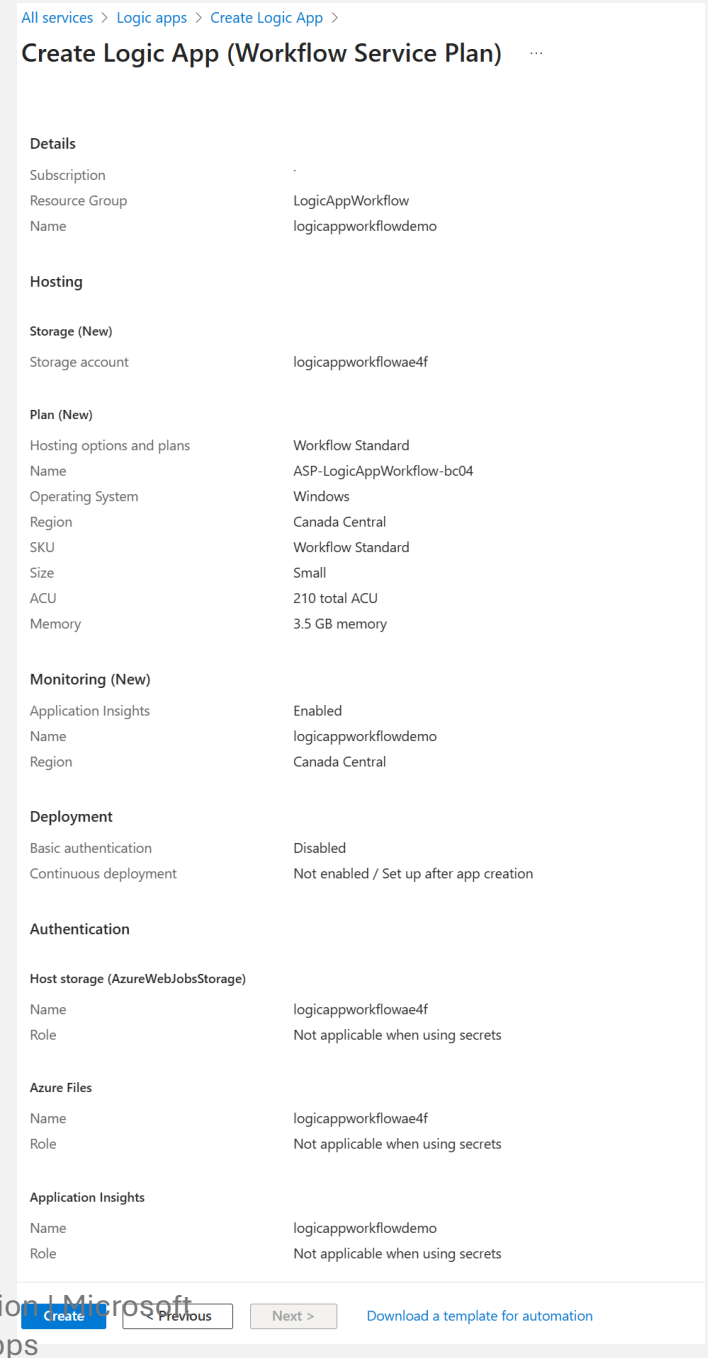
PerparimLabs

Create Logic App (Workflow Standard Plan)

- Created a new Logic App using the **Workflow Standard** plan, with integrated storage and Application Insights monitoring enabled.

The Standard plan hosts the Logic App on an App Service Plan for enterprise scalability and hybrid connectivity. It replaces the legacy Consumption model.

💡 *Note:* The new portal defaults to the **Standard hosting plan**, replacing the older Consumption model.

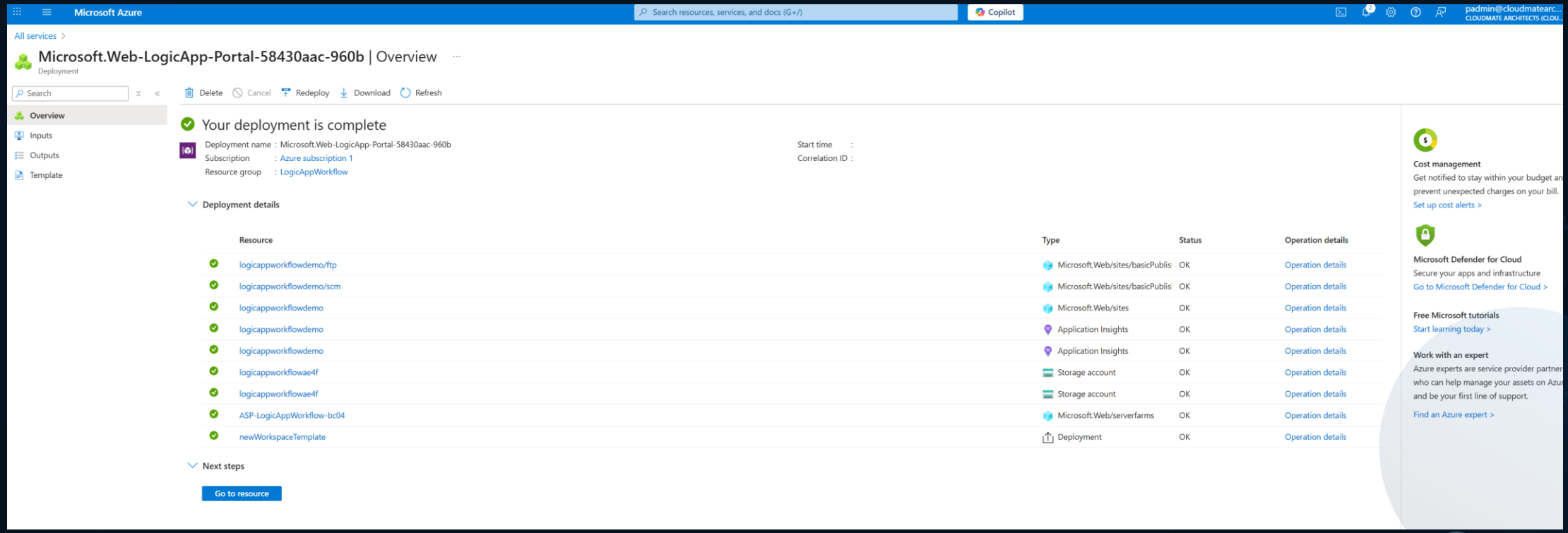


PerparimLabs

Deployment Complete

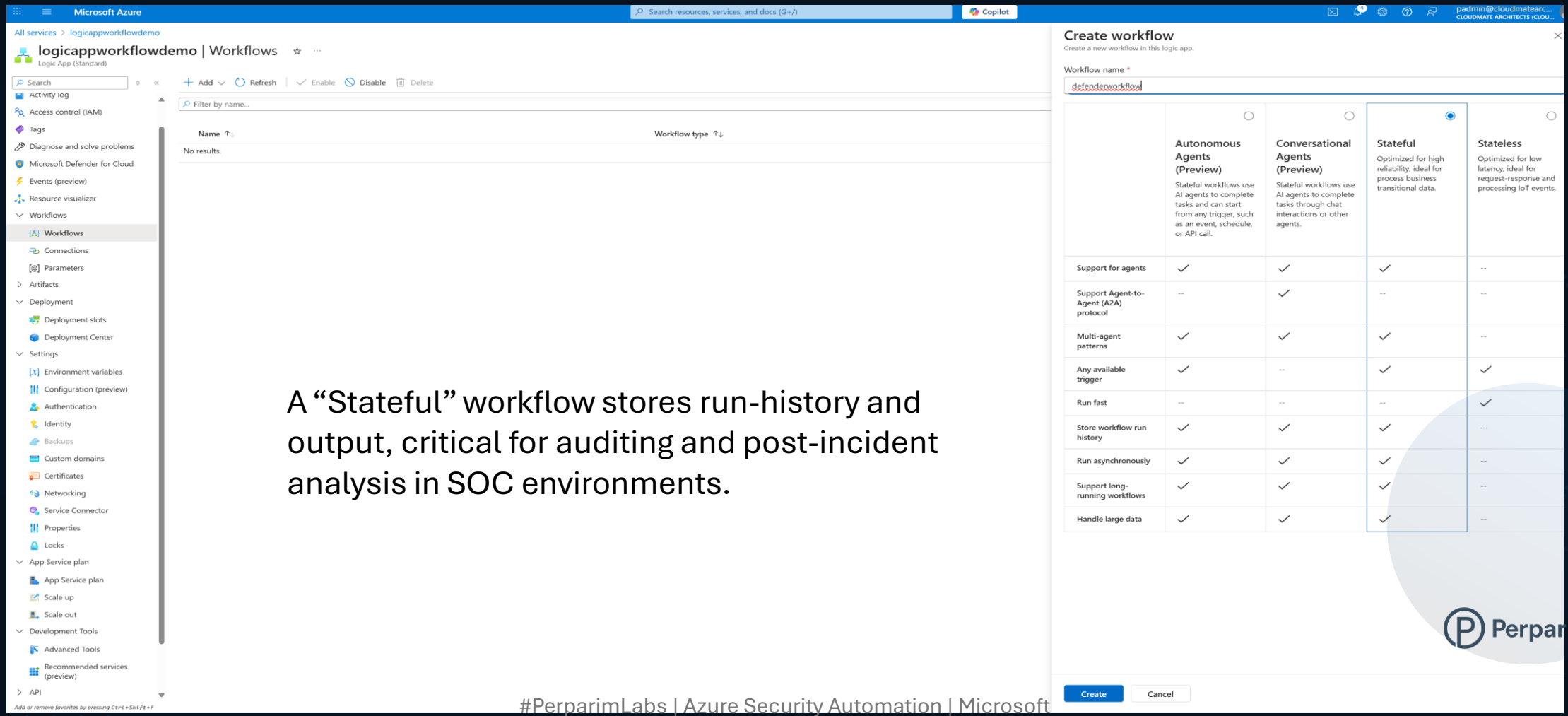
- Deployment succeeded — confirming Logic App, Storage Account, and App Service Plan resources created successfully.

App Service, Storage Account, and Application Insights are provisioned automatically to provide persistence, logging, and monitoring for each workflow run.



Create Workflow

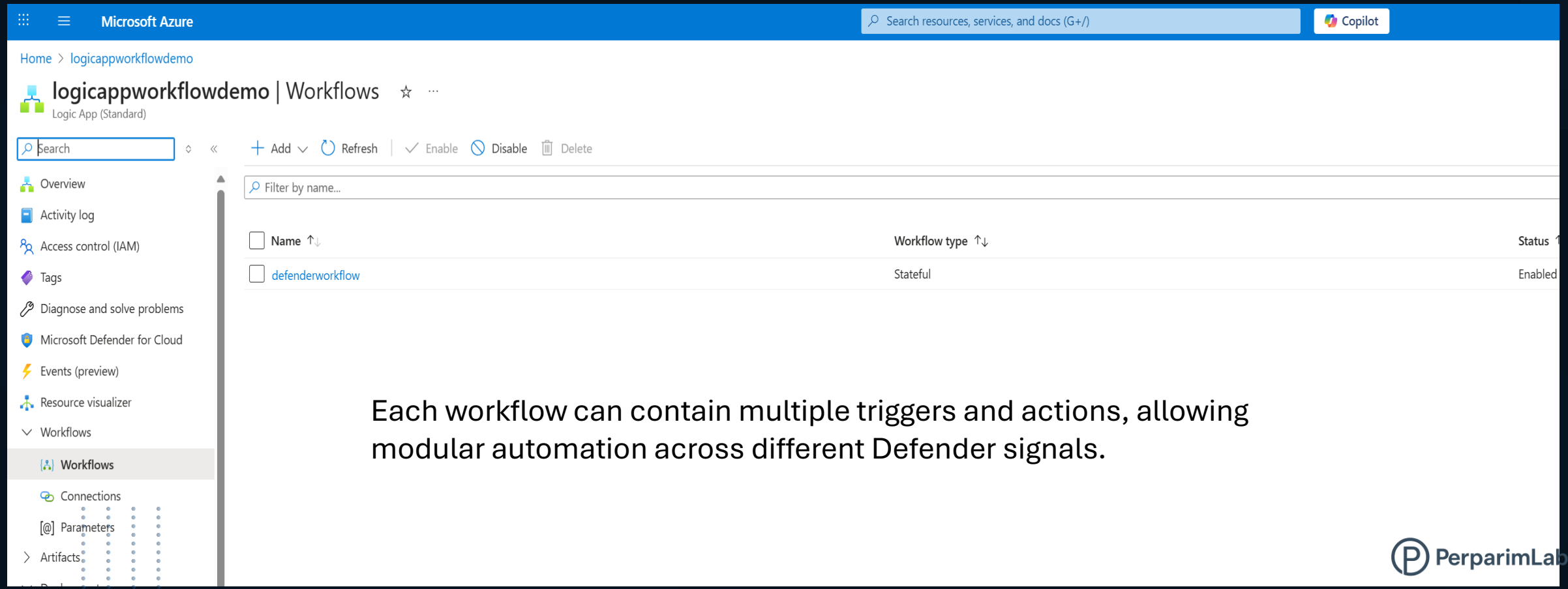
- Inside the Logic App, added a new workflow named **defenderworkflow** using the **Stateful** mode — optimized for long-running, reliable processes.



A “Stateful” workflow stores run-history and output, critical for auditing and post-incident analysis in SOC environments.

Workflow Created

- Workflow successfully created and enabled — ready to define triggers and actions.

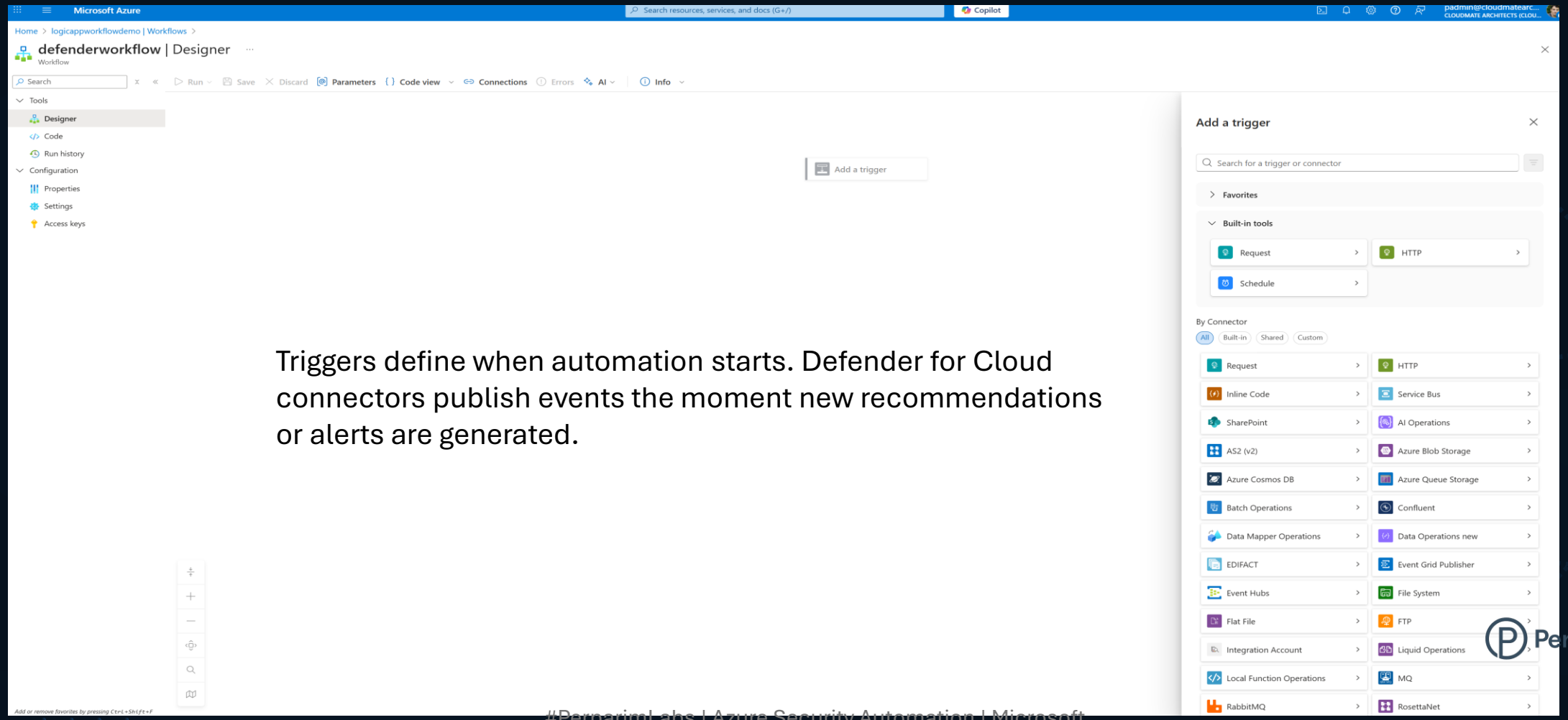


Each workflow can contain multiple triggers and actions, allowing modular automation across different Defender signals.

PerparimLabs

Add Trigger

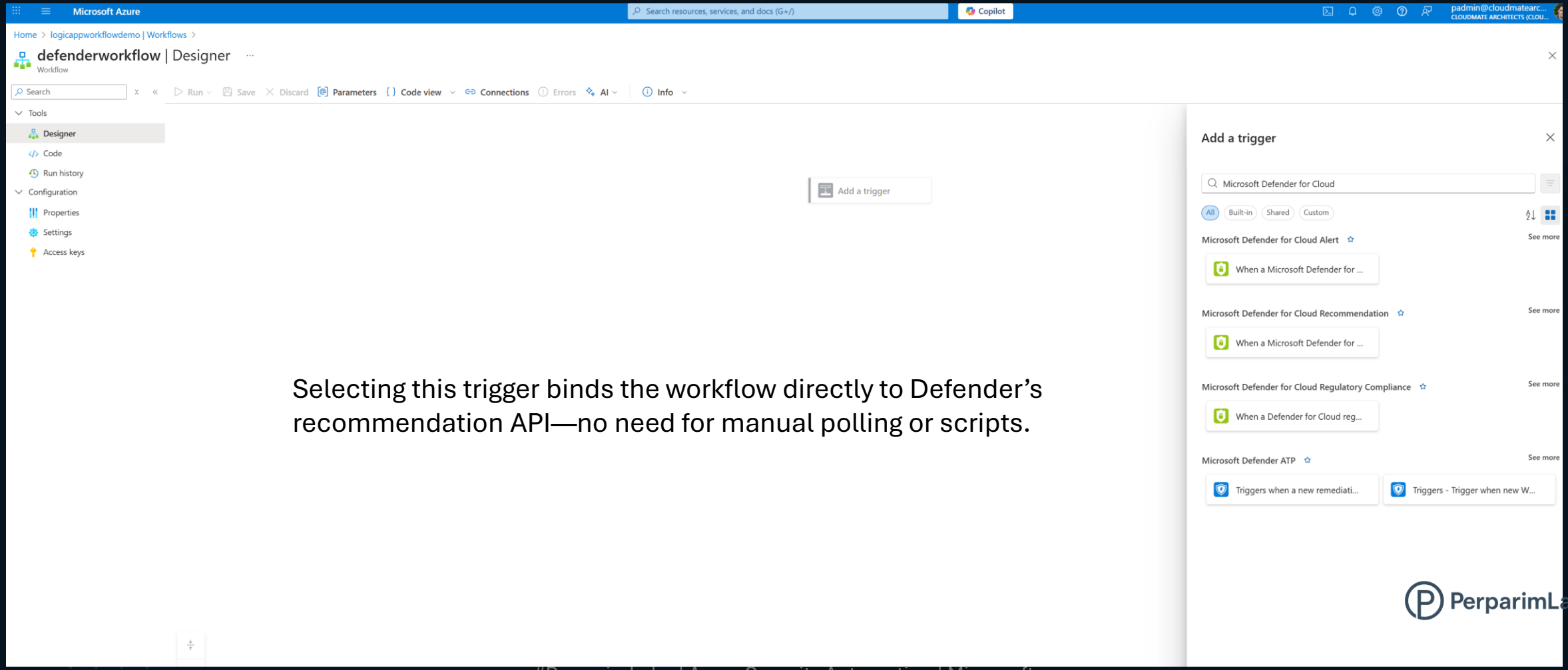
- Opened the **Designer** and selected the trigger source. Logic Apps Designer now provides built-in connectors for Defender, Azure, and third-party integrations.



Triggers define when automation starts. Defender for Cloud connectors publish events the moment new recommendations or alerts are generated.

Defender Trigger

- Selected **“When a Microsoft Defender for Cloud recommendation is created or triggered.”** This ensures automation activates instantly when new security recommendations are generated.



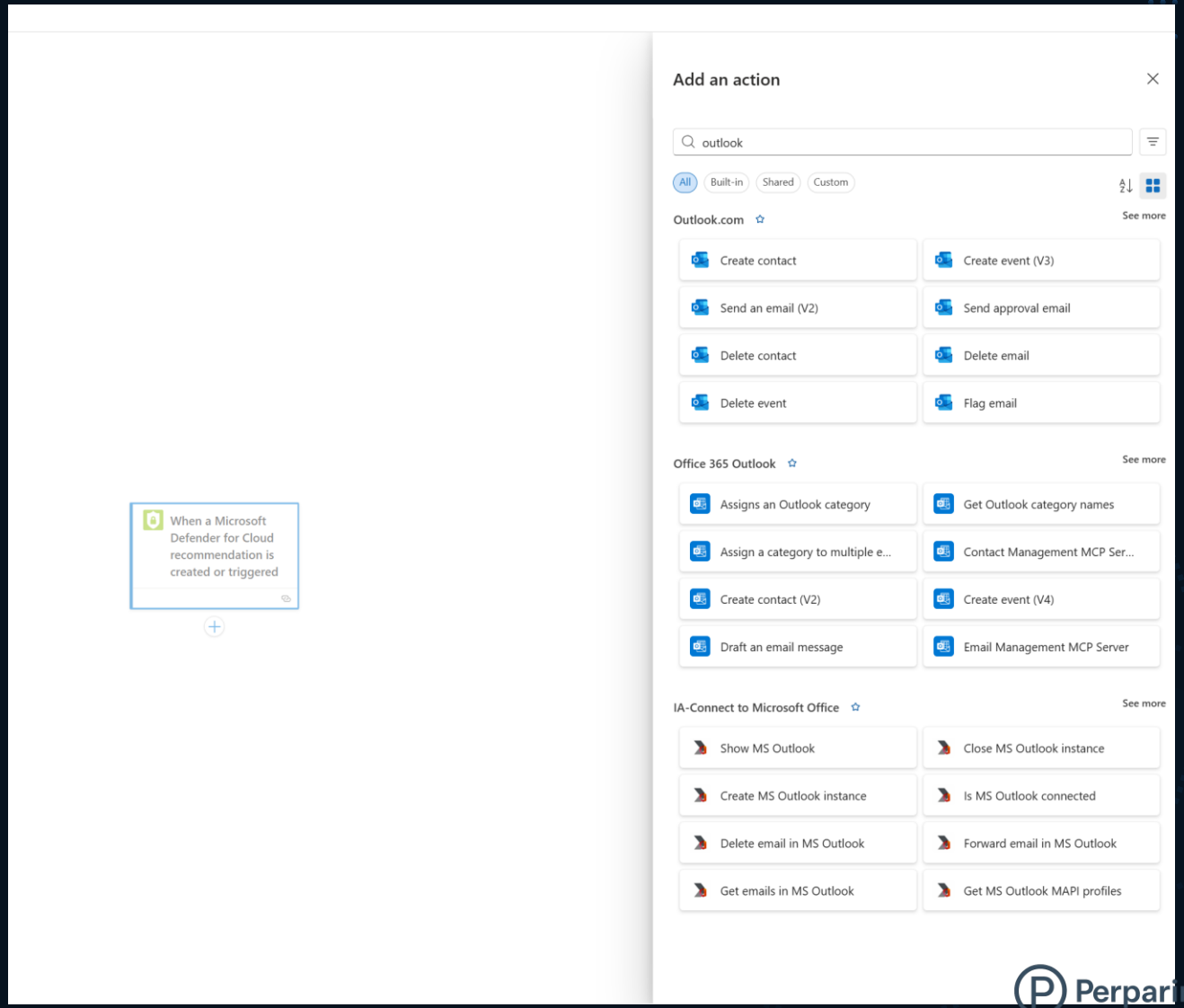
Selecting this trigger binds the workflow directly to Defender’s recommendation API—no need for manual polling or scripts.

PerparimLabs

Add Email Action

- Added an **Outlook (V2) Send Email** action to automatically alert the admin mailbox.

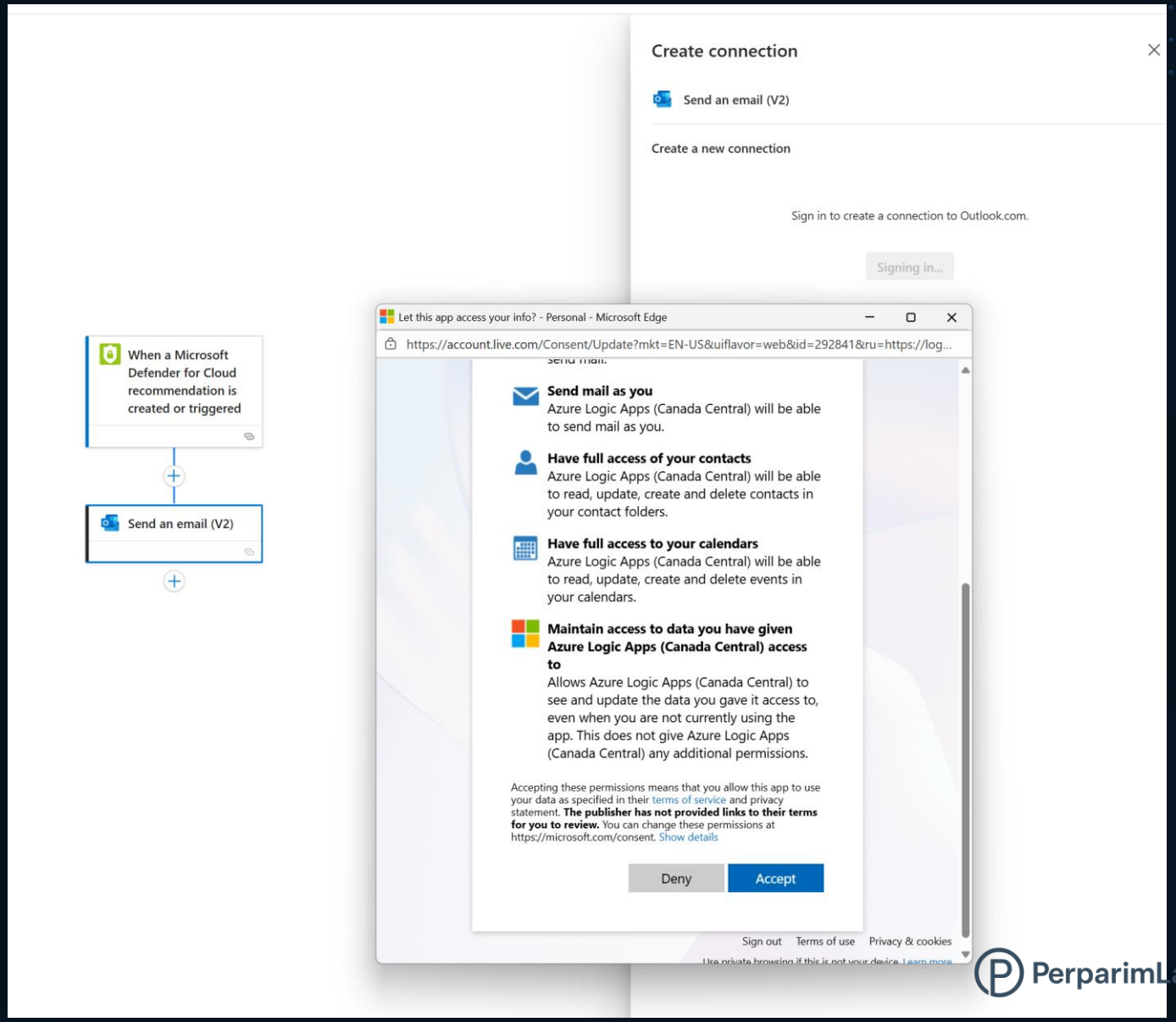
The Outlook connector is a quick notification channel; in production, this could integrate with Teams, ITSM, or Sentinel Playbooks.



Connect Outlook

- Authorized Azure Logic Apps (Canada Central) to send email using the connected Outlook account.

Uses secure OAuth 2.0 delegated permissions—no stored credentials—ensuring compliance with least-privilege principles.



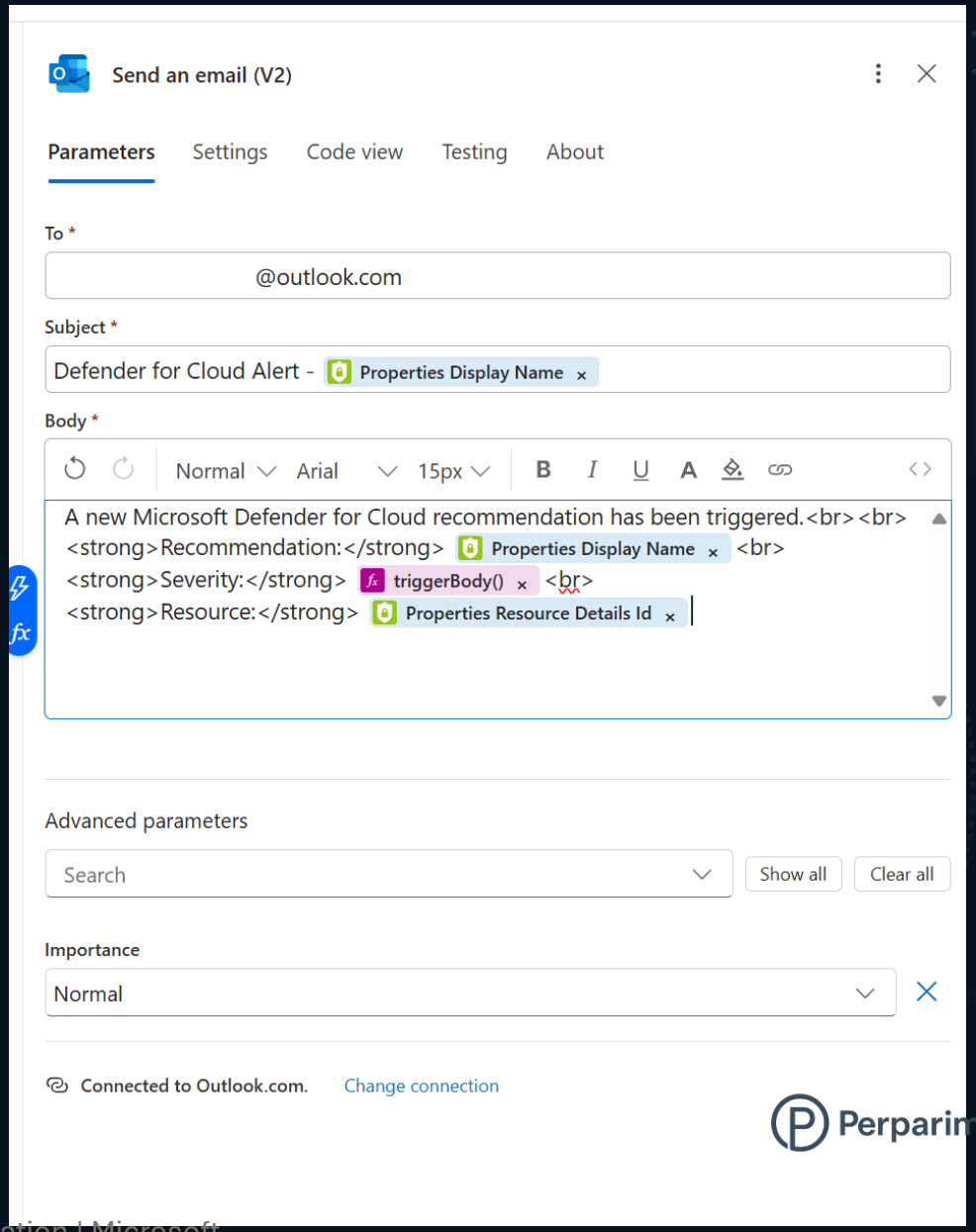
PerparimLabs

Configure Email Content

- Customized the email body with dynamic content:
- ➢ **Recommendation name**
- ➢ **Severity**
- ➢ **Resource details**

Dynamic content tokens pull real-time data (recommendation name, severity, resource ID) directly from Defender payloads, making alerts actionable.

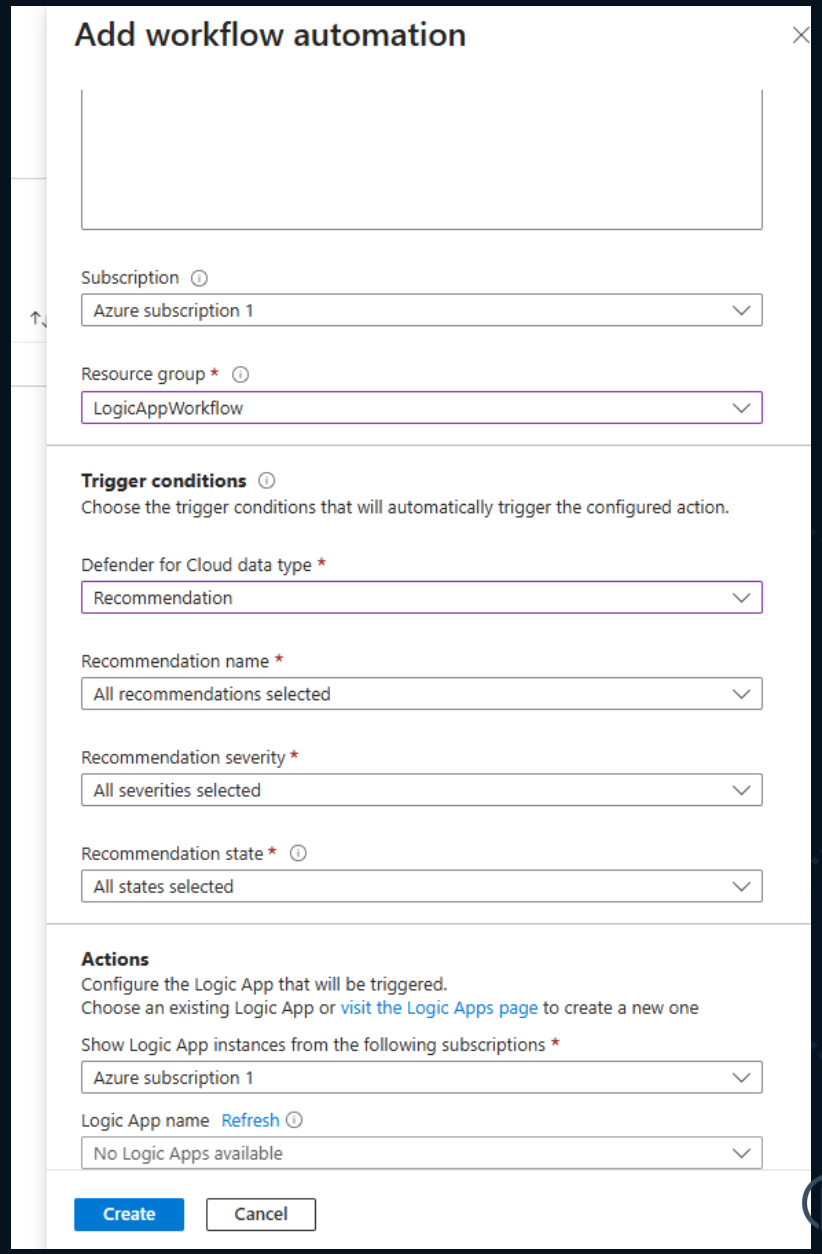
💡 *Tip:* You can format the body with HTML for rich, readable alerts.



Defender Workflow Automation Setup

- Opened **Defender for Cloud → Workflow Automation** to connect the Logic App. However, modern environments currently show:
- “No Logic Apps available”
- 🧩 *Reason:* Logic App (Standard) resources are not yet discoverable from Defender for Cloud automation panel — only **Consumption plans** appear there.

As of 2025, Defender for Cloud’s automation pane lists only Consumption Logic Apps. Standard-plan Logic Apps integrate through native triggers instead.



Summary

✅ **Lab Completed:**

- ➢ Built Logic App with Defender trigger and Outlook alert.
- ➢ Observed modern portal limitations (Standard vs. Consumption).
- ➢ Demonstrated full automation workflow concept.

This architecture establishes a reusable pattern: detect → notify → remediate.
Future enhancements can add playbooks, ticket creation, or auto-remediation.

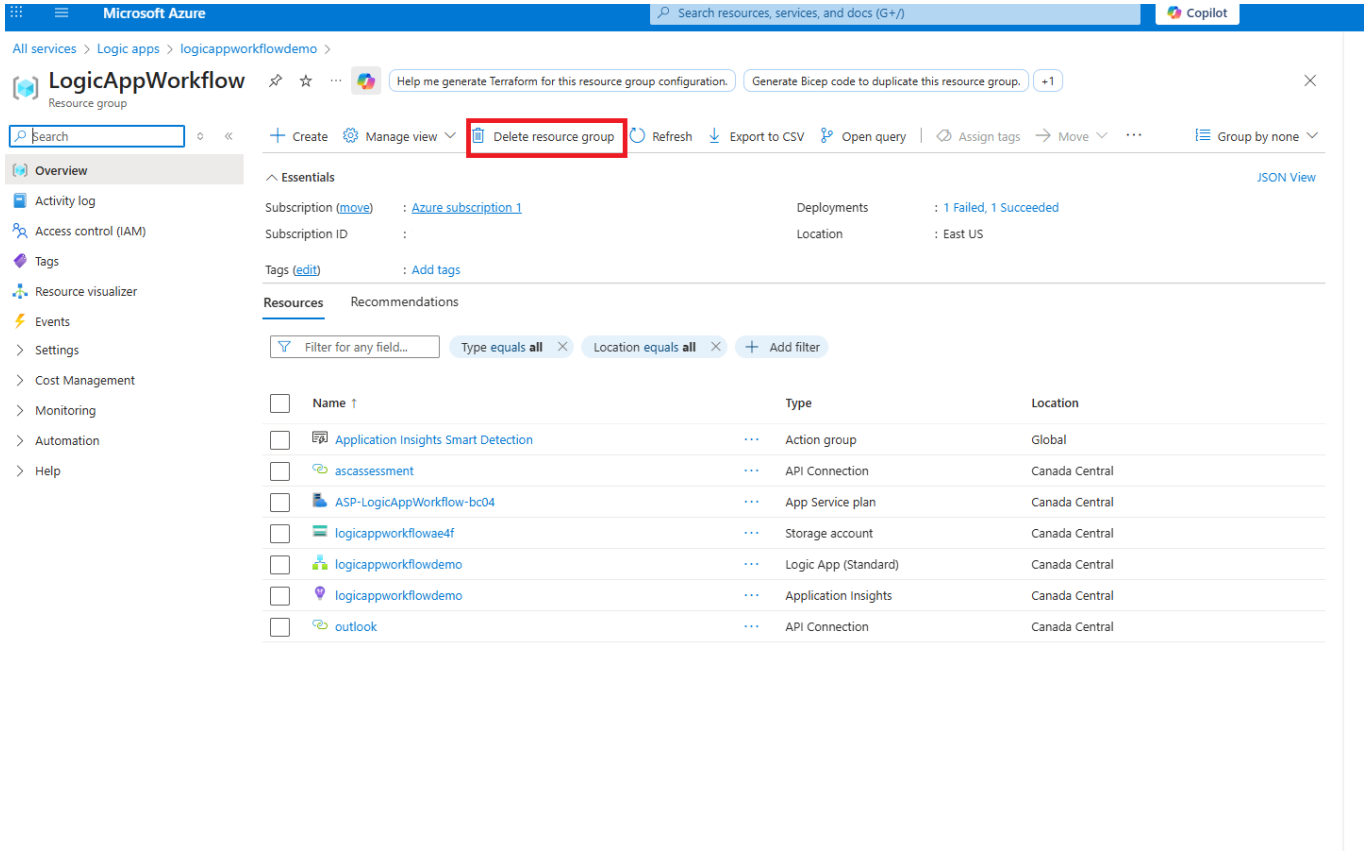
🧠 *Key Takeaway:*
Microsoft Defender for Cloud automation now integrates with **Logic Apps Standard**, but configuration visibility in Defender UI will be updated in future releases.

PerparimLabs

Cleanup

🧹 Delete the resource group **LogicAppWorkflow** to stop charges.

💡 Always remove unused Standard Logic Apps — they run under App Service Plans and can accumulate small costs.



Standard Logic Apps run persistently—deleting the resource group immediately halts compute billing.

PerparimLabs