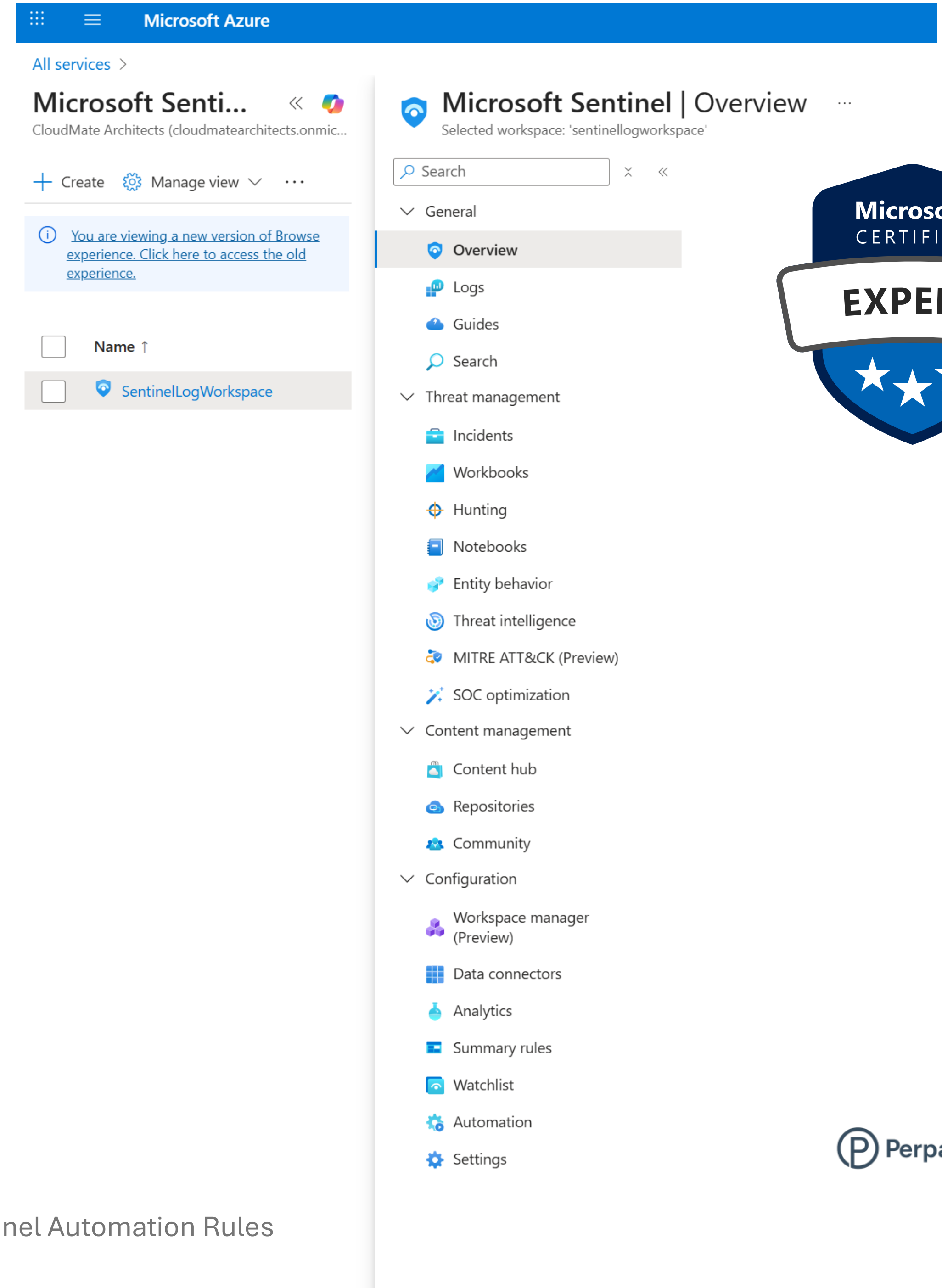
Automating Incident Response in Microsoft Sentinel

- Microsoft Sentinel empowers SOC teams with automation.
- Automation rules reduce noise, standardize responses, and accelerate incident handling.
- This project demonstrates building an automation rule to assign ownership of high-severity incidents.



Microsoft Sentinel | Overview

Selected workspace: 'sentinellogworkspace'

Microsoft Senti...

CloudMate Architects (cloudmatearchitects.onmic...

You are viewing a new version of Browse experience. Click here to access the old experience.

Microsoft CERTIFIED EXPERT

PerparimLabs

Why Automation Rules?

Streamline Incident Response → Automatically assign incidents to the right analyst.

Reduce Noise → Downgrade/close low-level alerts automatically.

Enrich Incidents → Add tags, tasks, or run playbooks with context.

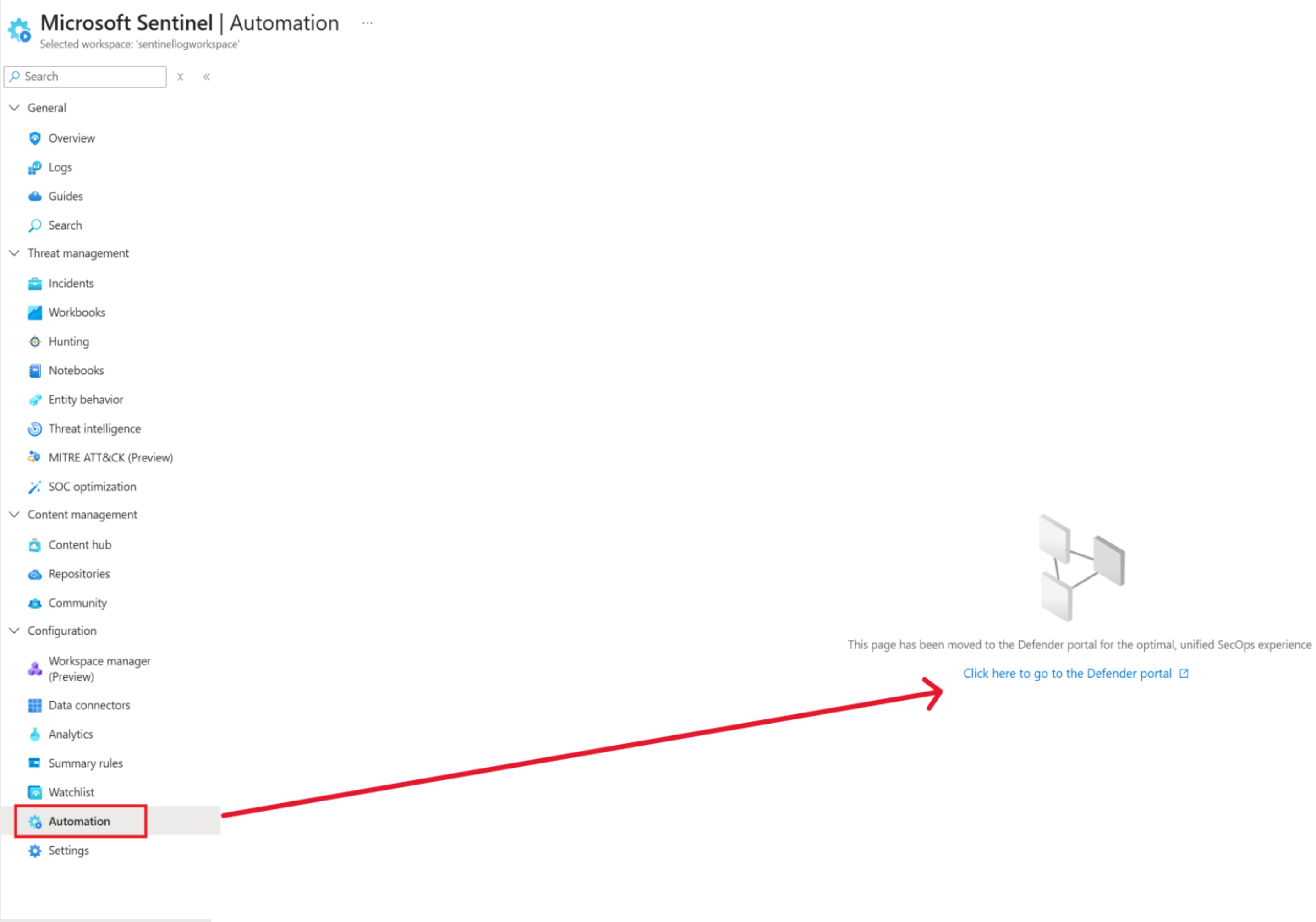
Manage Communication → Trigger notifications for critical incidents.

This sets the stage: automation is about **speed, accuracy, and efficiency**.

PerparimLabs

Where to Configure Rules

- Navigate to **Microsoft Sentinel → Configuration → Automation**.
- Sentinel automation rules are now integrated with the **Microsoft Defender portal** for unified SOC workflows.
- From here, analysts can create rules, link playbooks, and manage priorities.



Microsoft Sentinel | Automation

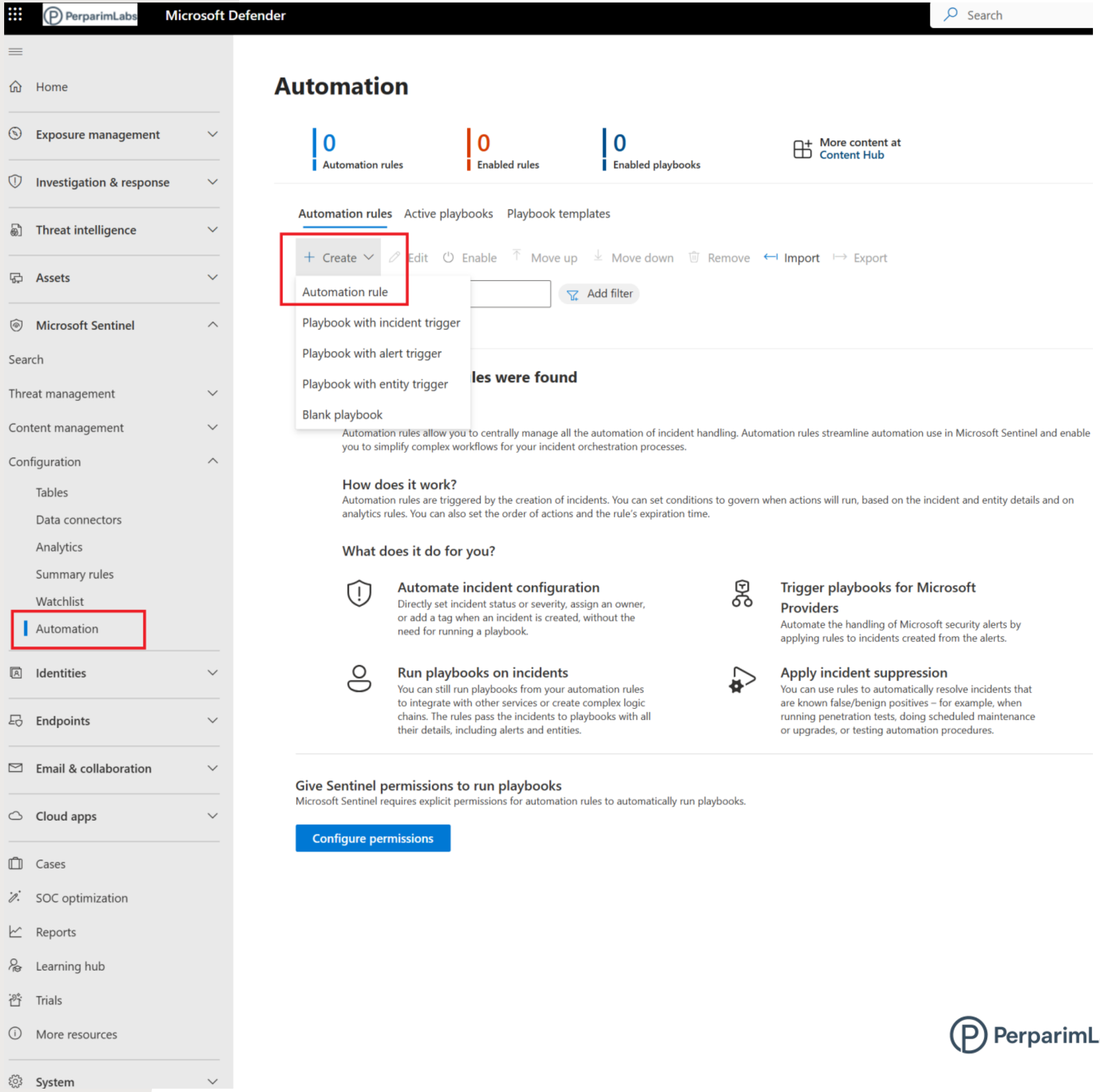
Selected workspace: 'sentinellogworkspace'

This page has been moved to the Defender portal for the optimal, unified SecOps experience

Click here to go to the Defender portal

Create New Automation Rule

- Start by selecting **+ Create → Automation Rule**.
- Automation rules use **Triggers → Conditions → Actions**.
- Example: *When a high-severity incident is created, assign to a specific analyst.*



Automation

les were found

Automation rules allow you to centrally manage all the automation of incident handling. Automation rules streamline automation use in Microsoft Sentinel and enable you to simplify complex workflows for your incident orchestration processes.

How does it work?

Automation rules are triggered by the creation of incidents. You can set conditions to govern when actions will run, based on the incident and entity details and on analytics rules. You can also set the order of actions and the rule's expiration time.

What does it do for you?

Automate incident configuration
Directly set incident status or severity, assign an owner, or add a tag when an incident is created, without the need for running a playbook.

Trigger playbooks for Microsoft Providers
Automate the handling of Microsoft security alerts by applying rules to incidents created from the alerts.

Run playbooks on incidents
You can still run playbooks from your automation rules to integrate with other services or create complex logic chains. The rules pass the incidents to playbooks with all their details, including alerts and entities.

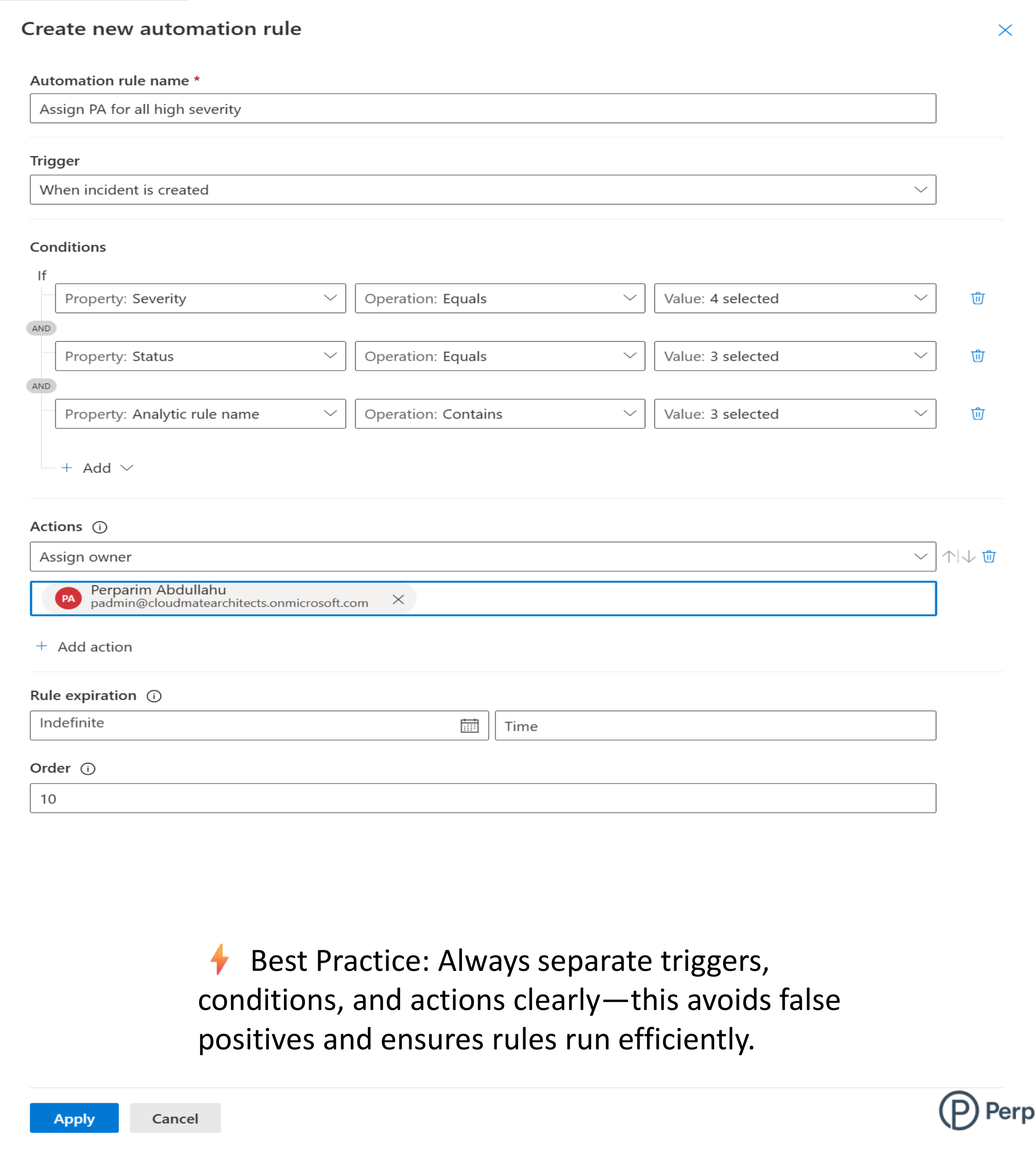
Apply incident suppression
You can use rules to automatically resolve incidents that are known false/benign positives – for example, when running penetration tests, doing scheduled maintenance or upgrades, or testing automation procedures.

Give Sentinel permissions to run playbooks

Microsoft Sentinel requires explicit permissions for automation rules to automatically run playbooks.

Define Conditions

- **Trigger**: *When incident is created*.
- **Conditions**:
  - Severity = High
  - Status = Active
  - Analytic Rule Name contains “Advanced Attack Detection”
- **Action**: Assign to analyst (Perparim Abdullahu).
- **Order**: 10 (best practice → space rules by 5–10 for flexibility).
- ⚡ **Key Point**: Triggers start the rule, conditions refine when it applies, and actions enforce the response.



Create new automation rule

Automation rule name *
Assign PA for all high severity

Trigger
When incident is created

Conditions

If

Property: Severity	Operation: Equals	Value: 4 selected
AND		
Property: Status	Operation: Equals	Value: 3 selected
AND		
Property: Analytic rule name	Operation: Contains	Value: 3 selected

+ Add

Actions ⓘ
Assign owner
PA Perparim Abdullahu padmin@cloudmatearchitects.onmicrosoft.com

+ Add action

Rule expiration ⓘ
Indefinite
Time

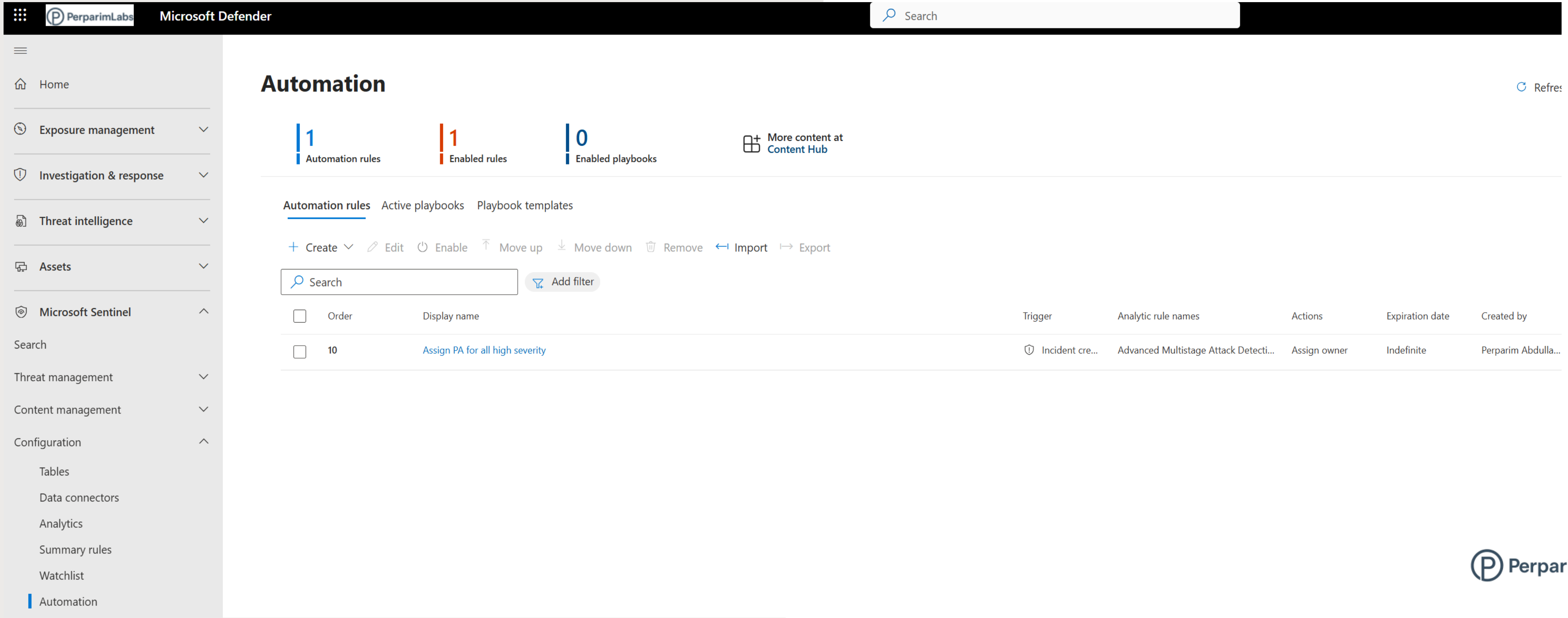
Order ⓘ
10

⚡ Best Practice: Always separate triggers, conditions, and actions clearly—this avoids false positives and ensures rules run efficiently.

PerparimLabs

Automation Rule in Action

- Rule is now active in Sentinel.
- All high-severity incidents will be automatically assigned to the owner.
- Saves analyst time, ensures accountability, and standardizes SOC workflows.



Automation

1	1	0
Automation rules	Enabled rules	Enabled playbooks

☐	Order	Display name	Trigger	Analytic rule names	Actions	Expiration date	Created by
☐	10	Assign PA for all high severity	Incident cre...	Advanced Multistage Attack Detecti...	Assign owner	Indefinite	Perparim Abdulla...

PerparimLabs

Knowledge Wrap-Up

Automation Rules = **Lightweight automation** inside Sentinel.

Best practices:

Use **broad triggers** with **refined conditions.**

Space rule order (5, 10, 15).

Combine with **Logic Apps Playbooks** for advanced actions.

Automations reduces MTTR (Mean Time to Respond) and standardizes SOC workflows—critical for real-world enterprises.

PerparimLabs