# Build Your First Analytics Rule in Microsoft Sentinel

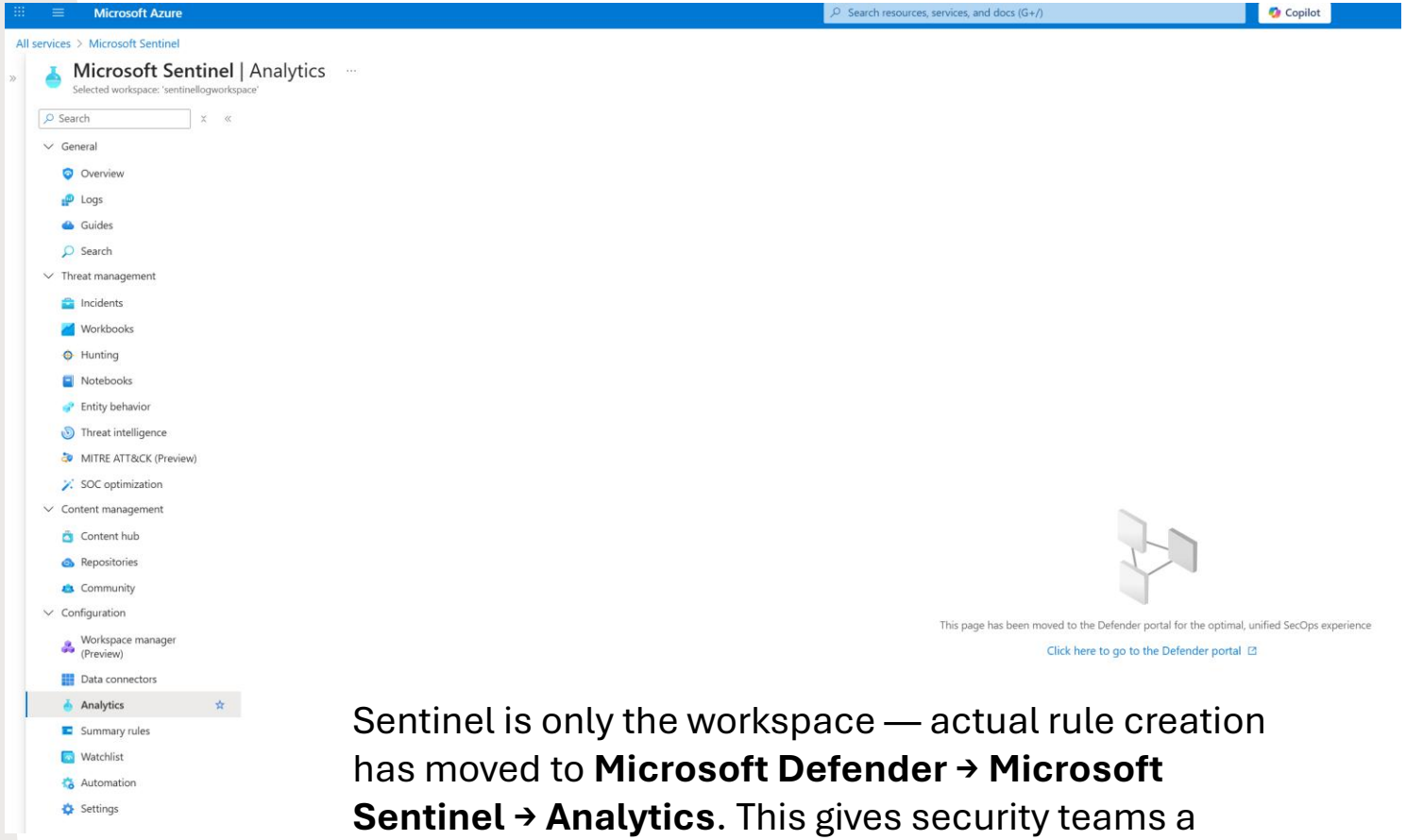
Detect high-risk logins with custom scheduled queries


**Microsoft Sentinel is now managed in the Microsoft Defender portal** — you create and manage all analytics rules from there. Sentinel is your SIEM (collect & analyze data), and Defender gives you a unified SecOps experience.

PerparimLabs

# Navigate to Analytics

- Go to **Microsoft Sentinel** in the Azure portal
- Under **Configuration**, click **Analytics**
- Notice it now redirects you to the **Microsoft Defender** portal

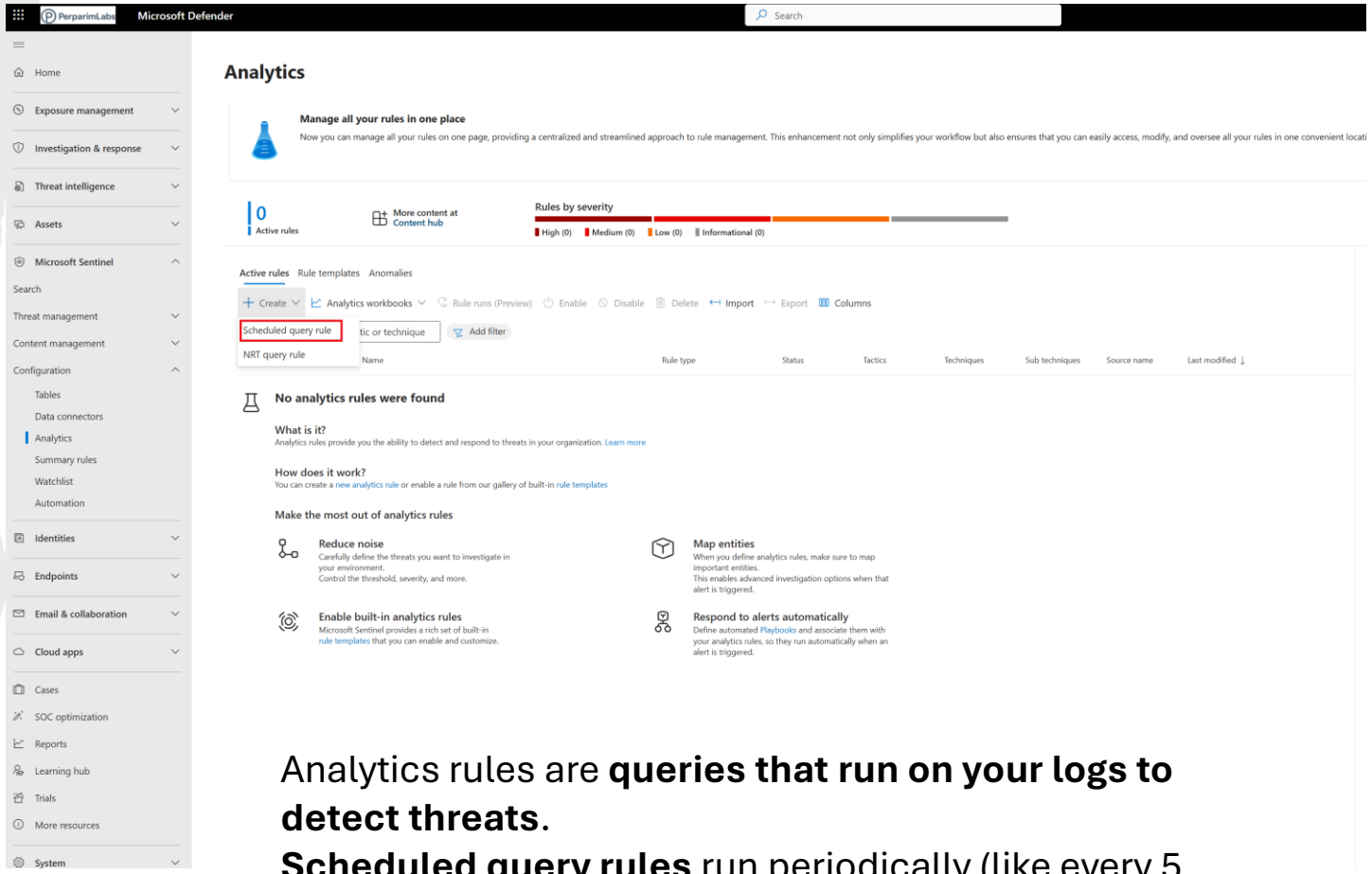



Sentinel is only the workspace — actual rule creation has moved to **Microsoft Defender → Microsoft Sentinel → Analytics**. This gives security teams a **centralized place** to build and manage rules.

PerparimLabs

# Create a Scheduled Query Rule

- In the **Defender > Analytics** page
- Click **Create ➜ Scheduled query rule**

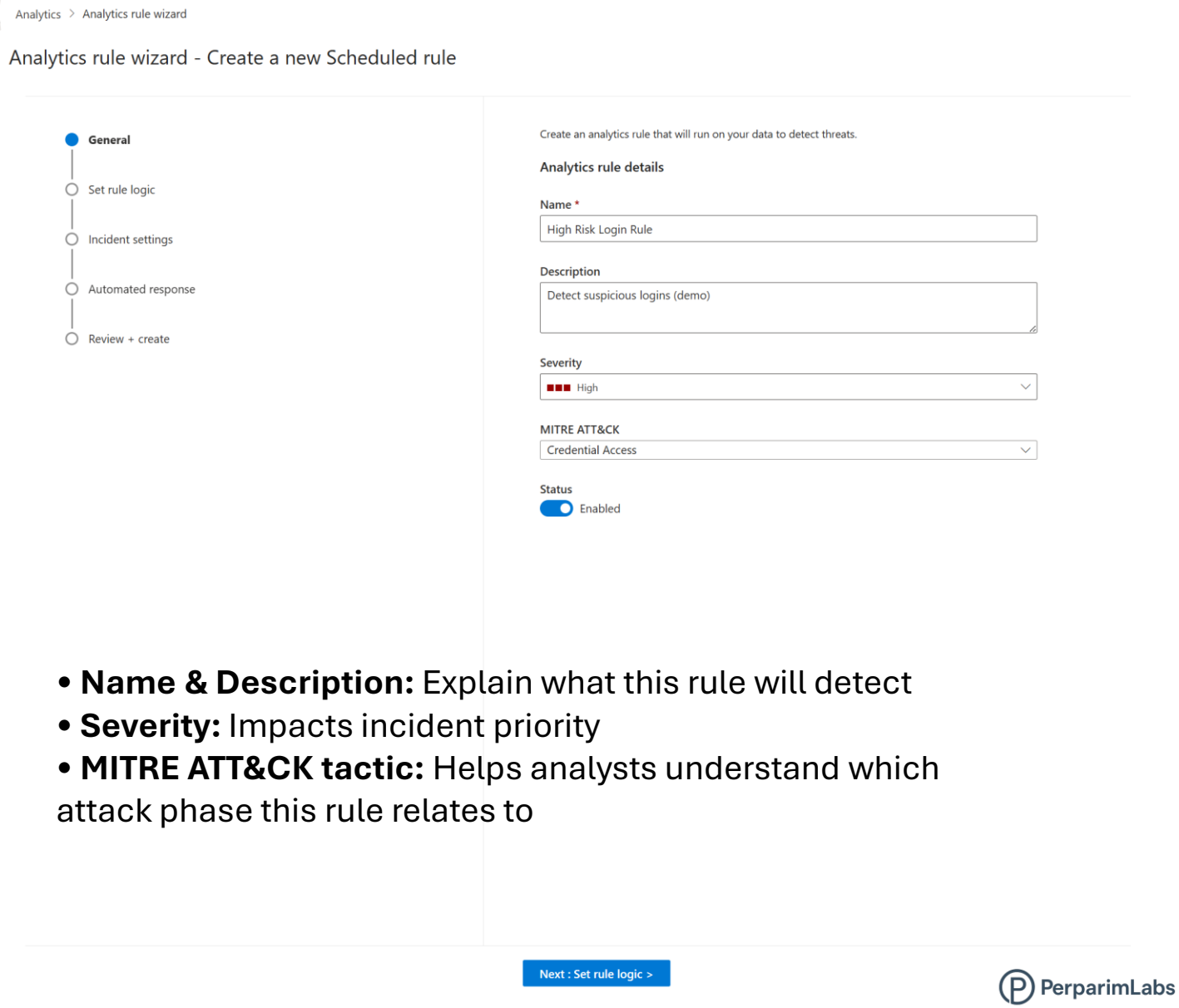



Analytics rules are **queries that run on your logs to detect threats**.
**Scheduled query rules** run periodically (like every 5 minutes) to **catch suspicious patterns automatically**.

PerparimLabs

# General Settings

- **Name:** High Risk Login Rule
- **Description:** Detect suspicious logins (demo)
- **Severity:** High
- **MITRE ATT&CK tactic:** Credential Access
- **Status:** Enabled




- **Name & Description:** Explain what this rule will detect
- **Severity:** Impacts incident priority
- **MITRE ATT&CK tactic:** Helps analysts understand which attack phase this rule relates to

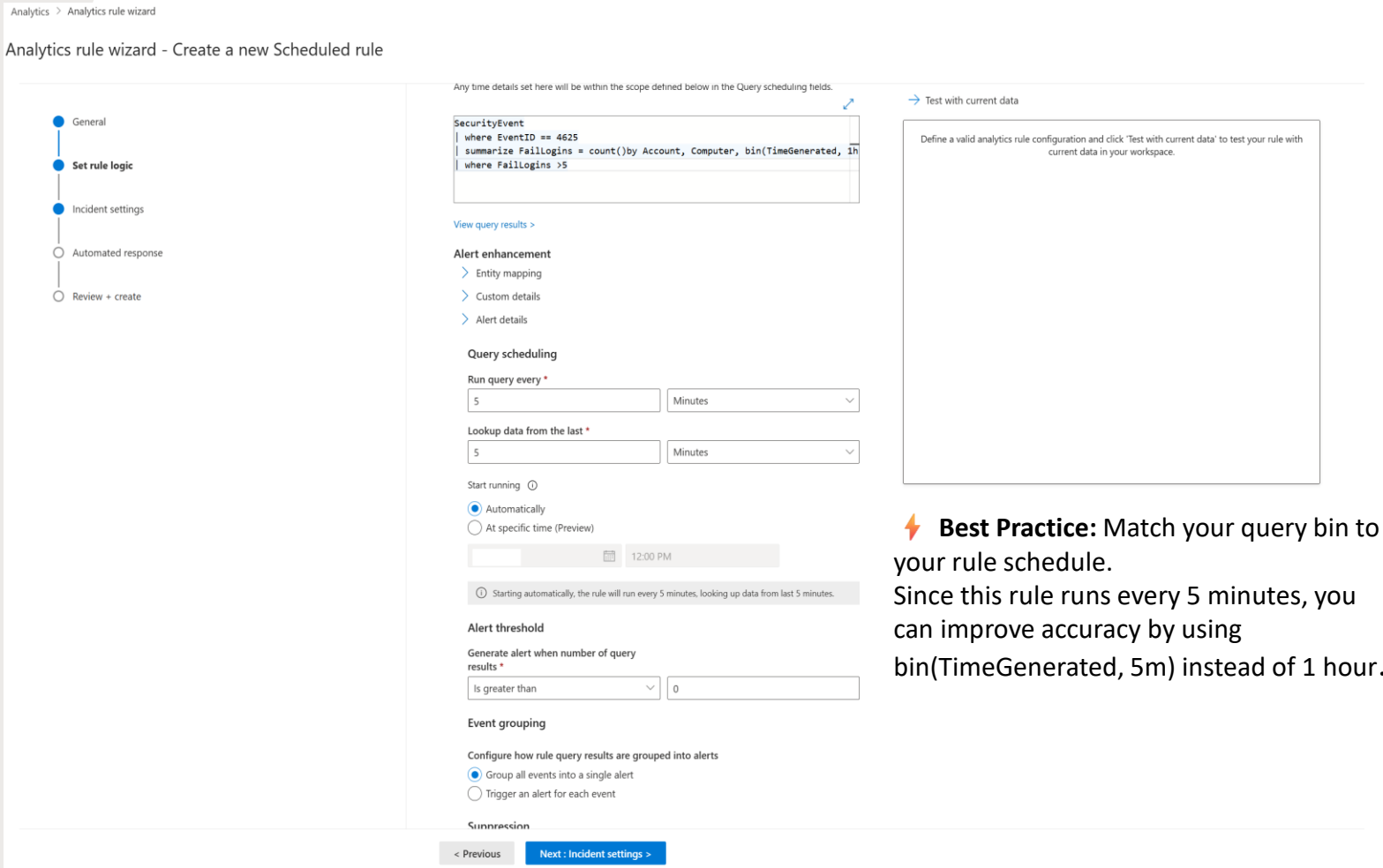
PerparimLabs

# Set Rule Logic

- Paste the KQL query:

SecurityEvent | where EventID == 4625 | summarize FailLogins = count() by Account, Computer, bin(TimeGenerated, 1h) | where FailLogins > 5

- Set **Run query every:** 5 minutes
- Set **Lookup data from last:** 5 minutes
- Set **Trigger alert if query returns more than 0 results**

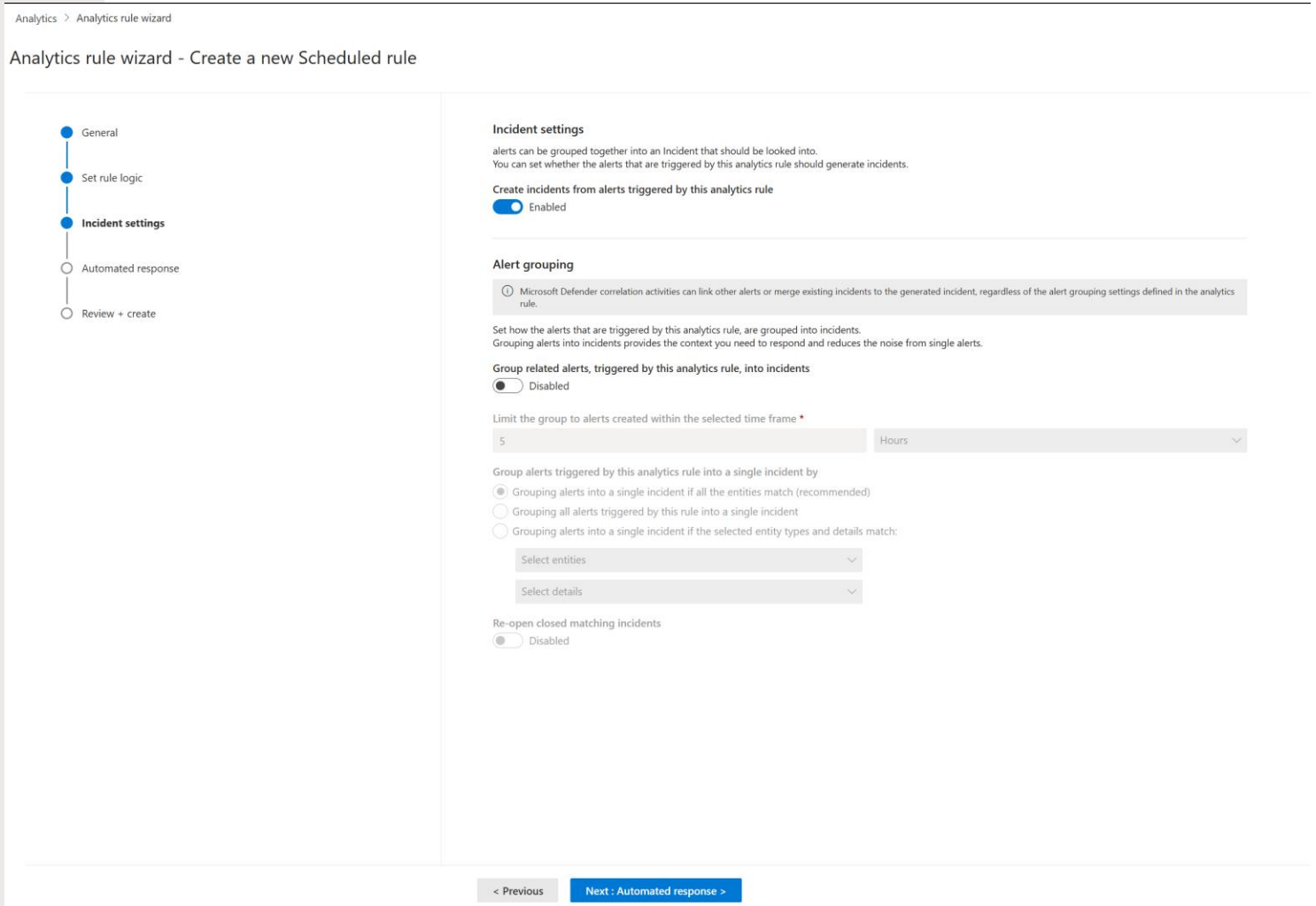



**Best Practice:** Match your query bin to your rule schedule.
Since this rule runs every 5 minutes, you can improve accuracy by using bin(TimeGenerated, 5m) instead of 1 hour.

PerparimLabs

# Incident Settings

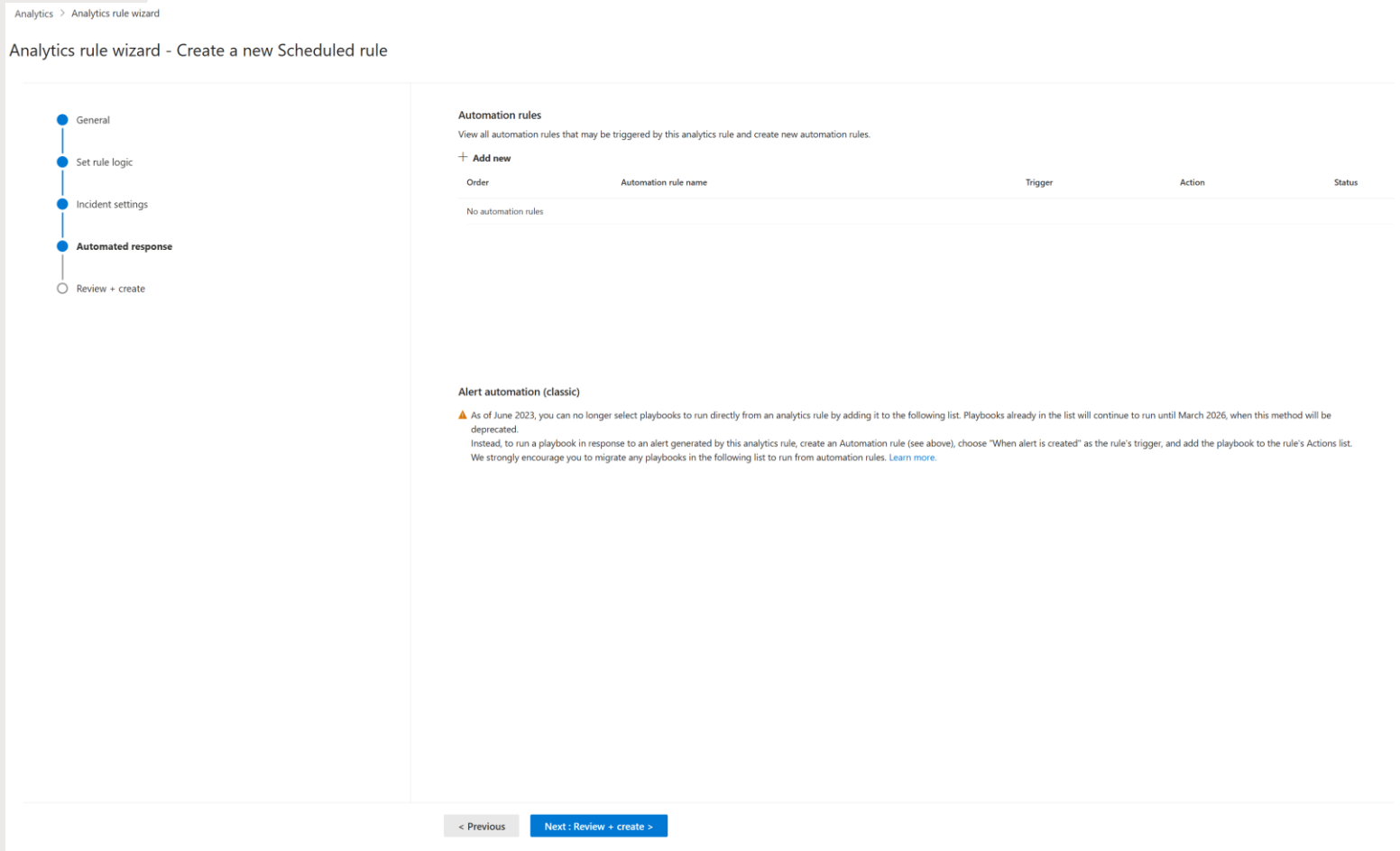
- Enable: **Create incidents from alerts triggered by this rule**
- Leave **Alert grouping** as default (Disabled)




PerparimLabs

# Automated Response

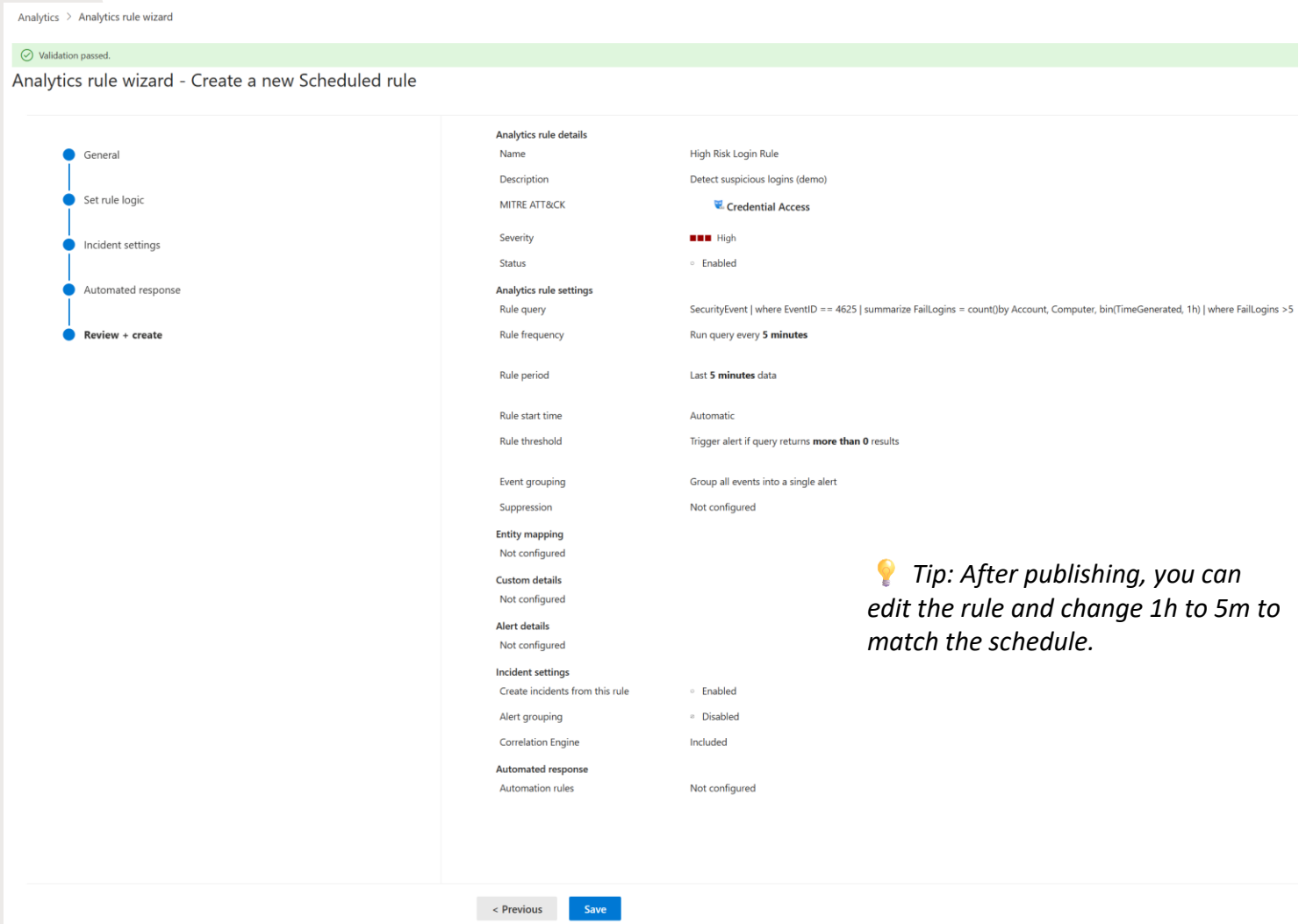
- Skip adding automation rules for now
- Click **Next: Review + create**




PerparimLabs

# Review and Create

- Review all settings
- Click **Create** to deploy the rule

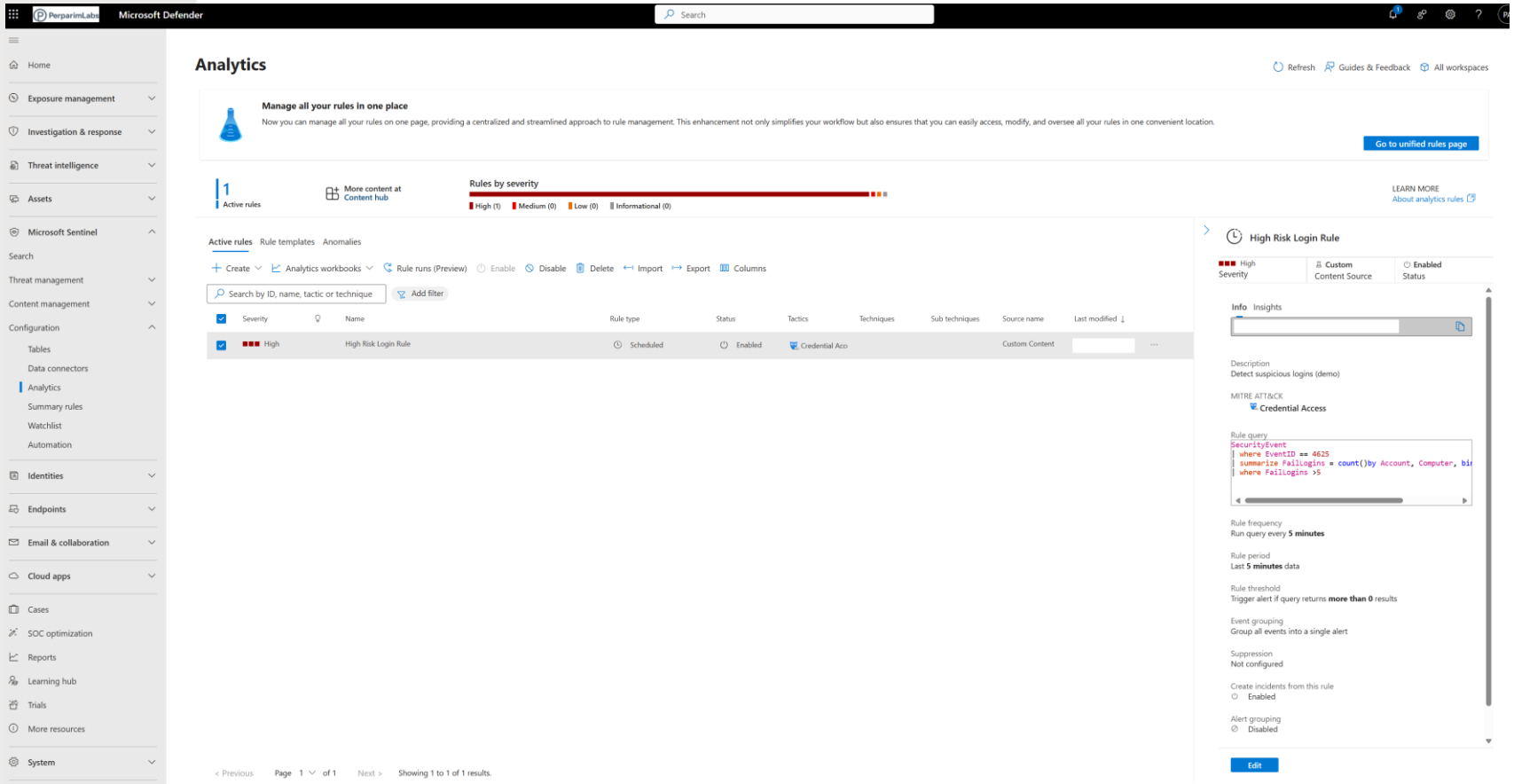



💡 *Tip: After publishing, you can edit the rule and change 1h to 5m to match the schedule.*

PerparimLabs

# Rule Created Successfully

- Confirm your rule is listed under **Active rules**
- Status: Enabled
- Severity: High
- Type: Scheduled




Your rule is now active ✅
It will run your query every 5 minutes and generate alerts if suspicious logins appear in the data.

PerparimLabs

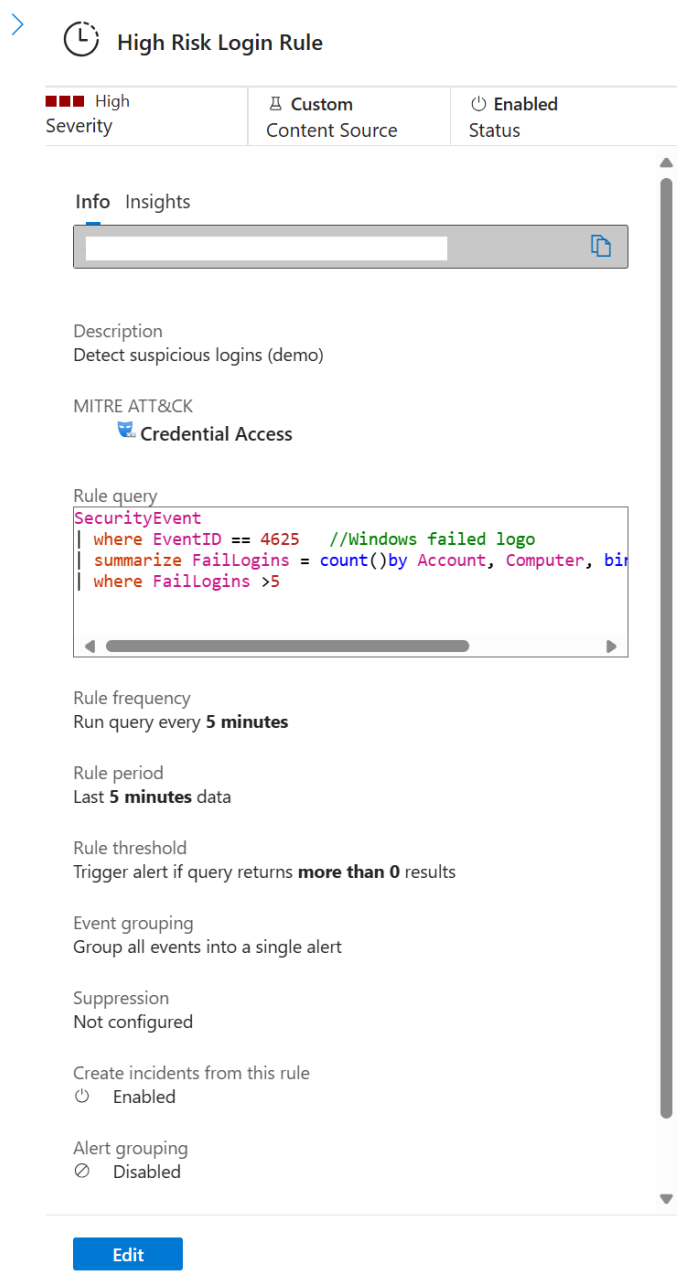
# 🛠 Optimize Your Rule

**Refine your KQL to match your schedule**

- Go back to your created rule → **Edit**
- Replace the old query (1h bin) with the optimized one (5m bin)

```
SecurityEvent
| where EventID == 4625 //
  Windows failed logon
| summarize FailLogins =
  count() by Account,
  Computer, bin(TimeGenerated,
  5m)
| where FailLogins > 5
```

📌 **Best Practice:** Always match your `bin()` time to your rule schedule for accurate results.




PerparimLabs