Build an NRT Analytics Rule

Real-Time Threat Detection with Microsoft Sentinel

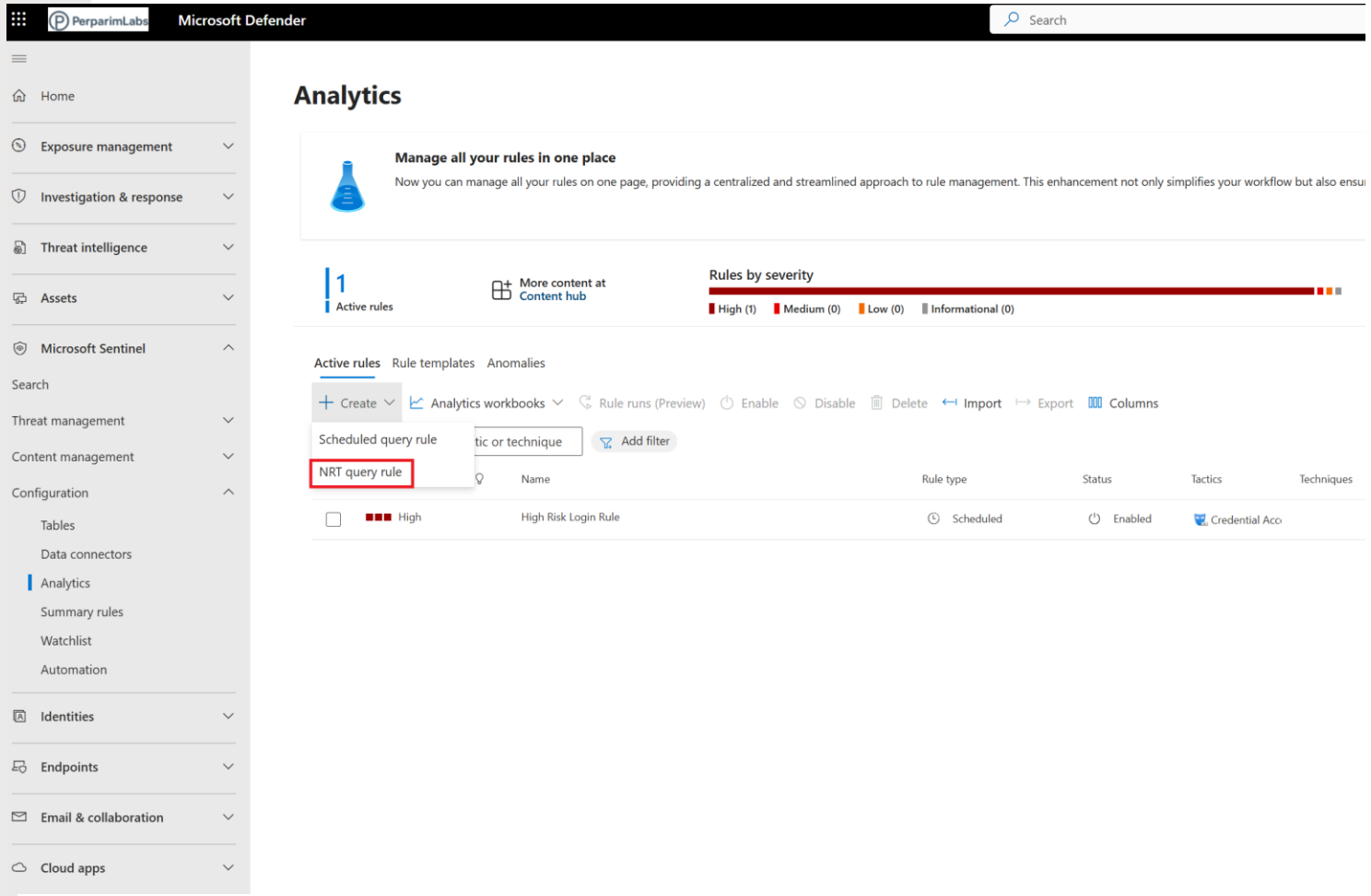
- **NRT (Near Real-Time) rules** trigger on *every single event* with almost **zero delay**
- Ideal for **high-risk signals** that can't wait for scheduled rule intervals
- Unlike Scheduled rules that run every 5 mins, NRT rules fire **instantly** when data is ingested
- Best used for **critical sign-ins, privileged actions, or malware detections**
- Powered by Kusto Query Language (KQL) for precise event logic
- Sentinel is the SIEM workspace; Defender XDR is the unified SecOps portal where rules now live.

💡 **Pro Insight:** Use NRT only for **low-volume, high-value** detections — they can be expensive if triggered often.

PerparimLabs

Navigate to Analytics

- Open **Microsoft Azure portal → Microsoft Sentinel**
- Select your **Sentinel workspace**
- Under **Configuration**, click **Analytics**
- This will open the **Microsoft Defender XDR** portal
- In Microsoft Defender XDR, click **Create → NRT query rule**

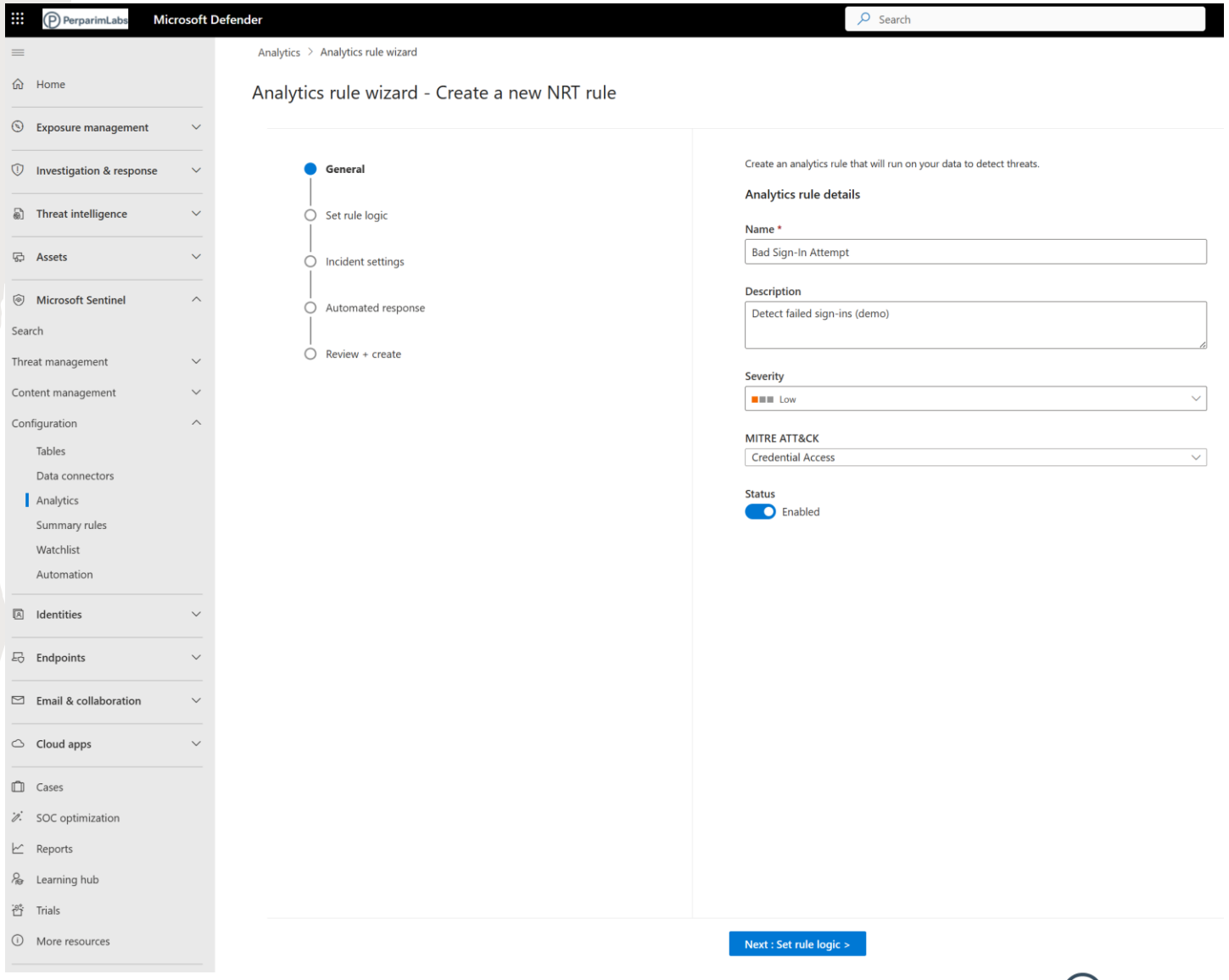


📌 *NRT = Near Real-Time — triggers on every event*

PerparimLabs

Define Rule Basics

- **Name:** Bad Sign-In Attempt
- **Description:** Detect failed sign-ins (demo)
- **Severity:** Low
- **MITRE ATT&CK:** Credential Access
- **Status:** Enabled



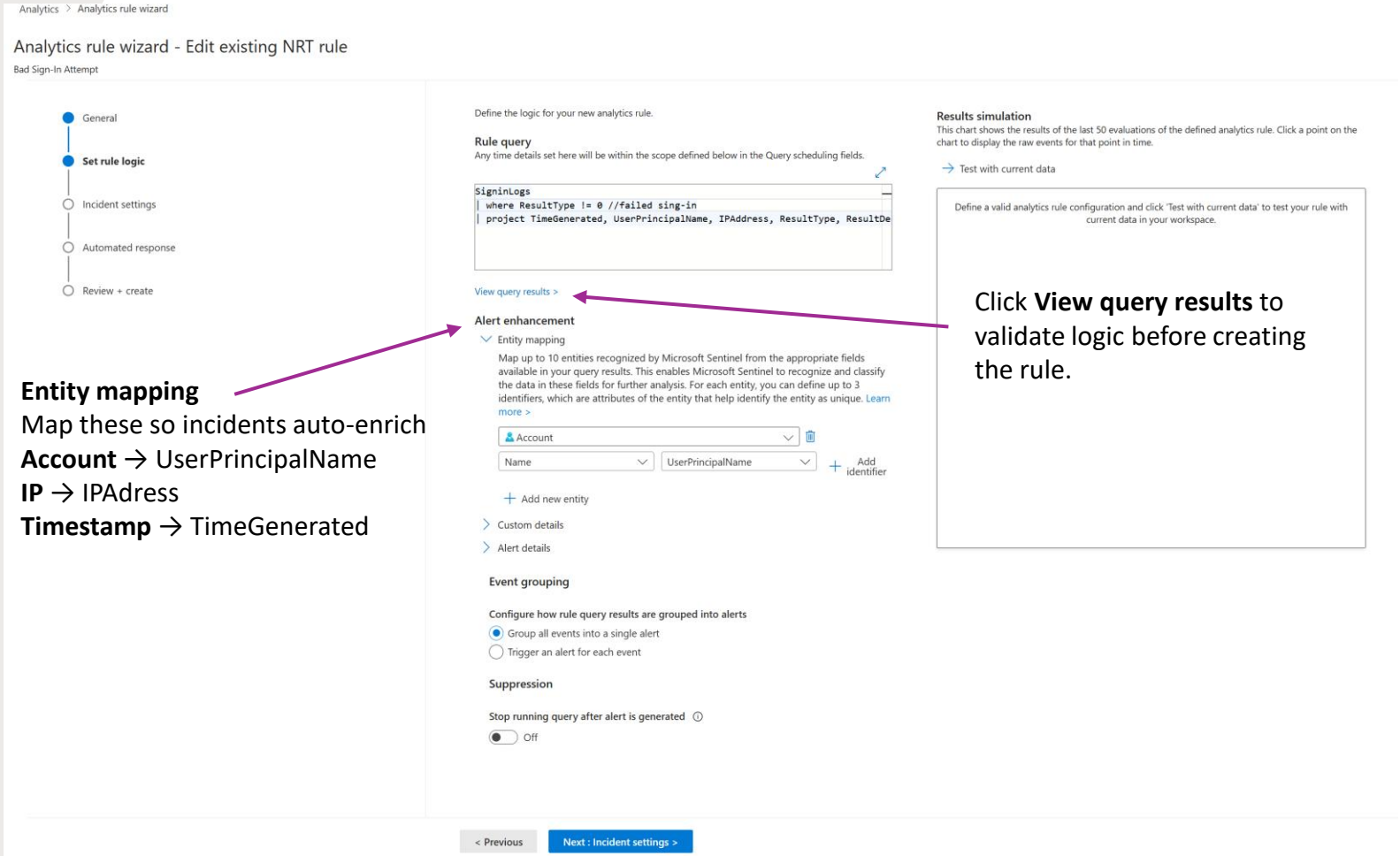
PerparimLabs

Write the KQL Query

- Use this query to detect failed sign-ins:

```
SigninLogs
| where ResultType != 0
| project TimeGenerated, UserPrincipalName, IPAddress, ResultType, ResultDescription
```

- Runs on every event (no schedule needed)
- Click **View query results** to test



Entity mapping
Map these so incidents auto-enrich
Account → UserPrincipalName
IP → IPAdress
Timestamp → TimeGenerated

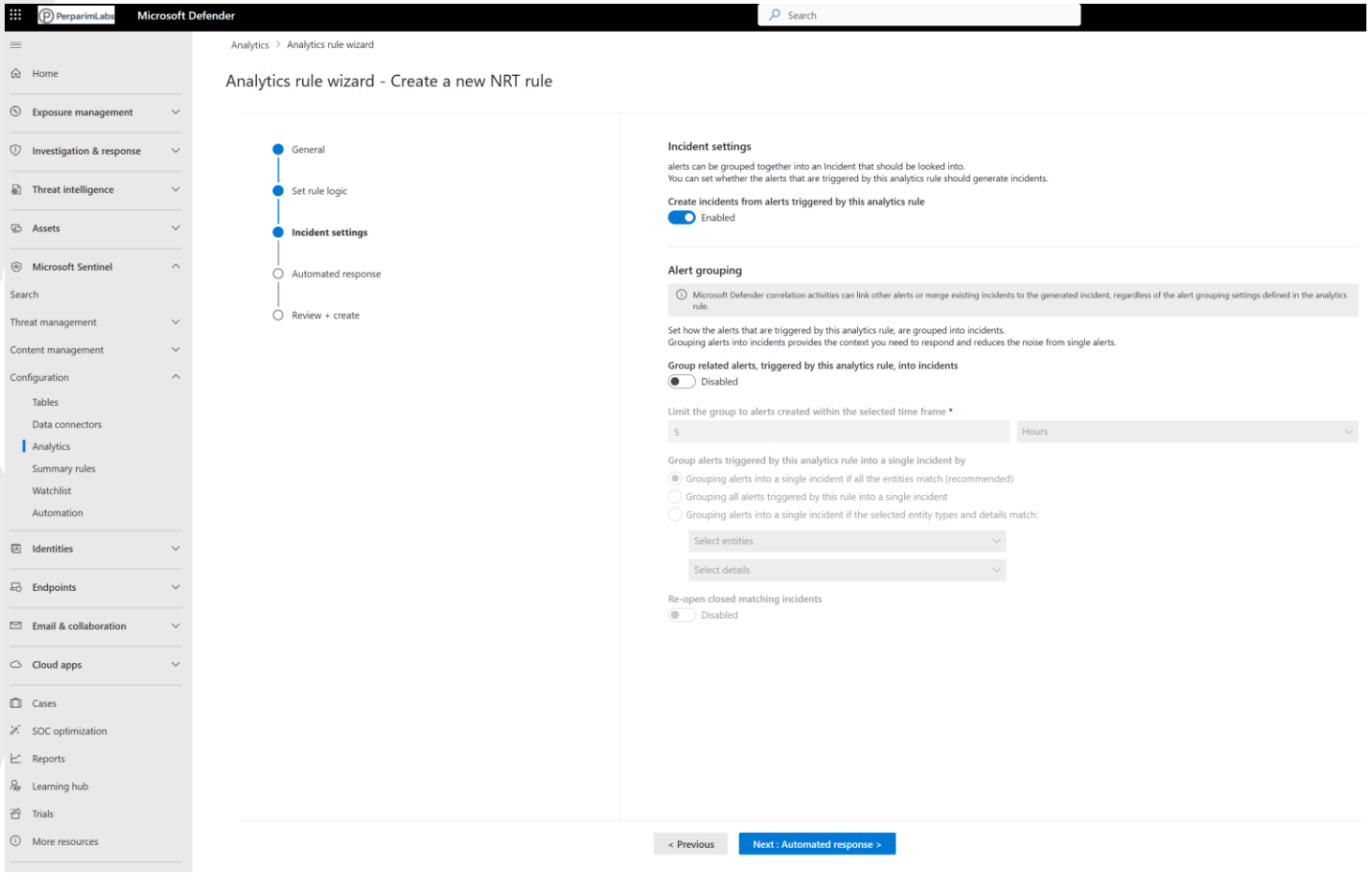
Click **View query results** to validate logic before creating the rule.

💡 *This runs immediately on every SigninLogs event ingested.*

PerparimLabs

Enable Incident Creation

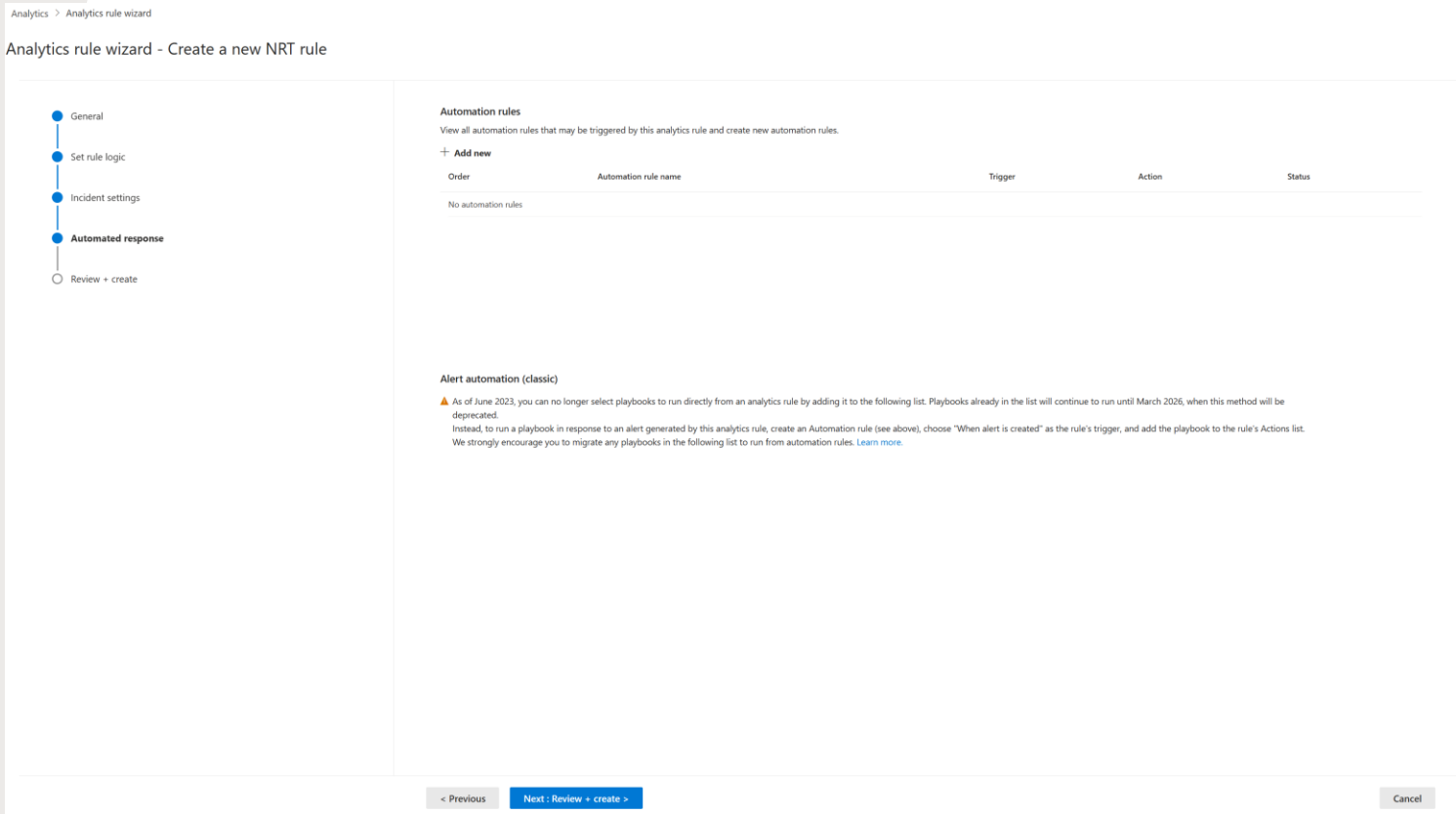
- Enable **Create incidents from alerts**
- Keep **Group related alerts** disabled
- This lets each alert create a new incident



PerparimLabs

Attach Automation (Optional)

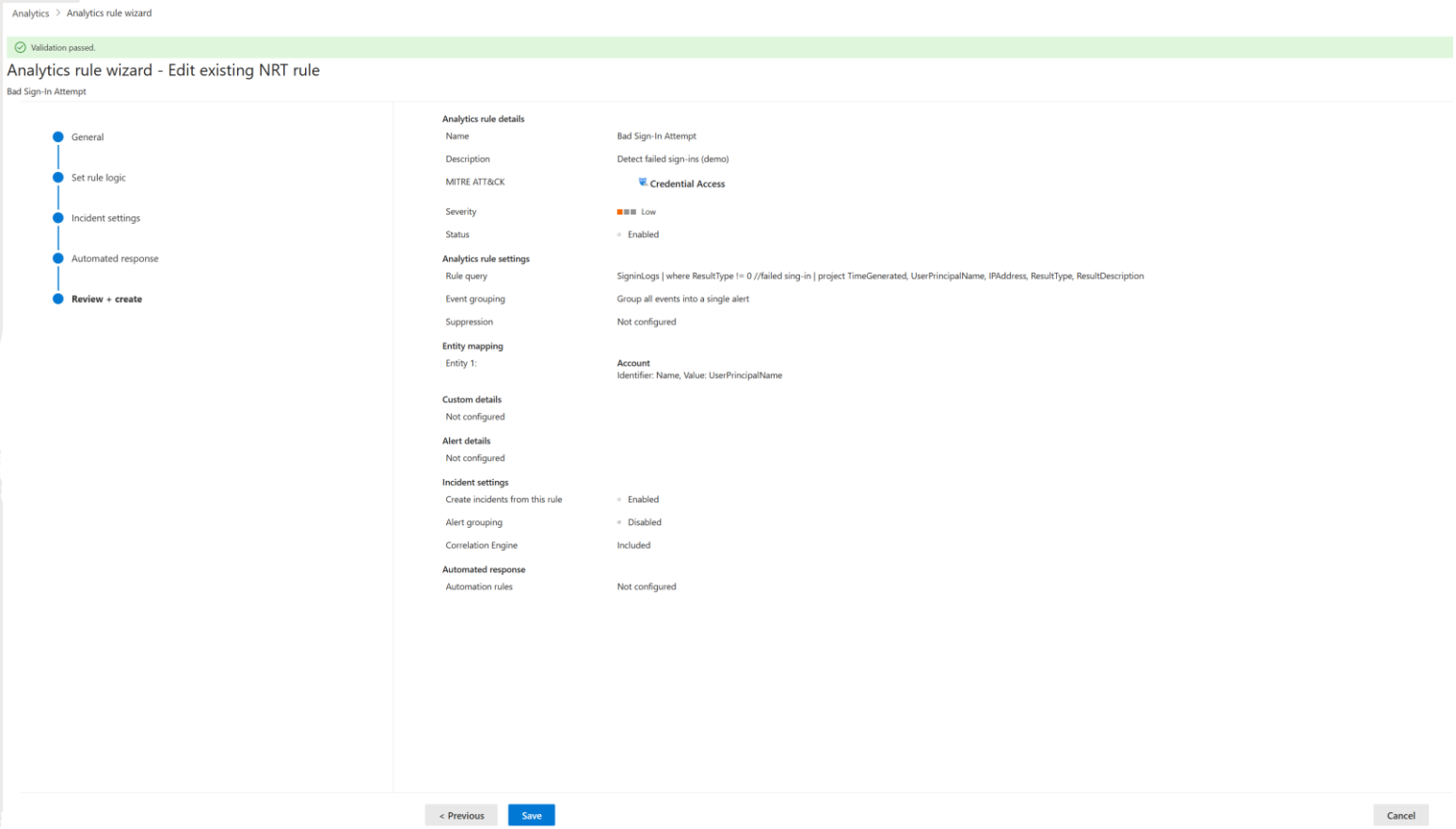
- You can link automation rules or playbooks
- We'll skip this for now



PerparimLabs

Review and Deploy

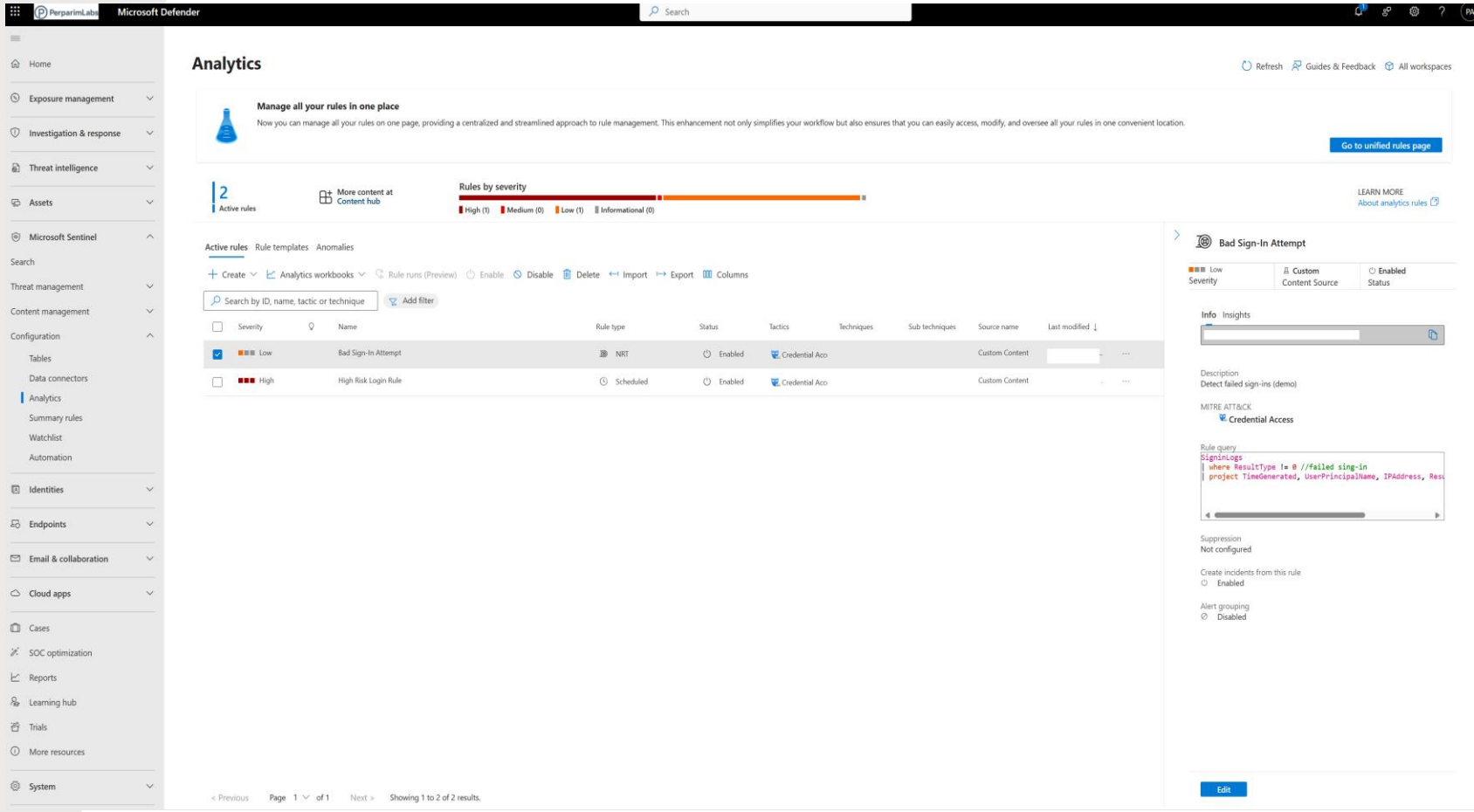
- Review all rule settings
- Click **Create** to deploy your NRT rule



PerparimLabs

Rule is Live

- Go to **Analytics → Active rules**
- Confirm:
  - **Type:** NRT
  - **Severity:** Low
  - **Status:** Enabled
- Your rule will now trigger on **every bad sign-in attempt**



NRT fires on every event—use for low-volume, high-value detections to avoid noise & cost.

PerparimLabs

✅ NRT Rule Successfully Deployed

- Real-Time Detection — Powered by Microsoft Sentinel

- You just built an **NRT Analytics Rule** that triggers on **every failed sign-in**
- This enables **instant detection and response** for high-risk activity
- A core step in building a **proactive SOC strategy**
- Keep optimizing with KQL and automation playbooks

PerparimLabs