

Build Your First Analytics Rule in Microsoft Sentinel

Microsoft
CERTIFIED

EXPERT

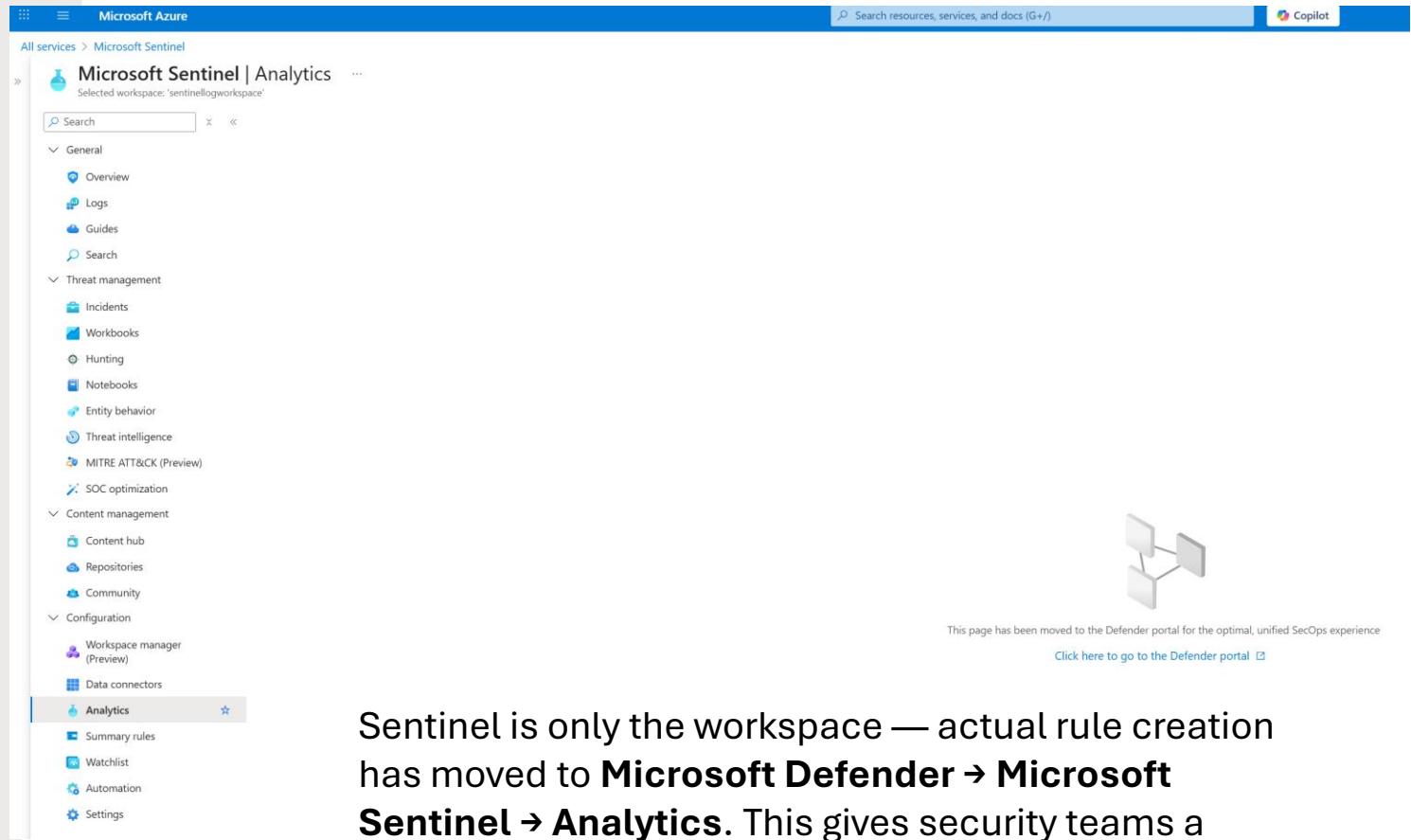


Detect high-risk logins with custom scheduled queries

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.

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



The screenshot shows the Microsoft Azure portal with the Microsoft Sentinel Analytics page. The left sidebar shows the Configuration menu with 'Analytics' selected. A message at the bottom right indicates the page has been moved to the Microsoft Defender portal for the optimal, unified SecOps experience. A 'Click here to go to the Defender portal' link is also present.

Microsoft Azure

Microsoft Sentinel | Analytics

Selected workspace: 'sentinellogworkspace'

Search

General

- Overview
- Logs
- Guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)
- SOC optimization

Content management

- Content hub
- Repositories
- Community

Configuration

- Workspace manager (Preview)
- Data connectors
- Analytics *
- Summary rules
- Watchlist
- Automation
- Settings

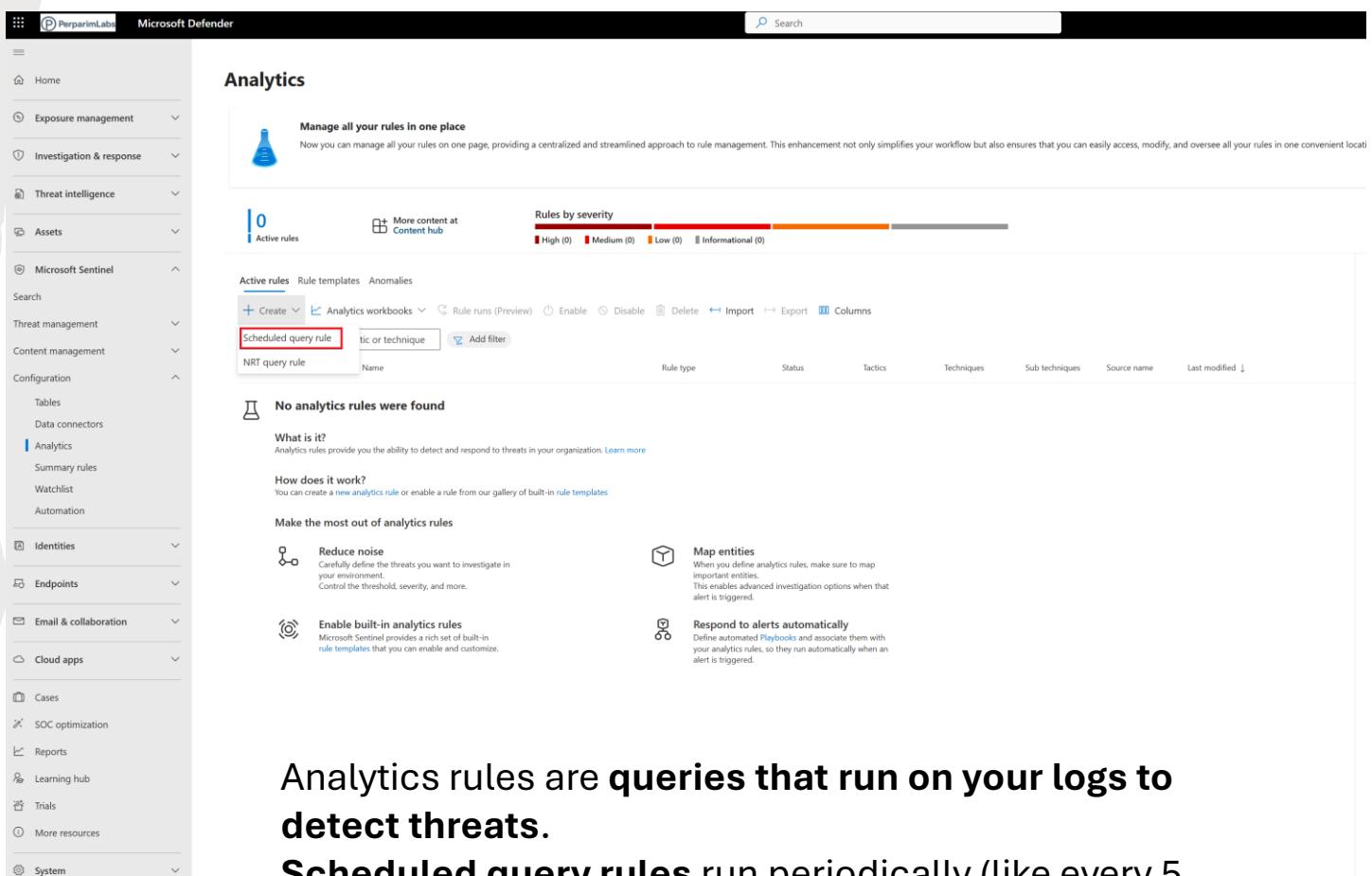
This page has been moved to the Defender portal for the optimal, unified SecOps experience

Click here to go to the 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.

Create a Scheduled Query Rule

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



The screenshot shows the Microsoft Defender Analytics page. The left sidebar includes sections for Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Identities, Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, More resources, and System. The main content area is titled 'Analytics' and features a heading 'Manage all your rules in one place'. It shows '0 Active rules' and a 'Rules by severity' bar with counts for High (0), Medium (0), Low (0), and Informational (0). Below this is a table with columns for Rule type, Status, Tactics, Techniques, Sub techniques, Source name, and Last modified. A red box highlights the 'Scheduled query rule' button in the 'Create' dropdown menu. The page also includes sections for 'What is it?', 'How does it work?', 'Make the most out of analytics rules', and 'Analytics rules are queries that run on your logs to detect threats.'

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**.

General Settings

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

Analytics > Analytics rule wizard

Analytics rule wizard - Create a new Scheduled rule

General

- General
- Set rule logic
- Incident settings
- Automated response
- Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *
High Risk Login Rule

Description
Detect suspicious logins (demo)

Severity
■■■ High

MITRE ATT&CK
Credential Access

Status
 Enabled

[Next : Set rule logic >](#)

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**

Analytics > Analytics rule wizard

Analytics rule wizard - Create a new Scheduled rule

Any time details set here will be within the scope defined below in the Query scheduling fields.

General

Set rule logic

Incident settings

Automated response

Review + create

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

[View query results >](#)

Alert enhancement

Entity mapping

Custom details

Alert details

Query scheduling

Run query every *

5 Minutes

Lookup data from the last *

5 Minutes

Start running

Automatically (radio button selected)

At specific time (Preview)

12:00 PM

Starting automatically, the rule will run every 5 minutes, looking up data from last 5 minutes.

Alert threshold

Generate alert when number of query results *

Is greater than 0

Event grouping

Configure how rule query results are grouped into alerts

Group all events into a single alert (radio button selected)

Trigger an alert for each event

Suppression

[Next : Incident settings >](#)

Test with current data

Define a valid analytics rule configuration and click 'Test with current data' to test your rule with current data in your workspace.

⚡ **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.

Incident Settings

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

Analytics > Analytics rule wizard

Analytics rule wizard - Create a new Scheduled rule

General
Set rule logic
Incident settings
Automated response
Review + create

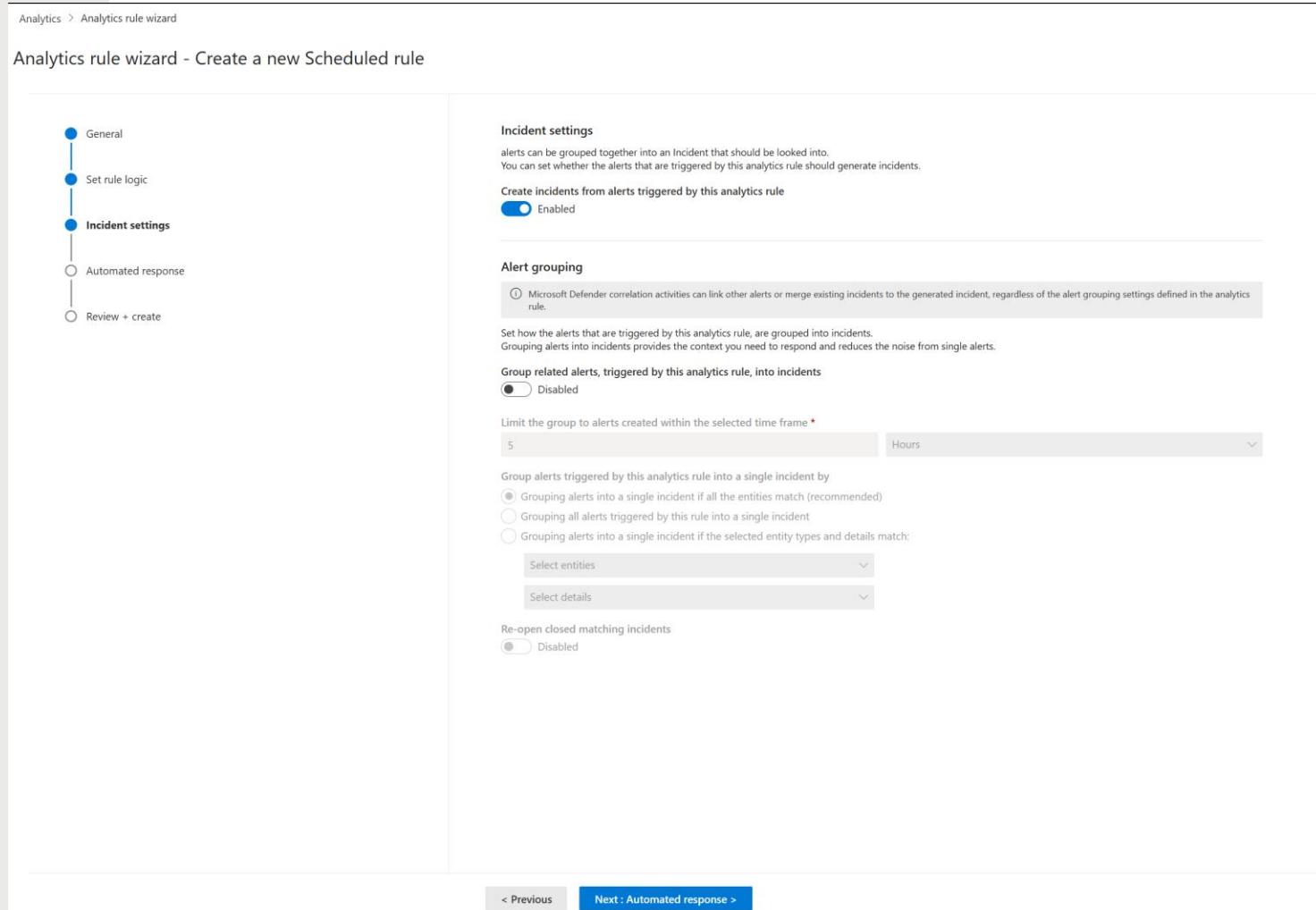
Incident settings
alerts can be grouped together into an incident that should be looked into.
You can set whether the alerts that are triggered by this analytics rule should generate incidents.
Create incidents from alerts triggered by this analytics rule
 Enabled

Alert grouping
Microsoft Defender correlation activities can link other alerts or merge existing incidents to the generated incident, regardless of the alert grouping settings defined in the analytics rule.
Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.
Group related alerts, triggered by this analytics rule, into incidents
 Disabled
Limit the group to alerts created within the selected time frame *
5 Hours

Group alerts triggered by this analytics rule into a single incident by
 Grouping alerts into a single incident if all the entities match (recommended)
 Grouping all alerts triggered by this rule into a single incident
 Grouping alerts into a single incident if the selected entity types and details match:
Select entities
Select details

Re-open closed matching incidents
 Disabled

< Previous **Next : Automated response >**



Automated Response

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

Analytics > Analytics rule wizard

Analytics rule wizard - Create a new Scheduled rule

General

Set rule logic

Incident settings

Automated response

Review + create

Automation rules

View all automation rules that may be triggered by this analytics rule and create new automation rules.

+ Add new

Order	Automation rule name	Trigger	Action	Status
No automation rules				

Alert automation (classic)

⚠ As of June 2023, you can no longer select playbooks to run directly from an analytics rule by adding it to the following list. Playbooks already in the list will continue to run until March 2026, when this method will be deprecated.

Instead, to run a playbook in response to an alert generated by this analytics rule, create an Automation rule (see above), choose "When alert is created" as the rule's trigger, and add the playbook to the rule's Actions list. We strongly encourage you to migrate any playbooks in the following list to run from automation rules. [Learn more](#).

< Previous

Next : Review + create >

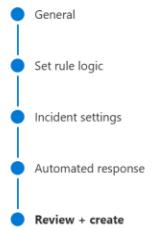
Review and Create

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

Analytics > Analytics rule wizard

Validation passed.

Analytics rule wizard - Create a new Scheduled rule



```
graph TD; A[General] --> B[Set rule logic]; B --> C[Incident settings]; C --> D[Automated response]; D --> E[Review + create];
```

Analytics rule details

Name	High Risk Login Rule
Description	Detect suspicious logins (demo)
MITRE ATT&CK	 Credential Access
Severity	 High
Status	<input type="radio"/> Enabled

Analytics rule settings

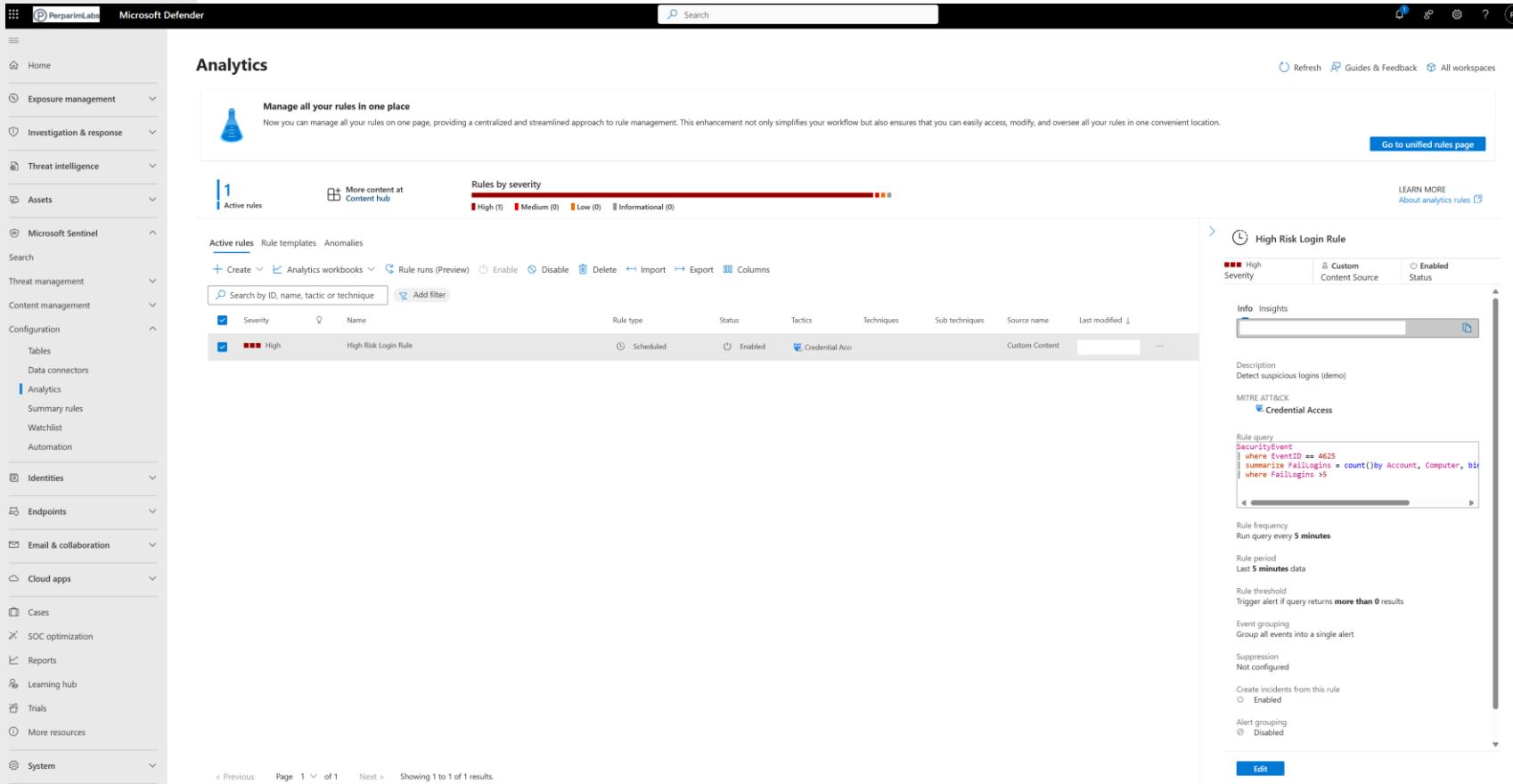
Rule query	SecurityEvent where EventID == 4625 summarize FailLogins = count() by Account, Computer, bin(TimeGenerated, 1h) where FailLogins > 5
Rule frequency	Run query every 5 minutes
Rule period	Last 5 minutes data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns more than 0 results
Event grouping	Group all events into a single alert
Suppression	Not configured
Entity mapping	Not configured
Custom details	Not configured
Alert details	Not configured
Incident settings	<input type="radio"/> Enabled
Alert grouping	<input type="radio"/> Disabled
Correlation Engine	Included
Automated response	Automation rules
Automation rules	Not configured

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

< Previous Save

Rule Created Successfully

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



The screenshot shows the Microsoft Defender Analytics interface. The left sidebar includes sections for Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Tables, Data connectors, Analytics (selected), Summary rules, Watchlist, Automation, Identities, Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, and System. The main content area is titled 'Analytics' and features a sub-section 'Manage all your rules in one place'. It shows 1 Active rule, a 'Rules by severity' chart with a single High severity rule, and a table of rules. The table includes columns for Severity (High), Name (High Risk Login Rule), Rule type (Scheduled), Status (Enabled), Tactics (Credential Access), Techniques, Sub techniques, Source name, and Last modified. The right side of the interface displays the details for the 'High Risk Login Rule', including its description ('Detect suspicious logins (demo)'), MITRE ATT&CK ('Credential Access'), rule query ('SecurityEvent | where EventID == 4625 | summarize FailLogins = count() by Account, Computer, bin | where FailLogins > 5'), rule frequency ('Run query every 5 minutes'), rule period ('Last 5 minutes data'), rule threshold ('Trigger alert if query returns more than 0 results'), event grouping ('Group all events into a single alert'), suppression ('Not configured'), and alert grouping ('Disabled').

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

🛠 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.

>  **High Risk Login Rule**

<input checked="" type="checkbox"/> High Severity	<input type="checkbox"/> Custom Content Source	<input type="checkbox"/> Enabled Status
---	--	---

Info Insights

Description
Detect suspicious logins (demo)

MITRE ATT&CK
 Credential Access

Rule query

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

Rule frequency
Run query every **5 minutes**

Rule period
Last **5 minutes** data

Rule threshold
Trigger alert if query returns **more than 0** results

Event grouping
Group all events into a single alert

Suppression
Not configured

Create incidents from this rule
 Enabled

Alert grouping
 Disabled

Edit