

Build Your First Analytics Rule in Microsoft Sentinel

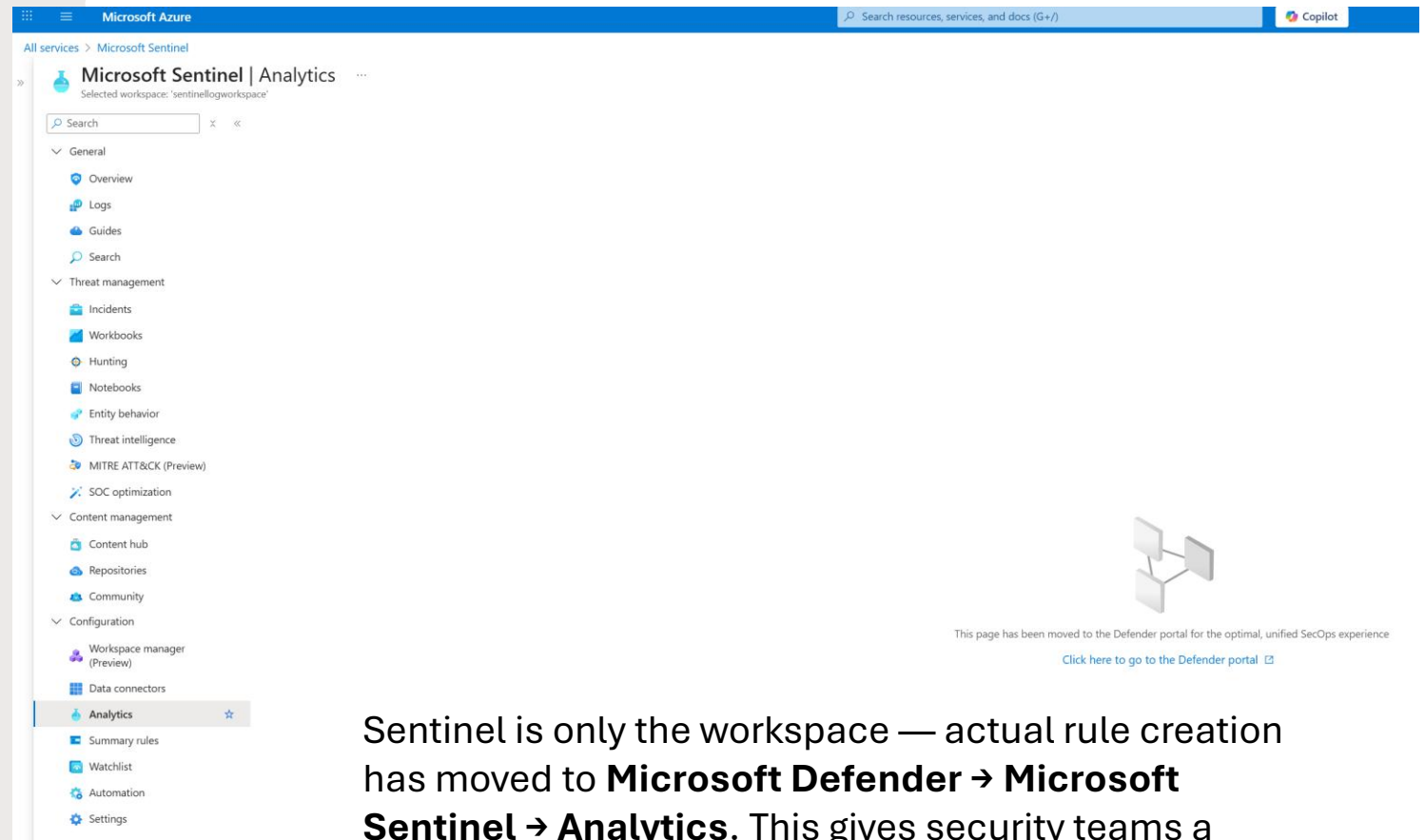
Detect high-risk logins with custom scheduled queries



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.

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.

Create a Scheduled Query Rule

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

The screenshot displays the Microsoft Defender Analytics interface. On the left, the navigation pane includes sections like 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 'Analytics' section is active, showing a 'Manage all your rules in one place' header. Below this, there's a 'Rules by severity' bar and a table of active rules. The 'Create' button is visible, and the 'Scheduled query rule' option is highlighted in the dropdown menu. The table below shows one rule, 'NRT query rule', with columns for Name, Rule type, Status, Tactics, Techniques, Sub techniques, Source name, and Last modified.

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

The screenshot displays the 'Analytics rule wizard' interface. On the left, a vertical navigation pane shows five steps: 'General' (selected with a blue dot), 'Set rule logic', 'Incident settings', 'Automated response', and 'Review + create'. The main content area is titled 'Create an analytics rule that will run on your data to detect threats.' and 'Analytics rule details'. It contains the following fields: 'Name' (text input with 'High Risk Login Rule'), 'Description' (text area with 'Detect suspicious logins (demo)'), 'Severity' (dropdown menu showing 'High' with three red squares), 'MITRE ATT&CK' (dropdown menu showing 'Credential Access'), and 'Status' (toggle switch labeled 'Enabled'). At the bottom right, there is a blue button labeled 'Next : Set rule logic >'. The PerparimLabs logo is in the bottom right corner.

- **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

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

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

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

```
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 * Minutes

Lookup data from the last * Minutes

Start running ⓘ

☒ Automatically

☐ At specific time (Preview)

ⓘ 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

Event grouping

Configure how rule query results are grouped into alerts

☒ Group all events into a single alert

☐ Trigger an alert for each event

Summary

< Previous **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

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

Analytics rule details

NameHigh Risk Login Rule

DescriptionDetect suspicious logins (demo)

MITRE ATT&CKCredential Access

SeverityHigh

StatusEnabled

Analytics rule settings

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

Rule frequencyRun query every 5 minutes

Rule periodLast 5 minutes data

Rule start timeAutomatic

Rule thresholdTrigger alert if query returns more than 0 results

Event groupingGroup all events into a single alert

SuppressionNot configured

Entity mapping

Not configured

Custom details

Not configured

Alert details

Not configured

Incident settings

Create incidents from this ruleEnabled

Alert groupingDisabled

Correlation EngineIncluded

Automated response

Automation rulesNot configured

< Previous Save

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

Rule Created Successfully

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

The screenshot displays the Microsoft Defender Analytics interface. On the left is a navigation pane with categories like 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 area is titled 'Analytics' and features a 'Manage all your rules in one place' section. Below this, a 'Rules by severity' bar shows 1 High rule, 0 Medium, 0 Low, and 0 Informational rules. A table lists active rules, with one rule visible: 'High Risk Login Rule' with a severity of High, status of Enabled, and type of Scheduled. To the right, a detailed view of the 'High Risk Login Rule' is shown, including its description 'Detect suspicious logins (demo)', MITRE ATT&CK category 'Credential Access', a KQL rule query, and configuration settings for frequency (5 minutes), period (5 minutes), threshold (more than 0 results), and suppression (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**


High Severity

Custom Content Source

Enabled Status

Info Insights

Description
Detect suspicious logins (demo)

MITRE ATT&CK
 Credential Access

Rule query

```
SecurityEvent  
| where EventID == 4625 //Windows failed logon  
| 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

Create incidents from this rule
☒ Enabled

Alert grouping
☐ Disabled

Edit