

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.

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**

The screenshot displays the Microsoft Defender XDR Analytics interface. The left sidebar contains a navigation menu with the following items: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Identities, Endpoints, Email & collaboration, and Cloud apps. The 'Configuration' section is expanded, showing 'Tables', 'Data connectors', 'Analytics', 'Summary rules', 'Watchlist', and 'Automation'. The 'Analytics' section is selected, showing a '1 Active rules' indicator and a 'Rules by severity' bar chart. The 'Create' button is highlighted with a red box, and a dropdown menu is open showing 'Scheduled query rule' and 'NRT query rule'. The 'NRT query rule' option is highlighted with a red box. Below the dropdown, a table of active rules is shown with columns: Name, Rule type, Status, Tactics, and Techniques. The table contains one rule, 'High Risk Login Rule', with a severity of 'High' and status 'Enabled'.

Name	Rule type	Status	Tactics	Techniques
High Risk Login Rule	Scheduled	Enabled	Credential Acc	

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

Define Rule Basics

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

Microsoft Defender

Analytics > Analytics rule wizard

Analytics rule wizard - Create a new NRT rule

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 *

Bad Sign-In Attempt

Description

Detect failed sign-ins (demo)

Severity

Low

MITRE ATT&CK

Credential Access

Status

Enabled

Next : Set rule logic >

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

Analytics > Analytics rule wizard

Analytics rule wizard - Edit existing NRT rule

Bad Sign-In Attempt

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

Define the logic for your new analytics rule.

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

```
SigninLogs  
| where ResultType != 0 //failed sign-in  
| project TimeGenerated, UserPrincipalName, IPAddress, ResultType, ResultDe
```

[View query results >](#)

Alert enhancement
Entity mapping
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

Account [Add identifier](#)

[+ Add new entity](#)

[Custom details](#)
[Alert details](#)

Event grouping
Configure how rule query results are grouped into alerts
☒ Group all events into a single alert
☐ Trigger an alert for each event

Suppression
Stop running query after alert is generated ☐
☒ Off

Results simulation
This chart shows the results of the last 50 evaluations of the defined analytics rule. Click a point on the chart to display the raw events for that point in time.

[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.

< Previous Next: Incident settings >



This runs immediately on every SigninLogs event ingested.

Enable Incident Creation

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

The screenshot shows the Microsoft Defender console 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, and More resources. The 'Analytics' section is expanded. The main area displays the 'Analytics rule wizard - Create a new NRT rule' with a progress bar showing steps: General, Set rule logic, Incident settings (current), Automated response, and Review + create. The 'Incident settings' section includes a toggle for 'Create incidents from alerts triggered by this analytics rule' which is set to 'Enabled'. Below this is the 'Alert grouping' section, which contains a warning about correlation activities, instructions on how alerts are grouped, and a toggle for 'Group related alerts, triggered by this analytics rule, into incidents' which is set to 'Disabled'. There are also dropdowns for 'Limit the group to alerts created within the selected time frame' (set to 5 hours) and 'Group alerts triggered by this analytics rule into a single incident by' (set to 'Grouping alerts into a single incident if all the entities match (recommended)'). At the bottom, there are navigation buttons: '< Previous' and 'Next : Automated response >'. The PerparimLabs logo is visible in the top left corner of the interface.

Attach Automation (Optional)

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

Analytics > Analytics rule wizard

Analytics rule wizard - Create a new NRT 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 >

Cancel

Review and Deploy

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

Analytics > Analytics rule wizard

Validation passed.

Analytics rule wizard - Edit existing NRT rule

Bad Sign-In Attempt

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

Analytics rule details

Name

Bad Sign-In Attempt

Description

Detect failed sign-ins (demo)

MITRE ATT&CK

Credential Access

Severity

Low

Status

Enabled

Analytics rule settings

Rule query

SignInLogs | where ResultType != 0 //failed sign-in | project TimeGenerated, UserPrincipalName, IPAddress, ResultType, ResultDescription

Event grouping

Group all events into a single alert

Suppression

Not configured

Entity mapping

Entity 1:

Account
Identifier: Name, Value: UserPrincipalName

Custom details

Not configured

Alert details

Not configured

Incident settings

Create incidents from this rule

Enabled

Alert grouping

Disabled

Correlation Engine

Included

Automated response

Automation rules

Not configured

< Previous

Save

Cancel

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**

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 is a 'Rules by severity' bar chart and a table of active rules. The table has columns for Severity, Name, Rule type, Status, Tactics, Techniques, Sub techniques, Source name, and Last modified. Two rules are listed: 'Bad Sign-In Attempt' (Low severity, NRT type, Enabled status) and 'High Risk Login Rule' (High severity, Scheduled type, Enabled status). The 'Bad Sign-In Attempt' rule is selected, and its details are shown on the right. These details include the rule's name, severity, status, and a 'Rule query' section containing a KQL query: `SigninLogs | where ResultType != 0 //failed sign-in | project TimeGenerated, UserPrincipalName, IPAddress, Res`. Other configuration options like 'Suppression', 'Create incidents from this rule', and 'Alert grouping' are also visible.

Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
Low	Bad Sign-In Attempt	NRT	Enabled	Credential Acc			Custom Content	
High	High Risk Login Rule	Scheduled	Enabled	Credential Acc			Custom Content	

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

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