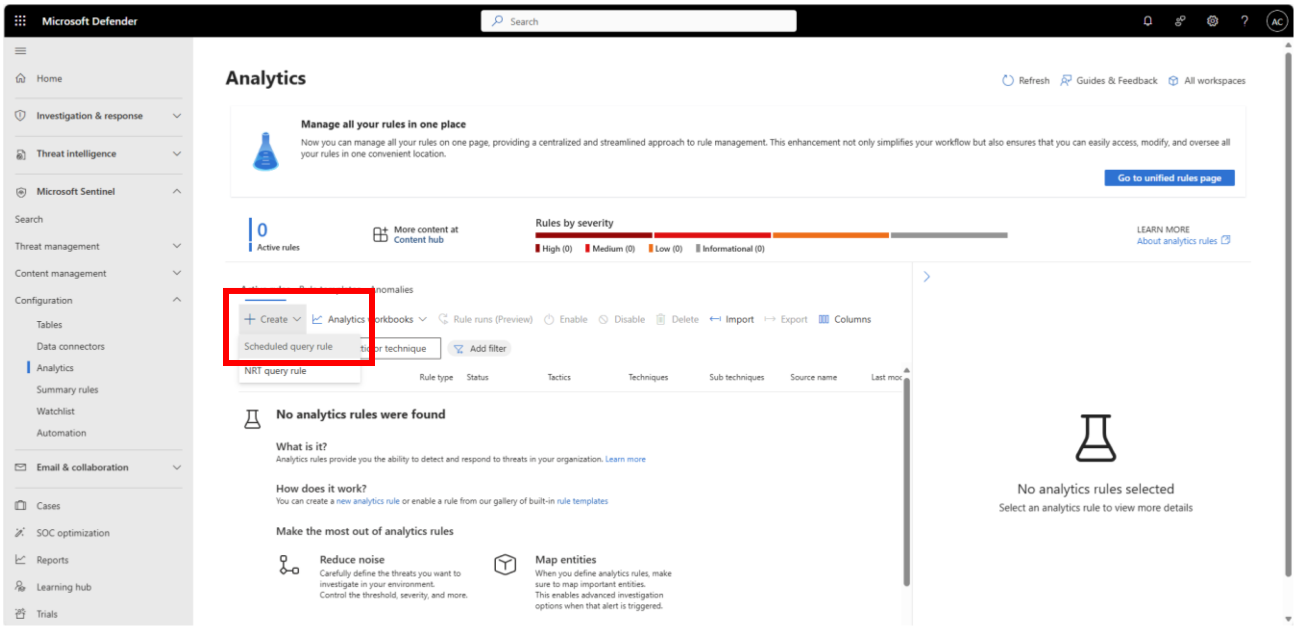
Threat Detection (Analytics) in Microsoft Sentinel

Adrian Cortez

Overview

Analytics in Microsoft Sentinel are automated rules and processes that analyze security data to detect suspicious activities or threats. They use built-in or custom queries to continuously monitor logs and trigger alerts, helping security teams identify and respond to potential attacks quickly and efficiently.

Schedule a Query Rule



Manage all your rules in one place

Now you can manage all your rules on one page, providing a centralized and streamlined approach to rule management. This enhancement not only simplifies your workflow but also ensures that you can easily access, modify, and oversee all your rules in one convenient location.

No analytics rules were found

What is it?
Analytics rules provide you the ability to detect and respond to threats in your organization. Learn more

How does it work?
You can create a new analytics rule or enable a rule from our gallery of built-in rule templates

Make the most out of analytics rules

Reduce noise
Carefully define the threats you want to investigate in your environment.
Control the threshold, severity, and more.

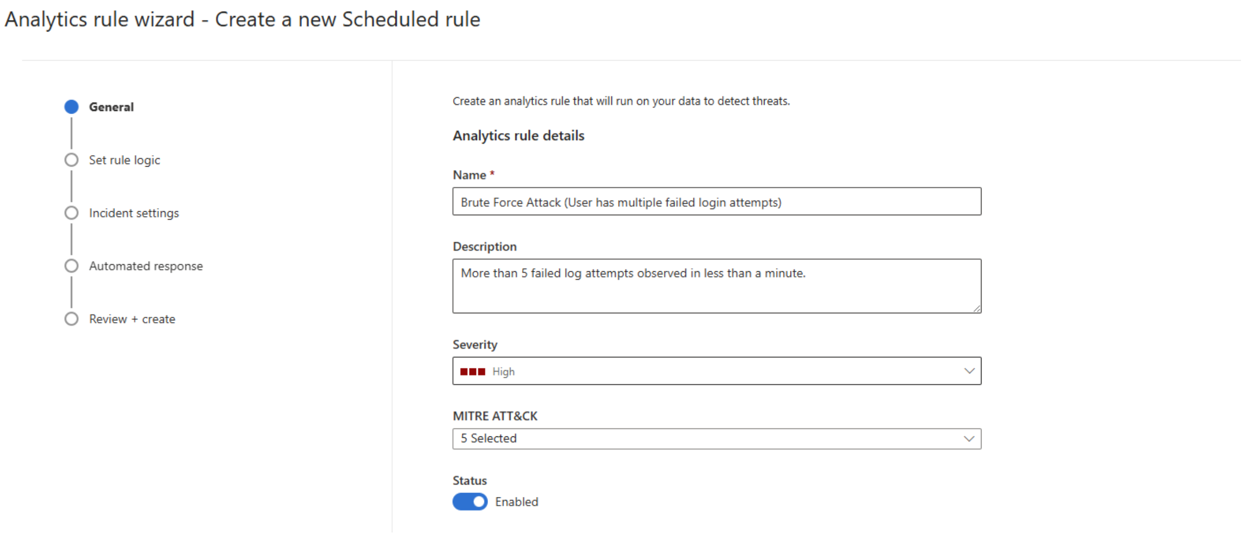
Map entities
When you define analytics rules, make sure to map important entities.
This enables advanced investigation options when that alert is triggered.

No analytics rules selected
Select an analytics rule to view more details

Describe the Rule (Ex: Brute Force)

1. Include severity and MITRE ATT&CK Technique
    a. MITRE ATT&CK is a globally recognized knowledge base that catalogs and describes the tactics, techniques, and procedures used by cyber attackers. It helps security professionals understand how adversaries operate, enabling better detection, prevention, and response to cyber threats by providing a detailed framework of attacker behaviors across different stages of an attack.
2. For MITRE ATT&CK, I selected initial access (attacker tries to gain entry) and credential access (attacker attempts to gain valid credentials)

a. T1110 - Brute Force
b. T1110.001 - Password Guessing
c. T1110.002 - Password Spraying



Analytics rule wizard - Create a new Scheduled 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

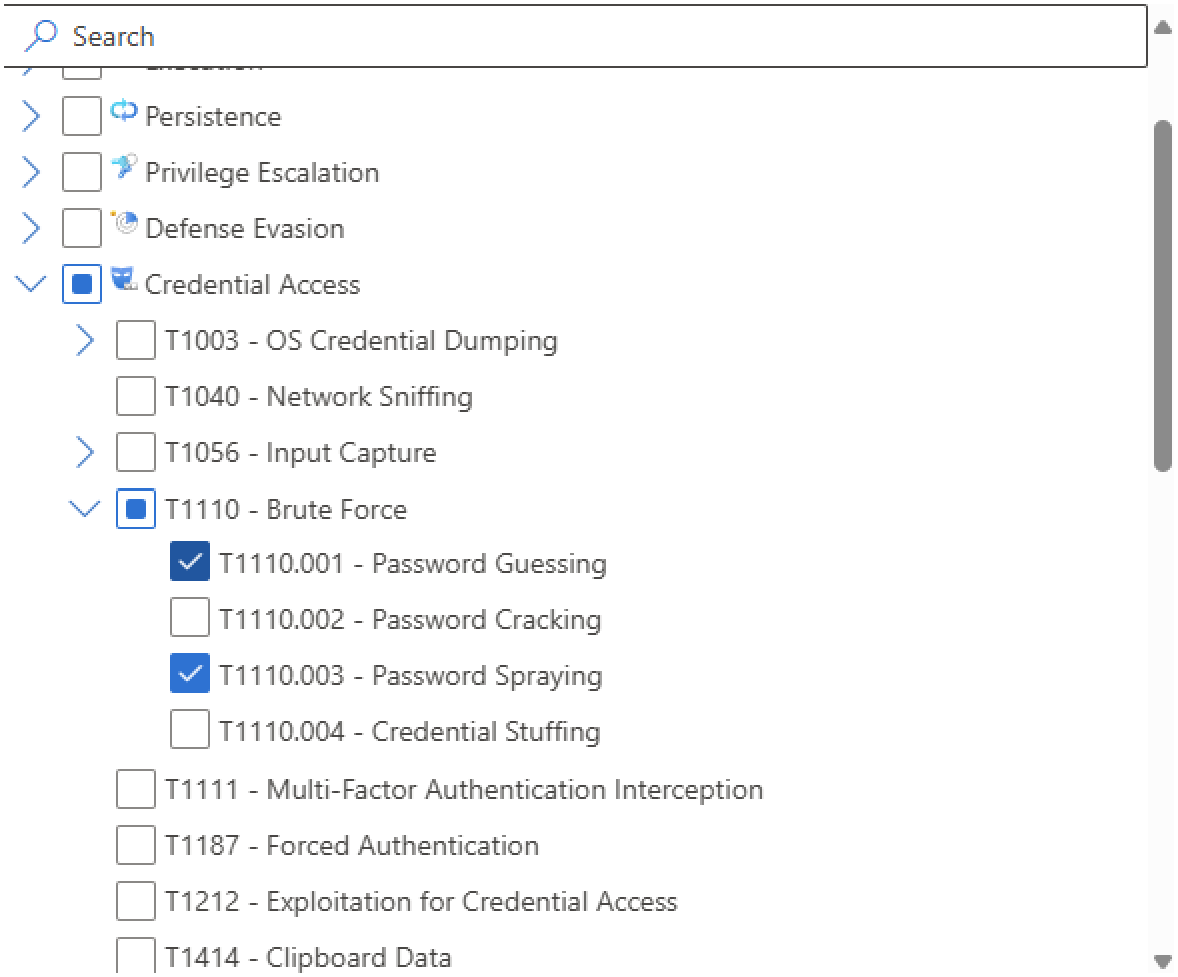
Name *
Brute Force Attack (User has multiple failed login attempts)

Description
More than 5 failed log attempts observed in less than a minute.

Severity
High

MITRE ATT&CK
5 Selected

Status
Enabled



Search

- ☐ Persistence
- ☐ Privilege Escalation
- ☐ Defense Evasion
- ■ Credential Access
  - ☐ T1003 - OS Credential Dumping
  - ☐ T1040 - Network Sniffing
  - ☐ T1056 - Input Capture
  - ■ T1110 - Brute Force
    - ☑ T1110.001 - Password Guessing
    - ☐ T1110.002 - Password Cracking
    - ☑ T1110.003 - Password Spraying
    - ☐ T1110.004 - Credential Stuffing
  - ☐ T1111 - Multi-Factor Authentication Interception
  - ☐ T1187 - Forced Authentication
  - ☐ T1212 - Exploitation for Credential Access
  - ☐ T1414 - Clipboard Data

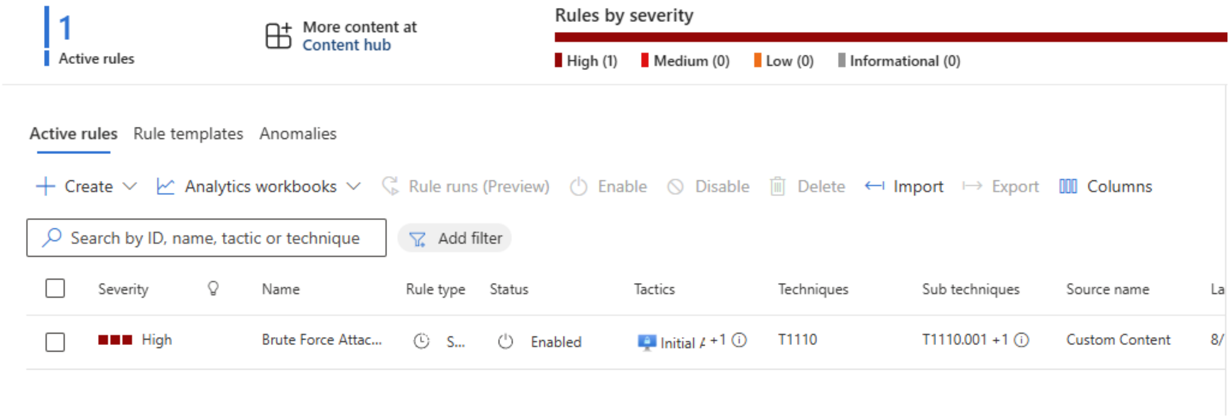
Create a Rule Query

Use the following query:

```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, Account, EventID, IpAddress
| where IpAddress != "-"
| summarize count() by Account, EventID, IpAddress,
bin(TimeGenerated, 1m)
| where count_ >= 5
```

This query searches for failed login events (EventID 4625) in SecurityEvent logs, extracts the IP address involved in each failure, then counts how many times each account is targeted from each IP address within 1-minute intervals. It filters to show only cases where there are 5 or more failed attempts in one minute from the same IP and account, which helps identify possible brute force attacks.

Complete the remaining steps and create the rule



1 Active rules

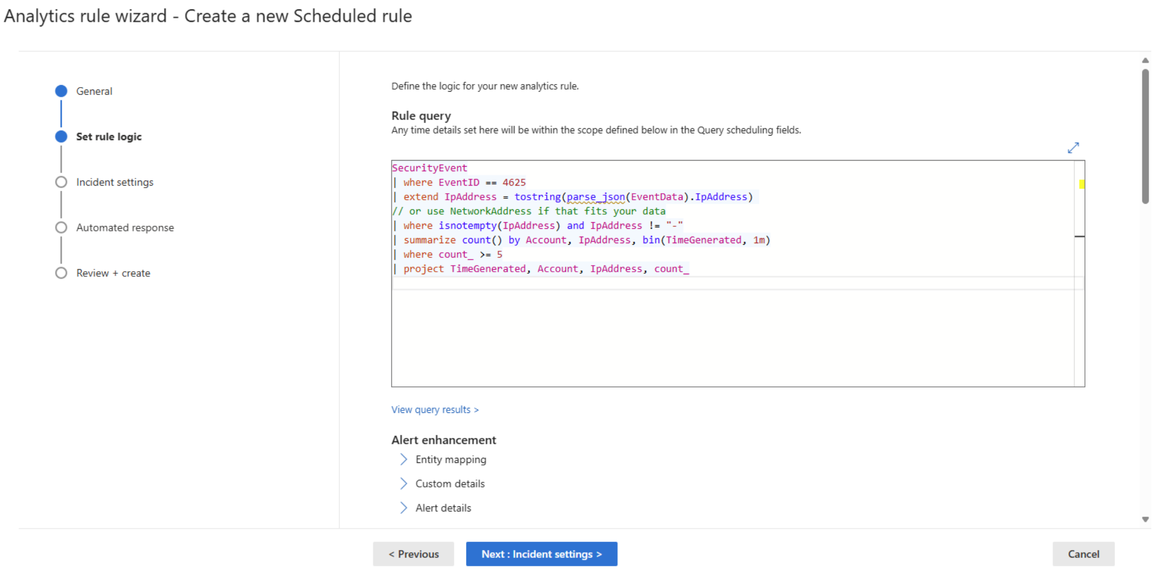
More content at Content hub

Rules by severity

High (1) Medium (0) Low (0) Informational (0)

Active rules | Rule templates | Anomalies

□	Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	La
□	🟥🟥🟥 High	Brute Force Attac...	S...	Enabled	Initial / +1	T1110	T1110.001 +1	Custom Content	8/



Analytics rule wizard - Create a new Scheduled rule

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.

```
SecurityEvent
| where EventID == 4625
| extend IpAddress = tostring(parse_json(EventData).IpAddress)
// or use NetworkAddress if that fits your data
| where isnotempty(IpAddress) and IpAddress != "-"
| summarize count() by Account, IpAddress, bin(TimeGenerated, 1m)
| where count_ >= 5
| project TimeGenerated, Account, IpAddress, count_
```

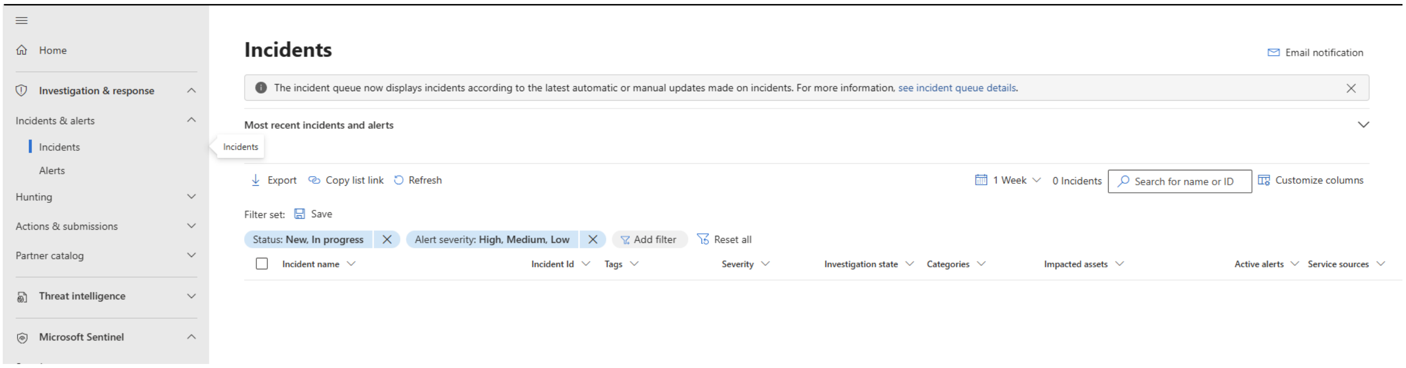
View query results >

Alert enhancement

Check Incidents Tab

Any incidents relating to a brute force attack will now be reported in Incidents & Alerts > Incidents

Before Brute Force Attack:



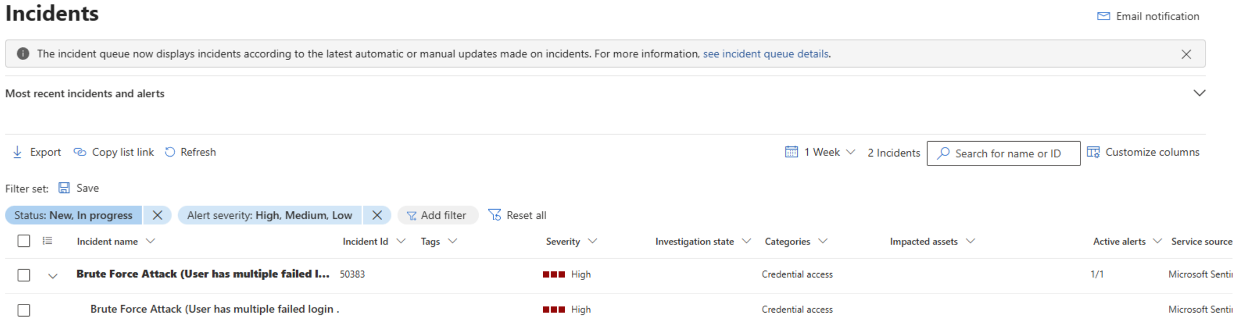
Incidents

The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, see incident queue details.

Most recent incidents and alerts

□	Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources

After Brute Force Attack:



Incidents

The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, see incident queue details.

Most recent incidents and alerts

Filter set: Save

Status: New, In progress

Alert severity: High, Medium, Low

Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service source
Brute Force Attack (User has multiple failed l...	50383		■■■ High		Credential access		1/1	Microsoft Senti
Brute Force Attack (User has multiple failed login .			■■■ High		Credential access			Microsoft Senti

Create NRT Query Rules

Near Real-Time analytic rules are designed to detect and alert on suspicious activity within a minute or so of the event being ingested, instead of running on a schedule like regular analytic tools.

These rules should be used for account compromise attempts, malware beaconing, privilege escalation, suspicious login locations, ransomware indicators, and more.

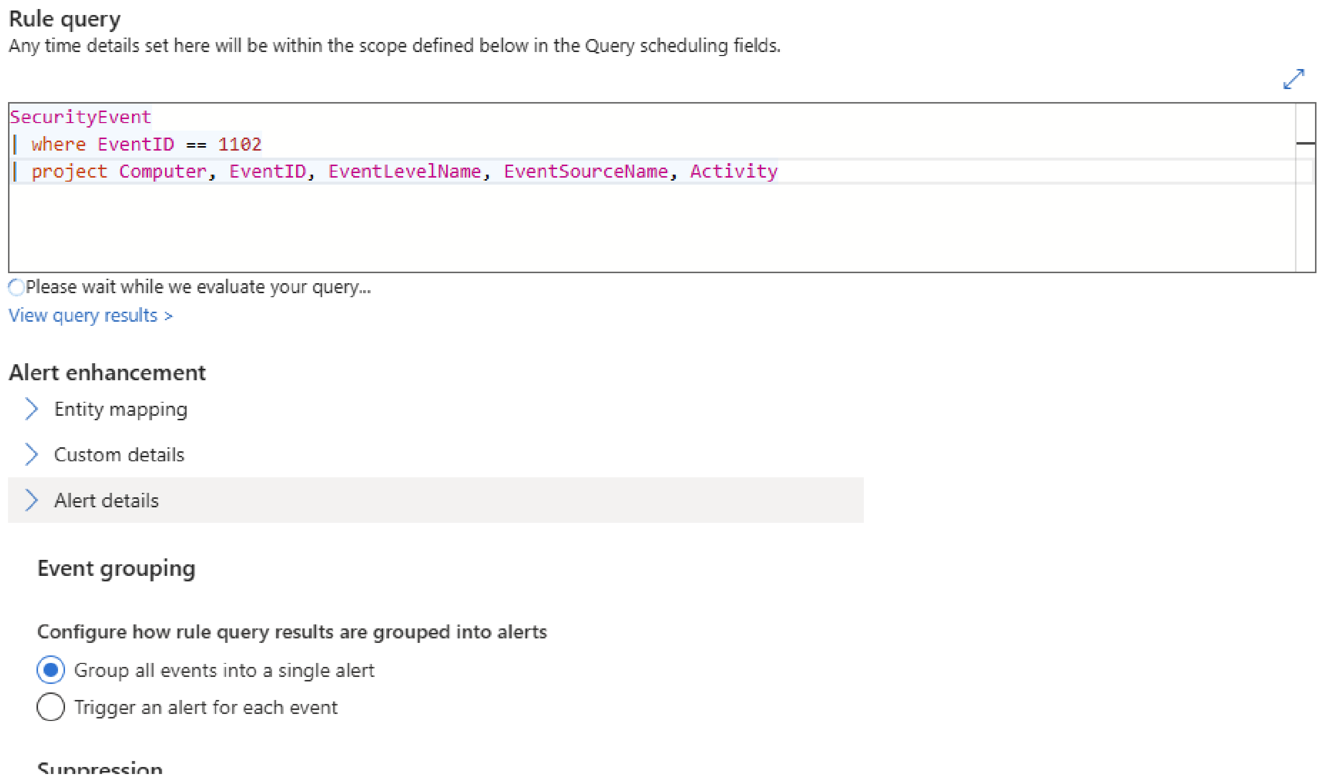
It’s important to note that these can generate more alerts if not tuned properly, so filtering with precise KQL queries is important.

In this example, we will create a rule for Audit Logs being cleared in a critical server. This is a strong indicator of malicious activity, as attackers often do cover their tracks after gaining access.

MITRE ATT&CK Mappings:

- T1070.001 – Indicator Removal on Host: Clear Windows Event Logs
- T0872 – Indicator Removal on Host
- T1630—Indicator Removal on Host
- TA0005 – Defense Evasion

Rule Query



Rule query

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

```
SecurityEvent
| where EventID == 1102
| project Computer, EventID, EventLevelName, EventSourceName, Activity
```

Please wait while we evaluate your query...

View query results >

Alert enhancement

Event grouping

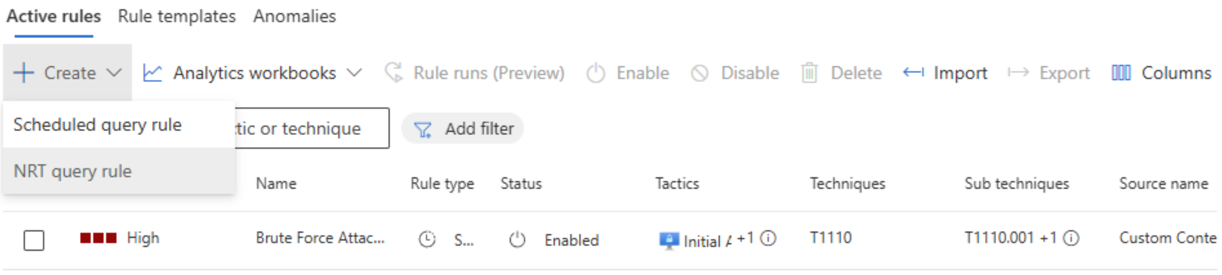
Configure how rule query results are grouped into alerts

● Group all events into a single alert

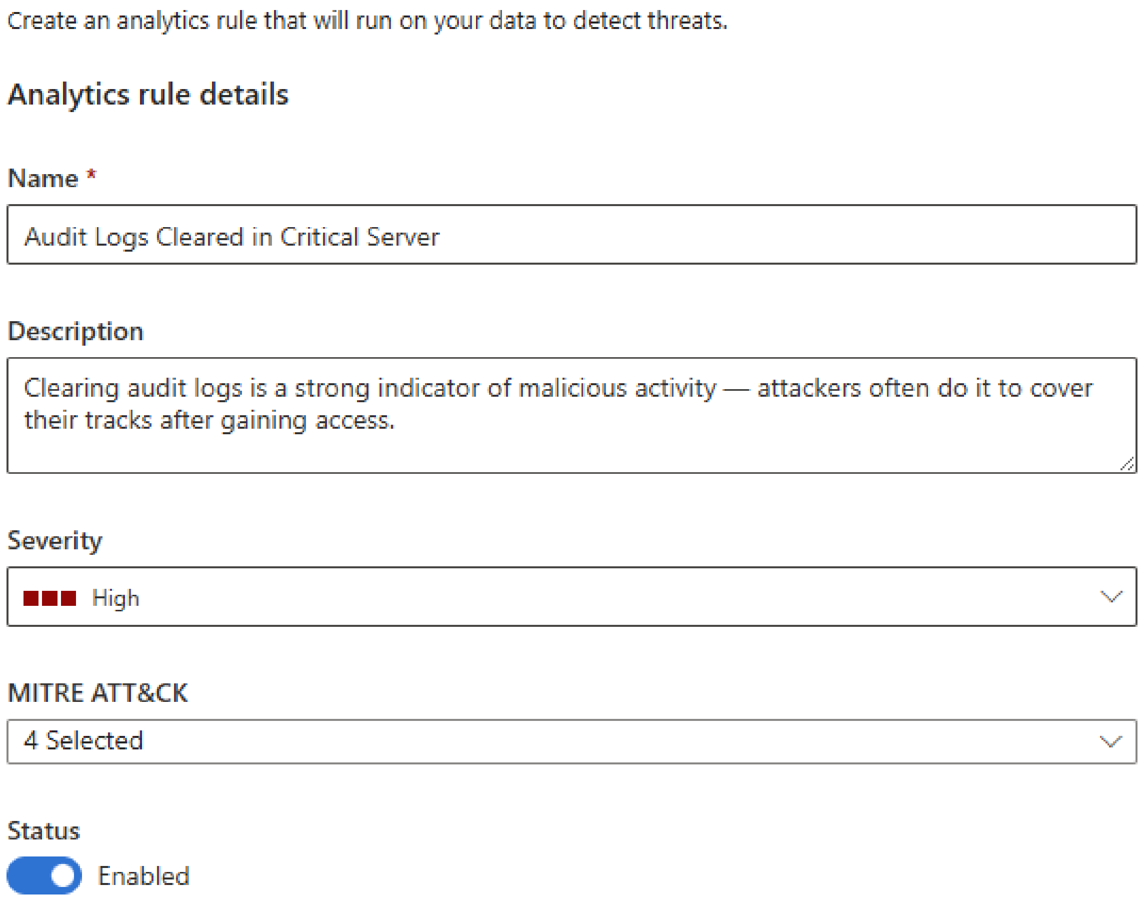
○ Trigger an alert for each event

Suppression

This query finds all cases where the Windows Security Audit Log was cleared, and lists the computer name, event details, and activity description.



		Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name
□	🟥🟥🟥 High	Brute Force Attac...	S...	Enabled	Initial A +1	T1110	T1110.001 +1	Custom Conte



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

Analytics rule details

Name *

Audit Logs Cleared in Critical Server

Description

Clearing audit logs is a strong indicator of malicious activity — attackers often do it to cover their tracks after gaining access.

Severity

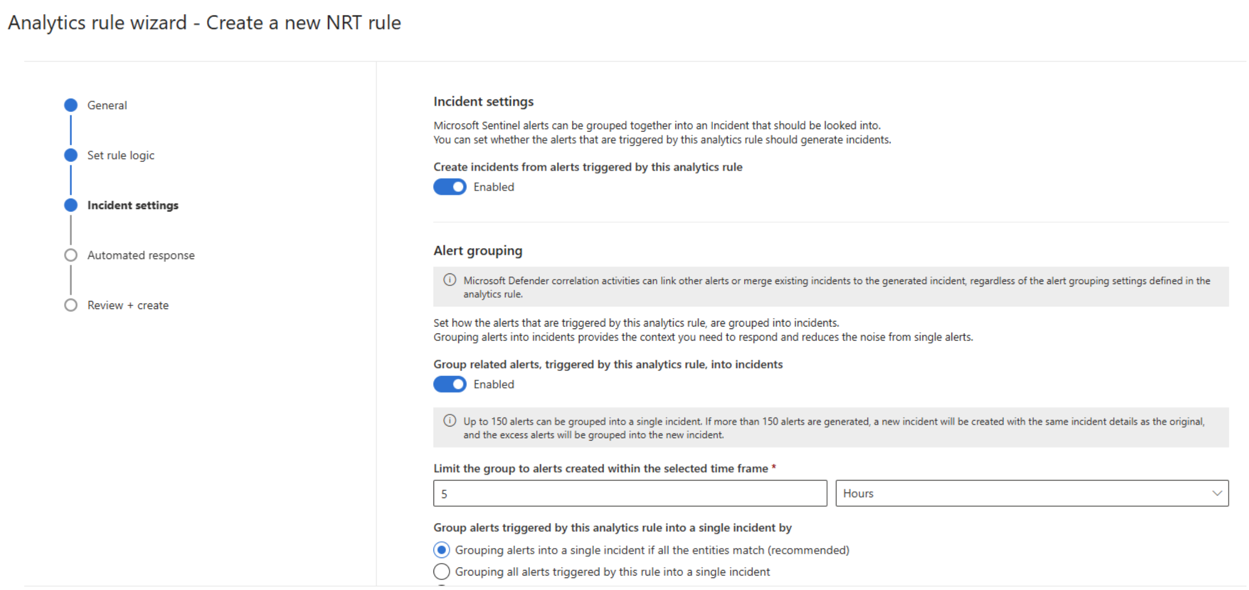
🟥🟥🟥 High

MITRE ATT&CK

4 Selected

Status

Enabled



Analytics rule wizard - Create a new NRT rule

Incident settings

Microsoft Sentinel 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.

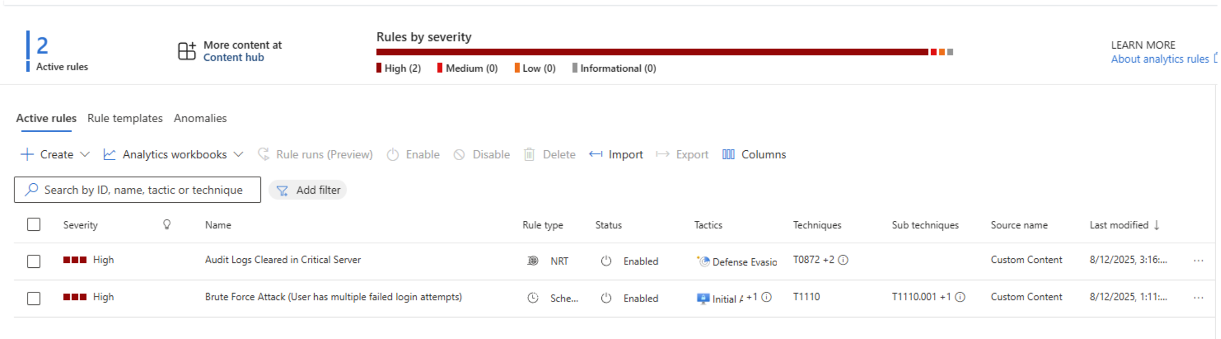
Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents
Enabled

ⓘ Up to 150 alerts can be grouped into a single incident. If more than 150 alerts are generated, a new incident will be created with the same incident details as the original, and the excess alerts will be grouped into the new incident.

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



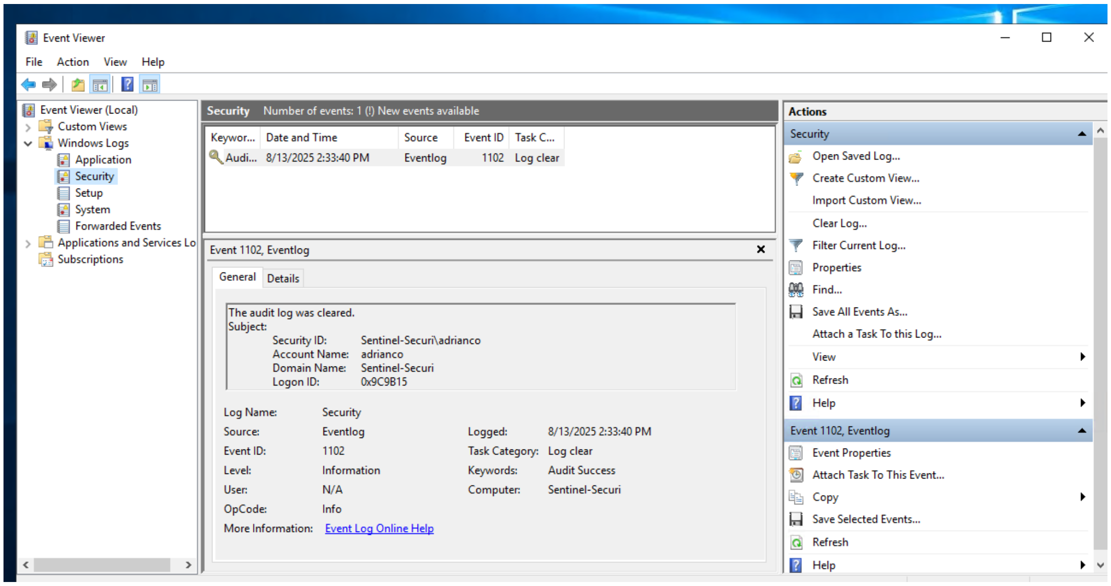
2
Active rules

Rules by severity
High (2) | Medium (0) | Low (0) | Informational (0)

□	Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified ↓
□	■■■ High	Audit Logs Cleared in Critical Server	NRT	Enabled	Defense Evasio	T0872 +2 ⓘ		Custom Content	8/12/2025, 3:16:...
□	■■■ High	Brute Force Attack (User has multiple failed login attempts)	Sche...	Enabled	Initial / +1 ⓘ	T1110	T1110.001 +1 ⓘ	Custom Content	8/12/2025, 1:11:...

Test the NRT Rule

Cleared logs on my VM



Security Number of events: 1 (!) New events available

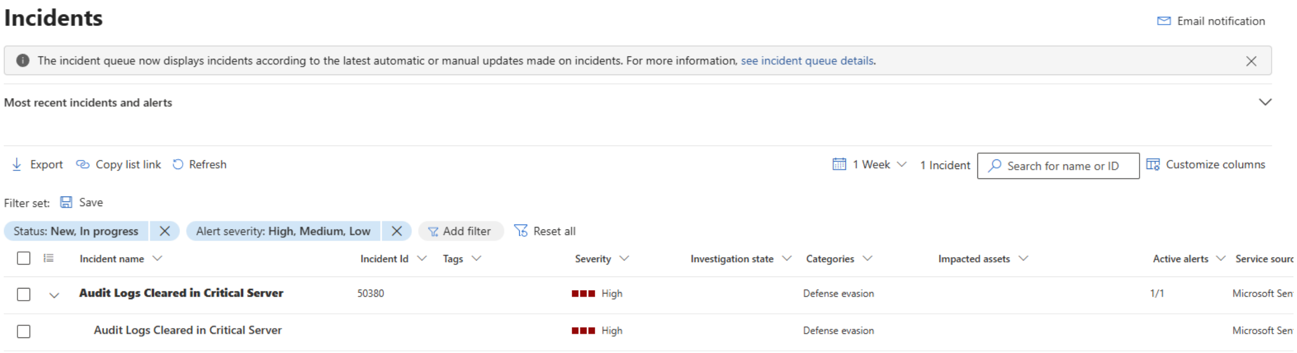
Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	8/13/2025 2:33:40 PM	Eventlog	1102	Log clear

Event 1102, Eventlog

```
The audit log was cleared.
Subject:
        Security ID:      Sentinel-Securi\adrianco
        Account Name:     adrianco
        Domain Name:      Sentinel-Securi
        Logon ID:         0x9C9B15
```

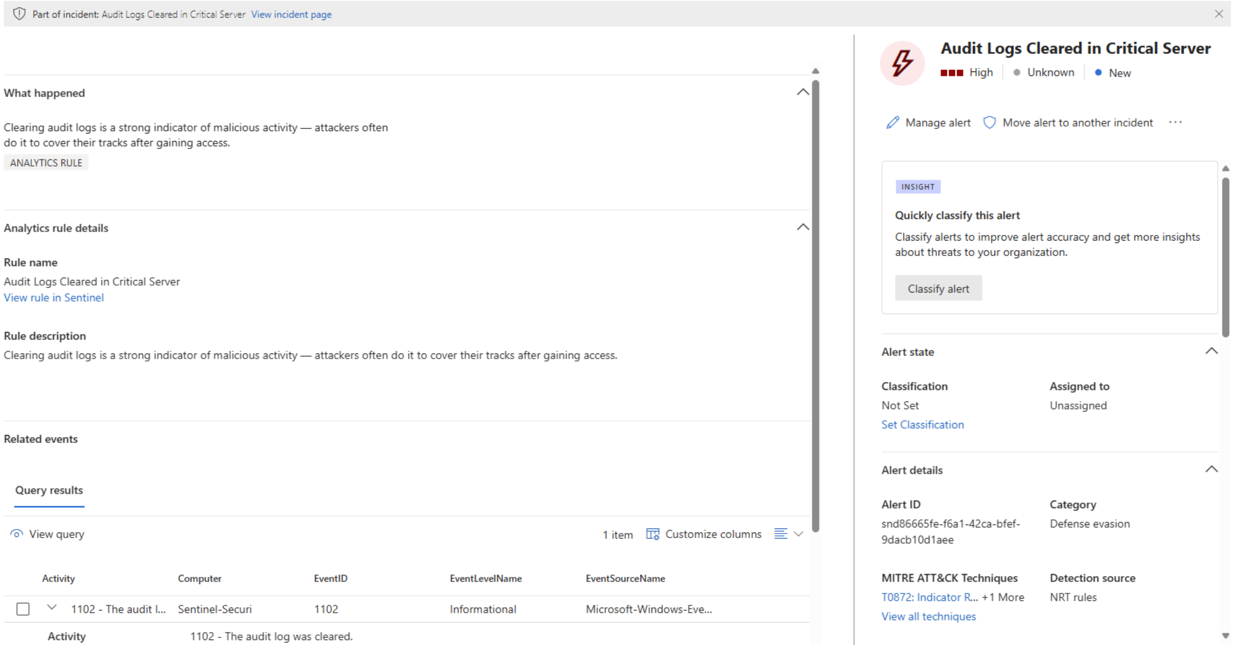
```
Log Name:          Security
Source:            Eventlog              Logged:          8/13/2025 2:33:40 PM
Event ID:          1102                  Task Category:   Log clear
Level:             Information           Keywords:        Audit Success
User:              N/A                   Computer:        Sentinel-Securi
OpCode:            Info
More Information:  Event Log Online Help
```

Checked Incidents, and sure enough an incident was reported



The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, see incident queue details.

☐	Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sourc
☐	**Audit Logs Cleared in Critical Server**	50380		■■■ High		Defense evasion		1/1	Microsoft Sen
☐	Audit Logs Cleared in Critical Server			■■■ High		Defense evasion			Microsoft Sen



Part of incident: Audit Logs Cleared in Critical Server View incident page

What happened

Clearing audit logs is a strong indicator of malicious activity — attackers often do it to cover their tracks after gaining access.

ANALYTICS RULE

Analytics rule details

Rule name

Audit Logs Cleared in Critical Server

View rule in Sentinel

Rule description

Clearing audit logs is a strong indicator of malicious activity — attackers often do it to cover their tracks after gaining access.

Related events

Query results

View query

1 item Customize columns

	Activity	Computer	EventID	EventLevelName	EventSourceName
□	1102 - The audit l...	Sentinel-Securi	1102	Informational	Microsoft-Windows-Eve...

Activity 1102 - The audit log was cleared.

Audit Logs Cleared in Critical Server

■■■ High | ● Unknown | ● New

Manage alert · Move alert to another incident · ···

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification	Assigned to
Not Set Set Classification	Unassigned

Alert details

Alert ID	Category
snd86665fe-f6a1-42ca-bfef-9dacb10d1aee	Defense evasion
MITRE ATT&CK Techniques	Detection source
T0872: Indicator R... +1 More View all techniques	NRT rules

Next Steps as a SOC Analyst

- Triage the incident
  - Check the incident details to get the machine name, username, time of event, and any other related information.
  - Confirm it’s not a false positive (Was this done by the IT department during maintenance?)
- Investigate in depth
  - Run a query to see what happened right before the log was cleared
  - Look for suspicious logon events, privilege changes, multiple failed logins, etc.
- Correlate with other Data Sources
  - Check Defender for Endpoint, firewall logs, or more.
  - Look for file access, PowerShell commands, or process creation events around the same time.
- Determine severity
  - Escalate to incident response if necessary
- Document everything

  - Add investigation steps, findings, and decision-making to the incident record
  - Include all information found
- Take preventative measures
  - Learn from the experience, and take measures to prevent it in the future