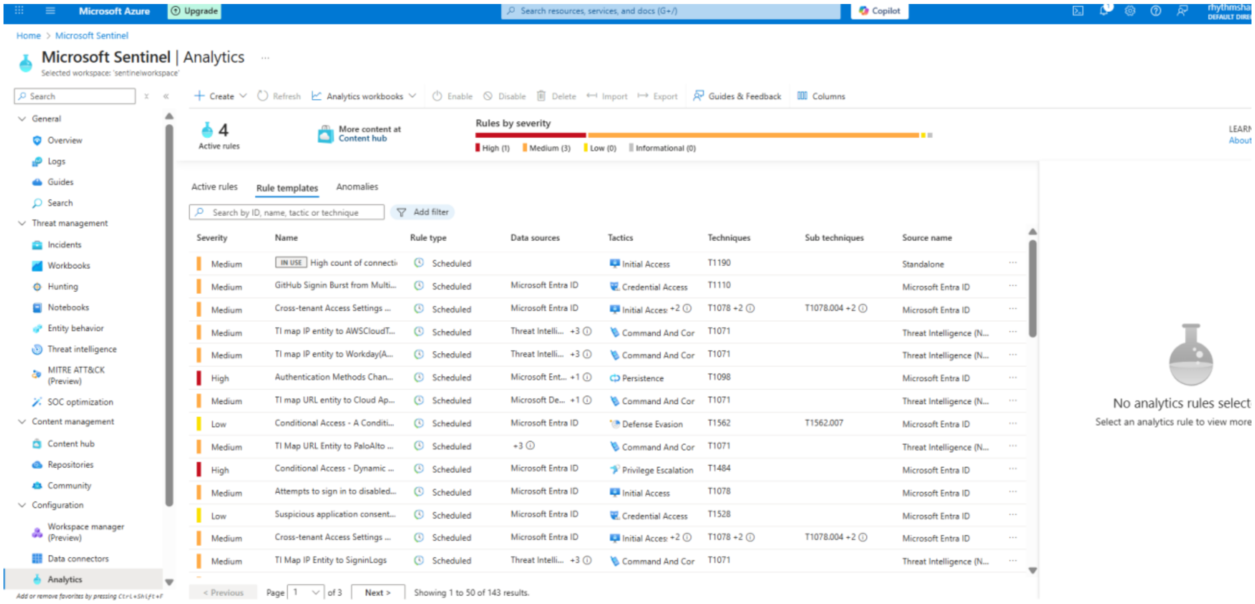
Analytics rules in Microsoft Sentinel

3.1 Analytics rules in Microsoft Sentinel are the **detection engine**. They continuously query ingested logs (using KQL) to identify suspicious activity, anomalies, or policy violations. When a rule's condition is met, Sentinel generates an **alert** and can group alerts into **incidents** for SOC investigation.



Home > Microsoft Sentinel

Microsoft Sentinel | Analytics

Selected workspace: 'sentinelworkspace'

4 Active rules

More content at Content hub

Rules by severity: High (1) Medium (3) Low (0) Informational (0)

Active rules | Rule templates | Anomalies

Severity	Name	Rule type	Data sources	Tactics	Techniques	Sub techniques	Source name
Medium	IN USE High count of connecti	Scheduled		Initial Access	T1190		Standalone
Medium	GitHub Signin Burst from Multi...	Scheduled	Microsoft Entra ID	Credential Access	T1110		Microsoft Entra ID
Medium	Cross-tenant Access Settings ...	Scheduled	Microsoft Entra ID	Initial Acces +2 ⓘ	T1078 +2 ⓘ	T1078.004 +2 ⓘ	Microsoft Entra ID
Medium	TI map IP entity to AWSCloudT...	Scheduled	Threat Intelli... +3 ⓘ	Command And Cor	T1071		Threat Intelligence (N...
Medium	TI map IP entity to Workday(A...	Scheduled	Threat Intelli... +3 ⓘ	Command And Cor	T1071		Threat Intelligence (N...
High	Authentication Methods Chan...	Scheduled	Microsoft Ent... +1 ⓘ	Persistence	T1098		Microsoft Entra ID
Medium	TI map URL entity to Cloud Ap...	Scheduled	Microsoft De... +1 ⓘ	Command And Cor	T1071		Threat Intelligence (N...
Low	Conditional Access - A Conditi...	Scheduled	Microsoft Entra ID	Defense Evasion	T1562	T1562.007	Microsoft Entra ID
Medium	TI Map URL Entity to PaloAlto ...	Scheduled	+3 ⓘ	Command And Cor	T1071		Threat Intelligence (N...
High	Conditional Access - Dynamic ...	Scheduled	Microsoft Entra ID	Privilege Escalation	T1484		Microsoft Entra ID
Medium	Attempts to sign in to disabled...	Scheduled	Microsoft Entra ID	Initial Access	T1078		Microsoft Entra ID
Low	Suspicious application consent...	Scheduled	Microsoft Entra ID	Credential Access	T1528		Microsoft Entra ID
Medium	Cross-tenant Access Settings ...	Scheduled	Microsoft Entra ID	Initial Acces +2 ⓘ	T1078 +2 ⓘ	T1078.004 +2 ⓘ	Microsoft Entra ID
Medium	TI Map IP Entity to SigninLogs	Scheduled	Threat Intelli... +3 ⓘ	Command And Cor	T1071		Threat Intelligence (N...

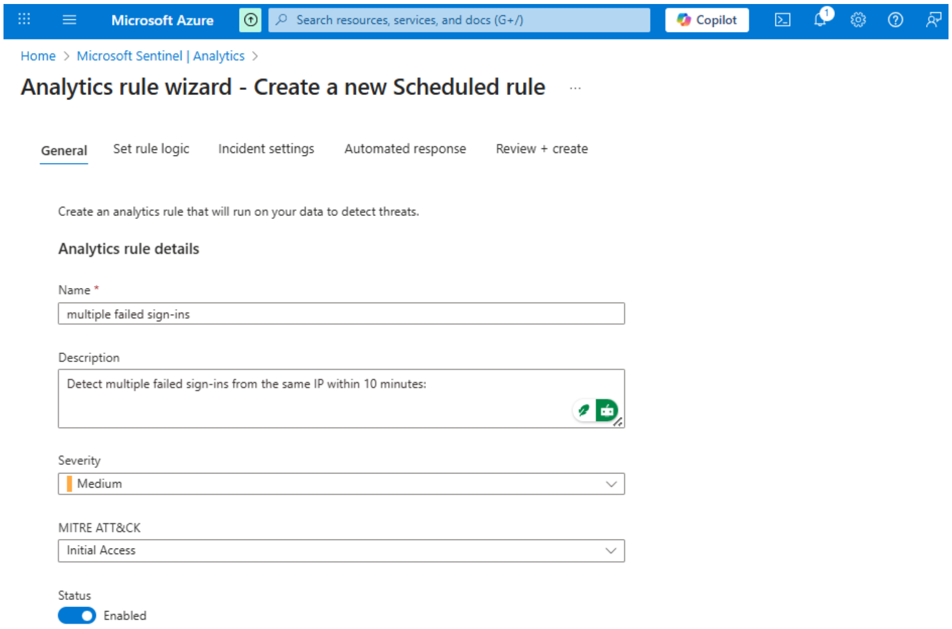
< Previous Page 1 of 3 Next > Showing 1 to 50 of 143 results.

No analytics rules select

Select an analytics rule to view more

3.1.1 We will create own query and test it

Scenario: Detect multiple failed sign-ins from the same IP within 10 minutes in Microsoft Entra ID



Home > Microsoft Sentinel | Analytics >

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 *: multiple failed sign-ins

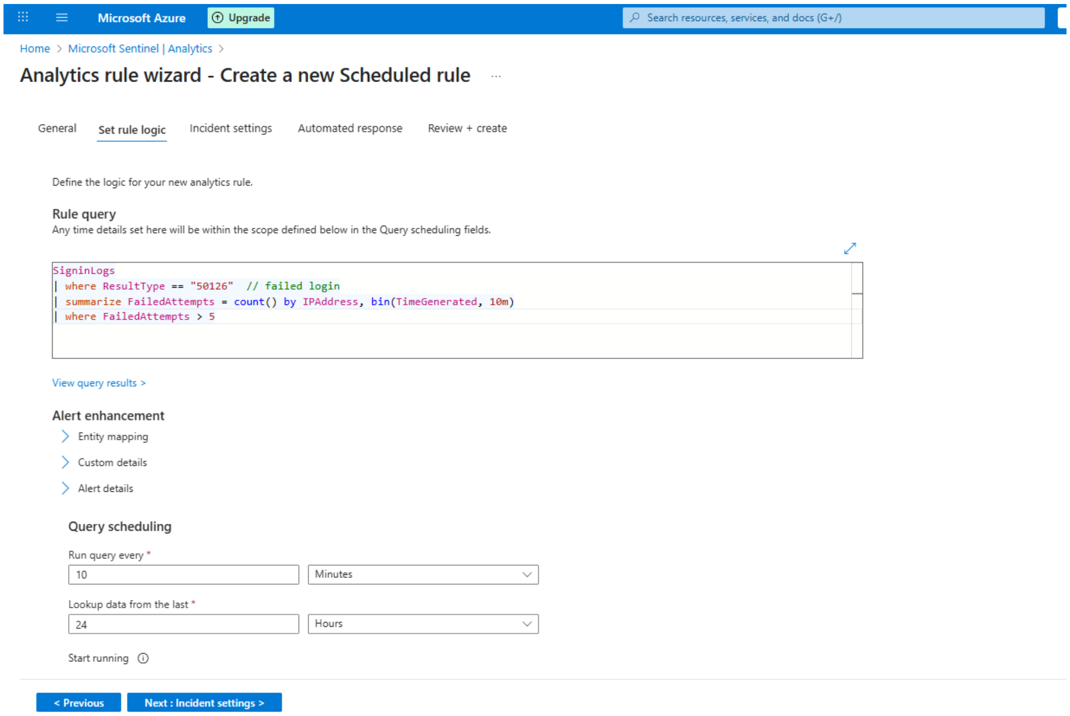
Description: Detect multiple failed sign-ins from the same IP within 10 minutes:

Severity: Medium

MITRE ATT&CK: Initial Access

Status: Enabled

3.1.2 Enter Query (Use KQL Language) and Set Scheduling according to environment



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.

```
SigninLogs
| where ResultType == "50126"  // failed login
| summarize FailedAttempts = count() by IPAddress, bin(TimeGenerated, 10m)
| where FailedAttempts > 5
```

Alert enhancement

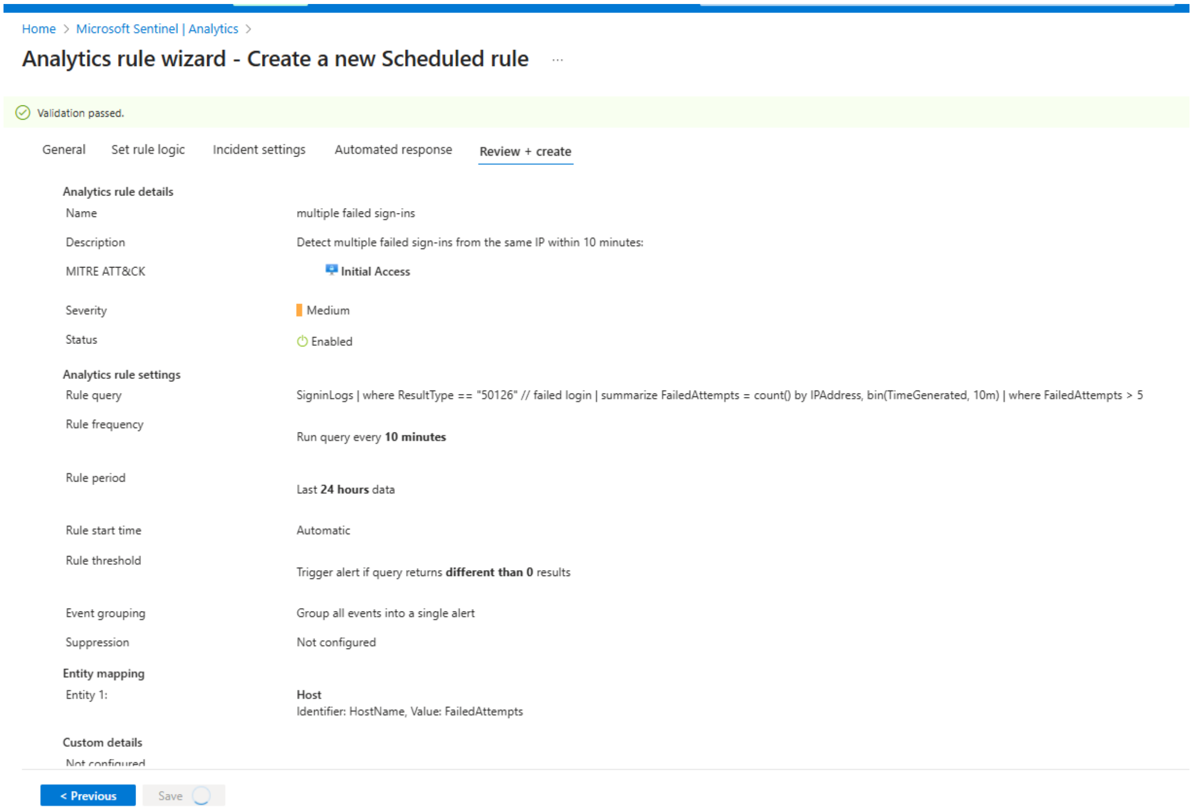
Query scheduling

Run query every *: 10 Minutes

Lookup data from the last *: 24 Hours

Start running

3.1.3 Save the Rule



Analytics rule wizard - Create a new Scheduled rule

Validation passed.

Analytics rule details

Name	multiple failed sign-ins
Description	Detect multiple failed sign-ins from the same IP within 10 minutes:
MITRE ATT&CK	Initial Access
Severity	Medium
Status	Enabled

Analytics rule settings

Rule query	SigninLogs | where ResultType == "50126" // failed login | summarize FailedAttempts = count() by IPAddress, bin(TimeGenerated, 10m) | where FailedAttempts > 5
Rule frequency	Run query every **10 minutes**
Rule period	Last **24 hours** data
Rule start time	Automatic
Rule threshold	Trigger alert if query returns **different than 0** results
Event grouping	Group all events into a single alert
Suppression	Not configured

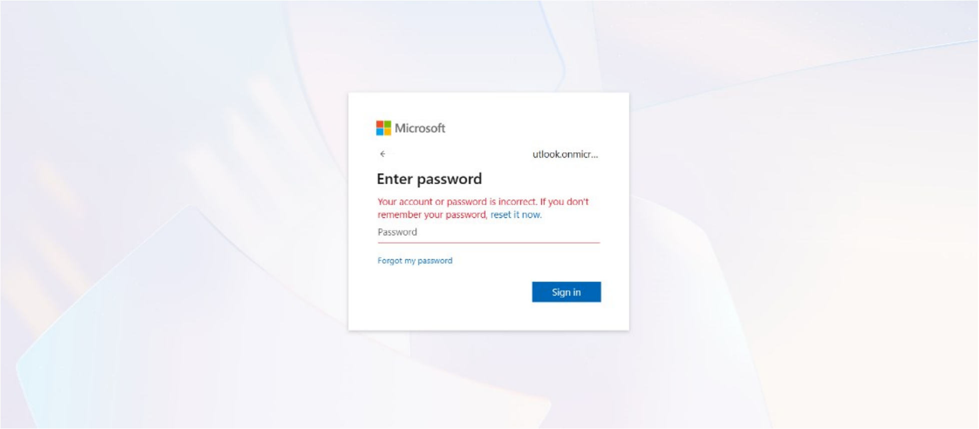
Entity mapping

Entity 1:	**Host** Identifier: HostName, Value: FailedAttempts

Custom details

Not configured

3.1.4 I attempted Falied Login to Check my Custom Analytics rule.

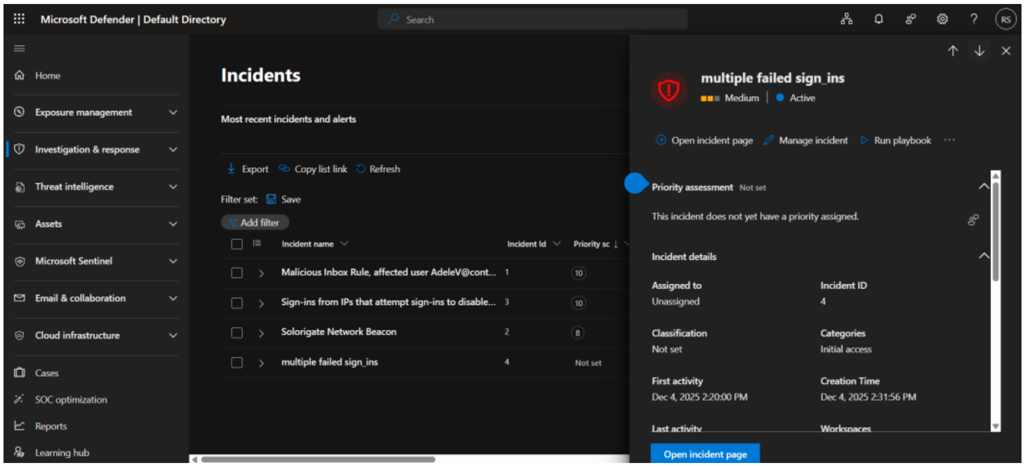


Enter password

Your account or password is incorrect. If you don't remember your password, reset it now.

Password

3.1.5 Incident has generated under incident tab



Incidents

Most recent incidents and alerts

Incident name	Incident Id	Priority sc
Malicious Inbox Rule, affected user AdeleV@cont...	1	10
Sign-ins from IPs that attempt sign-ins to disable...	3	10
Solorigate Network Beacon	2	8
multiple failed sign_ins	4	Not set

multiple failed sign_ins

Medium | Active

Priority assessment Not set

This incident does not yet have a priority assigned.

Incident details

Assigned to
Unassigned

Incident ID
4

Classification
Not set

Categories
Initial access

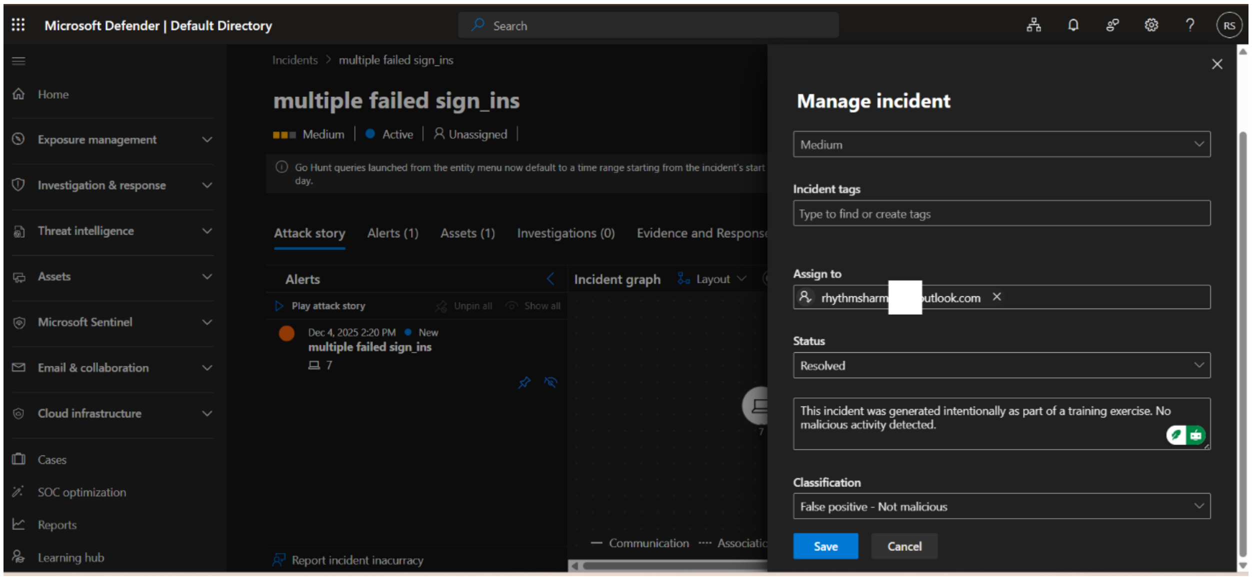
First activity
Dec 4, 2025 2:20:00 PM

Creation Time
Dec 4, 2025 2:31:56 PM

Last activity

Workspaces

3.1.6 Let’s Resolve the Incident



multiple failed sign_ins

Medium | Active | Unassigned |

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start day.

Dec 4, 2025 2:20 PM New
multiple failed sign_ins
7

Manage incident

Medium

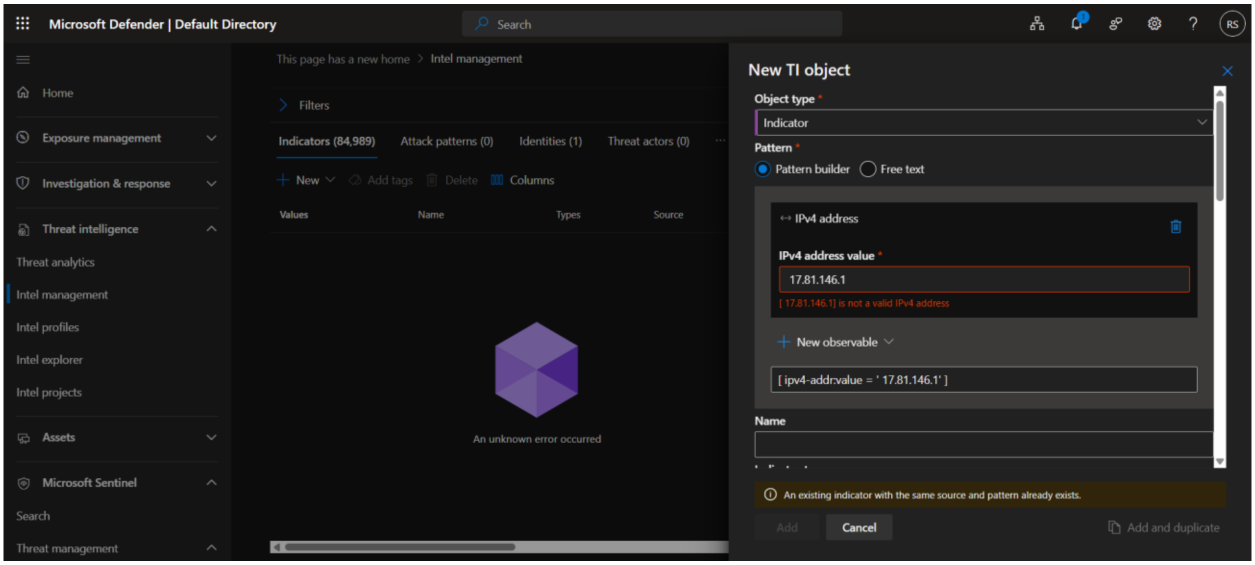
Incident tags: Type to find or create tags

Assign to: rhythmsharm[redacted]utlook.com ✕

Status: Resolved

This incident was generated intentionally as part of a training exercise. No malicious activity detected.

Classification: False positive - Not malicious



An unknown error occurred

New TI object

Object type *: Indicator

Pattern *: ● Pattern builder ○ Free text

↔ IPv4 address

IPv4 address value *: 17.81.146.1

[17.81.146.1] is not a valid IPv4 address

[ipv4-addr:value = ' 17.81.146.1']

Name

An existing indicator with the same source and pattern already exists.