

Microsoft Sentinel

What is it?

Microsoft Sentinel incidents are containers of threats in your organization – alerts, entities and any additional related evidence. An incident is created based on alerts that you have defined in the security analytics page. The properties related to the alerts, such as severity and status are set at the incident level.

How does it work?

Incidents are automatically created as a result of alerts triggered based on detections defined in 'Security analytics'. The incidents page provide a full view of all the context required for triage, investigation and response. For each incident, you can see the time it was generated and its status.

These are the types of activities you can perform with incidents



View related alerts

View all related alerts that are aggregated into an incident based on the alert trigger definition of the alert fusion strategy enabled. Review all details related to the alert in a unified location.



Triage and investigate

Review all related entities in the incident and additional contextual information meaningful to the triage process. Investigate the alerts and related entities to understand the scope of breach.



Incident management

Manage the lifecycle of the incident – assign to yourself for further investigation, change the status of the incident and update its severity after triage.



Respond to alerts in the incidents

Trigger playbooks on the alerts grouped in the incident to resolve the threat detected by the alert using playbooks.

Microsoft Sentinel provides the ability to collect , detect, investigate and respond to threats, incidents and risks that can occur against a organization.

Microsoft Sentinel provides a cloud based Security, Information, Events Management solution (SIEM). It gives us the collect and analyze logs from a variety of sources – on-premise, in the cloud ..anywhere we can imagine.

Life cycle – Collect, Investigate, Detect, Respond.

Collect from cloud infrastructure, collect from on premise, collect across different cloud infrastructures with the use of artificial intelligence and machine learning.

Azure services

Access Microsoft Sentinel from Azure Services



Create a resource



Resource groups



Microsoft Sentinel



Azure Active Directory



Microsoft Defender for...



Storage accounts



Azure Database for MySQL...



Azure Information...



Azure AD Security



All services

Recent resources

Name

Type

Last Viewed



MSDN Platforms

Subscription

2 weeks ago

[See all](#)

Navigate



Subscriptions



Resource groups



All resources



Dashboard

Tools



[Microsoft Learn](#)

Learn Azure with free online training from Microsoft



[Azure Monitor](#)

Monitor your apps and infrastructure



[Microsoft Defender for Cloud](#)

Secure your apps and infrastructure



[Cost Management](#)

Analyze and optimize your cloud spend for free

Show portal menu

Default Directory

+ Create ⚙️ Manage view ∨ 🔄 Refresh ⬇️ Export to CSV 🔗 Open query | 📁 View incidents | 🗣️ Feedback

Filter for any field...

Subscription == all

Resource group == all ✕

Location == all ✕

+ Add filter

Showing 0 to 0 of 0 records.

No grouping ∨

List view ∨

Name ↑↓

Resource group ↑↓

Location ↑↓

Subscription ↑↓

Directory ↑↓



No Microsoft Sentinel to display

See and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise.


[Create Microsoft Sentinel](#)


[Learn more](#)

Select Create Microsoft Sentinel;

[Home](#) > [Microsoft Sentinel](#) >

Add Microsoft Sentinel to a workspace ...

+ Create a new workspace  Refresh

 Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

Microsoft Sentinel provides intelligent security analytics across your enterprise. The data for this analysis is stored in an **Azure Monitor Log Analytics workspace**.



No workspaces found

[Create a new workspace](#)

Microsoft Sentinel needs a workspace to store all the data it collects, so if you don't already have a Workspace you need to click on Create a new workspace

Create Log Analytics workspace ...

Basics Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) ✕

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

[Create new](#)

Instance details

Name * ⓘ

Review + Create

« Previous

A resource group is a container that holds related resources for an Azure solution.

Name *

OK Cancel

While creating the workspace
You need to create a
Resource group.

What is Resource Group in Azure portal?
Resource groups are also called the central unit that acts like a logical container that holds all the Azure resources. You need a Resource Group to be created while creating any of the resources in Azure Portal.

Create Log Analytics workspace ...

Basics | Tags | Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) ×

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * **i**

MSDN Platforms ▼

Resource group * **i**

(New) rg sentinel ▼

[Create new](#)

Instance details

Name * **i**

sentinelws ✓

Region * **i**

West US ▼

Review + Create

« Previous

Next : Tags >

You also have to supply the Instance name and region

Create Log Analytics workspace ...

✔ Validation passed

Basics lags Review + Create



Log Analytics workspace

by Microsoft

Basics

Subscription	MSDN Platforms
Resource group	rgsentinel
Name	sentinelws
Region	West US

Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)
--------------	-----------------------------

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created. [Learn more](#) about Log Analytics pricing models.

Tags

(none)


Click on Create to create the workspace


 **Create**

« Previous


[Download a template for automation](#)

Add Microsoft Sentinel to a workspace ...

+ Create a new workspace  Refresh

 Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
 sentinelws	westus	rgsentinel	MSDN Platforms	Default Directory

Click on Add to add Microsoft Sentinel to a workspace


Add

Cancel

✔ Successfully added Microsoft Sentinel

Successfully added Microsoft Sentinel to workspace 'sentinelws', it might take a few minutes for your workspace to appear in Microsoft Sentinel workspaces list



Microsoft Sentinel | News & guides

Selected workspace: 'sentinelws'

Search (Ctrl+/)

Documentation

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

Content management

Content hub (Preview)

Repositories (Preview)

Community

Configuration

Data connectors

What's new Get started Free trial

Microsoft Sentinel

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.



Under configuration select data connectors



1. Collect data

Collect data at cloud scale across the enterprise, both on-premises and in multiple clouds

Connect



2. Create security alerts

Focus on what's important using analytics to create alerts

Create



3. Automate & orchestrate

Use or customize built-in playbooks to automate common tasks

Create



The Data connectors page, accessible from the Microsoft **Sentinel** navigation menu, shows the full list of connectors that Microsoft **Sentinel** provides, and their status. Select the connector you want to connect, and then select Open connector page. You'll need to have fulfilled all the prerequisites, and you'll see complete instruction

Search (Ctrl+)

Guides & Feedback Refresh

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors

122
Connectors

0
Connected

More content at
Content hub








Search by name or provider

Providers : All

Data Types : All

Status : All

Status ↑↓ Connector name ↑↓

	Juniper SRX (Preview) Juniper
	Microsoft 365 Defender (Preview) Microsoft
	Microsoft 365 Insider Risk Management (Preview) Microsoft
	Microsoft Defender for Cloud Microsoft
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity

Microsoft 365 Defender (Preview)

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence


Last data received

--

Related content


Open connector page


Microsoft 365 Defender (Preview) ...



Microsoft 365 Defender (Preview)

Not connected
Status

 **Microsoft**
Provider

 --
Last Log Received

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.


Microsoft 365 Defender suite includes:


- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence


Last data received

--

Related content

 **1**
Workbooks


 **4**
Queries

 **32**
Analytics rules templates

Data received

100

[Go to log analytics](#)

 Incidents

Instructions

Next steps



Prerequisites

To integrate with Microsoft 365 Defender (Preview) make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.



 **License:** M365 E5, M365 A5 or any other Microsoft 365 Defender eligible license.

Right away you can see that I don't have one of the prerequisites to work with Microsoft 365 Defender Preview



Active products in your environment

 Defender for Endpoint




Configuration

Connect incidents & alerts

Connect Microsoft 365 Defender incidents to your Microsoft Sentinel. Incidents will appear in the incidents queue.

Microsoft 365 Defender (Preview) ...



Microsoft 365 Defender (Preview)

Not connected Status

Microsoft Provider

Last Log Received --

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence

Last data received --

Related content

1 Workbooks

4 Queries

32 Analytics rules templates

Data received 100

[Go to log analytics](#)

Incidents

Instructions Next steps



Configuration

Connect incidents & alerts

Connect Microsoft 365 Defender incidents to your Microsoft Sentinel. Incidents will appear in the incidents queue.

[Connect incidents & alerts](#)

Turn off all Microsoft incident creation rules for these products. Recommended. ⓘ

Connect events

Connect logs from the following Microsoft 365 Defender products to Sentinel:

Microsoft Defender for Endpoint (0/10 connected) ⓘ


<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DeviceInfo	Machine information (including OS information)

Scrolling down the page I can click on connect incidents & alerts. The connect logs are listed.

Microsoft 365 Defender (Preview) ...

 **Connected successfully** ✕

Successfully connected 'Microsoft 365 Defender'.


Microsoft 365 Defender (Preview)
<<

Not connected
status

Microsoft
Provider

--
Last Log Received

Description

Microsoft 365 Defender is a unified, natively integrated, pre- and post-breach enterprise defense suite that protects endpoint, identity, email, and applications and helps you detect, prevent, investigate, and automatically respond to sophisticated threats.

Microsoft 365 Defender suite includes:

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender Alert Evidence

Last data received

Related content

1
Workbooks

4
Queries

32
Analytics rules templates

Data received

100

Go to log analytics

Incidents

Instructions Next steps



Configuration

Connect incidents & alerts

Connect Microsoft 365 Defender incidents to your Microsoft Sentinel. Incidents will appear in the incidents queue.

[Disconnect](#)

Connect events

Connect logs from the following Microsoft 365 Defender products to Sentinel:



Microsoft Defender for Endpoint (0/10 connected) ⓘ

Name

Description

DeviceInfo

Machine information (including OS information)

Microsoft Sentinel | Data connectors

Selected workspace: 'sentinelws'

Search (Ctrl+)

Guides & Feedback Refresh

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

Content management

Content hub (Preview)

Repositories (Preview)

Community

Configuration

Data connectors

Analytics

Watchlist

Automation

Settings

122
Connectors

4
Connected

More content at
[Content hub](#)

Search by name or provider







Providers : All

Data Types : All

Status : All

Status ↑↓

Connector name ↑↓

	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft
	Microsoft Defender for IoT (Preview) Microsoft
	Microsoft Defender for Office 365 (Preview) Microsoft
	Microsoft PowerBI (Preview) Microsoft

Since I don't have the license needed to Microsoft 365 Defender Preview, I will select another collector, Microsoft Defender for Identity and Open the connector page.

Microsoft Defender for Identity

Connected
Status

Microsoft
Provider

--
Last Log Receive


Description

Connect Microsoft Defender for Identity to gain visibility into the events and user analytics. Microsoft Defender for Identity identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Microsoft Defender for Identity enables SecOps analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

[Open connector page](#)

Microsoft Defender for Identity ...



Microsoft Defender for Identity

Not connected Status

Microsoft Provider

⌚ -- Last Log Received

Description

Connect Microsoft Defender for Identity to gain visibility into the events and user analytics. Microsoft Defender for Identity identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Microsoft Defender for Identity enables SecOp analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage




[Try now >](#)

[Deploy now >](#)

Last data received

--

Related content

   1

Instructions Next steps



Configuration

Connect Microsoft Defender for Identity to Microsoft Sentinel

If your tenant is running [Microsoft Defender for Identity](#) in Microsoft Defender for Cloud Apps, connect here to stream your Microsoft Defender Identity alerts into Microsoft Sentinel

In order to integrate with Microsoft Defender for Identity alerts, use **global administrator**, or **security administrator** permission.

Yes, I have connected Microsoft Defender for Identity to Microsoft Defender for Cloud Apps

Microsoft Defender for Identity

[Connect](#)

i Microsoft Defender for Identity alerts are connected through the Microsoft 365 Defender connector and automatically grouped into incidents. Incidents can be seen in the incidents queue.



Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.


[Enable](#)

Microsoft Defender for Identity

✔ Connected successfully

Successfully connected 'Microsoft Defender for Identity'.

Read the instructions carefully



Microsoft Defender for Identity

Connected Status

Microsoft Provider

Last Log Received

Description

Connect Microsoft Defender for Identity to gain visibility into the events and user analytics. Microsoft Defender for Identity identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Microsoft Defender for Identity enables SecOp analysts and security professionals struggling to detect advanced attacks in hybrid environments to:

- Monitor users, entity behavior, and activities with learning-based analytics
- Protect user identities and credentials stored in Active Directory
- Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
- Provide clear incident information on a simple timeline for fast triage

Try now >

Deploy now >

Last data received

Related content

Instructions

Next steps



Connect Microsoft Defender for Identity to Microsoft Sentinel

If your tenant is running [Microsoft Defender for Identity](#) in Microsoft Defender for Cloud Apps, connect here to stream your Microsoft Defender for Identity alerts into Microsoft Sentinel

In order to integrate with Microsoft Defender for Identity alerts, use **global administrator**, or **security administrator** permission.

Yes, I have connected Microsoft Defender for Identity to Microsoft Defender for Cloud Apps

Microsoft Defender for Identity [Disconnect](#)

i Microsoft Defender for Identity alerts are connected through the Microsoft 365 Defender connector and automatically grouped into incidents. Incidents can be seen in the incidents queue.



Create incidents - Recommended!

Create incidents automatically from all alerts generated in this connected service.

[Enable](#)


✔ Microsoft incident creation rule

Microsoft incident creation rule added successfully

Select Enable to create incidents from alerts

Microsoft Defender for Identity

On this page you can click on **go to log analytics** or you can go back to the menu and select **Analytics**

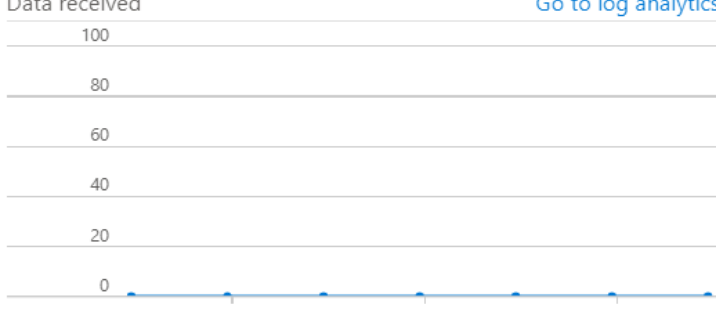


Microsoft Defender for Identity

Connected Status: Microsoft Provider | Last Log Received: --

0 Workbooks | 2 Queries | 1 Analytics rules templates

Data received: [Go to log analytics](#)



Total data received: **0**

Data types: SecurityAlert (AATP) --

Instructions Next steps

Query samples (2)

All logs

```
SecurityAlert | where ProductName == "Azure Advanced Threat Protection" | summarize arg_max(TimeGenerated, *) by SystemAlertId | sort by TimeGenerated
```

[Run](#)

Summarize by operation

```
SecurityAlert | where ProductName == "Azure Advanced Threat Protection" | summarize arg_max(TimeGenerated, *) by SystemAlertId | summarize count() by TimeGenerated | sort by TimeGenerated
```

[Run](#)



Relevant analytics templates (1)

[Go to analytics templates >](#)

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics	Tech
High	Create incidents based on Microsoft D...	Microsoft Secur...	Microsoft Defender ...		

Microsoft Sentinel | Data connectors

Selected workspace: 'workspacesentinel'

Search (Ctrl+ /)

Guides & Feedback Refresh

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors

122
Connectors

1
Connected

More content at
Content hub

office 365

Providers : All

Data Types : All

Status : All

Status ↑↓

Connector name ↑↓



Microsoft Defender for Office 365 (Preview)
Microsoft



Office 365
Microsoft

Let us take a look at an office 365 data connector

Office 365

Not connected to Microsoft Provider. Last Log Received: --

Description: The Office 365 activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, messages sent, changes to group events, set-mailbox and details of the user who performed the actions. By connecting Office 365 logs to Microsoft Sentinel you can use this data to view dashboards, create custom alerts, and improve your investigation process.

Data received: 100

Related content: 5 Workbooks, 3 Queries, 35 Analytics rules templates

Go to log analytics

- SharePoint
- Exchange
- Teams

Instructions Next steps



Prerequisites

To integrate with Office 365 make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.



Configuration

Connect Office 365 activity logs to your Microsoft Sentinel.

Select the record types you want to collect from your tenant and click **Apply Changes**.

- Exchange
- SharePoint
- Teams

Apply Changes

We are going to select all the boxes and Click on Apply changes



Prerequisites

To integrate with Office 365 make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on



Configuration

Connect Office 365 activity logs to your Microsoft Sentinel.

Select the record types you want to collect from your tenant and click **Apply C**

- Exchange
- SharePoint
- Teams

Apply Changes

✓ **Success**

Successfully applied changes

Microsoft Sentinel | News & guides

Selected workspace: 'workspacesentinel'

Search (Ctrl+*/*)

Documentation


Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors
- Analytics 
- Watchlist
- Automation
- Settings

What's new Get started Free trial

Once we have added data connectors and data begins flowing into the Workspace, the next thing we need to do is to analyze the data. We need to run queries across all of the data to find vulnerabilities. Under Configuration select Analytics.

Microsoft Sentinel

A cloud-native SIEM to help you focus on what matters most

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.



1. Collect data

Collect data at cloud scale across the enterprise, both on-premises and in multiple clouds

Connect



2. Create security a

Focus on what's impo analytics to create a

Create

There are 47 rules active

47
Active rules

Rules by severity

High (2) Medium (0) Low (0) Informational (45)

Active rules Rule templates

Search Add filter

<input type="checkbox"/> Severity ↑↓	↑↓ Name ↑↓	Rule type ↑↓	Status ↑↓	Tactics
<input type="checkbox"/> High	Advanced Multistage Attack Detection	Fusion	Enabled	
<input type="checkbox"/> High	Create incidents based on Microsoft Defender f...	Microsoft Secur...	Enabled	
<input type="checkbox"/> Informational	(Preview) Anomalous Account Creation	Anomaly	Enabled	P
<input type="checkbox"/> Informational	(Preview) Anomalous Account Deletion	Anomaly	Enabled	Ir
<input type="checkbox"/> Informational	(Preview) Anomalous Azure AD sign-in sessions	Anomaly	Enabled	Ir
<input type="checkbox"/> Informational	(Preview) Anomalous Azure operations	Anomaly	Enabled	Ir
<input type="checkbox"/> Informational	(Preview) Anomalous Code Execution	Anomaly	Enabled	E
<input type="checkbox"/> Informational	(Preview) Anomalous Failed Sign-in	Anomaly	Enabled	C

< Previous Page 1 of 1 Next >

If we select Rule templates, we will see that Microsoft provides us with a number of templates that we can select from. For Example we could select user login from different countries within 3 hours.

47
Active rules

Rules by severity

High (2)

Medium (0)

Low (0)

Informational (45)

LEARN MORE
About analytics rules

Active rules Rule templates

Search

Add filter

Severity ↑↓	Name ↑↓	Rule type ↑↓	Data sources	Tactics
High	TEARDROP memory-only dropper	Scheduled	Microsoft 365 Defender (Prev...	
High	Exchange SSRF Autodiscover ProxyShell - Det...	Scheduled	Azure Monitor (IIS)	Ini
High	Alsid Password Guessing	Scheduled	Alsid for Active Directory (Pre...	Cr
High	User login from different countries within 3 h...	Scheduled		Ini
High	Authentication Methods Changed for Privileg...	Scheduled	Azure Active Directory	Pe
High	SUNBURST and SUPERNOVA backdoor hashe...	Scheduled		
High	Solorigate Named Pipe	Scheduled	Security Events via Leg... +1 ⓘ	
High	Azure VM Run Command operation executed	Scheduled	Azure Activity	

< Previous Page 1 of 9 Next >

User login from different countries within 3 hours (.)

High
Severity

Scheduled
Rule Type

Initial Access (1)

Rule query

```
let timeframe = ago(3h);
let threshold = 2;
imAuthentication
| where TimeGenerated > timeframe
| where EventType=='Logon' and
EventResult=='Success'
| where ipnetaddr(CsrcCountry)
```

Note:

- You haven't used this template yet; You can use it to create analytics rules.

Create rule

Analytics rule wizard - Create new rule from template ...

User login from different countries within 3 hours (Uses Authentication Normalization)

General Set rule logic Incident settings (Preview) Automated response Review and create

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

Analytics rule details

Name *

User login from different countries within 3 hours (Uses Authentication Normalizat...

Description

This query searches for successful user logins from different countries within 3 hours.
To use this analytics rule, make sure you have deployed the [ASIM normalization

Tactics and techniques

Initial Access

Severity

High

Status

Enabled Disabled

Click on Next: Set rule logic

Next : Set rule logic >

Analytics rule wizard - Create new rule from template ...

User login from different countries within 3 hours (Uses Authentication Normalization)

Query scheduling

Run query every *

Lookup data from the last * ⓘ

Alert threshold

Generate alert when number of query results

*

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 ⓘ

On Off



Previous

Next : Incident settings (Preview) >

Analytics rule wizard - Create new rule from template ...

User login from different countries within 3 hours (Uses Authentication Normalization)

General Set rule logic **Incident settings (Preview)** Automated response Review and create

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 Disabled

Alert grouping

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 **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

Select entities



Select details



 Entity-based alert grouping can make use **only** of entities mapped using the new version, if any exist. Entities mapped with the old version (that appear in the query code) will be available for grouping **only** if there are no mappings defined using the new version.

Re-open closed matching incidents

Enabled Disabled



Previous

Next : Automated response >

Analytics rule wizard - Create new rule from template ...

User login from different countries within 3 hours (Uses Authentication Normalization)

General Set rule logic ● Incident settings (Preview) Automated response Review and create

Alert automation

Select playbooks to run when a new alert is generated from this analytics rule. The playbooks will receive the alert as their input. Only playbooks configured with the alert trigger can be selected.

Name

No playbooks selected

We can select a previously prepared playbook or we can add a new playbook.

Status

Playbooks in Microsoft Sentinel are **based on workflows built in Azure Logic Apps**, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.

Incident automation (preview)

View all automation rules that will be triggered by this analytics rule and create new automation rules. The automation rule will receive the incident as its input, as will any playbooks called by the automation rule. Only playbooks configured with the incident trigger can be called by automation rules.




+ Add new

Order	Automation rule name	Action
-------	----------------------	--------

Previous **Next : Review >**

General Set rule logic Incident settings (Preview) Automated response Review and create

Analytics rule details

Name	User login from different countries within 3 hours (Uses Authentication Normalization)
Description	This query searches for successful user logins from different countries within 3 hours. To use this analytics rule, make sure you have deployed the ASIM normalization parsers
Tactics and techniques	 Initial Access
Severity	 High
Status	 Enabled

Analytics rule settings

Rule query	<pre>let timeframe = ago(3h); let threshold = 2; imAuthentication where TimeGenerated > timeframe where EventType=='Logon' and EventResult=='Success' where isnotempty(SrcGeoCountry) summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct) , NumOfCountries = dcount(SrcGeoCountry)</pre>
------------	--

Previous

Create

This query will run at the scheduled time across the data

Search (Ctrl+)

Refresh Last 24 hours

- General
 - Overview
 - Logs
 - News & guides
 - Search (Preview)
- Threat management
 - Incidents
 - Workbooks
 - Hunting
 - Notebooks
 - Entity behavior
 - Threat intelligence
- Content management
 - Content hub (Preview)
 - Repositories (Preview)
 - Community
- Configuration
 - Data connectors
 - Analytics

Events 0 Alerts 0 Incidents 0

Incidents by status

New (0) Active (0) Closed (True Positive) (0) Closed (False Positive) (0)

LEARN MORE [Documentation](#)

Search (Ctrl+)

Refresh Last 24 hours

- General
 - Overview
 - Logs
 - News & guides
- Threat management
 - Incidents
 - Workbooks
 - Hunting
 - Notebooks
 - Entity behavior
 - Threat intelligence (Preview)
- Configuration
 - Data connectors
 - Analytics

Events 17.7K ↑ 2.7K Alerts 0 Incidents 9 ↓ 1

Incidents by status

New (9) Active (0) Closed (True Positive) (0) Closed (False Positive) (0)

Events and alerts over time

Alerts

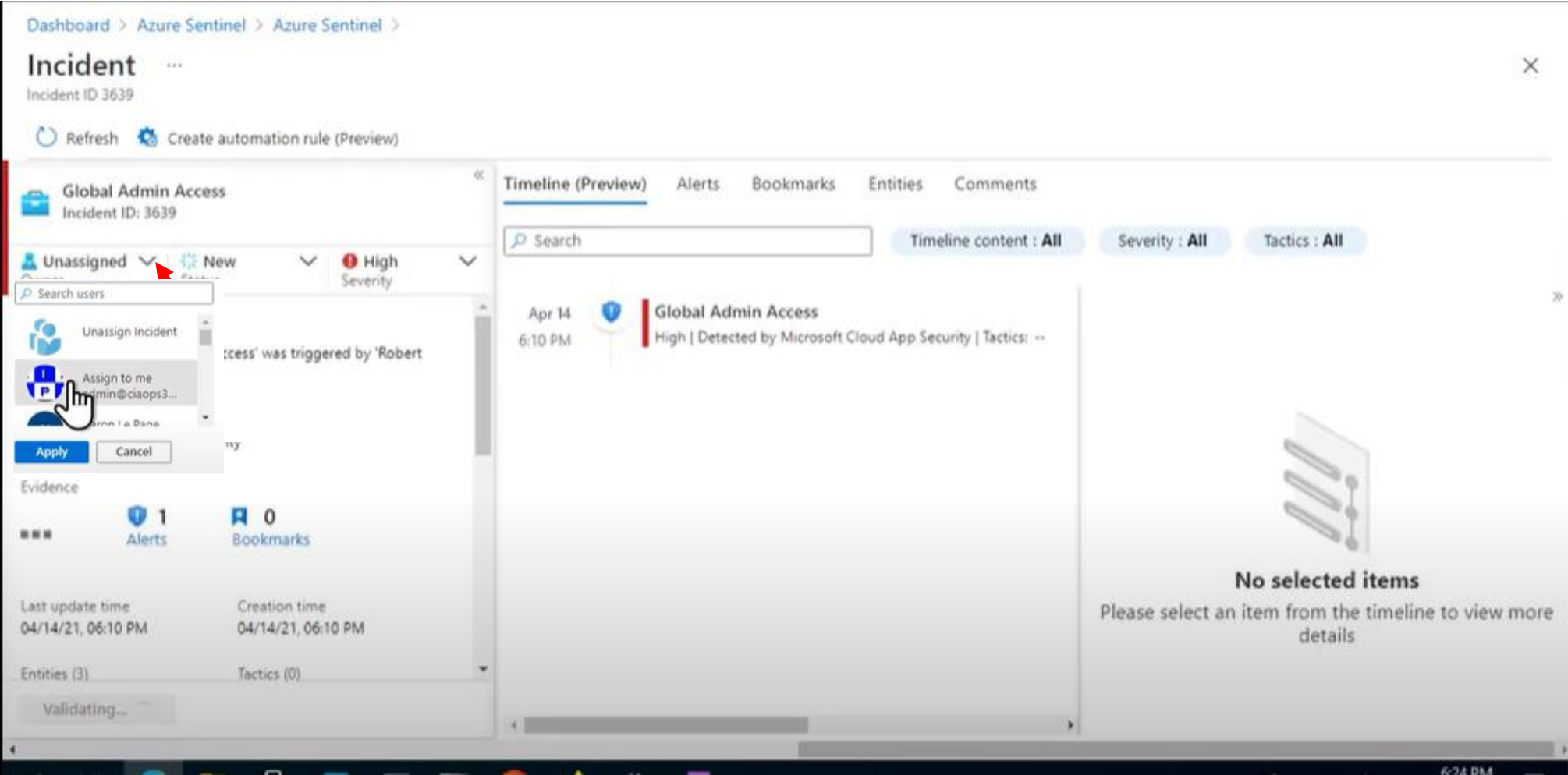
Alert Type	Count
ALERTS	0
O365API_CL	9.3K
AZUREMETRICS	7K
OFFICEACTIVITY	1K
OTHERS (9)	124

Recent incidents

Severity	Incident Name
High	Global Admin A
High	Global Admin A
Medium	Failed logins fr
Low	Logon from an
Low	Logon from an

Under recent incidents select Global Admin Access

Click the down arrow to the right of Assigned and select Assign to me the select Apply



Under New Status click on Active

The screenshot displays the Azure Sentinel incident management interface. At the top, the breadcrumb navigation shows 'Dashboard > Azure Sentinel > Azure Sentinel > Incident'. The incident title is 'Incident' with a three-dot menu icon, and the incident ID is 'Incident ID 3639'. Below the title, there are 'Refresh' and 'Create automation rule (Preview)' buttons.

The main content area is titled 'Global Admin Access' with incident ID 3639. It features a search bar and filter buttons for 'Timeline content : All', 'Severity : All', and 'Tactics : All'. The incident details on the left include the owner 'Robert Cra...', a 'New Status' dropdown menu, and a 'High Severity' indicator. The description is 'Activity policy 'Global Admin Access' on 'Crane''. The alert product name is 'Microsoft Cloud App Security'. Evidence shows 'N/A' for events, '1' for alerts, and '0' for bookmarks. The last update time is '04/14/21, 06:24 PM' and the creation time is '04/14/21, 06:10 PM'. There are 'Entities (3)' and 'Tactics (0)'. An 'Investigate' button is at the bottom left.

The 'New Status' dropdown menu is open, showing three options: 'New', 'Active', and 'Resolved'. A hand cursor is pointing at the 'Active' option. A red arrow points to the 'Apply' button at the bottom of the dropdown. The 'Timeline (Preview)' tab is active, showing a single event on 'Apr 14 6:10 PM' titled 'Global Admin Access' with a severity of 'High' and detected by 'Microsoft Cloud App Security'. The right side of the timeline is empty, displaying a message: 'No selected items. Please select an item from the timeline to view more details.'

On the left view a summary of what's going on. Click on global Admin Access in the middle pane then view information About Global Admin access in the right pane.

The screenshot displays the Azure Sentinel incident response interface. At the top, the breadcrumb navigation shows 'Dashboard > Azure Sentinel > Azure Sentinel > Incident'. The incident title is 'Incident' with a three-dot menu and a close button. Below the title, the incident ID is '3639'. There are buttons for 'Refresh' and 'Create automation rule (Preview)'. The main content area is divided into three panes:

- Left Pane:** Shows incident details for 'Global Admin Access' (Incident ID: 3639). It includes the owner 'Robert Cra...', status 'Active', and severity 'High'. It lists three entities: 'admin@ciaop...', '20.94.203.164', and 'Microsoft Tea...'. There are sections for 'Incident workbook' (Incident Overview) and 'Analytics rule' (Create incidents based on Microsoft Cloud App Security ale...). An incident link is provided: 'https://portal.azure.com/#asset/Microsoft_Azure_Sec...'. An 'Investigate' button is at the bottom.
- Middle Pane:** Titled 'Timeline (Preview)', it shows a search bar and filters for 'Timeline content: All', 'Severity: All', and 'Tactics: All'. A single event is listed: 'Apr 14 6:10 PM Global Admin Access High | Detected by Microsoft Cloud App Security | Tactics: --'. A red arrow points to this event.
- Right Pane:** Titled 'Global Admin Access', it shows a 'Security' category. It lists the same three entities as the left pane. It also displays 'System alert ID: Se4e8c2d-2f7c-18b5-31...', 'Rule name: --', 'Time generated: 04/14/21, 06:10 PM', 'Updates: 0', 'Start time: 04/14/21, 06:10 PM', 'End time: 04/14/21, 06:10 PM', and an 'Alert link'.

Select Alerts and view the Alert below

Dashboard > Azure Sentinel > Azure Sentinel >

Incident ...

Incident ID 3639

Refresh Create automation rule (Preview)

Global Admin Access
Incident ID: 3639

Robert Cra... Active High
Owner Status Severity

Analytics rule
Create incidents based on Microsoft Cloud App Security ale...

Tags

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Sec...

Last comment (Total: 0)

Write a comment...

Investigate

Timeline (Preview) **Alerts** Bookmarks Entities Comments

Search Severity: All

Severity	Alert name	Alert status	Alert ID	Product name	Events
High	Global Admin Access	New	5e4e8c2d-2f7c-18b5-...	Microsoft Cloud App S...	N/A

Selecting Entities shows the email address or account that caused the incident and you can see that It is generated from Microsoft teams

Dashboard > Azure Sentinel > Azure Sentinel >

Incident

Incident ID 3639

Refresh Create automation rule (Preview)

Global Admin Access
Incident ID: 3639

Robert Cra...
Owner

Active
Status

High
Severity

Analytics rule
Create incidents based on Microsoft Cloud App Security ale...

Tags
+

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Sec...

Last comment (Total: 0)

Write a comment...

Investigate

Timeline (Preview) Alerts Bookmarks **Entities** Comments

View entities full details [here](#)

Search

Entities : All

Name ↑↓	Type ↑↓
admin@ciaops365.com	Account
20.94.203.164	IP
Microsoft Teams	Cloud Application

We can now select Investigate

Dashboard > Azure Sentinel > Azure Sentinel >

Incident ...

Incident ID: 3639

Refresh Create automation rule (Preview)

Global Admin Access
Incident ID: 3639

Robert Cra...
Owner

Active
Status

High
Severity

Analytics rule
Create incidents based on Microsoft Cloud App Security ale...

Tags

Incident link

Last comment (Total: 0)

Investigate

Timeline (Preview) Alerts Bookmarks **Entities** Comments

[View entities full details here](#)

Entities : All

Name ↑↓	Type ↑↓
admin@ciaops365.com	Account
20.94.203.164	IP
Microsoft Teams	Cloud Application

Here we see an investigation graph. We can click on the last incident to find out more. We can also click on the name to view more information

Dashboard > Azure Sentinel > Azure Sentinel > Incident >

Investigation

Undo Redo

Global Admin Access Incident

High Severity **Active** Status

Robert Crane wner

4/14/2021, 6:25:03 PM Last incident update time

AccountName
admin

UpnSuffix
ps365.com

AadTenantId
5243d63d-7632-4d07-a77e-de0fea1b77a4

AadUserId
b75e7296-a058-4707-acb8-6021a3dca444

AadUserId
b75e7296-a058-4707-acb8-6021a3dca444

isDomainJoined
true

DisplayNam
Robert Cr

SyncFromAad
True

Address
20.94.203.164

FriendlyName
20.94.203.164

Timeline

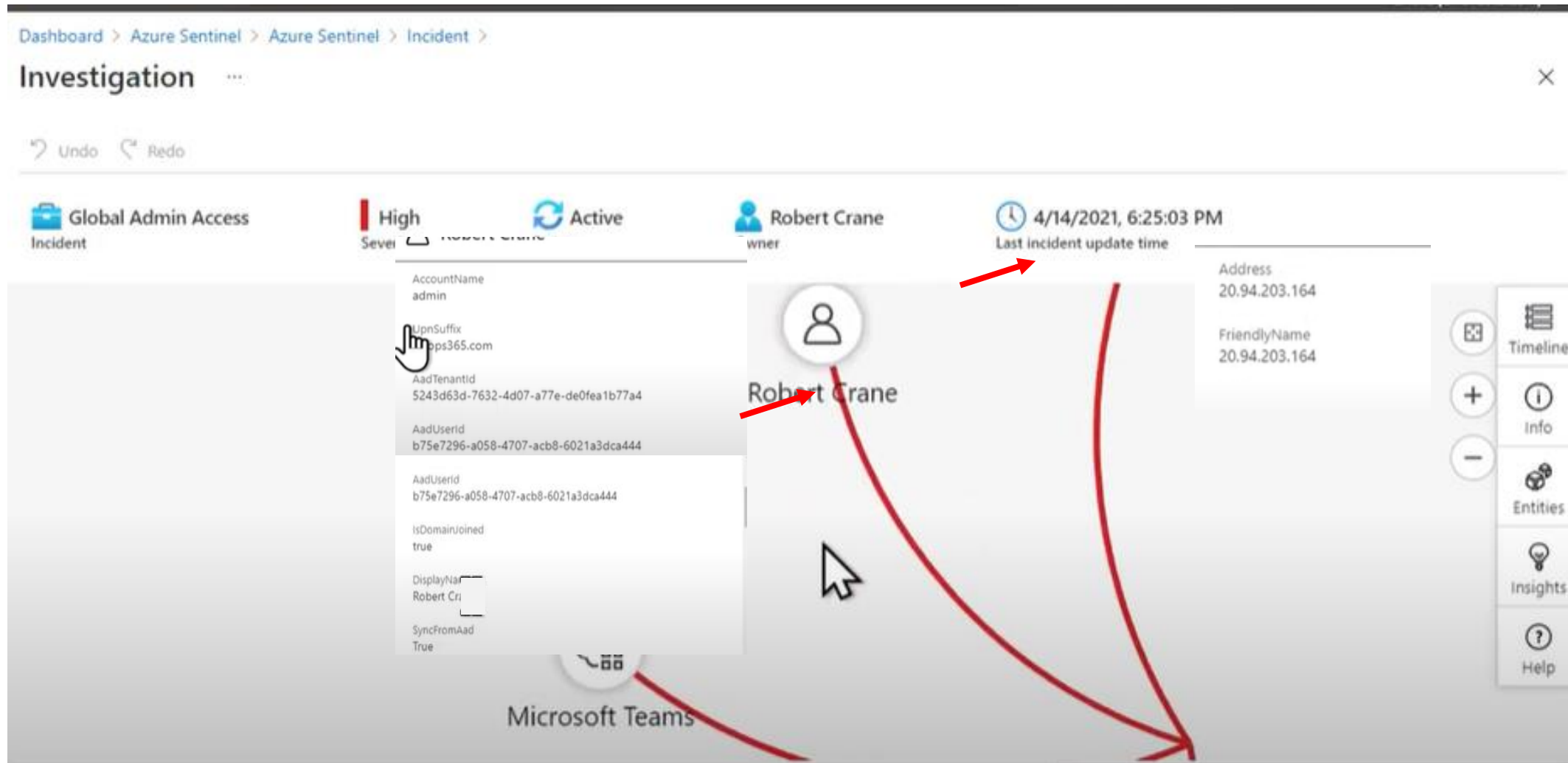
Info

Entities

Insights

Help

Microsoft Teams



Once the investigation is finished we can click on closed under Active Status, select Benign for the classification

Dashboard > Azure Sentinel > Azure Sentinel >

Incident

Incident ID 3639

Refresh Create automation rule (Preview)

Global Admin Access

Incident ID: 3639

Robert Cra... Owner Active Status High Severity

Analytics rule Create incidents base

Tags

Incident link <https://portal.azure>

Last comment

Write a comment...

Investigate

Active Status

New

Active

Closed

Select classification ^

- True Positive - suspicious activity
- Benign Positive - suspicious but expected
- False - incorrect alert logic
- False Positive - inaccurate data
- Undetermined

Apply Cancel

Timeline (Preview) Alerts Bookmarks Entities Comments

Search

Timeline content : All Severity : All Tactics : All

Apr 14 6:10 PM Global Admin Access High | Detected by Microsoft Cloud App Security | Tactics: --

Global Admin Access

Security

Entities (3)

- admin@ciaop...
- 20.94.203.164
- Microsoft Tea...

Tactics (0)

System alert ID

5e4e8c2d-2f7c-18b5-31...

Rule name

--

Time generated

04/14/21, 06:10 PM

Updates

0

Start time

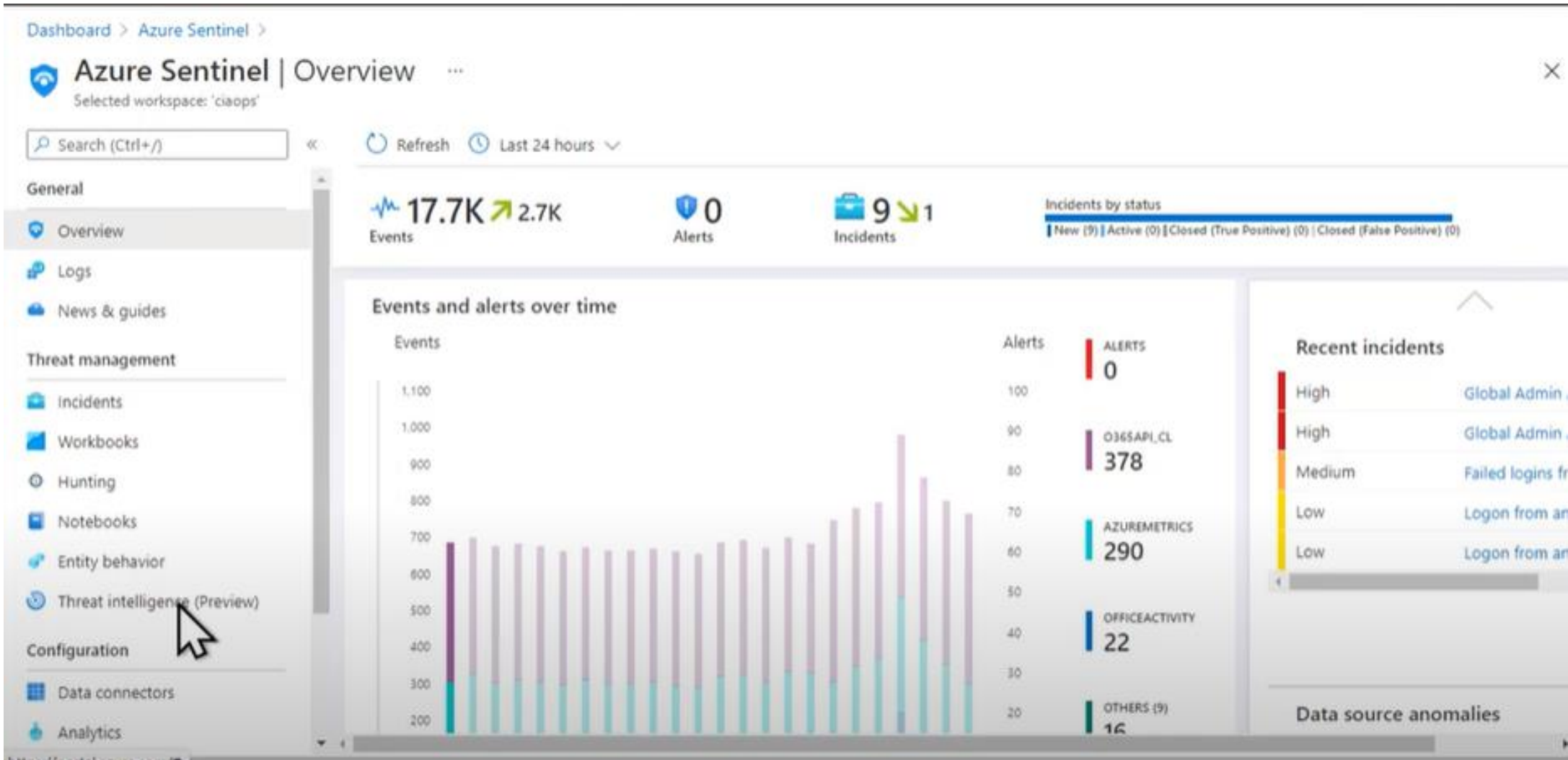
04/14/21, 06:10 PM

End time

04/14/21, 06:10 PM

Alert link

We could then work through each of the recent incidents.



Step 1: Select Data connectors to bring data in Microsoft Sentinel

Step 2: Analytics – the queries that run across that data on a regular basis

Step 3: The Overview that shows the incidents that we need to go in and investigate

