


Security Insight Foundations Deployment Guide


About

Security Insight Foundations is an Azure Marketplace, Azure Application deployment of Microsoft Sentinel with the ability to select a range of Microsoft Azure, Defender and M365 connectors and solutions.

Security Insight Foundations is deployed inside of a specific Resource Group and deploys nearly all required components for a Microsoft Sentinel deployment in a matter of minutes.

 This is a managed application deployment which means LAB3 has full control within the specific Resource Group. It is recommended to start with an empty resource group to limit the scope of permissions provided as part of the deployment.

To remove the deployment, delete the Resource Group. This will delete the Azure Application and all of the data.

 If the Resource Group is deleted there is no way to retain the log analytics or any data.

Inputs & Prerequisites

This deployment requires:

1. An Azure Subscription.
2. An empty Azure Resource Group on which you have Owner or Contributor permissions.
3. Optional - Ability to apply Azure Policy (Security Administrator permission at the tenant level).
4. Optional - Access to a repo such as GitHub or Azure DevOps to apply additional solutions and workbooks.

Deploy Security Insight Foundations From Azure Marketplace

▼ Locate the offer, select the Plan and click Create

1. From Azure Marketplace, Select the Security Insight Foundations Plan and click **Create**.

[Home](#) >

Security Insight

LAB3 Solutions



Security Insight [Remove from Favorites](#)

LAB3 Solutions | Azure Application

Plan

[Private](#) Security Insight Foundation... ▼

[Create](#)

[Overview](#) [Plans + Pricing](#) [Usage Information + Support](#) [Ratings + Reviews](#)

About

Security Insight leverages automation to provide greater threat detection & response for distributed and autonomous xOps teams. Think architectures in weeks and deployments in minutes, not months. Security Insight automates deployment, maintenance, and ongoing cyber security detection & response. It bridges *cloud* and *as a Service* to on premises security operations for businesses, government and Managed Security Service Providers (MSSP).

▼ Select the Subscription, Resource Group, Region and Application Name

Under the Basics tab select the Subscription, Resource Group, Region, and Application Name and click **Next:Features >**

[Home >](#) [Security Insight >](#)

Create Security Insight ...

LAB3 SECURITY INSIGHT LEVERAGES AUTOMATION TO PROVIDE GREATER THREAT DETECTION & RESPONSE FOR DISTRIBUTED AND AUTONOMOUS XOPS TEAMS

Think architectures in weeks and deployments in minutes, not months. Security Insight automates deployment, maintenance, and ongoing cyber security detection & response. It bridges *cloud* and *as a Service* to on premises security operations for businesses, government and Managed Security Service Providers (MSSP).

Security Insight provides rapid speed to value, security posture visibility, risk insight, and cyber security assurance automation for distributed and autonomous XOps teams.

Project details

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

Subscription * ⓘ	LAB3 Security Sandbox	▼
Resource group * ⓘ	(New) krsi	▼

[Create new](#)

Instance details

Region * ⓘ	Australia East	▼
------------	----------------	---

Managed Application Details

Provide a name for your managed application, and its managed resource group. Your application's managed resource group holds all the resources that are required by the managed application which the consumer has limited access to.

Application Name *	krsi	✓
Managed Resource Group * ⓘ	mrg-security_insight-20230623094730	✓

[Review + create](#)

[< Previous](#)

[Next : Features >](#)

▼ Enable the Log Sources for the Deployment

Under the Features tab enable the log sources required and click Next:Config >

Create Security Insight ...

Basics **Features** Config Review + create

Please select the features you would like to enable in Security Insight.
[Learn more](#)

Features

Select the features you would like to enable in Security Insight.
[Read more](#)

Select log sources * ⓘ

14 selected

- Select all
- Monitoring Dashboards
Sentinel Dashboards that provide enhanced visibility on security operations
- Office 365
Monitor activity on Office365 applications
- Azure Active Directory
Monitor user activity in Active Directory. Includes EUBA (End User Behavior Analytics)
- Azure Activity
Monitor activity on Azure Resources such as read/write/create/delete operations
- Azure DDOS
Monitor activity on the Azure DDOs service
- Azure DevOps
Monitor activity on Azure DevOps organisations
- Azure Firewall

[Review + create](#) [< Previous](#) [Next: Config >](#)

∨ Select the Log Retention and any Capacity Reservation

Under the Config tab select the Log Retention period in days that is required and if applicable a Capacity Reservation Tier for storage in GB and click Next : Review + create >

Create Security Insight ...

Basics Features **Config** Review + create

Please select any additional Microsoft Sentinel workspace configuration options.
[Learn more](#)

Workspace Configuration

Select the workspace configuration options for the Microsoft Sentinel workspace.
[Read more](#)

Log Retention (Days) * ⓘ	<input type="text" value="90"/>
Capacity Reservation Tier In GB ⓘ	<input type="text" value="0"/> ▼

Review + create


< Previous

Next : Review + create >

✓ Review and Agree to the Terms and Conditions

Review the information for any errors and check the box to agree to the terms and conditions and click Create.

Create Security Insight

 Validation Passed

Co-Admin Access Permission

By checking the box and clicking "Create" I give permission for the template provider referenced above (the "Provider") to have Administrative-level access to one or more Azure resources in order to provide support and management services for the template. In the event of an issue arising from a Provider's services or failure to provide services, your sole recourse is with the Provider. Unless Microsoft is the Provider, Microsoft (i) does not approve, monitor or manage the Provider's access, and (ii) bears no responsibility whatsoever for acts or omissions of a Provider.

I agree to the terms and conditions above. *

Basics

Subscription	LAB3 Security Sandbox
Resource group	krsti
Region	Australia East
Application Name	krsti
Managed Resource Group Name	mrg-security_insight-20230623094730

Features

Select log sources: Monitoring Dashboards, Office 365, Azure Active Directory, Azure Activity, Az...

Config

Log Retention (Days)	90
Capacity Reservation Tier In GB	0

Create

< Previous

Next

[Download a template for automation](#)

Deployment is in progress



lab3solutions.altra_security_insight_core-preview-20230315115335 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

Deployment is in progress

Deployment name: lab3solutions.altra_security_insight_core-previe... Start time: 3/15/2023, 12:05:27 PM
Subscription: LAB3 Security Sandbox Correlation ID: 2910eef0-8cce-4ec5-bdc2-96259af793d7

Deployment details


Resource	Type	Status	Operation details
No results.			

Give feedback

[Tell us about your experience with deployment](#)

Once the deployment is completed, Microsoft Sentinel can be accessed by going to Microsoft Sentinel in Azure Portal and looking for the Sentinel deployment (if there are multiple) with the similar resource group name as deployment name, eg mrg-altra_security_insight_core-preview-20230315115335.

Post Deployment Steps


 The below steps will typically require the person performing each function to have **Security Administrator** of the tenant and **Contributor** to the Resource Group that Security Insight has been deployed into.

Assign Microsoft Sentinel Roles


The following guide provides information on assigning Microsoft Sentinel Roles & permissions:

 [Roles and permissions in Microsoft Sentinel](#)

Apply Azure Policy for Diagnostic Settings (Enable Azure Logging)

 [Diagnostic settings in Azure Monitor - Azure Monitor](#)

 [Enable diagnostics settings by category group using built-in policies. - Azure Monitor](#)

 [Create diagnostic settings at scale using Azure policies and initiatives - Azure Monitor](#)

Enable Azure Active Directory Logging

 [Stream Azure Active Directory logs to Azure Monitor logs - Microsoft Entra](#)

Enable M365 Defender

 [Connect Microsoft 365 Defender data to Microsoft Sentinel](#)


Enable M365

 [Connect Microsoft Sentinel to other Microsoft services with an API-based data connector](#)

Enable Security Insight Threat Intelligence Feed

▼ Enable Security Insight Threat Intelligence Feed

Enable the Security Insight Threat Intelligence feed.

 The following directory roles are required (at a minimum) in the client environment:

- [Cloud Application Administrator](#) - to create an app registration and assign graph permissions

 An email address (distribution list) where daily activity reports will be sent is required

1. Enable **Threat Intelligence connector** in Microsoft Sentinel by going to Configuration, Data Connectors, Threat Intelligence Platforms (Preview), Open Connector page

124
Connectors

16
Connected

More content at
Content hub

Search by name or provider

Providers : All

Data Types : All

Status : All

Threat Intelligence Platforms (...)

Status ↑ Connector name

Microsoft

Threat Intelligence Platforms (Preview)
Microsoft

Connected
Status

Microsoft
Provider

23 Min...
Last Log Rec...

Description

Microsoft Sentinel integrates with Microsoft Graph Security API data sources to enable

2. Create the application registration

⚠ The application registration needs to be created inside the **client's tenant**

The app registration is what Security Insight Threat Intelligence uses to authenticate to the client tenant and submit threat indicators to their security graph.

1. Create a new application registration
2. Enter a name for the application. E.g. `app-security-cteye-intel`
3. Select "Accounts in this organization's directory only - Single tenant"
4. Click Register

Dashboard > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

app-security-cteye-intel

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (LAB3 PTY LTD only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform

✔ Note down the `ClientId` and `TenantId` of the app registration. You will need it when adding the client details to the CTEye application later

app-security-cteye-intel

Search (Ctrl+/) Delete Endpoints Preview features

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD)

Essentials

Display name : app-security-cteye-intel

Application (client) ID : 317d5d7c-4b74-4ee3-ac61-f881abfec47c

Object ID : 1c659f73-a106-4411-9630-716fa9089ec7

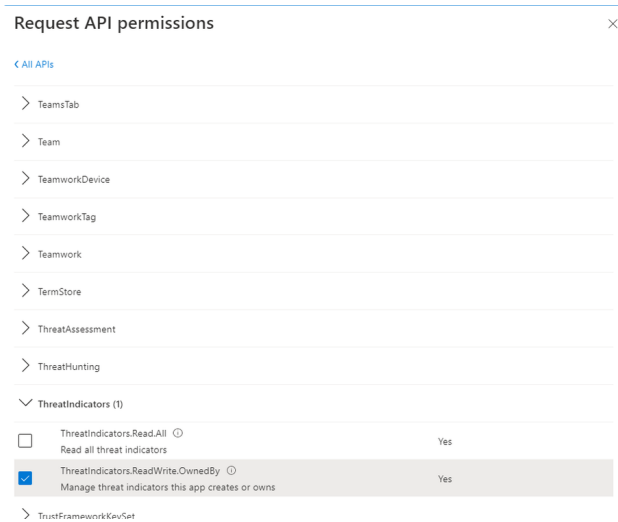
Directory (tenant) ID : e65107ae-deaa-4f76-b79e-c4b5067a5929

Supported account types : My organization only

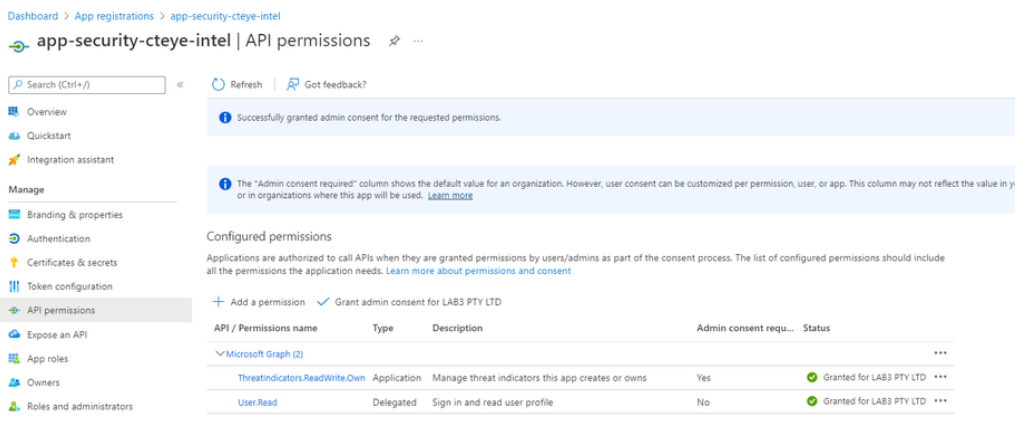
3. Grant graph permissions to the app registration

ⓘ Special permissions need to be granted to the app registration so it can submit intel to the Microsoft Security Graph

1. Click "API permissions"
2. Click "+Add a permission"
3. Click "Microsoft Graph"
4. Select Application permissions
5. Check the **ThreatIndicators.ReadWrite.OwnedBy** permission



6. Click "Add Permissions"
7. Click "Grant admin consent"
8. Click "Yes" to confirm the admin consent



4. Contact SI.Support@altra.cloud with the client notification email address, Client ID and Tenant ID to be onboarded to Threat Intelligence.


Enable Sentinel Repo for Content (Optional)

[Deploy custom content from your repository - Microsoft Sentinel](#)

Outputs

A successful deployment of Security Insight with the Microsoft Azure, Defender and M365 packages.

Managing Security Insight - Getting Started with Security Detection & Response

 Security Insight deploys sets of pre configured **content** to enable clients to start receiving alerts and incidents for specified data sources sooner and without additional configuration of Microsoft Sentinel.

 The Microsoft Sentinel Training Lab provides an overview of how to use Sentinel

 [Azure-Sentinel/Solutions/Training/Azure-Sentinel-Training-Lab at master · Azure/Azure-Sentinel](#)

Microsoft Sentinel **content** is Security Information and Event Management (SIEM) content that enables customers to ingest data, monitor, alert, hunt, investigate, respond, and connect with different products, platforms, and services in Microsoft Sentinel.

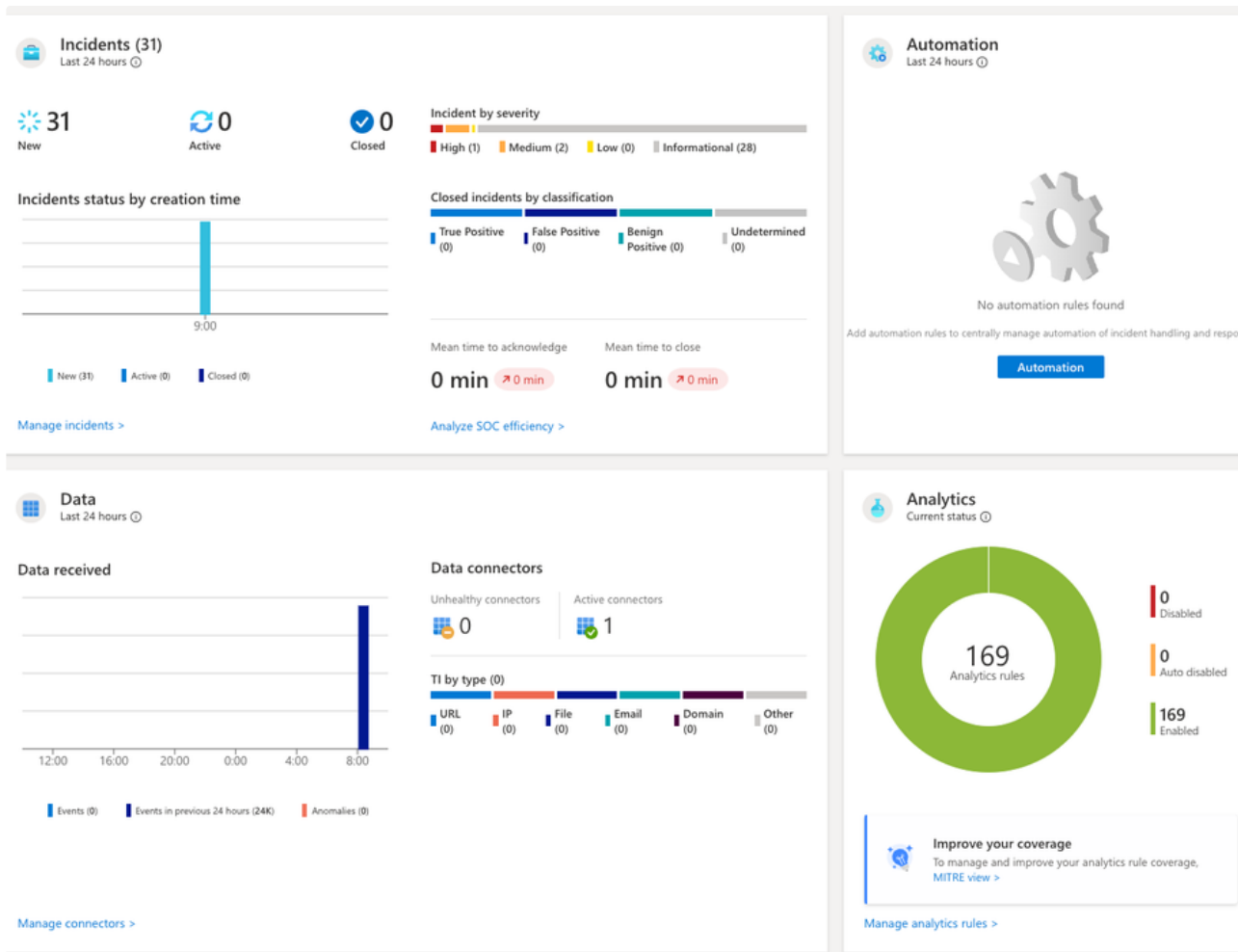
Content in Microsoft Sentinel includes any of the following types:

- **Data connectors** provide log ingestion from different sources into Microsoft Sentinel
- **Parsers** provide log formatting/transformation into ASIM formats, supporting usage across various Microsoft Sentinel content types and scenarios
- **Workbooks** provide monitoring, visualization, and interactivity with data in Microsoft Sentinel, highlighting meaningful insights for users
- **Analytics** rules provide alerts that point to relevant SOC actions via incidents
- **Hunting queries** are used by SOC teams to proactively hunt for threats in Microsoft Sentinel
- **Notebooks** help SOC teams use advanced hunting features in Jupyter and Azure Notebooks
- **Watchlists** support the ingestion of specific data for enhanced threat detection and reduced alert fatigue
- **Playbooks** and Azure Logic Apps custom connectors provide features for automated investigations, remediations, and response scenarios in Microsoft Sentinel

Overview Dashboard

Security Insight deploys a number of prepackaged Azure Monitor workbooks and visual dashboards. To get started with Security Detection and Response the Overview Dashboard provides a snapshot of the security posture of the organisation.

See  [Visualize collected data](#) for additional information.



Incidents

Before you begin managing incidents, it's important to understand the following key incident management concepts in Microsoft Sentinel:

- **Data connectors.** You can use data connectors in Microsoft Sentinel to ingest and collect data from security-related services. These events are forwarded to a Log Analytics workspace associated with Microsoft Sentinel. Events can be collected from Linux or Windows computers running the Log Analytics agent, from a Linux syslog server (for devices like firewalls or proxies), or directly from Microsoft Azure services.
- **Events.** Microsoft Sentinel stores events in a Log Analytics workspace. These events contain the details of security-related activity that you want to monitor with Microsoft Sentinel.
- **Analytic rules.** You can create analytics rules to detect important security events and generate alerts. You can create analytics rules by using built-in templates or by using custom Kusto Query Language (KQL) queries against Log Analytics workspaces in Sentinel.
- **Alerts.** Analytics rules generate alerts when they detect important security events. You can also configure alerts to generate incidents.
- **Incidents.** Microsoft Sentinel creates incidents from analytics rule alerts. Incidents can contain multiple related alerts. You'll use each incident as a starting point and tracking mechanism for investigation into security concerns in your environment.

The **Incidents** page provides a complete list of incidents in Microsoft Sentinel. It also provides basic incident information, including severity, ID, title, alerts, product names, created time, last update time, owner, and status. You can sort by any incident column and filter the incident list by name, severity, status, product name, or owner.

Selecting any incident will display more information about the incident in the **Details** column. This information can help you clarify the nature, context, and course of action for an incident.

The **Incident details** page provides a description of the incident and lists the evidence, entities, and tactics related to the incident. It also contains links to associated workbooks and the analytic rule that generated the incident.

You can further investigate an incident by selecting **Investigate** on the **Incident details** page. This action opens the investigation graph, a visual tool that helps to identify entities involved in the attack and the relationships between those entities. If the incident involves multiple alerts over time, you can also review the alert timeline and correlations between alerts.

You can select each entity on the graph to observe more information about the entity. This information includes relationships to other entities, account usage, and data flow information. For each information area, you can go to the related events in Log Analytics and add the related alert data into the graph.

See [Navigate and investigate incidents in Microsoft Sentinel](#) for more information.

The screenshot displays the Microsoft Sentinel incident management interface. At the top, there are navigation options like 'Create incident (Preview)', 'Refresh', and 'Last 24 hours'. Below this, a summary shows '31 Open incidents', '31 New incidents', and '0 Active incidents'. A bar chart indicates 'Open incidents by severity' with 1 High, 2 Medium, 0 Low, and 28 Informational incidents. The main table lists incidents with columns for Severity, Incident ID, Title, Alerts, Product names, and Created time. The right-hand pane provides detailed information for incident ID 30, including a description, alert product names, evidence counts, last update and creation times, entities, tactics and techniques, incident workbook, analytics rule, tags, and incident link.

Severity	Incident ID	Title	Alerts	Product names	Created time
Medium	30	Malicious Inbox Rul...	6	Microsoft Sentinel	04/14/23, 12:02 PM
Medium	29	Sign-ins from IPs th...	6	Microsoft Sentinel	04/14/23, 12:02 PM
High	31	Solorigate Network ...	6	Microsoft Sentinel	04/14/23, 12:02 PM
Informational	28	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	27	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	26	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	25	LAB ³ - Device Info L...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	24	LAB ³ - Device Netw...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	23	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	22	LAB ³ - Device File C...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	21	LAB ³ - Device Logon...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	20	Altra - Monitor Audi...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	19	LAB ³ - Device Image...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	18	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	17	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	16	LAB ³ - Device Proce...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	15	LAB ³ - Device Netw...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	14	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	13	LAB ³ - Email Url Info...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	12	Altra - Monitor Offic...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	11	Altra - Monitor Azur...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	10	LAB ³ - Device Regist...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	9	LAB ³ - Cloud App Ev...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	8	LAB ³ - Device Events...	1	Microsoft Sentinel	04/14/23, 11:45 AM
Informational	7	LAB ³ - Identity Quer...	1	Microsoft Sentinel	04/14/23, 11:45 AM

Entity Behaviour

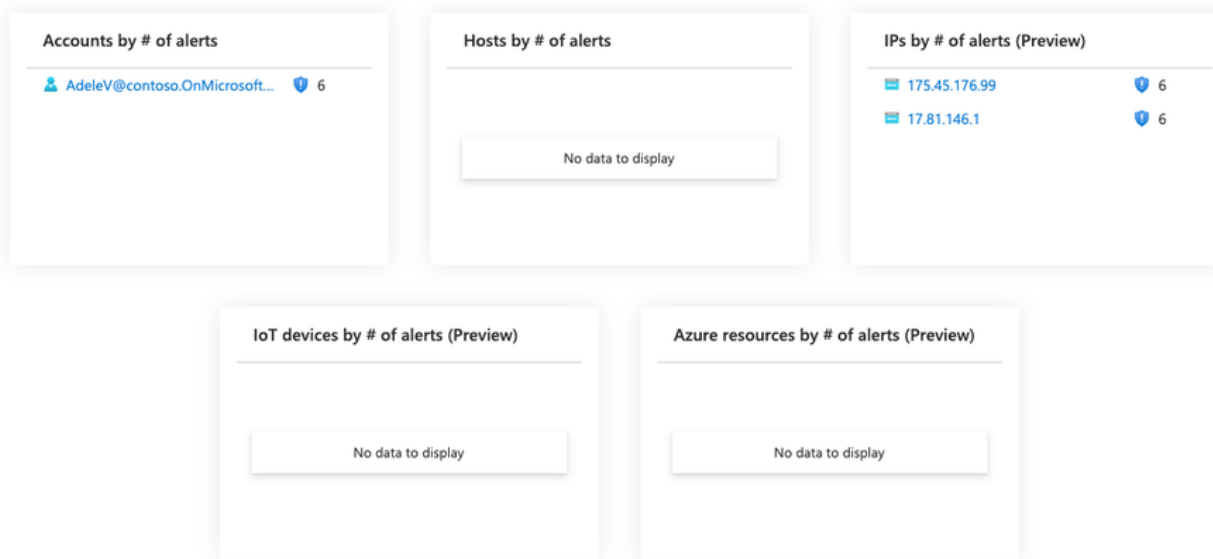
The Entity behavior page allows you to search for entities or select from the list of already displayed entities. Once selected the Entity page is displayed with information and timeline of alerts and activities

The Incident Investigation Graph includes an option for **Insights**. Insights display information from the Entity behavior data.

Entity pages are designed to be part of multiple usage scenarios, and can be accessed from incident management, the investigation graph, bookmarks, or directly from the entity search page under **Entity behavior analytics** in the Microsoft Sentinel main menu.



Search for accounts, hosts, IP addresses, IoT devices or Azure resources



Logs

Microsoft Sentinel Logs provide you access to the various logs collected from the security connectors. Microsoft Sentinel collects these logs from its integrated connectors and stores them in the Azure Log Analytics workspace. The Log Analytics workspace is a repository that stores data and configuration information. You can create queries to filter important information, which you can then use to create analytics rules and detect threats.

You can search for specific logs on the **Microsoft Sentinel Logs** page, which you can access from the navigation pane in Microsoft Sentinel.

The **Logs** page has four main parts:

- The page header contains links to the **Queries**, **Query explorer**, settings, and help section.
- The **Tables** pane displays collected data from the logs in tables, each comprising multiple columns.
- The query pane is where you write your own query expressions.
- The query result pane displays the results of your queries.

One of the primary activities of a security team is to search logs for specific events. For example, you might search logs for the activities of a specific user within a given time-frame.

In Microsoft Sentinel, you can search across long time periods in large datasets by using a search job. While you can run a search job on any type of log, search jobs are ideally suited to search archived logs. If you need to do a full investigation on archived data, you can restore that data into the hot cache to run high performing queries and analytics.

Use a search job when you start an investigation to find specific events in logs within a given time frame. You can search all your logs to find events that match your criteria and filter through the results.

Search in Microsoft Sentinel is built on top of search jobs. Search jobs are asynchronous queries that fetch records. The results are returned to a search table that's created in your Log Analytics workspace after you start the search job. The search job uses parallel processing to run the search across long time spans, in large datasets. So search jobs don't impact the workspace's performance or availability.

Search results remain in a search results table that has a ***_SRCH** suffix.

Use search to find events in any of the following log types:

- Analytics logs
- Basic logs

Before you start a search job, be aware of the following limitations:

- Optimized to query one table at a time.
- Search date range is up to one year.
- Supports long running searches up to a 24-hour time-out.
- Results are limited to one million records in the record set.
- Concurrent execution is limited to five search jobs per workspace.
- Limited to 100 search results tables per workspace.
- Limited to 100 search job executions per day per workspace.

When you need to do a full investigation on data stored in archived logs, restore a table from the Search page in Microsoft Sentinel. Specify a target table and time range for the data you want to restore. Within a few minutes, the log data is restored and available within the Log Analytics workspace. Then you can use the data in high-performance queries that support full KQL.

A restored log table is available in a new table that has a ***_RST** suffix. The restored data is available as long as the underlying source data is available. But you can delete restored tables at any time without deleting the underlying source data. To save costs, we recommend you delete the restored table when you no longer need it.

Before you start to restore an archived log table, be aware of the following limitations:

- Restore data for a minimum of two days.
- Restore data more than 14 days old.
- Restore up to 60 TB.
- Restore is limited to one active restore per table.
- Restore up to four archived tables per workspace per week.
- Limited to two concurrent restore jobs per workspace.

To restore archived log data in Microsoft Sentinel, specify the table and time range for the data you want to restore. Within a few minutes, the log data is available within the Log Analytics workspace. Then you can use the data in high-performance queries that support full KQL.

You can restore archived data directly from the Search page or from a saved search.

To save costs, it is recommend you delete the restored table when you no longer need it. When you delete a restored table, Azure doesn't delete the underlying source data.

Reporting and Workbooks

Most of the data connectors Microsoft Sentinel uses to ingest data come with their own workbooks. You can get better insight into the data that is being ingested by using tables and visualizations, including bar and pie charts. You can also make your own workbooks from the beginning instead of using the predefined templates.

You can access the **Workbook** page from the Microsoft Sentinel from the navigation pane.


The **Workbook** page consists of the:

- Workbook header. You can add a new workbook and review the saved workbooks and templates that are available on the **Workbook** page.
- Templates section. You can access existing workbook templates on the **Templates** tab. You can save some of the workbooks for quick access and they'll appear on the **My workbooks** tab.

From the **Templates** page, you can select an existing workbook to display a details pane for it, which contains additional information for the templates. The details pane also contains information about the required data types and data connectors that must be connected to Microsoft Sentinel. You can also review how the report will display.

See [Create a Power BI report from Microsoft Sentinel data](#) for creating PowerBI reports.

Support & Feedback

 The most common reason for deployment failures is as a result of resource limits in the Azure subscription or insufficient permissions. Check that subscription limits have not been reached and then delete the failed deployment and try a new deployment. If the deployment fails please email the error reason to SI.Support@altra.cloud.

Email support is available for product deployment issues relating to Security Insight. This does not include any Azure problems or issues. Please email SI.Support@altra.cloud including any error messages and we will endeavour to respond within two business days.

We are unable to assist with any other issues or provide any assistance in terms of using Microsoft Sentinel such as using the toolsets or writing custom analytics or playbooks.

Any feedback or feature requests may also be sent to SI.Support@altra.cloud.

Microsoft Documentation

[Detect and respond to modern attacks with unified SIEM and XDR capabilities](#)

[Security incident management in Microsoft Sentinel - Training](#)

[Identify threats with Behavioral Analytics - Training](#)

[Query, visualize, and monitor data in Microsoft Sentinel - Training](#)

[Microsoft Sentinel documentation](#)

[Microsoft Sentinel data connectors](#)

[Microsoft Sentinel Pricing | Microsoft Azure](#)

[Create a codeless connector for Microsoft Sentinel](#)

[Azure-Sentinel/Solutions/Training/Azure-Sentinel-Training-Lab at master · Azure/Azure-Sentinel](#)