Welcome to the Nashua CLOUD .NET User Group

Akumina, Nashua, NH (Online)

Tuesday, April 20th, 2021

About me!

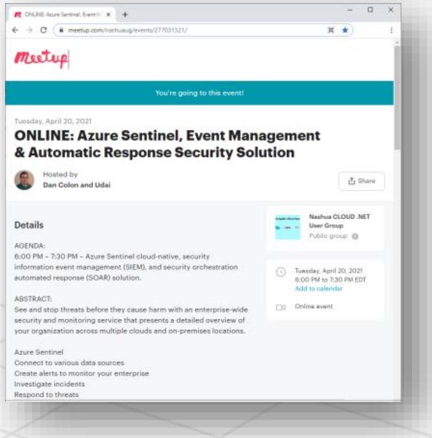
Daniel Colón

https://www.linkedin.com/in/danielecolon/

A+, Security+, Azure Solutions Architect Expert

New Hampshire Cloud User Group

https://www.meetup.com/nashuaug



ONLINE: Azure Sentinel, Event M
meetup.com/nashuaug/events/277031321/
Meetup
Share

You're going to this event!

Tuesday, April 20, 2021

ONLINE: Azure Sentinel, Event Management & Automatic Response Security Solution

Hosted by
Dan Colon and Udai

Details

AGENDA:
6:00 PM – 7:30 PM – Azure Sentinel cloud-native, security information event management (SIEM), and security orchestration automated response (SOAR) solution.

ABSTRACT:
See and stop threats before they cause harm with an enterprise-wide security and monitoring service that presents a detailed overview of your organization across multiple clouds and on-premises locations.

Azure Sentinel
Connect to various data sources
Create alerts to monitor your enterprise
Investigate incidents
Respond to threats

Nashua CLOUD .NET User Group
Public group

Tuesday, April 20, 2021
6:00 PM to 7:30 PM EDT
Add to calendar

Online event

CompTIA A+

CompTIA Security+

Microsoft CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT

Azure Sentinel

Security Information Event Management (SIEM) and
Security Orchestration Automated Response (SOAR) solution

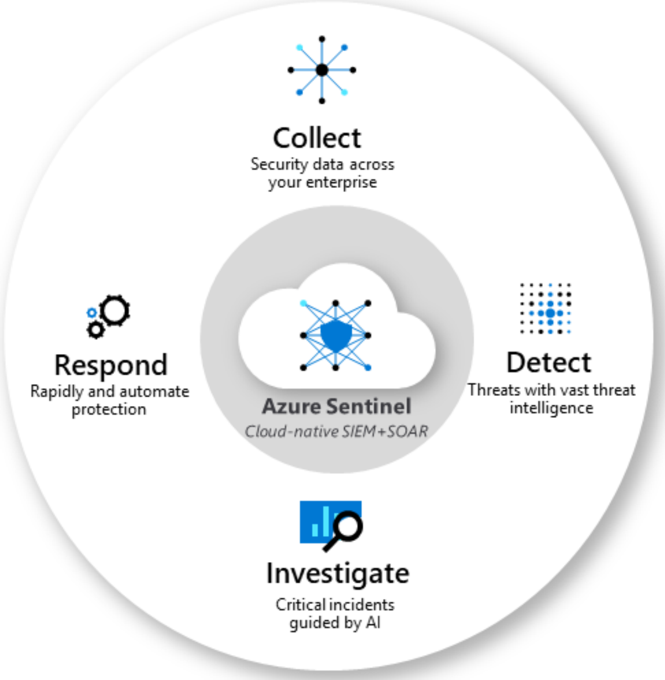
Agenda

- Azure Sentinel
- Onboarding of Azure Sentinel
- Configuration
- Threat Management

Azure Sentinel

Intelligent security analytics and threat intelligence in a single solution for alert detection, threat visibility, proactive hunting, and threat response.

- Collect Data
- Detect
- Investigate
- Respond

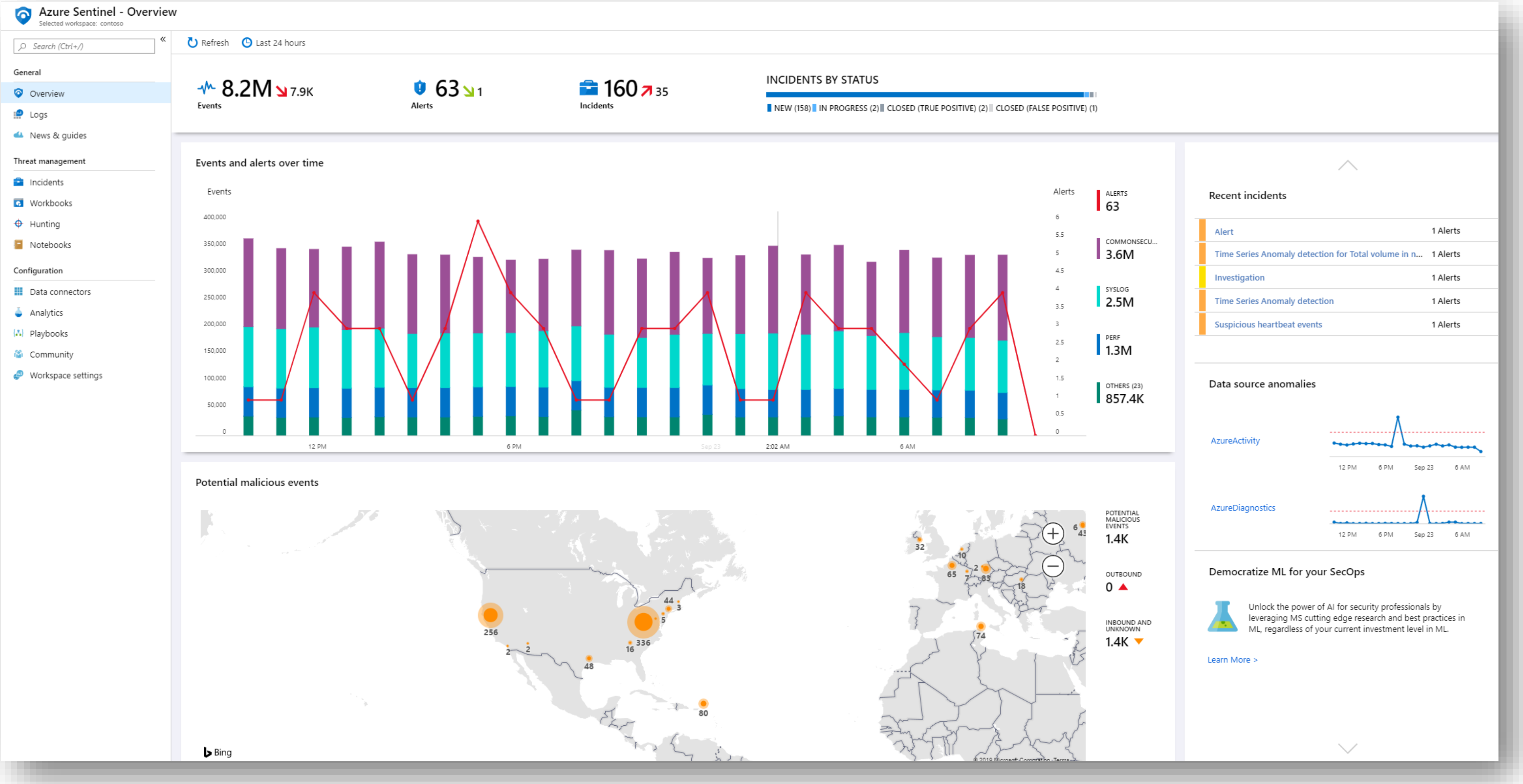

Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Azure Sentinel
Cloud-native SIEM+SOAR
Detect
Threats with vast threat intelligence
Investigate
Critical incidents guided by AI

https://docs.microsoft.com/en-us/azure/sentinel/overview

Azure Sentinel - Use Cases

- Manage incidents across cloud and on-prem
- Automatically respond to potential threats
- Detect previously undetected threats

Azure Sentinel - Overview



Recent incidents	
Alert	1 Alerts
Time Series Anomaly detection for Total volume in n...	1 Alerts
Investigation	1 Alerts
Time Series Anomaly detection	1 Alerts
Suspicious heartbeat events	1 Alerts

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility

Onboarding

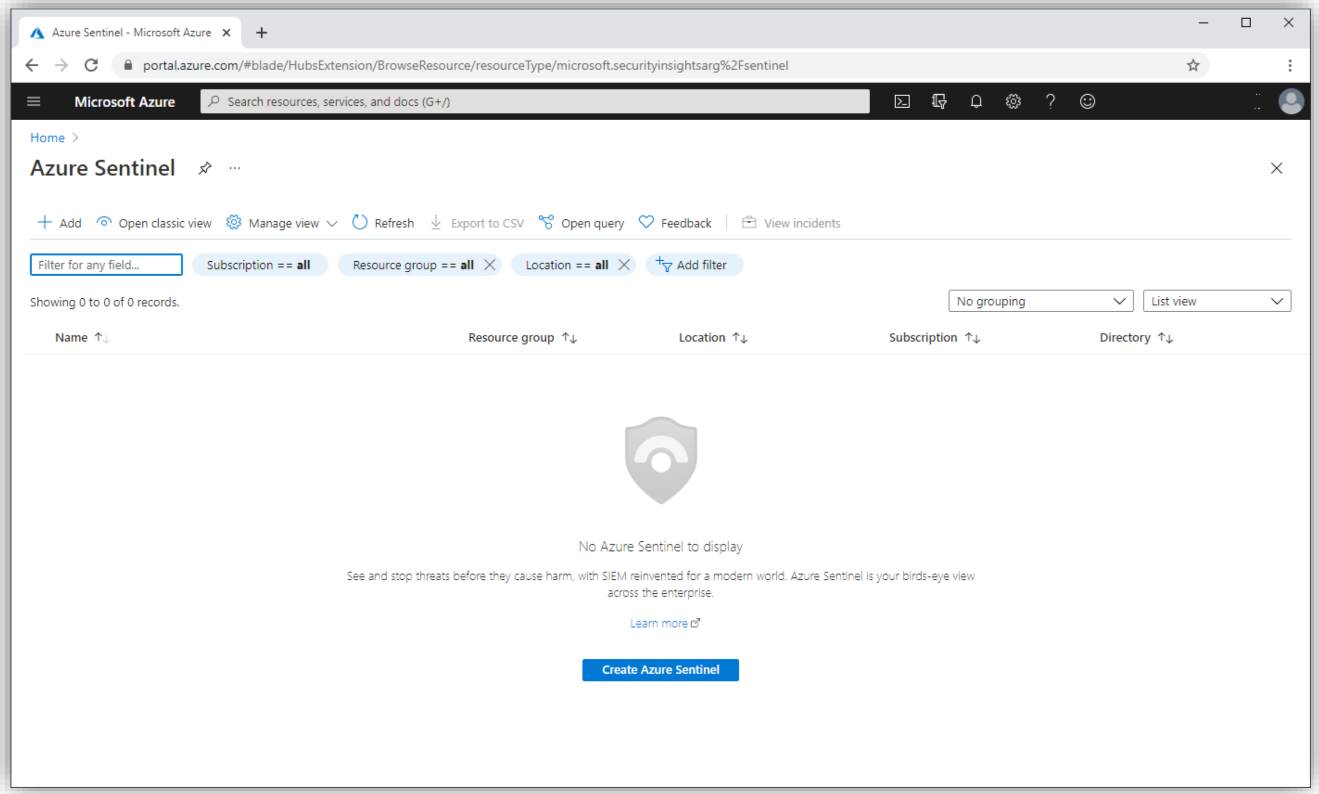
- Enable Azure Sentinel
- Create Azure Analytics Workspace
- Amount of data collected affects pricing

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

Onboarding – Enabling Azure Sentinel

Nothing special here

Azure Sentinel needs at least one workspace to work with



portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/microsoft.securityinsightsarg%2Fsentinel

Azure Sentinel

Subscription == all

Resource group == all

Location == all

Showing 0 to 0 of 0 records.

No grouping

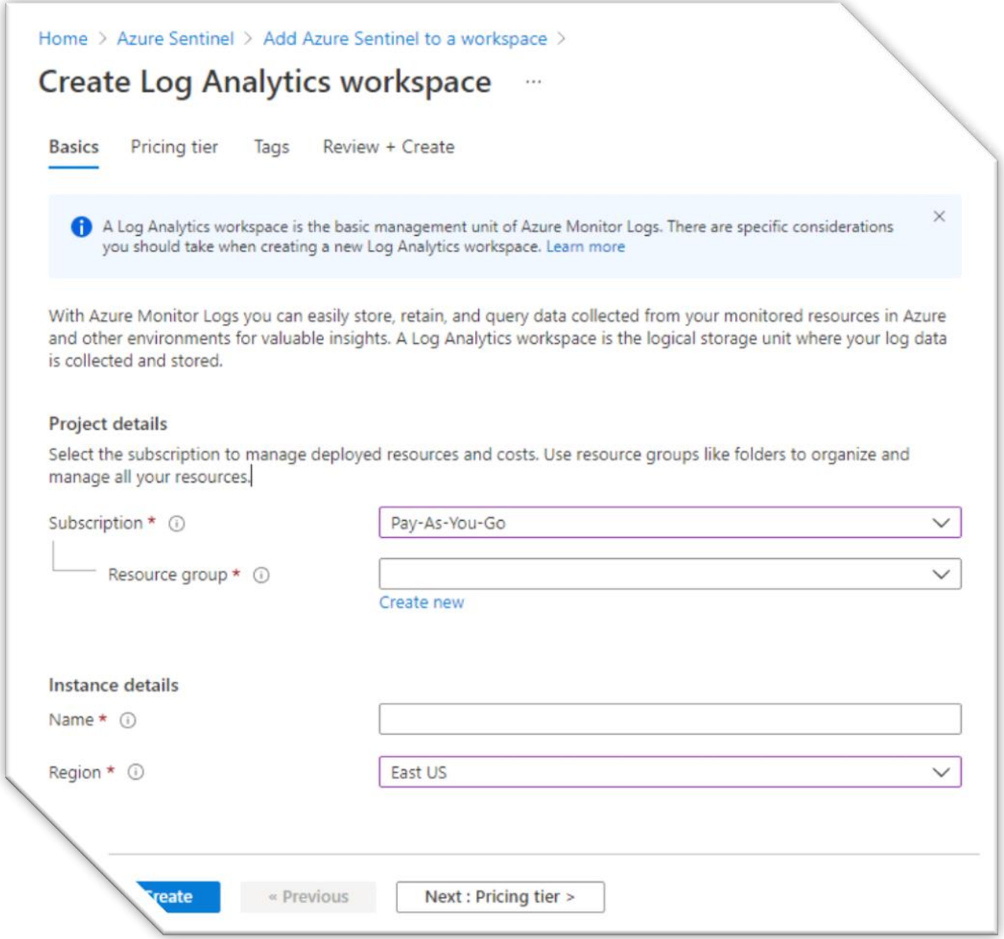
List view

No Azure Sentinel to display

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

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

Onboarding - Azure Analytics Workspace



Create Log Analytics workspace ...

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.

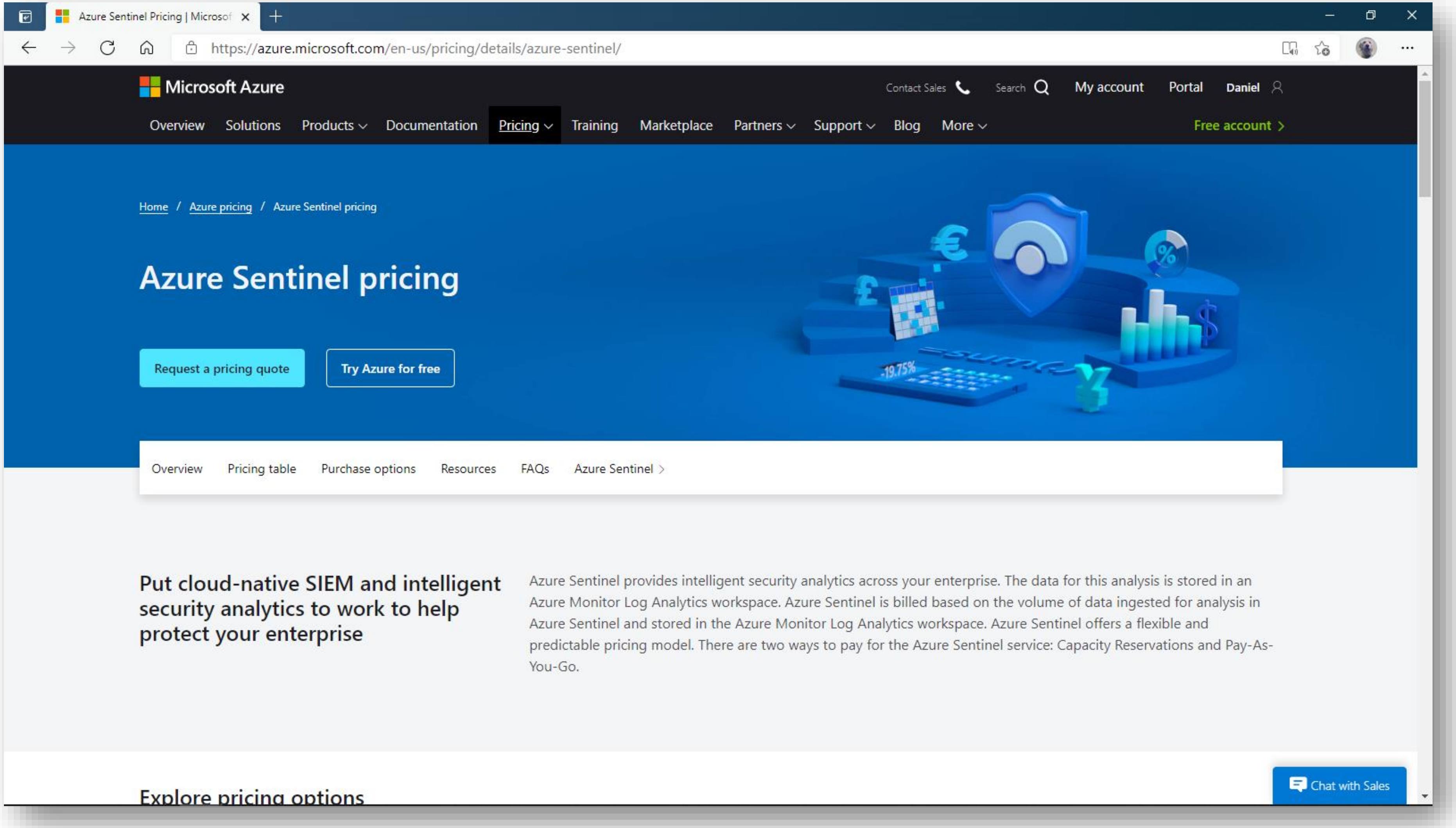
Subscription *	Pay-As-You-Go
Resource group *	
	Create new

Instance details

Name *	
Region *	East US

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace

Onboarding – Cost Considerations



Azure Sentinel pricing

Put cloud-native SIEM and intelligent security analytics to work to help protect your enterprise

Azure Sentinel provides intelligent security analytics across your enterprise. The data for this analysis is stored in an Azure Monitor Log Analytics workspace. Azure Sentinel is billed based on the volume of data ingested for analysis in Azure Sentinel and stored in the Azure Monitor Log Analytics workspace. Azure Sentinel offers a flexible and predictable pricing model. There are two ways to pay for the Azure Sentinel service: Capacity Reservations and Pay-As-You-Go.

Explore pricing options

https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/#pricing

Demo

Onboarding

Configuration

Data connectors

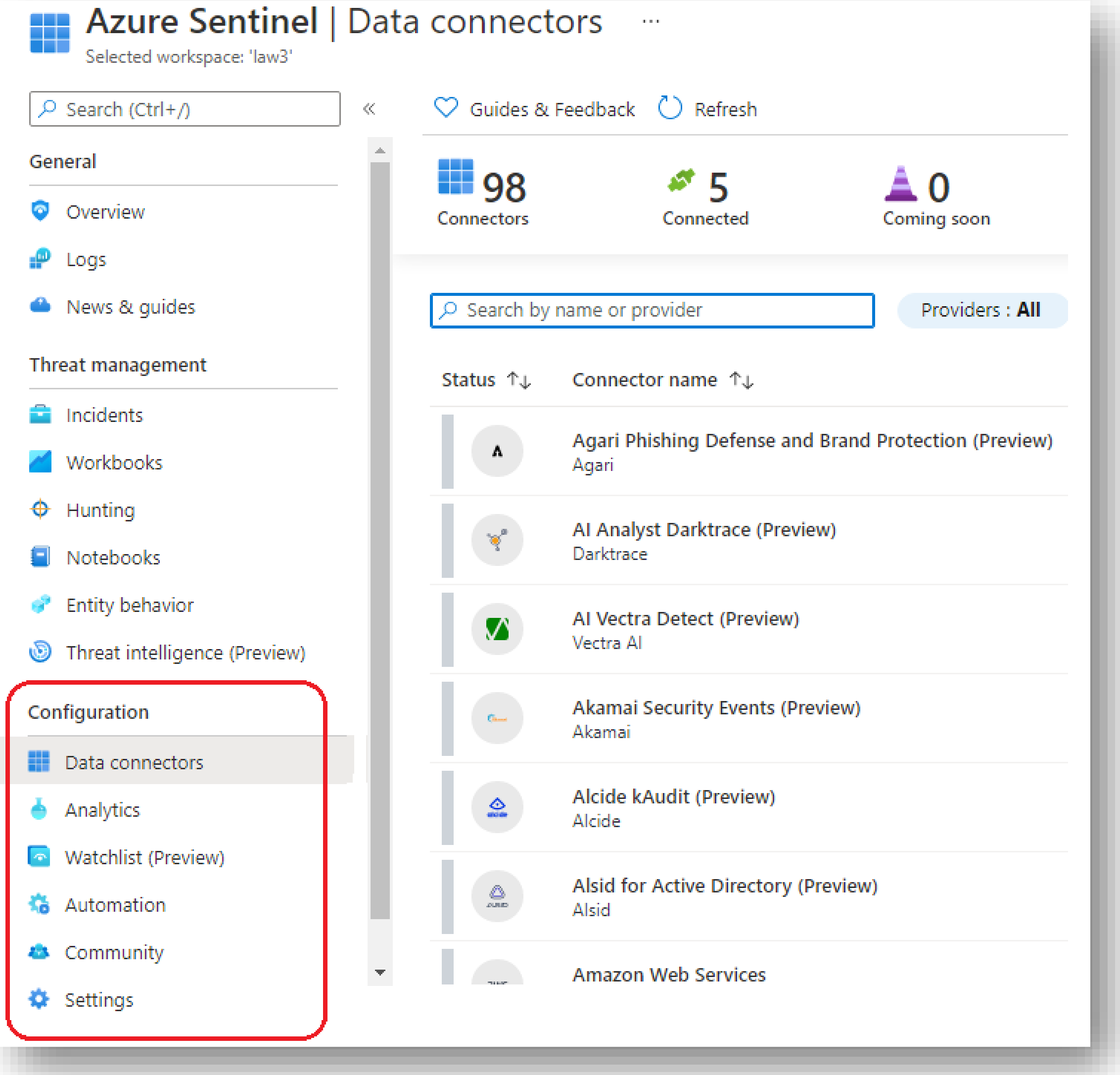
Analytics

Watchlist

Automation

Community

Settings



Azure Sentinel | Data connectors

Selected workspace: 'law3'

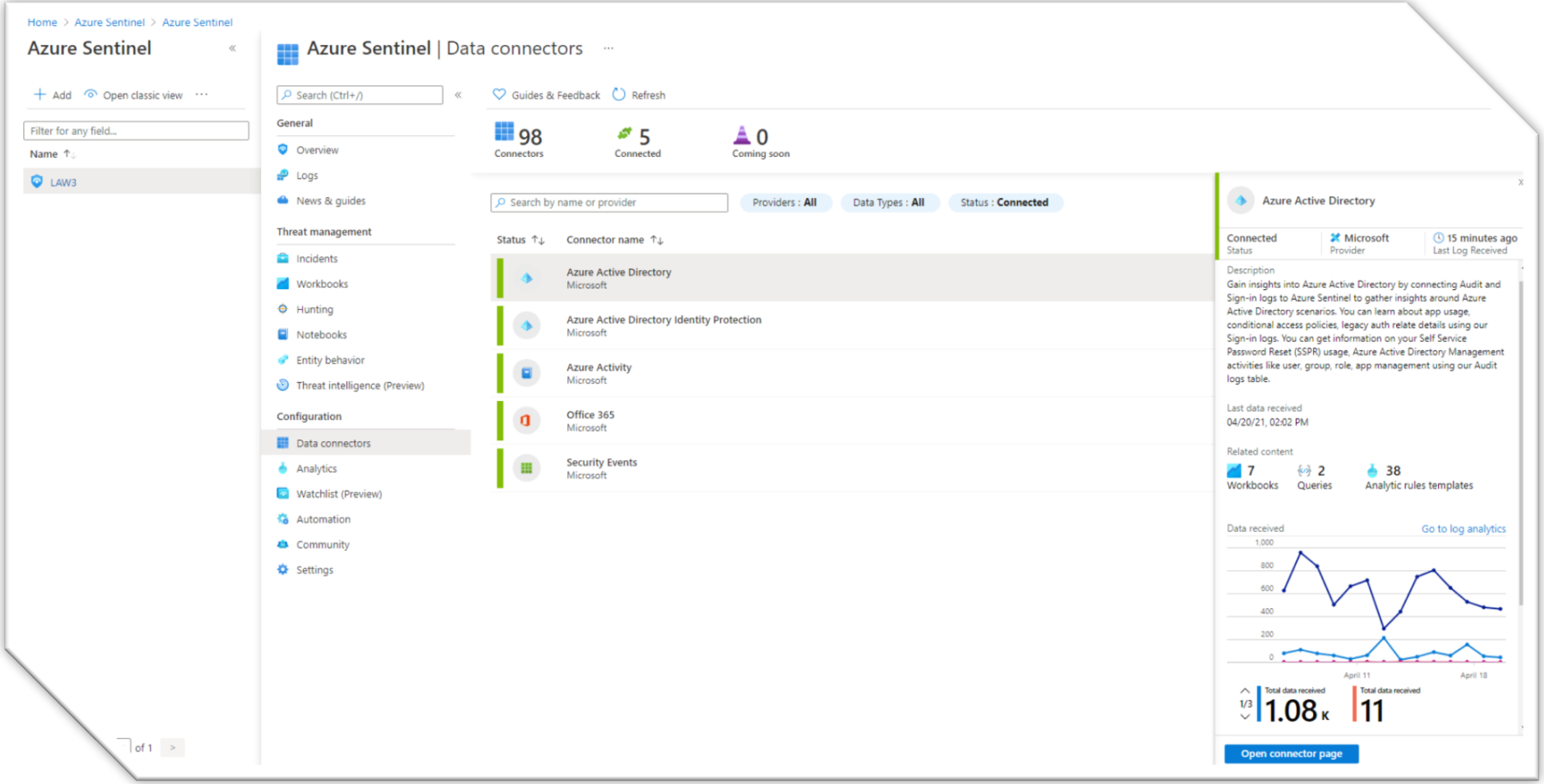
98 Connectors

5 Connected

0 Coming soon

Status ↑↓	Connector name ↑↓
	Agari Phishing Defense and Brand Protection (Preview) Agari
	AI Analyst Darktrace (Preview) Darktrace
	AI Vectra Detect (Preview) Vectra AI
	Akamai Security Events (Preview) Akamai
	Alcide kAudit (Preview) Alcide
	Alsid for Active Directory (Preview) Alsid
	Amazon Web Services

Configuration – Data Connectors



Status ↑↓	Connector name ↑↓
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Office 365 Microsoft
	Security Events Microsoft

Azure Active Directory

Connected	Microsoft	15 minutes ago
Status	Provider	Last Log Received

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received
04/20/21, 02:02 PM

Related content

7	2	38
Workbooks	Queries	Analytic rules templates

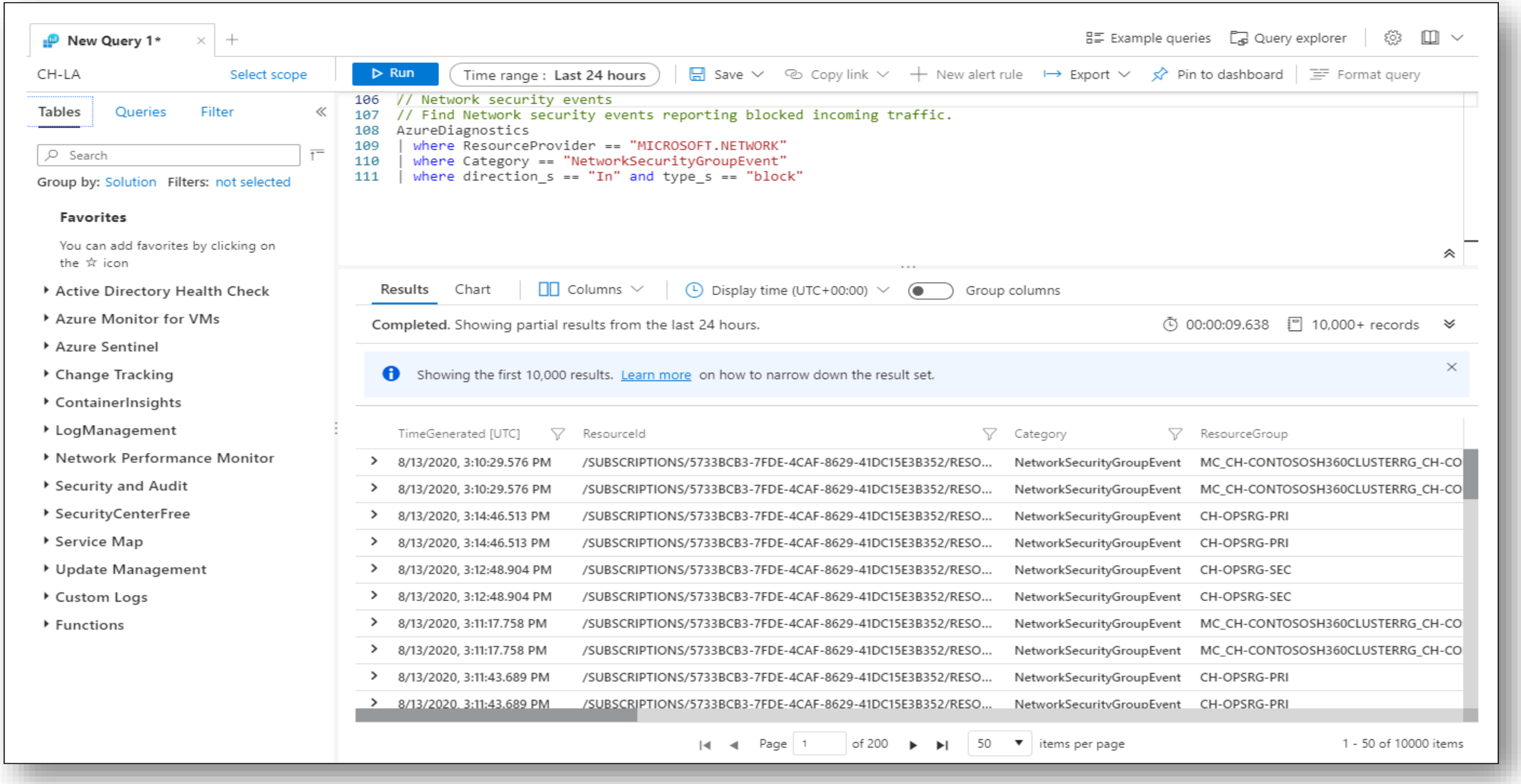
Data received — Go to log analytics

Total data received 1.08 K

Total data received 11

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace

Configuration - Analytics



```
// Network security events
// Find Network security events reporting blocked incoming traffic.
AzureDiagnostics
| where ResourceProvider == "MICROSOFT.NETWORK"
| where Category == "NetworkSecurityGroupEvent"
| where direction_s == "In" and type_s == "block"
```

Completed. Showing partial results from the last 24 hours. 00:00:09.638 10,000+ records

Showing the first 10,000 results. Learn more on how to narrow down the result set.

TimeGenerated [UTC]	ResourceId	Category	ResourceGroup
8/13/2020, 3:10:29.576 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	MC_CH-CONTOSOSH360CLUSTERRG_CH-CO
8/13/2020, 3:10:29.576 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	MC_CH-CONTOSOSH360CLUSTERRG_CH-CO
8/13/2020, 3:14:46.513 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	CH-OPSRG-PRI
8/13/2020, 3:14:46.513 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	CH-OPSRG-PRI
8/13/2020, 3:12:48.904 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	CH-OPSRG-SEC
8/13/2020, 3:12:48.904 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	CH-OPSRG-SEC
8/13/2020, 3:11:17.758 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	MC_CH-CONTOSOSH360CLUSTERRG_CH-CO
8/13/2020, 3:11:17.758 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	MC_CH-CONTOSOSH360CLUSTERRG_CH-CO
8/13/2020, 3:11:43.689 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	CH-OPSRG-PRI
8/13/2020, 3:11:43.689 PM	/SUBSCRIPTIONS/5733BCB3-7FDE-4CAF-8629-41DC15E3B352/RESO...	NetworkSecurityGroupEvent	CH-OPSRG-PRI

Demo

Configuration

Threat Management

Incidents

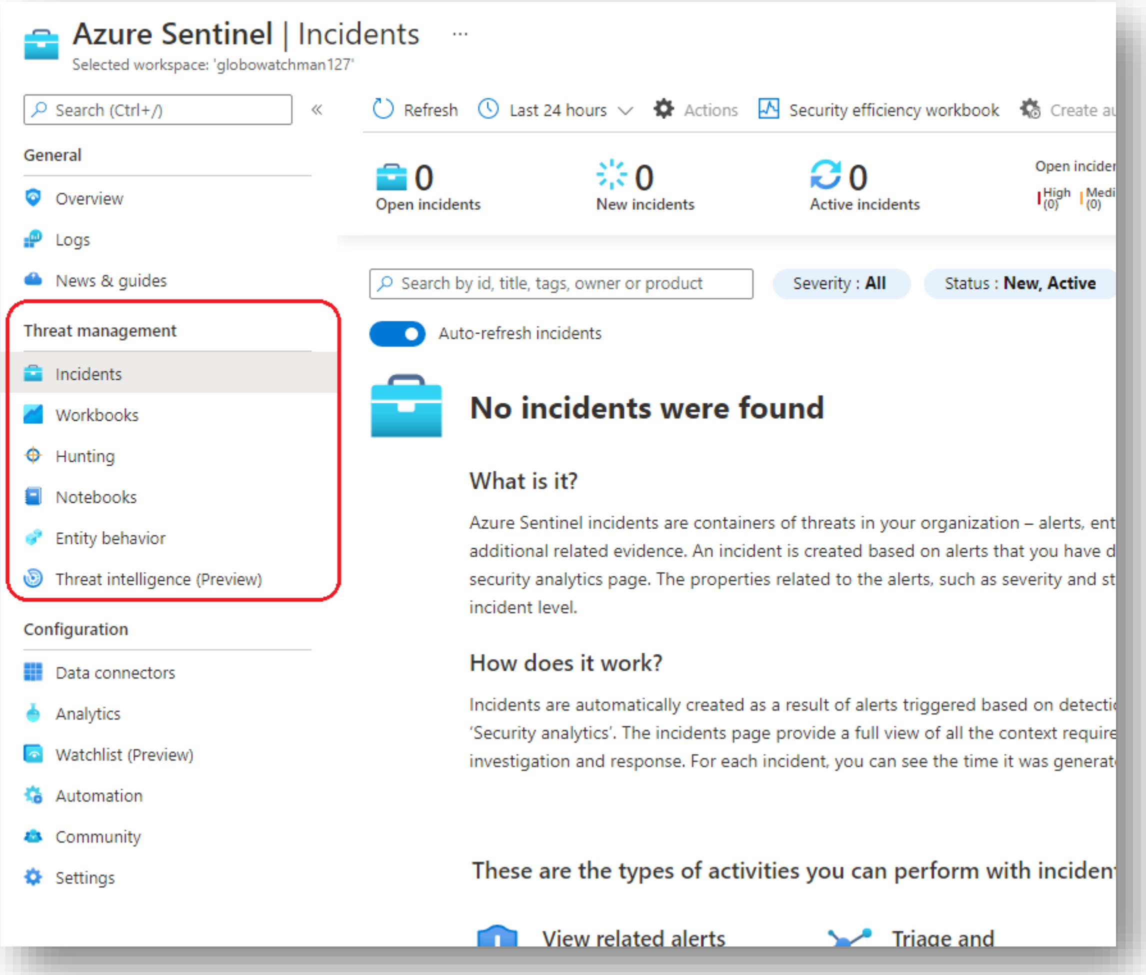
Workbooks

Hunting

Notebooks

Entity behavior

Threat Intelligence



Azure Sentinel | Incidents ···

Selected workspace: 'globowatchman127'

Search (Ctrl+/) «

Refresh | Last 24 hours | Actions | Security efficiency workbook | Create au

0 Open incidents

0 New incidents

0 Active incidents

Open inciden

High (0) Medi (0)

General

- Overview
- Logs
- News & guides

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence (Preview)

Configuration

- Data connectors
- Analytics
- Watchlist (Preview)
- Automation
- Community
- Settings

Search by id, title, tags, owner or product | Severity : **All** | Status : **New, Active**

Auto-refresh incidents

No incidents were found

What is it?

Azure Sentinel incidents are containers of threats in your organization – alerts, ent additional related evidence. An incident is created based on alerts that you have d security analytics page. The properties related to the alerts, such as severity and st incident level.

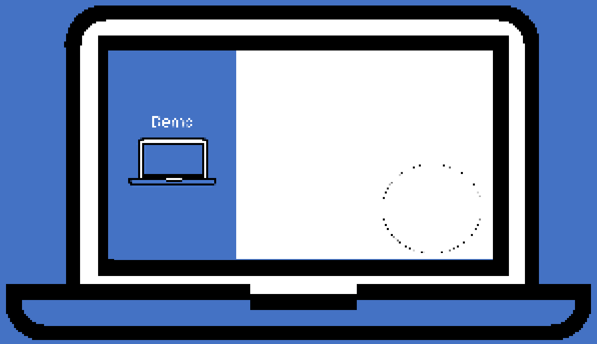
How does it work?

Incidents are automatically created as a result of alerts triggered based on detecti 'Security analytics'. The incidents page provide a full view of all the context require investigation and response. For each incident, you can see the time it was generat

These are the types of activities you can perform with incident

View related alerts | Triage and

Demo



Summary

- Easy to get started
- Helps reduce the noise
- Lowers the cost through automation

Resources

- Azure Sentinel uses Azure Logic Apps to implement automation
  https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook
- Azure Sentinel uses Azure Monitor Log Analytics's KQL to build queries
  https://docs.microsoft.com/en-us/azure/data-explorer/kusto/concepts/
- Azure Sentinel GitHub Community
  https://github.com/Azure/Azure-Sentinel