Azure Security with AAD, Defender, Purview, and Sentinel

Instructors: Jeremy Nathan and Logan Hillard

Jeremy Nathan

✉ jnathan@jncomputertraining.com

https://www.jncomputertraining.com

in https://www.linkedin.com/in/jeremy-nathan-mct

About Me

Advisor
Technology Trainer
Course Developer
Data Analyst
Microsoft Certified Trainer
Independent Contractor

From
Chattanooga, TN

MICROSOFT CERTIFIED TRAINER
Microsoft
MCT
Trainer
2021 - 2022

Microsoft
CERTIFIED
DATA ANALYST
ASSOCIATE
★★

Logan Hillard

✉ l.hillard@lngit.com

https://lngit.com

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

About Me

Certified CompTIA Network
Engineer Penetration Tester
Security and Fundamentals
Technology Trainer
Course Developer
Independent Contractor

From
Dallas-Fort Worth, TX

CompTIA PenTest+ CERTIFIED·CE

CompTIA Network+ CERTIFIED·CE

CompTIA Linux+ CERTIFIED·CE

Ask Questions!

Type questions in the chat for everyone or in Q&A; I will answer them live

Class Timeline

Azure AD Security (40 minutes)

- Why Azure? Why Microsoft? What are the pros/cons?
- Multi-factor authentication (MFA), zero trust, security fundamentals, types of threats
- Privileged Identity Management (PIM), Identity Access Management(IAM or RBAC)
- Azure AD (AAD) sign-in and audit logs, different log retentions based on subscription
- Analyze sign-In logs in AAD

Microsoft 365 Defender and Microsoft Purview (10 minutes)

- How to use Defender to view alerts and incidents. Look at live attack on an endpoint
- Presentation: How Microsoft Purview can help a company easily handle compliance. Look at the options in Purview
- Discuss how Defender can bring Cybersecurity to your business (SIEM, WAF)

Azure Sentinel (10 minutes)

- Has anyone been in an active incident response? What tools were used and what was the result?
- How to use Azure Sentinel to investigate, respond to and hunt for threats (SOAR, Threat Hunting Platform)
- Querying system information using Kusto Query Language (KQL) via Azure Monitor
- Use pre-packaged KQL to run queries in Azure Sentinel.

Why Azure/Defender/Sentinel?

- Product/solution from one of the largest big data/cyber vendors in the space

- Very easy to implement/roll out as it’s a cloud SIEM; extremely simple client onboarding especially for cloud resources

- Supports most Windows/Linux OS’s as well as any client that supports REST API

- If already in azure, can easily spin up a SOC anywhere in the world; support for AWS resources/connectors

Why do we not have a SOC?

1. Can’t support the budget
   - How much does it cost you to be down?
   - Is it “when?” or “if?” an outage/incident happens?

2. Can’t support 24/7
   - Vendors can help cover (MSSP) 24/7 or only at night/after hours/weekends

3. Can’t support the infrastructure
   - That’s what Azure monitor is for!

4. No corporate appetite
   - Back to 1st point

Where does all this fit into our time budget?

1. Cybersecurity

2. Defense in Depth

3. Zero Trust

Cybersecurity Fundamentals

- Cyber is a balance between Usability and Security
  - Business wants Usability
  - Cyber wants Security
- Corporate Acceptance
  - Biggest barrier to entry to get an organization to Zero Trust
- Updates to your systems
  - Is anyone planning on going to Win11 soon?
- Backups
  - When was the last time you verified your backups?
  - Are they redundant?
- User Training
  - Even the CEO's?
- Better AV
  - Start communicating with security vendors

Defense in Depth

- Defense in Depth – Defend at Every Level
- Start monitoring ASAP; you can’t defend what you can’t see
- Hire pentesters; Don’t rely on compliance to keep your organization secure
- Don’t just setup security tools, Maintain your tools

Zero Trust

- Top-Down Organizational Policy
- Requires a dedicated team to complete successfully, in a reasonable timeline and under budget
- Networking, Cyber, Infra, Application; All facets of the business are required
- Is a journey; Can take an organization 9-36 months depending on size and complexity; Multiple phases/completion milestones
- Cost can be $$$
  - Investment in your cyber posture to reduce costs from incidents/resource usage/etc

Categories of Threats

1. Random Phish

2. Targeted Phish
   - Business Email Compromise (BEC) → $$$

3. Opportunistic Attackers/Script Kiddies

4. Targeted Attacker (last one you can defend against)

5. Nation State/Advanced (Good Luck)

Insider Threats – Provocation, Opportunity, Rationalization

- Identity Access Management (IAM)
- Privileged Identity Management (PIM)
- Data Loss Protection (DLP)

Microsoft Azure Security

Office 365 – SaaS, think Office products

Azure AD – Basic Authentication Service, includes basic logs

Monitor – Underlying monitoring service for most other services

Defender – Cloud SIEM, alerts and incidents

Sentinel – Cloud Threat Hunting/SOAR

Purview – Cloud Compliance

Microsoft Licenses Breakdown

- Full Chart
  - Why can’t I open this? What does my error say?
- List of Licenses
- Microsoft 365 E3
  - Supports some of the security features but missing out on Full Defender & Sentinel
- Microsoft 365 E5
  - Provides the most security features
- Microsoft 365 F3
  - Only $8/user but comes with less features

- Government G1, G3, G5

Identity Access Management (IAM)

- Included with All Azure Licenses
- Entire point of this is to keep every user from being Global Admins; Least Privilege
- Also known as RBAC; More Granular control of user rights and privileged access
- Conditional access calendar date related with a specific end date
- Default roles already built in (will mostly suffice), but allows to be more specific
- Allows custom roles to be created and assigned

Azure AD Privileged Identity Management (PIM)

- Comes with E5 Licensing
- Management Utility for access control
- Time based access depending the time of day
- Allows for approval process for activation of any privileged roles
- “Justification” feedback from approvals

Multi-factor authentication (MFA)

- Extremely important; blocks most modern attack types by default
- Time consuming and can annoy users, implement **now** and investigate other solutions to spare users later(SSO, hardware tokens, passwordless, etc.)
- Don’t use push notifications, easiest MFA type to bypass

Azure AD (AAD) sign-in and audit logs

- Available with All Office/Azure Licenses

- Can be used to monitor access and administrative changes

- Low-level monitoring built into Azure

- May be the first place you look during an incident

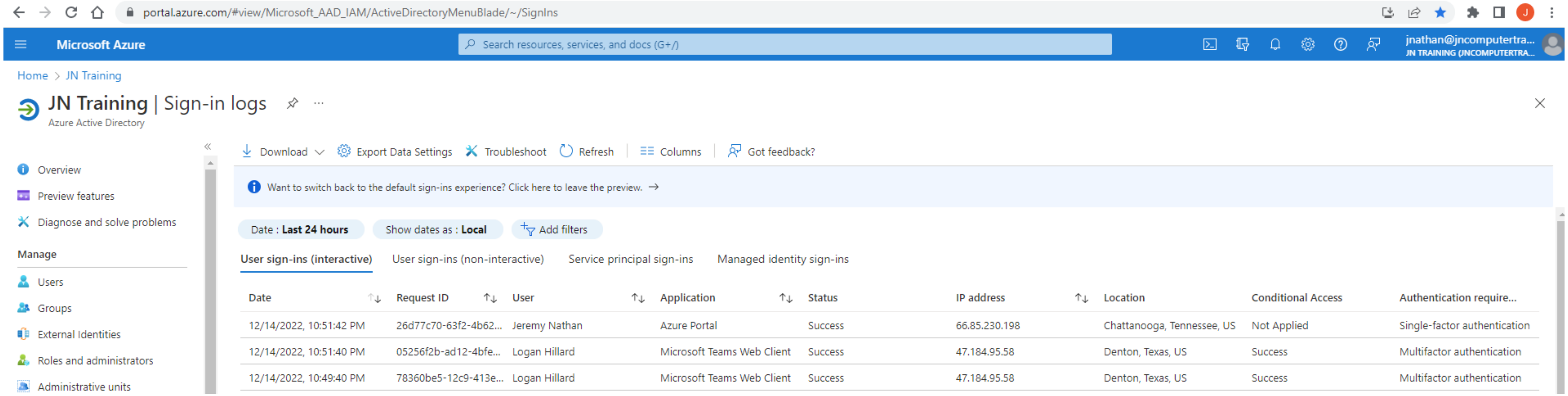
- Retention depends on license

Different log retentions based on subscription

- Standard Office 365 subscriptions will only allow 7 days of retention
- Most Azure subscriptions will allow for 30 days of retention
- Can archive logs to an Azure storage account for extended retention

Exercise: Analyze sign-In logs in AAD

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/SignIns


portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/SignIns
Microsoft Azure
Search resources, services, and docs (G+/)
jnathan@jncomputertra...
JN TRAINING (JNCOMPUTERTRA...
Home > JN Training
JN Training | Sign-in logs
Azure Active Directory
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Download
Export Data Settings
Troubleshoot
Refresh
Columns
Got feedback?
Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 24 hours**

Show dates as : **Local**

Date	Request ID	User	Application	Status	IP address	Location	Conditional Access	Authentication require...
12/14/2022, 10:51:42 PM	26d77c70-63f2-4b62...	Jeremy Nathan	Azure Portal	Success	66.85.230.198	Chattanooga, Tennessee, US	Not Applied	Single-factor authentication
12/14/2022, 10:51:40 PM	05256f2b-ad12-4bfe...	Logan Hillard	Microsoft Teams Web Client	Success	47.184.95.58	Denton, Texas, US	Success	Multifactor authentication
12/14/2022, 10:49:40 PM	78360be5-12c9-413e...	Logan Hillard	Microsoft Teams Web Client	Success	47.184.95.58	Denton, Texas, US	Success	Multifactor authentication

Microsoft 365 Defender

Cloud Security Information and Event Management (SIEM) for endpoints, applications, and just about anything else you can think of.

Microsoft 365 defender assists your busy security team to detect attacks. According to Microsoft documentation, “Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.”

Defender lives in:

https://security.microsoft.com/

Microsoft Security Readiness Resources

https://microsoft.github.io/PartnerResources/modern-workplace/security/

Enable all Defender services across the environment

https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security

Microsoft Defender for Endpoint

Extremely simple to roll out; automated and manual. Supports Windows, Linux, and Mac (11,12,13).

Endpoint Detection and Response (EDR) platform that helps secure the endpoint for your Defense in Depth strategy.

Responsible for creating alerts based on Indicators of Compromise (IoC's) from any endpoints that have been onboarded to the service. Windows Defender runs natively on all modern Windows OS's, but with Defender for Endpoint all data can be ingested and analyzed by Azure, helping SOC (Security Operations Center) analysts respond to alerts and incidents quickly.

By combining all the IoC's from an attack into an incident, SOC analysts can quickly respond and understand attacks.

Safe Links and Safe Attachments

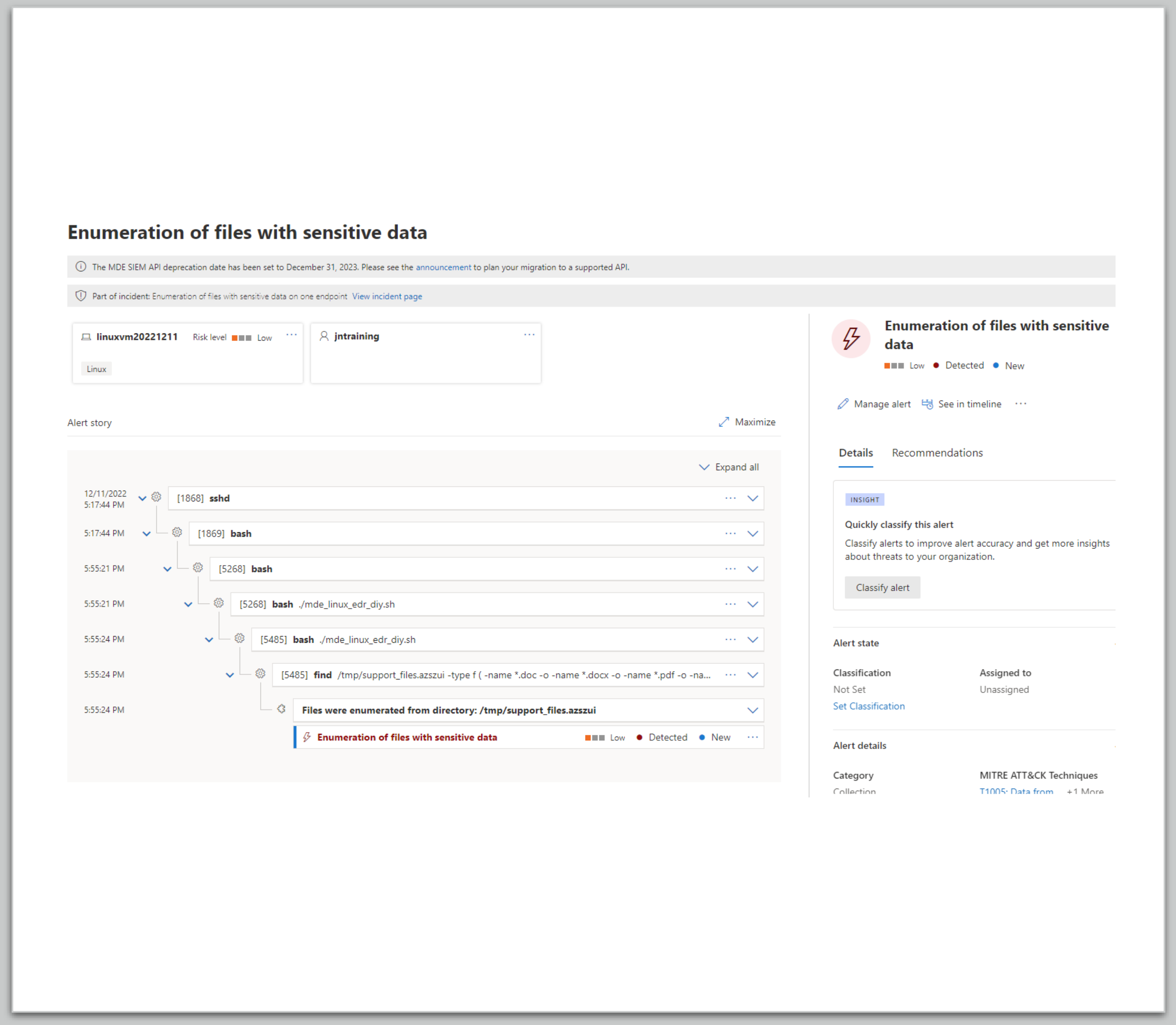
- Used to be called Advanced Threat Protection (ATP); Prevents many phishing vectors
- Provides URL Scanning, mail flow review, and time-of-click verification of URL’s, links and attachments
- Must enable preset security template, not enabled by default
- Protects outlook/email, Teams, and other office applications

Defender for Cloud Apps

- Now part of Defender
- Helps identify application usage and mitigate Shadow IT via Cloud Discovery
- Conditional access/Cloud Access Security Broker (CASB)
- Policy Control and Sanctioning of Apps

Look at a live attack on an endpoint

- Demonstration of an attack against a VM running the Azure Monitor agent and what the SOC Analyst can see via the Defender and Sentinel portals



Enumeration of files with sensitive data

ⓘ The MDE SIEM API deprecation date has been set to December 31, 2023. Please see the announcement to plan your migration to a supported API.

Part of incident: Enumeration of files with sensitive data on one endpoint View incident page

linuxvm20221211 Risk level ■■■ Low ···
Linux

jntraining ···

Alert story ⤢ Maximize

Expand all

```
12/11/2022 5:17:44 PM  [1868] sshd
5:17:44 PM             [1869] bash
5:55:21 PM             [5268] bash
5:55:21 PM             [5268] bash ./mde_linux_edr_diy.sh
5:55:24 PM             [5485] bash ./mde_linux_edr_diy.sh
5:55:24 PM             [5485] find /tmp/support_files.azszui -type f ( -name *.doc -o -name *.docx -o -name *.pdf -o -na...
5:55:24 PM             Files were enumerated from directory: /tmp/support_files.azszui
                       Enumeration of files with sensitive data  ■■■ Low  ● Detected  ● New
```

Enumeration of files with sensitive data

■■■ Low ● Detected ● New

Manage alert | See in timeline | ···

Details | Recommendations

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

Category	MITRE ATT&CK Techniques
Collection	T1005: Data from +1 More

Microsoft Sentinel

- Scalable, cloud-native solution
- Security orchestration, automation, and response (SOAR)
- Threat Hunting Platform
- **Collect data at cloud scale** across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect previously undetected threats and** minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
- **Investigate threats with artificial intelligence**, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
- **Respond to incidents rapidly** with built-in orchestration and automation of common tasks.

Microsoft Sentinel

- Sentinel is your birds-eye view of security over the enterprise ran in Azure. An on-premises SIEM would cost $$$$ for the physical infrastructure. Sentinel gives you visibility into any part of your environment to better maintain your organizations security posture.

- Azure Sentinel can help supplement other Azure security tools like Defender by integrating and ingesting data from other sources via data connectors. Sentinel supports a variety of data sources (including others CSP's like AWS) as well as 200+ standard IT vendor playbooks in the space.

Azure Sentinel Overview

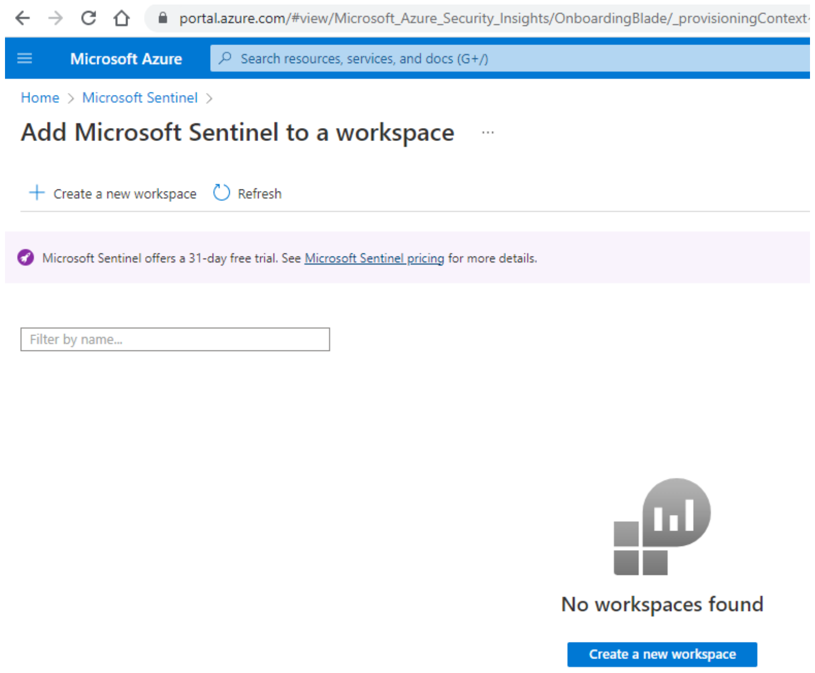
1) Collect Data via data connectors
2) Create visual interactive reports of your environment based on that data with workbooks
3) Utilize analytics rules alongside Microsoft Machine Learning (ML) to correlate alerts into incidents
4) Automate and orchestrate remediation and other tasks (SOAR) via playbooks with all your current systems
5) Perform Threat Hunting across the environment, utilizing MITRE framework and Jupyter notebooks to help support your SOC

Create Microsoft Sentinel

1) Create a new workspace

2) Create a Microsoft Sentinel Workspace

3) To make sure you can use all Sentinel features raise retention to 90 days



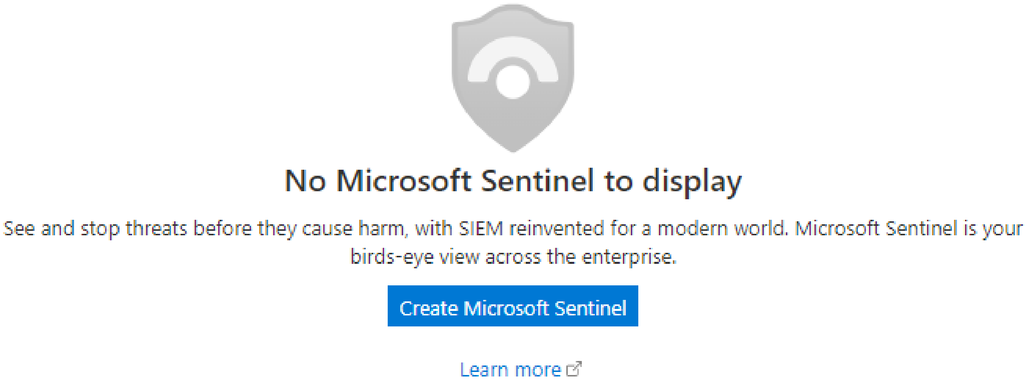
portal.azure.com/#view/Microsoft_Azure_Security_Insights/OnboardingBlade/_provisioningContext-

Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace

Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

No workspaces found

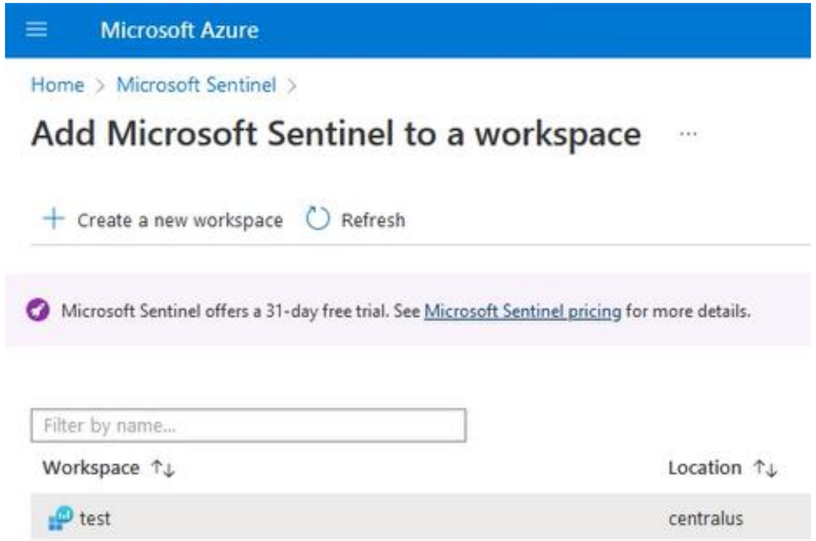


No Microsoft Sentinel to display

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.

Add Microsoft Sentinel to the workspace

1) Click on the workspace
Add Microsoft Sentinel to the workspace

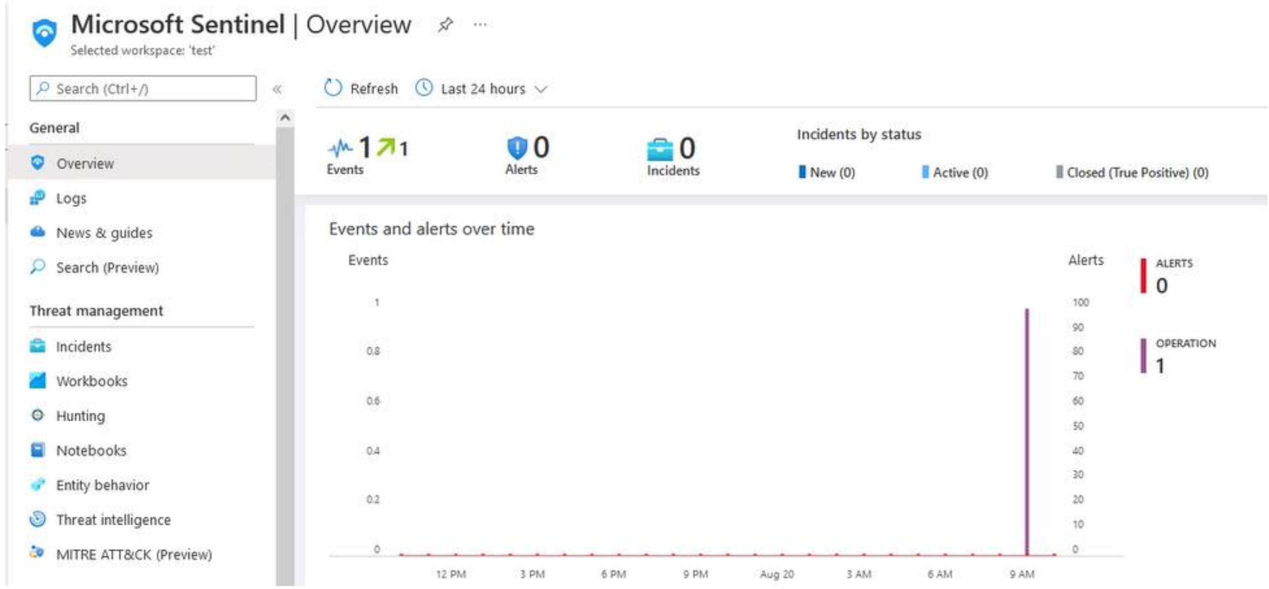


Add Microsoft Sentinel to a workspace

Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

Workspace ↑↓	Location ↑↓
test	centralus

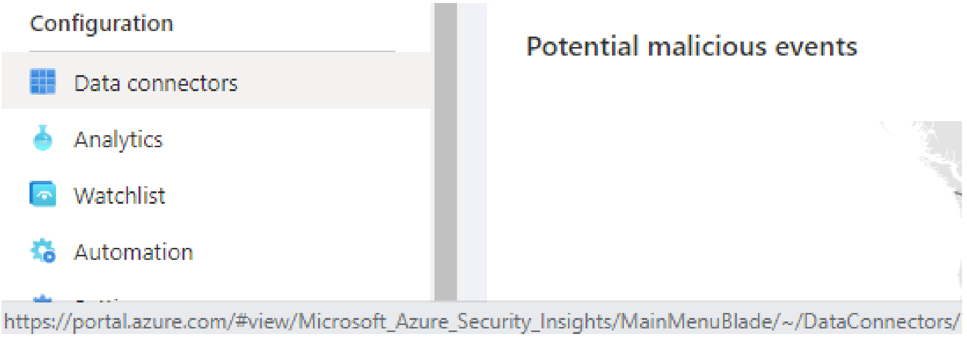
2) Go to your resource group and click on Sentinel button
Now you are the Sentinel Overview page



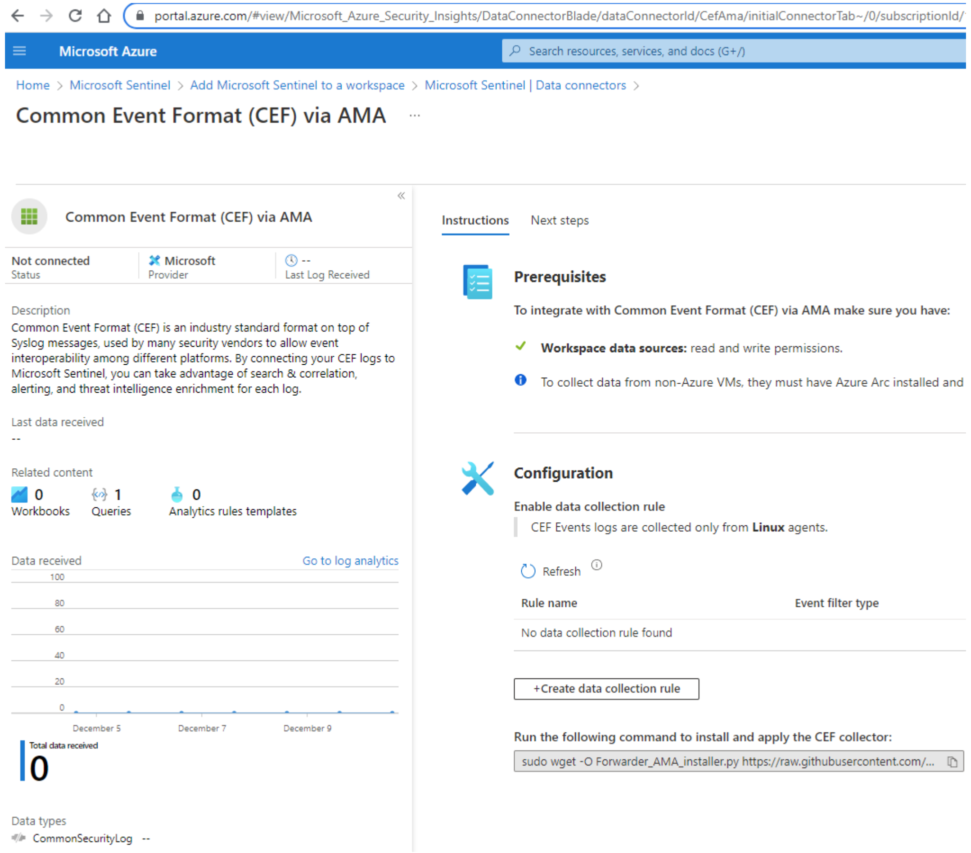
Set Up Data Connectors

1) Click on Data connectors and add any sources of data you want to monitor from your environment

2) Once you find a source, click on it and install it following any instructions it has in the popup pane.



https://portal.azure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/DataConnectors/


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Data connectors >
Instructions
Next steps
Refresh
+Create data collection rule
100
80
60
40
20
0
December 5
December 7
December 9

portal.azure.com/#view/Microsoft_Azure_Security_Insights/DataConnectorBlade/dataConnectorId/CefAma/initialConnectorTab~/0/subscriptionId/

Common Event Format (CEF) via AMA

Common Event Format (CEF) via AMA

Not connected
Status

Microsoft
Provider

--
Last Log Received

Description
Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms. By connecting your CEF logs to Microsoft Sentinel, you can take advantage of search & correlation, alerting, and threat intelligence enrichment for each log.

Last data received
--

Related content
0 Workbooks
1 Queries
0 Analytics rules templates

Data received
Go to log analytics

Total data received
0

Data types
CommonSecurityLog --

Prerequisites

To integrate with Common Event Format (CEF) via AMA make sure you have:

✓ **Workspace data sources:** read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and

Configuration

Enable data collection rule

> CEF Events logs are collected only from **Linux** agents.

Rule name	Event filter type
No data collection rule found	

Run the following command to install and apply the CEF collector:

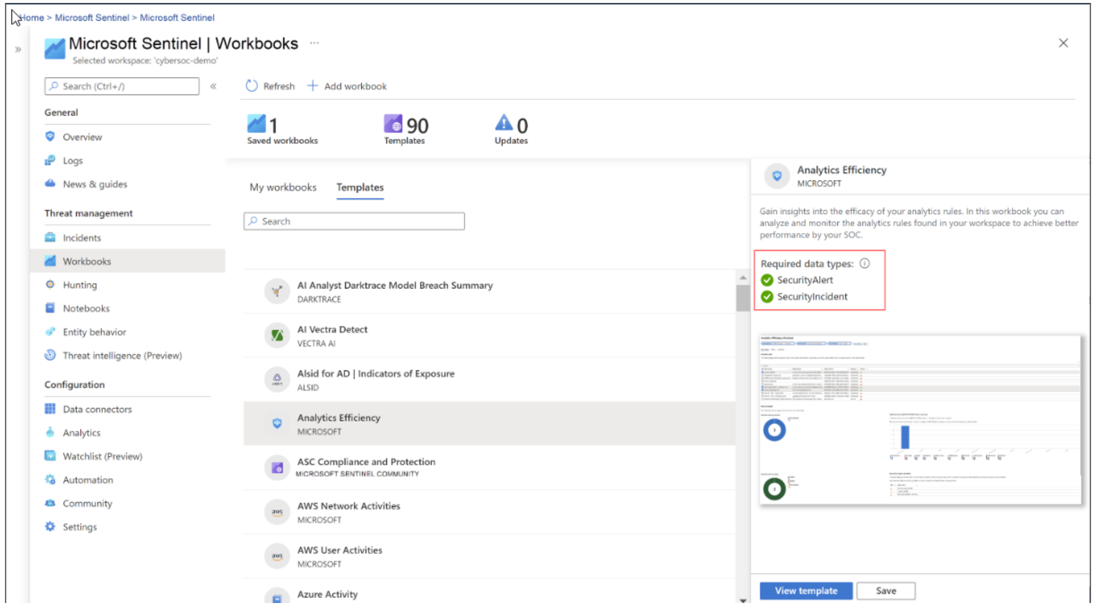
```
sudo wget -O Forwarder_AMA_installer.py https://raw.githubusercontent.com/...
```

Use Watchlists to monitor Priority Assets

Watchlists can help your organization monitor priority assets, users, or other resources to better identify potential attacks or malicious activity.

- **Investigate threats** and respond to incidents quickly with the rapid import of IP addresses, file hashes, and other data from CSV files. After you import the data, use watchlist name-value pairs for joins and filters in alert rules, threat hunting, workbooks, notebooks, and general queries.
- **Import business data** as a watchlist. For example, import user lists with privileged system access, or terminated employees. Then, use the watchlist to create allowlists and blocklists to detect or prevent those users from logging in to the network.
- **Reduce alert fatigue**. Create allowlists to suppress alerts from a group of users, such as users from authorized IP addresses that perform tasks that would normally trigger the alert. Prevent benign events from becoming alerts.
- **Enrich event data**. Use watchlists to enrich your event data with name-value combinations derived from external data sources.

Visualize the Data with Workbooks



Gain insights into the efficacy of your analytics rules. In this workbook you can analyze and monitor the analytics rules found in your workspace to achieve better performance by your SOC.

Required data types:
- ✓ SecurityAlert
- ✓ SecurityIncident

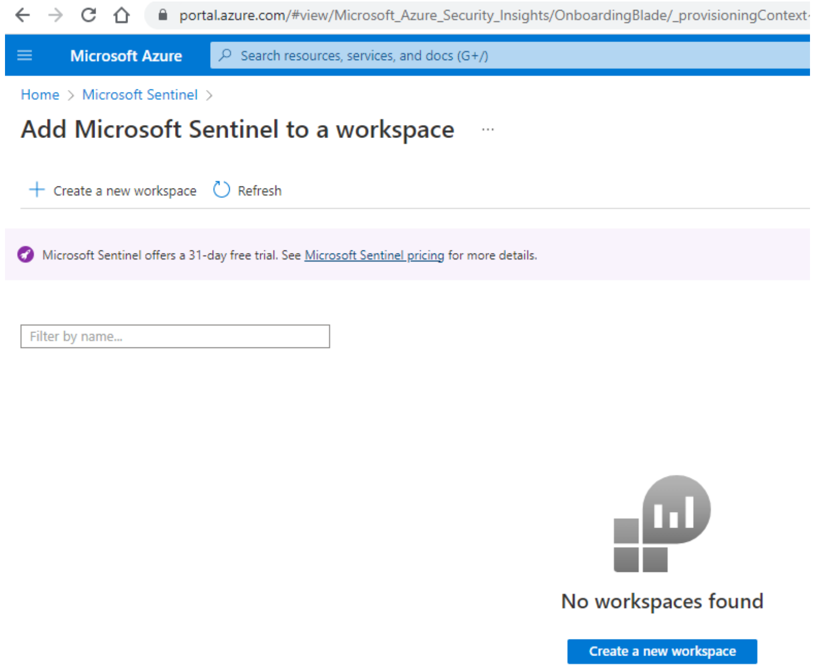
Utilize Workbooks to help visually analyze the data in Sentinel

Correlate alerts into Incidents

1) Utilize Analytics rules to help correlate events and alerts into incidents. ML built-in via Fusion.

2) Can create custom rules to help search for specific events

3) These analytics connect the dots, by combining low fidelity alerts about different entities into potential high-fidelity security incidents.



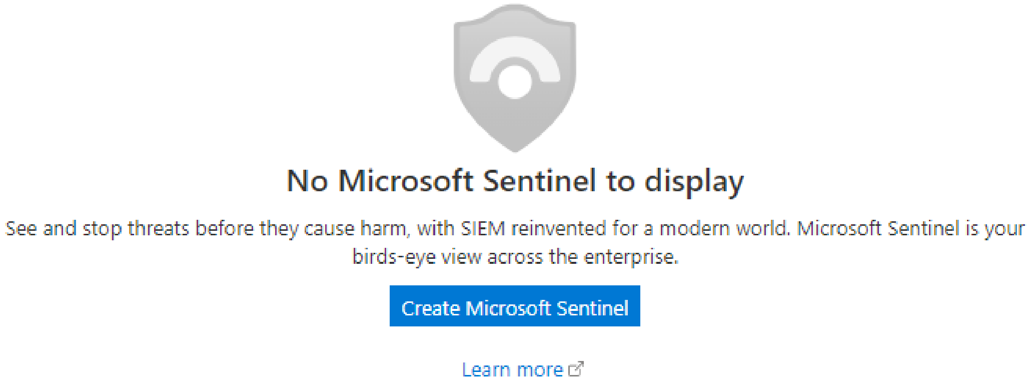
portal.azure.com/#view/Microsoft_Azure_Security_Insights/OnboardingBlade/_provisioningContext-

Home > Microsoft Sentinel >

Add Microsoft Sentinel to a workspace

Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

No workspaces found



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.

Threat Hunting

The Microsoft Sentinel Threat Hunting platform allows you to proactively search for potential incidents and IoC's based on the latest cybersecurity news or other form of actionable information. Rather than waiting for a detection to occur to respond, Threat Hunting helps allow a SOC to mitigate active breaches/threats and respond quickly real-world attacks.

- **Run queries** from the hunting platform to proactively search for active or old threats anywhere Sentinel is connected. Utilize pre-built queries (KQL) to search for specific phases of the attack chain.
- **Utilize MITRE** concepts and categorization to better understand and explain active threats to management and C Suite.
- **Bookmark** unusual or suspicious results from a query in order to refer back to them later. This information can be used as a reference when creating an incident or simply enriching an ongoing investigation. Escalate severe findings directly to incidents.
- **Use Jupyter Notebooks** to help automate and enrich your queries, allowing additional ML, visualization and data analysis.

Automate and orchestrate remediation and other tasks (SOAR) via playbooks

Simplify automation of remediations and orchestration of tasks across a variety of vendors to help support SOC technicians and increase their efficiency to free up their time for more proactive tasks in the environment. This increases the overall security posture of the organization and has a compounding effect as the automation tools/solutions come online.

- **Automate remediation** to help reduce the workload on SOC technicians, freeing them up to perform more proactive security tasks, increasing efficiency overall.

- **Orchestrate tasks** via a highly extensible architecture that enables scalable automation as new technologies and threats emerge. Over 200+ vendors supported.

- **Build playbooks** via Azure Logic Apps (no-code solution) or choose from a growing gallery of official and shared playbooks to help with automated remediation.

Microsoft Purview

- Platform as a service built on Apache Atlas
- Protects data by using metadata
- Classifies sensitive data like ssn, date of birth, bank accounts using tags
- Handles risk and compliance by categorizing data
- Governs data by managing data lifecycle

Microsoft Purview Part 2

- Scans on-premises and multicloud data sources
- Data scanned includes databases, Azure data lakes, blob storage and files
- Shows how data is mapped and organized by lineage
- Glossary to categorize data
- Search for data

Microsoft Purview

Purview looks at metadata

1) You need to create a Purview account in Azure Portal

2) You need to make a collection to organize data with a map view

Use Role assignments to restrict permissions

Purview uses managed service identity (MSI)

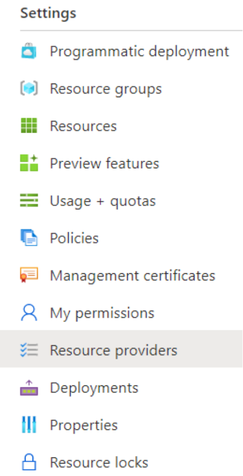
Scan rule sets

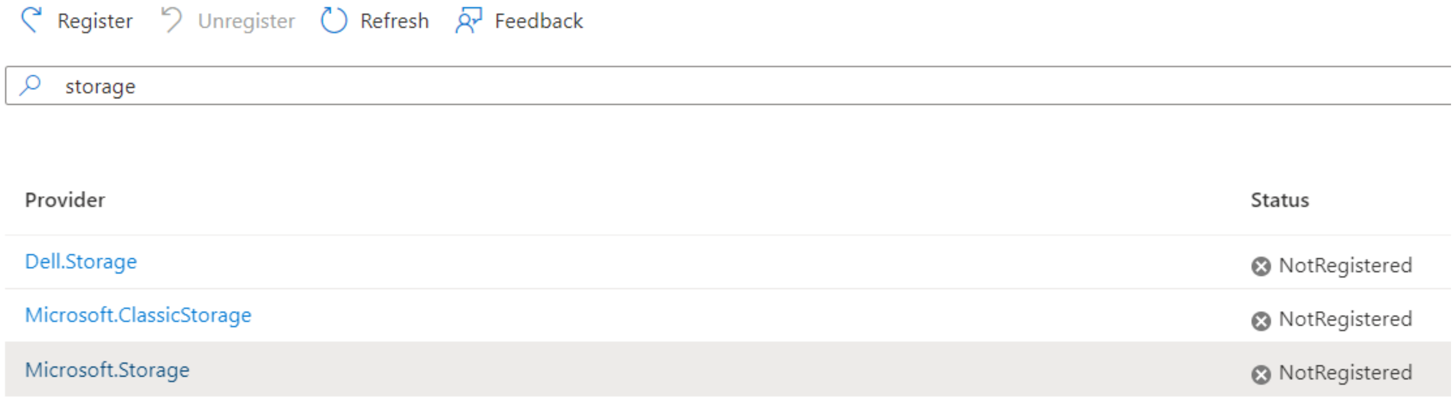
* Make sure you turn off rules when you are not using them…they cost money

Set data policies (preview) in Purview

- If you get an error 21005 - The resource providers Microsoft.Storage and Microsoft.EventHub are not registered for subscription, then you need to register your Microsoft.Storage and Microsoft.EventHub.

1. Go to your subscription and click on Resource providers under settings
2. Search for Microsoft.Storage and click on the line and click on Register





storage

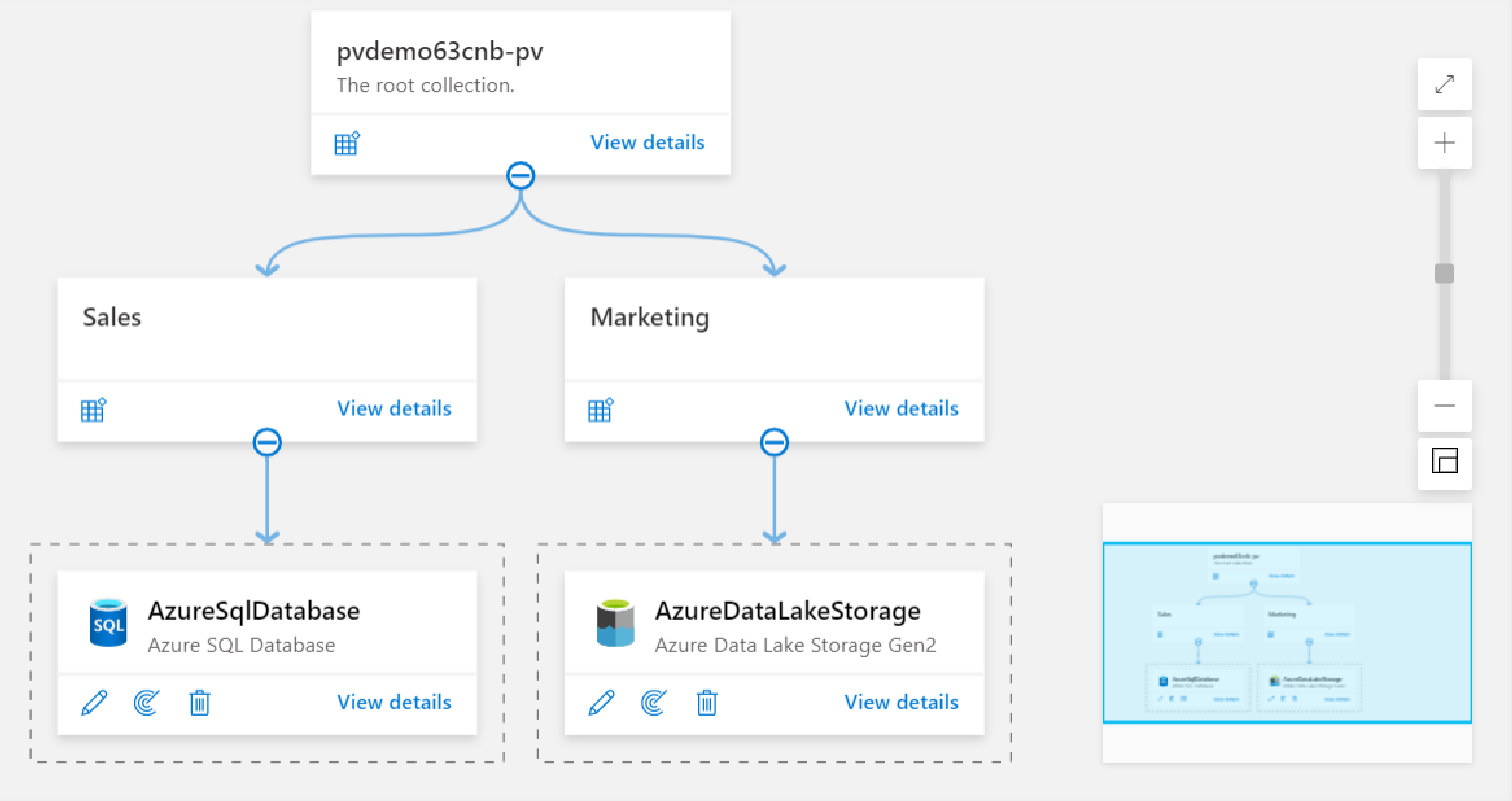
Provider	Status
Dell.Storage	⊗ NotRegistered
Microsoft.ClassicStorage	⊗ NotRegistered
Microsoft.Storage	⊗ NotRegistered

Microsoft Purview

- Deploy Purview Demo: https://aka.ms/pvdemo
- Change the SQL login and password to at least a 12 character password

* This demo uses Azure resources $$$
* Delete when finished!

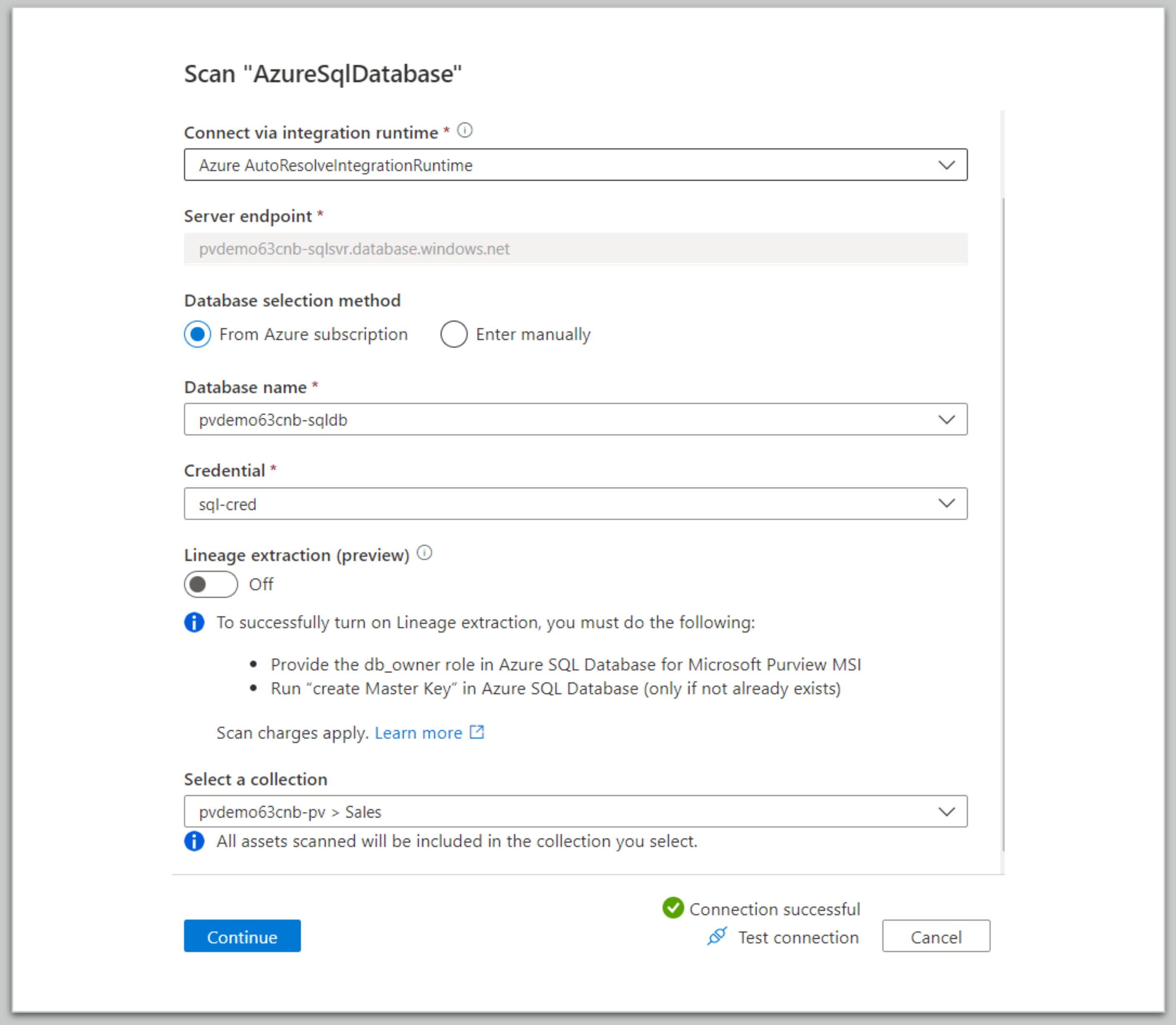
Go to Purview account, data map, and click on the plus to drill-down into the data sources.



Scan with Purview

In AzureDataLakeStorage, click on View Details to see the scan. Click new scan and test the connection.

Test the connection for the Azure SQL Database with these options



Scan "AzureSqlDatabase"

Connect via integration runtime * ⓘ

Azure AutoResolveIntegrationRuntime

Server endpoint *

pvdemo63cnb-sqlsvr.database.windows.net

Database selection method

● From Azure subscription ○ Enter manually

Database name *

pvdemo63cnb-sqldb

Credential *

sql-cred

Lineage extraction (preview) ⓘ

Off

To successfully turn on Lineage extraction, you must do the following:

- Provide the db_owner role in Azure SQL Database for Microsoft Purview MSI
- Run "create Master Key" in Azure SQL Database (only if not already exists)

Scan charges apply. Learn more

Select a collection

pvdemo63cnb-pv > Sales

All assets scanned will be included in the collection you select.

✓ Connection successful

Azure Log Analytics

Azure Log Analytics is the workspace that holds logs from Azure Monitor

- Logs in Monitor are the same as Sentinel
- Log Analytics Demo https://aka.ms/lademo
- Use Kusto Query Language (KQL) to query logs
- Querying the logs is free. Storage for the uses Azure resources

* Table names, column names, KQL functions and text are all case sensitive

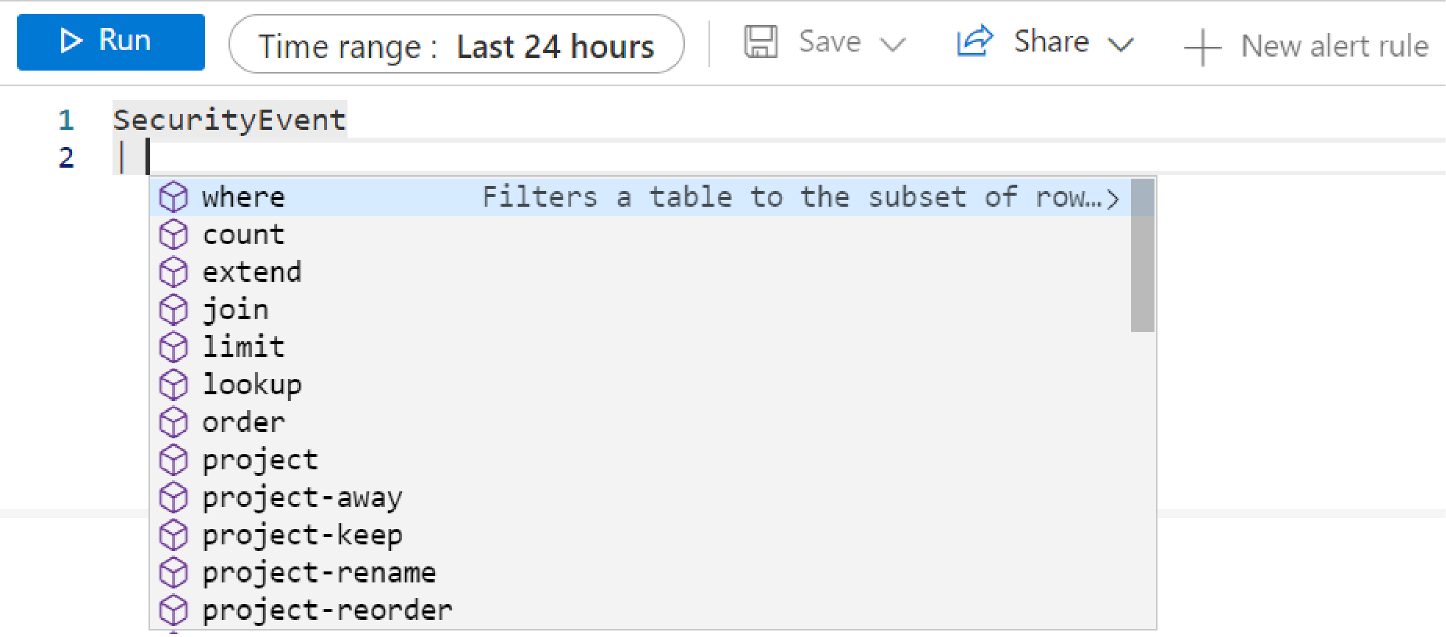
Kusto Query Language (KQL)

- KQL queries source data from Azure log **tables** just like SQL does for SQL Server tables.
- Some of this data you can query come from OS systems that create logs, counters, metrics such as CPU use, IoT devices creating a lot of telemetry data such as temperature sensors on machines.
- There is a lot of data on failures such as machine turning off, successful and unsuccessful authentications, etc.

- Click on Shift Enter to run or click on Run

KQL to Query SecurityEvents

You will see intellisense to show you possibilities while typing KQL
Add commands with the pipe |



```
SecurityEvent
|
```

KQL Functions

https://learn.microsoft.com/en-us/azure/data-explorer/kql-quick-reference

where
ago
summarize
search
project
count
take
extend
render
case
sort
by
distinct
Top
and

KQL String Operators

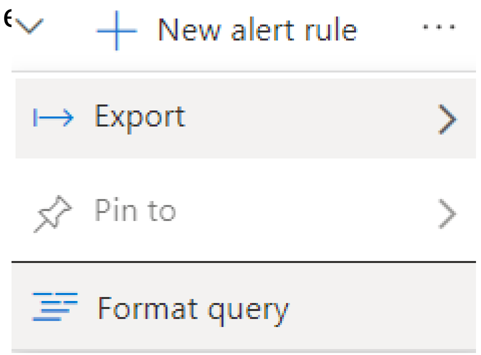
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/datatypes-string-operators

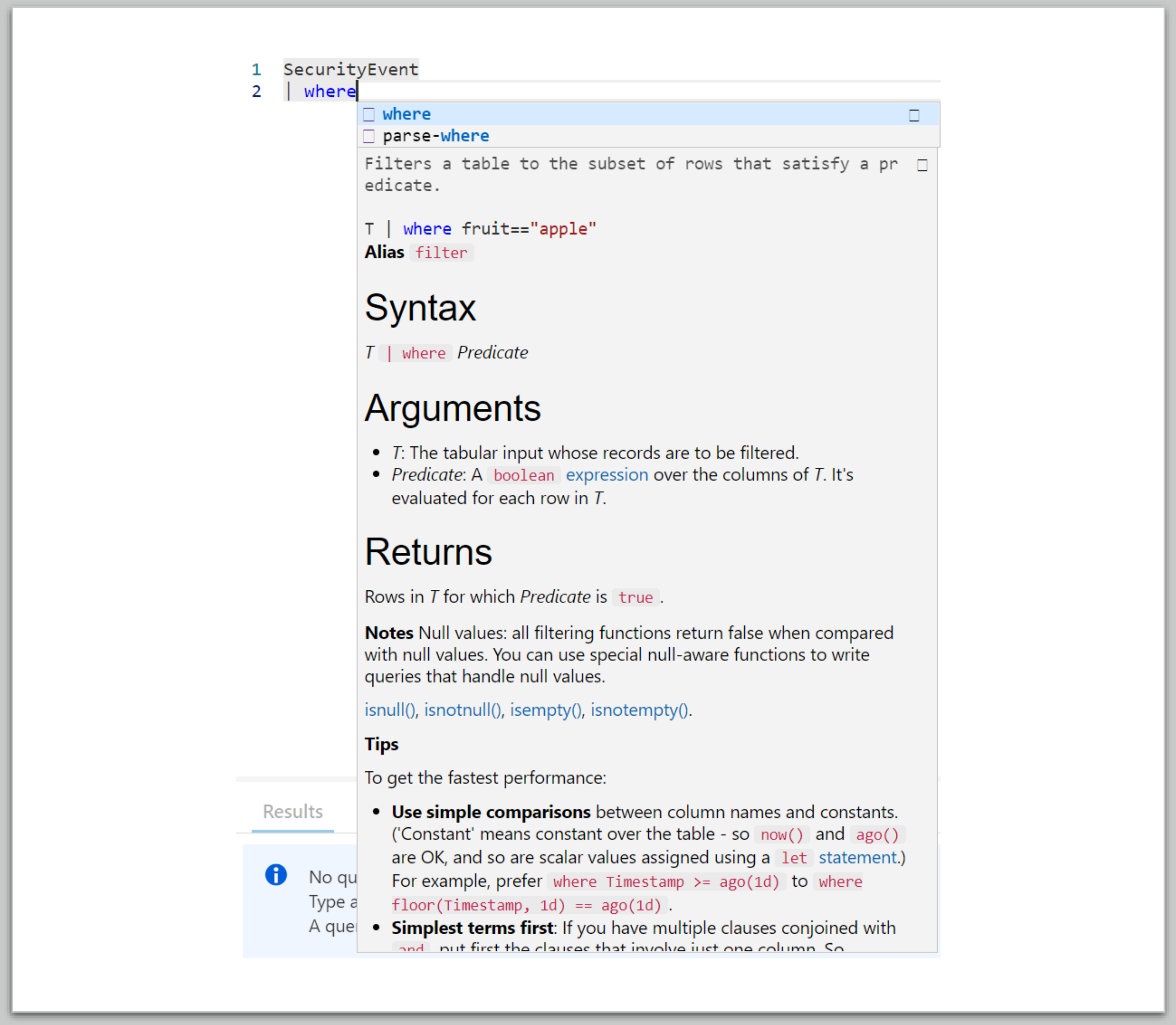
Operator	Description	Case-Sensitive	Example (yields true)
==	Equals	Yes	“AbC” == “AbC”
!=	Not equals	Yes	“abc” != “ABC”
contains	RHS occurs as a subsequence of LHS	No	"FabriKam" contains "BRik"
Has	Right-hand-side (RHS) is a whole term in left-hand-side (LHS)	No	"North America" has "america"
In	Equals to any of the elements	Yes	"abc" in ("123", "345", "abc")
Startswith	RHS is an initial subsequence of LHS	No	"Fabrikam" startswith "fab"

KQL Syntax

To learn the syntax, click on the arrow or ellipsis to the right of the word, in this case is where

You can autoformat a KQL query by clicking the





```
SecurityEvent
| where
```

□ where
□ parse-where

```
Filters a table to the subset of rows that satisfy a pr
edicate.

T | where fruit=="apple"
```

Alias `filter`

Syntax

T `| where` *Predicate*

Arguments

- *T*: The tabular input whose records are to be filtered.
- *Predicate*: A `boolean` expression over the columns of *T*. It's evaluated for each row in *T*.

Returns

Rows in *T* for which *Predicate* is `true` .

Notes Null values: all filtering functions return false when compared with null values. You can use special null-aware functions to write queries that handle null values.

isnull(), isnotnull(), isempty(), isnotempty().

Tips

To get the fastest performance:

- **Use simple comparisons** between column names and constants. ('Constant' means constant over the table - so `now()` and `ago()` are OK, and so are scalar values assigned using a `let` statement.) For example, prefer `where Timestamp >= ago(1d)` to `where floor(Timestamp, 1d) == ago(1d)` .
- **Simplest terms first**: If you have multiple clauses conjoined with `and` , put first the clauses that involve just one column. So

Your First KQL

Run this KQL to see every row of SecurityEvent table

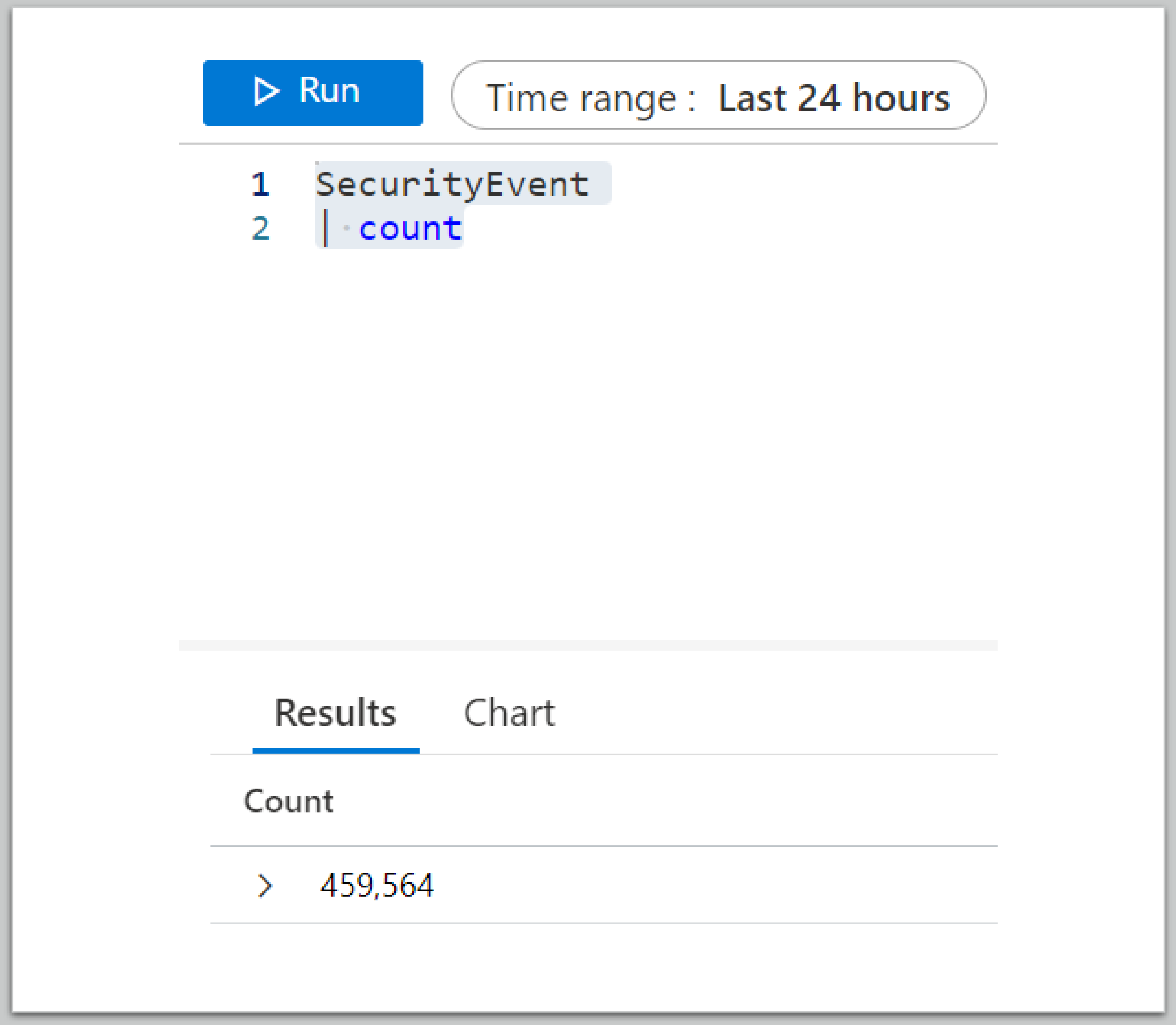
SecurityEvent

Results section is at the bottom of the screen where you will see the output

See count of SecurityEvent table

SecurityEvent

| count



```
SecurityEvent
| count
```

Count
459,564

Important KQL Queries

*Always use a where clause of time immediately to reduce the time to run the query
*Do not press F5 as this will refresh your browser. Instead press Shift+Enter to run the query

See the last 100 records from the current type back in time:

```
SecurityEvent
| take 100
```

To see everything that was inserted into the log store from now until a certain time ago:

```
SecurityEvent
| where TimeGenerated >= ago(1d)
```

To run everything from now until the last 30 minutes:

```
SecurityEvent
| where TimeGenerated >= now(-30m)
```

More KQL

To filter the output use project which lets you display the names of the columns you want returned.

```
SecurityEvent
| where TimeGenerated >= now(-30m)
| project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
```

You can make more where clauses by typing another | where. Here you see only EventID equal to 4688

```
SecurityEvent
| where TimeGenerated >= now(-30m)
| where EventID == 4688
| project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
```

With the same consecutive clauses, you can combine the second one with an “and”

```
SecurityEvent
| where TimeGenerated >= now(-30m) and EventID == 4688
```

Visual KQL

Make charts with

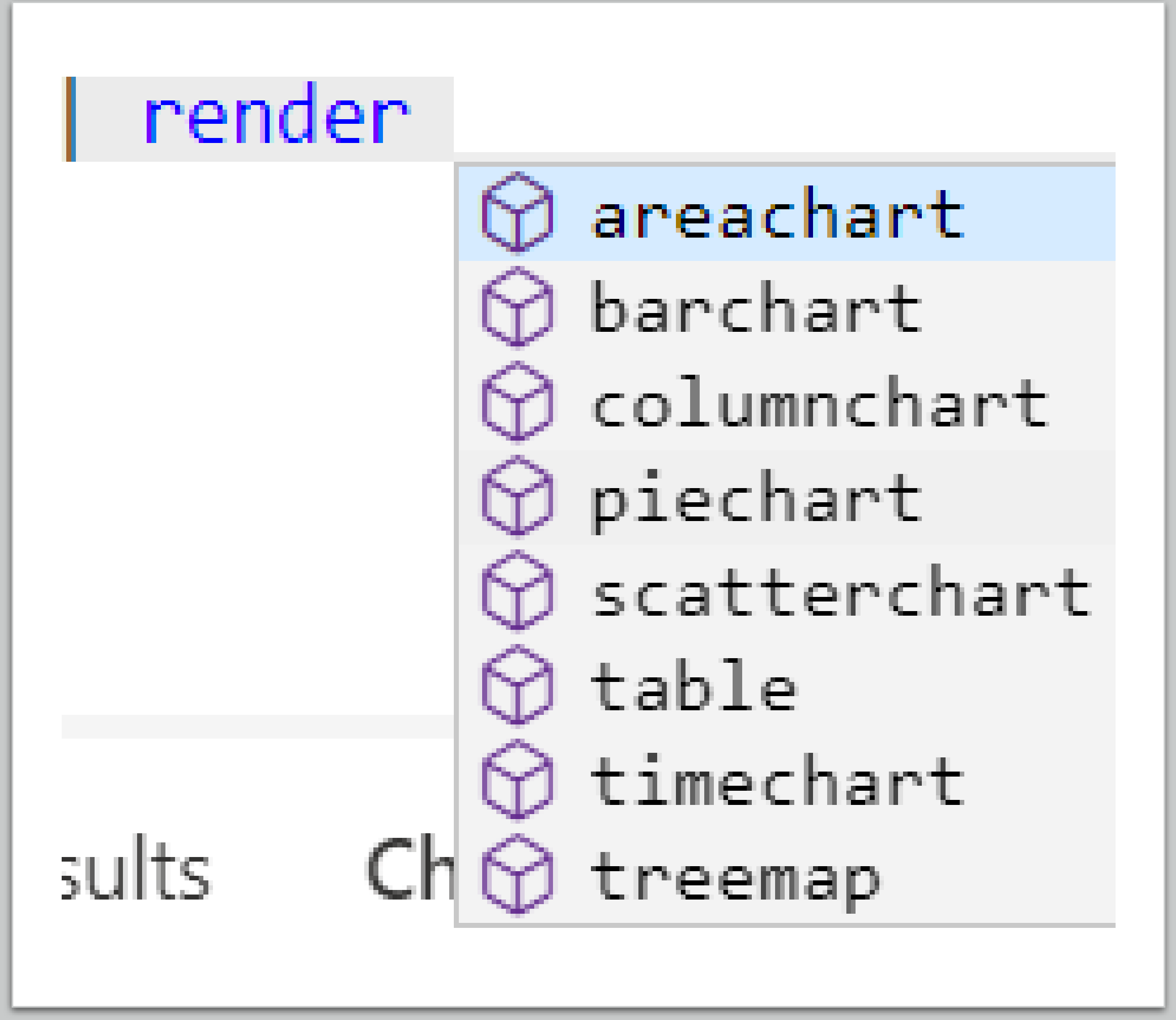
SecurityEvent

| where TimeGenerated >= now(-30m)

| where EventID == 4688

| project TimeGenerated, Account, Computer, EventID, Activity, IpAddress

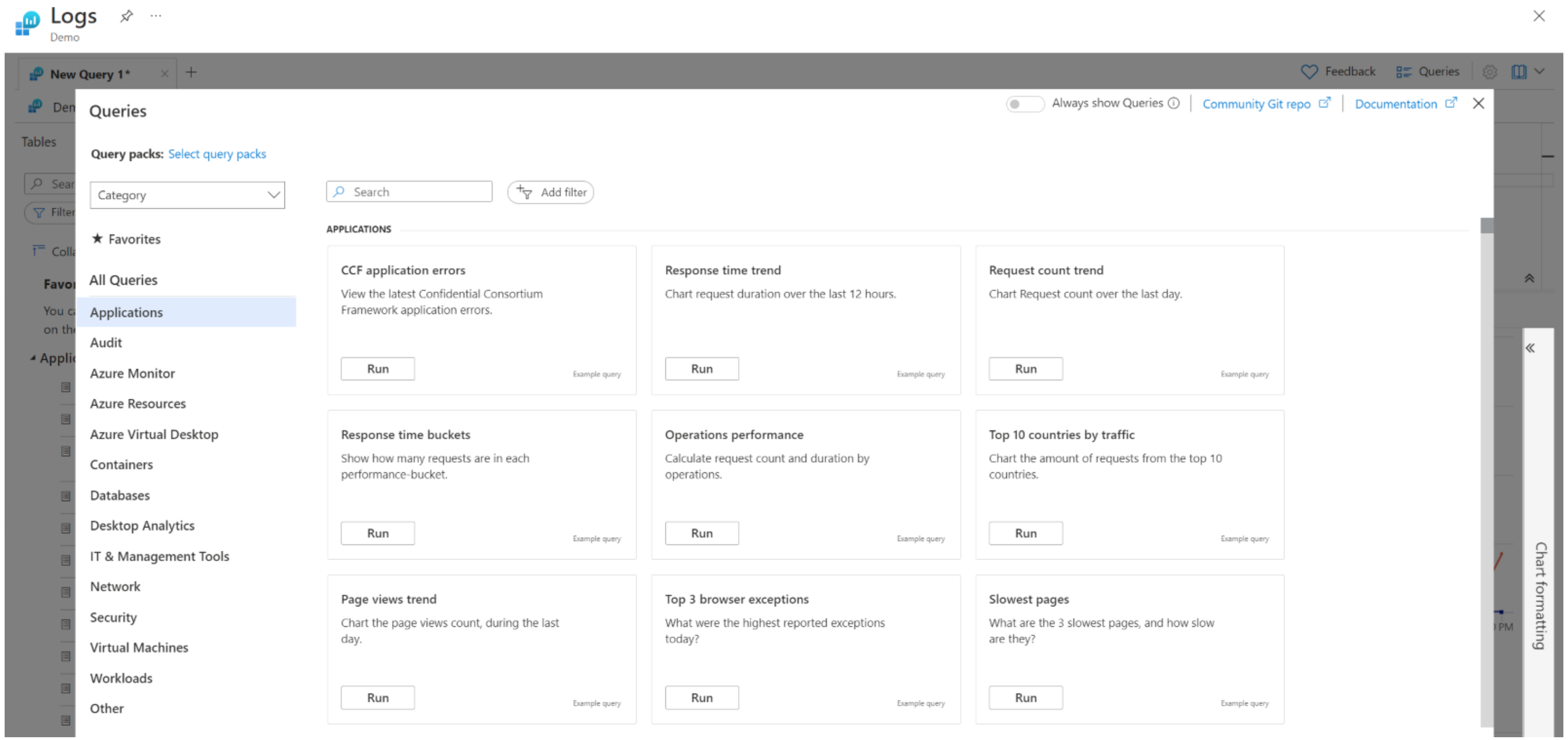
| render piechart



```
| render
```

Pre-built KQL

Microsoft has pre-set KQL queries that you can just click on the top and run
Click on Queries in the top-right corner



Queries

Query packs: Select query packs

○ Always show Queries ⓘ | Community Git repo | Documentation

Category

Search

Add filter

★ Favorites

All Queries

Applications

Audit

Azure Monitor

Azure Resources

Azure Virtual Desktop

Containers

Databases

Desktop Analytics

IT & Management Tools

Network

Security

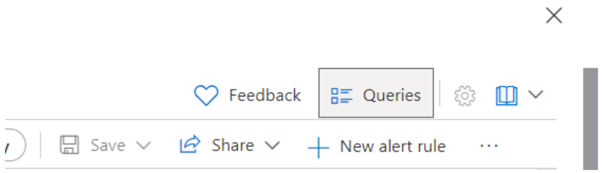
Virtual Machines

Workloads

Other

APPLICATIONS

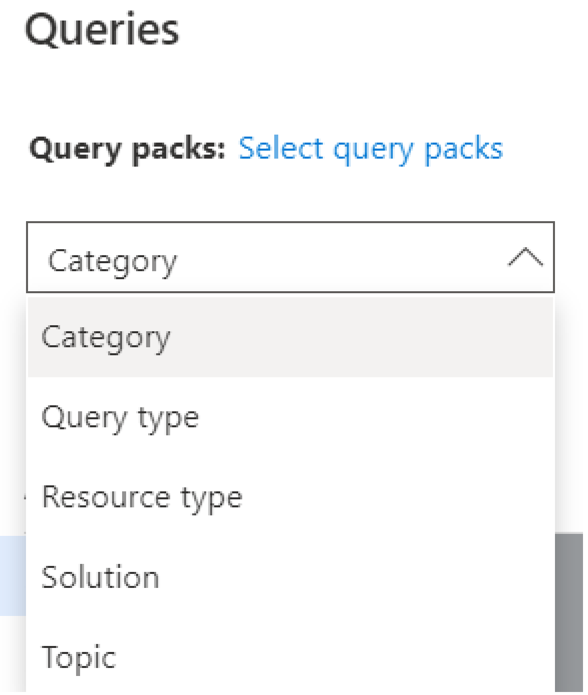
CCF application errors View the latest Confidential Consortium Framework application errors. Run Example query	**Response time trend** Chart request duration over the last 12 hours. Run Example query	**Request count trend** Chart Request count over the last day. Run Example query
Response time buckets Show how many requests are in each performance-bucket. Run Example query	**Operations performance** Calculate request count and duration by operations. Run Example query	**Top 10 countries by traffic** Chart the amount of requests from the top 10 countries. Run Example query
Page views trend Chart the page views count, during the last day. Run Example query	**Top 3 browser exceptions** What were the highest reported exceptions today? Run Example query	**Slowest pages** What are the 3 slowest pages, and how slow are they? Run Example query



Sort, Filter and Search Pre-built KQL

Click on drop-down on category, select query type
You will see all queries

Filter and search for topics



Q & A

What questions do you have?

Ask now in the Q & A section or email Jeremy at jnathan@jncomputertraining.com and Logan at Logan Hillard l.hillard@lngit.com

It was great working with you; see you next time!