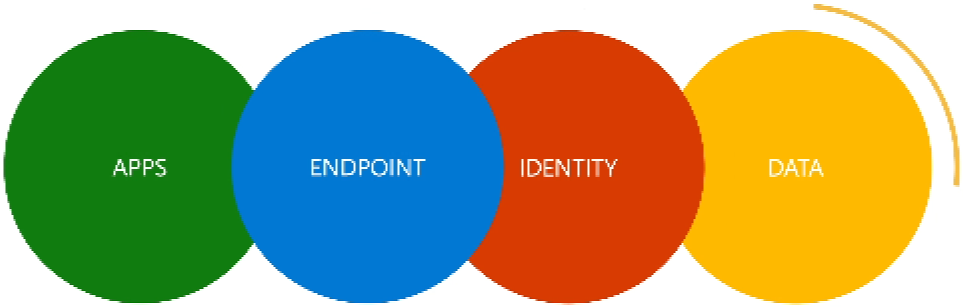
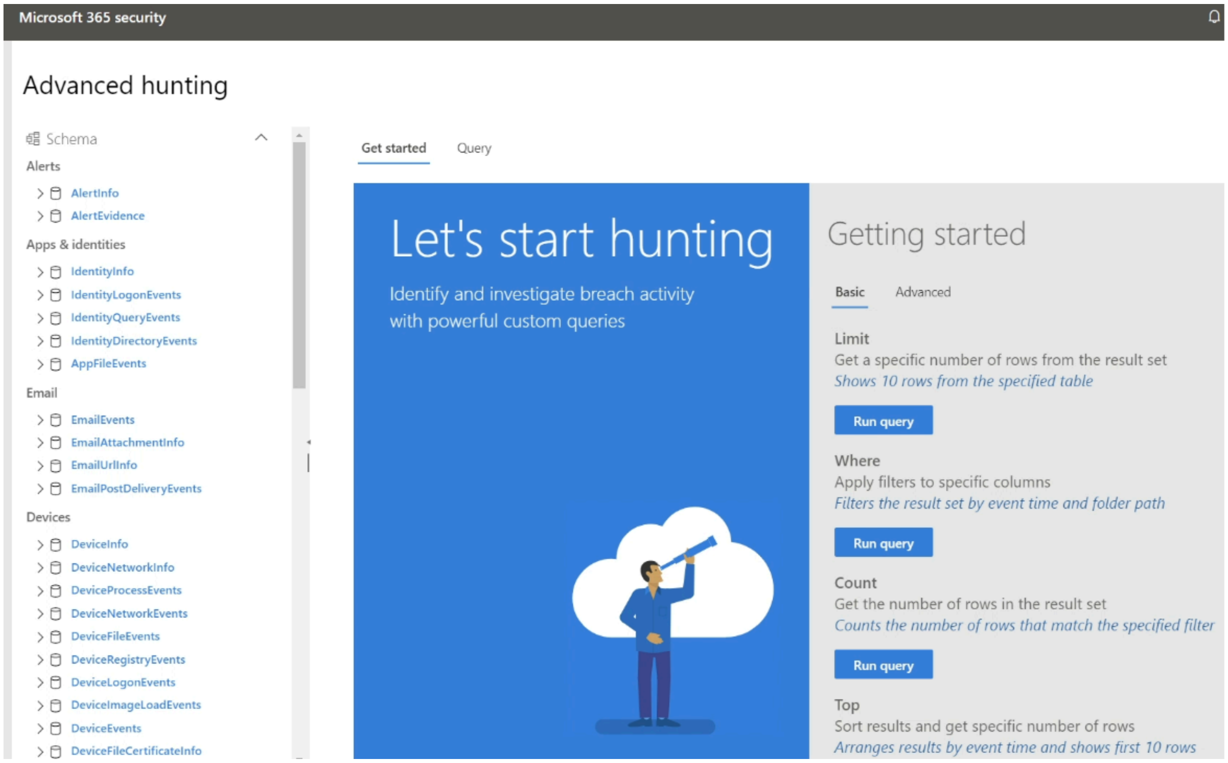
Explore advanced hunting

By: Ryan Stewart



Advanced hunting serves as a **query-driven** threat-hunting tool, empowering you to delve into a span of **30 days' worth of raw data**. With this capability, you can actively scrutinize network events to pinpoint threat indicators and entities. The versatile access to data provides unrestricted opportunities for hunting down **both** recognized and potential threats.



Microsoft 365 security

Advanced hunting

Schema

Alerts
- AlertInfo
- AlertEvidence

Apps & identities
- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- AppFileEvents

Email
- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents

Devices
- DeviceInfo
- DeviceNetworkInfo
- DeviceProcessEvents
- DeviceNetworkEvents
- DeviceFileEvents
- DeviceRegistryEvents
- DeviceLogonEvents
- DeviceImageLoadEvents
- DeviceEvents
- DeviceFileCertificateInfo

Get started | Query

Let's start hunting

Identify and investigate breach activity with powerful custom queries

Getting started

Basic | Advanced

Limit
Get a specific number of rows from the result set
Shows 10 rows from the specified table
Run query

Where
Apply filters to specific columns
Filters the result set by event time and folder path
Run query

Count
Get the number of rows in the result set
Counts the number of rows that match the specified filter
Run query

Top
Sort results and get specific number of rows
Arranges results by event time and shows first 10 rows

You can use the same threat-hunting queries to build custom detection rules. These rules run automatically to check for and then respond to suspected breach activity, misconfigured machines, and other findings. The **advanced hunting** capability supports queries that check a broader data set from:

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

To use advanced hunting, **turn on Microsoft Defender XDR.**

Data freshness and update frequency

Advanced hunting data can be categorized into **two distinct types**, each consolidated differently.

- **Event or activity data**—populates tables about alerts, security events, system events, and routine assessments. Advanced hunting receives this data almost immediately after the sensors that collect them successfully transmit them to the corresponding cloud services. For example, you can query event data from healthy sensors on workstations or domain controllers almost immediately after they're available on Microsoft Defender for Endpoint and Microsoft Defender for Identity.

- **Entity data**—populates tables with information about users and devices. This data comes from both relatively static data sources and dynamic sources, such as Active Directory entries and event logs. To provide fresh data, tables are updated with any new information every 15 minutes, adding rows that might not be fully populated. Every 24 hours, data is consolidated to insert a record that contains the latest, most comprehensive data set about each entity.

Time zone

Time information in advanced hunting is in the **UTC zone.**

Data schema

The **advanced hunting schema** is made up of multiple tables that provide either event information or information about devices, alerts, identities, and other entity types. To effectively build queries that span multiple tables, you need to understand the tables and the columns in the advanced hunting schema.

Get schema information

While constructing queries, use the built-in schema reference to quickly get the following information about each table in the schema:

- Table description—type of data contained in the table and the source of that data.
- Columns—all the columns in the table.
- Action types—possible values in the ActionType column representing the event types supported by the table. This information is provided only for tables that contain event information.
- Sample query—example queries that feature how the table can be utilized.

Custom detections

With custom detections, you can **proactively** monitor for and **respond** to various events and system states, including suspected breach activity and misconfigured endpoints. This is made possible by customizable detection rules that automatically trigger alerts and response actions.

Custom detections work with **advanced hunting,** which provides a powerful, flexible **query language** that covers a broad set of event and system information from your network. You can set them to run at regular intervals, generating alerts and taking response actions whenever there are matches.

Custom detections provide:

- Alerts for rule-based detections built from advanced hunting queries
- Automatic response actions that apply to files and devices

Create detection rules

To create detection rules:

1. Prepare the query.

In **Microsoft Defender Security Center,** go to Advanced hunting and select an existing query or create a new query. When using a new query, run the query to identify errors and understand possible results.

Important

To prevent the service from returning too many alerts, each rule is limited to generating only 100 alerts whenever it runs. Before creating a rule, tweak your query to avoid alerting for normal, day-to-day activity.

To use a query for a custom detection rule, the query must return the following columns:

- Timestamp
- DeviceId
- ReportId

Simple queries, such as those that don't use the project or summarize operator to customize or aggregate results, typically return these common columns.

There are various ways to ensure more complex queries return these columns. For example, if you prefer to aggregate and count by DeviceId, you can still return Timestamp and ReportId by getting them from the most recent event involving each device.

The sample query below counts the number of unique devices (DeviceId) with antivirus detections and uses this to find only those devices with more than five detections. To return the latest Timestamp and the corresponding ReportId, it uses the summarize operator with the arg_max function.

2. Create a new rule and provide alert details.

With the query in the query editor, select Create detection rule and specify the following alert details:

- **Detection name**—name of the detection rule
- **Frequency**—interval for running the query and taking action. See additional guidance below
- **Alert title**—title displayed with alerts triggered by the rule

- **Severity**—potential risk of the component or activity identified by the rule.

- **Category**—type of threat component or activity, if any.

- **MITRE ATT&CK techniques**—one or more attack techniques identified by the rule as documented in the MITRE ATT&CK framework. This section isn't available with certain alert categories, such as malware, ransomware, suspicious activity, and unwanted software

- **Description**—more information about the component or activity identified by the rule

- **Recommended actions**—additional actions that responders might take in response to an alert

3. Rule frequency

When saved, a new custom detection rule immediately runs and checks for matches from the past 30 days of data. The rule then runs again at fixed intervals and lookback durations based on the frequency you choose:

- **Every 24 hours**—runs every 24 hours, checking data from the past 30 days

- **Every 12 hours**—runs every 12 hours, checking data from the past 48 hours

- **Every 3 hours**—runs every 3 hours, checking data from the past 12 hours

- **Every hour**—runs hourly, checking data from the past 4 hours

- **Continuous (NRT)**—runs continuously, checking data from events as they are collected and processed in near real-time (NRT)

Select the frequency that matches how closely you want to monitor detections, and consider your organization's capacity to respond to the alerts.

Note

Setting a custom detection to run in Continuous (NRT) frequency allows you to increase your organization's ability to identify threats faster.

4. Choose the impacted entities.

Identify the columns in your query results where you expect to **find the main affected** or impacted entity. For example, a query might return both device and user IDs. Identifying which of these columns represents the main impacted entity helps the service aggregate relevant alerts, correlate incidents, and target response actions.

You can select only one column for each entity type. Columns that aren't returned by your query can't be selected.

5. Specify actions.

Your custom detection rule can automatically take actions on files or devices that are returned by the query.

Actions on devices

These actions are applied to devices in the DeviceId column of the query results:

- **Isolate device—**applies full network isolation, preventing the device from connecting to any application or service, except for the Defender for Endpoint service.

- **Collect investigation package—**collects device information in a ZIP file.

- **Run antivirus scan**—performs a full Microsoft Defender Antivirus scan on the device

- **Initiate investigation**—starts an automated investigation on the device

Actions on files

These actions are applied to files in the SHA1 or the InitiatingProcessSHA1 column of the query results:

- **Allow/Block—**automatically adds the file to your custom indicator list so that it's always allowed to run or blocked from running. You can set the scope of this action so that it's taken only on selected device groups. This scope is independent of the scope of the rule.

- **Quarantine file—**deletes the file from its current location and places a copy in quarantine

6. Set the rule scope.

Set the scope to specify which devices are covered by the rule:

- All devices

- Specific device groups

Only data from devices in scope will be queried. Also, actions will be taken only on those devices.

7. Review and turn on the rule.

After reviewing the rule, select **Create to save it**. The custom detection rule immediately runs. It runs again based on configured frequency to check for matches, generate alerts, and take response actions.