



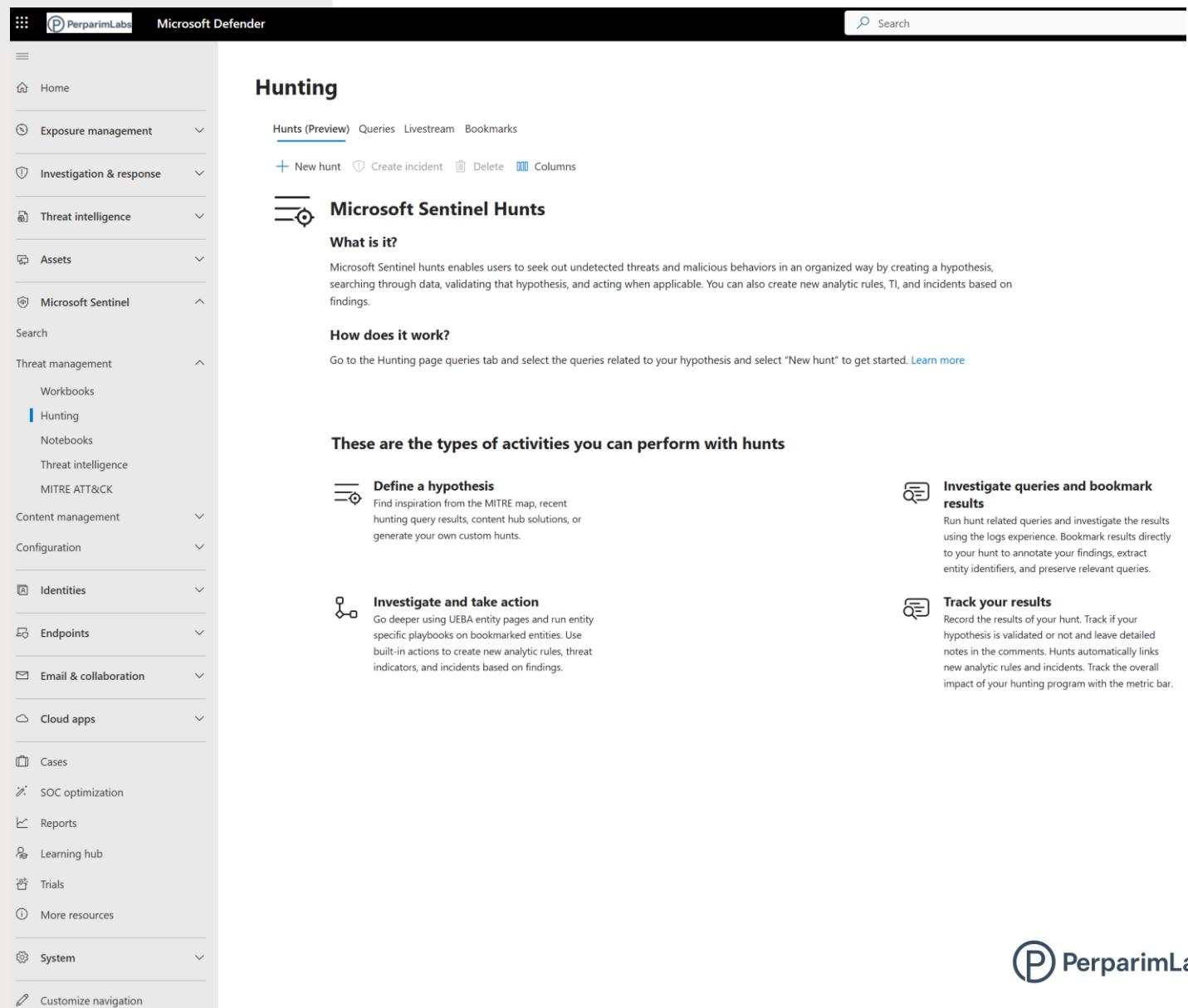
# Threat Hunting in Microsoft Sentinel

## Using Built-in Queries to Detect Suspicious Activity

- Threat hunting = proactive search for threats that haven't triggered alerts.
- Sentinel leverages log data + built-in KQL queries.
- Goal: detect hidden attacks, lateral movement, open ports, or risky behaviors.

# Hunting Entry

- Navigate to **Microsoft Sentinel > Hunting**.
- The Hunting blade centralizes all hunting queries from **Content Hub**.
- SOC teams use this to **test hypotheses**, investigate data, and take action.



## Hunting

Hunts (Preview) Queries Livestream Bookmarks

+ New hunt Create incident Delete Columns

### Microsoft Sentinel Hunts

**What is it?**

Microsoft Sentinel hunts enables users to seek out undetected threats and malicious behaviors in an organized way by creating a hypothesis, searching through data, validating that hypothesis, and acting when applicable. You can also create new analytic rules, TI, and incidents based on findings.

**How does it work?**

Go to the Hunting page queries tab and select the queries related to your hypothesis and select "New hunt" to get started. [Learn more](#)

**These are the types of activities you can perform with hunts**

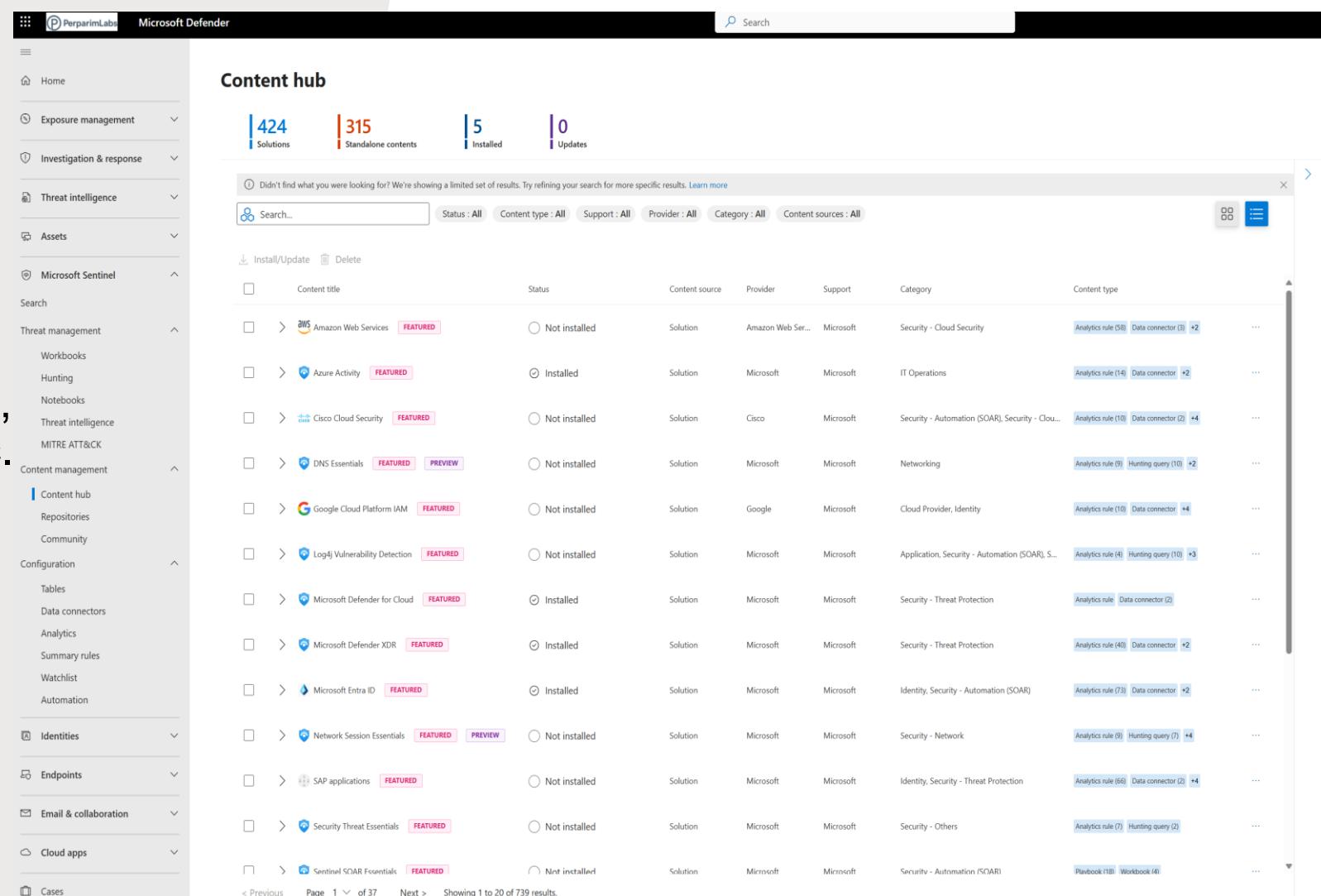
- Define a hypothesis**  
Find inspiration from the MITRE map, recent hunting query results, content hub solutions, or generate your own custom hunts.
- Investigate and take action**  
Go deeper using UEBA entity pages and run entity specific playbooks on bookmarked entities. Use built-in actions to create new analytic rules, threat indicators, and incidents based on findings.
- Investigate queries and bookmark results**  
Run hunt related queries and investigate the results using the logs experience. Bookmark results directly to your hunt to annotate your findings, extract entity identifiers, and preserve relevant queries.

**Track your results**  
Record the results of your hunt. Track if your hypothesis is validated or not and leave detailed notes in the comments. Hunts automatically links new analytic rules and incidents. Track the overall impact of your hunting program with the metric bar.

# Content Hub Providers

- Hunting queries are powered by installed **solutions/connectors**.
- Each provider (Microsoft Entra ID, Defender XDR, Azure Activity, etc. brings:
  - Prebuilt queries
  - Data connectors
  - Analytics rules
- Installing these ensures you have the **queries + data** needed.

💡 Tip: More connectors = richer hunting capability.



The screenshot shows the Microsoft Defender Content hub interface. The left sidebar includes sections for Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel (with sub-options for Workbooks, Hunting, Notebooks, Threat intelligence, and MITRE ATT&CK), Content management (with sub-options for Content hub, Repositories, Community, Configuration, Tables, Data connectors, Analytics, Summary rules, Watchlist, and Automation), Identities, Endpoints, Email & collaboration, Cloud apps, and Cases. The main content area is titled 'Content hub' and displays statistics: 424 Solutions, 315 Standalone contents, 5 Installed, and 0 Updates. A search bar and filters (Status: All, Content type: All, Support: All, Provider: All, Category: All, Content sources: All) are at the top. Below is a table with columns: Content title, Status, Content source, Provider, Support, Category, and Content type. The table lists various providers and their offerings, such as AWS, Azure Activity, Cisco Cloud Security, DNS Essentials, Google Cloud Platform IAM, Log4j Vulnerability Detection, Microsoft Defender for Cloud, Microsoft Defender XDR, Microsoft Entra ID, Network Session Essentials, SAP applications, Security Threat Essentials, and Sentinel SOAR Essentials. Each row includes a 'Download' and 'Install/Update' button. The bottom of the page shows page navigation and a note: 'Showing 1 to 20 of 739 results.'

Running hunts is free; **data ingestion** is billed via Log Analytics.

# Query Library

- Sentinel provides **181+ hunting queries** mapped to MITRE ATT&CK tactics.
- Examples:
  - Port scanning activity
  - Phishing attempts
  - Lateral movement detection
- Queries are categorized by **tactics** (**Initial Access, Persistence, Impact, etc.**).

PerparamLabs Microsoft Defender

Search

Home

Exposure management

Investigation & response

Threat intelligence

Assets

Microsoft Sentinel

Search

Threat management

Workbooks

Hunting

Notebooks

Threat intelligence

MITRE ATT&CK

Content management

Content hub

Repositories

Community

Configuration

Tables

Data connectors

Analytics

Summary rules

Watchlist

Automation

Identities

Endpoints

Email & collaboration

Cloud apps

Cases

## Hunting

12 / 181 Active / total queries | 0 / 0 Result count / queries run | 0 Livestream Results | 0 My bookmarks | More content at Content hub

Hunts (Preview) Queries Livestream Bookmarks

1 Reconnaissance 0 Resource Development 86 Initial Access 27 Execution 8 Persistence 12 Privilege Escalation 23 Defense Evasion 9 Credential Access 5 Discovery 12 Lateral Movement 5 Collection 9 Command And Control 6 Exfiltration 19 Impact

Last 24 hours + New query Run all queries Delete Hunt actions Columns

Search queries Add filter

Query	Results	Results delta	Results delta percentage	Content source	Data sources	Tactics	Techniques
MDO_Countofrecipientemailaddressesbysubject	--	--	--	Content hub		Initial Access	T1566
Detections by detection methods	--	--	--	Content hub		Initial Access	T1566
Dropping Payload via certutil	--	--	--	Content hub		Initial Access	T1566
Malware detections by detection methods	--	--	--	Content hub		Initial Access	T1566
Rare Process as a Service	--	--	--	Content hub		Persistence	T1543, T1543.003
Azure Network Security Group NSG Administrative Opera...	--	--	--	Content hub	AzureActivity	Impact	T1496
Safe Attachments detections	--	--	--	Content hub		Initial Access	T1566
DoppelPaymer Stop Services	--	--	--	Content hub		Execution	T1566
Remote File Creation with PsExec	--	--	--	Content hub		Lateral Movement	T1566
PowerShell Downloads	--	--	--	Content hub		Execution	T1566
Deletion of data on multiple drives using cipher.exe	--	--	--	Content hub		Impact	T1566
Detect MailSniper	--	--	--	Content hub		Initial Access	T1566
Port opened for an Azure Resource	--	--	--	Content hub	AzureActivity	Command and Control	T1071, T1571 + 1
Determine Successfully Delivered Phishing Emails by top I...	--	--	--	Content hub		Initial Access	T1566
DoppelPaymer Procdump	--	--	--	Content hub		Credential Access	T1566
LemonDuck Registration Function	--	--	--	Content hub		Execution	T1566
Automated email notifications and suspicious sign-in acti...	--	--	--	Content hub		Initial Access	T1566

< Previous Page 1 of 4 Next > Showing 1 to 50 of 181 results.

# Selecting a Query

- Example query: **Port opened for an Azure Resource.**
- Purpose: detects ports opened on VMs or Arc-enabled servers.
- Shows KQL script on the right-hand pane.
- You can **run as-is** or **customize KQL** (e.g., change timeframe).

**Hunting**

12 / 181 Active / total queries | 0 / 0 Result count / queries run | 0 Livestream Results | 0 My bookmarks | More content at Content hub

Hunts (Preview) Queries Livestream Bookmarks

1 Reconnaissance 0 Resource Development 86 Initial Access 27 Execution 8 Persistence 12 Privilege Escalation 23 Defense Evasion 9 Credential Access 5 Discovery 12 Lateral Movement 5 Collection 9 Command And Control 6 Exfiltration 19 Impact

Last 24 hours + New query Run selected queries Delete Hunt actions Columns

port

Query	Results	Results delta	Results delta percentage	Content source	Data sources	Tactics	Techniques	...
<input checked="" type="checkbox"/> <span>star</span> Port opened for an Azure Resource	--	--	--	Content hub	AzureActivity	<input type="checkbox"/> Command & Control	T1071, T1571 + 1	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Check for multiple signs of Ransomware Activity	--	--	--	Content hub		<input type="checkbox"/> Execution	Impact	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> MITRE - Suspicious Events	--	--	--	Content hub				<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Hunt for malicious attachments using external IOC source	--	--	--	Content hub		<input type="checkbox"/> Initial Access	T1566	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Detect Potential kerberoast Activities	--	--	--	Content hub		<input type="checkbox"/> Lateral Movement	T1558.003	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Hunt for malicious URLs using external IOC source	--	--	--	Content hub		<input type="checkbox"/> Initial Access	T1566	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Appspot Phishing Abuse	--	--	--	Content hub		<input type="checkbox"/> Initial Access	T1566	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Suspicious Spoolsv Child Process	--	--	--	Content hub		<input type="checkbox"/> Privilege Escalation	Impact	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> TI Map File Entity to WireData Event	--	--	--	Content hub		<input type="checkbox"/> Impact		<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Files Copied to USB Drives	--	--	--	Content hub		<input type="checkbox"/> Exfiltration		<span>Info</span> ...
<input type="checkbox"/> <span>star</span> TI Map File Entity to VMConnection Event	--	--	--	Content hub		<input type="checkbox"/> Impact		<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Service Accounts Performing Remote PS	--	--	--	Content hub		<input type="checkbox"/> Lateral Movement		<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Email malware detection report	--	--	--	Content hub		<input type="checkbox"/> Initial Access	T1566	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Unusual Volume of file deletion by users	--	--	--	Content hub		<input type="checkbox"/> Impact		<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Email containing malware accessed on a unmanaged devi...	--	--	--	Content hub		<input type="checkbox"/> Execution	T1204	<span>Info</span> ...
<input type="checkbox"/> <span>star</span> SAM Name Change CVE-2021-42278	--	--	--	Content hub		<input type="checkbox"/> Privilege Escalation		<span>Info</span> ...
<input type="checkbox"/> <span>star</span> Credential Harvesting Using LaZagne	--	--	--	Content hub		<input type="checkbox"/> Credential Access		<span>Info</span> ...

< Previous Page 1 of 1 Next > Showing 1 to 29 of 29 results.

Port opened for an Azure Resource

Content hub Content source Results AzureActivity Data sources

Version 2.0.1 Source name Azure Activity Supported by Microsoft Corporation Email

Description Identifies what ports may have been opened for a given Azure Resource over the last 7 days

Query

```
let lookback = 7d;
AzureActivity
| where TimeGenerated > ago(lookback)
| where OperationNameValue has_any ("ipfilterrules", "se")
// Choosing Accepted here because it has the Rule Attribute
| where ActivityStatusValue == "Accepted"
// If there is public info, include it
| extend parsed_properties = parse_json(tostring(parse_j
| extend PublicIPAddressVersion = case(Properties_has_cs
| extend protocol = case(Properties_has_cs_protocol, to
| extend sourcePortRange = case(Properties_has_cs_sourc
| summarize StartTime = min(TimeGenerated), EndTime = ma
ActivityStatusValue, ActivitySubstatus, SubscriptionId,
```

View query results >

Entity types

- Account
- IP

Tactics

- Command And Control
- Impact

The command and control tactic represents how adversaries communicate with systems under their control within a target network.  
read more on attack.mitre.org

Impact

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.  
read more on attack.mitre.org

Techniques

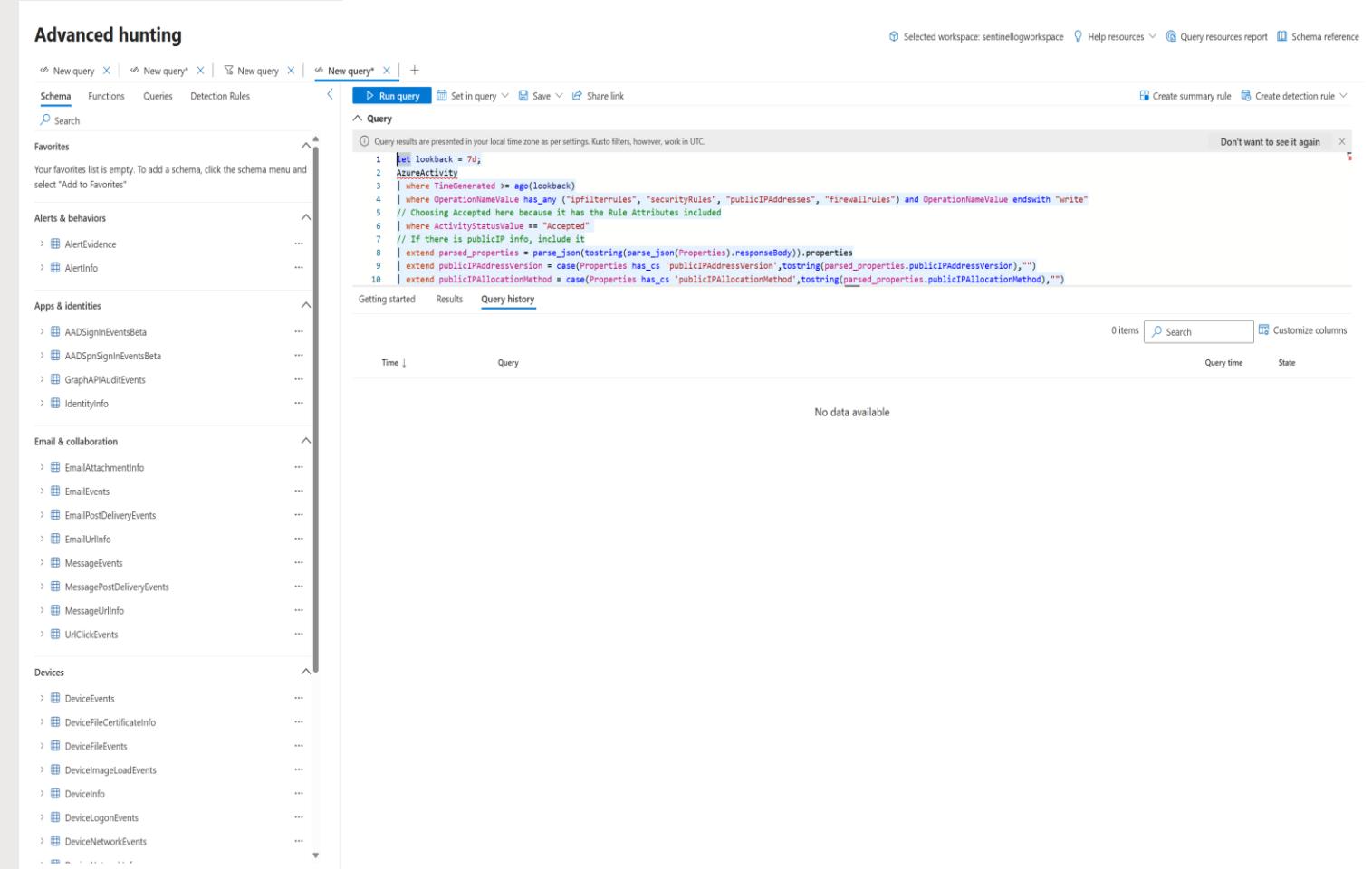
- T1071 Application Layer Protocol
- T1571 Non-Standard Port
- T1496 Resource Hijacking

Right pane shows KQL + related entity types and ATT&CK mapping

# Running the Query

- Run queries directly in **Advanced Hunting**.
- Output: list of matching activities (if detected).
- Even with **no results**, this demonstrates:
  - Query syntax
  - Data sources checked
  - Baseline validation
- **Time range matters** (retention + lookback window control what you see).

 *Tip:* In real SOC, lack of results still validates your baseline security posture.



The screenshot shows the Microsoft Sentinel Advanced Hunting interface. The left sidebar contains a navigation tree with sections: Favorites, Alerts & behaviors, Apps & identities, Email & collaboration, and Devices. The main area is titled 'Query' and contains the following Kusto query:

```
1 let lookback = 7d;
2 AzureActivity
3 | where TimeGenerated > ago(lookback)
4 | where OperationNameValue has_any ("ipfilterrules", "securityRules", "publicIPAddresses", "firewallrules") and OperationNameValue endswith "write"
5 // Choosing Accepted here because it has the Rule Attributes included
6 | where ActivityStatusValue == "Accepted"
7 // If there is publicIP info, include it
8 | extend parsed_properties = parse_json(tostring(parse_json(Properties).responseBody)).properties
9 | extend publicIPAddressVersion = case(Properties has_cs 'publicIPAddressVersion', tostring(parsed_properties.publicIPAddressVersion), "")
10 | extend publicIPAllocationMethod = case(Properties has_cs 'publicIPAllocationMethod', tostring(parsed_properties.publicIPAllocationMethod), "")
```

The results pane below shows the message 'No data available'.

The screenshot shows the Microsoft Sentinel Advanced hunting interface. On the left, a sidebar navigation includes Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Workbooks, Hunting, Notebooks, Threat intelligence, MITRE ATT&CK, Content management, Content hub, and Repositories. The main area is titled 'Advanced hunting' and shows a query history entry. The query is:

```
1 let lookback = 7d;
2 AzureActivity
3 | where TimeGenerated >= ago(lookback)
4 | where OperationNameValue has_any ("ipfilterrules", "securityRules", "publicIPAddresses", "firewallrules") and OperationNameValue endswith "write"
5 // Choosing Accepted here because it has the Rule Attributes included
6 | where ActivityStatusValue == "Accepted"
7 // If there is publicIP info, include it
8 | extend parsed_properties = parse_json(tostring(parse_json(Properties).responseBody)).properties
9 | extend publicIPAddressVersion = case(Properties has_cs 'publicIPAddressVersion',tostring(parsed_properties.publicIPAddressVersion),"")
10 | extend publicIPAllocationMethod = case(Properties has_cs 'publicIPAllocationMethod',tostring(parsed_properties.publicIPAllocationMethod),"")
```

The query history table shows one item:

Time	Query	Query time	State
2025 1:08:38 PM	let lookback = 7d; AzureActivity   where TimeGenerated >= ago(lookback)   where OperationNameValue has_any ("ipfilterrules", "securityRules", "publicIPAddresses", "firewallrules") and OperationNameValue endswith "write" // Choosing Accepted here because it has the Rule Attributes included   where AC Show full query	0.01s	Completed

# Query History

- All executed hunts are logged in **Query History**.
- **Save / Share link** to reuse with your team or convert to a detection rule later.
- Useful for:
  - Tracking which hunts were performed
  - Sharing queries with SOC teams
  - Building repeatable playbooks

# Key Takeaways

- Threat hunting = proactive defense.
- Sentinel gives **prebuilt KQL queries** from Content Hub.
- You can:
  1. Run & customize queries.
  2. Investigate suspicious activity.
  3. Feed results into **alerts, incidents, or playbooks**.
- Hunting complements **automation & analytics** for complete SOC coverage.
- Convert useful hunts to **analytics rules** or **automation** (SOAR) for continuous coverage.