

# 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.

The screenshot shows the Microsoft Defender Hunting page. The left sidebar contains a navigation menu with the following items: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management (with sub-items: Workbooks, Hunting, Notebooks, Threat intelligence, MITRE ATT&CK), Content management, Configuration, Identities, Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, More resources, System, and Customize navigation. The main content area is titled 'Hunting' and includes tabs for 'Hunts (Preview)', 'Queries', 'Livestream', and 'Bookmarks'. Below the tabs are buttons for '+ New hunt', 'Create incident', 'Delete', and 'Columns'. The 'Hunts (Preview)' tab is active, showing the 'Microsoft Sentinel Hunts' section. This section includes a 'What is it?' description, a 'How does it work?' description, and a list of activities: 'Define a hypothesis', 'Investigate and take action', 'Investigate queries and bookmark results', and 'Track your results'. The 'PerparimLabs' logo is visible in the top right corner of the interface.

Microsoft Defender

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.

PerparimLabs

# 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. On the left is a navigation pane with categories like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Configuration, Identities, Endpoints, Email & collaboration, Cloud apps, and Cases. The main area is titled 'Content hub' and displays statistics: 424 Solutions, 315 Standalone contents, 5 Installed, and 0 Updates. Below this is a search bar and filters for Status, Content type, Support, Provider, Category, and Content sources. A table lists various providers with columns for Content title, Status, Content source, Provider, Support, Category, and Content type. Providers listed include Amazon Web Services, 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 entry shows its status (Not installed or Installed) and available content types like Analytics rules and Data connectors.

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.).

The screenshot displays the Microsoft Sentinel Hunting interface. The left sidebar shows the navigation menu with categories like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, Identities, Endpoints, Email & collaboration, Cloud apps, and Cases. The main content area is titled 'Hunting' and shows a summary of 12/181 active queries, 0/0 result counts, and 0 live stream results. Below this, there are tabs for Hunts (Preview), Queries, Livestream, and Bookmarks. A horizontal bar categorizes queries by MITRE ATT&CK tactics: Reconnaissance (1), Resource Development (0), Initial Access (86), Execution (27), Persistence (8), Privilege Escalation (12), Defense Evasion (23), Credential Access (9), Discovery (5), Lateral Movement (12), Collection (5), Command And Control (9), Exfiltration (6), and Impact (19). A search bar and filters are available. The main table lists queries with columns for Query, Results, Results delta, Results delta percentage, Content source, Data sources, Tactics, and Techniques. The table shows 181 results, with the first 50 displayed.

Query	Results	Results delta	Results delta percentage	Content source	Data sources	Tactics	Techniques
MDO_Countofrecipientsemailaddressesbysubject	--	--	--	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	Defense
Remote File Creation with PsExec	--	--	--	Content hub		Lateral Movement	
PowerShell Downloads	--	--	--	Content hub		Execution	
Deletion of data on multiple drives using cipher.exe	--	--	--	Content hub		Impact	
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	
LemonDuck Registration Function	--	--	--	Content hub		Execution	Persistence
Automated email notifications and suspicious sign-in acti...	--	--	--	Content hub		Initial Access	T1566

# 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).

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

The screenshot displays the Microsoft Sentinel Hunting interface. The main panel shows a list of queries, with 'Port opened for an Azure Resource' selected and highlighted by a red box. The right-hand pane provides a detailed view of this query, including its KQL script, related entity types, and ATT&CK mappings.

**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 Add filter

Query	Results	Results delta	Results delta percentage	Content source	Data sources	Tactics	Techniques
<input checked="" type="checkbox"/> <input type="star"/> Port opened for an Azure Resource	--	--	--	Content hub	AzureActivity	Command and Control	T1071, T1571 +1
<input type="checkbox"/> <input type="star"/> Check for multiple signs of Ransomware Activity	--	--	--	Content hub		Execution	T1027
<input type="checkbox"/> <input type="star"/> MITRE - Suspicious Events	--	--	--	Content hub			
<input type="checkbox"/> <input type="star"/> Hunt for malicious attachments using external IOC source	--	--	--	Content hub		Initial Access	T1566
<input type="checkbox"/> <input type="star"/> Detect Potential kerberoast Activities	--	--	--	Content hub		Lateral Movement	T1558.003
<input type="checkbox"/> <input type="star"/> Hunt for malicious URLs using external IOC source	--	--	--	Content hub		Initial Access	T1566
<input type="checkbox"/> <input type="star"/> Appspot Phishing Abuse	--	--	--	Content hub		Initial Access	T1566
<input type="checkbox"/> <input type="star"/> Suspicious Spoolsv Child Process	--	--	--	Content hub		Privilege Escalation	
<input type="checkbox"/> <input type="star"/> TI Map File Entity to WireData Event	--	--	--	Content hub		Impact	
<input type="checkbox"/> <input type="star"/> Files Copied to USB Drives	--	--	--	Content hub		Exfiltration	
<input type="checkbox"/> <input type="star"/> TI Map File Entity to VMConnection Event	--	--	--	Content hub		Impact	
<input type="checkbox"/> <input type="star"/> Service Accounts Performing Remote PS	--	--	--	Content hub		Lateral Movement	
<input type="checkbox"/> <input type="star"/> Email malware detection report	--	--	--	Content hub		Initial Access	T1566
<input type="checkbox"/> <input type="star"/> Unusual Volume of file deletion by users	--	--	--	Content hub		Impact	
<input type="checkbox"/> <input type="star"/> Email containing malware accessed on a unmanaged devi...	--	--	--	Content hub		Execution	T1204
<input type="checkbox"/> <input type="star"/> SAM Name Change CVE-2021-42278	--	--	--	Content hub		Privilege Escalation	
<input type="checkbox"/> <input type="star"/> Credential Harvesting Using LaZagne	--	--	--	Content hub		Credential Access	

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

**Port opened for an Azure Resource**

Content hub | 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 Attrib
// where ActivityStatusValue == "Accepted"
// If there is publicIP info, include it
| extend parsed_properties = parse_json(tostring(parse_j
| extend publicIpAddressVersion = case(Properties has_cs
| extend publicIPAllocationMethod = case(Properties has_
// Include rule attributes for context
| extend access = case(Properties has_cs 'access', tostri
| extend description = case(Properties has_cs 'descriptio
| extend destinationPortRange = case(Properties has_cs '
| extend direction = case(Properties has_cs 'direction',
| 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: 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 | T1571 | T1496

Application Layer Protocol | Non-Standard Port | Resource Hijacking

View results

# 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 displays the Microsoft Sentinel Advanced Hunting interface. On the left, a sidebar lists various data sources under categories like 'Alerts & behaviors', 'Apps & identities', 'Email & collaboration', and 'Devices'. The main panel shows a Kusto query being executed. The query is as follows:

```
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), '')
```

Below the query editor, the 'Results' tab is active, showing a table with columns 'Time', 'Query', 'Query time', and 'State'. The table is empty, displaying 'No data available'.

Advanced hunting

Selected workspace: sentinellogworkspace | Help resources | Query resources report | Schema reference

Run query | Set in query | Save | Share link

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
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), "")
```

Getting started | Results | Query history

1 item | Search | Customize columns

Time ↓	Query	Query time	State
<input type="checkbox"/> 2025 1:08:38 PM	<pre>let lookback = 7d; AzureActivity   where TimeGenerated &gt;= 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</pre> <a href="#">Show full query</a>	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.