

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

# How to Use Orbital Advanced Search in Your Secure Endpoint Workflows

Subtitle goes here

Brian McMahon, Technical Marketing Engineer  
BRKSEC-1016

# Cisco Webex App

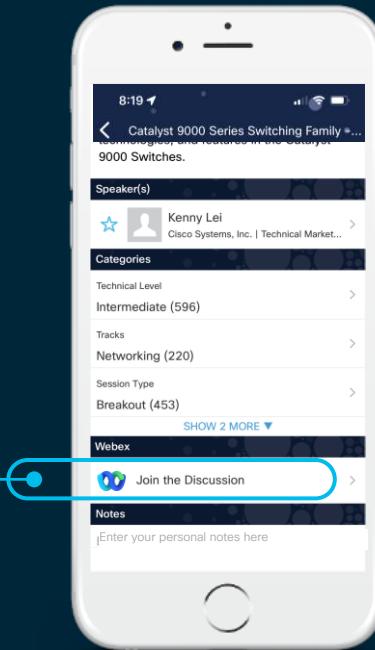
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

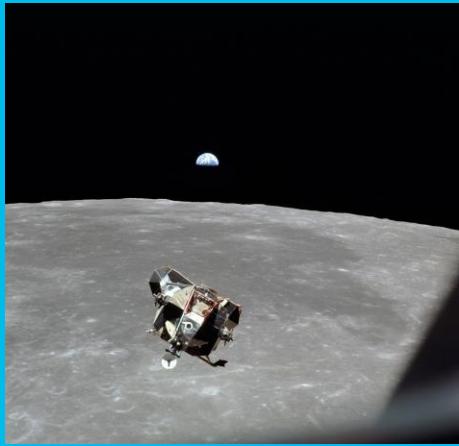
Webex spaces will be moderated by the speaker until June 17, 2022.



# Agenda

- Introduction to Orbital
- Searches: Building, Borrowing, Stealing
- Running a Search: Scheduled, Event-Driven, On-Demand
- Using Orbital with SecureX Orchestration
- Conclusion

# Introduction to Orbital



## What is Orbital?

Image source:  
Apollo 11 Lunar Module Eagle rendezvousing with Command module  
Columbia in lunar orbit  
By Michael Collins - NASA (hi-res), Public Domain,  
<https://commons.wikimedia.org/w/index.php?curid=506841>

- Orbital Advanced Search is a feature of Cisco Secure Endpoint available with the Advantage license and higher.
- Orbital searches provide SQL-like queries of attributes on a running system.
- The underlying technology is osquery.
- Searches can be run on demand, scheduled, or via scripts and automation.

# Why Use Orbital?

- Use case: Threat Hunting
  - Hypothesis-driven hunting
  - Malware Analytics searches
- Use case: Incident Response
  - Forensic snapshots
  - ATT&CK framework
- Use case: IT Operations
  - Not just for SecOps
- Use case: Vulnerability Management and Compliance
  - Remediate, but verify

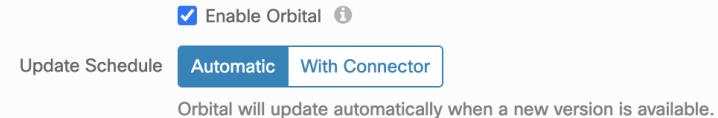
# What do I need to start using Orbital?

- Cisco Secure Endpoint with Advantage or Premier license
- OS requirements:
  - Windows 10 (1803 or later) / 11
  - Windows Server 2016 / 2019 / 2022
  - macOS 10.15 / 11 / 12
  - RHEL (and compatible) 6.10 / 7 (7.2 or later) / 8
  - Ubuntu 18.04 / 20.04
  - Oracle Linux (UEK) 7 / 8
  - Debian 10 / 11

# What do I need to start using Orbital?

- Secure Endpoint version requirements:
  - Windows connector 7.1.5 +
  - macOS connector 1.16.0 +
  - Linux connector 1.17.0 +
- Orbital ✓ Enabled under Advanced Settings in Policy

## Orbital



- Not currently available for Private Cloud

# A Closer Look at osquery

- Originally developed by Facebook, then open-sourced
- Exposes an operating system as a relational database
- Cross-platform support (Windows, macOS, Linux, FreeBSD)
- Docs and schemas at <https://osquery.io>

The screenshot shows the osquery.io website. At the top, there is a navigation bar with links for HOME, SCHEMA, BLOG, DOCS, GITHUB, and DOWNLOADS. The main content area features a heading "osquery/osquery" and "Performant endpoint visibility" above a list of supported platforms: Apple, Linux, macOS, Windows, and FreeBSD. Below this, there are three examples of schema data: "etc\_hosts" (showing address and hostnames), "shell\_history" (showing a log of sudo commands), and "os\_version" (showing build, version, and patch information).

Address	Hostnames
127.0.0.1	localhost

Time	Command
10:03AM	sudo adduser gust
10:04AM	sudo visudo

Build	17A362
Version	10.1.13
Patch	6

# Okay ... so, why pay for Orbital if osquery is free?

- Extensive catalog of prebuilt searches, continually updated with Talos threat intel, and mapped to MITRE ATT&CK
- Secure Endpoint console integration with forensic snapshots and automated actions
- SecureX integration (ribbon, orchestration workflows)
- Secure Malware Analytics integration

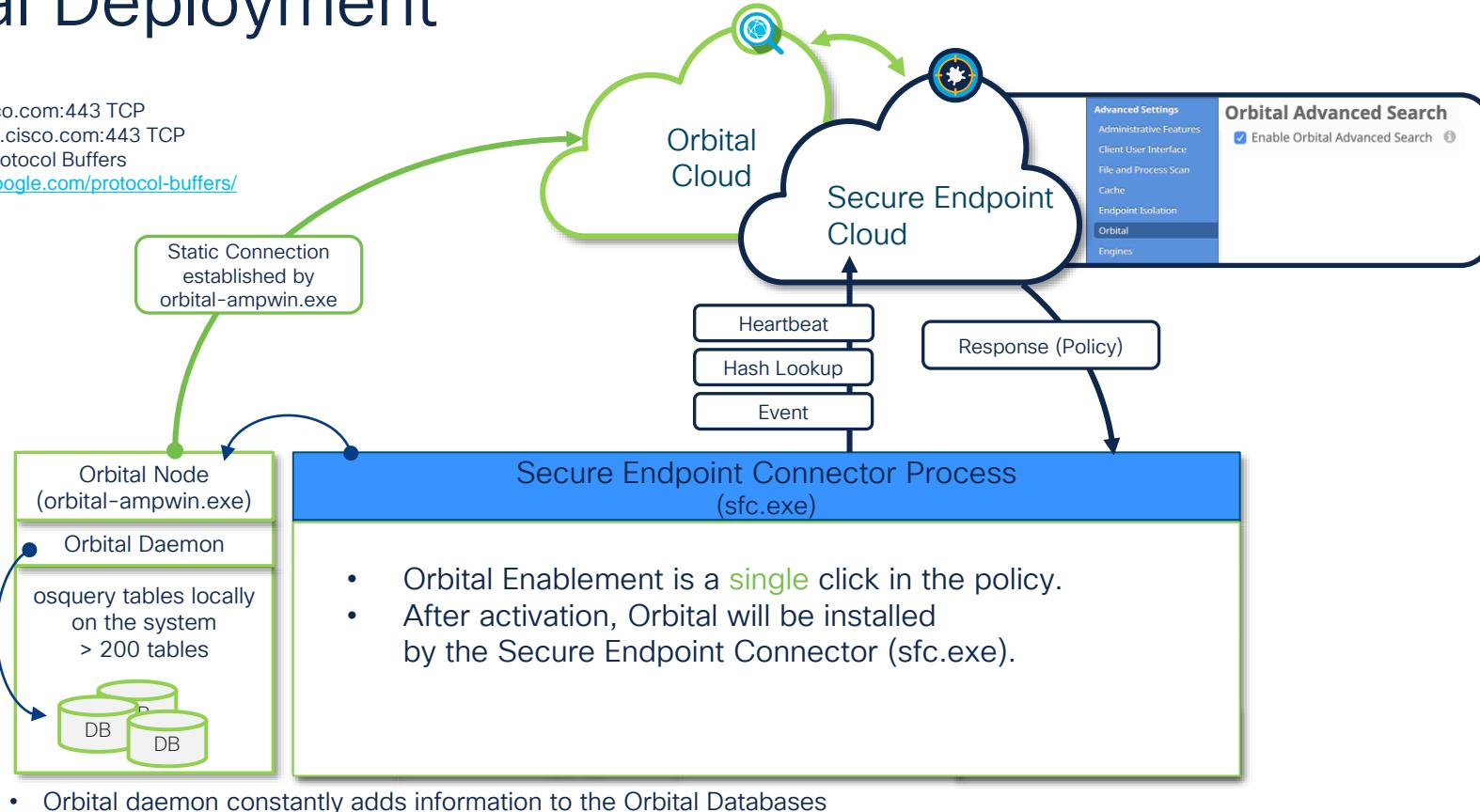
# Okay ... so, why pay for Orbital if osquery is free? (Part 2)

- Ability to schedule query runs in the portal
- APIs for search submission and result processing
- Linked queries let you use the results from one search to fine-tune the next one
- If you're using the Premier license threat hunting, and/or Secure Endpoint Pro MEDR, Orbital is a key component of those services

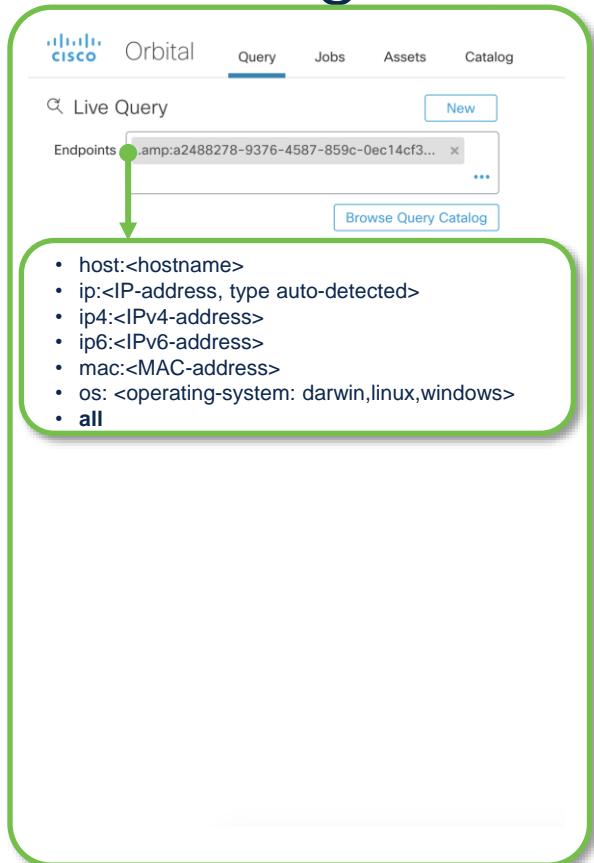
# Overview of Orbital Deployment Process

# Orbital Deployment

- orbital[.eu].amp.cisco.com:443 TCP
- ncp[.eu].orbital.amp.cisco.com:443 TCP
- Based on Google Protocol Buffers  
<https://developers.google.com/protocol-buffers/>

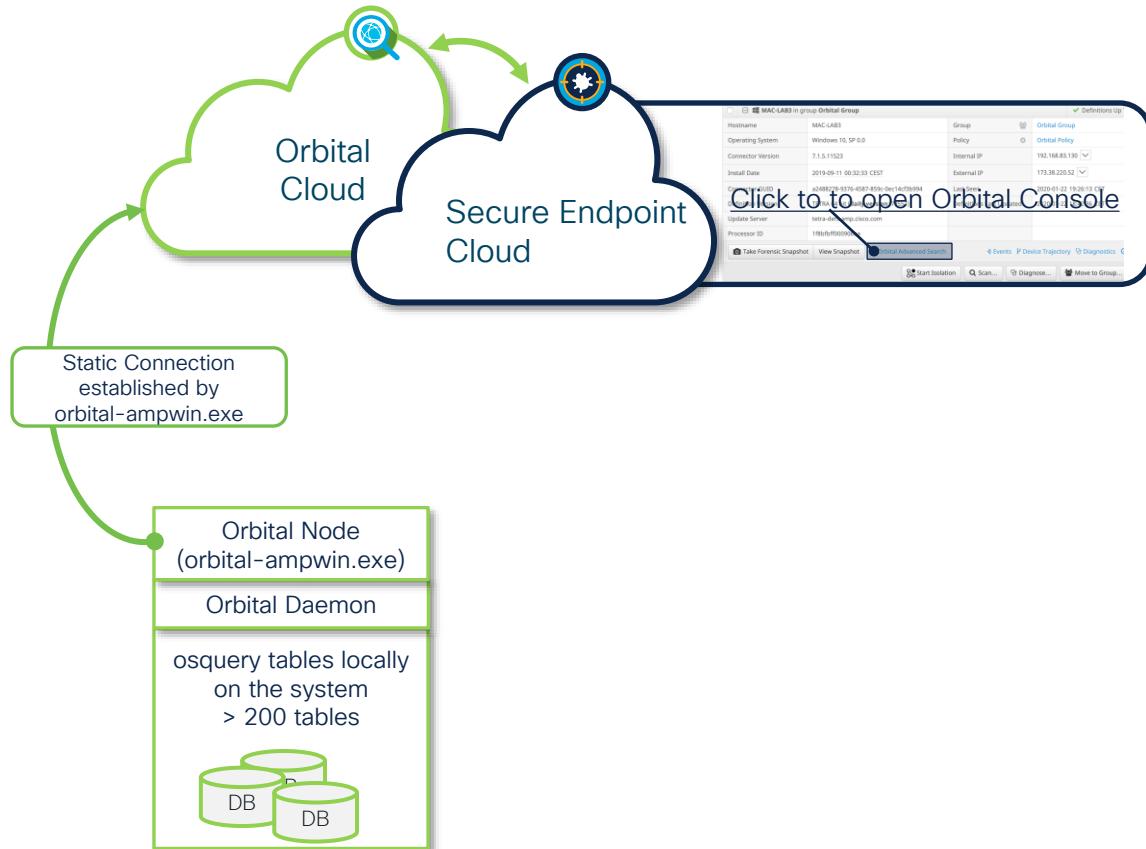


# Running a Query

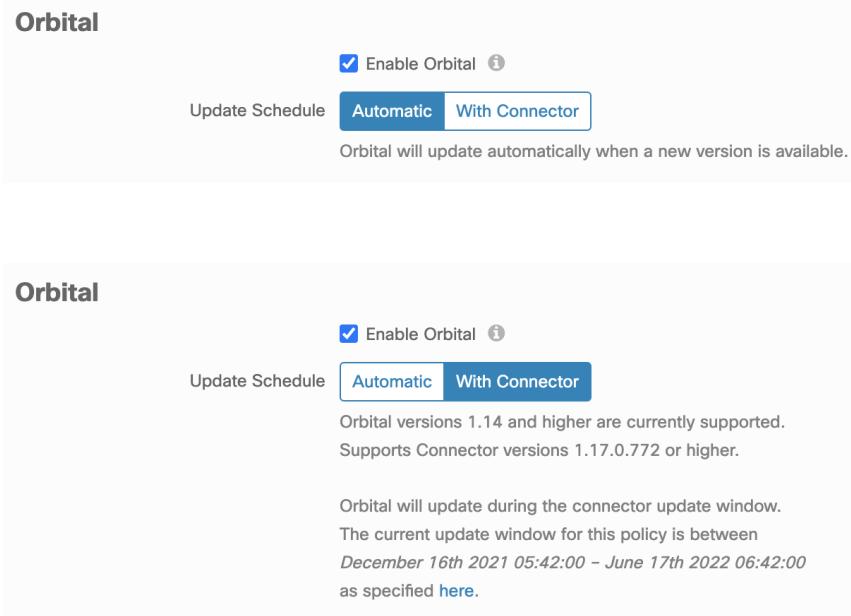


The screenshot shows the Cisco Orbital web interface. The top navigation bar includes 'Orbital', 'Query' (which is highlighted in blue), 'Jobs', 'Assets', and 'Catalog'. Below the navigation is a search bar labeled 'Live Query' with a 'New' button. A list of endpoints is shown, with the first item being 'Endpoints &:a2488278-9376-4587-859c-0ec14cf3...'. A 'Browse Query Catalog' button is also present. A green callout box highlights a list of query filters:

- host:<hostname>
- ip:<IP-address, type auto-detected>
- ip4:<IPv4-address>
- ip6:<IPv6-address>
- mac:<MAC-address>
- os: <operating-system: darwin,linux,windows>
- all



# Orbital Updates on the Endpoint



The image contains two side-by-side screenshots of the Cisco Orbital interface. Both screenshots show the 'Orbital' configuration page with the following elements:

- Enable Orbital:** A checked checkbox with a help icon.
- Update Schedule:** A dropdown menu with two options: **Automatic** (selected) and **With Connector**.
- Text below Update Schedule:** Orbital will update automatically when a new version is available.
- Second Screenshot Details:** Orbital versions 1.14 and higher are currently supported. Supports Connector versions 1.17.0.772 or higher. Orbital will update during the connector update window. The current update window for this policy is between December 16th 2021 05:42:00 – June 17th 2022 06:42:00 as specified [here](#).

- Orbital updates are released every two weeks or so.
- With “Automatic” selected as your update schedule, the endpoints will apply the updates when they become available.
- If you need to exercise more control over your endpoint updates, choose “With Connector” instead; Orbital on the endpoints will be updated to the latest version at the same time as the new connector version.

# Orbital Cloud Console: Dashboard

Orbital

Dashboard    Query    Results    Endpoints    Catalog

Last 24 hours    Auto Refresh

Dashboard    Organization Metrics    My Metrics    0% prior period

Active Queries: 0    Hosts Queried: 0    Hosts Seen: 4    Average Query Time: —    Custom Queries: 0    Node Version Status: 5 Supported, 0 Unsupported, 0 Rejected

RECENT QUERIES

Job	Time	Endpoints	Result	Status
Job 2022-02-09 01:55:08	2022-02-09 01:55:08	0	0	✓ Completed
Live Query 2021-12-18 00:01:12	2021-12-18 00:01:12	0	0	✓ Completed
Live Query 2021-12-17 23:18:05	2021-12-17 23:18:05	0	0	✓ Completed
Live Query 2021-12-17 23:07:02	2021-12-17 23:07:02	0	0	✓ Completed
Live Query 2021-12-17 22:36:59	2021-12-17 22:36:59	0	0	✓ Completed

Results during past day

Top Catalog Queries

No catalog queries in the last 24 hours. [View Catalog](#).

# Orbital Cloud Console: Query

Orbital Dashboard Query Results Endpoints Catalog

brmcmaho@cisco.com SECURE

## Query

Endpoints *Add host:hostname, IP, MAC, node ID, or Connector GUID*

Search Query Catalog  [Browse](#)

Custom SQL *ex. SELECT column\_name FROM table\_name;*

[Live Query](#) [Schedule Query](#)

### Favorites

Last Logged ... DNS Cache M... File Search Scheduled Ta... Scheduled Ta... Hidden Sched...

### My Recent Queries

Forensic Snap... Linux Log4j M... Linux Log4j M... Linux Log4j M... Linux Log4j M... Linux Log4j M...

### Featured

#### Orbiting the Cloud(s)

The purpose of this article is to briefly explore a set of osquery tables that we recently discovered here at Query Corner Headquarters, providing metadata for instances running in the AWS and Azure clouds. If your cloud provider of choice is Amazon, then the table you want is called `ec2_instance_metadata`, and the simplest way to use it is a custom query: `SELECT ...`

[AWS EC2 Instance](#)

[Azure Instance](#)

#### Xanthe - Docker Aware Miner - TALOS

Xanthe is a multi-modular botnet that drops a payload to mine Monero cryptocurrency and employs various methods to spread across networks, mainly harvesting client-side certificates to gain access to known hosts using ssh, or spreading to systems with an incorrectly configured Docker API. Two additional bash scripts terminate security services,...

[Xanthe Filepath](#)

[Xanthe Crontab](#)

#### Two Views of PrintNightmare

Hard-copy printing may feel very "old school" now, but a recent flurry of activity related to the print spooler service on Windows operating systems has brought one of the oldest IT applications back into the spotlight again. Since this vulnerability is being actively exploited, of course now is an excellent time to devote a bit of attention to figuring out where in our...

[Running Services Search: Spooler](#)

[Verify GPO Mitigation](#)

#### Explore More Queries

Chrome Browser Extensions M...

Registry Key Search

ARP Cache Inspection

# Orbital Cloud Console: Results

Orbital Dashboard Query **Results** Endpoints Catalog

Show Live Queries Download JSON Refreshed 2022-05-13 23:50:41

Name	Status	Created	Endpoints	Interval	Results	Result Rows	Type	Catalog	Creator	Remote Data Store	Errors
Job 2022-02-09 01:55:08	✓ Completed	2022-02-09 01:58:35	2022-02-09 01:55:08	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-11-19 22:18:11	✓ Completed	2021-11-19 22:21:50	2021-11-19 22:18:11	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-10-20 23:53:18	✓ Completed	2021-10-21 00:13:31	2021-10-20 23:53:18	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-09-03 04:44:57	✓ Completed	2021-09-03 05:05:27	2021-09-03 04:44:57	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-09-03 04:44:50	✓ Completed	2021-09-03 04:45:56	2021-09-03 04:44:50	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-09-03 03:26:14	✓ Completed	2021-09-03 03:30:25	2021-09-03 03:26:14	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-09-03 03:26:08	✓ Completed	2021-09-03 03:46:17	2021-09-03 03:26:08	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-09-03 03:26:00	✓ Completed	2021-09-03 03:27:37	2021-09-03 03:26:00	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-09-03 03:25:50	✓ Completed	2021-09-03 03:27:47	2021-09-03 03:25:50	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-09-03 03:25:35	✓ Completed	2021-09-03 03:45:37	2021-09-03 03:25:35	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-05-25 04:43:43	✓ Completed	2021-05-25 04:44:53	2021-05-25 04:43:43	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-04-21 05:16:10	✓ Completed	2021-04-21 05:17:10	2021-04-21 05:16:10	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2020-12-14 18:13:41	✓ Completed	2020-12-14 18:15:50	2020-12-14 18:13:41	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2020-12-14 18:13:26	✓ Completed	2020-12-14 18:14:30	2020-12-14 18:13:26	0	0	0	Secure End...	Forensic Sn...	Brian McM...	***	0

# Orbital Cloud Console: Endpoints

Orbital Dashboard Query Results Endpoints **Endpoints** Catalog

brmcaho@cisco.com SECURE

Endpoints Organization Metrics My Metrics Last 24 hours Download all as CSV Refreshed 2022-05-13 23:46:52

Hosts Seen: 4 ▲ 0% prior period Hosts Queried: 0 ▲ 0% prior period Node Version Status: 5 Supported, 0 Unsupported, 0 Rejected

Search Endpoints host:hostname, IP, MAC, node ID or Connector GUID

Hostname	Added To Orbital	Last Seen	Active IP	OS	MAC	Node Version	Interfaces
~2.local	2021-09-02 05:26:00	2022-05-13 22:57:28	172.27.20.22/24	Darwin 21.4.0 Darwin Kernel...	38:f9:d3:8...	1.18.4	10
~1.local	2021-09-02 05:09:29	2022-05-13 23:41:13	172.27.20.40/24	Darwin 19.6.0 Darwin Kernel...	14:7d:da:c...	1.18.4	6
~0.local	2021-09-02 02:38:45	2022-05-13 23:22:54	192.168.0.13/22	Darwin 21.4.0 Darwin Kernel...	14:7d:da:0...	1.18.4	9
~ok.local	2021-09-01 22:32:57	2022-05-13 21:16:06	172.27.20.27/24	Darwin 19.6.0 Darwin Kernel...	c4:b3:01:d...	1.18.4	9
~1-89V2	2021-08-31 23:17:16	2022-05-13 23:18:13	10.155.76.28/22	Darwin 20.6.0 Darwin Kernel...	88:66:5a:5...	1.18.4	8

# Orbital Cloud Console: Catalog

Orbital Dashboard Query Results Endpoints Catalog

brmcaho@cisco.com SECURE

## Query Catalog

Filters [Reset](#)

Search Catalog

Name	Created	Updated	ID	OS	Category	ATT&CK™ Tactic
Accessibility Features File Replacement Monitoring	2019-02-28	2019-08-16	file_replacement_monitoring	Windows	Threat Hunting	Persistence Defense Evasion
Account Excluded From Sync Monitoring	2019-11-22	2021-07-15	accounts_excluded_from_sync_monitoring	Windows	Posture Assessment	Defense Evasion
Active Directory Configuration Monitoring	2021-03-05	2021-08-10	macos_ad_config_monitoring	Mac	Posture Assessment	
Active Directory Replication from Non Machine Account Monitor...	2020-09-23	2021-09-27	windows_dcsync_non_machine_account_monitoring	Windows	Threat Hunting Forensics	Credential Access
Aedebug Registry Key Monitoring	2019-04-09	2021-07-15	aedebug_registry_key_monitoring	Windows	Posture Assessment Forensics	Persistence Defense Evasion
Antimalware Scan Interface (AMSI) FeatureBits Configuration	2021-06-18	2021-06-28	windows_registry_amsi_feature_bits	Windows	Posture Assessment	
Apple System Log (ASL) System Events Monitoring	2021-03-02	2021-08-11	macos_asl_monitoring	Mac	Threat Hunting Forensics	
Apple System Log tccd Service Events Monitoring	2022-01-13	2022-01-13	macos_asl_tccd_service_monitoring	Mac	Posture Assessment Forensics	Persistence Privilege Escalation
Application Compatibility Shims Search	2019-05-16	2019-08-14	shims_param_search	Windows	Posture Assessment	Persistence Privilege Escalation

# Orbital Cloud Console: Help



- The “?” icon takes you to online help.
- You can also browse directly to:  
<https://orbital.amp.cisco.com/help/>
- This is also where the Orbital release notes are kept, under “What’s New?”

The screenshot shows the Orbital Help page. The left sidebar contains a navigation menu with sections like Orbital Help, System Requirements, SecureX Sign-on, Orbital User Interface, Orbital APIs, and Client Authentication. The main content area is titled "Orbital Help" and discusses the service's purpose and supported platforms. It also includes sections for "Important Points of Note", "About", "User Interface", "SecureX Sign-On", and "Support".

**Orbital Help**

Cisco Orbital is a service that adds [osquery](#) to [Secure Endpoint](#) to support detailed and fast queries for incident responders. Orbital is available on the following platforms:

- Windows 10 (1803 or later) / 11
- Windows Server 2016 / 2019 / 2022
- macOS 10.15 / 11 / 12
- RedHat Enterprise Linux (and compatible distributions) 6.10 / 7 (7.2 or later) / 8
- Ubuntu 18.04 / 20.04
- Oracle Linux (UEK) 7 / 8
- Debian 10 / 11

**Important Points of Note:**

- Orbital supports the use of [proxies](#), except SSL terminating proxies. All operating systems can be used with [proxies](#).
- The screen captures in these [Help](#) topics may not always reflect the latest product names or UI enhancements.
- Apple's M1 hardware is not currently supported.

**About:**

- [What is Orbital?](#) – What is Orbital and how can you use it?
- [How Do I Get Orbital?](#) – How can you get Orbital?
- [Requirements](#) – What do you need to use Orbital?
- [Quick Start](#) – How do you use Orbital to query Secure Endpoint endpoints?
- [Orbital APIs](#) – How to write applications that use Orbital.
- [Remote Data Stores](#) – Use the Orbital Remote Data Stores interface to send results to your choice of destinations.

**User Interface:**

- [Query](#) – Run and schedule queries.
  - [Schedule Orbital Query](#) – How to create Orbital scheduled queries.
- [Results](#) – Results are used to manage queries.
- [Endpoints](#) – View detailed endpoint information.
- [Catalog](#) – Find queries designed by Cisco to search and investigate.

**SecureX Sign-On**

- [SecureX Sign-On Integration](#) – Using Orbital with a SecureX Sign-On account.
- [SecureX New Account](#) – How to create a new SecureX account.

**Support:**

- [Orbital Nodes](#) – Discussion on Orbital Nodes.

# Searches: Building, Borrowing, Stealing

# Orbital Search DIY (Do It Yourself)

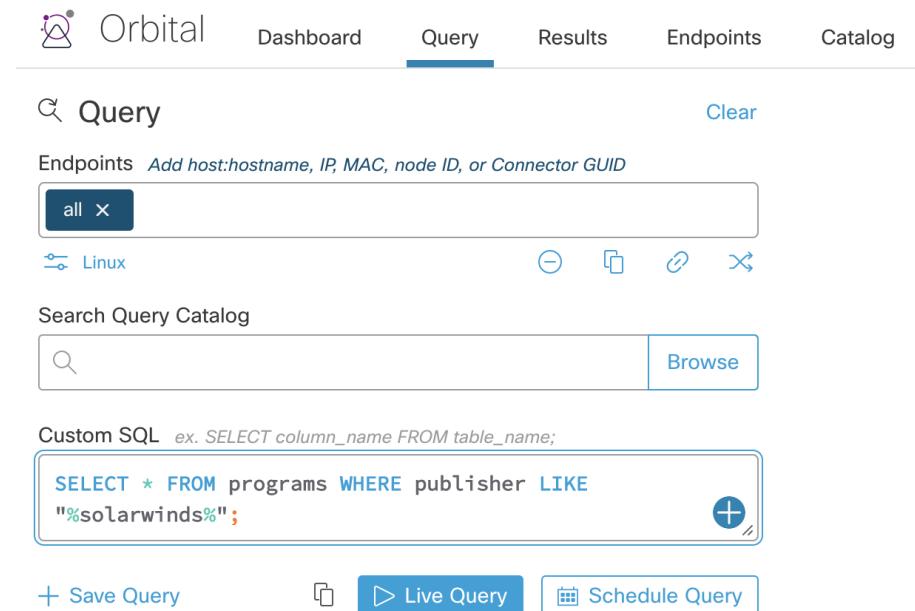
- You can type (or cut and paste) a query into the “Custom SQL” field.
- The query can be run immediately or scheduled.
- Custom queries can be saved, and will show up as “Organization Queries” in the Query Catalog filter.

## Query Catalog

Filters

Reset

 Organization Queries



The screenshot shows the Orbital Search interface with the 'Query' tab selected. At the top, there is a navigation bar with 'Orbital', 'Dashboard', 'Query' (which is highlighted in blue), 'Results', 'Endpoints', and 'Catalog'. Below the navigation bar, there is a search bar labeled 'Query' with a 'Clear' button. Underneath the search bar, there is a section for 'Endpoints' with a placeholder 'Add host:hostname, IP, MAC, node ID, or Connector GUID' and a dropdown menu currently set to 'all'. To the right of the endpoints section are four small icons: a minus sign, a copy icon, a link icon, and a close icon. Below the endpoints section is a 'Search Query Catalog' input field with a magnifying glass icon and a 'Browse' button. Further down is a 'Custom SQL' section with a placeholder 'ex. SELECT column\_name FROM table\_name;' and a text input field containing the query: 'SELECT \* FROM programs WHERE publisher LIKE "%solarwinds%"'. To the right of this input field is a blue plus icon with a white circle. At the bottom of the interface are three buttons: '+ Save Query', 'Save Query' (with a save icon), and 'Live Query' (with a play icon). There is also a 'Schedule Query' button.

# A Closer Look at the Query Catalog

## □ Query Catalog

Filters

[Reset](#)

 Organization Queries

 Favorite Queries

 Deprecated Queries

> Categories

> Operating System

> ATT&CK™ Tactics

> ATT&CK™ Techniques

- The catalog contains hundreds of prebuilt queries, mapped to general categories and to the MITRE ATT&CK framework.
- Each entry includes a plain-language description of what it does.
- Catalog queries can be used as they are, or modified by specifying parameters on the query page, or simply used as the starting point for creating your own queries.



## Query Catalog

Filters Reset Organization Queries Favorite Queries

## Categories

 Forensics Live Acquisition Of Volatile Data Malware Posture Assessment Threat Hunting

## Operating System

 Mac Windows

## ATT&amp;CK™ Tactics

 Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discovery Lateral Movement Collection Command and Control

## Search Catalog



Name	Created	Updated	ID	OS	Category	ATT&CK™ Tactic	ATT&CK™ Technique
Accessibility Features File Replacement Monitoring	2019-02-28	2019-08-16	file_replacement_monitoring	Windows	Threat Hunting	Persistence Defense Evasion	Accessibility Features
Account Excluded From Sync Monitoring	2019-11-22	2021-07-15	accounts_excluded_from_sync_monitoring	Windows	Posture Assessment	Defense Evasion	
Active Directory Configuration Monitoring	2021-03-05	2021-08-10	macos_ad_config_monitoring	MacOS	Posture Assessment		
Active Directory Replication from Non Machine Account Monitor...	2020-09-23	2021-04-15	windows_dcsync_non_machine_account_monitoring	Windows	Posture Assessment Threat Hunting Forensics	Credential Access	Credential Dumping
Aedebug Registry Key Monitoring	2019-04-09	2021-07-15	aedebug_registry_key_monitoring	Windows	Posture Assessment Forensics	Persistence Defense Evasion	Modify Registry
Antimalware Scan Interface (AMSI) FeatureBits Configuration	2021-06-18	2021-06-28	windows_registry_amsi_feature_bits	Windows	Posture Assessment		
Apple System Log (ASL) System Events Monitoring	2021-03-02	2021-08-11	macos_asl_monitoring	MacOS	Posture Assessment Threat Hunting Forensics		
Application Compatibility Shims Search	2019-05-16	2019-08-14	shims_param_search	Windows	Posture Assessment	Persistence Privilege Escalation	Application Shimming

## Query Catalog

Filters	Reset
<input type="checkbox"/> Organization Queries	
<input type="checkbox"/> Favorite Queries	
Categories	
<input type="checkbox"/> Forensics	
<input type="checkbox"/> Live Acquisition Of Volatile Data	
<input type="checkbox"/> Malware	
<input type="checkbox"/> Posture Assessment	
<input type="checkbox"/> Threat Hunting	
Operating System	
<input type="checkbox"/> Mac	
<input type="checkbox"/> Windows	
ATT&CK™ Tactics	
<input type="checkbox"/> Initial Access	
<input type="checkbox"/> Execution	
<input type="checkbox"/> Persistence	
<input type="checkbox"/> Privilege Escalation	

### Search Catalog



macos

Name	Created	Updated	ID	OS	Category
Active Directory Configuration Monitoring	2021-03-05	2021-08-10	macos_ad_config_monitoring	MacOS	Posture Assessment
Apple System Log (ASL) System Events Monitoring	2021-03-02	2021-08-11	macos_asl_monitoring	MacOS	Posture Assessment Threat Hunting Forensics
Application Layer Firewall (ALF) Monitoring	2019-03-06	2021-08-10	macos_alf_monitoring	MacOS	Posture Assessment
Application Layer Firewall (ALF) Service Exceptions Monitoring	2019-03-06	2021-08-10	macos_alf_exceptions_monitoring	MacOS	Posture Assessment
Application Layer Firewall (ALF) Services Allowed Networks Monitoring	2019-03-27	2021-08-10	macos_alf_explicit_auths_monitoring	MacOS	Posture Assessment
Application Schemes And Handlers Monitoring	2020-03-18	2021-08-11	macos_app_schemes_monitoring	MacOS	Posture Assessment
Application with ACL in the Keychain Monitoring	2021-03-02	2021-08-10	macos_keychain_acls_monitoring	MacOS	Posture Assessment Forensics
Application, System, and Mobile App Crashes Monitoring	2019-11-25	2021-08-10	macos_crashes_monitoring	MacOS	Forensics Threat Hunting
...					

## Application, System, and Mobile App Crashes Monitoring

+ Add to new query

## CREATED

Created by Cisco 2019-11-25 18:09:04. Updated 2021-08-10 22:36:14.

## DESCRIPTION

This query is applicable to MacOS. It retrieves the following data from the MacOS system and application crash logs:

- uid - user ID of the crashed process
- username - user name of the crashed process
- datetime - date/type that the crash occurred
- pid - pid of the crashed process
- thread - thread ID which crashed
- path - path to the crashed process
- crash\_path - location of the log file
- type - type of crash log
- identifier - identifier of the crashed process
- responsible - process responsible for the crashed process
- exception\_type - exception type of the crash
- exception\_codes - exception codes from the crash
- exception\_notes - exception notes from the crash

## ID

macOS\_crashes\_monitoring

## OS

MacOS

## CATEGORIES

Forensics Threat Hunting

## PARAMETERS

username\_pattern:

default: .\* multiple: false nameVal: TEXT

path\_pattern:

default: .\* multiple: false nameVal: TEXT

responsible\_pattern:

default: .\* multiple: false nameVal: TEXT

## SQL

```
SELECT c.uid, u.username, datetime AS "Date Crash Occured", c.pid, c.crashed_thread, c.path, c.crash_path, c.type, c.identifier, c.responsible, c.exception_type, c.exception_codes, c.exception_notes FROM users u CROSS JOIN crashes c USING (uid) WHERE u.username LIKE
regex_match(u.username, (SELECT v FROM __vars WHERE n = "username_pattern"), 0) AND c.path LIKE
regex_match(c.path, (SELECT v FROM __vars WHERE n = "path_pattern"), 0) AND c.responsible LIKE
regex_match(c.responsible, (SELECT v FROM __vars WHERE n = "responsible_pattern"), 0) ORDER BY
datetime DESC;
```

## Query

[New](#)Endpoints [Add host:hostname, IP, MAC, node ID, or AMP Connector GUID](#)

...

[Add Random Endpoints](#)[Clear](#)[Copy Endpoints](#)

### Search Query Catalog

 Catalog query added [Browse](#)Custom SQL *ex. SELECT column\_name FROM table\_name;*

Catalog queries run independently

⊕

[Number](#)

10

[OS](#)

Windows

Mac

[Add](#)[Live Query](#)[Schedule Job](#)

### Application, System, and Mobile App Crashes Monitoring X

```
SELECT c.uid, u.username, datetime AS "Date Crash  
Occured", c.pid, c.crashed_thread, c.path,  
c.crash_path, c.type, c.identifier, c.responsible,  
c.exception_type, c.exception_codes, c.exception_notes  
FROM users u CROSS JOIN crashes c USING (uid) WHERE  
u.username LIKE regex_match(u.username, (SELECT v FROM  
__vars WHERE n = "username_pattern"), 0) AND c.path  
LIKE regex_match(c.path, (SELECT v FROM __vars WHERE n  
= "path_pattern"), 0) AND c.responsible LIKE  
regex_match(c.responsible, (SELECT v FROM __vars WHERE  
n = "responsible_pattern"), 0) ORDER BY datetime DESC;
```

#### PARAMETERS [i](#)

Username Pattern

.\*

Path Pattern

.\*

## Query

New

76 rows from 2 endpoints

View on Jobs page

Download

i

Endpoints Add host:hostname, IP, MAC, node ID, or AMP Connector GUID

host:BRMCMHAO-M-89V2 X

host:S-MacBook-Air-2.local X

...

## Search Query Catalog

Catalog query added

Browse

Custom SQL ex. `SELECT column_name FROM table_name;`

Catalog queries run independently



Live Query



Schedule Job

## Application, System, and Mobile App Crashes Monitoring X

```
SELECT c.uid, u.username, datetime AS "Date Crash Occured", c.pid, c.crashed_thread, c.path, c.crash_path, c.type, c.identifier, c.responsible, c.exception_type, c.exception_codes, c.exception_notes
FROM users u CROSS JOIN crashes c USING (uid) WHERE
u.username LIKE regex_match(u.username, (SELECT v FROM __vars WHERE n = "username_pattern"), 0) AND c.path
LIKE regex_match(c.path, (SELECT v FROM __vars WHERE n = "path_pattern"), 0) AND c.responsible LIKE
regex_match(c.responsible, (SELECT v FROM __vars WHERE n = "responsible_pattern"), 0) ORDER BY datetime DESC;
```

## PARAMETERS i

Username Pattern

\*

Path Pattern

\*

HOSTNAME	BRMCMHAO-M-89V2	▼
ACTIVE IP	142.254.14.242	
NODE ID	J_zBWo--yU73iAwEfOtiXg	
REPORTED	2021-10-20 23:41:07	

HOSTNAME	S-MacBook-Air-2.lo...	▼
ACTIVE IP	142.254.14.242	
NODE ID	CMB2ym-ihx5HU73eUwU...	
REPORTED	2021-10-20 23:41:05	

## Application, System, and Mobile App Crashes Data

uid	username	Date Crash Occured	pid	crashed_thread	path
<b>BRMCMHAO-M-89V2</b>					
501	brmcmaho	2021-10-20 15:40:59.684 -...	91569	0	/Library/ScriptingA
501	brmcmaho	2021-10-20 13:12:57.485 -...	23339	0	/Library/ScriptingA
0	root	2021-10-20 07:52:54.699 -...	84520	6	/usr/sbin/bluetooth
501	brmcmaho	2021-10-20 07:14:05.248 -...	67894	0	/Applications/Xcode
501	brmcmaho	2021-10-19 22:36:52.569 -...	64982	0	/Library/ScriptingA
501	brmcmaho	2021-10-19 13:38:32.152 -...	43124	0	/Applications/Xcode
501	brmcmaho	2021-10-19 08:59:23.008 -...	31710	24	/Users/USER/Library
501	brmcmaho	2021-10-19 07:52:35.379 -...	98353	0	/Applications/Xcode
501	brmcmaho	2021-10-18 13:48:13.627 -...	17287	0	/Library/ScriptingA
501	brmcmaho	2021-10-18 12:23:47.819 -...	76227	0	/Library/ScriptingA
501	brmcmaho	2021-10-18 08:46:49.708 -...	78205	0	/Library/ScriptingA
501	brmcmaho	2021-10-18 08:05:12.106 -...	57938	0	/Applications/Xcode
501	brmcmaho	2021-10-17 16:18:12.352 -...	1532	0	/Applications/Xcode
501	brmcmaho	2021-10-17 15:39:07.768 -...	47757	0	/Library/ScriptingA
501	brmcmaho	2021-10-17 15:06:04.506 -...	39943	0	/Library/ScriptingA
501	brmcmaho	2021-10-17 14:52:53.161 -...	36938	0	/Library/ScriptingA
501	brmcmaho	2021-10-17 02:08:41.816 -...	29386	0	/Applications/Xcode
501	brmcmaho	2021-10-16 12:37:41.523 -...	16559	0	/Applications/Xcode
brmcmaho		2021-10-16 12:01:37.423 -...	6056	0	/Library/ScriptingA



# Example: Threat Hunting with the Query Catalog

- “Hermetic Wiper” malware was identified in February, using signed drivers as a vector. (See <https://blog.talosintelligence.com/2022/02/threat-advisory-hermeticwiper.html> for details.)
- Queries added to the Orbital Catalog to look

Search Catalog

THURSDAY, FEBRUARY 24, 2022

Threat Advisory: HermeticWiper



THREAT ADVISORY

TALOS

THIS POST IS ALSO AVAILABLE IN:

日本語 (Japanese)

Українська (Ukrainian)

Update: March 1, 2022

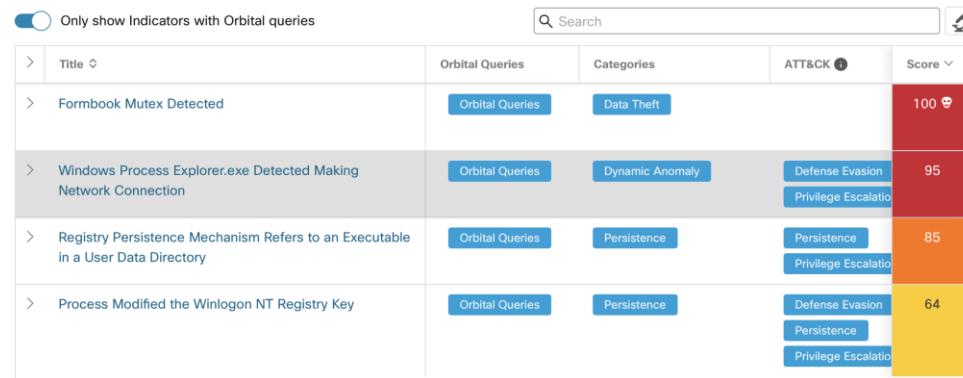
Cisco Talos is aware of reporting related to additional components discovered to be associated with ongoing HermeticWiper attacks. These additional components include:

- HermeticWizard, which allows HermeticWiper to be propagated to and deployed on additional

# Using Secure Malware Analytics as a Query Source

- Cisco Secure Malware Analytics (ex-Threat Grid) produces behavioral indicators (BIs) from samples.
- Some BIs are well suited to turn into Orbital queries.
- Secure Malware Analytics can do this for you in a single click!

## Behavioral Indicators



The screenshot shows a table titled 'Behavioral Indicators' with a search bar and a filter for 'Orbital queries'. The table has columns for Title, Orbital Queries, Categories, ATT&CK, and Score. The rows list various behavioral indicators with their corresponding scores and associated ATT&CK techniques.

Title	Orbital Queries	Categories	ATT&CK	Score
Formbook Mutex Detected	Orbital Queries	Data Theft	Defense Evasion, Privilege Escalation	100
Windows Process Explorer.exe Detected Making Network Connection	Orbital Queries	Dynamic Anomaly	Defense Evasion, Privilege Escalation	95
Registry Persistence Mechanism Refers to an Executable in a User Data Directory	Orbital Queries	Persistence	Persistence, Privilege Escalation	85
Process Modified the Winlogon NT Registry Key	Orbital Queries	Persistence	Defense Evasion, Persistence, Privilege Escalation	64

# Using Secure Malware Analytics as a Query Source

Report / Samples / Ponuda u prilogu.exe

Local Data - United States

Metrics

Metadata

**Indicators**

Network

HTTP Traffic

DNS Traffic

TCP/IP Streams

Extracted Domains

Processes

Artifacts

Registry Activity

Consolidated

Created Keys

Modified Keys

Deleted Keys

Only show Indicators with Orbital queries

Report FP/FN  Resub

Search

Title	Orbital Queries	Categories	ATT&CK	Score
Formbook Mutex Detected				
Score: 100 💀 Hits: 1				
Description				
Formbook is a data stealing malware. This threat is capable of key logging, making screenshots, clipboard monitoring, and grabbing passwords and network requests. Communication with command and control server can lead to additional infections and sensitive data exfiltration.				
Trigger				
This indicator triggers when a mutant known to be associated with Formbook is detected.				
Process	Process Name	Mutant Name	Actions	
Process 57	raserver.exe	8-3503835S2BFHHZ	<input type="button"/> Orbital Query	

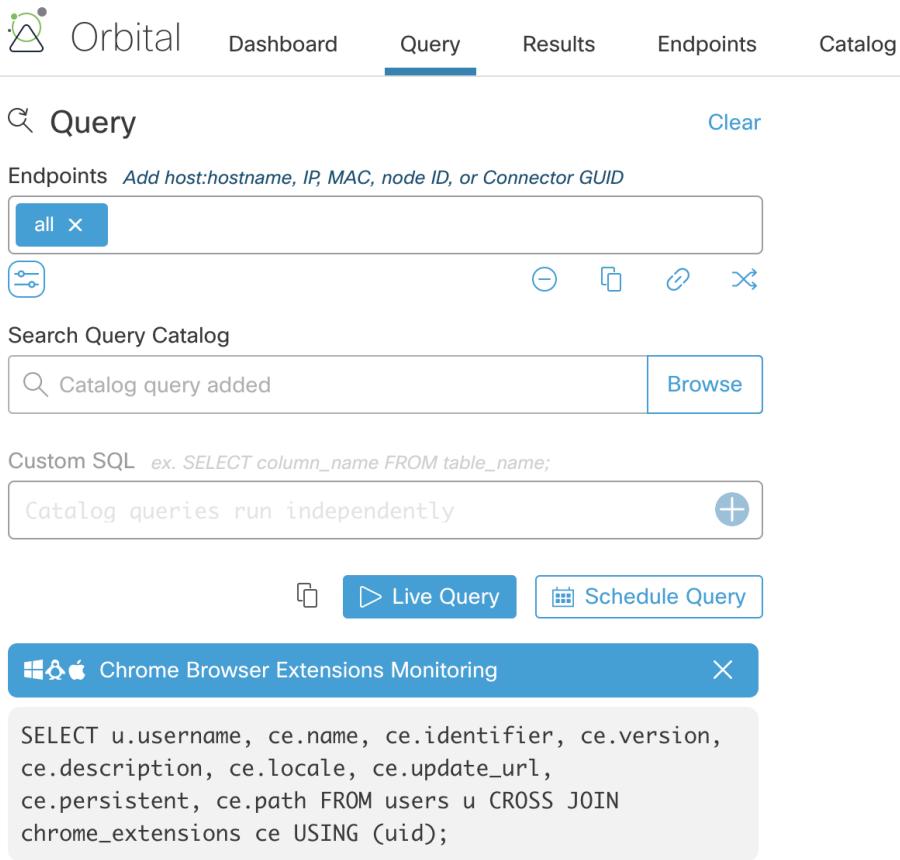
- Just click the “Orbital Query” button on the BI of interest.

# Using Secure Malware Analytics as a Query Source

- An Orbital query is automatically set up with all the fields populated, and ready to run.
- Pick your targets, and run the query to find out if the observed BI is present elsewhere inside your organization.

The screenshot shows the Secure Malware Analytics query interface. At the top, there is a search bar labeled 'Query' with 'Endpoints' and 'Add host:hostname, IP, MAC, node ID, or Connector GUID' placeholder text. To the right are 'Clear' and 'Reset' buttons. Below the search bar is an 'Operating System Filter' section with checkboxes for 'Windows endpoints' (checked), 'Mac endpoints', and 'Linux endpoints'. A 'Browse' button is located to the right of this section. The main query area is titled 'Custom SQL' with the placeholder 'ex. SELECT column\_name FROM table\_name;'. Below this is a text box containing the query: 'Catalog queries run independently'. At the bottom of the interface are three buttons: a clipboard icon, a 'Live Query' button (which is blue and highlighted), and a 'Schedule Query' button. A separate window titled 'Process Mutex Search' shows the query: 'SELECT object\_name FROM winbaseobj WHERE object\_type="Mutant" AND object\_name LIKE (SELECT v FROM \_\_vars WHERE n="mutex"));'. Below this is a 'PARAMETERS' section with a 'Mutex' parameter set to '8-3503835SZBFHHZ'.

# Running a Search: Scheduled, Event-Driven, On-Demand



The screenshot shows the Orbital interface with the 'Query' tab selected. The search bar at the top contains the text 'Chrome Browser Extensions Monitoring'. Below the search bar, there is a section for 'Endpoints' with a placeholder 'Add host:hostname, IP, MAC, node ID, or Connector GUID'. A 'Catalog' section shows a query named 'Catalog query added' with a 'Browse' button. A 'Custom SQL' section contains the following code:

```
SELECT u.username, ce.name, ce.identifier, ce.version, ce.description, ce.locale, ce.update_url, ce.persistent, ce.path FROM users u CROSS JOIN chrome_extensions ce USING (uid);
```

Here, we have selected the “Chrome Browser Extensions Monitoring” catalog entry, which is applicable across multiple platforms.

So we could just select “all” endpoints as our target, and let it run like that.

We could also enter specific endpoints as the target of the search, by IP or MAC address, hostname, connector GUID, etc.

## Query

Clear

Endpoints *Add host:hostname, IP, MAC, node ID, or Connector GUID*

### Operating System Filter

 Catalog query added

Browse

Custom SQL *ex. SELECT column\_name FROM table\_name;*

Catalog queries run independently



Live Query

Schedule Query

### Chrome Browser Extensions Monitoring



```
SELECT u.username, ce.name, ce.identifier, ce.version,
ce.description, ce.locale, ce.update_url,
ce.persistent, ce.path FROM users u CROSS JOIN
chrome_extensions ce USING (uid);
```

Or, if we're interested in one specific operating system, we could specify that.

## Query

Endpoints *Add host:hostname, IP, MAC, node ID,*

### Operating System Filter

Windows endpoints  
 Mac endpoints  
 Linux endpoints



## Query

[Clear](#)Endpoints [Add host:hostname, IP, MAC, node ID, or Connector GUID](#) 

### Search Query Catalog

[Add Random Endpoints](#) Catalog query added[Browse](#)Custom SQL *ex. SELECT column\_name FROM table\_name;*

Catalog queries run independently

[Live Query](#) [Schedule Query](#)

### Chrome Browser Extensions Monitoring

```
SELECT u.username, ce.name, ce.identifier, ce.version,
ce.description, ce.locale, ce.update_url,
ce.persistent, ce.path FROM users u CROSS JOIN
chrome_extensions ce USING (uid);
```

Or, we can add a random subset of endpoints, if we want to get a statistical sampling of our environment.

The random endpoints can also be limited by operating system.

### Add Random Endpoints

#### Number

#### os

- Windows
- Mac
- Linux

[Add](#)



## Query

[Clear](#)Endpoints [Add host:hostname, IP, MAC, node ID, or Connector GUID](#)



Search Query Catalog

Catalog query added [Bro](#)

Custom SQL ex. SELECT column\_name FROM table\_name;

Catalog queries run independently

[Live Query](#)

### Chrome Browser Extensions Monitoring

```
SELECT u.username, ce.name, ce.identifier, ce.version, ce.description, ce.locale, ce.update_url, ce.persistent, ce.path FROM users u CROSS JOIN chrome_extensions ce USING (uid);
```

#### Link Queries

- Job 2022-02-09 01:55:08
- Live Query 2021-12-18 00:01:12
- Live Query 2021-12-17 23:18:05
- Live Query 2021-12-17 23:07:02
- Live Query 2021-12-17 22:36:59
- Live Query 2021-12-17 22:33:42
- Live Query 2021-12-17 22:16:20
- Job 2021-11-19 22:18:11
- Live Query 2021-11-04 03:17:55

[Add](#)

“Linked Queries” allow you to use the results of one query to target another. Only endpoints that return a *non-empty* result for the first query are eligible for the second.

This lets you focus potentially resource-intensive threat hunting queries on only those nodes that are actually of interest for the hunt.

## Query

Clear

Endpoints [Add host:hostname, IP, MAC, node ID, or Connector GUID](#)

host:BRMCMAHO-M-89V2 



Search Query Catalog

 Catalog query added

[Browse](#)

Custom SQL *ex. SELECT column\_name FROM table\_name;*

Catalog queries run independently



 [Live Query](#)

 [Schedule Query](#)

In many threat hunting and incident response scenarios, you'll want to run your queries, and process the results, immediately.

That's what the "Live Query" button is there for.

## Schedule Orbital Query

X

### Query Name

Query 2022-06-13 07:20:05

25/1000

Schedule every

for

*1 result set per endpoint possible  
pending node availability.*

Run Once

### Remote Data Store

None

[Add Remote Data Store](#)



Go to Result

Schedule

Cancel

For compliance, base-lining, and verification purposes, you may want to run queries on a regular schedule.

They can run on a time cadence (from 5 minutes to 30 days) over a period of up to two years.

A Remote Data Store is useful for offline long-term

☐ ▼ Apple Brian's iMac in group Family Systems ✓ Definitions Up To Date 

Hostname	Brian's iMac	Group	 Family Systems
Operating System	OS X 12.4.0	Policy	 Home and Family Mac Protect
Connector Version	1.16.0.841	Internal IP	172.16.1.1 
Install Date	2021-09-01 22:06:35 PDT	External IP	142.16.12.12 
Connector GUID	0a66d064-5ca0-418c-bb32-d9a82c37d972	Last Seen	2022-06-13 00:27:52 PDT
Definition Version	ClamAV (osx.cvd: 1189)	Definitions Last Updated	2022-06-12 05:34:44 PDT
Update Server	clam-defs.amp.cisco.com		
Mac Hardware ID	c3de448f-aec8-5d5a-ae5d-f99a91c04d44		

Cisco Secure Endpoint (Advantage license or higher) also incorporates a very useful special kind of Orbital query: the Forensic Snapshot. This is a predefined set of information about the state of the operating system that can be captured at a point in time, referenced in the Device Trajectory, and downloaded for further analysis.

# Using Orbital with SecureX Orchestration



Search activities



## CORE

Calculate Date

Calculate Date Time Difference

Convert Json to Xml

Convert Xml to Json

Escape Regex Metacharacters

Find String

Format Date

JSONPath Query

Match Regex

Parse Date

Replace String

Set Variables

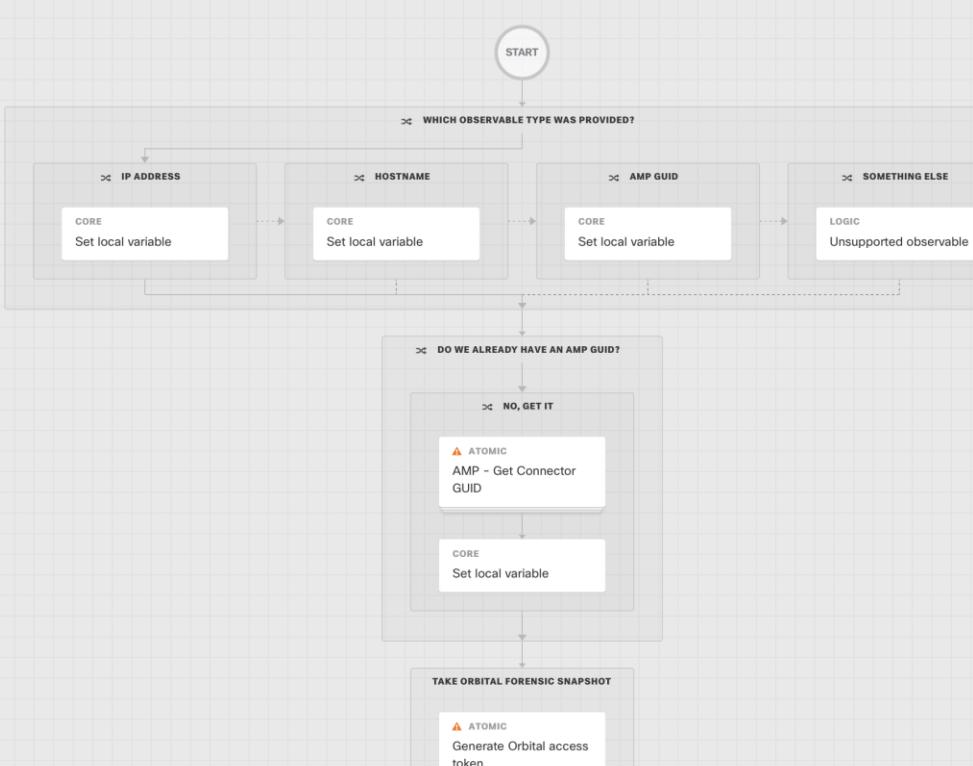
Sleep

Split String

Substring



0



## PROPERTIES

Take Forensic Snapshot And Isolate

## Version

## Git Repository

Github\_Target\_Workflows



## Git Version

initial commit -6/29/2020, 12:20:04 AM ⓘ

[Load New Version](#)

## General

## Display Name

Take Forensic Snapshot and Isolate

## Owner

brmcmaho@cisco.com

## Description

[Executes an Orbital forensic snapshot and enables AMP host isolation]  
[Supported observables: IP address, hostname, AMP GUID]

## Workflow Description:

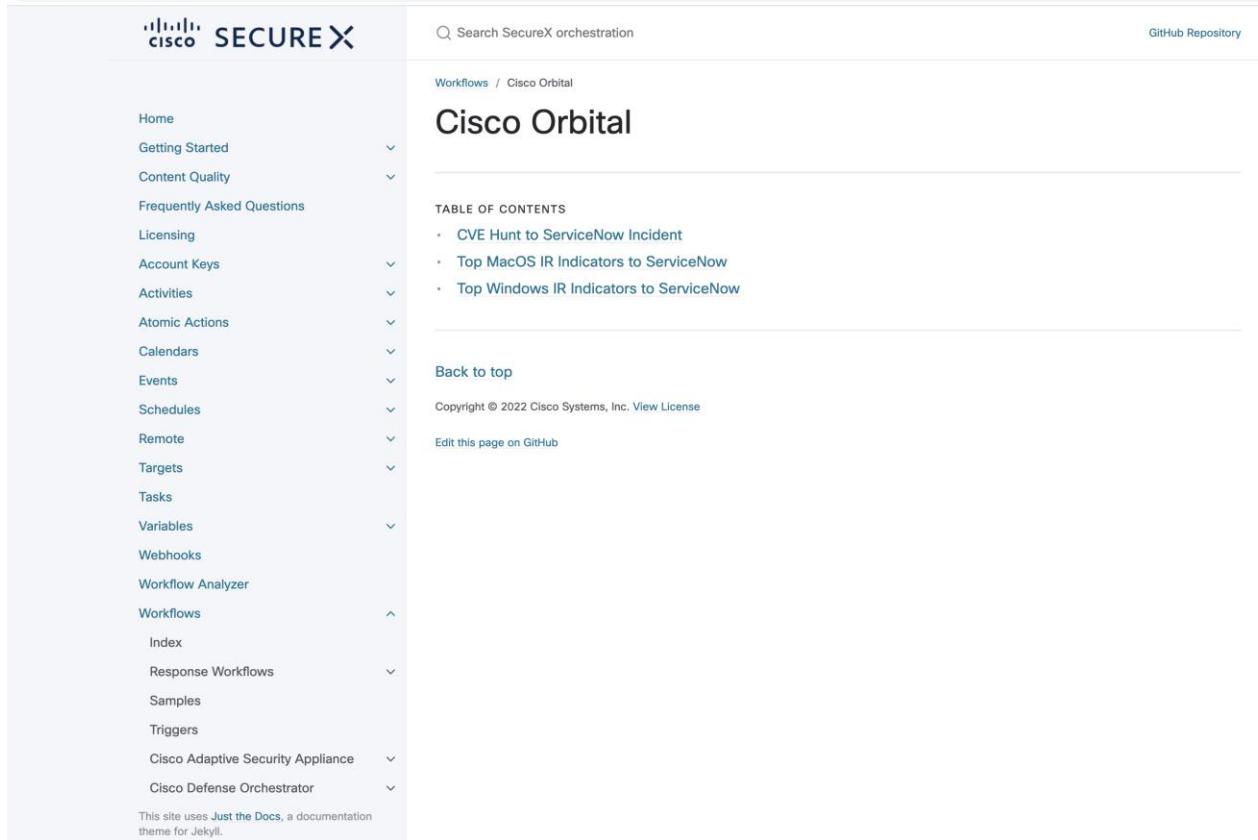
 Clean up after successful execution Is atomic workflow

## Group Name ⓘ

Select

# Orbital Workflows in SecureX Orchestration

ciscosecurity.github.io/sxo-05-security-workflows/workflows/orbital/



The screenshot shows a documentation page for Cisco Orbital Workflows. The left sidebar contains a navigation menu with sections like Home, Getting Started, Content Quality, Frequently Asked Questions, Licensing, Account Keys, Activities, Atomic Actions, Calendars, Events, Schedules, Remote, Targets, Tasks, Variables, Webhooks, Workflow Analyzer, Workflows (which is the current section), Index, Response Workflows, Samples, Triggers, Cisco Adaptive Security Appliance, and Cisco Defense Orchestrator. The main content area has a search bar, a GitHub Repository link, and a breadcrumb navigation path: Workflows / Cisco Orbital. The title is "Cisco Orbital". Below the title is a "TABLE OF CONTENTS" section with three items: "CVE Hunt to ServiceNow Incident", "Top MacOS IR Indicators to ServiceNow", and "Top Windows IR Indicators to ServiceNow". At the bottom of the page are links for "Back to top", "Copyright © 2022 Cisco Systems, Inc. View License", and "Edit this page on GitHub". A note at the bottom states: "This site uses Just the Docs, a documentation theme for Jekyll."

# Orbital Workflows in SecureX Orchestration

Workflows / Cisco Orbital / CVE Hunt to ServiceNow Incident

## CVE Hunt to ServiceNow Incident

WORKFLOW #0009

This workflow uses Cisco Orbital to look for endpoints that are vulnerable for a given CVE. For demonstration purposes we use CVE-2020-0796 which has been added to Orbital as a catalog query. After the Orbital query is executed, we open a ServiceNow incident with the results.

Overview

[GitHub](#)

### Change Log

Date	Notes
Nov 24, 2020	- Initial release
Sep 10, 2021	- Updated to use the new <code>system atomics</code>

See the [Important Notes](#) page for more information about updating workflows

### Requirements

- The following `system atomics` are used by this workflow:
  - Orbital - Query All Endpoints
  - Threat Response - Generate Access Token
- The following atomic actions must be imported before you can import this workflow:
  - ServiceNow - Create Incident ([CiscoSecurity\\_Atomics](#))

# Talos Queries on Github

github.com/Cisco-Talos/osquery\_queries

Product Team Enterprise Explore Marketplace Pricing

Search Sign in Sign up

Cisco-Talos / osquery\_queries Public

Code Issues Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Code

	linux_attacks	Add vulnerability queries
	linux_forensics	All remaining quote fixes
	linux_malware	add recursive %
	macos_attacks	added new packs
	macos_forensics	added new packs
	macos_malware	Fixed Quotation
	packs	New Query: Whiterabbit Ransomware Ransom Note
	win_attacks	Add potential queries
	win_forensics	New queries: MuddyWater Part 2
	win_malware	New Query: Whiterabbit Ransomware Ransom Note
	LICENSE-GPL-2.0	add win_malware pack
	LICENSE.md	LICENSE fix
	README.md	updates

README.md

## Cisco Talos Osquery queries

About

Cisco Orbital - Osquery queries by Talos

Readme View license 68 stars 23 watching 22 forks

Releases

No releases published

Packages

No packages published

Contributors 4

SecsAndCyber Matthew Molyett

jospalme

cmarczewski Christopher Marczewski

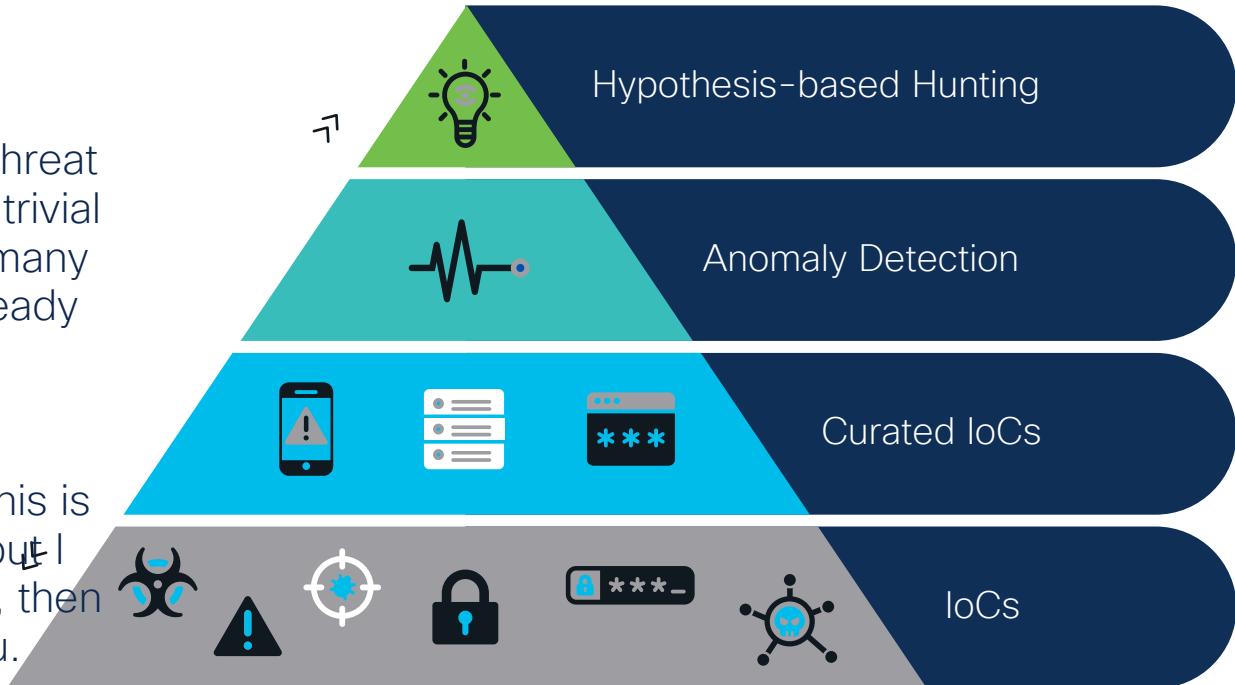
dkorzhev Dmytro Korzhev

# Oh, and one more thing...

Building out an in-house threat hunting capability is not a trivial task, especially when so many security operators are already struggling to keep up.



If your response to all of this is “yeah, that sounds cool, but I don’t have the time for it”, then we have a solution for you.



## Certutil.exe Executed by Schtasks.exe (Demo Data)

 1 Compromise Observed 0 1 Require Attention 0 0 In Progress 0 0 Resolved

## Overview

Incident Started at 	2022-06-13 05:08:42 PDT
Incident Discovered on 	2022-06-13 05:14:09 PDT
MITRE   ATT&CK'	<b>Tactics</b> TA0005: Defense Evasion TA0002: Execution TA0001: Initial Access TA0003: Persistence T1059: Command and Scripting Interpreter T1202: Indirect Command Execution <b>Techniques</b> T1027: Obfuscated Files or Information T1053: Scheduled Task/Job T1204: User Execution T1546: Event Triggered Execution T1566: Phishing
Summary	<p>The affected host executed schtasks.exe to schedule the launch of certutil.exe. The surrounding data of this hunt lead are as follows:</p> <ul style="list-style-type: none"> <li>The user opened a malicious Word document from a phishing email</li> <li>The Word document dropped two VBScripts</li> <li>Word created a scheduled task to launch certutil.exe, which is unusual for parent-child relationships</li> <li>Word executes one of the VBScripts it had dropped earlier using WMIC. (AMP detects launching of WScript by Word)</li> <li>WScript runs reconnaissance commands to discover the network information, domain controller list etc. and stores data in recon.txt</li> <li>WScript creates an archive called sweetz.cab of stolen data using makecab utility</li> <li>WScript uploads that cab file to a suspicious FTP server</li> <li>WScript starts collecting sensitive information such as passwords in a file called goodies.txt</li> <li>WScript makes an archive and uploads it via FTP</li> <li>Certutil.exe executes via the earlier scheduled task, due to COM hijacking, it launches a PowerShell script (simply shows a dialog box demonstrating arbitrary code execution)</li> </ul>
Remediation	<p>We recommend the following:</p> <ul style="list-style-type: none"> <li>Isolation of the affected hosts from the network</li> <li>Perform forensic investigation           <ul style="list-style-type: none"> <li>Review all activity performed by host users</li> <li>Review all activities of affected hosts</li> <li>Upload all files found under the following folders to ThreatGrid for analysis, then delete all malicious files</li> </ul> </li> </ul>

# Conclusion

This board

Search Security Blogs



Technology &amp; Support



For Partners



Customer Connection



Webex



Events



Members &amp; Recognition

[Cisco Community](#) / [Technology and Support](#) / [Security](#) / [Security Blogs](#) / [Orbital Query Corner - Update](#)

## Orbital Query Corner - Update

[AMP for Endpoints](#)[Endpoint Security](#)[Orbital Advanced Search](#)

1606



15



2

VIEWS

HELPFUL

COMMENTS

Ask a Question

Create

[+ Discussion](#) [+ Blog](#) [+ Document](#)[+ Event](#) [+ Video](#) [+ Project Story](#)

brmcmaho Cisco Employee

07-28-2021 09:43 AM

"What is this 'Orbital Query Corner' thing", you ask? It's the name of an occasional series of articles, each discussing one particular point or use case for the Orbital advanced search feature that is available in Cisco Secure Endpoint starting at the Advantage level.

The idea behind this series is that, while Orbital is a tremendously powerful tool, it may seem like a daunting thing to get to know, especially if you don't happen to be a guru-level expert in both SQL-style queries and Windows internals. These documents are intended to explore ways to use the power of Orbital in small bite-sized pieces; sometimes the topic will be driven by current events, and sometimes the theme will be a bit more general, but always kept short and informal.

### Find more resources

- [Discussions](#)
- [Videos](#)
- [Blogs](#)
- [Project Gallery](#)
- [Documents](#)
- [Events](#)
- [New Community Member Guide](#)

# Resources

- FAQ  
<https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/amp-endpoints-faq.html>
- Privacy Data Sheet  
[https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search\\_keyword=orbital](https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=orbital)
- Cisco Orbital Help  
<https://orbital.amp.cisco.com/help/>
- Cisco Community  
<https://community.cisco.com/t5/endpoint-security/bd-p/discussions-endpoint-security>
- Orbital Tutorial Videos  
<https://learningnetwork.cisco.com/s/orbital-advanced-search-how-to-videos>

# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](http://www.cisco.com/go/certs)

## Learn



### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train



### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify



### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

### Cisco Guided Study Groups

180-day certification prep program with learning and support

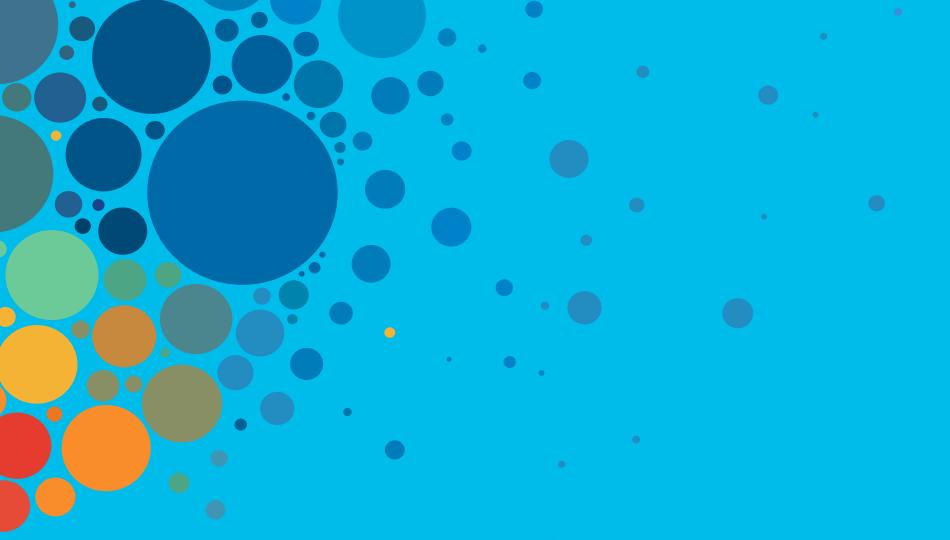
### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](http://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

ALL IN

#CiscoLive