
cisco Live!
ALL IN

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

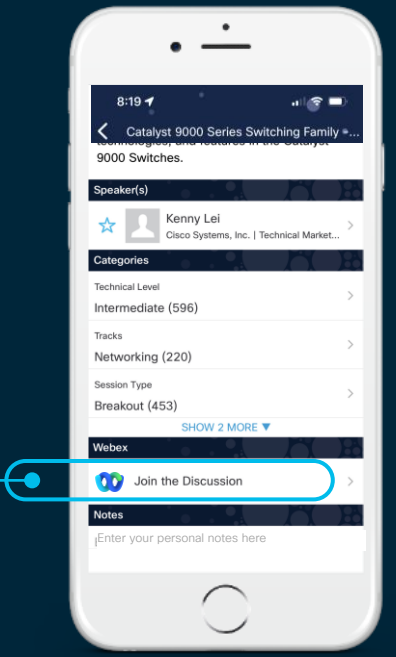
Cisco Webex App

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



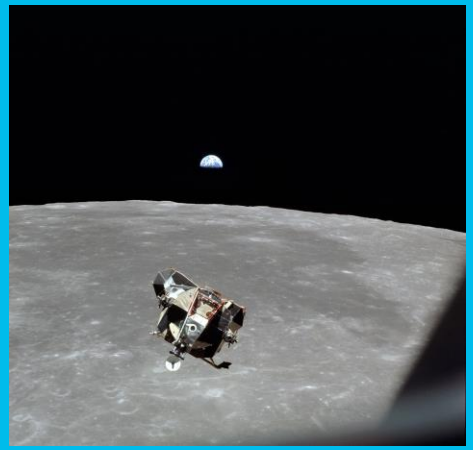
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1016

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?

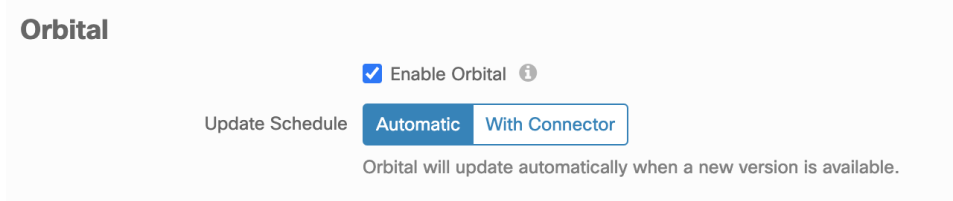
- Use case: Threat Hunting
  - Hypothesis-driven hunting
  - Malware Analytics searches
- Use case: Incident Response
  - Forensic snapshots
  - ATT&CK framework
- Use case: IT Operations
  - Not just for SecOps
- Use case: Vulnerability Management and Compliance
  - Remediate, but verify

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?

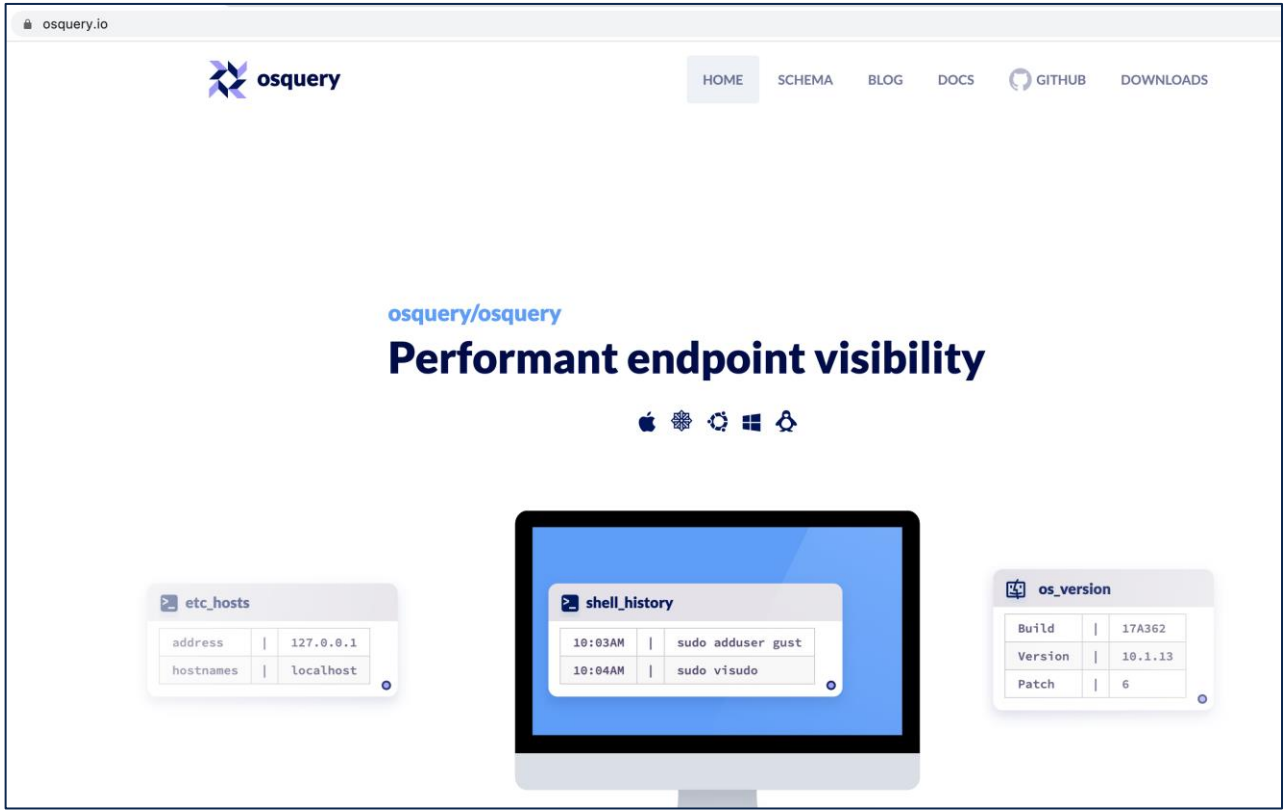
- Secure Endpoint version requirements:
  - Windows connector 7.1.5 +
  - macOS connector 1.16.0 +
  - Linux connector 1.17.0 +
- Orbital √ Enabled under Advanced Settings in Policy



- 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



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

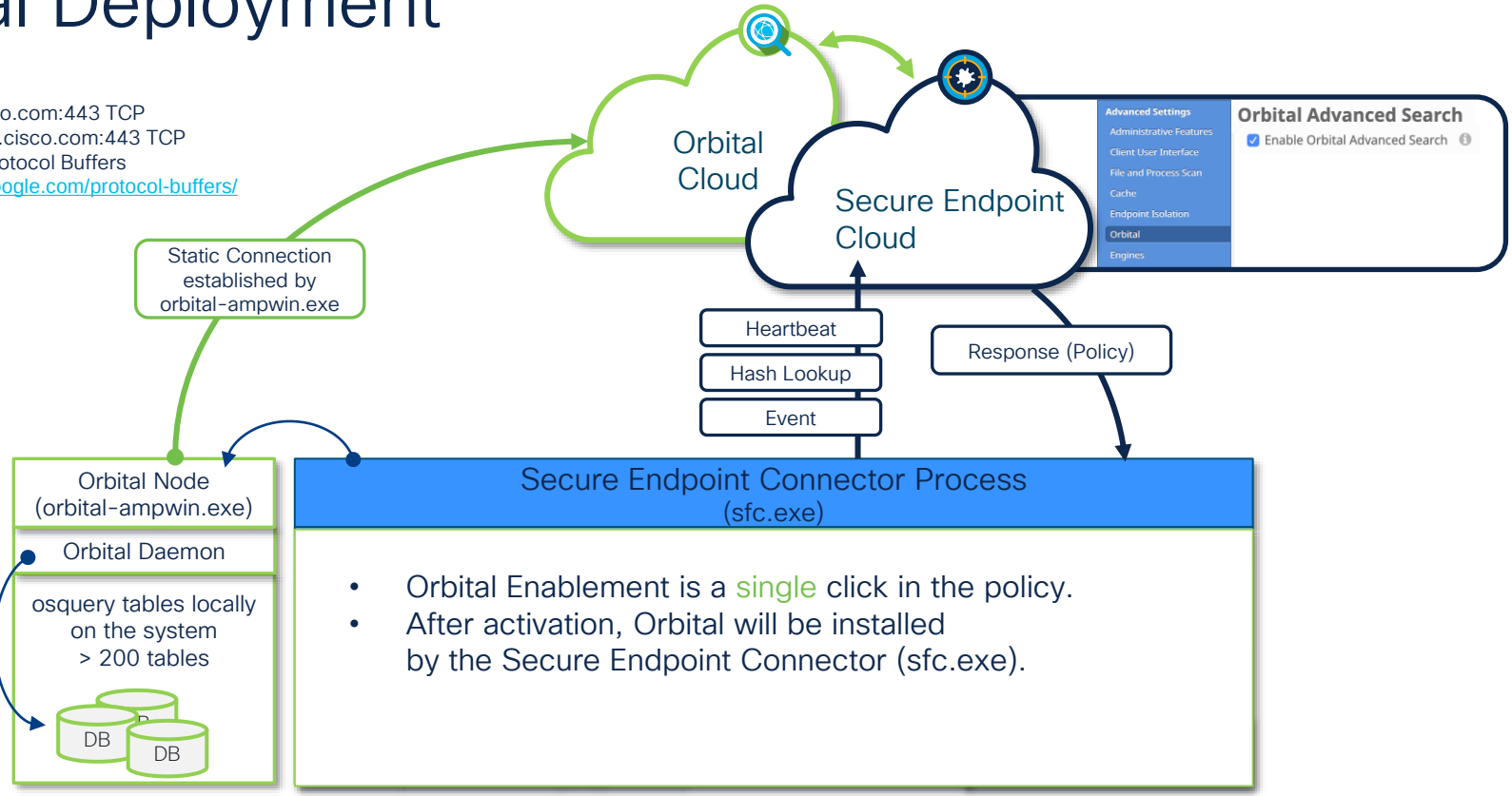
Okay … so, why pay for Orbital if osquery is free? (Part 2)

- 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

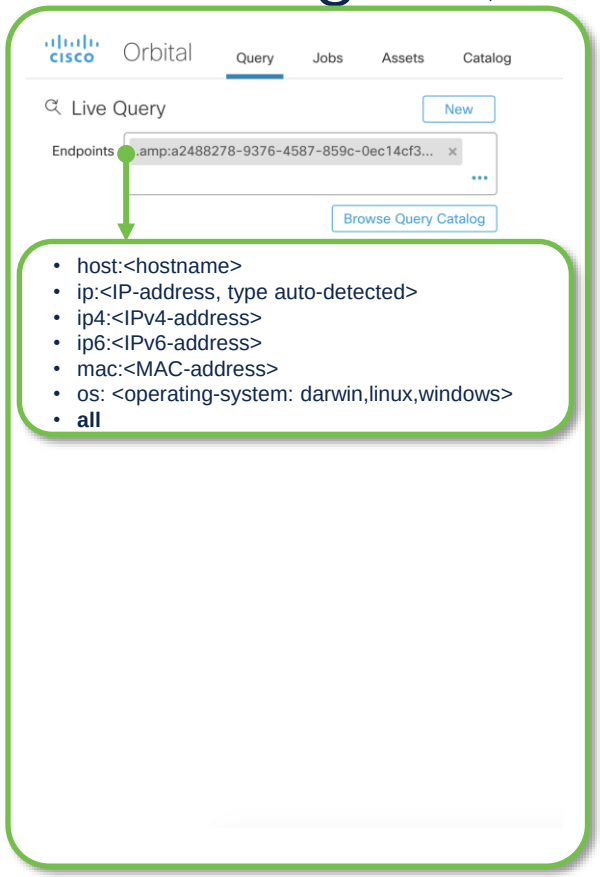
Orbital Deployment

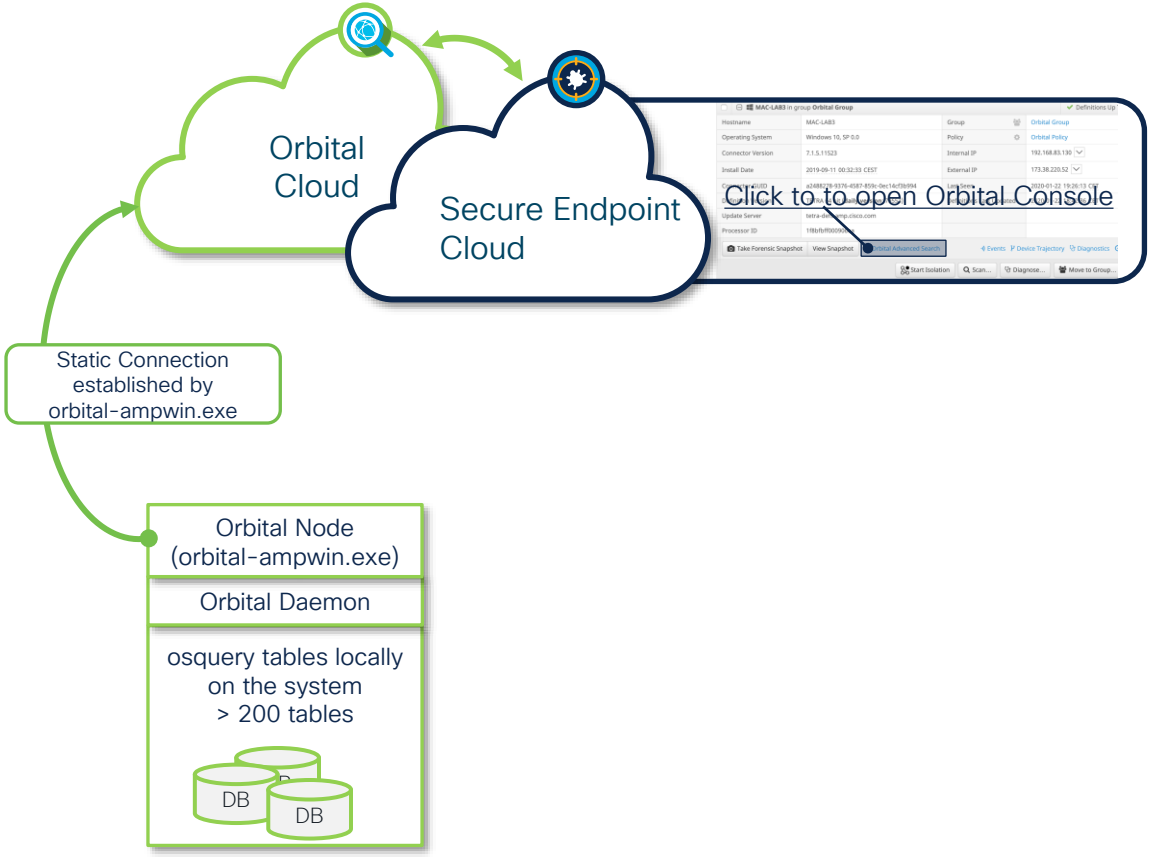
- orbital[.eu].amp.cisco.com:443 TCP
- ncp[.eu].orbital.amp.cisco.com:443 TCP
- Based on Google Protocol Buffers
  https://developers.google.com/protocol-buffers/



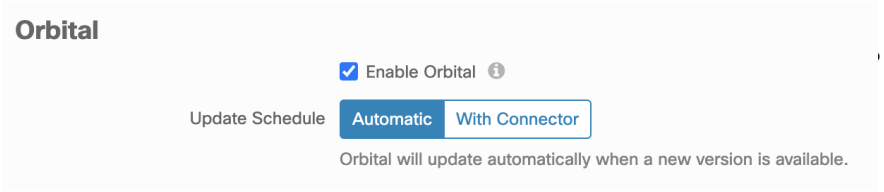
- Orbital daemon constantly adds information to the Orbital Databases

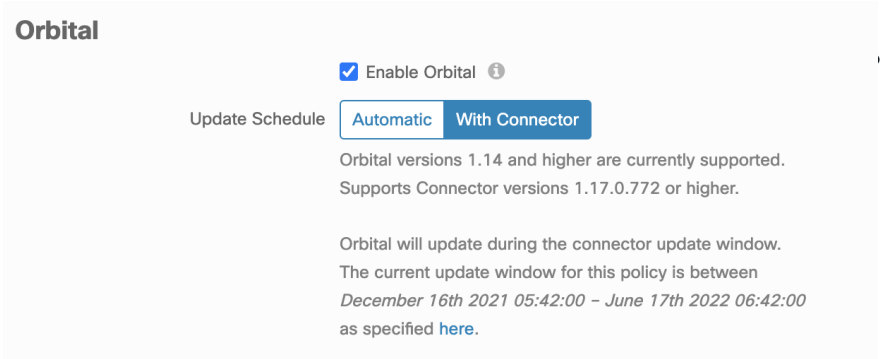
Running a Query





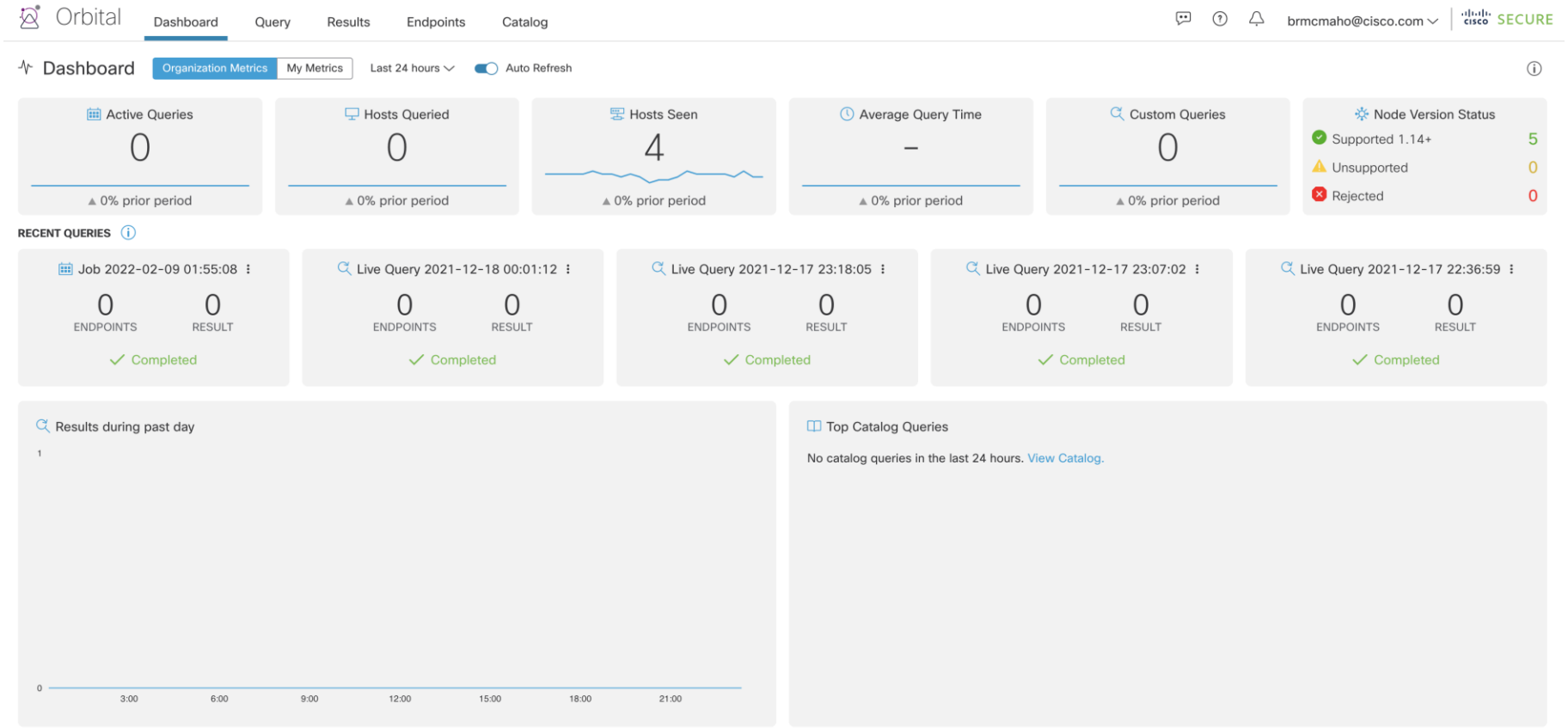
Orbital Updates on the Endpoint



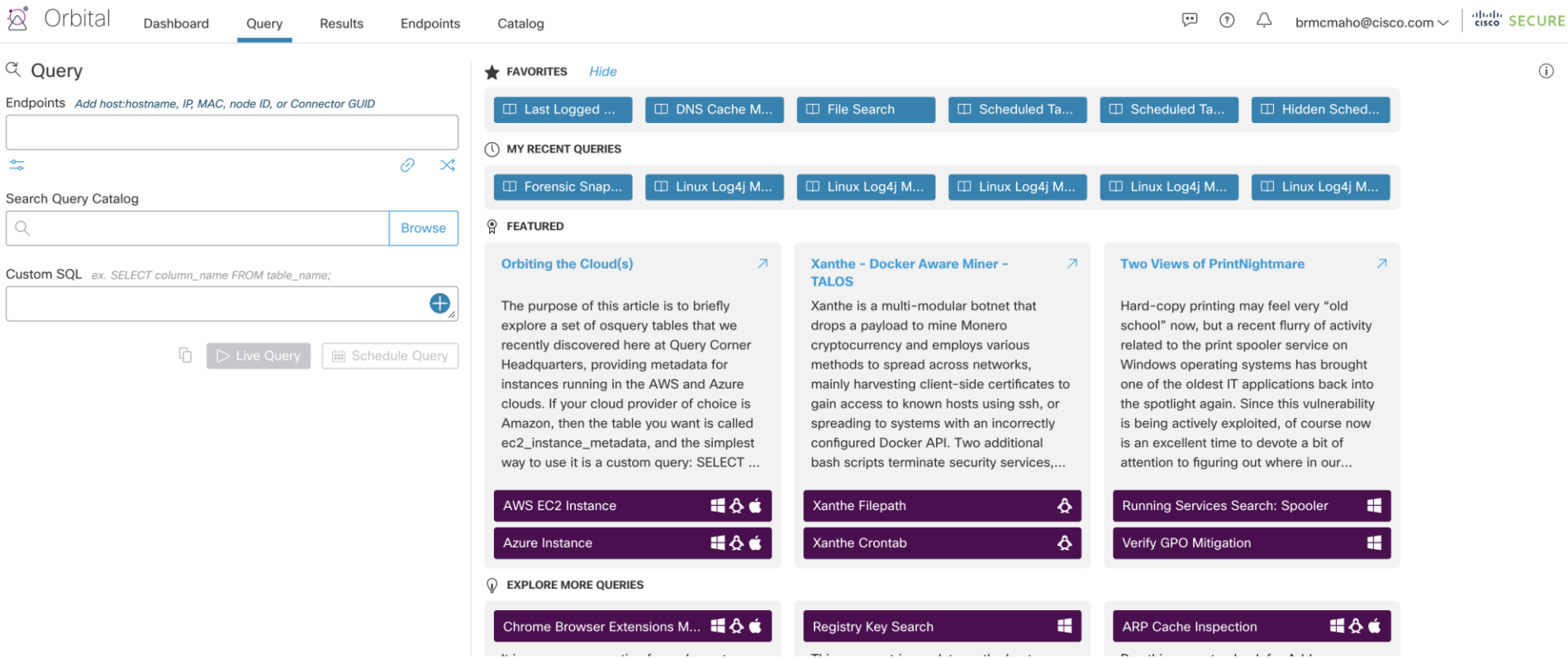


- Orbital updates are released every two weeks or so.
- With “Automatic” selected as your update schedule, the endpoints will apply the updates when they become available.
- If you need to exercise more control over your endpoint updates, choose “With Connector” instead; Orbital on the endpoints will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

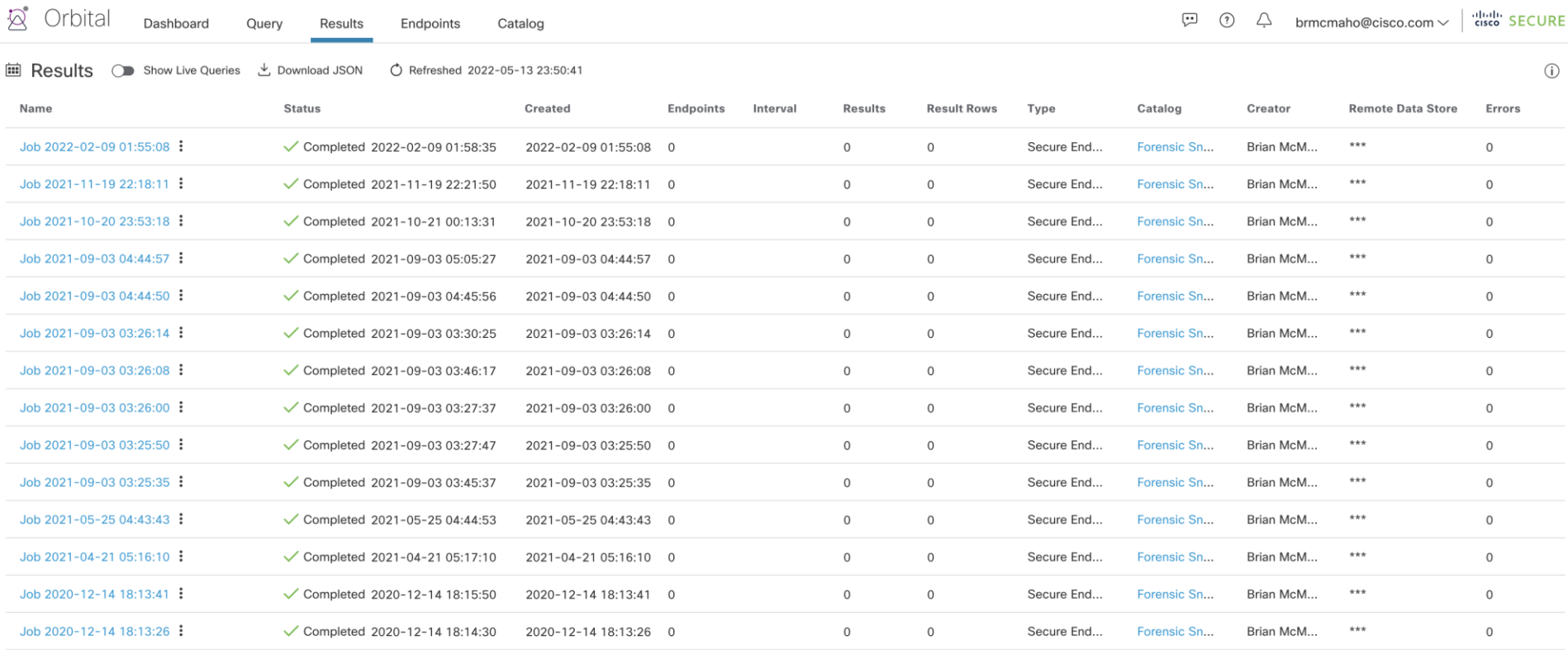
Orbital Cloud Console: Dashboard



Orbital Cloud Console: Query

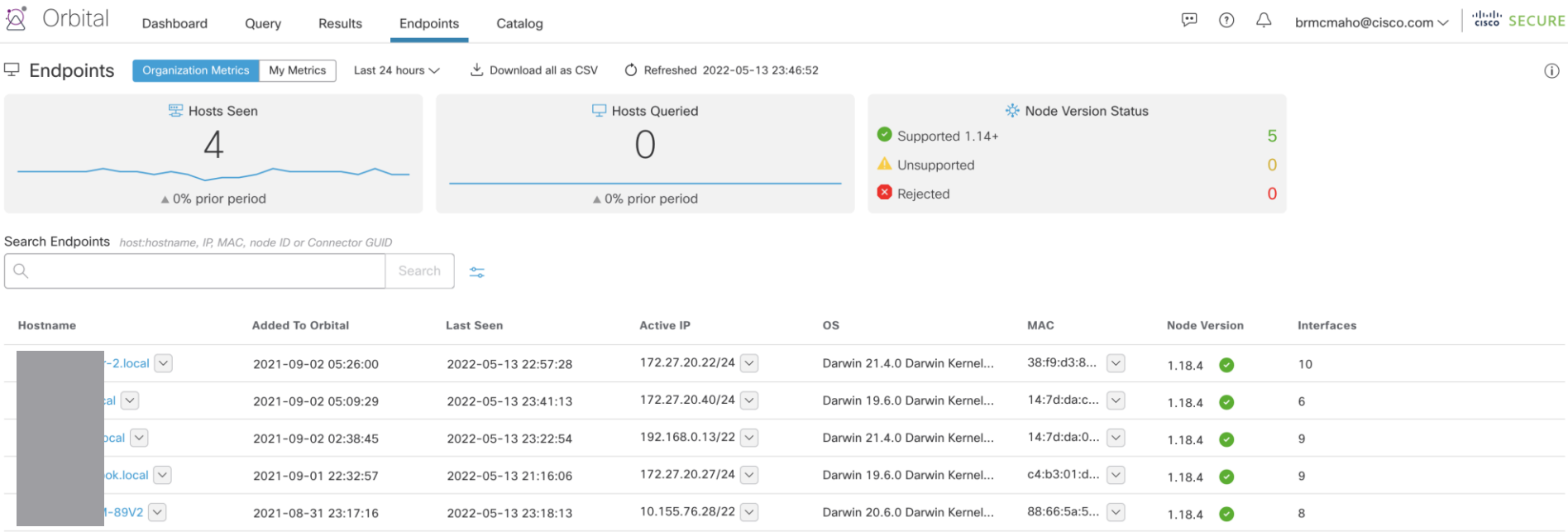


Orbital Cloud Console: Results

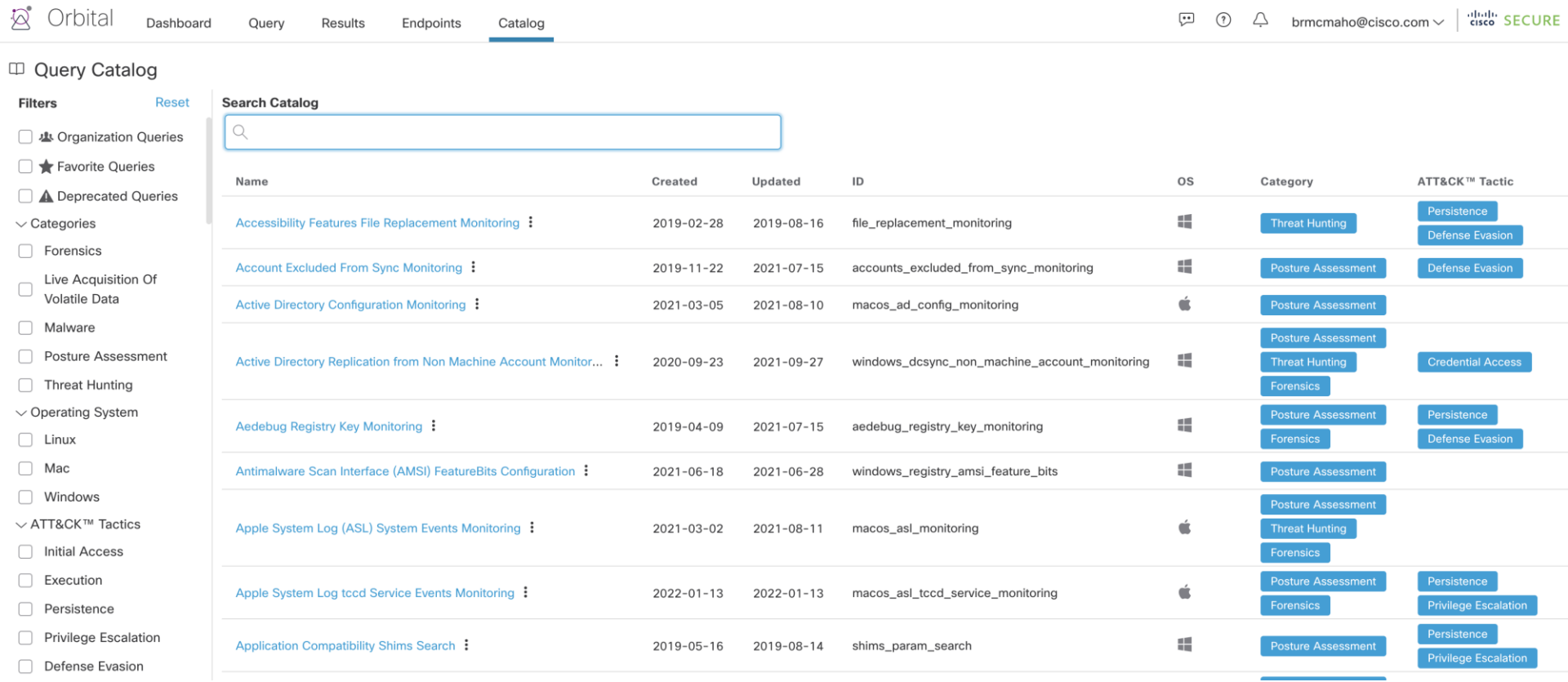


Name	Status	Created	Endpoints	Interval	Results	Result Rows	Type	Catalog	Creator	Remote Data Store	Errors
Job 2022-02-09 01:55:08	Completed 2022-02-09 01:58:35	2022-02-09 01:55:08	0		0	0	Secure End...	Forensic Sn...	Brian McM...	***	0
Job 2021-11-19 22:18:11	Completed 2021-11-19 22:21:50	2021-11-19 22:18:11	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

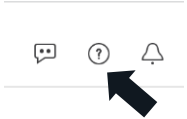
Orbital Cloud Console: Endpoints



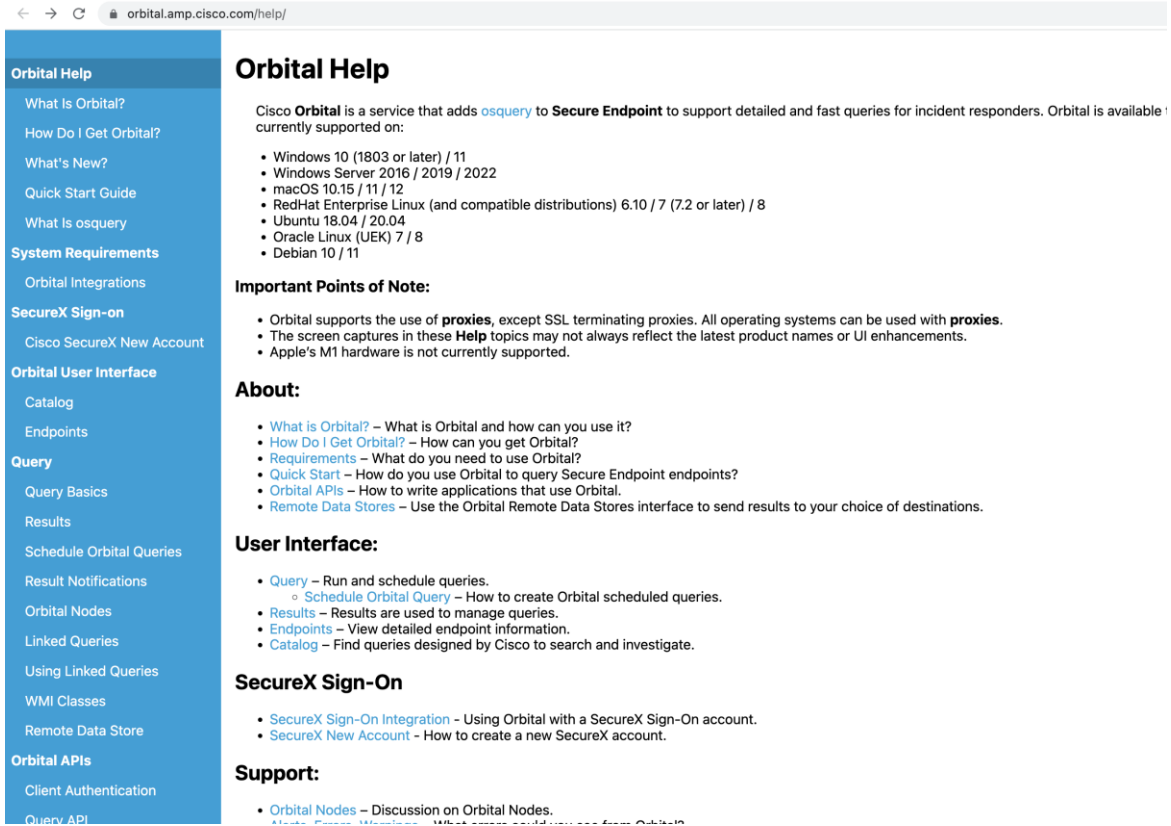
Orbital Cloud Console: Catalog



Orbital Cloud Console: Help



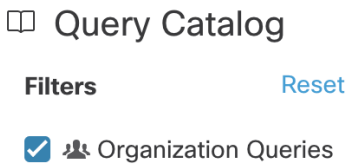
- The “?” icon takes you to online help.
- You can also browse directly to: https://orbital.amp.cisco.com/help/
- This is also where the Orbital release notes are kept, under “What’s New?”

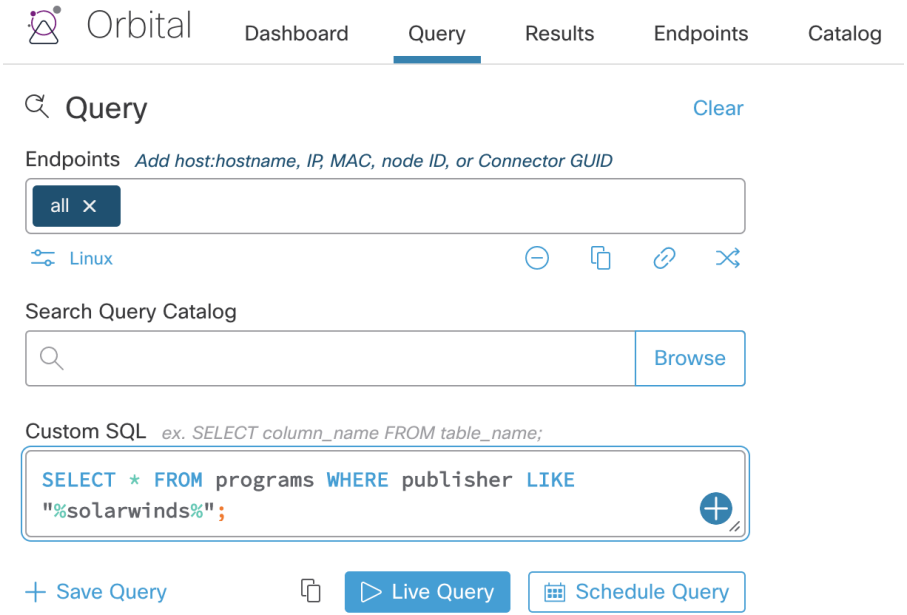


Searches: Building, Borrowing, Stealing

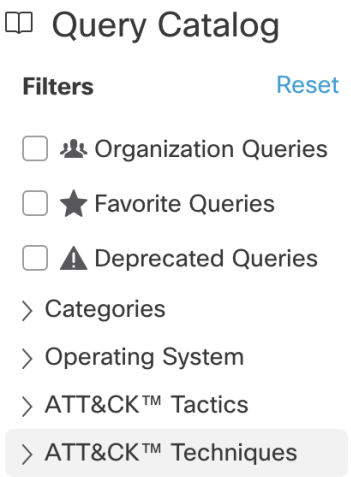
Orbital Search DIY (Do It Yourself)

- 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.





A Closer Look at the Query Catalog



- 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&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

< 1 2 3 4 ... 14 15 >

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&CK™ Tactics
- [ ] Initial Access
- [ ] Execution
- [ ] Persistence
- [ ] 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 Mo...	2019-03-06	2021-08-10	macos_alf_exceptions_monitoring	MacOS	Posture Assessment
Application Layer Firewall (ALF) Services Allowed Netw...	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 Craches Monitoring	2019-11-25	2021-08-10	macos_crashes_monitoring	MacOS	Forensics, Threat Hunting

Application, System, and Mobile App Craches Monitoring

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

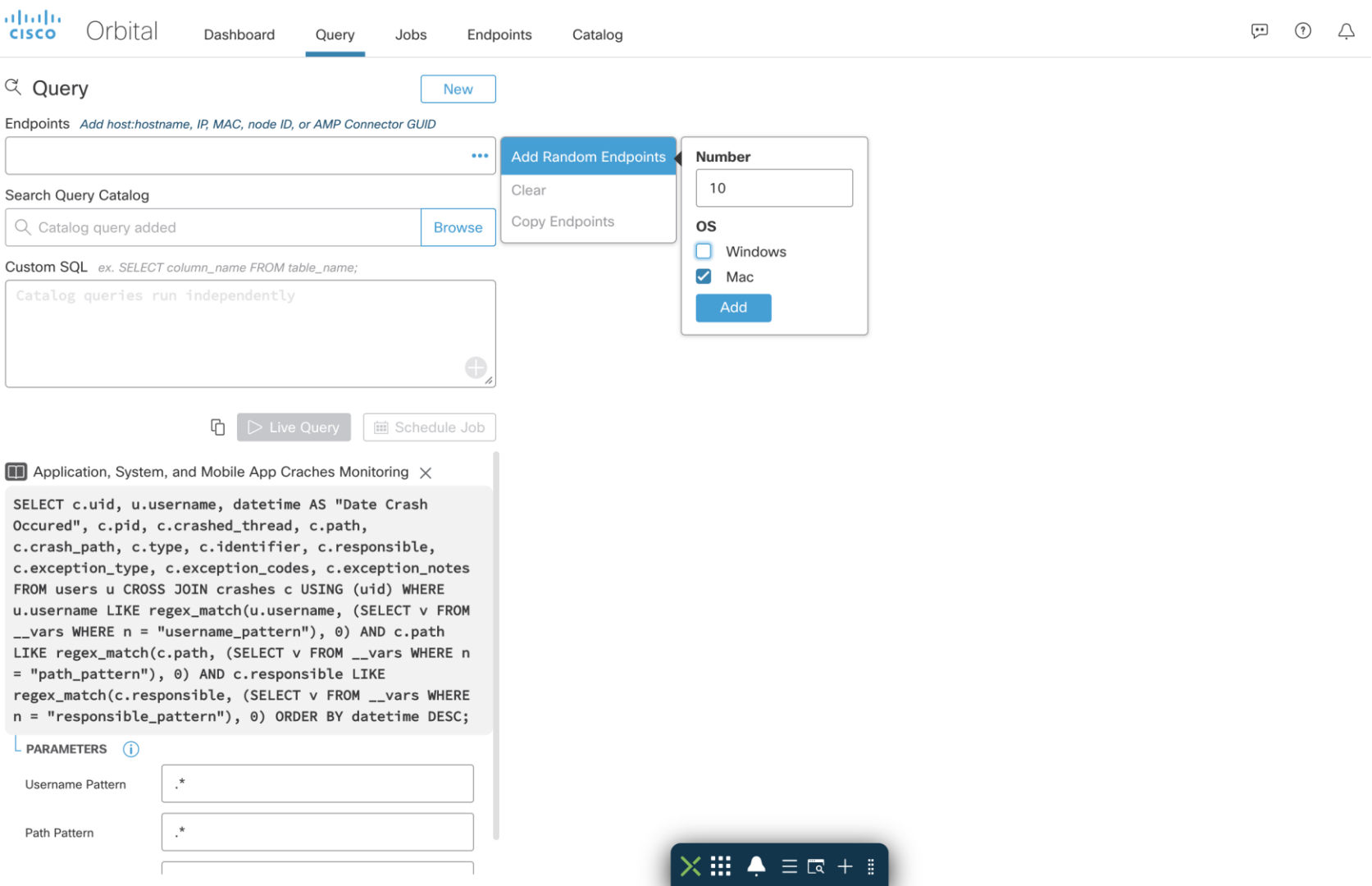
path_pattern:
default: .* *multiple:* false *nameVal:* TEXT

responsible_pattern:
default: .* *multiple:* false *nameVal:* TEXT

SQL

+ Add to new query

```
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;
```


cisco Orbital
Dashboard
Query
Jobs
Endpoints
Catalog
Query
New
Endpoints Add host:hostname, IP, MAC, node ID, or AMP Connector GUID
Add Random Endpoints
Clear
Copy Endpoints
Number
10
OS
Windows
Mac
Add
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 Craches Monitoring
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
Username Pattern
.*
Path Pattern
.*

Query

New

76 rows from 2 endpoints | View on Jobs page | Download

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

host:BRMCMAHO-M-89V2 × host:S-MacBook-Air-2.local ×

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 Craches Monitoring ×

```
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

Username Pattern	.*
Path Pattern	.*

HOSTNAME	BRMCMAHO-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 Craches Data

uid	username	Date Crash Occured	pid	crashed_thread	path
BRMCMAHO-M-89V2					
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/Xcoc
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/Xcoc
501	brmcmaho	2021-10-19 08:59:23.008 -...	31710	24	/Users/USER/Libra
501	brmcmaho	2021-10-19 07:52:35.379 -...	98353	0	/Applications/Xcoc
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/Xcoc
501	brmcmaho	2021-10-17 16:18:12.352 -...	1532	0	/Applications/Xcoc
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/Xcoc
501	brmcmaho	2021-10-16 12:37:41.523 -...	16559	0	/Applications/Xcoc
	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

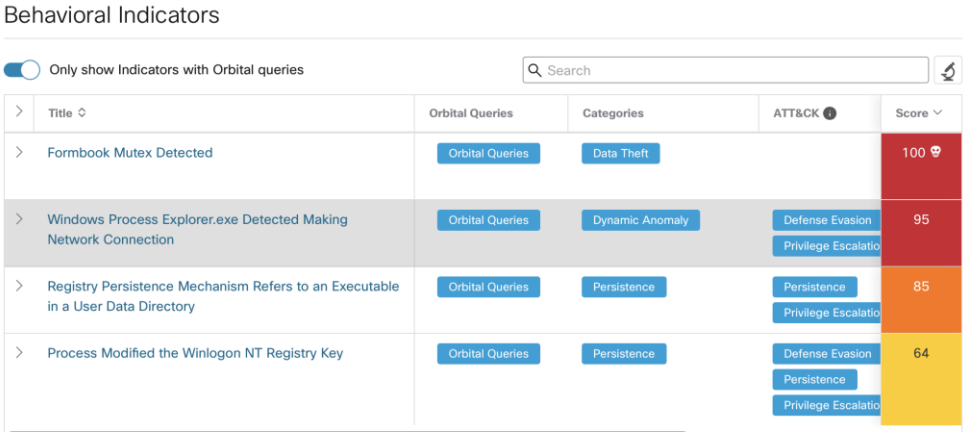
hermetic

Name	Created	Updated	ID	OS	Category	ATT&CK™ Tactic	ATT&CK™ Technique
Driver Loaded Windows Event Logs	2022-02-24	2022-02-24	windows_eventlogs_driver_loaded		Posture Assessment, Forensics, Threat Hunting	Persistence, Execution	Service Execution
Windows Registry CrashControl Monitoring	2022-02-24	2022-02-24	windows_registry_crashcontrol		Posture Assessment, Forensics		

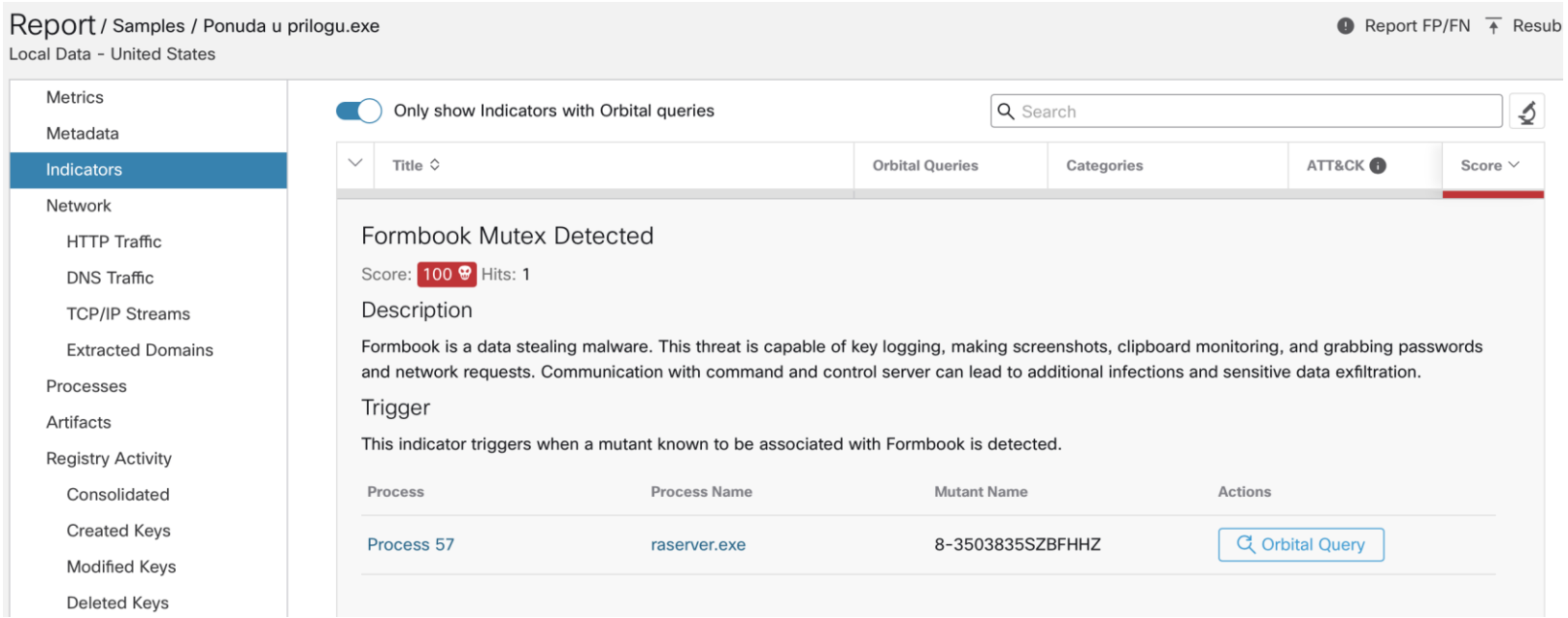
< 1 >

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!



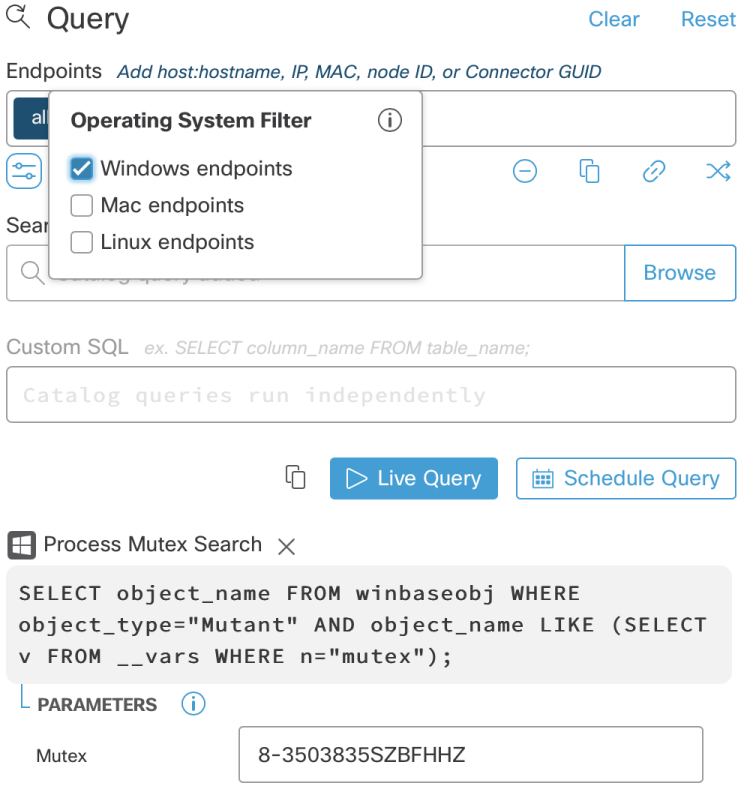
Using Secure Malware Analytics as a Query Source



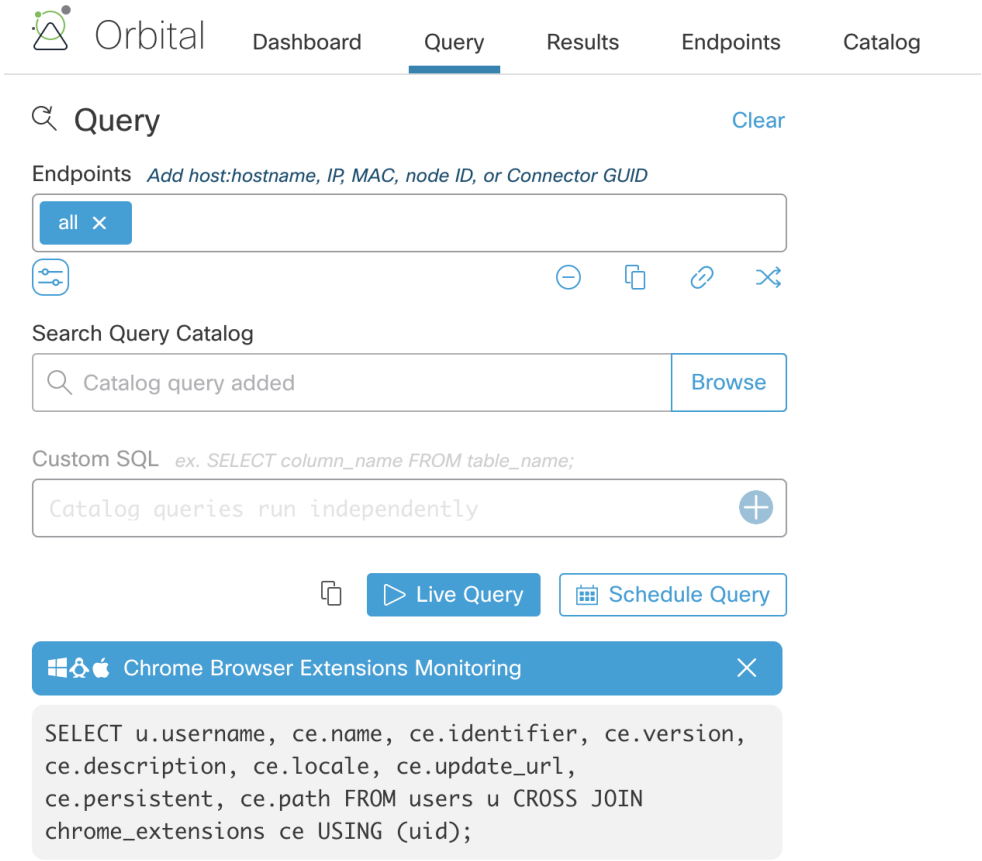
- Just click the “Orbital Query” button on the BI of interest.

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.



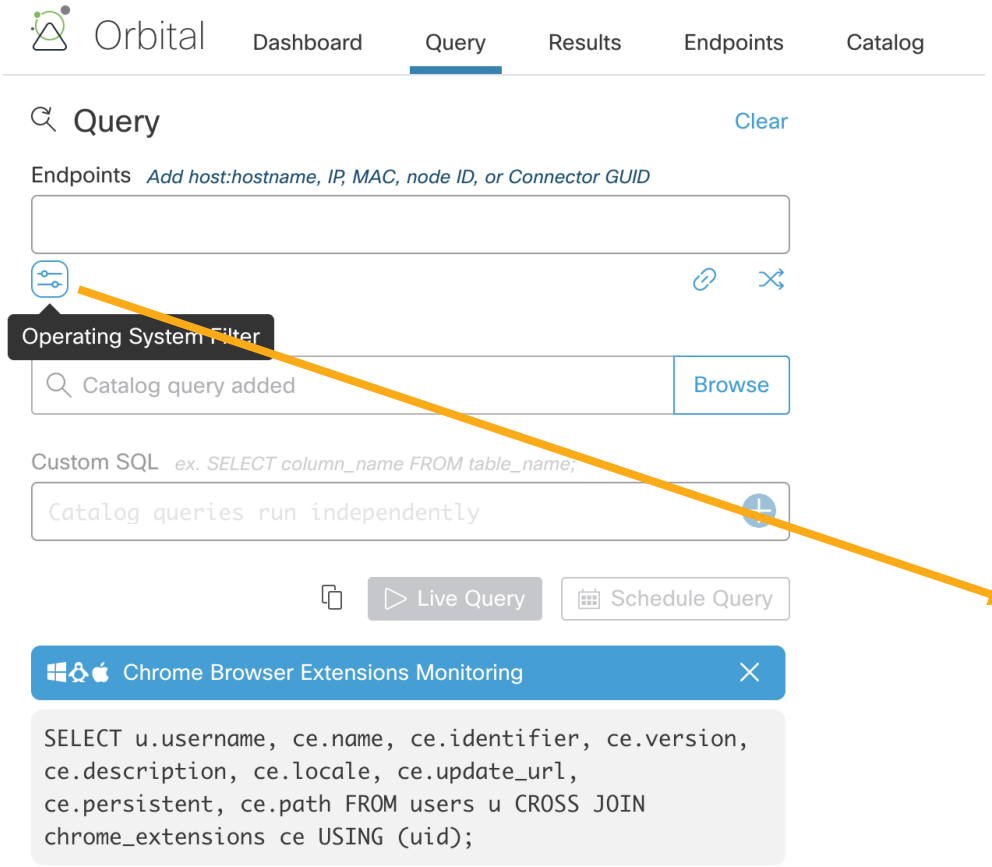
Running a Search: Scheduled, Event-Driven, On-Demand



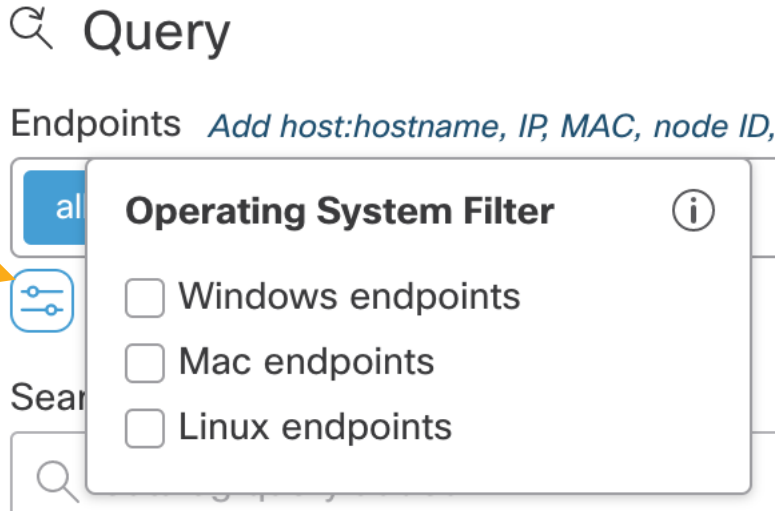
Here, we have selected the "Chrome Browser Extensions Monitoring" catalog entry, which is applicable across multiple platforms.

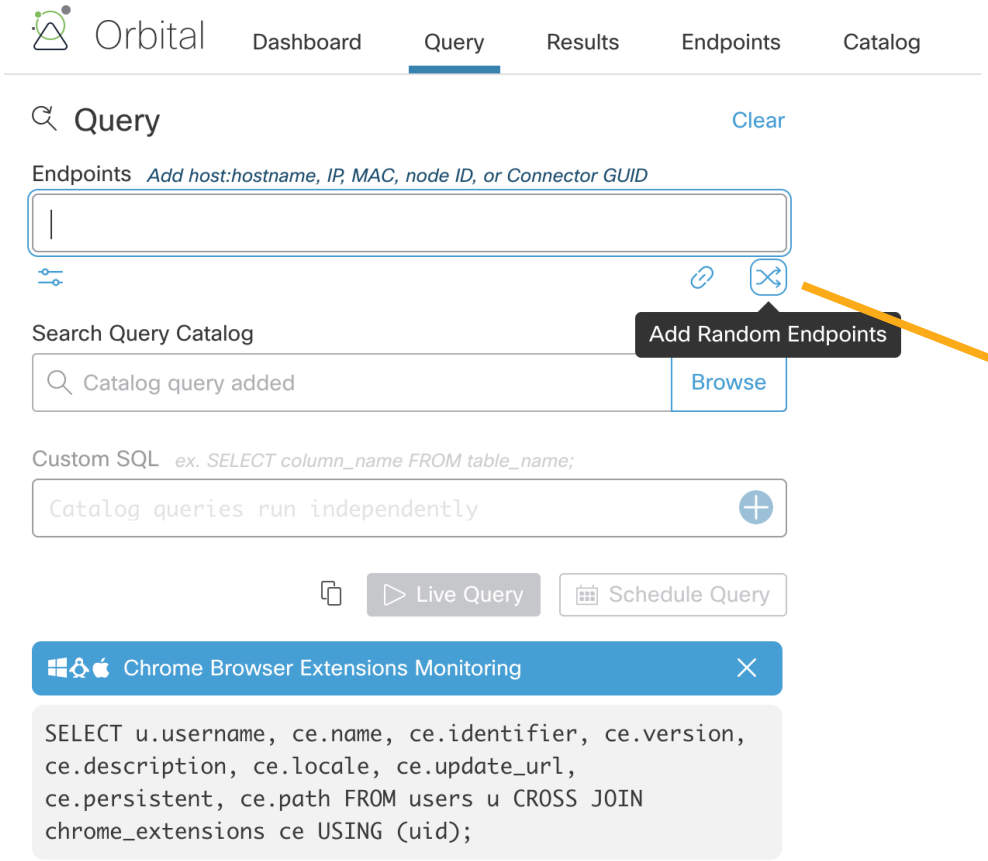
So we could just select "all" endpoints as our target, and let it run like that.

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



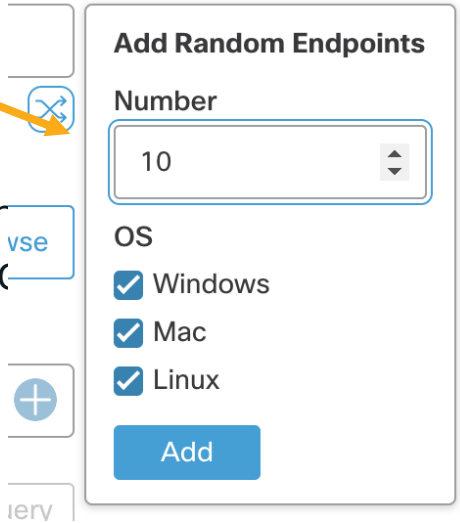
Or, if we're interested in one specific operating system, we could specify that.

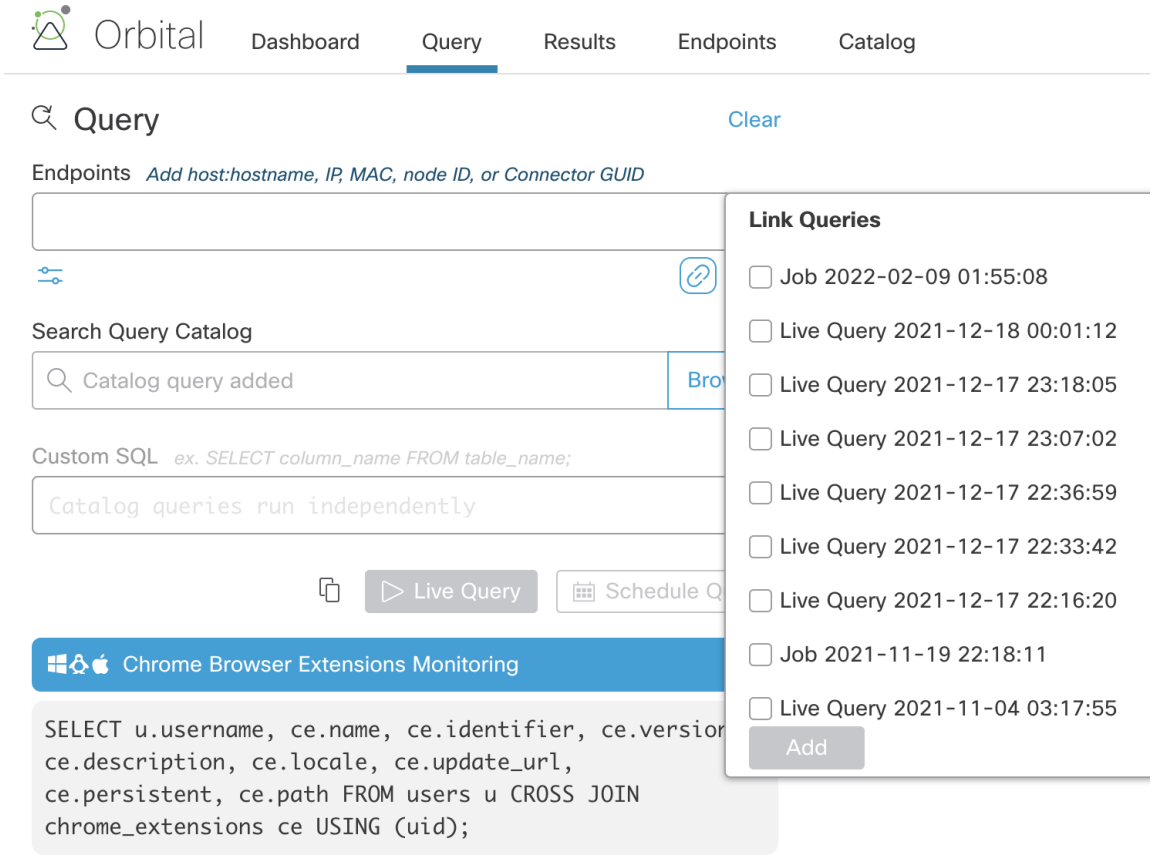




Or, we can add a random subset of endpoints, if we want to get a statistical sampling of our environment.

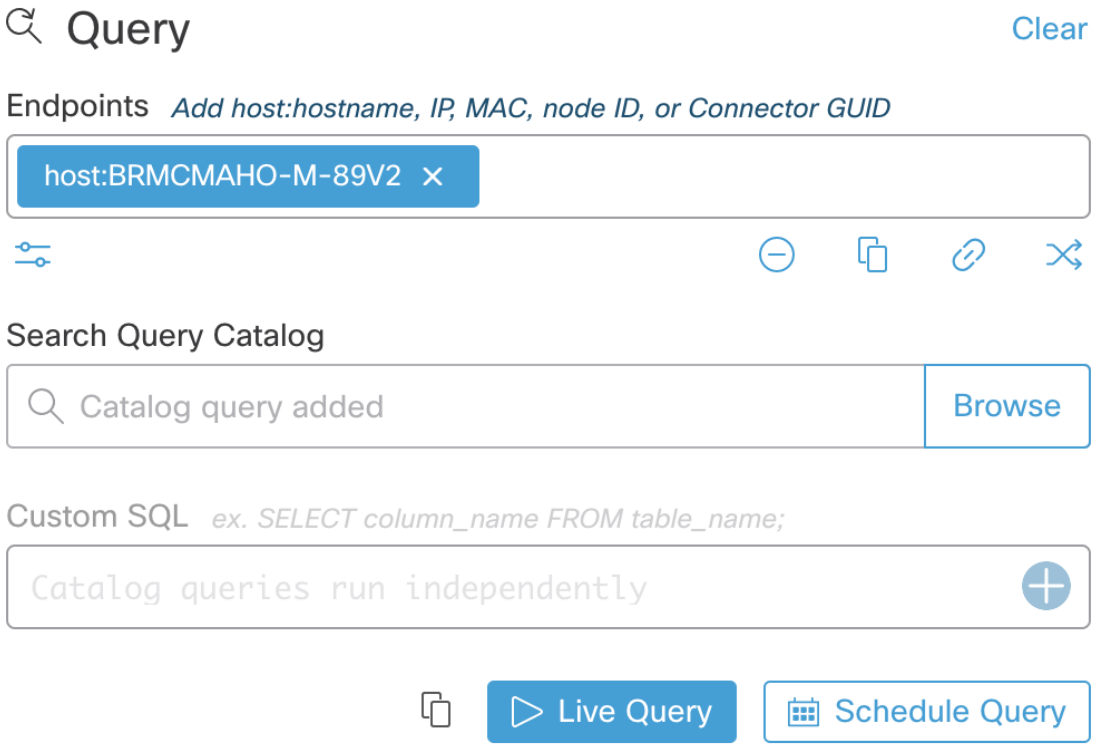
The random endpoints can also be limited by operating system.





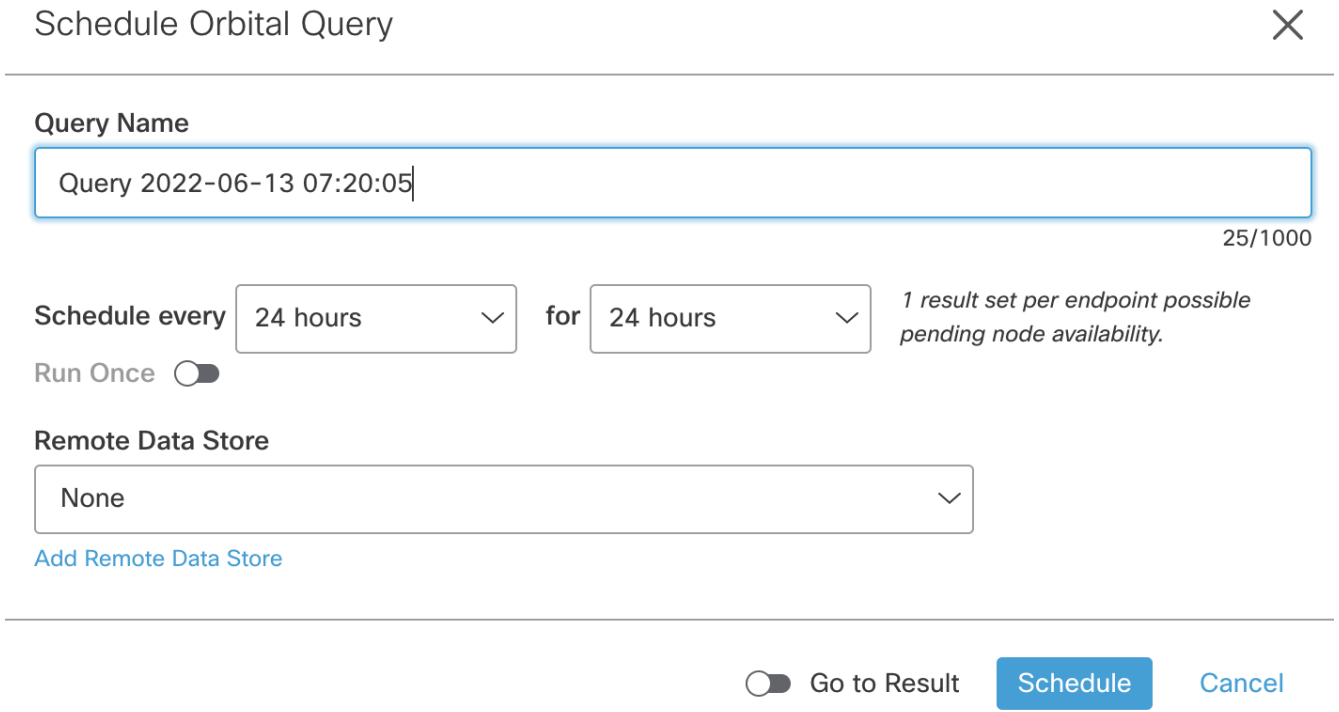
"Linked Queries" allow you to use the results of one query to target another. Only endpoints that return a *non*-empty result for the first query are eligible for the second.

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



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

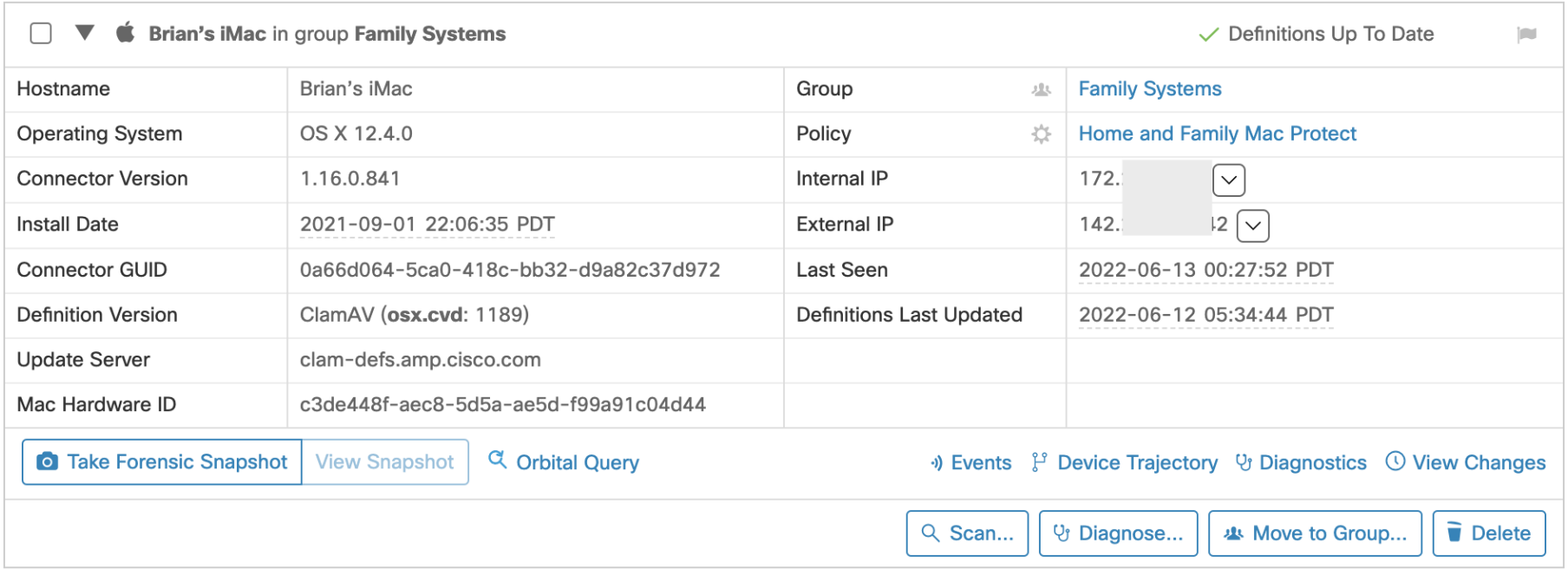
That's what the "Live Query" button is there for.



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

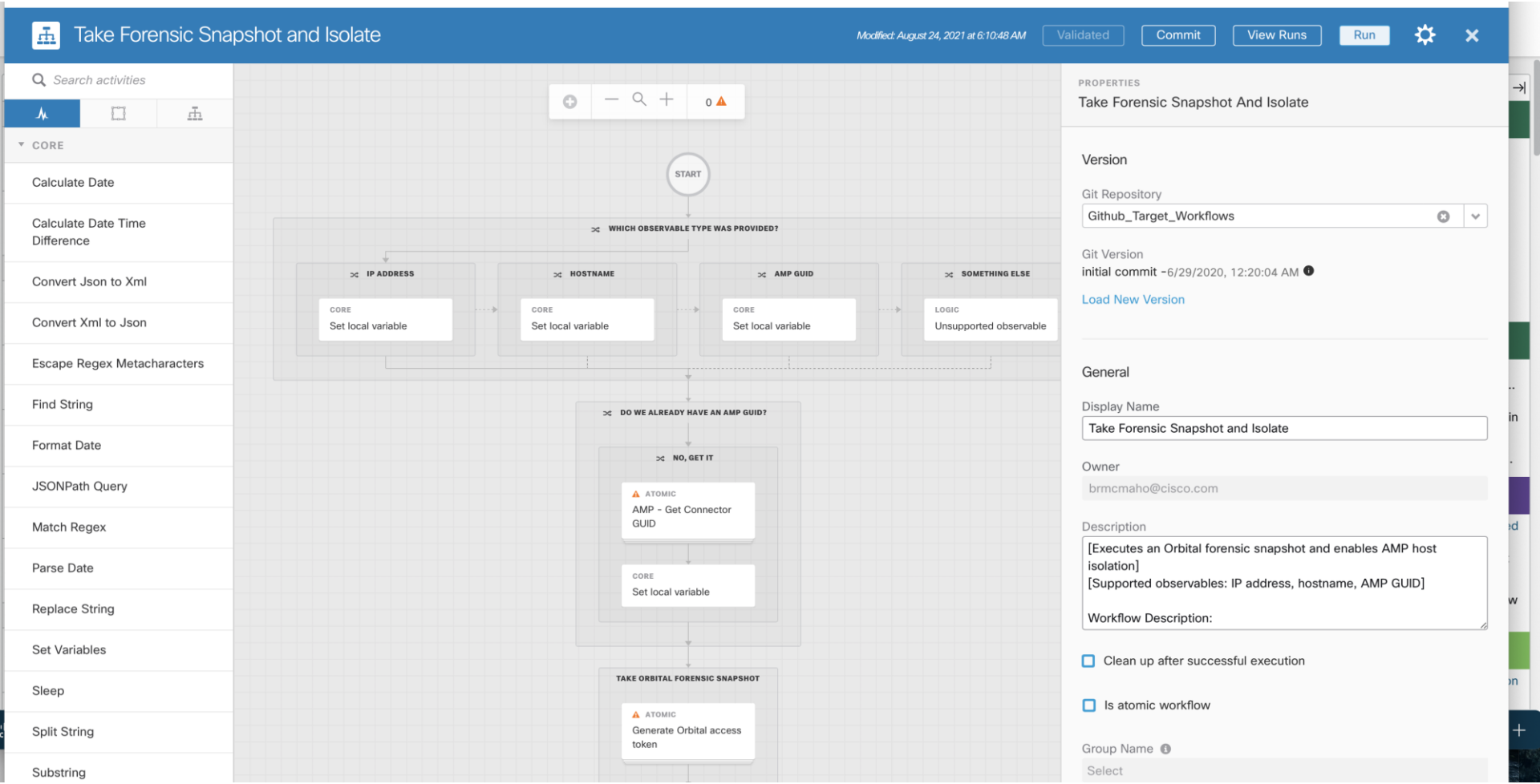
They can run on a time cadence (from 5 minutes to 30 days) over a period of up to two years.

A Remote Data Store is useful for offline long-term

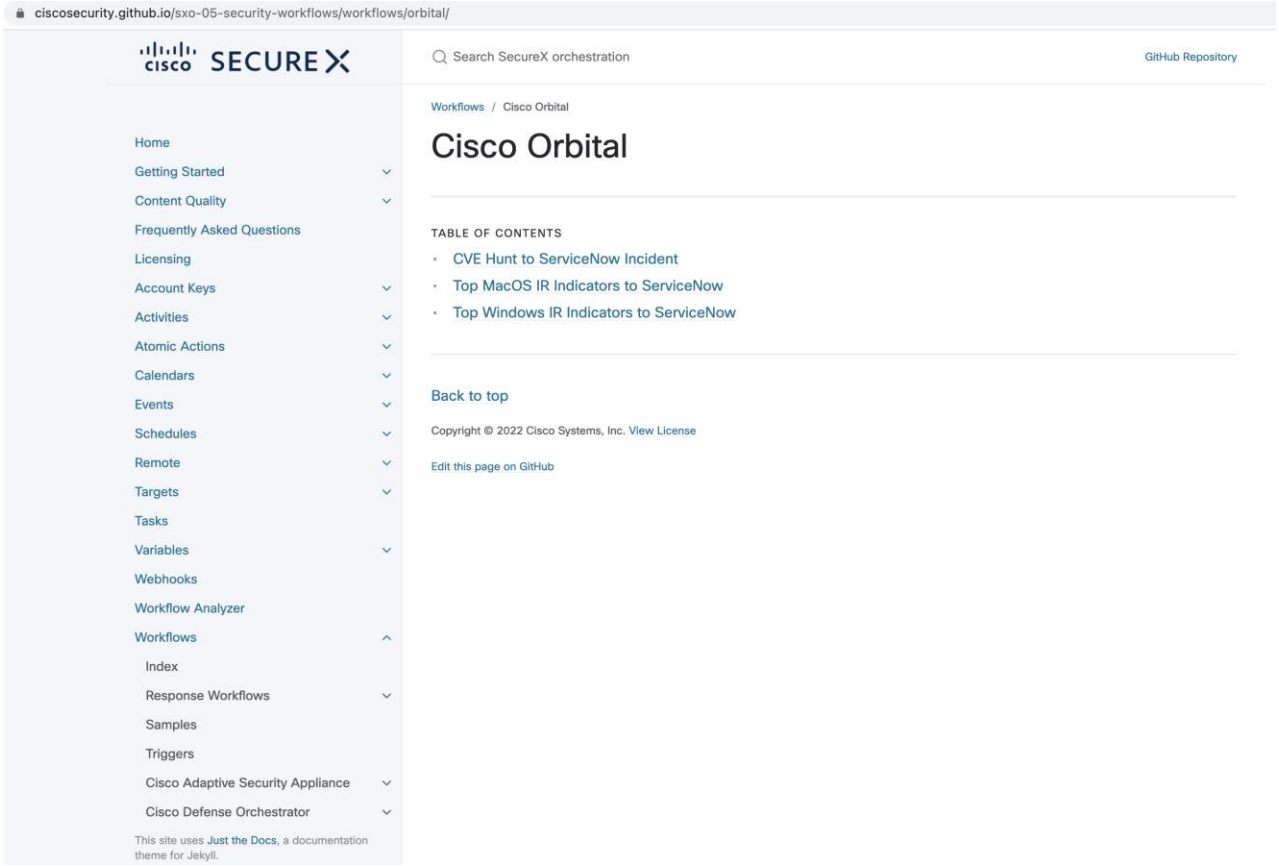


Cisco Secure Endpoint (Advantage license or higher) also incorporates a very useful special kind of Orbital query: the Forensic Snapshot. This is a predefined set of information about the state of the operating system that can be captured at a point in time, referenced in the Device Trajectory, and downloaded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

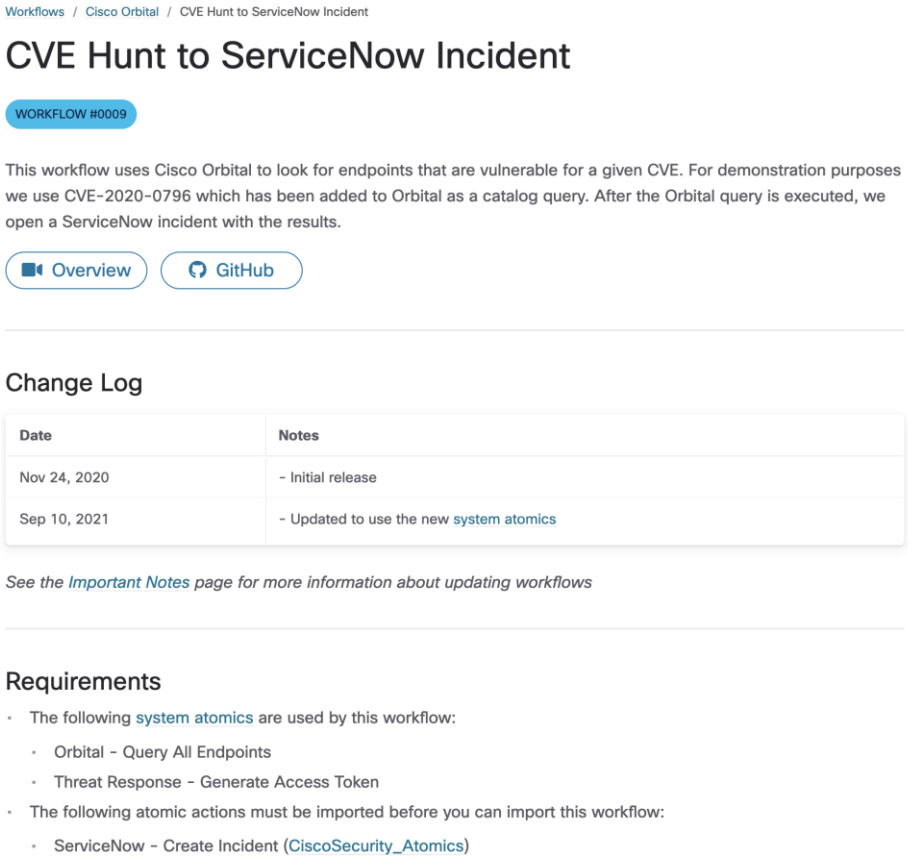
Using Orbital with SecureX Orchestration


Take Forensic Snapshot and Isolate
Modified: August 24, 2021 at 6:10:48 AM
Validated
Commit
View Runs
Run
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
START
WHICH OBSERVABLE TYPE WAS PROVIDED?
IP ADDRESS
CORE
Set local variable
HOSTNAME
CORE
Set local variable
AMP GUID
CORE
Set local variable
SOMETHING ELSE
LOGIC
Unsupported observable
DO WE ALREADY HAVE AN AMP GUID?
NO, GET IT
ATOMIC
AMP - Get Connector GUID
CORE
Set local variable
TAKE ORBITAL FORENSIC SNAPSHOT
ATOMIC
Generate Orbital access token
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



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

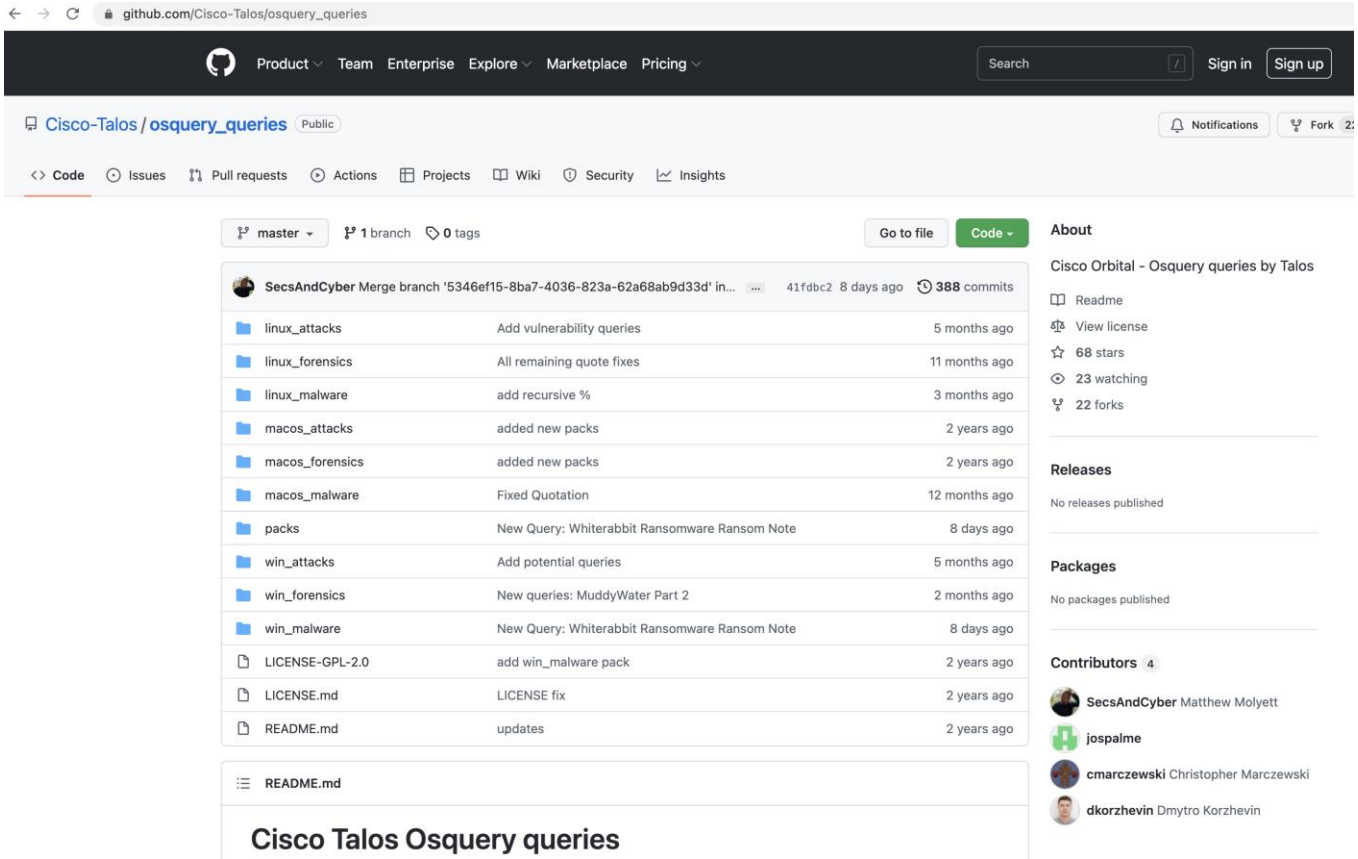
Date	Notes
Nov 24, 2020	- Initial release
Sep 10, 2021	- Updated to use the new system atomics

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)

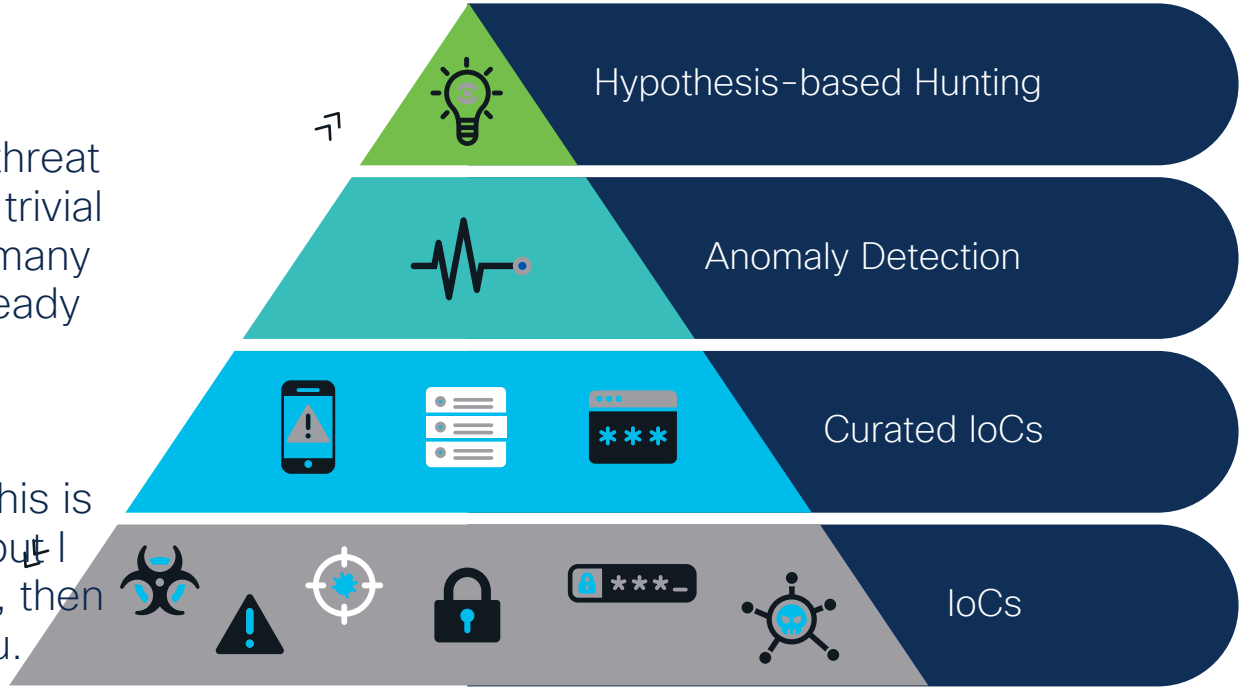
Talos Queries on Github

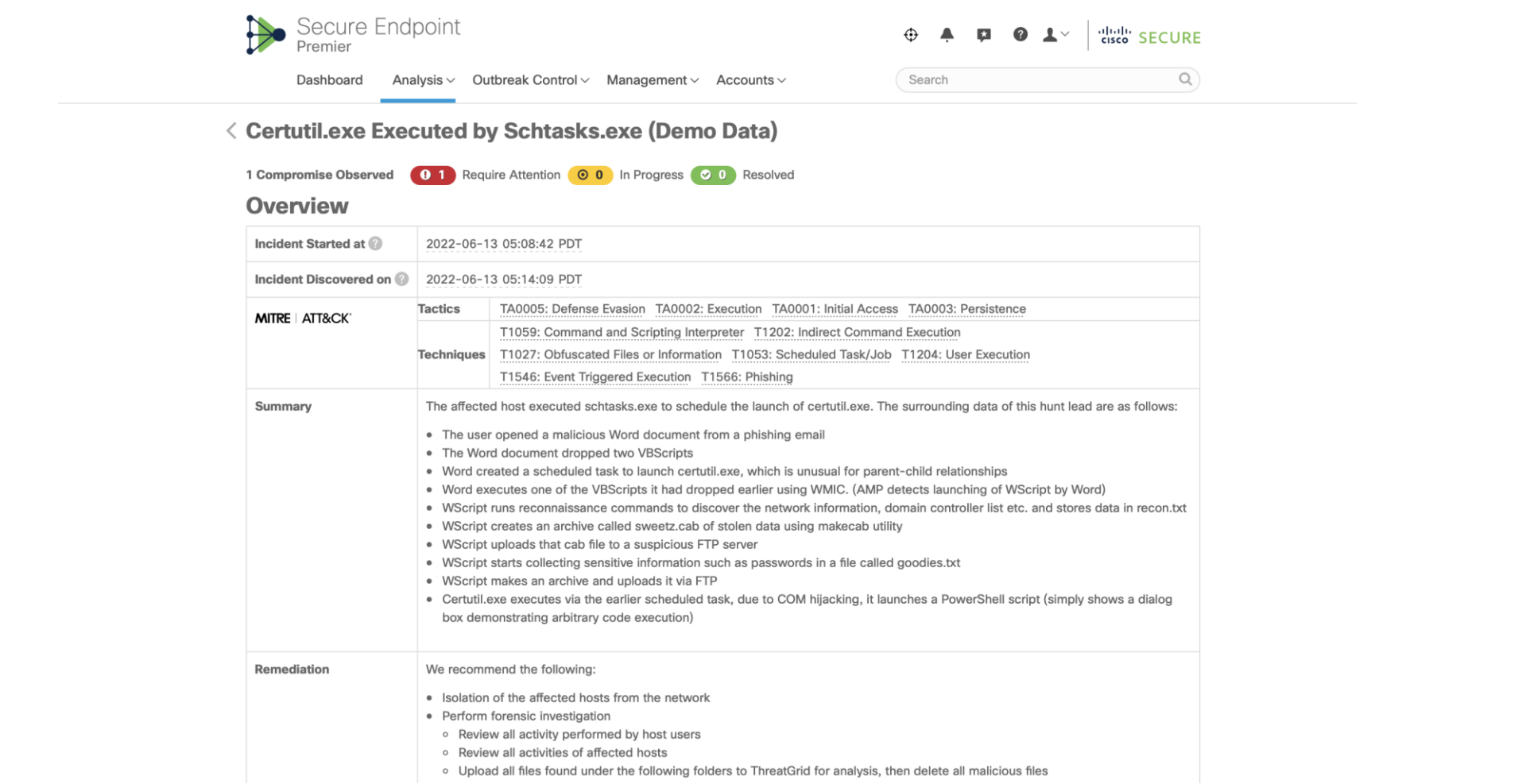


Oh, and one more thing...

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.





Conclusion

Orbital Query Corner - Update

AMP for Endpoints | Endpoint Security | Orbital Advanced Search

1606 VIEWS | 15 HELPFUL | 2 COMMENTS

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.

Ask a Question

Create
+ Discussion + Blog + Document
+ Event + Video + Project Story

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
- 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

Pay for Learning with Cisco Learning Credits

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

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

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

cisco Live!

Thank you


cisco Live!
ALL IN