
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

Orbital Endpoint Search

Real Time Investigation on the Endpoint
Endpoint Investigation with Orbital on Secure Endpoint

Thorsten Schranz, Technical Marketing Engineer – Secure Endpoint

BRKSEC-2107

Agenda

- Cisco Secure Endpoint – Summary
- How orbital extends SecureX Architecture
- Enable / Deploy Orbital
- Problems solved
  - How Orbital works
  - Query (SQL) → Sequence
- Demo

Endpoint Protection/Detection/EDR Summary

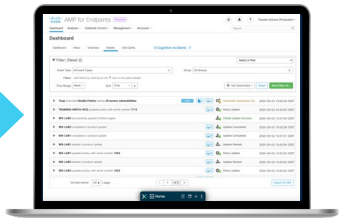
Real Time
File Scan
Script Scan
ExPloit Prevention
Ransomware

System Process Prot.
Behavioral Prot. (new)
ATT&CK®

Real time
Machine Learning
Malware Grouping

AMP Backend
Cloud Detection Engines + Integrations
(e.g. Cognitive)
ATT&CK®

Malware Analytics
File Analysis
ATT&CK®



Protection & Detection

Endpoint

Connector Software

- File (Activity / Upload)
- Process
- Network
- Command Line
- Events

Endpoint Protection/Detection/EDR Summary

Real Time and Retrospection

Automated Actions
- Move to Group
- Node Isolation
- File Analysis
- Forensic Snapshot

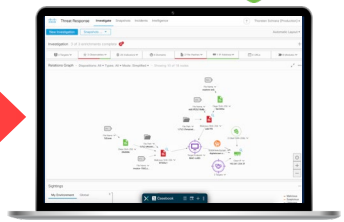
SecureX Orchestration
- Orchestration
- SecureX Modules

Threat Investigation
- Heatmap, DT, Events, IOC
- Indicators (ATT&CK)
- Threat Response
- Pivot Menus, Ribbon

Hunting Services
- SecureX Threat Hunting Premier
- Talos IR

Detection
Response
Hunting

Endpoint
SecureX
Threat Response
Orbital



Architecture
- Each Cloud Service provides features, which are available in the SecureX architecture
- Orbital provides the Real Time Investigation features to query endpoint information

Statements
- SecureX Orchestration != SecureX Module
- SecureX Threat Hunting is not a product
- Pivot Menus and Ribbon are provided by SecureX. The Ribbon includes different apps, e.g. Casebook, Incident or Orbital
- Orbital: access to Ribbon app, Pivot Menu and requests information from other Cisco Security APIs

Endpoint Protection/Detection/EDR Summary

Automated Actions

Real Time and Retrospection

- Move to Group
- Node Isolation
- File Analysis
- Forensic Snapshot

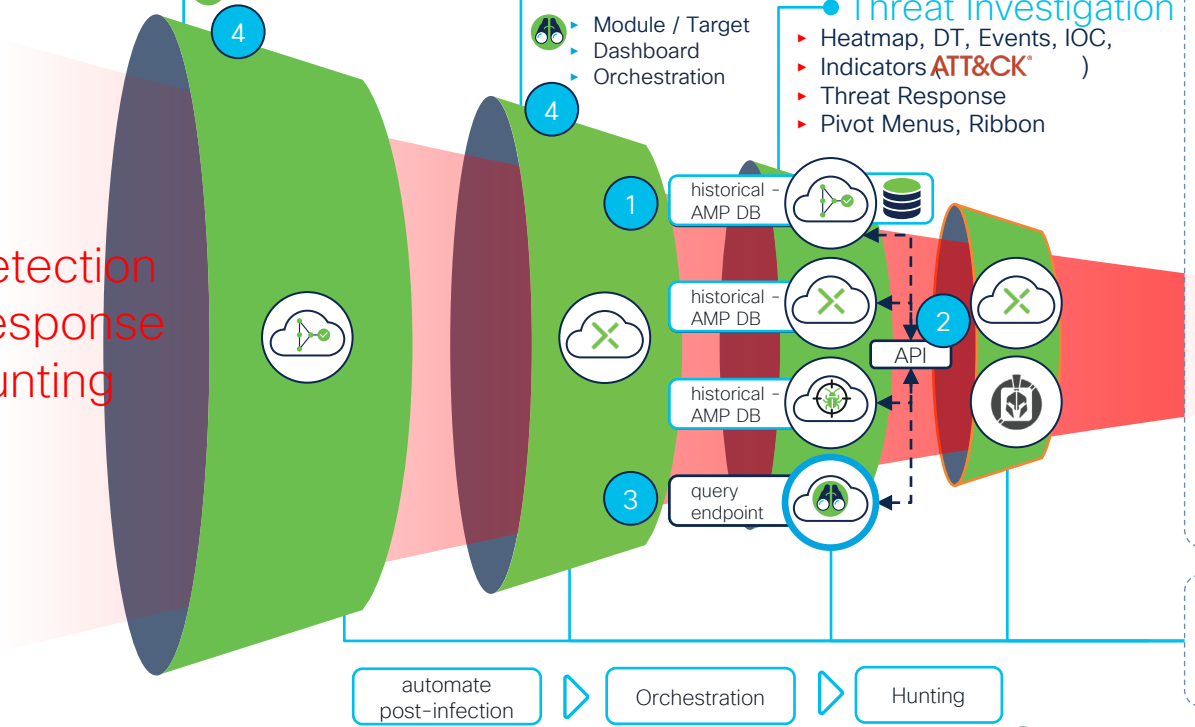
SecureX Orchestration

- Orchestration
- SecureX Modules
  - Module / Target
  - Dashboard
  - Orchestration

Threat Investigation

- Heatmap, DT, Events, IOC,
- Indicators (ATT&CK)
- Threat Response
- Pivot Menus, Ribbon

Detection
Response
Hunting



automate post-infection ▷ Orchestration ▷ Hunting

Statements

1. any historical data is stored in the AMP backend. The data is generated by the Connector when monitoring endpoint activity
2. SecureX Dashboard data information or a Threat Response investigation, directly queries AMP DB. There is **NO** data copied between cloud services.
   No SIEM is needed.
3. Orbital Endpoint Software generates informaton OnDemand. The footprint on the endpoint is very small.
4. Orbital provides different Services like:
   - Generating an Endpoint Forensic Snapshot
   - Module for Threat Response / Target for Orchestration. Provides data for Dashboard. Provides Long Term Investigation (Jobs), Ribbon
   - Investigate directly from Analysis Report

Endpoint

Connector Software

Endpoint Protection/Detection/EDR Summary

Automated Actions

Real Time and Retrospection

- Move to Group
- Node Isolation
- File Analysis
- Forensic Snapshot

SecureX Orchestration

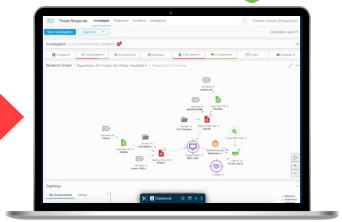
- Orchestration
- SecureX Modules
  - Module / Target
  - Dashboard
  - Orchestration

Threat Investigation

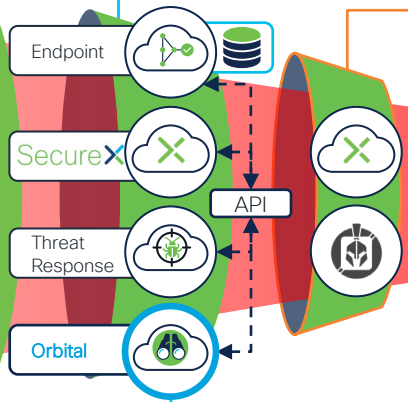
- Heatmap, DT, Events, IOC,
- Indicators (ATT&CK®)
- Threat Response
- Pivot Menus, Ribbon

Hunting Services

- SecureX Threat Hunting Premier +
- Talos IR



Detection
Response
Hunting



Investigation

Automation
Orchestration
Response
Threat Hunting

- Link TR Snapshot to Casebook(s)
- Link TR Snapshot to Incident(s)
- Assign Incident to User(s)

It is important to see Orbital not as a point of product, it is an important part of the SecureX architecture

Activate Orbital

Activate Orbital

SecureX Getting Started Guide

Endpoints Package Comparison

License

- Essential
- Advantage ✓
- Premier ✓

Orbital Enhancements

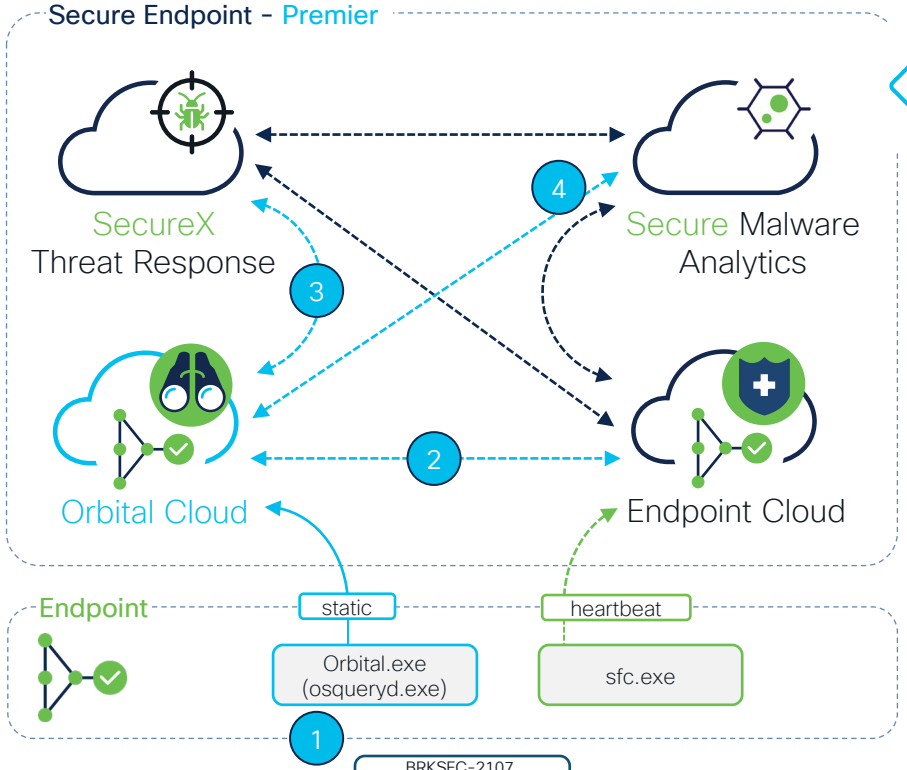
1
- Dashboard Tiles
- Orbital Status in the Ribbon
- Start a Query from Ribbon
- Open and login using SSO
- Orchestration

2
- Forensic Snapshot
- Start Real Time investigation
- Deployment

3
- Start Real Time investigation

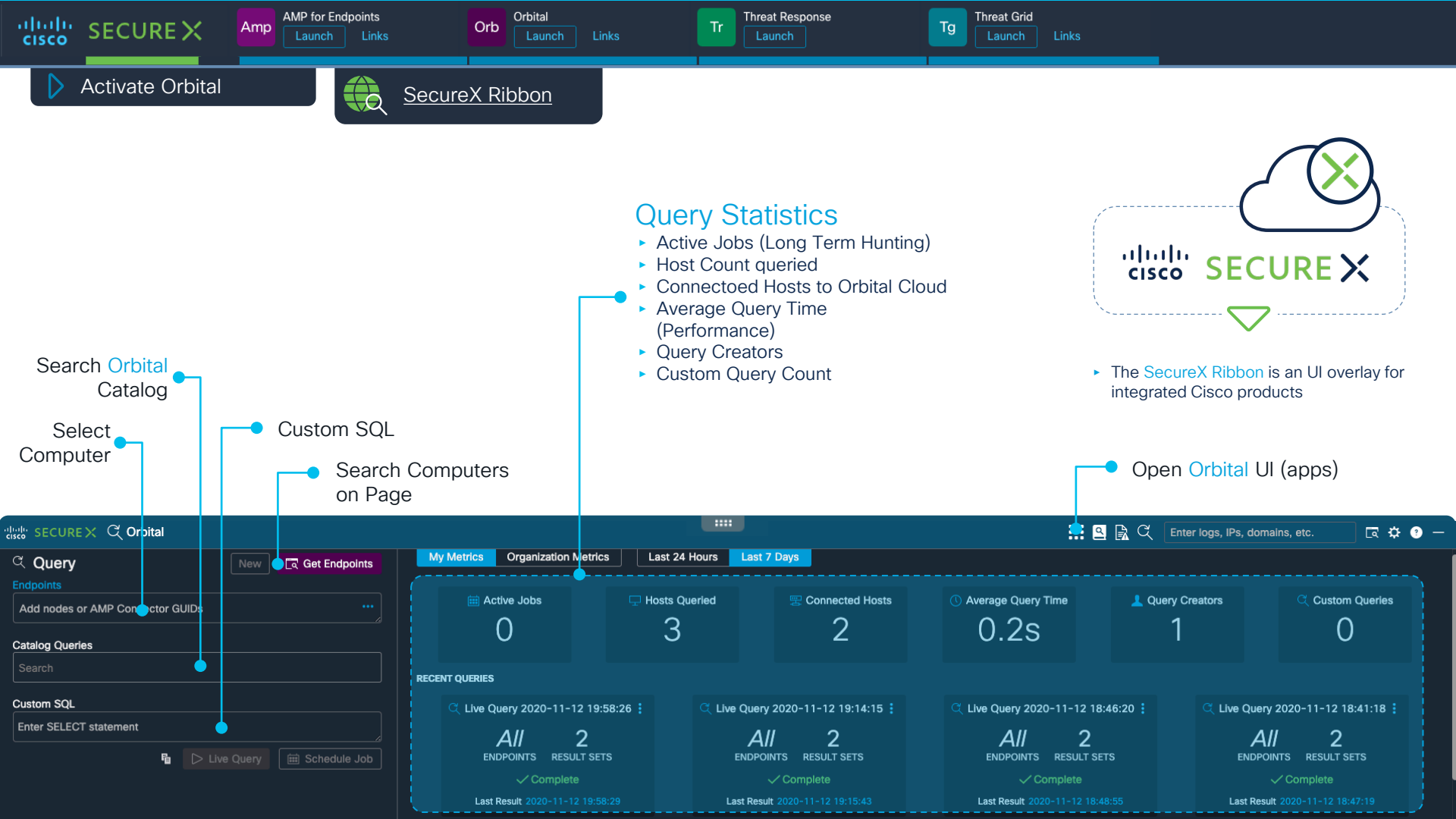
4
- Verify Behaviour Indicators

Only show Indicators with Orbital queries



1 cisco SECURE X

- Activate SecureX in any way
- Check your license
- Login to Orbital UI
- Deploy Orbital


cisco SECURE X
Amp AMP for Endpoints Launch Links
Orb Orbital Launch Links
Tr Threat Response Launch
Tg Threat Grid Launch Links
Activate Orbital
SecureX Ribbon
Query Statistics
Active Jobs (Long Term Hunting)
Host Count queried
Connectoed Hosts to Orbital Cloud
Average Query Time (Performance)
Query Creators
Custom Query Count
cisco SECURE X
The SecureX Ribbon is an UI overlay for integrated Cisco products
Search Orbital Catalog
Select Computer
Custom SQL
Search Computers on Page
Open Orbital UI (apps)
SECURE X Orbital
Enter logs, IPs, domains, etc.
Query
New
Get Endpoints
Endpoints
Add nodes or AMP Connector GUIDs
Catalog Queries
Search
Custom SQL
Enter SELECT statement
Live Query
Schedule Job
My Metrics
Organization Metrics
Last 24 Hours
Last 7 Days
Active Jobs 0
Hosts Queried 3
Connected Hosts 2
Average Query Time 0.2s
Query Creators 1
Custom Queries 0
RECENT QUERIES
Live Query 2020-11-12 19:58:26
All ENDPOINTS 2 RESULT SETS
Complete
Last Result 2020-11-12 19:58:29
Live Query 2020-11-12 19:14:15
All ENDPOINTS 2 RESULT SETS
Complete
Last Result 2020-11-12 19:15:43
Live Query 2020-11-12 18:46:20
All ENDPOINTS 2 RESULT SETS
Complete
Last Result 2020-11-12 18:48:55
Live Query 2020-11-12 18:41:18
All ENDPOINTS 2 RESULT SETS
Complete
Last Result 2020-11-12 18:47:19

Activate Orbital

SecureX Integrations

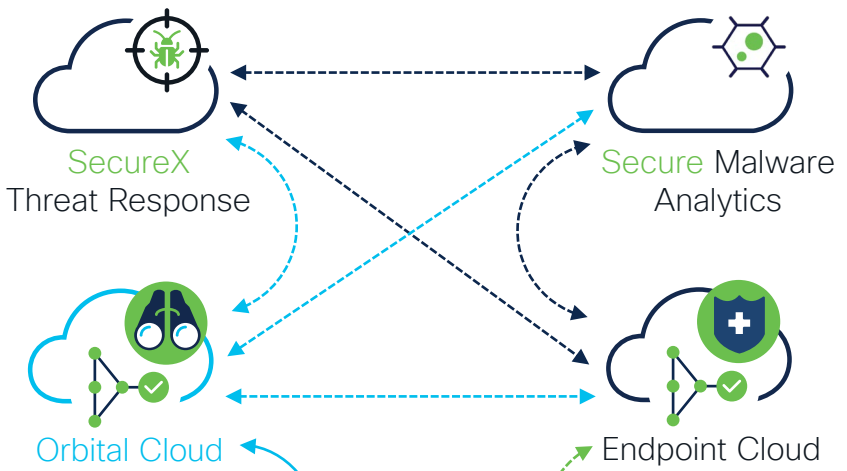
SecureX Integration Partners

Serverless Relay Step-by-Step Guide

3rd Party Vendor list

- Abuse IPDB
- AlienValult OTX
- APIVoid
- CyberCrime Tracker*
- Cyberprotect Threatscore
- Farsight Security
- Google Chronicle
- Google Safe Browsing
- Google VirusTotal
- Have I Been Pwned
- Microsoft Graph Security
- Pulsedive
- SecurityTrails
- See One Feed App
- Shodan
- SpyCloud
- urlscan.io
- Gigamon ThreatINSIGHT
- Qualys IOC
- Radware WAF and DDoS
- Signal Sciences
- Threat Score

Secure Endpoint – Premier

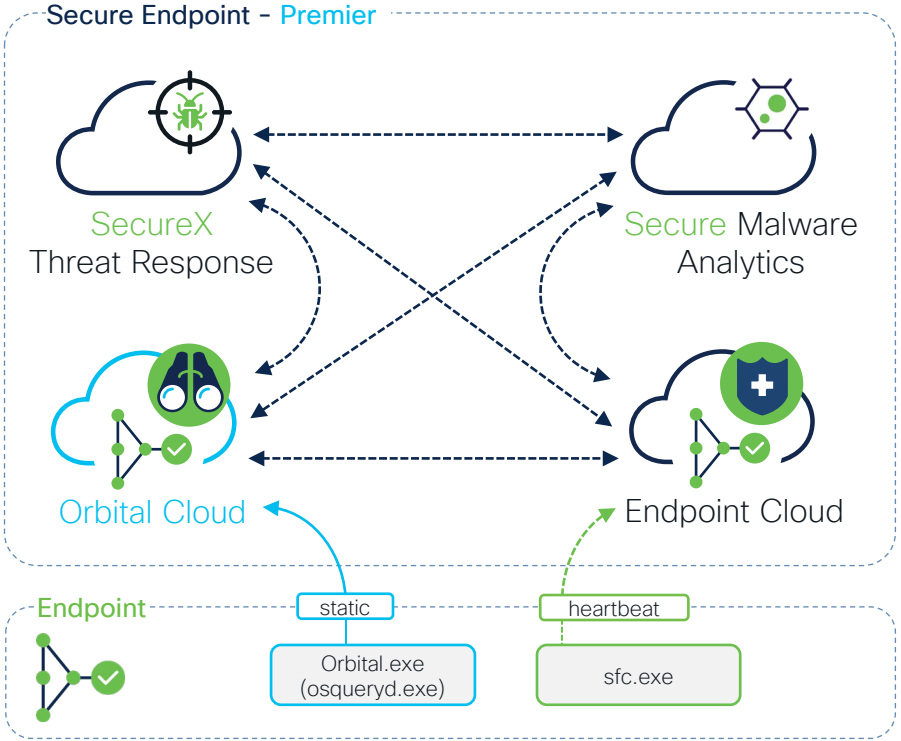


- Configure 3rd Party Modules
- marked integrations provide a free to use community version
- Serverless Relays "translate" information between Cisco and other vendors

- Activate Orbital
- SecureX Integrations
- SecureX Orchestration

SecureX Pre-defines workflows

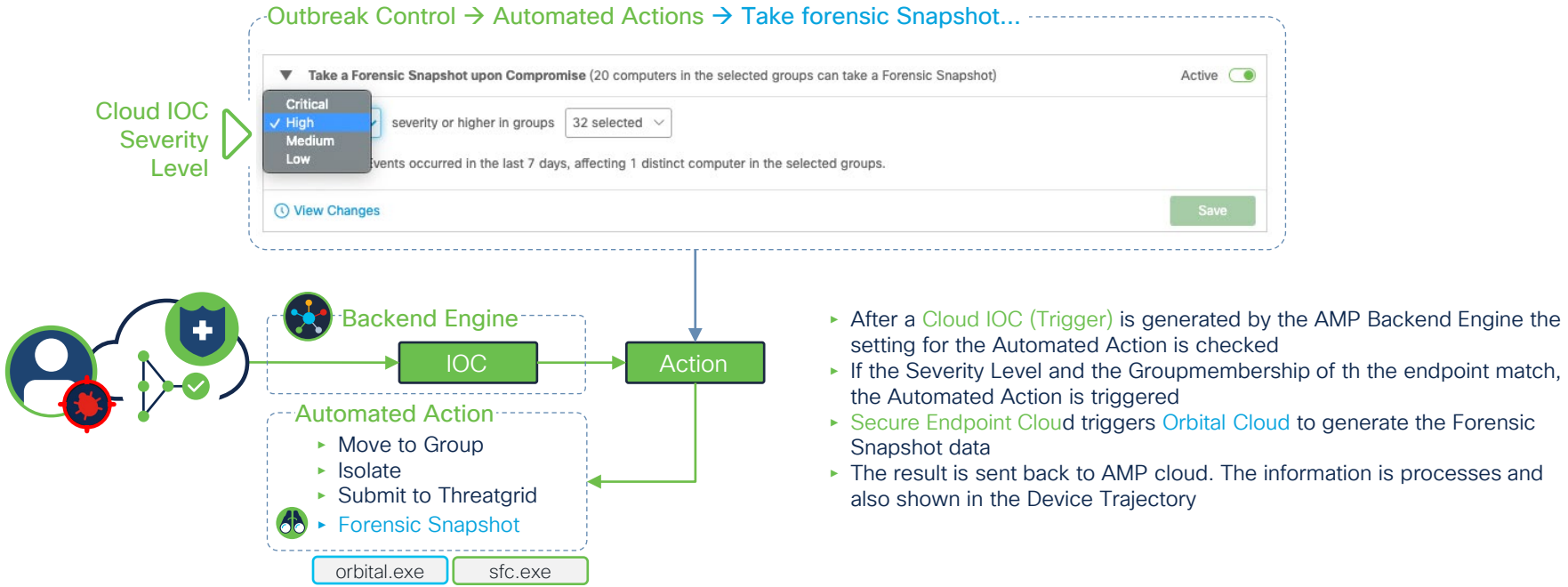
- Move Computer to AMP Triage Group
- AMP Host Isolation with Tier 2 Approval
- Take Forensic Snapshot and Isolate
- Take Orbital Forensic Snapshot



- Activate the pre-defined Workflows

- Activate Orbital
- SecureX Integrations
- SecureX Orchestration

Workflow vs. automated Action



- After a Cloud IOC (Trigger) is generated by the AMP Backend Engine the setting for the Automated Action is checked
- If the Severity Level and the Groupmembership of th the endpoint match, the Automated Action is triggered
- Secure Endpoint Cloud triggers Orbital Cloud to generate the Forensic Snapshot data
- The result is sent back to AMP cloud. The information is processes and also shown in the Device Trajectory

- Activate Orbital
- SecureX Integrations
- SecureX Orchestration

Workflow vs. automated Action

SecureX Orchestration Videos

External Triggers

Cisco Devices + 3rd Party

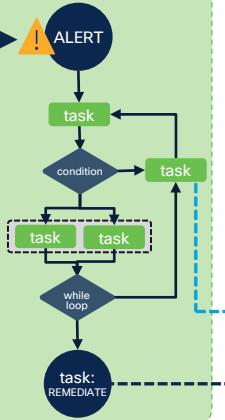
- AMPQ
- SNMP
- Kafka
- Native Integration

3

Targets (2)

- Mail / Web
- Intelligences
- User Directory
- ITSM
- WebEx
- Threat Response
- API available

Workflow Logic (1)



Design Thinking

1. Think about which tasks you want to automate
2. Where SecureX can connect to (Targets)
3. Any System which may trigger an automated process (AO workflow)

task: REMEDIATE | task: QUERY | task: INCIDENT | task: RESPONSE | task: RESPONSE

Existing Architecture

Backend Engine

IOC → Action

Query/Trigger Endpoint

Automated Action

- Move to Group
- Isolate
- Submit to Threatgrid
- Forensic Snapshot

orbital.exe | sfc.exe

Orbital

Start Query

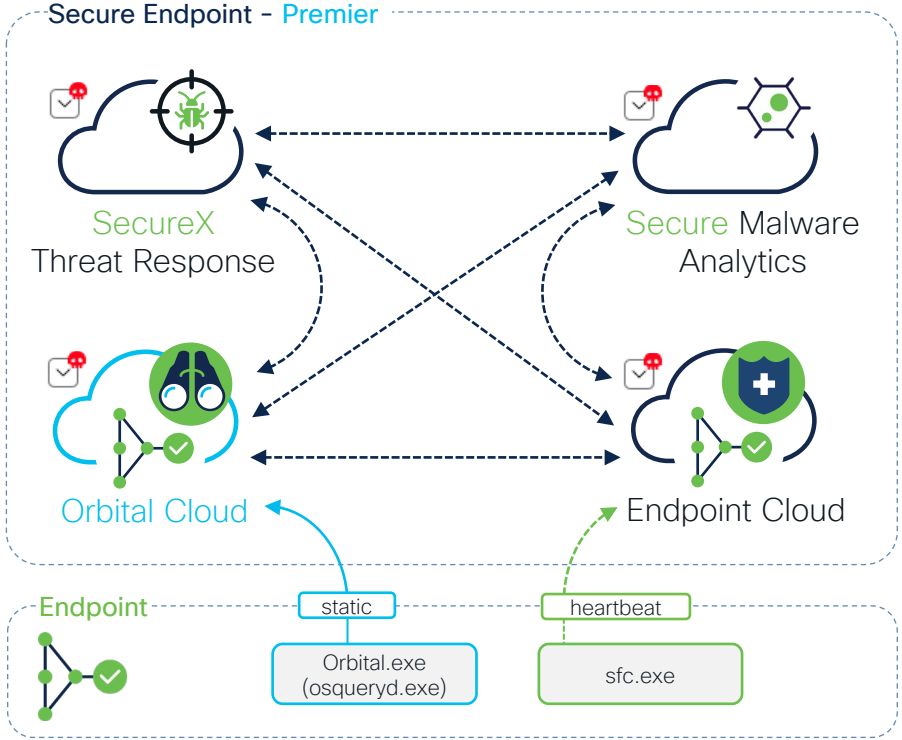
Information for Incident App

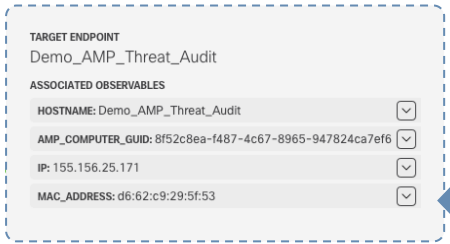
Automate Hunting

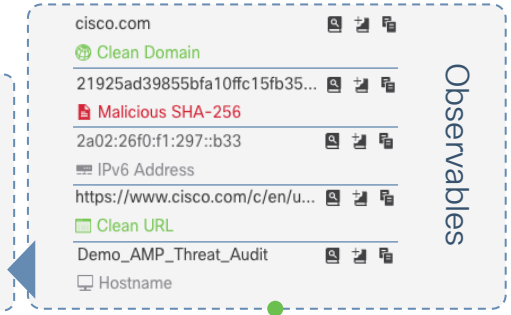
- Activate Orbital
- SecureX Integrations
- SecureX Orchestration

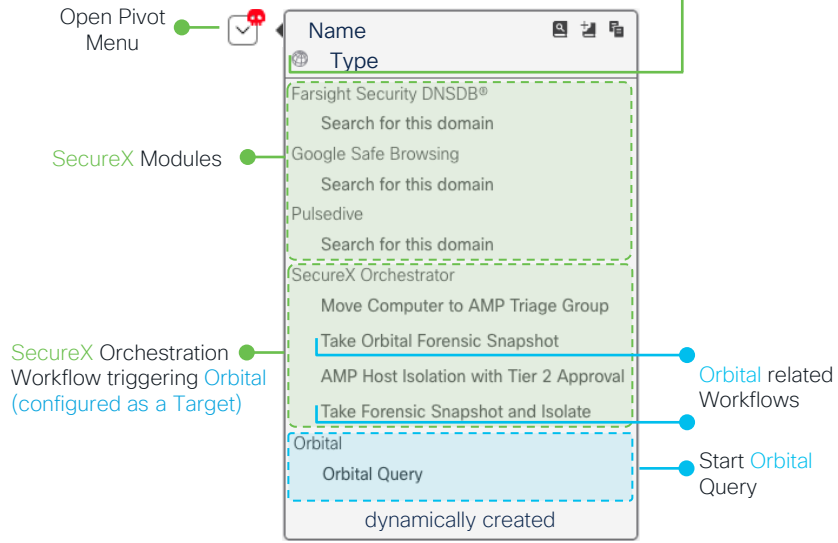
Pivot Menu explained

Pivot Menu







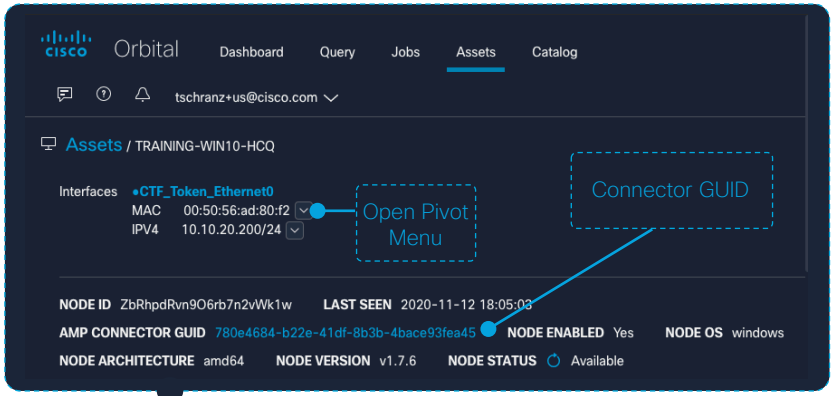


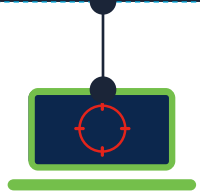
**other options like White/Black-Listing, Malware Analytics and more not shown.

Problems solved

Deployment with a single policy setting

Deployment Strategy Guide





Network

Memory

Endpoint

sfc.exe

Orbital.exe (osqueryd.exe)

static TLS secured

Policy: Orbital

Orbital Advanced Search

Enable Orbital Advanced Search

heartbeat TLS secured

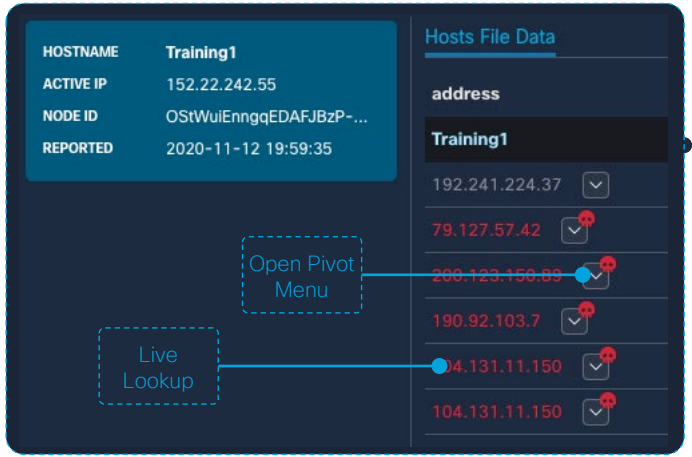
- Policy
- Updates
- Isolation Action

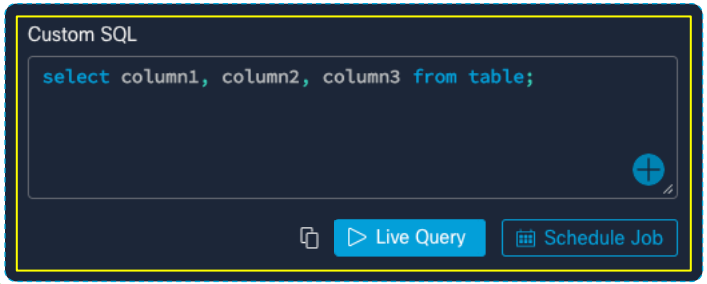
- File, Process, Network, Command Line - activity
- Engine Events
- File upload for Secure Malware Analysis

- Deployment with a single policy setting
- Easy Query Language - SQL

Available Tables

Everything in SQL



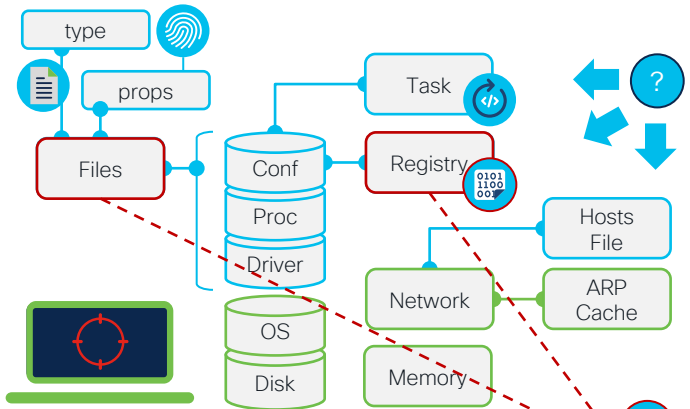


- Orbital endpoint provides virtual tables, which can be queries using SQL
- Select a pre-defined query or write our own SQL statement (Query)
- After clicking the „Live Query“ button, the endpoint pulls the query from the Orbital cloud using the existing connection
- The result is processed by Orbital backend
- The Orbital result shows the Pivot Menu and data is enriched using Cisco Security APIs.

Deployment with a single policy setting

Easy Query Language - SQL

Endpoint Information Lookup



select column1, column2 from startup_items;

startup_items

- Configuration behind every table
- Tables are filled OnDemand
- Included Information about information from files which are automatically executed and informaton from the registry

1 Orbital.exe reads the configuration behind a requested SQL statement

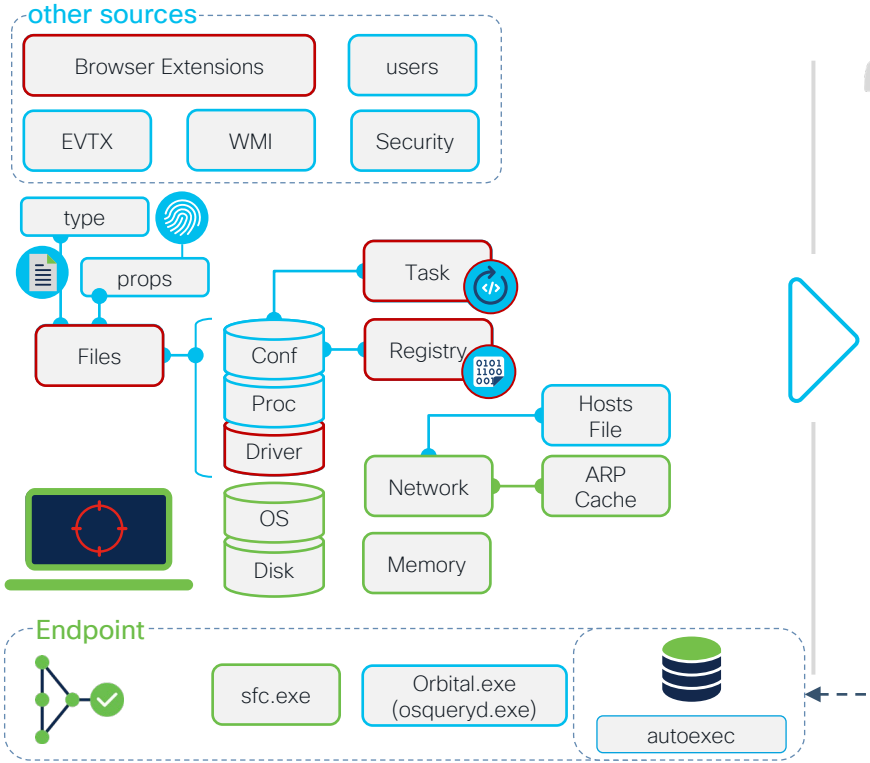
? How to access the needed information on the endpoint?
- Files are not readable
- Files are hidden
- Information is encrypted or protected by the OS
- Information is stored in „database like“ files
- Administrative permissions needed
- What and how something is executed automatically on the endpoint

2 Orbital.exe finds the information on the endpoint and writes it to the database

3 Orbital.exe sends back the SQL query result

- Deployment with a single policy setting
- Easy Query Language - SQL

Endpoint Information Lookup




```
select column1, column2 from autoexec;
```

autoexec

- Configuration behind every table
- Tables are filled OnDemand

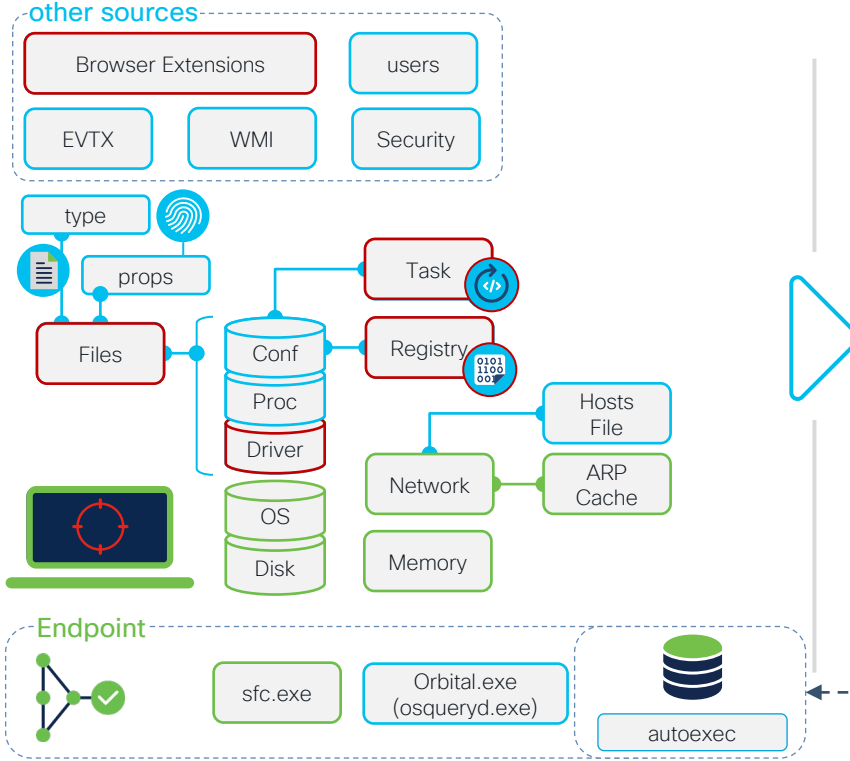
- What and how something is executed automatically on the endpoint
- Query multiple sources including startup items with a single query

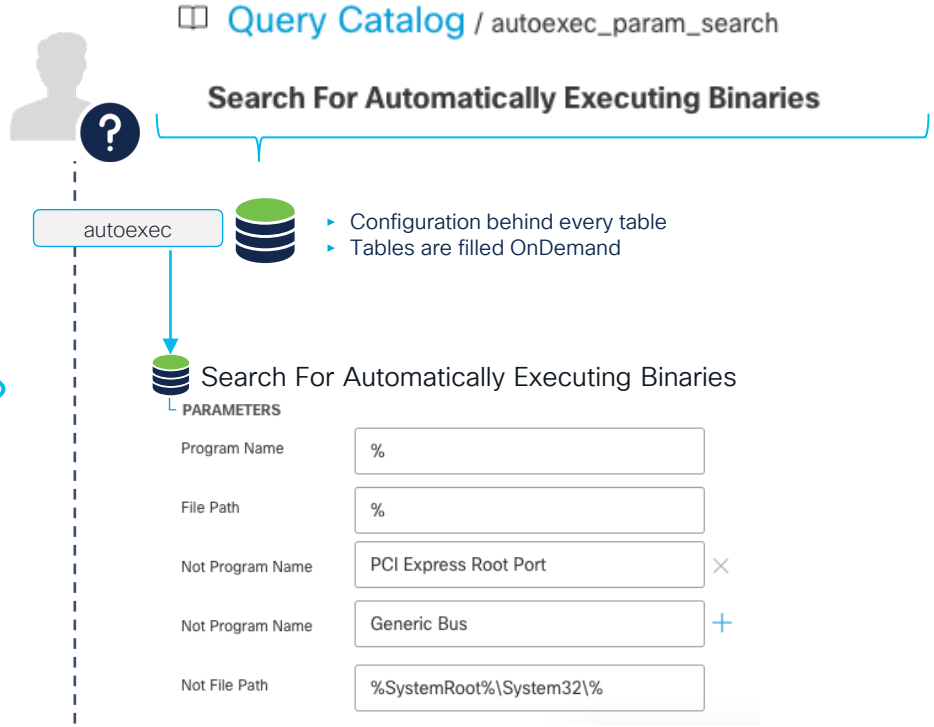
autoexec: aggregate of executables that will automatically execute on the target machine.
This is an amalgamation of other tables like services, scheduled_tasks, startup_items and more

- drivers
- ie_extensions
- scheduled_tasks
- services
- startup_items

- Deployment with a single policy setting
- Easy Query Language - SQL

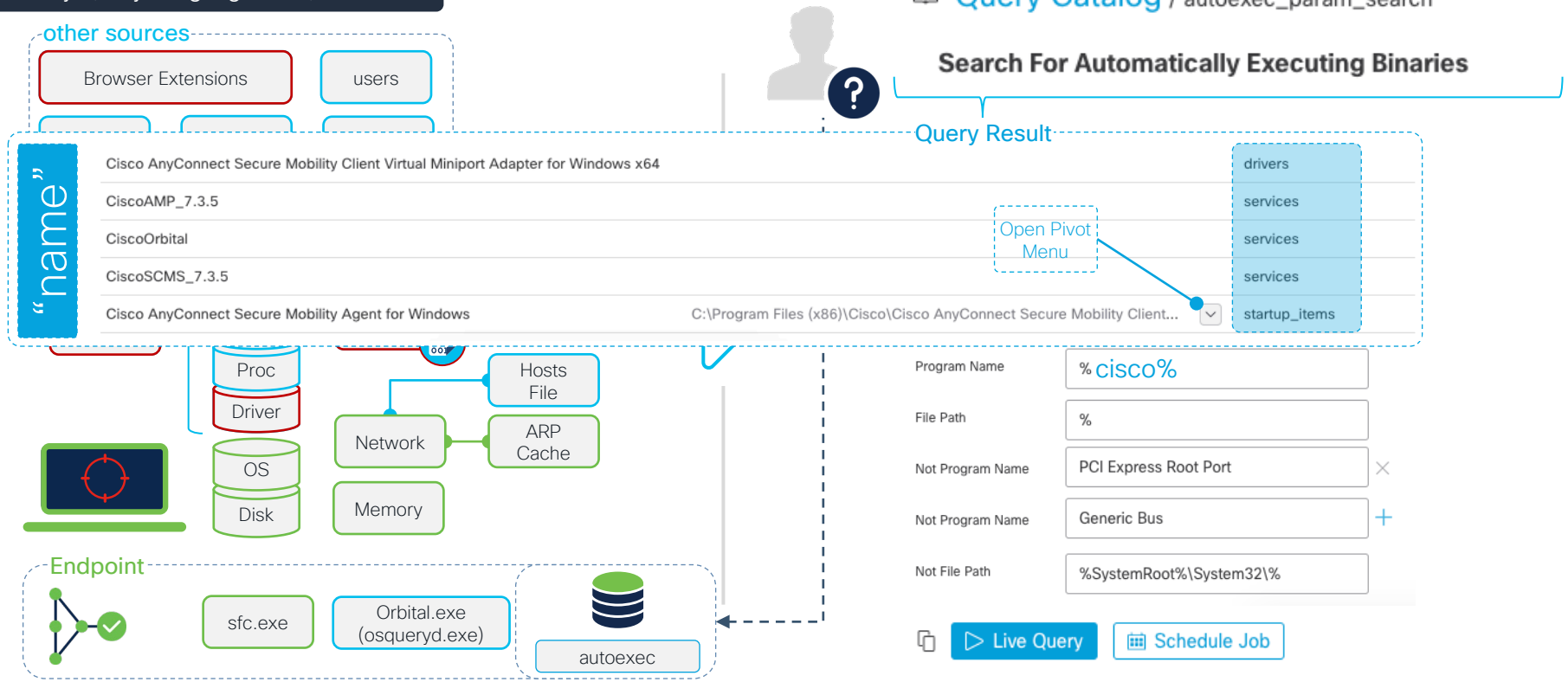
- Endpoint Information Lookup





- Deployment with a single policy setting
- Easy Query Language - SQL

- Endpoint Information Lookup



Deployment with a single policy setting

Easy Query Language - SQL

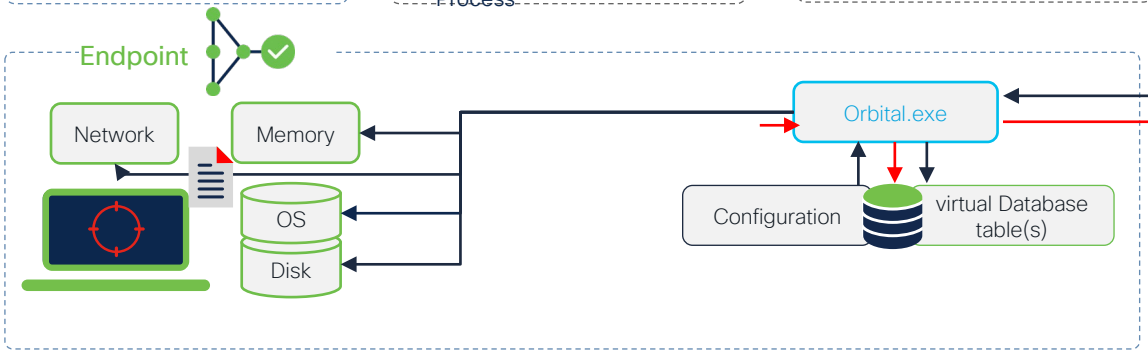
Information Lookup Summary

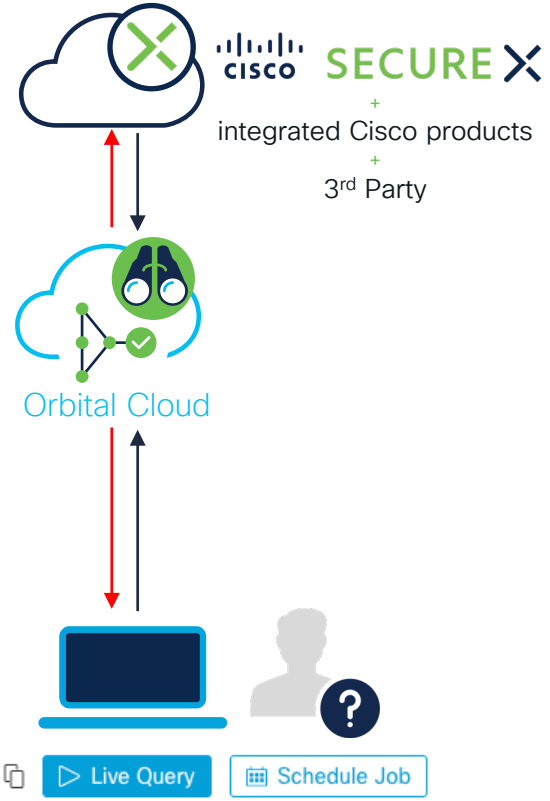
Easy
- installed programs
- running programs
- established network connections
- startup items
- file search
- firewall status

Suspicious Stuff
- Application Shims
- LLMNR Monitoring
- Low Privilege File Associations
- Malware Trickbot Mutex
- Parent Process not Explorer
- Unusual Svchost Parent Process

Custom Query

```
Select column1, column2
from
Orbital_SQ_Table;
```





- Analyst types a SQL statement
- Orbital Cloud gets triggered by a SecureX integrated product or during an Orchestration Workflow
- Orbital.exe generates an empthy virtual table and looks at the configuration behind

- Orbital.exe queries the right information from several sources from the endpoint
- The information is written to the virtual Database(ses) and the SQL statement gets executed

- Orbital Cloud provides the query result to the analyst or to integrated products

cisco Live!

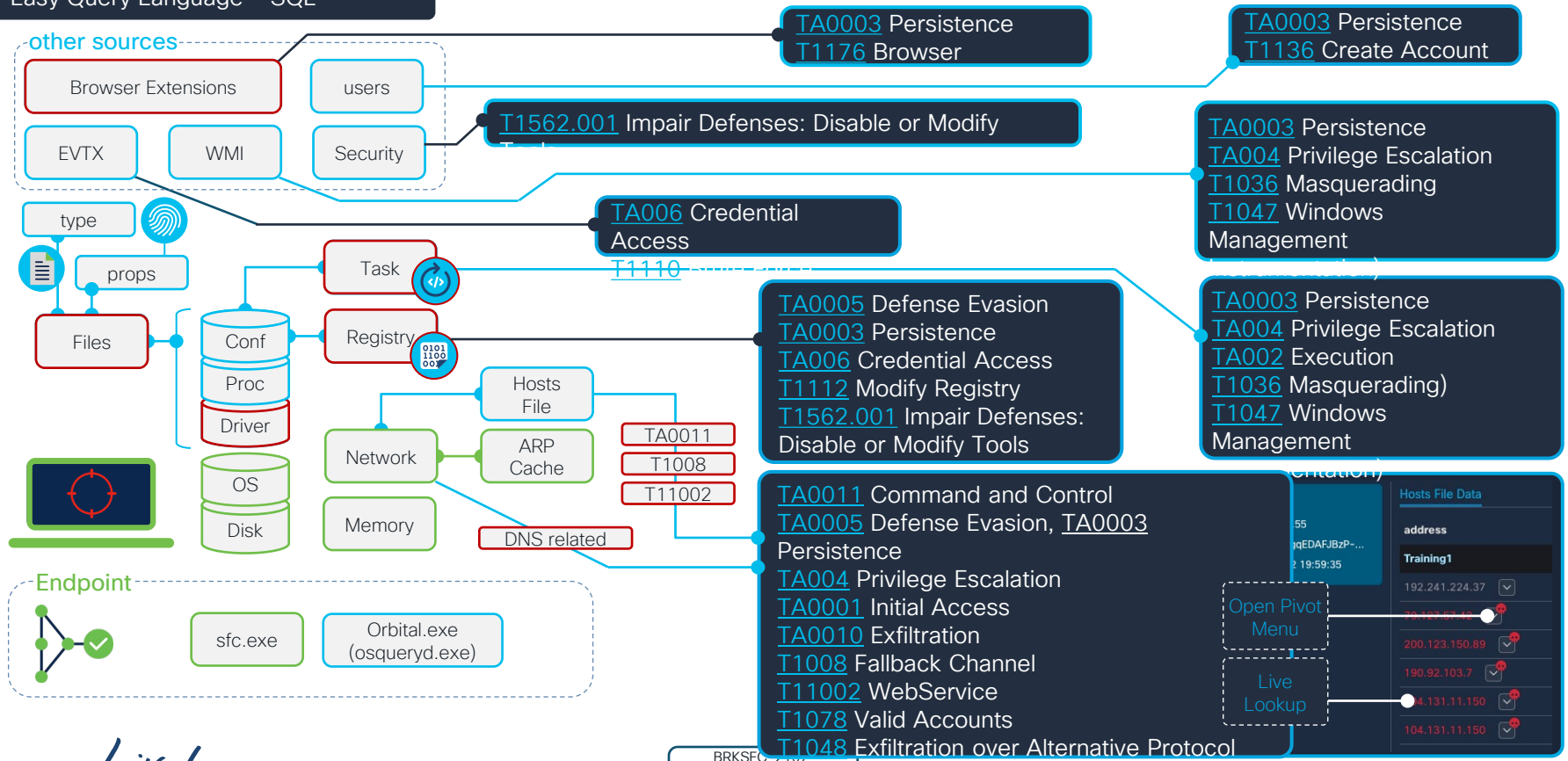
Deployment with a single policy setting

Easy Query Language - SQL

Endpoint Information Lookup

Contextual Information

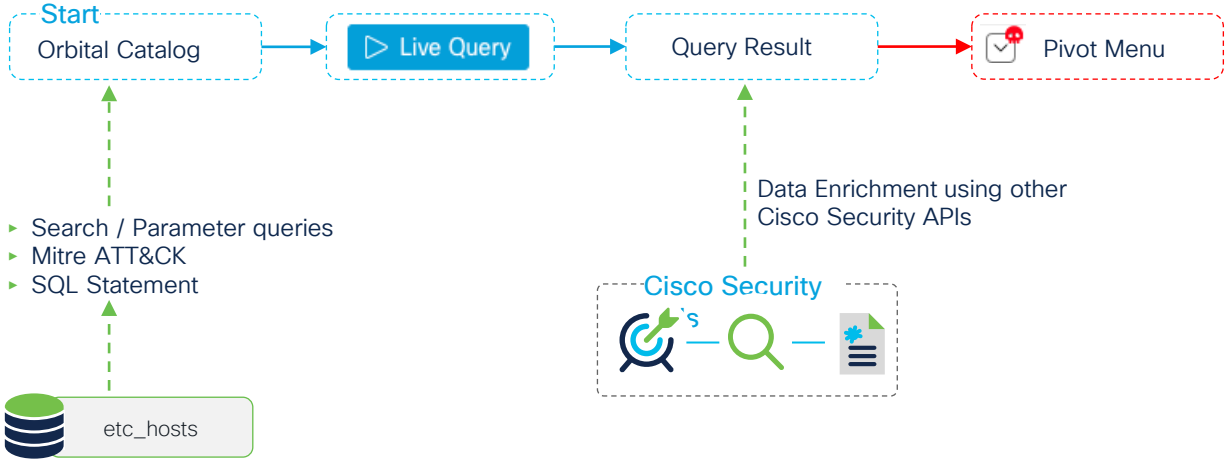
- Mitre Tactique: **TA**x
- Mitre Technique: **T**x



Orbital DEMO

Demo 1:
The Catalog

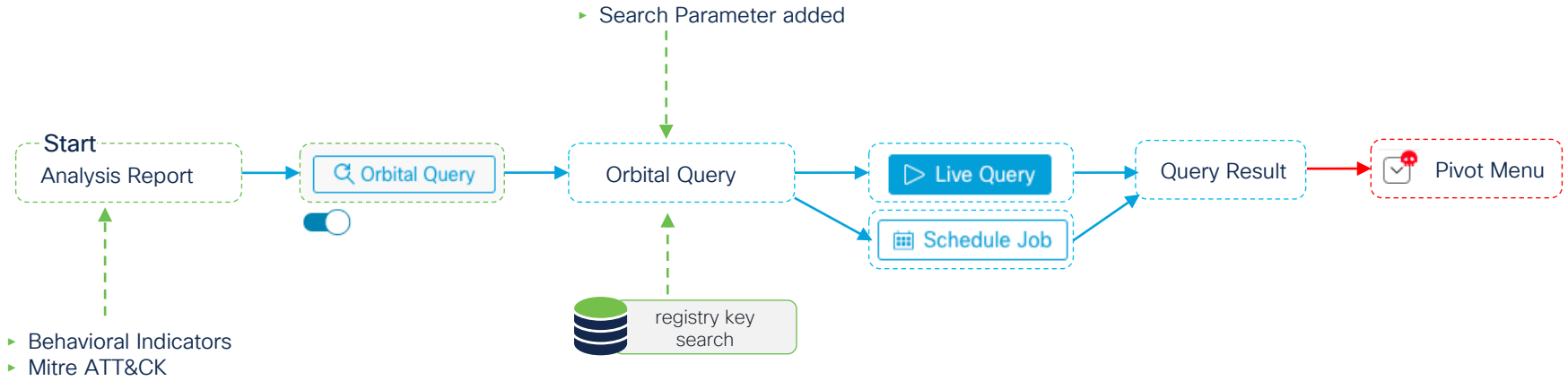
using the Query Catalog



Demo 2:
Analysis Report

cisco Live!

Verify Secure Malware Analytics Sample Report



Demo 3: Endpoint IOC

Relationship between Scheduled Task, Mitre, Cloud IOC and Orbital

Scheduled Task

Action: Start a program
Program: C:\Windows\System32\cmd.exe
Arguments: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -encoded cABpAG4AZwAgAGcAbwBvAGcAbABlAC4AYwBvAG0A

Mitre
TA0005: Defense Evasion
TA0002: Execution
TA0003: Persistence

Windows OS
Scheduled Task
includes
Windows OS
Task Argument
command Line
Cloud IOC
forwarded
Windows OS
Connector SW
monitored

Parameter Search
Orbital Query
Query Result
scheduled_tasks_param_search query
PARAMETERS
Task Name %
Task Action % encoded%

? what triggered the encoded command line included in the Task Action?
? startup_items?

Mitre
T1140 : Deobfuscate/Decode Files or Information

Cloud IOC Command Line

C:\Windows\System32\cmd.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -encoded cABpAG4AZwAgAGcAbwBvAGcAbABlAC4AYwBvAG0A
(Decoded: ping google.com)

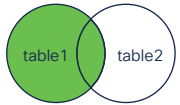
Demo 4: Custom Query (Memory Forensic)

Custom Query

SQL Joins

Available Tables

Custom Query: Which DLLs are loaded into running processes, are they known and how they are signed??

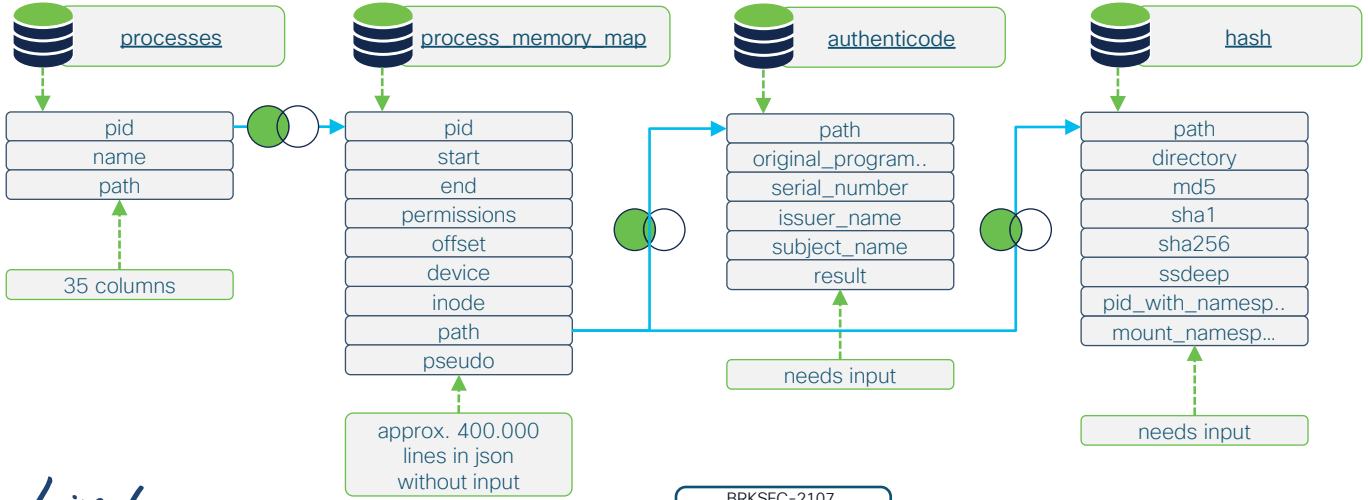


Left Join

- INNER JOIN: Returns records that have matching values in both tables
- LEFT JOIN: Returns all records from the left table, and the matched records from the right table
- Other joins not supported

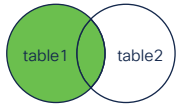
Start
Expand my Toolset

SQL
Generate Statement



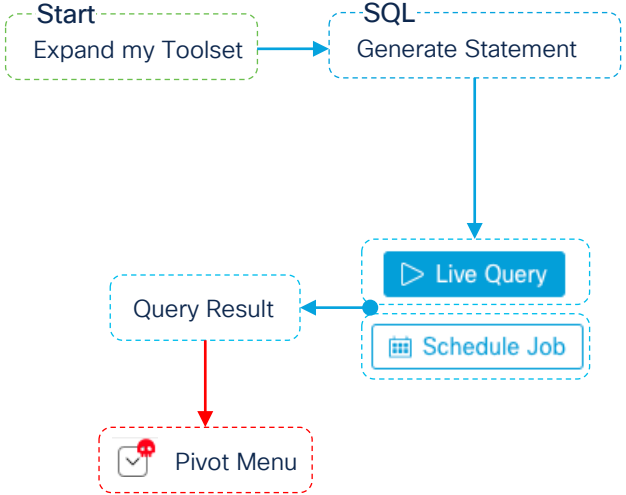
- Custom Query
- SQL Joins
- Available Tables

Custom Query: Which DLLs are loaded into running processes, are they known and how they are signed??



Left Join

- INNER JOIN: Returns records that have matching values in both tables
- LEFT JOIN: Returns all records from the left table, and the matched records from the right table
- Other joins not supported



Do NOT change, will break observable enrichment

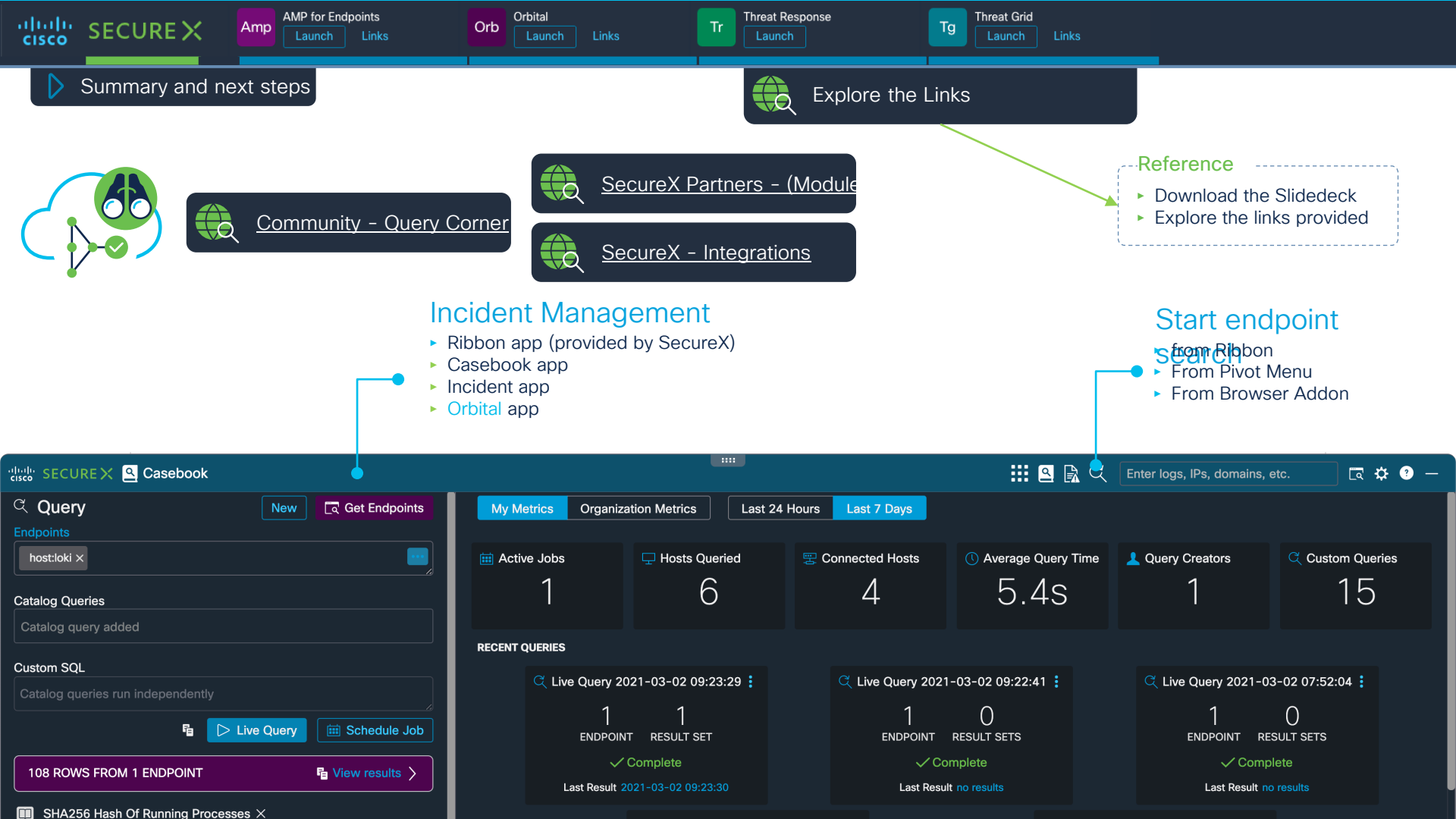
SQL Joins

Customize query
- Path of process
- Path of loaded DLL

```
select DISTINCT p.pid, p.name AS "Process Name",
p.path AS "Process Path",
pm.path AS "DLL-Loaded-path",
sha256,
a.issuer_name AS "DLL-Cert-Issuer_Name",
a.subject_name AS "DLL-Cert-Subject_Name",
a.result
from processes p

LEFT JOIN process_memory_map pm ON p.pid=pm.pid
LEFT JOIN authenticode a ON pm.path = a.path
LEFT JOIN hash h ON h.path=pm.path

-- WHERE p.path LIKE "%:\windows%"
WHERE pm.path != ""
AND pm.path NOT LIKE "%windows\system32%"
AND pm.path LIKE "%.dll"
-- This row can be used to filter for untrusted signing certificates
-- AND a.result NOT LIKE "trusted"
-- AND pm.path like "%cisco%"
-- AND pm.path like "%filezilla%"
ORDER BY p.pid;
```


SECURE X
Amp
AMP for Endpoints
Launch
Links
Orb
Orbital
Launch
Links
Tr
Threat Response
Launch
Tg
Threat Grid
Launch
Links
Summary and next steps
Explore the Links
Reference
Download the Slidedeck
Explore the links provided
Community - Query Corner
SecureX Partners - (Module
SecureX - Integrations
Incident Management
Ribbon app (provided by SecureX)
Casebook app
Incident app
Orbital app
Start endpoint search
from Ribbon
From Pivot Menu
From Browser Addon
SECURE X
Casebook
Enter logs, IPs, domains, etc.
Query
New
Get Endpoints
Endpoints
host:loki
Catalog Queries
Catalog query added
Custom SQL
Catalog queries run independently
Live Query
Schedule Job
108 ROWS FROM 1 ENDPOINT
View results
SHA256 Hash Of Running Processes
My Metrics
Organization Metrics
Last 24 Hours
Last 7 Days
Active Jobs
1
Hosts Queried
6
Connected Hosts
4
Average Query Time
5.4s
Query Creators
1
Custom Queries
15
RECENT QUERIES
Live Query 2021-03-02 09:23:29
1 ENDPOINT
1 RESULT SET
Complete
Last Result 2021-03-02 09:23:30
Live Query 2021-03-02 09:22:41
1 ENDPOINT
0 RESULT SETS
Complete
Last Result no results
Live Query 2021-03-02 07:52:04
1 ENDPOINT
0 RESULT SETS
Complete
Last Result no results

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive