cisco Live!

#CiscoLiveAPJC

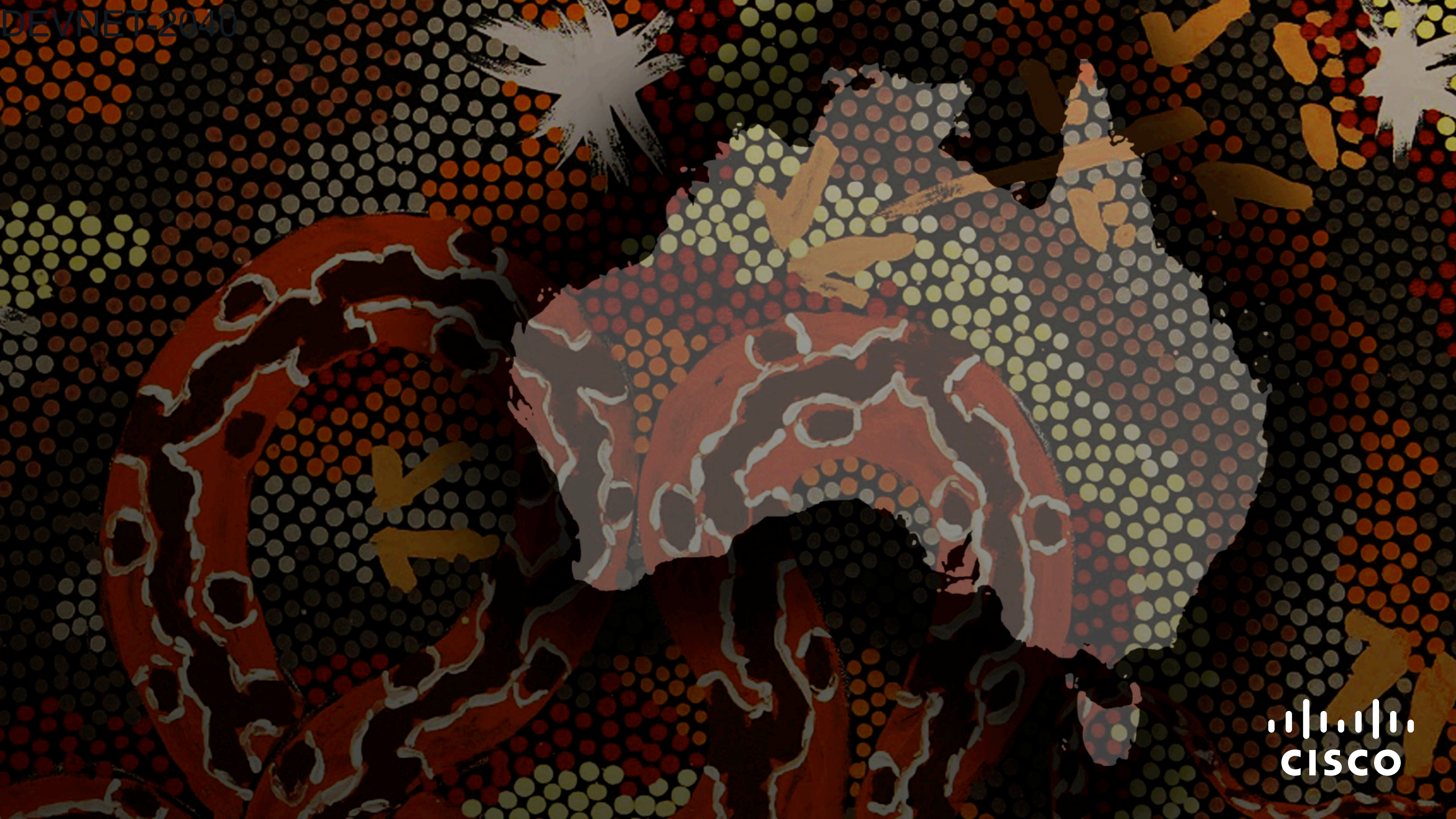
The bridge to possible

Leveraging Cisco Security APIs for Threat Hunting

Based on Automated Alerting and Intel-Driven Detections

Oxana Sannikova, Cybersecurity TSA, GSAT

DEVNET-2040



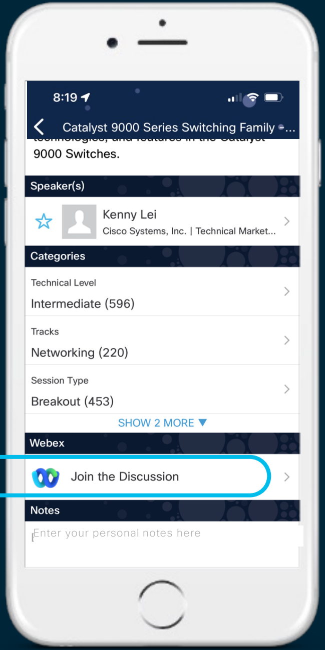
Cisco Webex App

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



8:19

Catalyst 9000 Series Switching Family -...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Webex spaces will be moderated
by the speaker until Thursday 22 December, 2022.

https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2040

A little bit about me

- Work:
  - Global Security Architecture Team
  - 14 years at Cisco, 18 years in security industry
  - Past exp.: Perl, PHP, Network monitoring automation
  - Current coding exp.: Python, Java Script
  - Automation tools: SecureX orchestration
- Play:
  - 7 years in Canada
  - Hobby: urban sketching

GLOBAL SECURITY ARCHITECTURE TEAM
GSAT
SECURING THE WORLD AT EVERY TURN

CISCO
CSAP
FY09
Sales Associates Program

GIAC PYTHON CODER
GPYC

SP
Cisco Security Programmability Team
T

CISCO CERTIFIED
DEVNET
Associate

CISCO CERTIFIED
CCIE
SECURITY

Agenda

- Threat Hunting Maturity
- Automating detection and alerting
- Automating forensics gathering
- Takeaways
- Resources

Threat Hunting Maturity

Common Threat Hunting challenges

Limited Resources

- Shortage of experienced Threat Hunters
- Infrastructure, architecture and methodology

Alert Priority

- Flood of alerts daily
- Difficult to prioritize investigations
- Difficult to identify the source of the threat

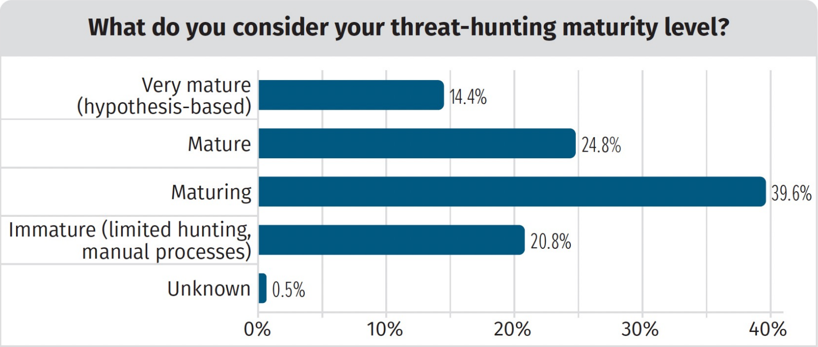
Effective Intel use

- Difficult to operationalize threat intelligence
- Often unreliable and out-of-date

Lack of Internet-wide Threat Visibility

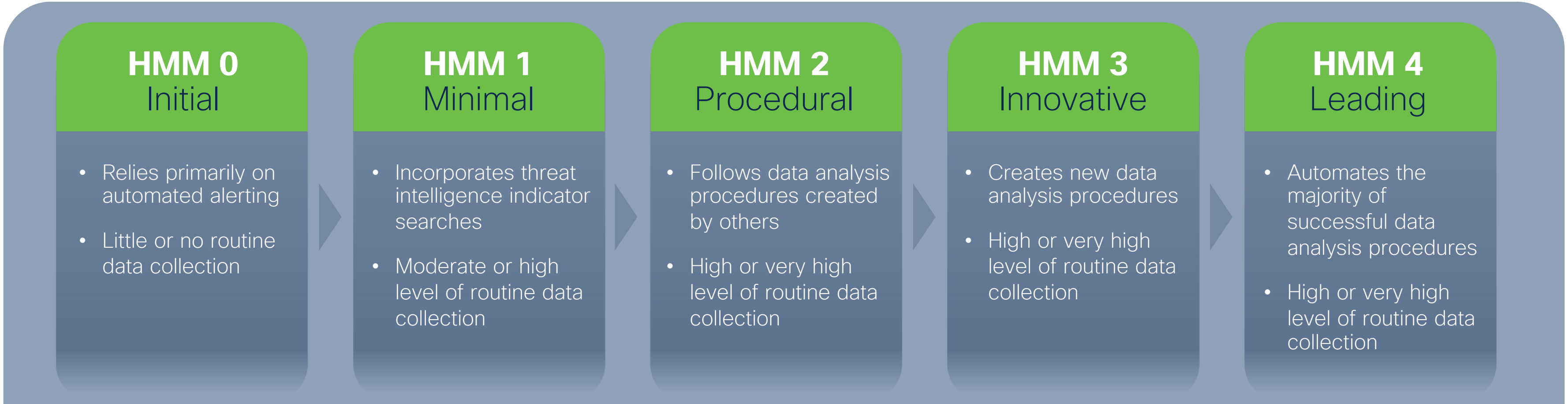
- Identify where attackers stage attacks
- How domains, IPs, ASNs, and malware are connected

Triage
Reactive


What do you consider your threat-hunting maturity level?

*

Hunting
Proactive


HMM 0
Initial

- Relies primarily on automated alerting
- Little or no routine data collection

HMM 1
Minimal

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collection

HMM 2
Procedural

- Follows data analysis procedures created by others
- High or very high level of routine data collection

HMM 3
Innovative

- Creates new data analysis procedures
- High or very high level of routine data collection

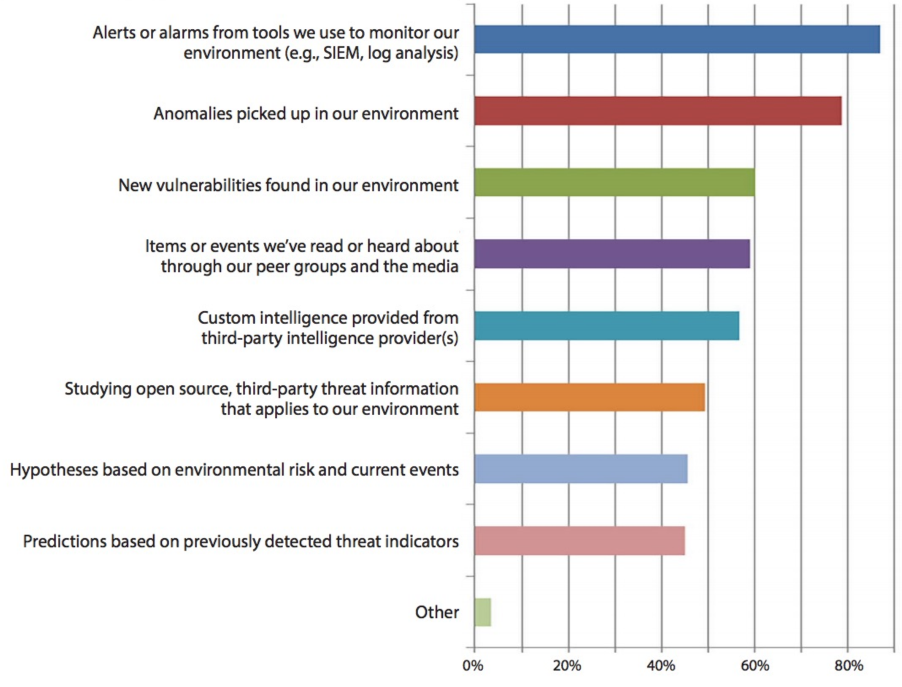
HMM 4
Leading

- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

David Bianco, "A Simple Hunting Maturity Model," Enterprise Detection & Response blog, Oct. 15, 2015,
http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

* https://www.sans.org/white-papers/sans-2021-survey-threat-hunting-uncertain-times/

What Activities Would Initiate an Active Threat Hunt in Your Environment?

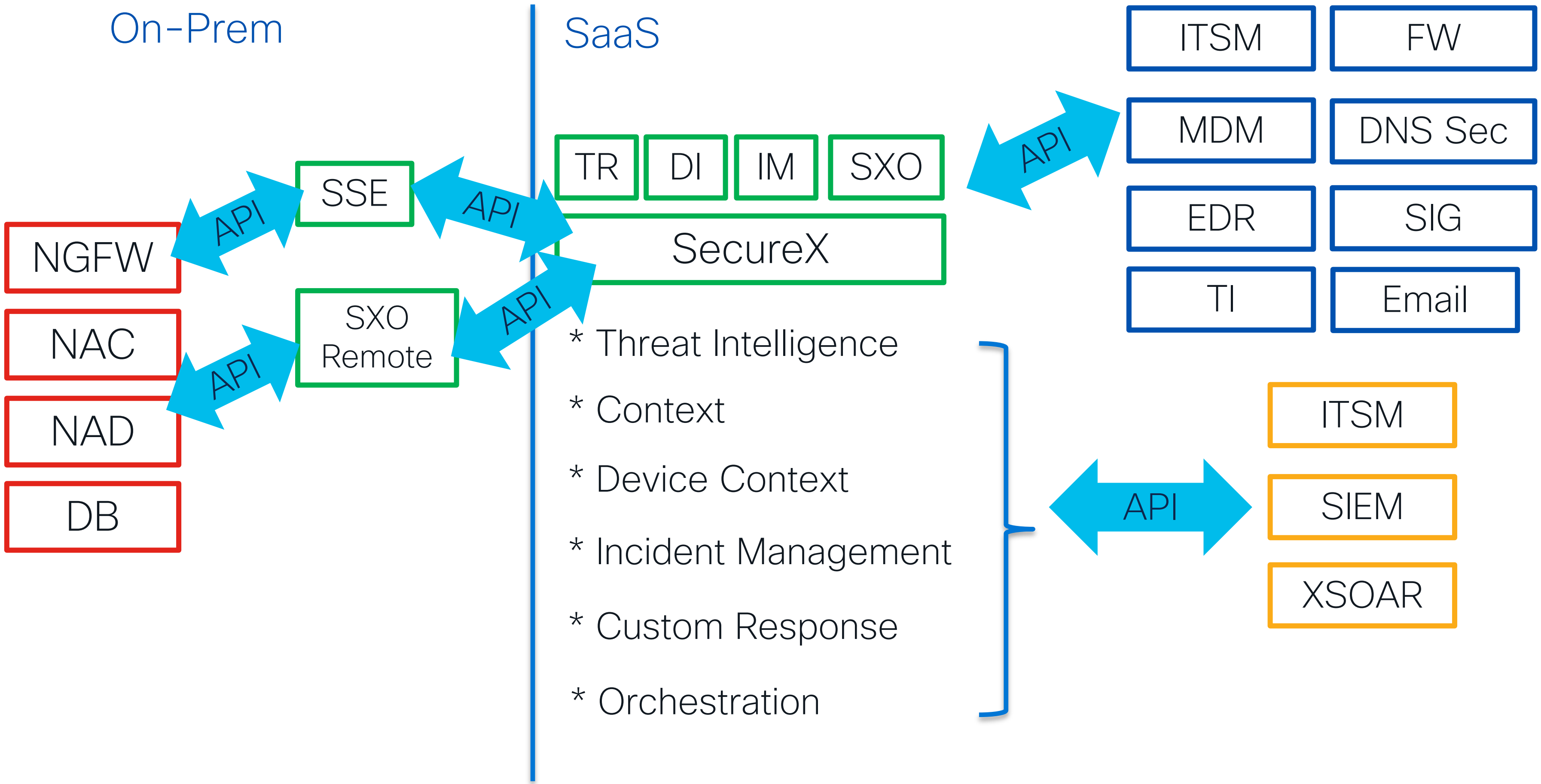


Automation helps to focus on creating a stream of new hunting processes which result in constant improvement of detection processes as a whole.

A Framework for Cyber Threat Hunting by sqrrl

TH based on automated alerting using intel-driven detections

SecureX



On-Prem

SaaS

NGFW

NAC

NAD

DB

API

SSE

API

SXO Remote

API

API

TR

DI

IM

SXO

SecureX

API

ITSM

FW

MDM

DNS Sec

EDR

SIG

TI

Email

* Threat Intelligence

* Context

* Device Context

* Incident Management

* Custom Response

* Orchestration

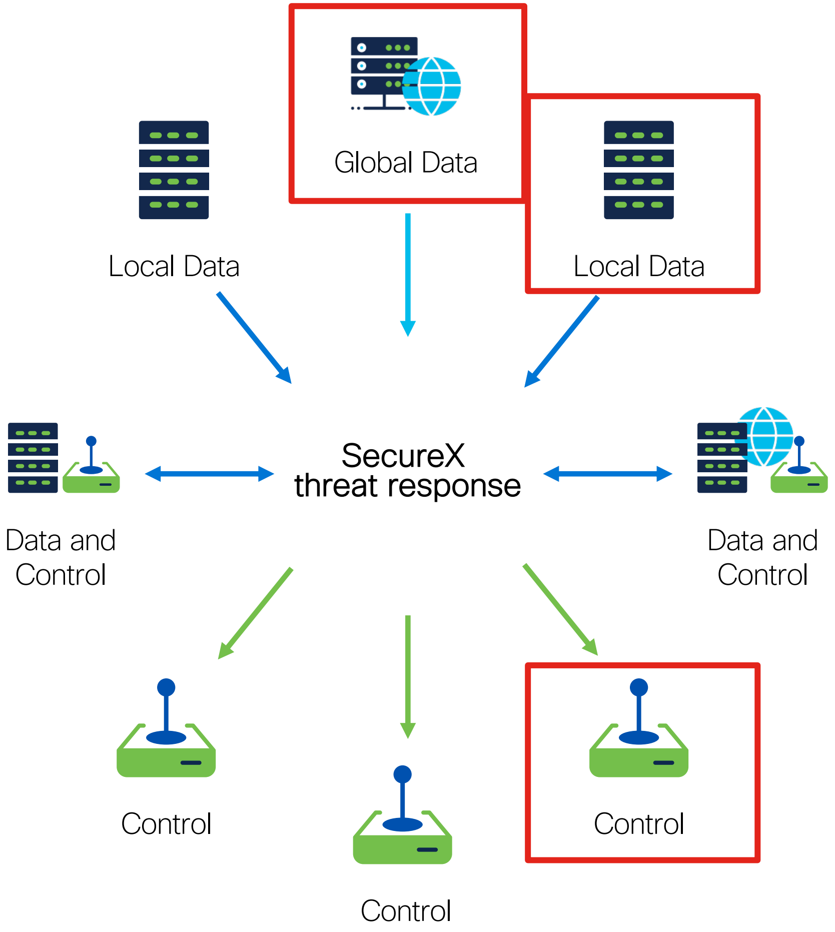
API

ITSM

SIEM

XSOAR

API aggregation at work



SecureX APIs

Inspect	Pull observables out of formatted or unformatted text
Enrich	Search for additional information about those observables. Also contains Refer endpoint for pivoting into other products
Response	Take actions on observables (for example, add to blocklist).
OAuth	Use credentials and get access tokens.
Global Intel	Read global threat intelligence.
Private Intel	Read and write user-provided threat intelligence. Used by the Incident Manager. This API can be used to add 3rd Party data in Threat Response

DEMO: OpenPhish URLs to SecureX Threat Intelligence Feeds and Umbrella Destinations Lists

Scenario

CISCO SECURE X

ORCHESTRATION

THREAT RESPONSE

Umbrella

DUO

NGFW

Gather OSINT

- Pull OpenPhish phishing URL feed every 24 hours

DELIBERATE

- Check each URL disposition withing SecureX Global Intelligence DB

CREATE JUDGEMENT

- If disposition is Unknown, create new Judgement in Private Intelligence DB

ADD TO FEED

- Link Judgement to indicator which is attached to the feed

ADD TO UMBRELLA

- Add URL to Umbrella Destination block list which is attached to DNS policy

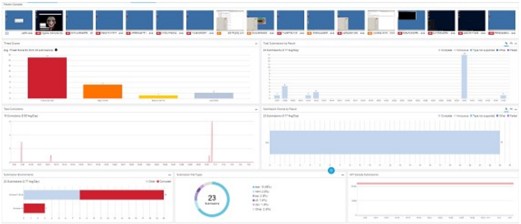
Secure Malware Analytics

Secure Malware Analytics API Use Cases

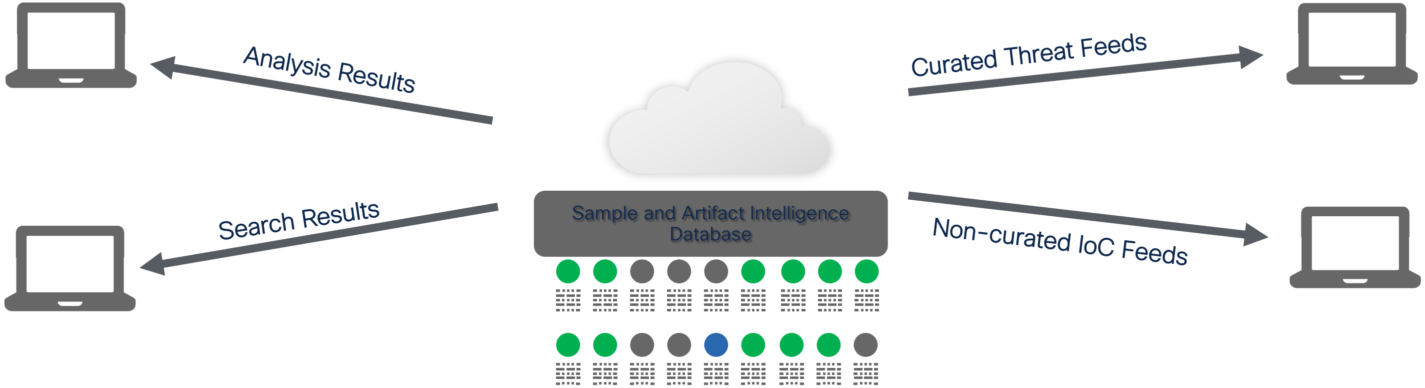
- Query Malware Intelligence
- Retrieve Curated Intelligence Feeds
- Sample Analysis Collection
- Submit Samples for Analysis
- Usage Statistics and Data

Secure Malware Analytics API

Malware Analysis & Threat Intelligence



Threat Intelligence: Delivery



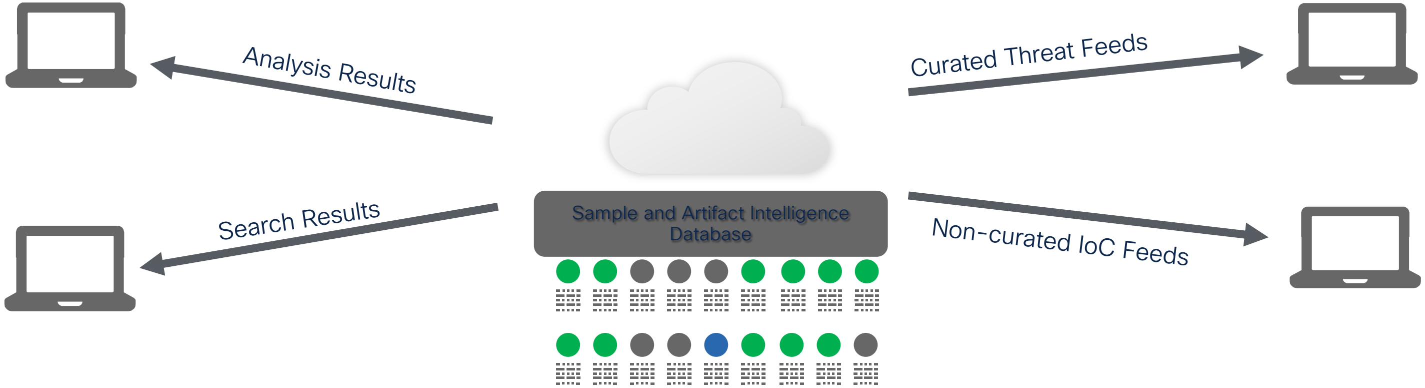
Analysis and Search Results

- User, org, or global analysis results per sample
- Search across samples for key elements
- Download artifacts, pcaps, etc

Threat Intel Data Feeds

- Threat feeds with context / metadata
- Create custom feeds or download 15 curated batch feeds
- Various formats (JSON, STIX, CSV, Snort)

Threat Intelligence: Delivery



Analysis and Search Results

- User, org, or global analysis results per sample
- Search across samples for key elements
- Download artifacts, pcaps, etc

Threat Intel Data Feeds

- Threat feeds with context / metadata
- Create custom feeds or download 16 curated batch feeds
- Various formats (JSON, STIX, CSV, Snort)

Secure Malware Analytics APIs

Feed details summary:

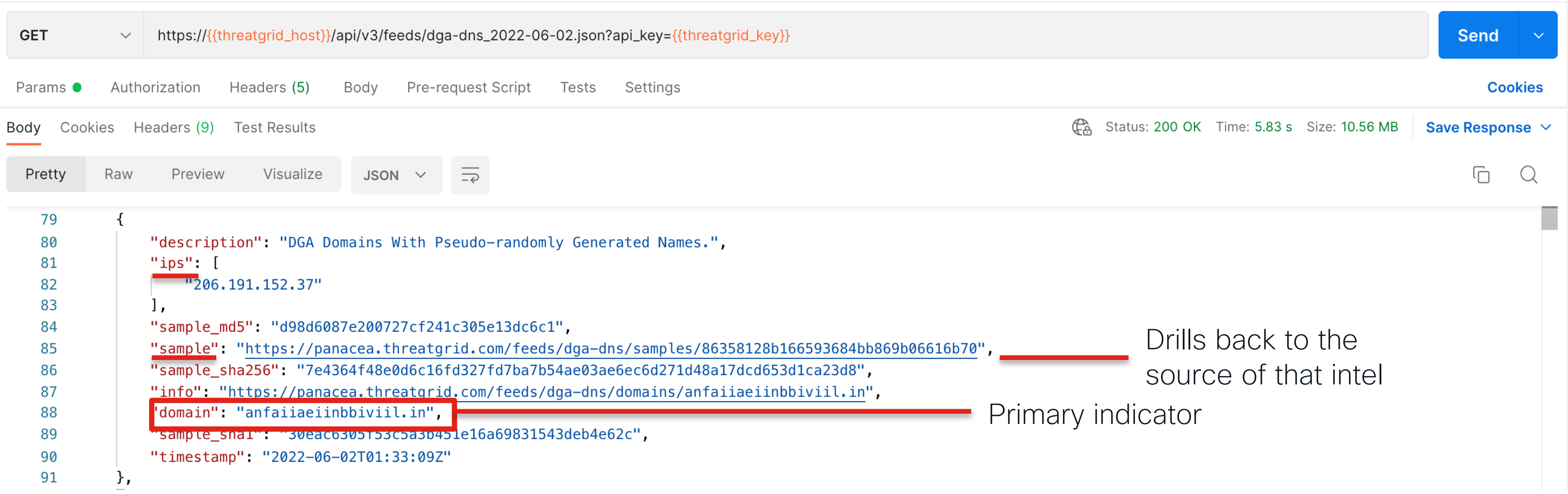
	Sample Feeds	IOC feeds	Curated Feeds
Version	/v2	/v2	/v3
Endpoint	/samples/feeds/	/iocs/feeds/	/feeds/
Content	All observables seen	Observables seen in all BIs	Observables seen as part of a trusted high confidence BI triggering
FP rate*	High	Medium	Low
Pre-whitelisted	No	No	Yes
Filterable to only you/org?	Yes	Yes	No
Output Formats	JSON	JSON	JSON/CSV/Snort/STIX**
Request Complexity	Low	Low	Lowest

* The factual FP rate is 0; these were all seen. The functional FP rate, as an indicator of local compromise, is dependent on the details of the observation and varies from feed to feed.

** additional formats not available for all curated feeds

EXAMPLE: Working with Secure Malware Analytics Curated Feeds & Analysis Reports

Working with Secure Malware Analytics Curated Feeds



https://{{threatgrid_host}}/api/v3/feeds/dga-dns_2022-06-02.json?api_key={{threatgrid_key}}

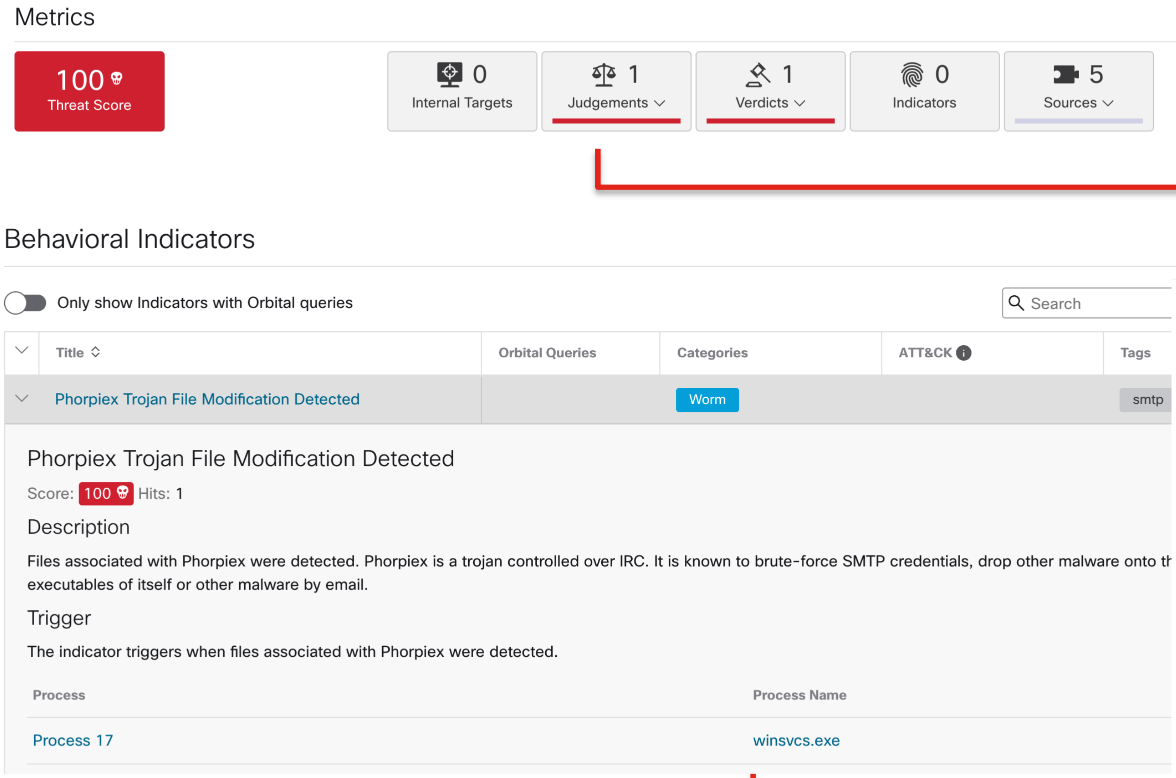
Status: 200 OK Time: 5.83 s Size: 10.56 MB

```
    {
        "description": "DGA Domains With Pseudo-randomly Generated Names.",
        "ips": [
            "206.191.152.37"
        ],
        "sample_md5": "d98d6087e200727cf241c305e13dc6c1",
        "sample": "https://panacea.threatgrid.com/feeds/dga-dns/samples/86358128b166593684bb869b06616b70",
        "sample_sha256": "7e4364f48e0d6c16fd327fd7ba7b54ae03ae6ec6d271d48a17dcd653d1ca23d8",
        "info": "https://panacea.threatgrid.com/feeds/dga-dns/domains/anfaiiaeiinbbiviil.in",
        "domain": "anfaiiaeiinbbiviil.in",
        "sample_sha1": "30eac6305f53c5a3b451e16a69831543deb4e62c",
        "timestamp": "2022-06-02T01:33:09Z"
    },
```

Drills back to the source of that intel

Primary indicator

Secure Malware Analytics Curated Feeds



Metrics

100 Threat Score

0	1	1	0	5
Internal Targets	Judgements ⌵	Verdicts ⌵	Indicators	Sources ⌵

Behavioral Indicators

○ Only show Indicators with Orbital queries

Search

Title	Orbital Queries	Categories	ATT&CK	Tags
Phorpiex Trojan File Modification Detected		Worm		smtp

Phorpiex Trojan File Modification Detected

Score: 100 Hits: 1

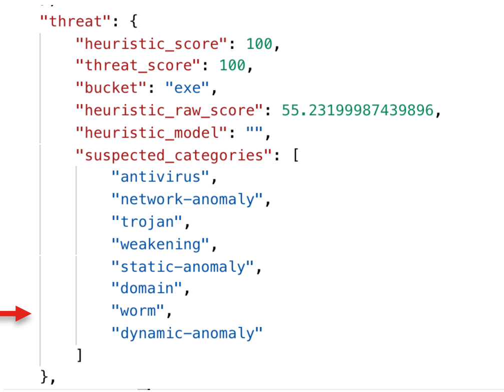
Description

Files associated with Phorpiex were detected. Phorpiex is a trojan controlled over IRC. It is known to brute-force SMTP credentials, drop other malware onto th executables of itself or other malware by email.

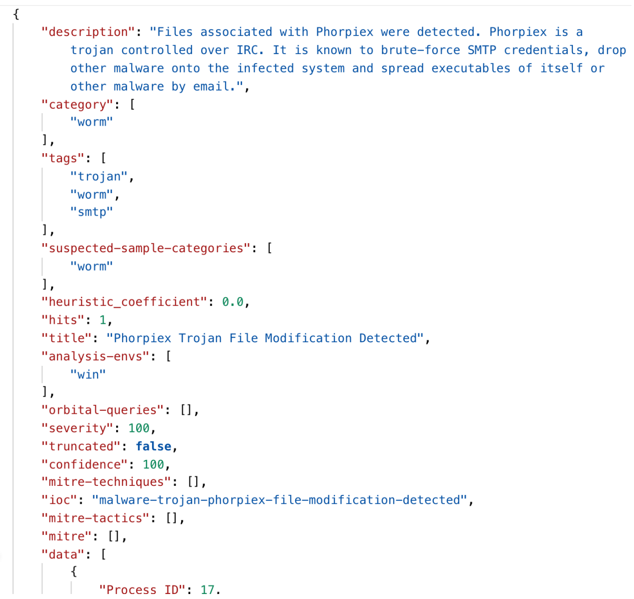
Trigger

The indicator triggers when files associated with Phorpiex were detected.

Process	Process Name
Process 17	winsvcs.exe



```
"threat": {
    "heuristic_score": 100,
    "threat_score": 100,
    "bucket": "exe",
    "heuristic_raw_score": 55.23199987439896,
    "heuristic_model": "",
    "suspected_categories": [
        "antivirus",
        "network-anomaly",
        "trojan",
        "weakening",
        "static-anomaly",
        "domain",
        "worm",
        "dynamic-anomaly"
    ]
},
```



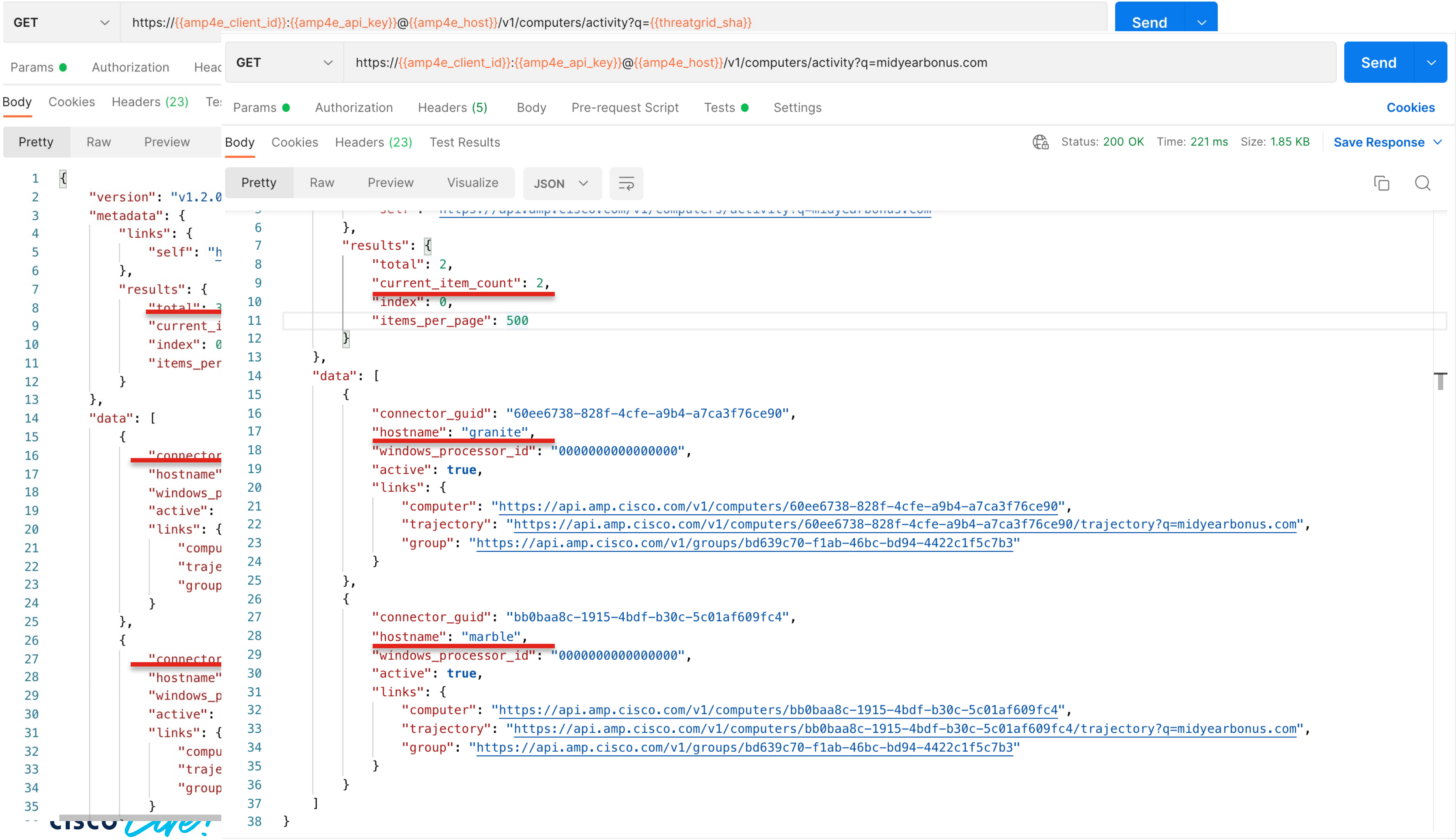
```
{
    "description": "Files associated with Phorpiex were detected. Phorpiex is a
        trojan controlled over IRC. It is known to brute-force SMTP credentials, drop
        other malware onto the infected system and spread executables of itself or
        other malware by email.",
    "category": [
        "worm"
    ],
    "tags": [
        "trojan",
        "worm",
        "smtp"
    ],
    "suspected-sample-categories": [
        "worm"
    ],
    "heuristic_coefficient": 0.0,
    "hits": 1,
    "title": "Phorpiex Trojan File Modification Detected",
    "analysis-envs": [
        "win"
    ],
    "orbital-queries": [],
    "severity": 100,
    "truncated": false,
    "confidence": 100,
    "mitre-techniques": [],
    "ioc": "malware-trojan-phorpiex-file-modification-detected",
    "mitre-tactics": [],
    "mitre": [],
    "data": [
        {
            "Process ID": 17,
```

Automated forensics gathering

Cisco Secure Endpoint

Cisco Secure Endpoint use cases

- GET /v1/computers/activity
  - Provides you with the ability to search all computers across your organization for any events or activities associated with a file or network operation, and returns computers matching that criteria.
  - This endpoint requires a q parameter which is a freeform query string. It currently accepts:
    - an IPv4 address: 1.0.0.0
    - a SHA256
    - a filename
    - a URL fragment
  - There is a hard limit of 5000 historical entries searched for this endpoint.



GET https://{{amp4e_client_id}}:{{amp4e_api_key}}@{{amp4e_host}}/v1/computers/activity?q={{threatgrid_sha}}

```
{
    "version": "v1.2.0
    "metadata": {
        "links": {
            "self": "h
        },
        "results": {
            "total": 3
            "current_i
            "index": 0
            "items_per
        }
    },
    "data": [
        {
            "connector
            "hostname"
            "windows_p
            "active":
            "links": {
                "compu
                "traje
                "group
            }
        },
        {
            "connector
            "hostname"
            "windows_p
            "active":
            "links": {
                "compu
                "traje
                "group
            }
```

GET https://{{amp4e_client_id}}:{{amp4e_api_key}}@{{amp4e_host}}/v1/computers/activity?q=midyearbonus.com

Status: 200 OK Time: 221 ms Size: 1.85 KB

```
            "self": "https://api.amp.cisco.com/v1/computers/activity?q=midyearbonus.com"
        },
        "results": {
            "total": 2,
            "current_item_count": 2,
            "index": 0,
            "items_per_page": 500
        }
    },
    "data": [
        {
            "connector_guid": "60ee6738-828f-4cfe-a9b4-a7ca3f76ce90",
            "hostname": "granite",
            "windows_processor_id": "0000000000000000",
            "active": true,
            "links": {
                "computer": "https://api.amp.cisco.com/v1/computers/60ee6738-828f-4cfe-a9b4-a7ca3f76ce90",
                "trajectory": "https://api.amp.cisco.com/v1/computers/60ee6738-828f-4cfe-a9b4-a7ca3f76ce90/trajectory?q=midyearbonus.com",
                "group": "https://api.amp.cisco.com/v1/groups/bd639c70-f1ab-46bc-bd94-4422c1f5c7b3"
            }
        },
        {
            "connector_guid": "bb0baa8c-1915-4bdf-b30c-5c01af609fc4",
            "hostname": "marble",
            "windows_processor_id": "0000000000000000",
            "active": true,
            "links": {
                "computer": "https://api.amp.cisco.com/v1/computers/bb0baa8c-1915-4bdf-b30c-5c01af609fc4",
                "trajectory": "https://api.amp.cisco.com/v1/computers/bb0baa8c-1915-4bdf-b30c-5c01af609fc4/trajectory?q=midyearbonus.com",
                "group": "https://api.amp.cisco.com/v1/groups/bd639c70-f1ab-46bc-bd94-4422c1f5c7b3"
            }
        }
    ]
}
```

Cisco Secure Endpoint API use cases

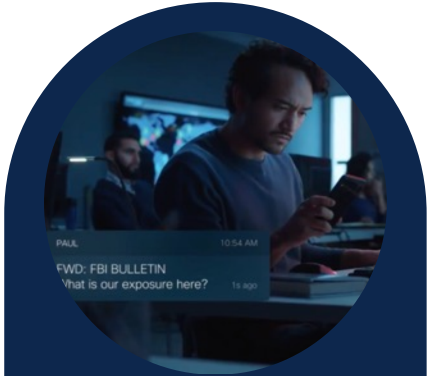
- GET /v1/vulnerabilities
  - This is a general query interface for vulnerabilities. This is analogous to the Vulnerable Software view on the Cisco Secure Endpoints Console.
  - The list item contains a summary of information on the vulnerability, including: application name and version, SHA-256 value for the executable file, Connectors on which the vulnerable application was observed, the most recent CVSS score.
- GET /v1/vulnerabilities/{:sha256}/computers
  - Provides a list of computers on which the vulnerability has been observed with given SHA-256.
- GET /v1/computers/{:connector_guid}/vulnerabilities
  - Provides a list of vulnerabilities observed on a specific computer.

Cisco Secure Endpoint API use cases – cont.

- GET /v1/computers/{:connector_guid}/trajectory
  - Provides list of all activities associated with a particular computer. This is analogous to the Device Trajectory on the Cisco Secure Console.
- GET /v1/computers/{:connector_guid}/user_trajectory
  - Fetch a specific computer's trajectory with given connector_guid and filter for events with user name activity
- GET /v1/app_trajectory/queries
  - Retrieves app_trajectory queries for a given ios bundle id.

Relentless Breach Defense

Orbital Advanced Search
Use Cases



Threat Hunting

Search for malicious artifacts in near real-time to accelerate your hunt for threats.

Incident Investigation

Get to the root cause of the incident fast, to speed up remediation.

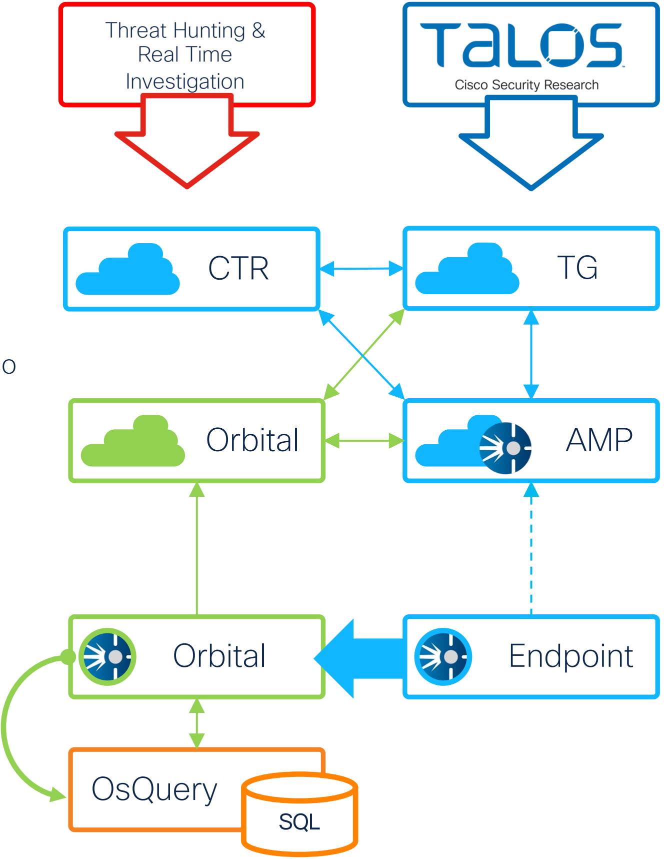
Vulnerability and Compliance

Check system status (OS versions, patches etc.), ensuring hosts comply with policies.

IT Operations

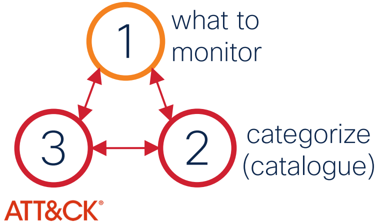
Track disk space, memory, and other IT operations artifacts quickly.

Orbital Advanced Search - Architecture



Query Catalog managed by Cisco includes predefined queries

ATT&CK® linked to queries (catalogue)



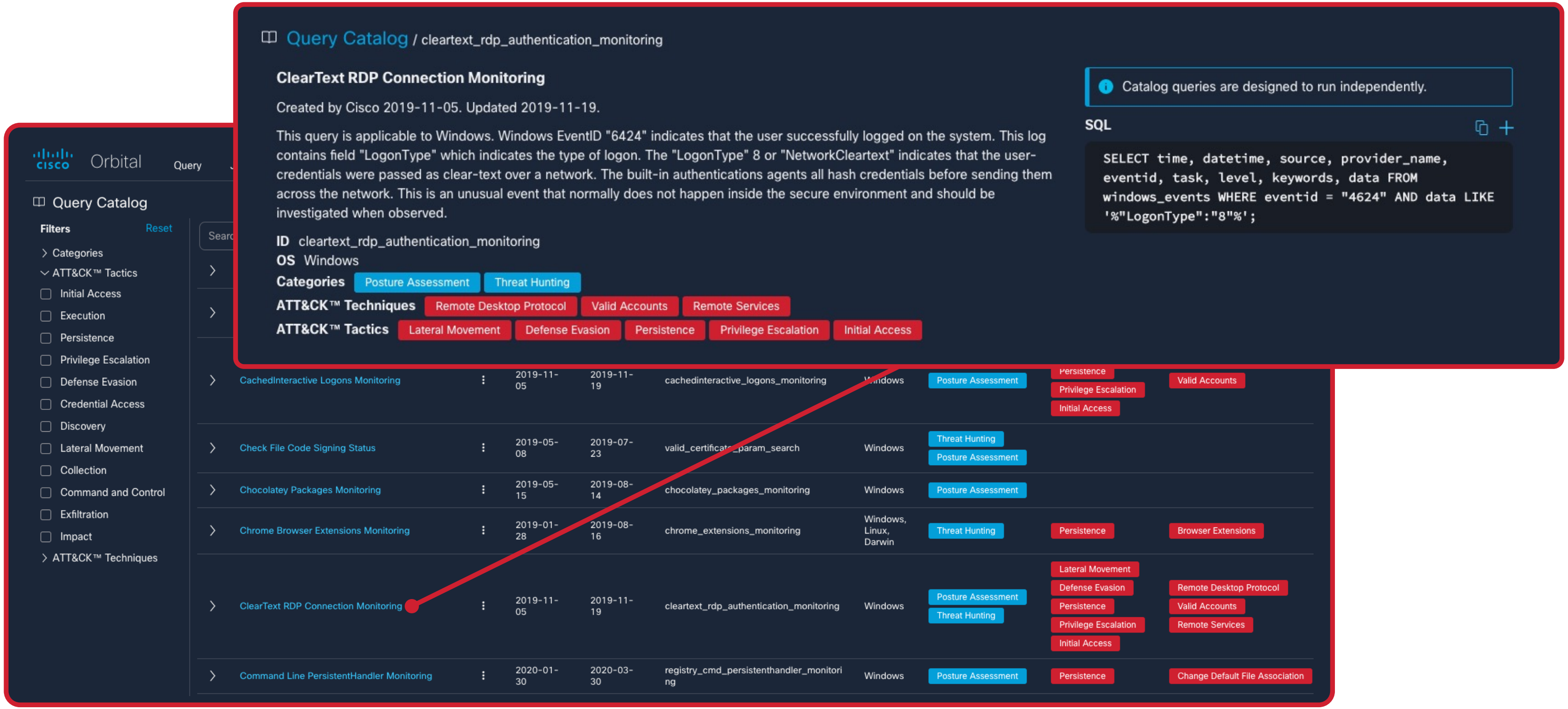
Easy Examples

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

Sophisticated Examples

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

Orbital Advanced Search – Query Catalog



Query Catalog / cleartext_rdp_authentication_monitoring

ClearText RDP Connection Monitoring

Created by Cisco 2019-11-05. Updated 2019-11-19.

This query is applicable to Windows. Windows EventID "6424" indicates that the user successfully logged on the system. This log contains field "LogonType" which indicates the type of logon. The "LogonType" 8 or "NetworkCleartext" indicates that the user-credentials were passed as clear-text over a network. The built-in authentications agents all hash credentials before sending them across the network. This is an unusual event that normally does not happen inside the secure environment and should be investigated when observed.

ID cleartext_rdp_authentication_monitoring
OS Windows
Categories Posture Assessment | Threat Hunting
ATT&CK™ Techniques Remote Desktop Protocol | Valid Accounts | Remote Services
ATT&CK™ Tactics Lateral Movement | Defense Evasion | Persistence | Privilege Escalation | Initial Access

Catalog queries are designed to run independently.

SQL

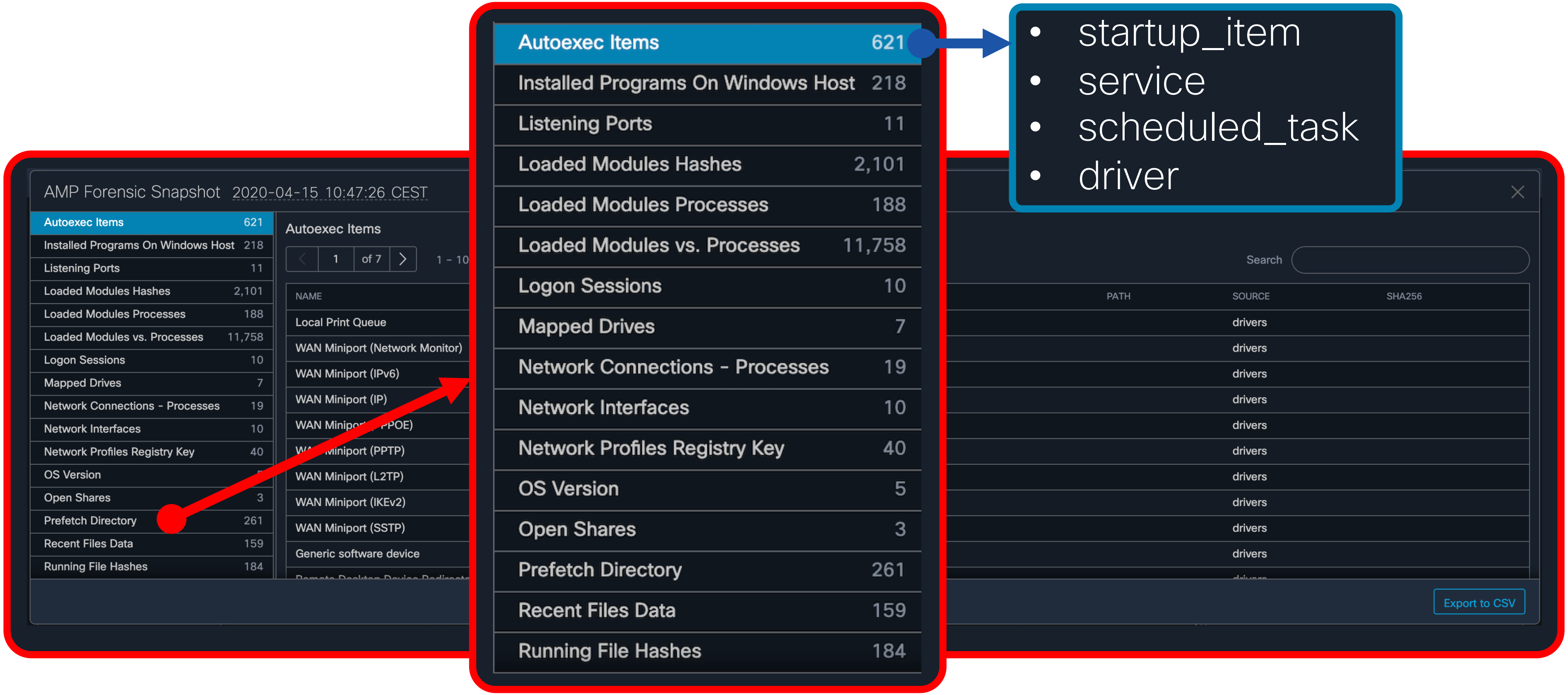
```
SELECT time, datetime, source, provider_name,
eventid, task, level, keywords, data FROM
windows_events WHERE eventid = "4624" AND data LIKE
'%"LogonType":"8"%';
```

CachedInteractive Logons Monitoring	2019-11-05	2019-11-19	cachedinteractive_logons_monitoring	Windows	Posture Assessment	Persistence Privilege Escalation Initial Access	Valid Accounts
Check File Code Signing Status	2019-05-08	2019-07-23	valid_certificate_param_search	Windows	Threat Hunting Posture Assessment		
Chocolatey Packages Monitoring	2019-05-15	2019-08-14	chocolatey_packages_monitoring	Windows	Posture Assessment		
Chrome Browser Extensions Monitoring	2019-01-28	2019-08-16	chrome_extensions_monitoring	Windows, Linux, Darwin	Threat Hunting	Persistence	Browser Extensions
ClearText RDP Connection Monitoring	2019-11-05	2019-11-19	cleartext_rdp_authentication_monitoring	Windows	Posture Assessment Threat Hunting	Lateral Movement Defense Evasion Persistence Privilege Escalation Initial Access	Remote Desktop Protocol Valid Accounts Remote Services
Command Line PersistentHandler Monitoring	2020-01-30	2020-03-30	registry_cmd_persistenthandler_monitoring	Windows	Posture Assessment	Persistence	Change Default File Association

Orbital APIs

- Query API - This API requests scheduling a query and returns a job object that provides information needed to collect results.
- Results API - This API collects results from Orbital from a query created either by the Orbital User Interface, your applications or the Query API. Orbital will provide results as soon as they are received from a node, and will retain them for at least 24 hours but no longer than 48 hours.

Orbital Advanced Search – Forensic Snapshot Details



AMP Forensic Snapshot 2020-04-15 10:47:26 CEST

Autoexec Items	621
Installed Programs On Windows Host	218
Listening Ports	11
Loaded Modules Hashes	2,101
Loaded Modules Processes	188
Loaded Modules vs. Processes	11,758
Logon Sessions	10
Mapped Drives	7
Network Connections - Processes	19
Network Interfaces	10
Network Profiles Registry Key	40
OS Version	
Open Shares	3
Prefetch Directory	261
Recent Files Data	159
Running File Hashes	184

Autoexec Items

NAME	PATH	SOURCE	SHA256
Local Print Queue		drivers	
WAN Miniport (Network Monitor)		drivers	
WAN Miniport (IPv6)		drivers	
WAN Miniport (IP)		drivers	
WAN Miniport (PPPOE)		drivers	
WAN Miniport (PPTP)		drivers	
WAN Miniport (L2TP)		drivers	
WAN Miniport (IKEv2)		drivers	
WAN Miniport (SSTP)		drivers	
Generic software device		drivers	
Remote Desktop Device Redirecto		drivers	

Autoexec Items	621
Installed Programs On Windows Host	218
Listening Ports	11
Loaded Modules Hashes	2,101
Loaded Modules Processes	188
Loaded Modules vs. Processes	11,758
Logon Sessions	10
Mapped Drives	7
Network Connections - Processes	19
Network Interfaces	10
Network Profiles Registry Key	40
OS Version	5
Open Shares	3
Prefetch Directory	261
Recent Files Data	159
Running File Hashes	184

- startup_item
- service
- scheduled_task
- driver

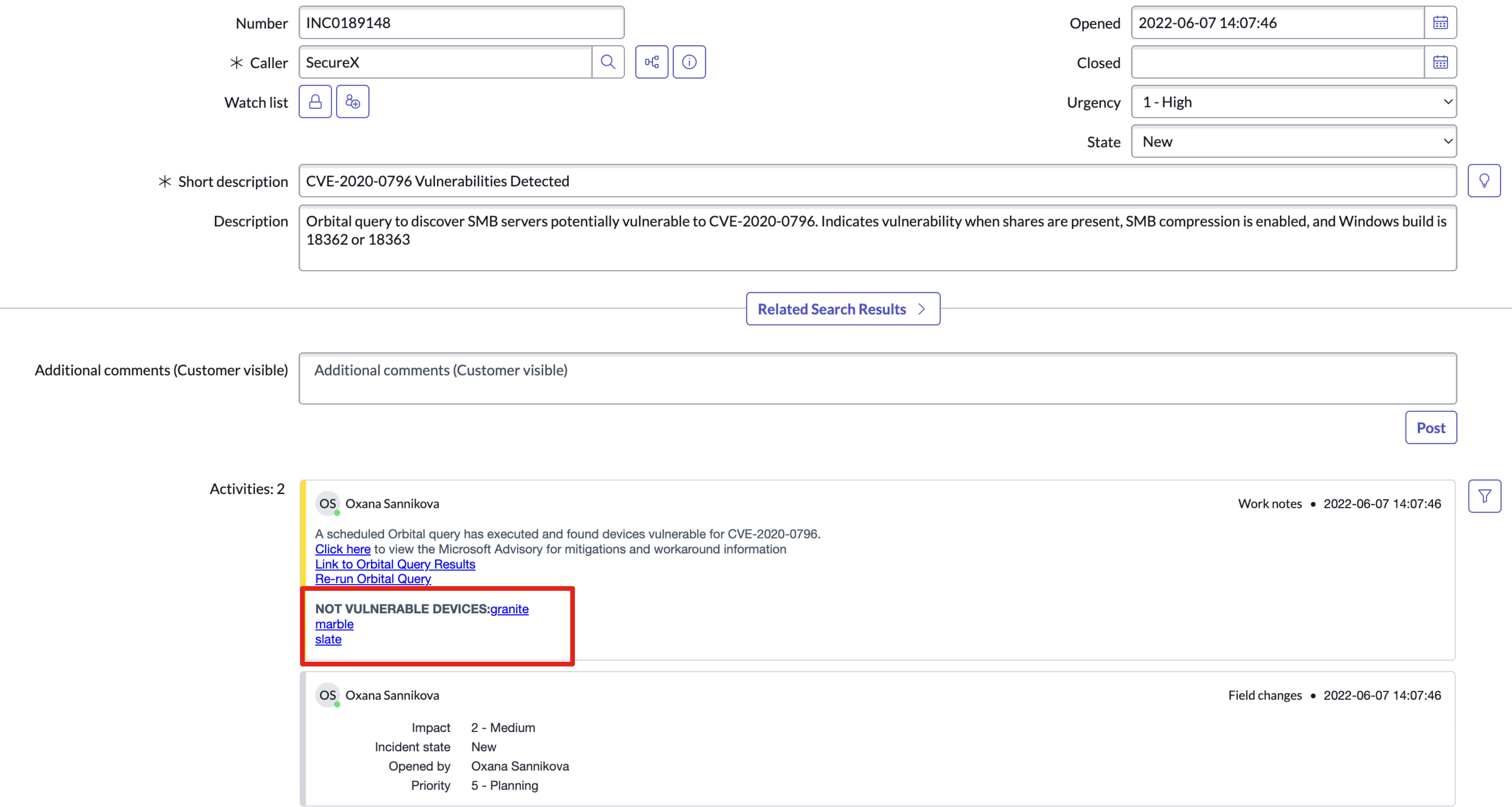
Orbital Advanced Search

Forensic Snapshot Advantages

- Includes information commonly extracted from a full memory snapshot
- It is very small in size, just text
- Can be fully automated using Automated Actions
- Snapshot events are shown in the Device Trajectory
- Orbital Jobs allow for regularly scheduled queries
- Fully automated, even for off-network endpoints
- Multiple Snapshots can be stored per endpoint
- Forensic Snapshot information is available within minutes in the AMP Console (for online endpoints).

Example: Orbital CVE Hunt to ServiceNow incident

https://ciscosecurity.github.io/sxo-05-security-workflows/workflows/orbital/0009-cve-hunt-to-servicenow



Number INC0189148

✱ Caller SecureX

Watch list

Opened 2022-06-07 14:07:46

Closed

Urgency 1 - High

State New

✱ Short description CVE-2020-0796 Vulnerabilities Detected

Description Orbital query to discover SMB servers potentially vulnerable to CVE-2020-0796. Indicates vulnerability when shares are present, SMB compression is enabled, and Windows build is 18362 or 18363

Additional comments (Customer visible)

Activities: 2

OS Oxana Sannikova — Work notes • 2022-06-07 14:07:46

A scheduled Orbital query has executed and found devices vulnerable for CVE-2020-0796.
Click here to view the Microsoft Advisory for mitigations and workaround information
Link to Orbital Query Results
Re-run Orbital Query

NOT VULNERABLE DEVICES:granite
marble
slate

OS Oxana Sannikova — Field changes • 2022-06-07 14:07:46

Impact	2 - Medium
Incident state	New
Opened by	Oxana Sannikova
Priority	5 - Planning

Key Takeaways

- Automation is the key answer to the main SOC challenges
- Cisco Security solutions have robust APIs to support these use cases and lower the level of efforts required by customers
- Main API use cases: Automated alerting, operationalizing threat intelligence, proactive threat hunting, forensics gathering

Cisco Live Hands-On Labs

- Threat Hunting using Cisco Security APIs – HOLSEC-2021
- Secure X Orchestration – DEVWKS-2205
- Crash Course: Automating with SecureX Orchestration – HOLPRG-2001
- Building 3rd Party Integrations with Cisco SecureX – HOLSEC-3003

Related sessions – Introduction to SecureX

SecureX All The Things (With Hosted and Remote Relays) - BRKSEC-1483
Ben Greenbaum, Sr Product Manager, Cisco Systems, Inc. - Distinguished Speaker

Save Countless Hours with SecureX's Latest Feature: Device Insights - BRKSEC-2754
Aaron Woland, Distinguished Engineer, Cisco Systems, Inc. - Distinguished Speaker

Prepare Your Defence with Cisco SecureX Orchestration - BRKSEC-3404
Hakan Nohre, Technical Solutions Architect, Cisco Systems, Inc. - Distinguished Speaker

Getting started with SecureX orchestration workflows and atomics - DEVWKS-2190
Matt Vander Horst, Technical Marketing Engineer, Cisco Systems, Inc.

Security Automation: Developing with SecureX - DEVNET-1083
Matt Vander Horst, Technical Marketing Engineer, Cisco Systems, Inc.

Webhooks in SecureX orchestration - DEVLIT-1553
Matt Vander Horst, Technical Marketing Engineer, Cisco Systems, Inc.

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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 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

The bridge to possible

Thank you

cisco Live!

#CiscoLiveAPJC