

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Threat Hunting with Cisco Security APIs

Based on Automated Alerting and Intel-Driven Detections

Oxana Sannikova, Global Network Security Automation Team Leader
DEVNET-3142

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

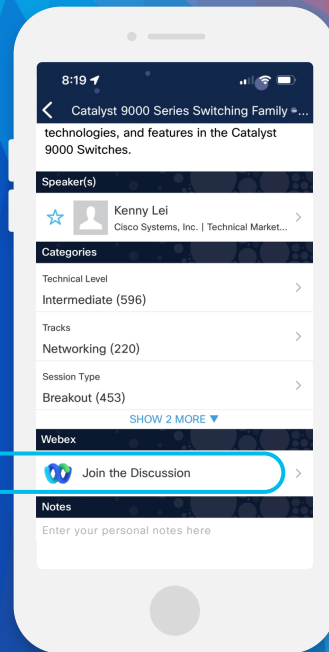
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-3142>

A little bit about me

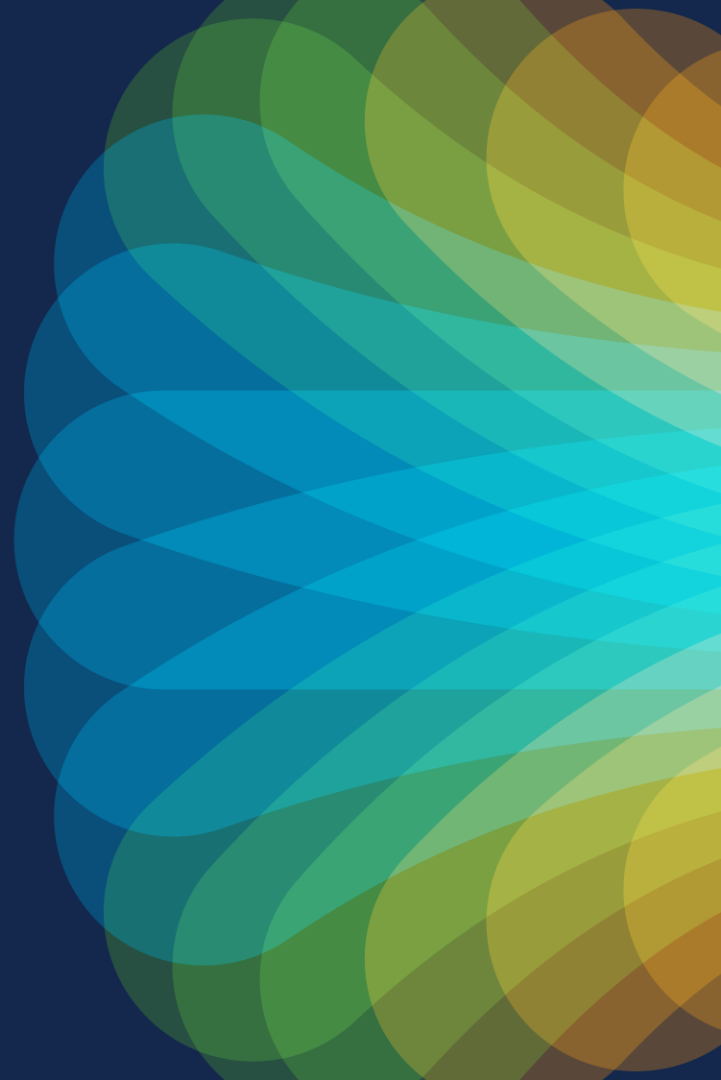
- Work:
 - Global Security Architecture Team
 - 15 years at Cisco, 19 years in security industry
 - Past exp.: Perl, PHP, Network monitoring automation
 - Current coding exp.: Python, Java Script
- Life:
 - 7 years in Canada
 - Hobby: urban sketching



Agenda

- Threat Hunting Maturity
- Automation use cases:
 - Make threat intelligence actionable
 - Detection and alerting
 - 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

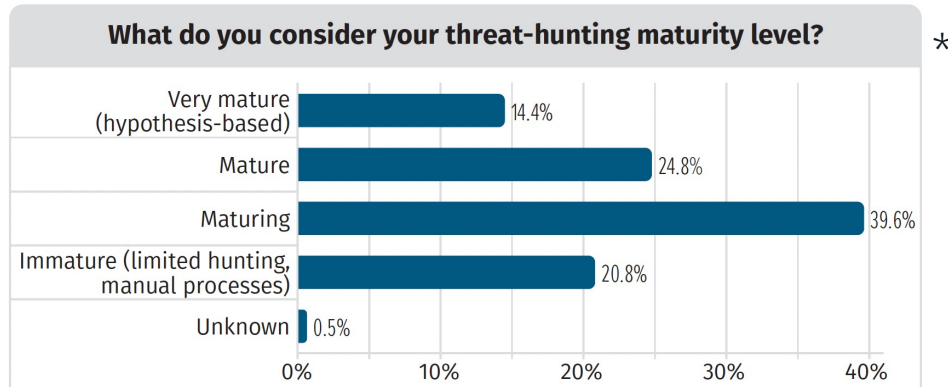
- Difficult to operationalize threat intelligence
- Often unreliable and out-of-date



Lack of Internet-wide Threat Visibility

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

Triage
Reactive



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

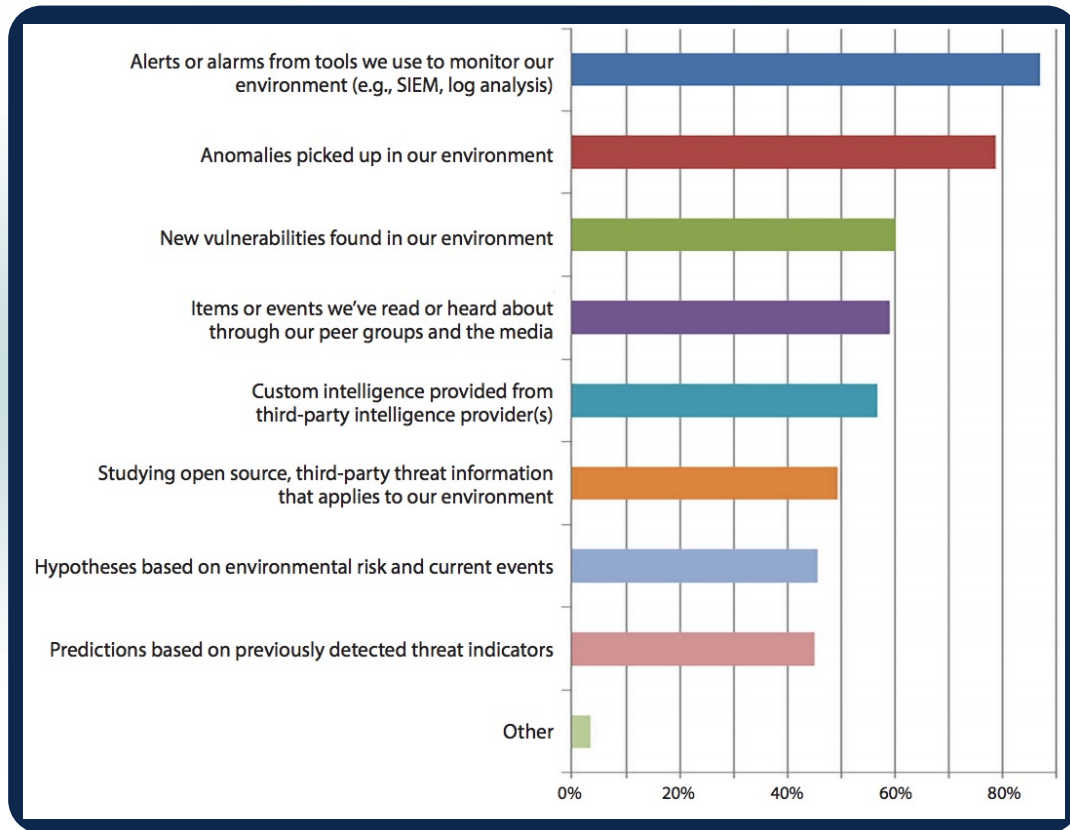
HMM 4 Leading

- 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.”

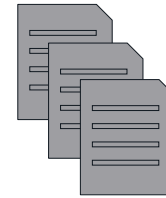
A Framework for Cyber Threat Hunting by sqrrl

Leveraging built-in threat intelligence

Secure Malware Analytics

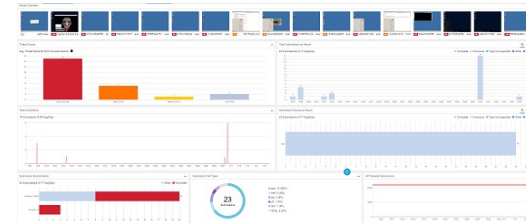
Secure Malware Analytics API Use Cases

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

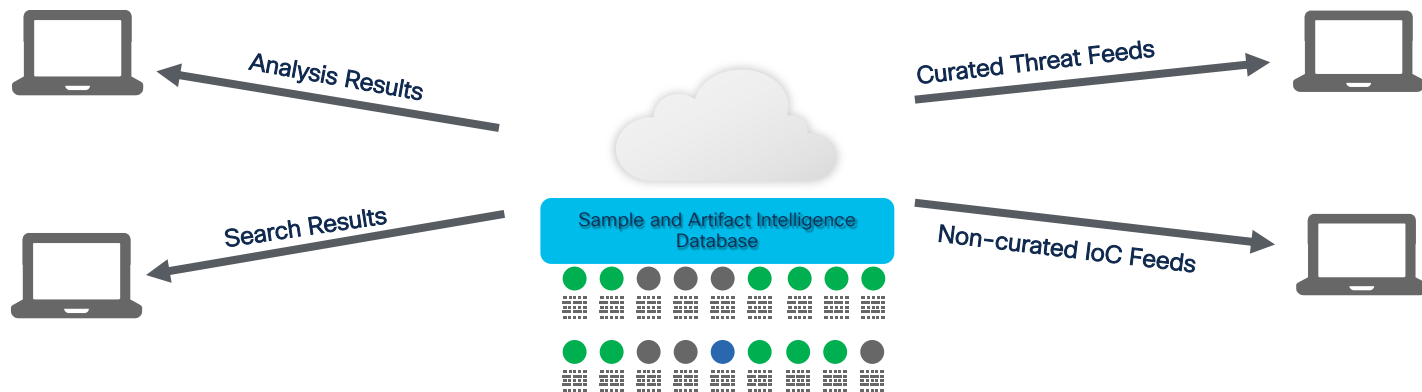


Secure Malware Analytics API

Malware Analysis & Threat Intelligence



Threat Intelligence: Delivery



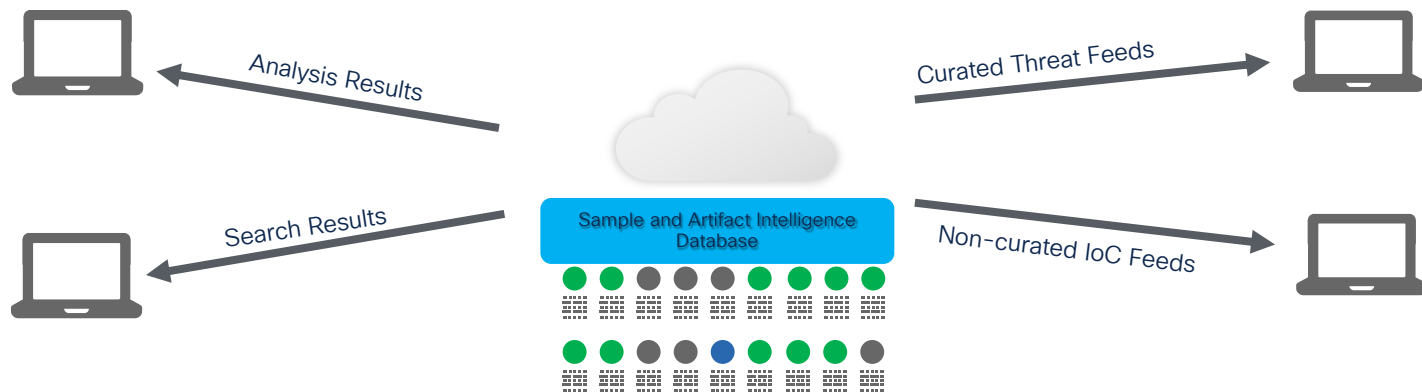
Analysis and Search Results

- 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

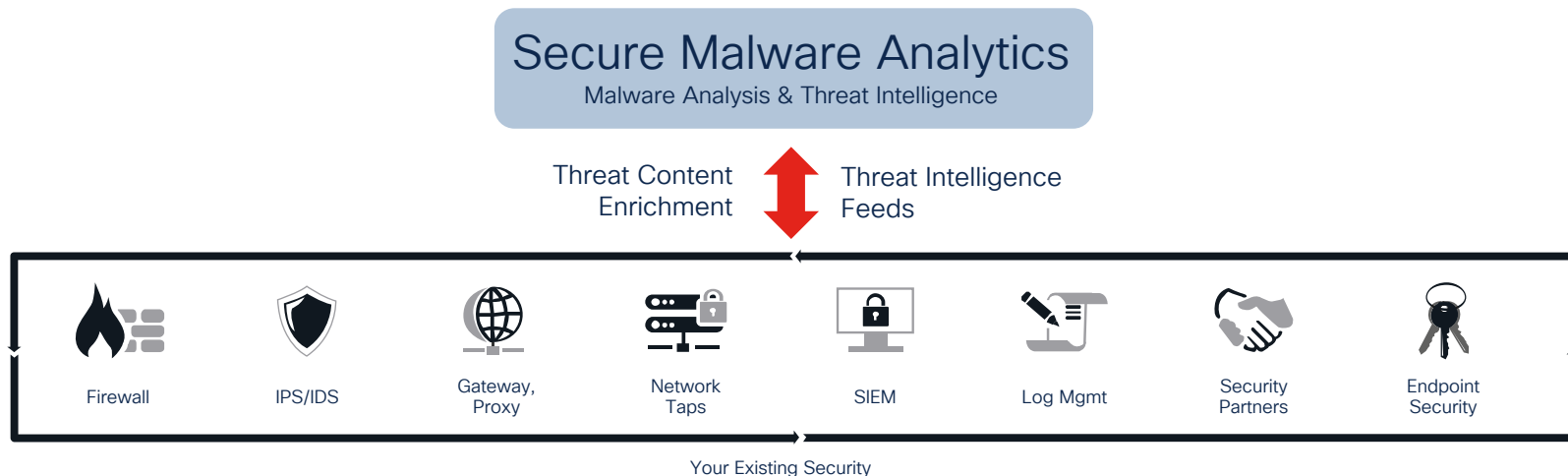
Threat Intel Data Feeds

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

Secure Malware Analytics API:

Security Integration and Automation

- Secure Malware Analytics REST API automates sample analysis, enrichment and reporting
 - Automate submission from numerous technologies (host or network)
 - Pull results into numerous technologies



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/Short/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

Working with Secure Malware Analytics Curated Feeds

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

Params Authorization Headers (5) Body Pre-request Script Tests Settings Cookies

Body Cookies Headers (9) Test Results Status: 200 OK Time: 5.83 s Size: 10.56 MB Save Response

Pretty Raw Preview Visualize JSON

```
79 {
80   "description": "DGA Domains With Pseudo-randomly Generated Names.",
81   "ips": [
82     "206.191.152.37"
83   ],
84   "sample_md5": "d98d6087e200727cf241c305e13dc6c1",
85   "sample": "https://panacea.threatgrid.com/feeds/dga-dns/samples/86358128b166593684bb869b06616b70",
86   "sample_sha256": "7e4364f48e0d6c16fd327fd7ba7b54ae03ae6ec6d271d48a17dcd653d1ca23d8",
87   "info": "https://panacea.threatgrid.com/feeds/dga-dns/domains/anfaiaeiinbbiviil.in",
88   "domain": "anfaiaeiinbbiviil.in",
89   "sample_sha1": "30eac6305f53c5a3b451e16a69831543deb4e62c",
90   "timestamp": "2022-06-02T01:33:09Z"
91 },
```

Drills back to the source of intelligence

Primary indicator

Behavior Indicators

>

Title ▾

>

Remcos Registry Key Detected 🔍

>

.NET Process Used in Potential Process

>

Artifact Flagged Malicious by Antivirus

>

Process Attempted to Stop WinDefend

>

Cisco Umbrella Flagged Domain As A Control Server

>

Domain in Cisco Umbrella Block List

>

Excessive Remote Process Code Inject

▼

Title ▾

▼

Remcos Registry Key Detected 🔍

Categories

Remote-Access Trojan...

ATT&CK ⓘ

Collection

Command and Control

Credential Access

Tags

RAT

registry

trojan

Indicator Score ⓘ ▾

100 🚫

Remcos Registry Key Detected

Indicator Score: 100 🚫 Hits: 1

Description

Remcos is a Remote Access Tool (RAT) with features which include key-logging, screen capture, webcam and microphone recording, and a lot more. A registry key associated with Remcos was detected.

Trigger

This indicator triggers when a registry key associated with Remcos RAT is seen.

Process	Process Name	RegKey Name	RegKey Value Name	RegKey Data	Actions
Process 43	RegSvcs.exe	USER\S-1-5-21-2580483871-590521980-3826313501-500\SOFTWARE\ROCJDFTER-K7DGLB	licence	D9482868EAC3DB1DED7282B481B37664	🔍 Orbital Query

MITRE ATT&CK

attack.mitre.org

Tactic: Credential Access 🔍 📄

Technique: Input Capture 📄

Read Descriptions

Tactic: Collection 🔍 📄

Technique: Input Capture 📄

Technique: Screen Capture 📄

Technique: Video Capture 📄

Technique: Audio Capture 📄

Read Descriptions

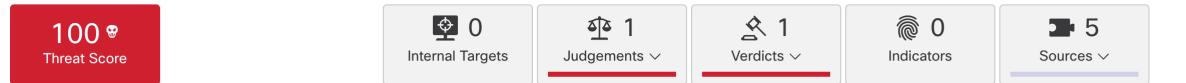
Tactic: Command and Control 🔍 📄

Technique: Ingress Tool Transfer 📄

Read Descriptions

Secure Malware Analytics Curated Feeds

Metrics



```
"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"  
  ],  
}
```

Behavioral Indicators

☐ Only show Indicators with Orbital queries

▼	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 the infected system and spread 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

```
{  
  "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-objs": [  
    "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 and Orbital APIs

Cisco Secure Endpoint Use Cases

- **GET**
`/v1/computers/activity?q=midyearbonus.com`
 - Searches all computers for any events or activities associated with a file or network operation, returns computers matching that criteria.
 - Requires a **q** parameter which accepts:
 - an IPv4 address: 1.0.0.0
 - a SHA256
 - a filename
 - a URL fragment
 - Hard limit of 5000 historical entries searched.

```
"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/trajectories",
      "group": "https://api.amp.cisco.com/v1/groups/bd639c70-..."
    }
  },
  {
    "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/trajectories",
      "group": "https://api.amp.cisco.com/v1/groups/bd639c70-..."
    }
  }
]
```

2 computers
connected to
midyearbonus.com

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.

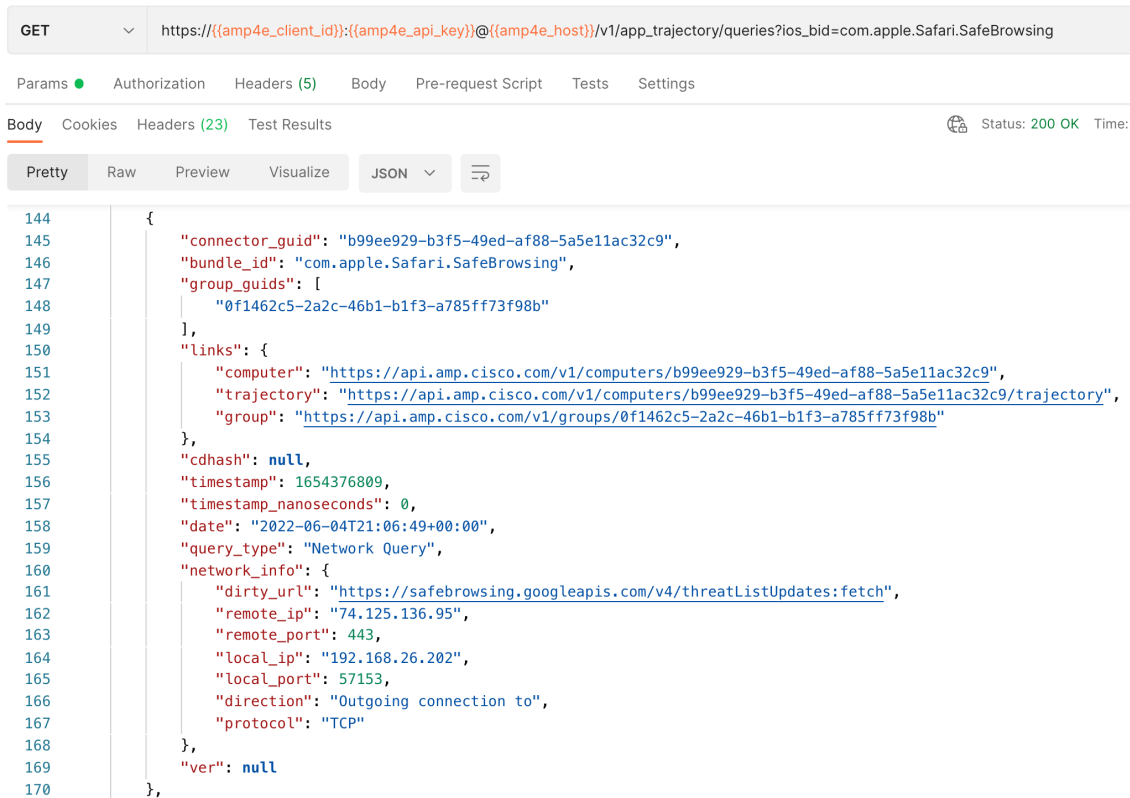
Cisco Secure Endpoint API Use Cases – cont.

- GET
`/v1/computers/{:connector_guid}/trajactory`
 - All activities associated with a particular computer (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

```
{
  "timestamp": 1654506418,
  "timestamp_nanoseconds": 412317470,
  "date": "2022-06-06T09:06:58+00:00",
  "event_type": "Executed by",
  "group_guids": [
    "bd639c70-f1ab-46bc-bd94-4422c1f5c7b3"
  ],
  "file": {
    "disposition": "Unknown",
    "file_name": "midyearbonus.com",
    "file_path": "/c:/users/admin/downloads/midyearbonus/midyearbonus/midyearbonus.com",
    "file_type": "PE Executable",
    "identity": {
      "sha256": "0d5a1c01c2706c8b66ba953dbe01f265d7d38e9b02aa41bc4f62239e9acb8067"
    },
    "parent": {
      "disposition": "Clean",
      "identity": {
        "sha256": "ff79d3c4a0b7eb191783c323ab8363ebd1fd10be58d8bcc96b07067743ca81d5"
      }
    }
  }
}
```

Cisco Secure Endpoint API Use Cases – cont.

- GET
`/v1/app_trajectory/queries`
- Retrieves app_trajectory queries for a given ios bundle id.



```
GET https://(amp4e_client_id):(amp4e_api_key)@((amp4e_host))/v1/app_trajectory/queries?ios_bid=com.apple.Safari.SafeBrowsing

Params Authorization Headers (5) Body Pre-request Script Tests Settings

Body Cookies Headers (23) Test Results

Pretty Raw Preview Visualize JSON

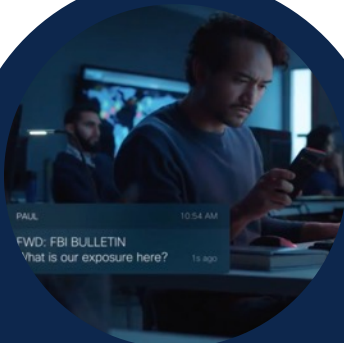
{
  "connector_guid": "b99ee929-b3f5-49ed-af88-5a5e11ac32c9",
  "bundle_id": "com.apple.Safari.SafeBrowsing",
  "group_guids": [
    "0f1462c5-2a2c-46b1-b1f3-a785ff73f98b"
  ],
  "links": {
    "computer": "https://api.amp.cisco.com/v1/computers/b99ee929-b3f5-49ed-af88-5a5e11ac32c9",
    "trajectory": "https://api.amp.cisco.com/v1/computers/b99ee929-b3f5-49ed-af88-5a5e11ac32c9/trajectory",
    "group": "https://api.amp.cisco.com/v1/groups/0f1462c5-2a2c-46b1-b1f3-a785ff73f98b"
  },
  "cdhash": null,
  "timestamp": 1654376809,
  "timestamp_nanoseconds": 0,
  "date": "2022-06-04T21:06:49+00:00",
  "query_type": "Network Query",
  "network_info": {
    "dirty_url": "https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch",
    "remote_ip": "74.125.136.95",
    "remote_port": 443,
    "local_ip": "192.168.26.202",
    "local_port": 57153,
    "direction": "Outgoing connection to",
    "protocol": "TCP"
  },
  "ver": null
}
```



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

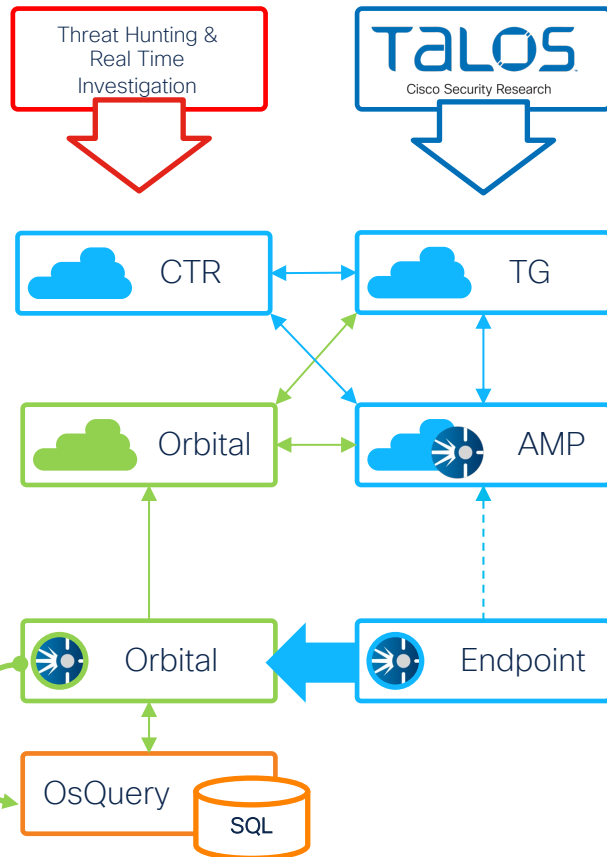
Check system status (OS versions, patches etc.), ensuring hosts comply with policies.



IT Operations

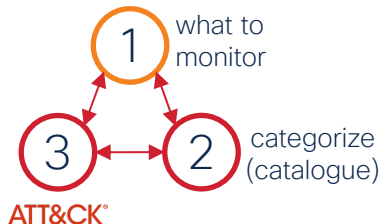
Track disk space, memory, and other IT operations artifacts quickly.

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

The screenshot displays the Cisco Orbital Query Catalog interface. On the left, a sidebar contains a 'Query Catalog' section with a 'Filters' panel. The 'Filters' panel includes 'Categories' (ATT&CK™ Tactics) and a list of tactics: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Below this is the 'ATT&CK™ Techniques' section. The main content area shows a list of queries. The 'ClearText RDP Connection Monitoring' query is highlighted with a red dot and a red line pointing to a detailed modal window. The modal window provides the following information:

- Query Catalog / cleartext_rdp_authentication_monitoring**
- ClearText RDP Connection Monitoring**
- Created by Cisco 2019-11-05. Updated 2019-11-19.**
- Description:** This query is applicable to Windows. Windows EventID "4624" 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

On the right side of the modal, there is a note: 'Catalog queries are designed to run independently.' Below this is a 'SQL' section with a code block containing the following query:

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

Below the modal, a table lists several queries with their details and associated categories/tactics:

Query Name	Created	Updated	ID	OS	Categories	ATT&CK™ Techniques	ATT&CK™ Tactics
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 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	5
Open Shares	3
Prefetch Directory	261
Recent Files Data	159
Running File Hashes	184

Autoexec Items

< 1 of 7 > 1 - 100

NAME

Local Print Queue

WAN Miniport (Network Monitor)

WAN Miniport (IPv6)

WAN Miniport (IP)

WAN Miniport (PPPoE)

WAN Miniport (PPTP)

WAN Miniport (L2TP)

WAN Miniport (IKEv2)

WAN Miniport (SSTP)

Generic software device

Remote Desktop Device Redirector

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

Search

PATH

SOURCE

SHA256

drivers

drivers

drivers

drivers

drivers

drivers

drivers

drivers

drivers

drivers

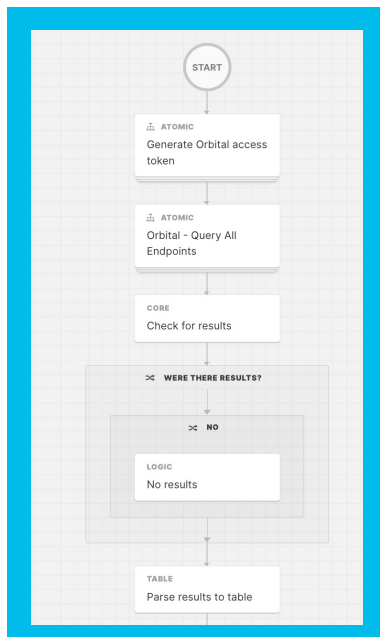
drivers

Export to CSV

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.

Example: Orbital CVE Hunt to ServiceNow incident



The image shows a ServiceNow incident form. The incident number is INC0189148, opened on 2022-06-07 14:07:46. The caller is SecureX, and the urgency is 1 - High. The short description is 'CVE-2020-0796 Vulnerabilities Detected'. The description is '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'. The form includes a 'Related Search Results' link, a 'Post' button, and a list of activities. The first activity, by Oxana Sannikova, states that a scheduled query was executed and found devices vulnerable to CVE-2020-0796, with links to Microsoft Advisory, Orbital Query Results, and Re-run Orbital Query. It also lists 'NOT VULNERABLE DEVICES: granite, marble, slate'. The second activity, also by Oxana Sannikova, shows field changes: Impact (2 - Medium), Incident state (New), Opened by (Oxana Sannikova), and Priority (5 - Planning).

Cisco XDR Workflow
Video

Orbital Advanced Search

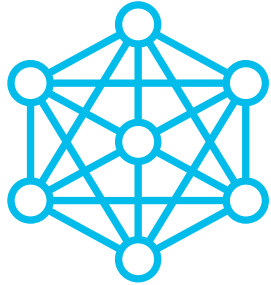
Forensic Snapshot Advantages

- 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).

Automated alerting using intel-driven detections

Cisco XDR

A vast ecosystem of integrations



Telemetry and Detections

Cisco XDR leverages multiple sources of telemetry and detections to achieve cross-product detections and outcomes

Action and Response

Multiple types of response actions are available across products such as network, endpoint, email, and others

Cisco and Third Party

Leverage integrations with existing products, whether they are from Cisco or from a third party

Investigate with intelligence, context and response

Cisco XDR Investigate



Are these observables suspicious or malicious?

Observables:

- File hash
- IP address
- Domain
- URL
- Email addresses
- Etc.

Have we seen these observables?
Where?

Which endpoints connected to
the domain/URL?

What can I do about it right now?

Cisco XDR APIs

[Documentation](#)

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
Automate	Interact with the backend of the low-to-no-code Automation engine in Cisco XDR, manage objects, retrieve Workflow Run information and execute Workflows via API.

Intro to Cisco XDR Automate

Process **automation**
made simple with a
no/low-code drag-
drop interface



Investigate

Reduce research and response times with workflows and playbooks that execute at machine speed



Automate

Eliminate repetitive tasks and reduce MTTR to increase productivity and focus on mission-critical projects



Integrate

Unique turnkey approach to quickly integrate with other systems and solutions to expand your toolbox



Scale

Automation that scales infinitely and never takes a day off, delivering the same SLA around the clock

DEMO: Jira – Cisco XDR Automate



Jira and Cisco XDR Automate:

Automated issue creation, escalation and response



ORCHESTRATION



THREAT RESPONSE

Jira



OpenPhish

Gather OSINT

- Pull OpenPhish phishing URL feed every 12 hours.

DELIBERATE

- Check each URL disposition within Global Intelligence DB.

CREATE JIRA ISSUE

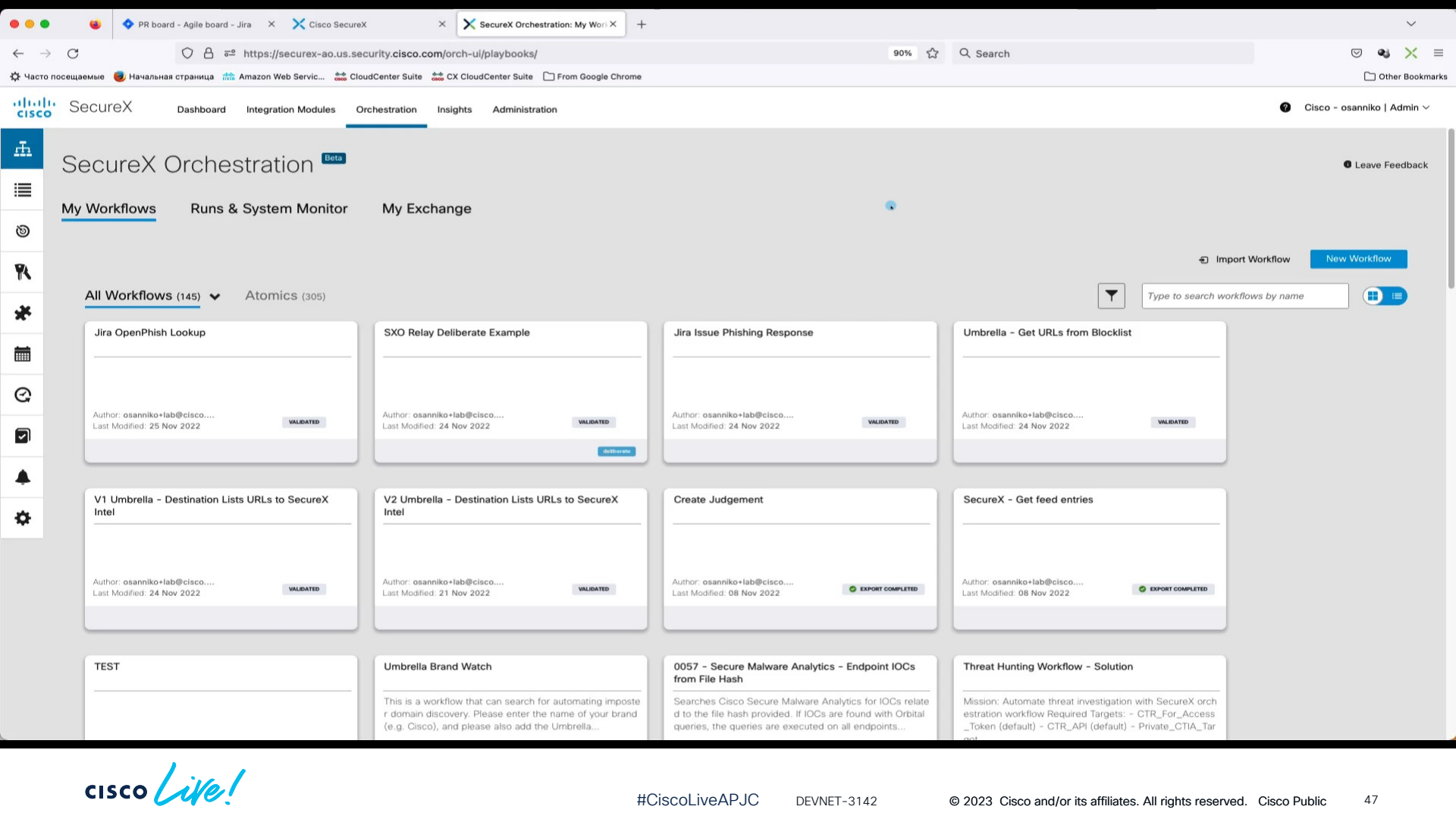
- If disposition is Unknown, create new Jira Issue.

RESPONSE

- Perform investigation, if sightings found, create investigation snapshot and escalate the issue.

CLOSE ISSUE

- If no sightings found – close the issue.



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

Scenario



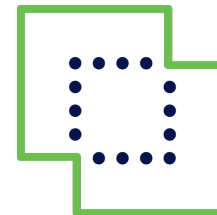
ORCHESTRATION



Umbrella



NGFW



Gather OSINT

- Pull OpenPhish phishing URL feed every 12 hours

DELIBERATE

- Check each URL disposition within SecureX Global Intelligence DB

CREATE JUDGEMENT

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

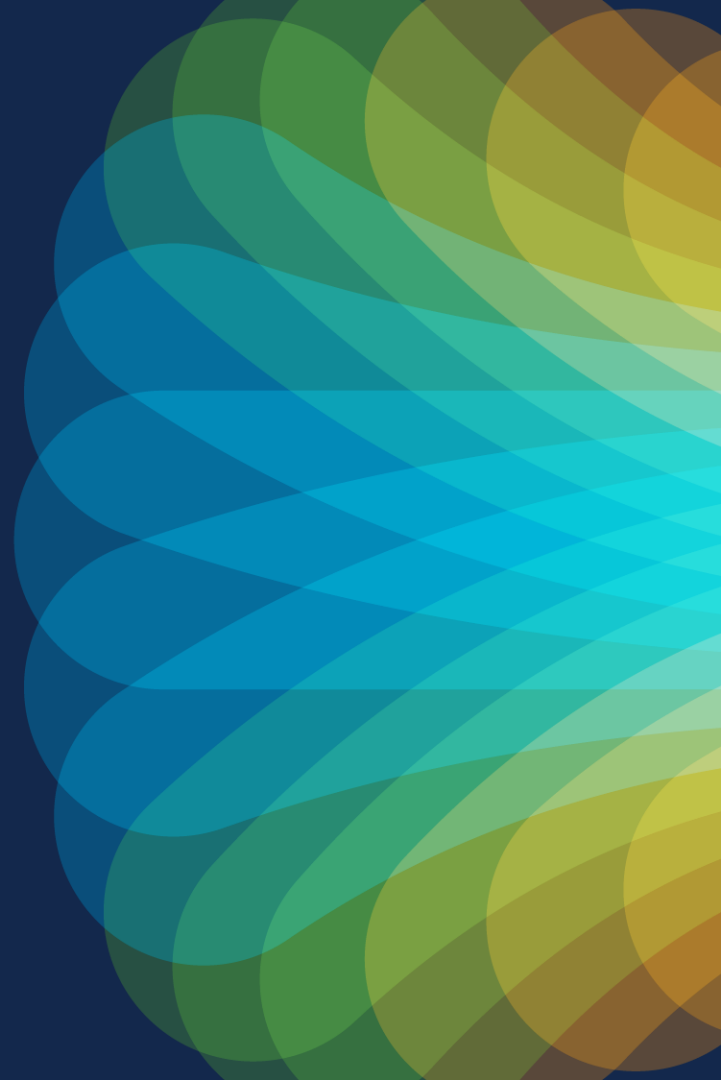
ADD TO FEED

- 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

DEMO: Ask OpenAI



Ask OpenAI

The screenshot displays the Cisco SecureX dashboard with the following components:

- Umbrella Request Summary:** Shows 97,117 Total Requests and 9 Total Blocked.
- SMA Email Incoming Threat Messages Summary:** Includes a list of items: Reputation Filtering (56,98k), Invalid Recipients (957), Anti-Spam (1), Anti-Virus (116), and Advanced Malware Protection (68). A circular progress indicator shows 59K.
- Casebook:** A search bar and a list of cases. The selected case is "Cisco Secure Email - URL suspicious in email - paul@internetsinkhole.com".
- Case Details:**
 - Overview:** Shows the case title, creation date (Feb 4, 2023, 3:28:30 PM), and owner (Alexandre Argeris).
 - Details:** Lists the case summary and linked incidents.
 - Observables (5):** A list of observables including 1 Cisco Message ID, 2 Emails, 1 Email Subject, and 1 URL.
 - Notes:** A list of notes including "Subject: Free Grant Donation!", "Date: Sat, 4 Feb 2023 20:28:07 +0000 (UTC)", "To: paul@internetsinkhole.com", "Cisco Message ID: 8347", "From: recheh@baror-pro.co.il", and "Cisco Secure Malware Analytics Sample ID: 77b254c31217c503f90eb53f5e0b0e06".

Key Takeaways

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



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

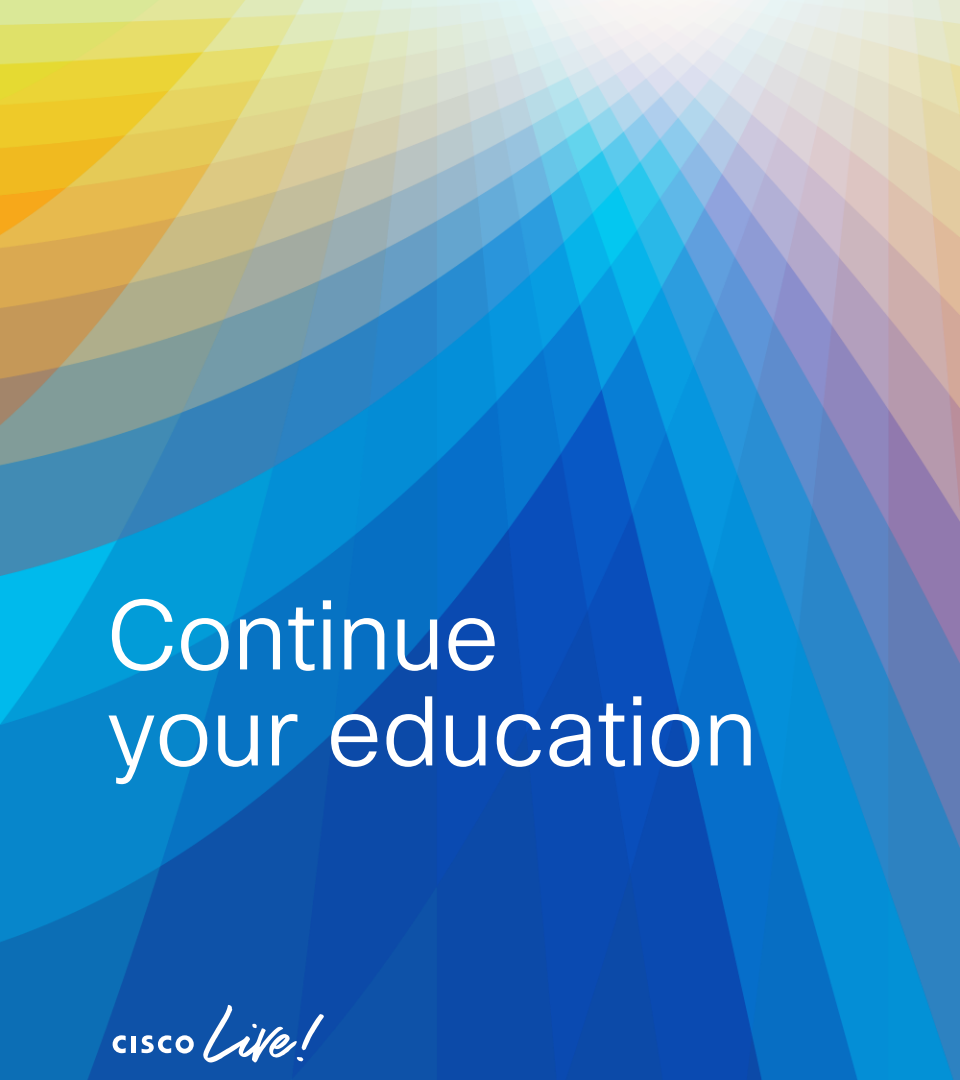
- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



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



Continue your education

CISCO *Live!*

- Visit developer.cisco.com/security
- Check out [DevNet Automation YouTube channel](#)
- [Cisco Security Postman Collection](#)
- Join [Security Programmability Community](#)



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC