

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Leveraging Cisco Security APIs for threat hunting

Based on automated alerting and intel-driven detections

Oxana Sannikova,
XDR & SNA TME Leader, Security Business Group
DEVNET-3098

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-3098>



A little bit about me

• Work:

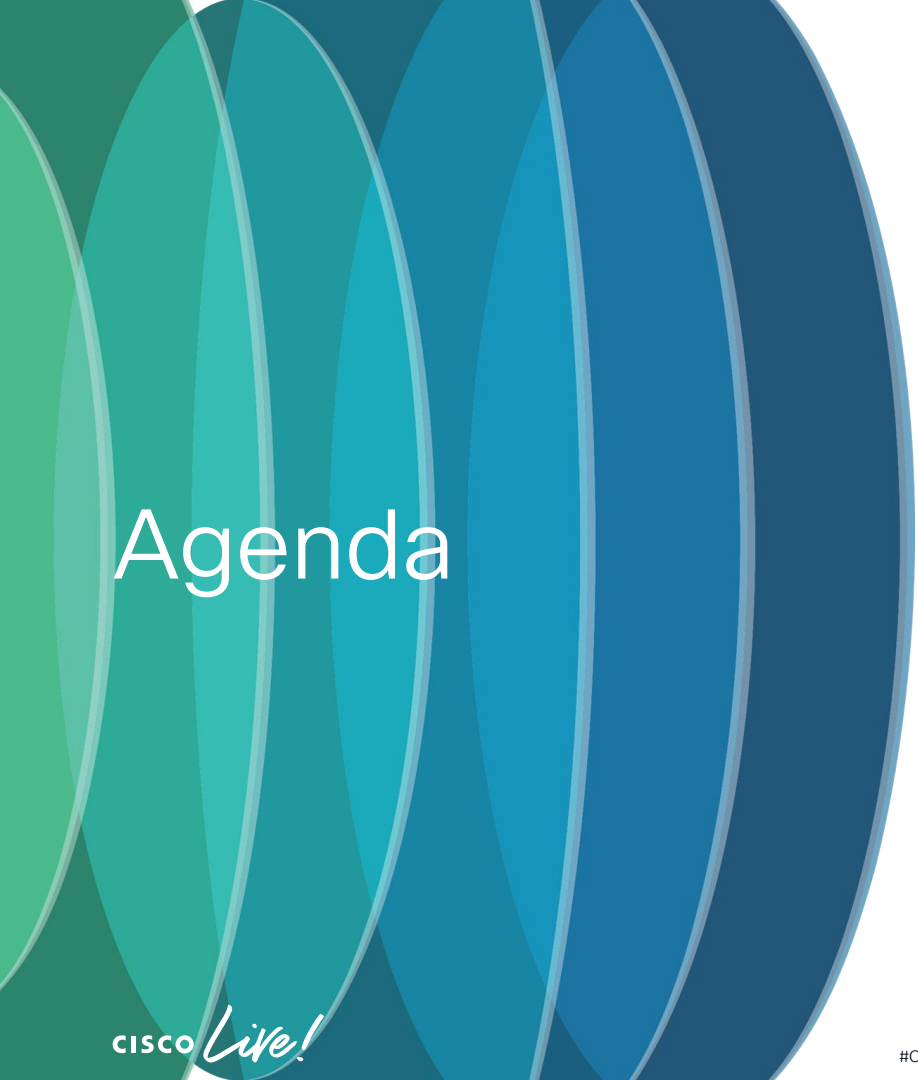
- XDR & SNA Technical Marketing Engineering Team Leader
- Past: Global Security Network Automation Team Leader
- 16 years at Cisco, 20 years in security industry
- Current coding exp.: Python, Java Script, low to no-code automation
- Past exp.: Perl, PHP, Network monitoring automation

• Life:

- 7 years in Canada
- Hobby: urban sketching

cisco *Live!*

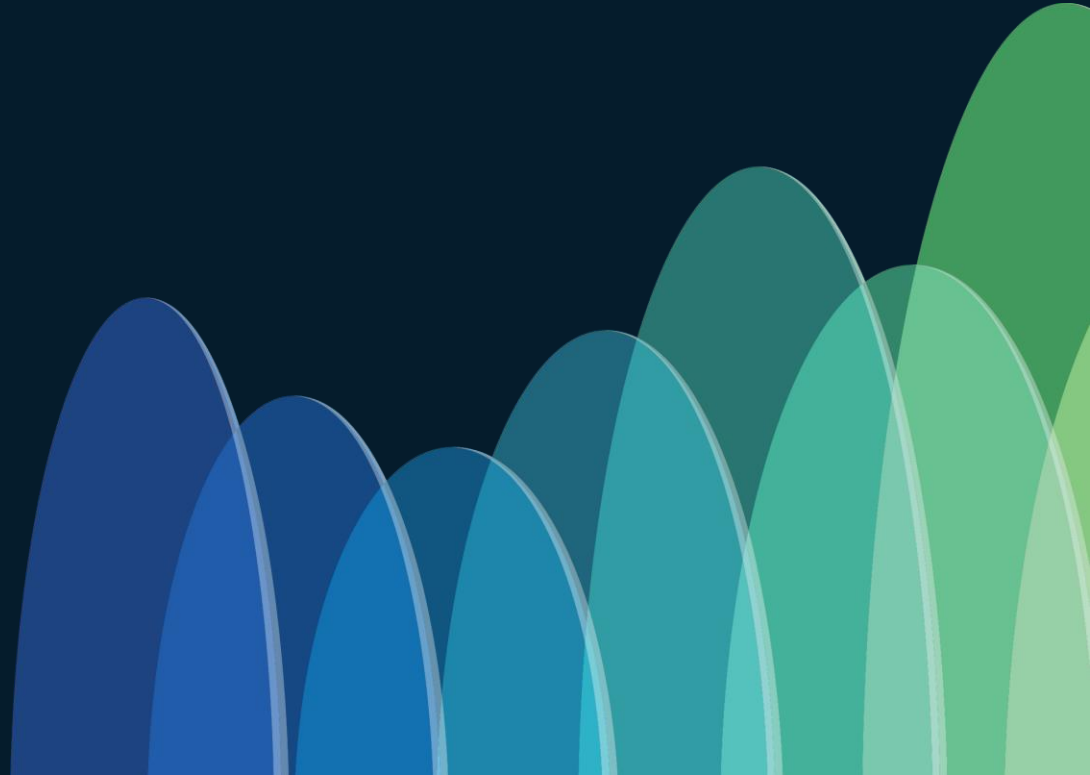




Agenda

- Threat Hunting Maturity
- Automation use cases:
 - Make threat intelligence actionable
 - Detection and alerting
 - Extended Detection and Response
 - Breach Attack Simulation
- 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 prioritise investigations
- Difficult to identify the source of the threat



Effective Intel use

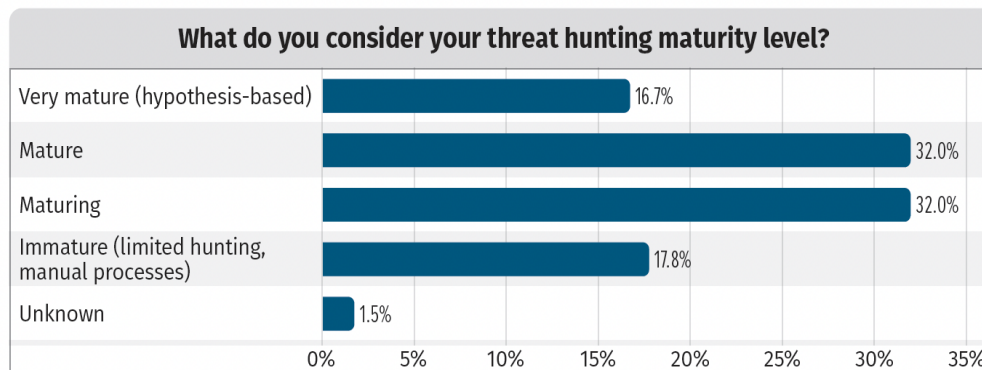
- Difficult to operationalise threat intelligence
- Often unreliable and out-of-date



Lack of Internet-wide Threat Visibility

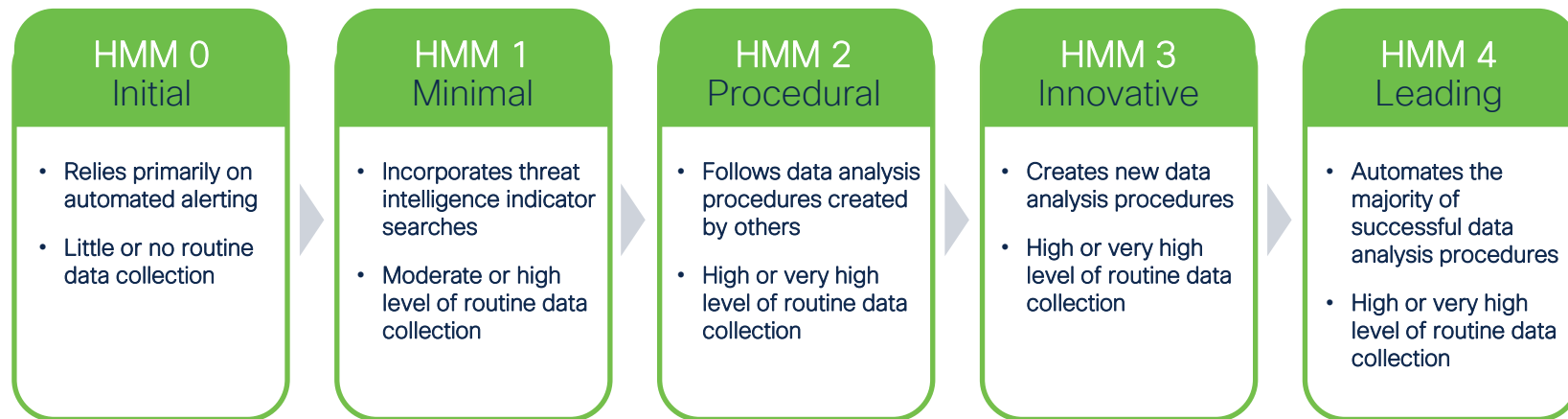
- Identify where attackers stage attacks
- How domains, IPs, ASNs, and malware are connected

Triage
Reactive



*

Hunting
Proactive



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>

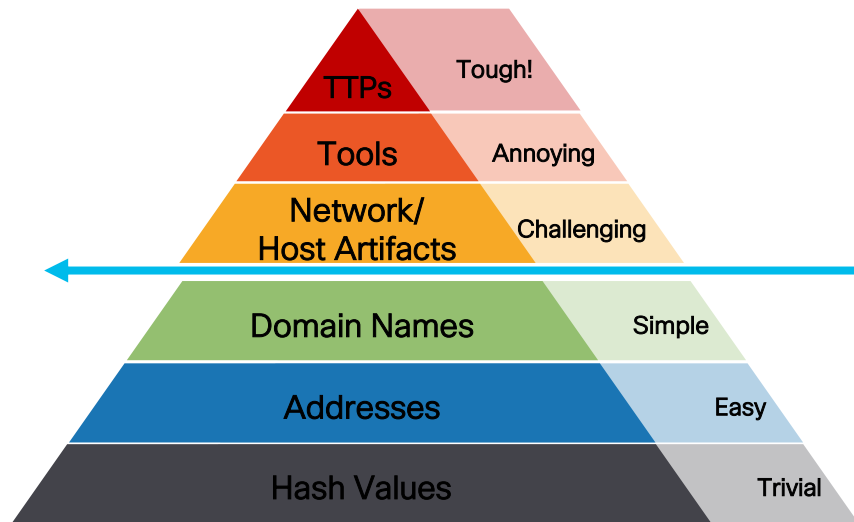
* <https://www.sans.org/white-papers/sans-2024-threat-hunting-survey-hunting-normal-within-chaos>

“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

Commodity Based Controls will Fail!

Concentrate on the root of the problem to achieve security enlightenment



The Problem

- TTPs are the recipe with the ingredients for adversarial success
- Much more difficult for the adversary to overcome
- Defenders' opportunity to cause pain

The Symptom

- Commodity based controls
- Reduces noise
- Easy for the adversary to overcome
- Adversaries' opportunity to cause pain

From David Bianco: <https://www.sans.org/tools/the-pyramid-of-pain>

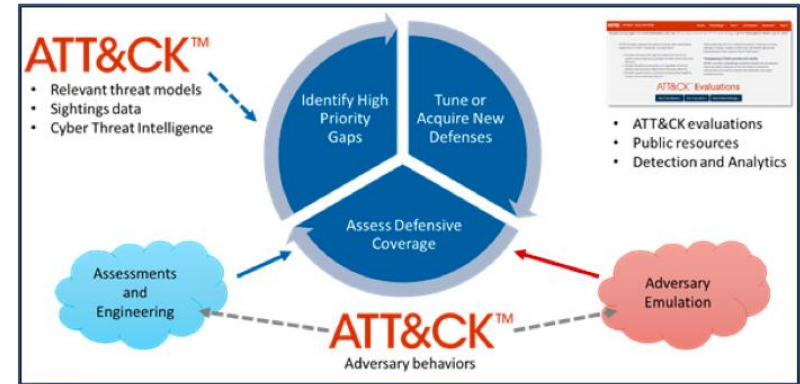
Who and What is MITRE ATT&CK?

- Who is MITRE Corporation?
 - Not-for-profit, US company with multiple federally funded R&D centers (FFRDCs)
 - Public-private partnerships in many areas, including cybersecurity
 - Same folks who brought us CVE database and CWE Programs
- What is ATT&CK
 - Adversarial Tactics, Techniques, and Common Knowledge – Non-Profit Organisation
 - Born in 2013 to document tactics, techniques, and procedures (TTPs) that APTs leverage
 - Globally-accessible knowledge base that's community driven
 - Used for the development of specific threat models & methodologies in the private sector, in government, and in the cybersecurity product and service community.
 - Focuses on the adversarial perspective (**who**), their goals (**why**), and the methods (**how**) used to achieve these goals.
 - Where is ATT&CK being leveraged?
 - Red Teaming, Gap Analysis / Assessments, Adversary Emulation

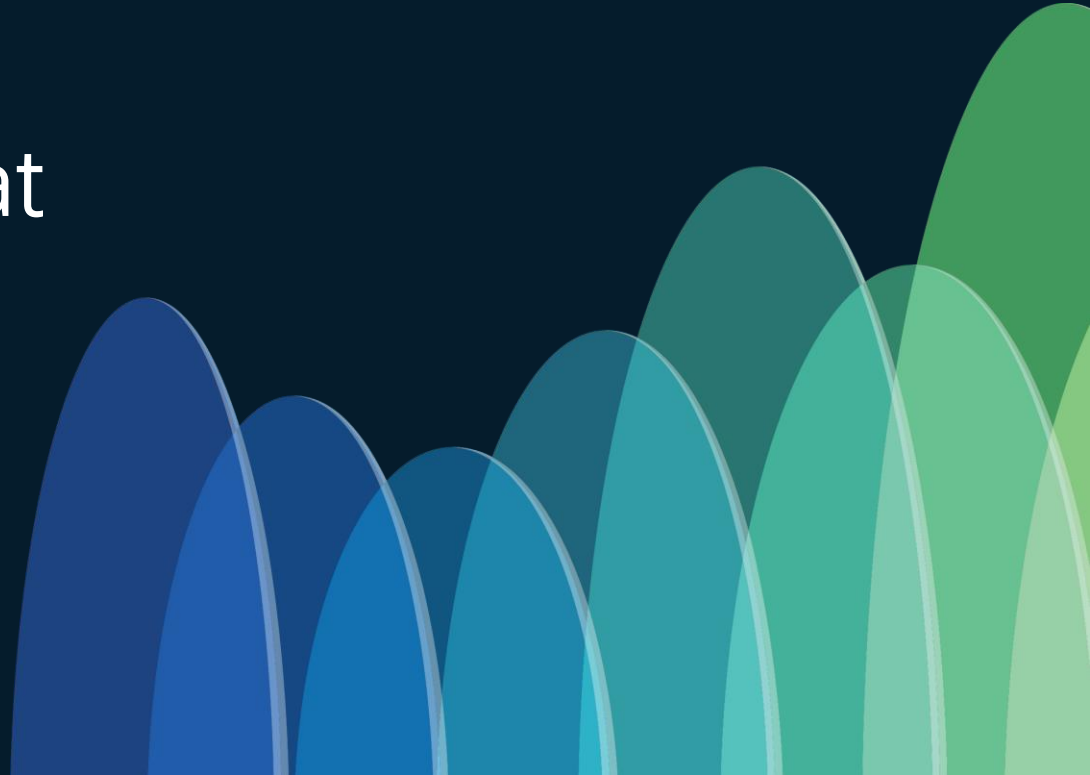
The MITRE logo consists of the word "MITRE" in a bold, blue, sans-serif typeface.The ATT&CK logo features the text "ATT&CK" in a large, bold, orange-red sans-serif font, with a trademark symbol. Below it, the words "Adversarial Tactics, Techniques & Common Knowledge" are written in a smaller, dark blue sans-serif font.

So that's nice, but what can we do with it?

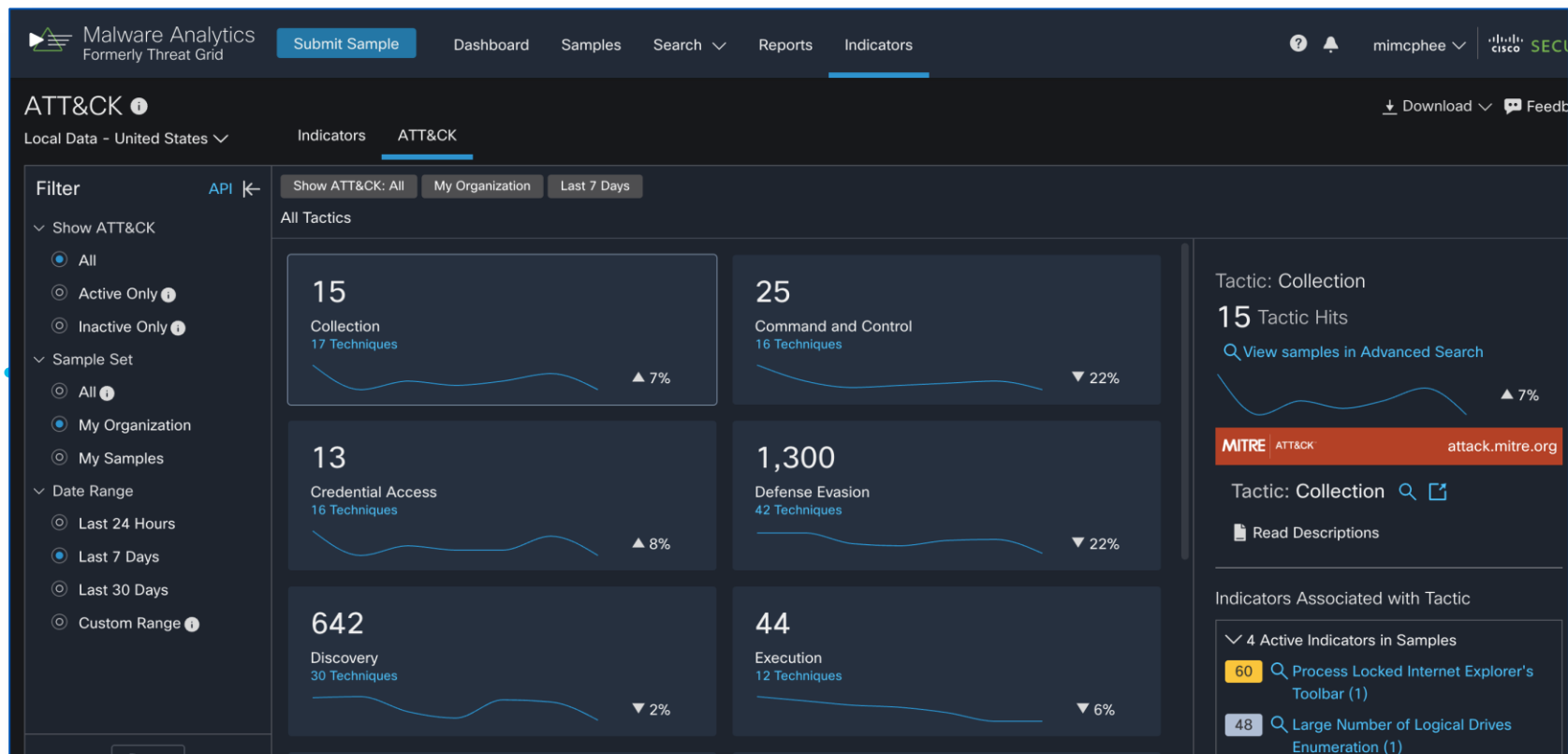
- Threat intelligence
- Detection and analytics
- Adversary emulation
- Assess coverage: do defenses stack up against the bad guys?
- **Prioritise gaps**: ID highest priorities
- Tune defenses: modify or acquire new!



Leveraging threat intelligence



Cisco Secure Malware Analytics



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 with MITRE ATT&CK

>

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 Injection

▼

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	RegSvc.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

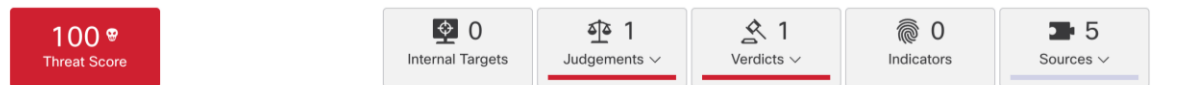
Tactic: Command and Control 🔍 📄

Technique: Ingress Tool Transfer 📄

Read Descriptions

Secure Malware Analytics Curated Feeds

Metrics



Behavioral Indicators

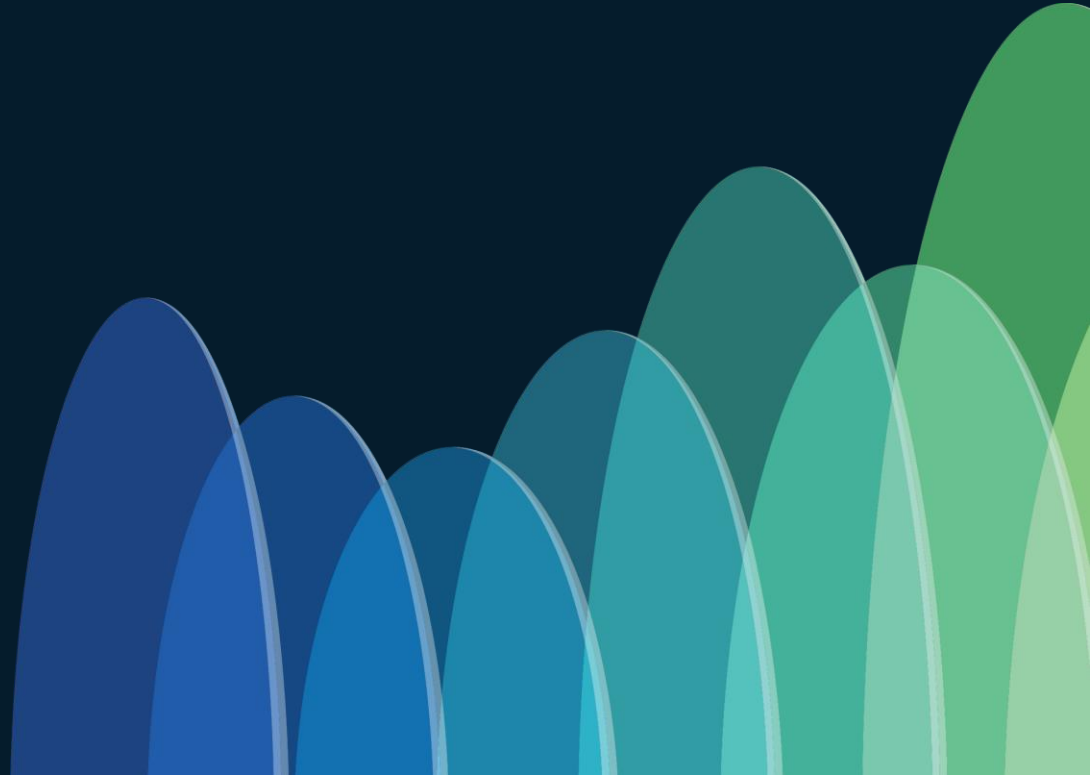
☐ Only show Indicators with Orbital queries

▼ Title ↕	Orbital Queries	Categories	ATT&CK ⓘ	Tags				
▼ Phorpiex Trojan File Modification Detected		Worm		smtp				
<h2>Phorpiex Trojan File Modification Detected</h2> <p>Score: 100 🛡️ Hits: 1</p> <h3>Description</h3> <p>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.</p> <h3>Trigger</h3> <p>The indicator triggers when files associated with Phorpiex were detected.</p> <table><thead><tr><th>Process</th><th>Process Name</th></tr></thead><tbody><tr><td>Process 17</td><td>winsvcs.exe</td></tr></tbody></table>					Process	Process Name	Process 17	winsvcs.exe
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.
    }
  ]
}
```

Detection and Alerting



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

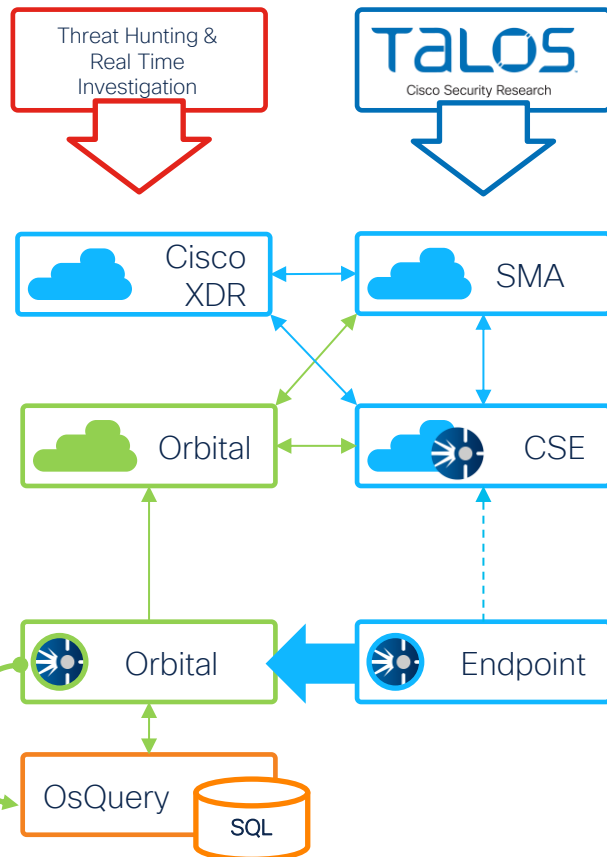
Check system status (OS versions, patches etc.), ensuring hosts comply with policies.



IT Operations

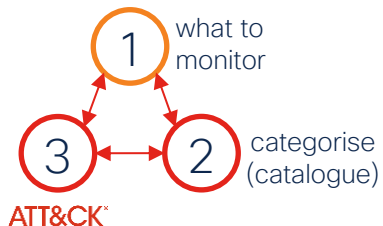
Track disk space, memory, and other IT operations artifacts quickly.

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 these are 'ATT&CK™ Techniques'. 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.

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 "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

SQL

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

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

- startup_item
- service
- scheduled_task
- driver

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 Redirection

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

Search

PATH

SOURCE

SHA256

drivers

drivers

drivers

drivers

drivers

drivers

drivers

drivers

drivers

drivers

drivers

Export to CSV

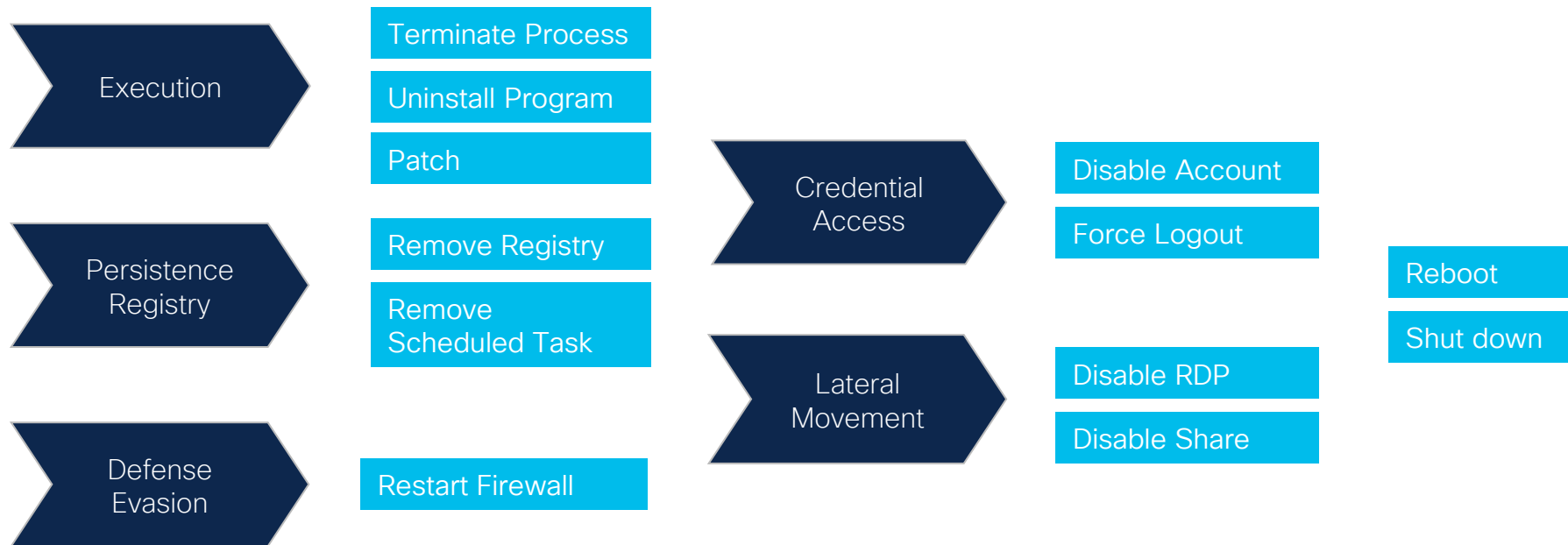
Orbital Queries API

- **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.

[API Documentation](#)

Remote Scripts – Responding Surgically

Powered by Orbital, embedded into EDR & XDR



Orbital Scripts API

- **Scripts API** - This API provides the means to either create a Python script or select one from the Catalog, send it to one or more endpoints, execute the script on the endpoint or endpoints and returns a job object that provides information needed to collect results.
- **Results API** - This API collects results from Orbital from a script exsecurity either by the Orbital User Interface, your applications or the Scripts API.

[API Documentation](#)

Cisco XDR Automation Workflow

Cisco Orbital - Take Forensic Snapshot (Linux)

Cisco Managed

This workflow initiates a Cisco Orbital forensic snapshot for the endpoint identified by the provided observable. This version of the workflow takes a forensic snapshot...

[Learn More](#) [Install](#)

Cisco Orbital - Take Forensic Snapshot (macOS)

Cisco Managed

This workflow initiates a Cisco Orbital forensic snapshot for the endpoint identified by the provided observable. This version of the workflow takes a forensic snapshot...

[Learn More](#) [Install](#)

Cisco Orbital - Take Forensic Snapshot (Windows)

Cisco Managed

This workflow initiates a Cisco Orbital forensic snapshot for the endpoint identified by the provided observable. This version of the workflow takes a forensic snapshot...

[Learn More](#) [Uninstall](#)

Cisco Orbital - Execute Query for Incident Assets

Cisco Managed

This workflow works with an incident automation rule or playbook task to execute an Orbital query on an XDR incident's assets.

[Learn More](#) [Uninstall](#)

Cisco Orbital - Execute Script for Incident Assets

Cisco Managed

This workflow works with an incident automation rule or playbook task to execute an Orbital script on an XDR incident's assets.

[Learn More](#) [Install](#)

Cisco Orbital - Execute Script for Selected Assets

Cisco Managed

This workflow works with an incident response playbook to execute an Orbital script on user-selected assets from an XDR incident. This workflow can either execute a...

[Learn More](#) [Install](#)

Cisco Orbital - Execute Query for Selected Assets

Cisco Managed

This workflow works with an incident response playbook to execute an Orbital query on user-selected assets from an XDR incident. This workflow can either execute a...

[Learn More](#) [Install](#)

Cisco XDR Individual Activities

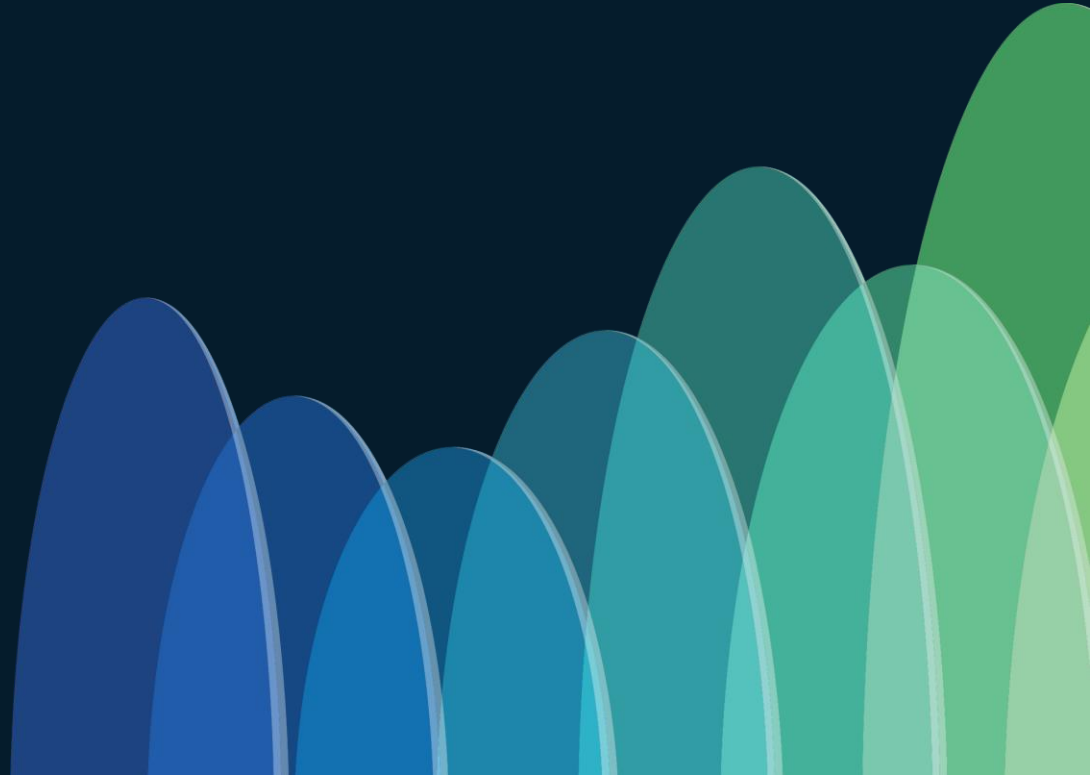
Cisco Orbital

- Orbital - Query - Get Job Results
- Orbital - Query - Get Job by ID
- Orbital - Query - Run Query
- Orbital - Query - Run Query (All Endpoints)
- Orbital - Script - Cancel Job
- Orbital - Script - Get Job Results
- Orbital - Script - Get Job by ID
- Orbital - Script - Get Organization Catalog Scripts
- Orbital - Script - Get Stock Catalog Scripts
- Orbital - Script - Run Script

Example: [Orbital CVE Hunt to ServiceNow Incident Demo](#)

cisco *Live!*

Extended Detection and Response



The Cisco approach to XDR

Detect more, act faster, elevate productivity, build resilience

Detect
the most
sophisticated
threats



- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimised for multi-vendor environments

Act on
what *truly*
matters, faster



- Prioritise threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations

Elevate
productivity



- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

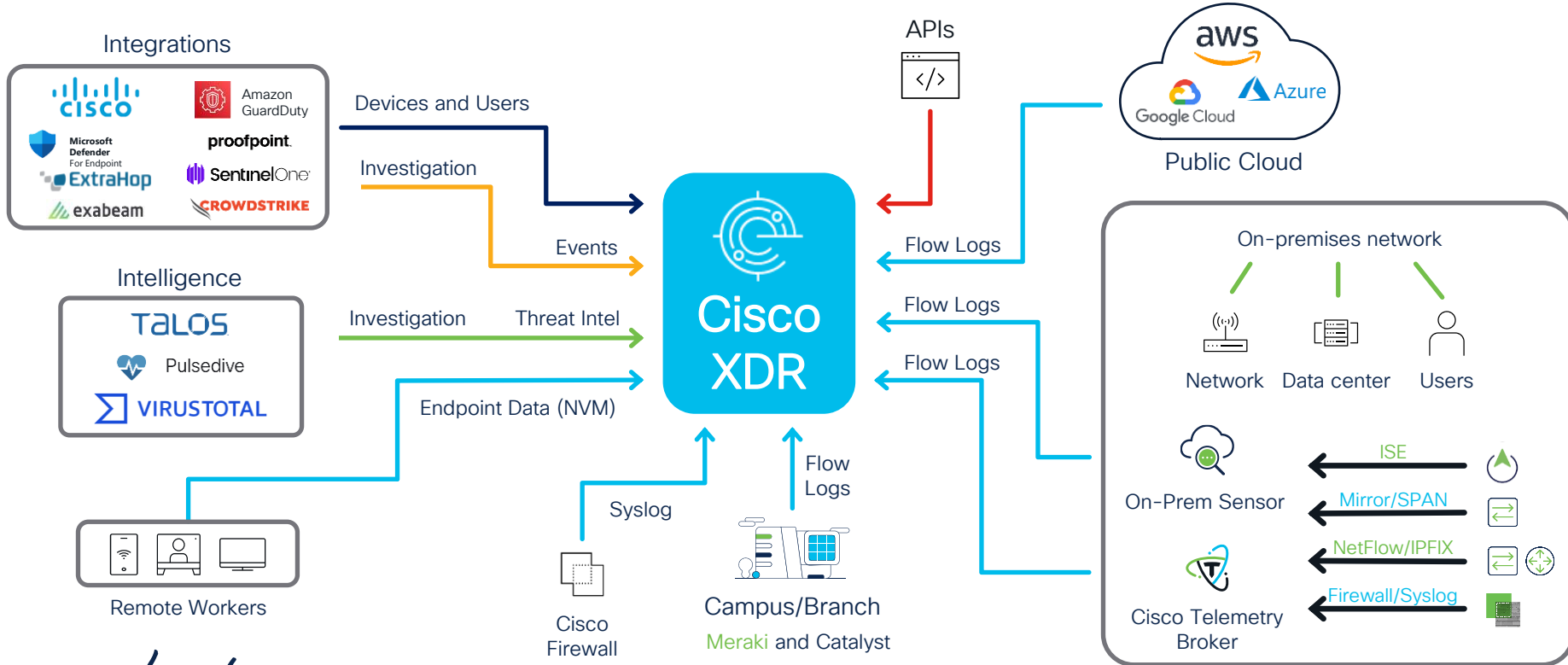
Build resilience



- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, every day with continuous, quantifiable improvement

Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



XDR APIs

[Documentation](#)



Automation



Response



Enrich



Inspect



Private Intelligence



Proxy



Public Intelligence



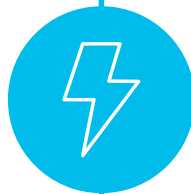
Devices

Automation outcomes



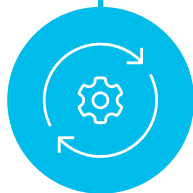
Investigate

Reduce time to investigate by automating data collection and incident generation



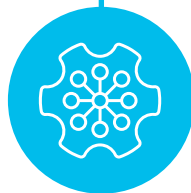
Respond

Automated or one-click responses that can combine multiple products in one action



Simplify

Eliminate repetitive tasks that waste valuable analyst time



Integrate

Bring products and services together in new ways to address emerging threats

Incident playbooks: Automation rules

- Allow various types of events to cause workflows to run.
- **Approval Task Rule:** An approval task is acted upon within XDR Automation.
- **Email Rule:** An email is received in a pre-defined inbox being monitored for new messages.
- **Incident Rule:** A matching incident is created in the XDR incident manager.
- **Schedule Rule:** A specific date, time, or interval of time has passed.
- **Webhook Rule:** An HTTP call was made to a specific webhook URL.

Triggers

To add a trigger to a workflow, configure an automation rule that determines when a workflow is executed, such as when an incident, specific event occurs, or on a schedule.

Automation Rules

Events

Webhooks

Calendars

Schedules

Search

Type

Q Search



Select



[Reset All](#)

Display name

On/off

Type

Owner

Hourly Workflow



Schedule

user@cisco.com

Incoming Webhook



Webhook

user@cisco.com

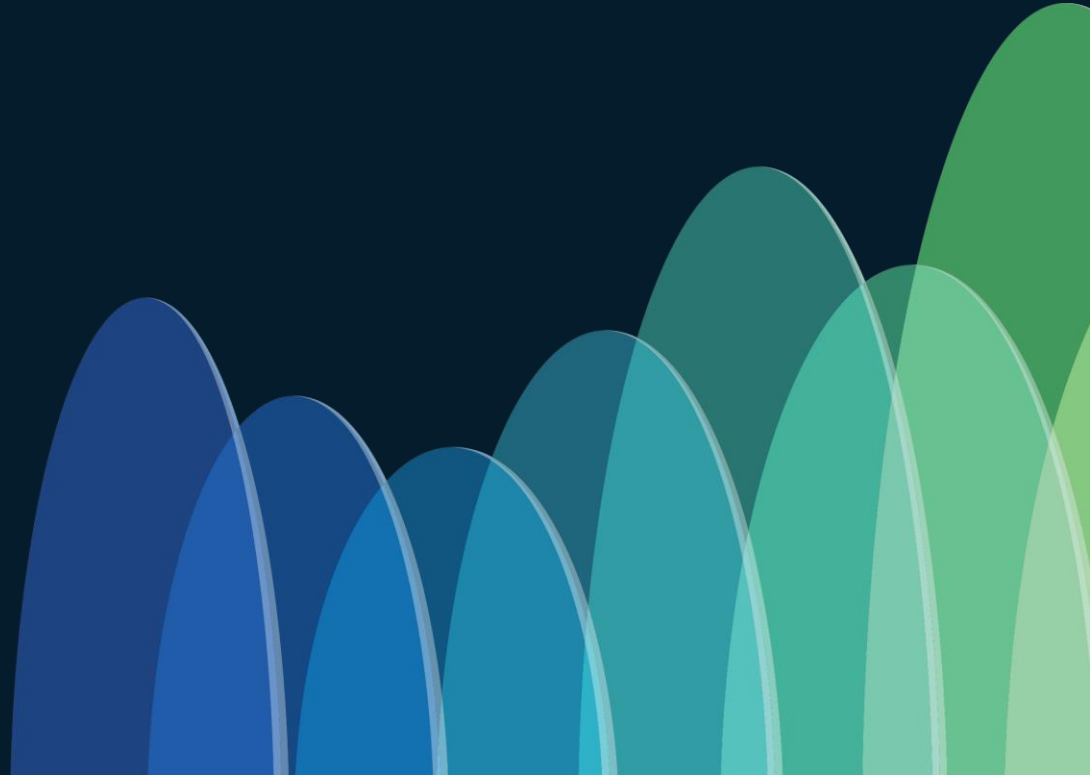
Incident Notification



Incident

user@cisco.com

Breach Attack Simulation



Adversarial Emulation

Gather
Threat
Intelligence

Extract
Techniques

Analyse and
Organise

Develop
Tools

Emulate the
Adversary

Overview of Breach Attack Simulation

Breach Attack Simulation focuses on simulating an attack on an organisations network or system for the sole purpose to determine the overall security posture currently in place.

- Provides a testing methodology to simulate attacks against the organisations.
- Helps identify weaknesses and vulnerabilities across a variety of attack vectors that could be exploited by attackers.
- Determines security effectiveness and opportunities to close the gaps in people, process, and technology.

Breach Attack Simulation: Process

Breach attack simulation is focused on the adversarial elements in order to compromise a network or system. This includes from an adversarial perspective:

1. **Reconnaissance:** the goal is to locate opportunities of weakness by identify attack vectors. This is accomplished by gathering information about the systems and networks the adversary is targeting.
2. **Vulnerability Scanning:** the goal is to understand weaknesses within the networks and systems and determine how to take advantage of this opportunity. This is accomplished by leveraging automated tools to identify vulnerabilities within the systems and networks being targeted.
3. **Exploitation:** the goal is to exploit weaknesses found in the systems and networks identified from reconnaissance and vulnerability scanning.

Breach Attack Simulation: Process

4. **Privilege Escalation:** the goal is to elevate the adversaries' privileges on the target network or systems to gain access to resources and data.
5. **Lateral Movement:** the goal is to navigate laterally to additional systems and networks to gain further access to resources and data.
6. **Data Exfiltration:** the goal is to exfiltrate sensitive data from the target network or systems and invoke the will of the adversary.

Tools of Focus

Opensource Breach Attack Simulation



[Overview Demo](#)

Commercial Breach Attack Simulation
ATTACKIQ

DEMO:
Adversaries Emulation with MITRE
Caldera and Automated Response

DEMO:

Adversaries Emulation with AttackIQ

← Back to all Workflows

Secure Firewall - Generate Snort Rule with OpenAI

Last Modified: February 1, 2024 at 3:06:28 p.m.

Share Validated View Runs Run Settings

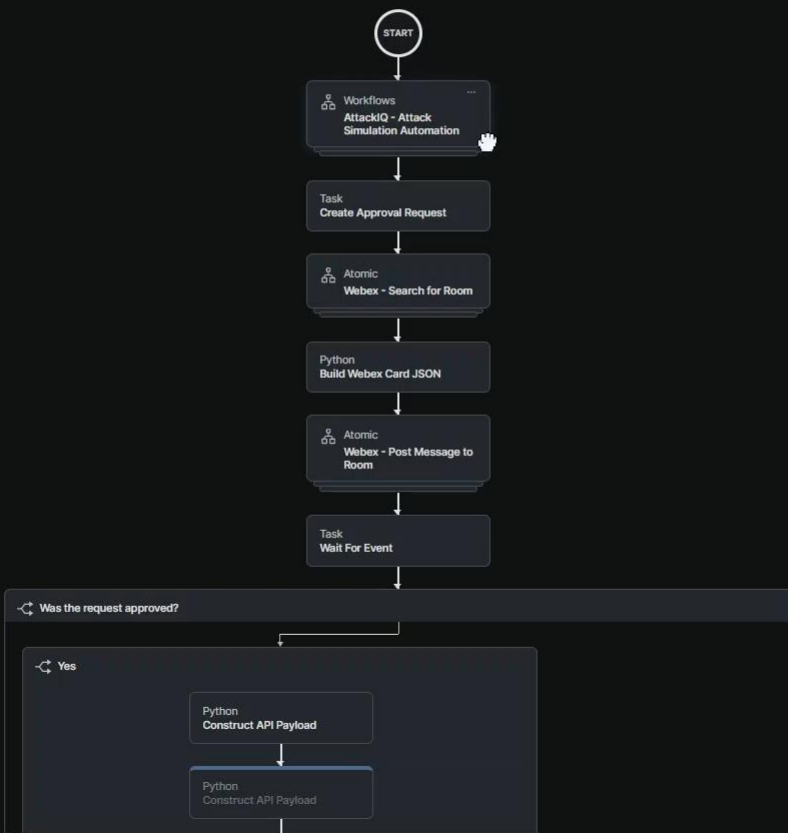
Search activities

Activities Logic Workflows

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
- To Lower
- To Upper
- Trim String
- XPath Query
- XSL Transform

Ansible Tower



Workflow Properties Secure Firewall - Generate Snort Rule With OpenAI

General

Display Name 49 / 64

Secure Firewall - Generate Snort Rule with OpenAI

Owner osanniko@cisco.com

Description 0 / 1024

☐ Clean up after successful execution
If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

☐ Is atomic workflow
An atomic workflow will be listed under the Activity Group header you select or create in the list to the left.

Category

Select

Version

Git Repository

Select

Git Version

No Versions Available

Exchange

There is no Exchange version.

Response Actions

Observable Type(s)

Select

Variables

Name	Type	Scope	Value	Required
------	------	-------	-------	----------

Key Takeaways

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

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



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

Contact me at: osanniko@cisco.com



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC