CISCO
SECURE

CISCO The bridge to possible

Get Started with SecureX

Cisco Customer Experience

Juan Jose Ponce

Customer Success Specialist

June 2022

CISCO SECURE

Panelists

CISCO The bridge to possible

Fran Pena

Divya Jain

Dominik Stefaniak

Vladimir Andryushchenko

David Graff

Artemio Romero

Reorganize your cybersecurity teams with the help of SecureX

NAH, I'M NOT WORRIED ABOUT CLOUD SECURITY. MY STORED DATA IS SO DISORGANIZED THEY'D NEVER BE ABLE TO FIND ANYTHING!

Author: Unknown

Agenda

1. SecureX Value Proposition
2. Understanding SecureX
3. Demo. SecureX Automated Incident Management
4. Services for SecureX
5. Closing and Q&A

SecureX Value Proposition

Cisco Umbrella

Cisco Secure Endpoint

Cisco Secure Firewall

Employee

ESA/CES

The Corporate Premises

Secure Endpoint (Cloud)

ThreatGRID®

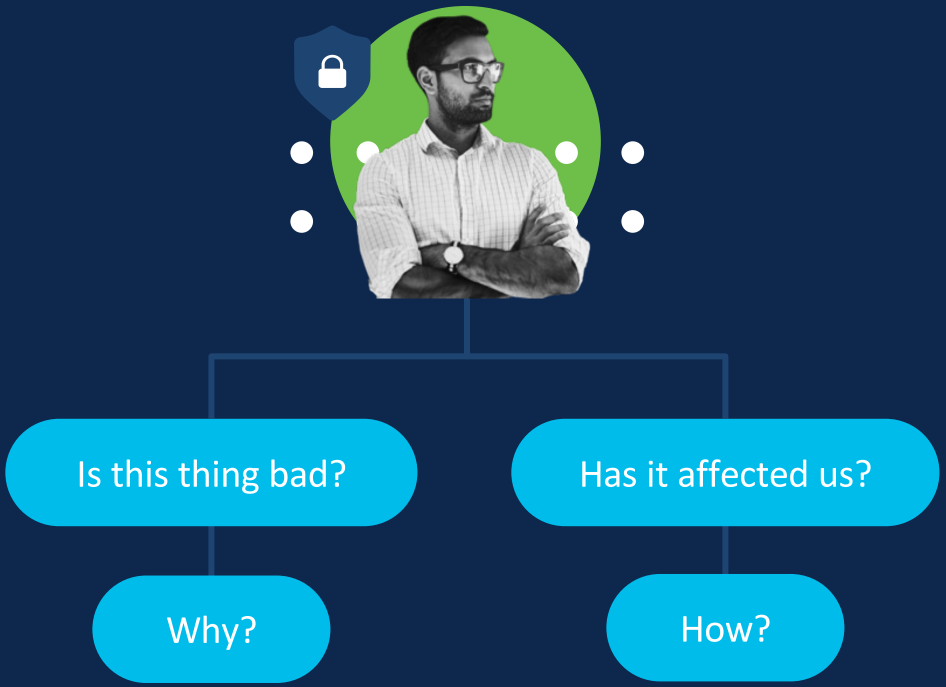
Secure Malware Analytics

TALOS

Top Customer Challenge

Security Does Not Work Together

Security Operations



Is this thing bad?

Has it affected us?

Why?

How?

Technologies and Intelligence

- Threat Intel
- Endpoint Security
- SIEM
- Next-Gen IPS
- Malware Detection
- Secure Internet Gateway
- Email Security
- Web Security
- Third-Party Sources
- Network Analytics
- Next-Gen Firewall
- Identity Management

Entitlement Integrations

What is SecureX

A Cloud-Native, Built-In Platform Experience Within Our Portfolio

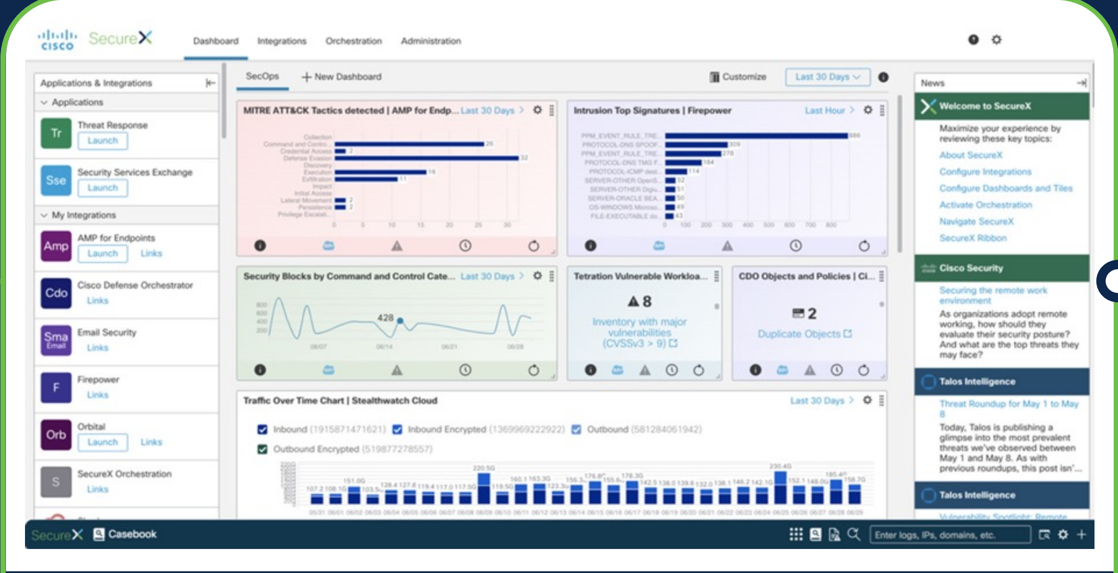
Cisco Secure

Network

Endpoint

Cloud

Applications



Maximize your experience by reviewing these key topics:

About SecureX

Configure Integrations

Configure Dashboards and Tiles

Activate Orchestration

Navigate SecureX

SecureX Ribbon

Securing the remote work environment

As organizations adopt remote working, how should they evaluate their security posture? And what are the top threats they may face?

Threat Roundup for May 1 to May 8

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between May 1 and May 8. As with previous roundups, this post isn'...

Vulnerability Spotlight: Remote

Unified Visibility

SECURE X

Detection Analytics

Investigation Remediation

Managed Policy

Orchestration Automation

Customer Infrastructure

Third-Party/ITSM

Intelligence

Identity

SIEM/SOAR

Customer Teams

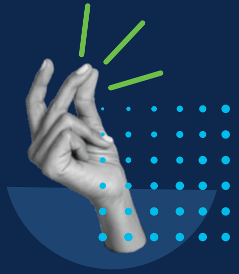
SecOps

ITOps

NetOps

CX Cisco Customer Experience

SecureX Unlocks Value for Your Customers

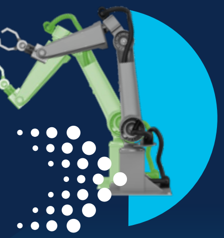


Integrated & Open for

Simplicity

Unified In One Location for

Visibility



Maximized Operational

Efficiency

SECURE X

Integrations
built-in, pre-built
or custom

Ribbon & Sign-on
never leaves you
maintains context

Dashboard
customizable for what
matters to you

Threat Response
is at the core
of the platform

Orchestration
drag-drop GUI
for no/low code

Device Insights
device inventory with the
contextual awareness

Cisco
Customer Experience

Partners

Meaningful Integrations to Protect your Network

Third-Party Security

Operational tools, intelligence sources, infrastructure
protections and visibility

Cisco Infrastructure

Networking, collaboration, server/app, and Multicloud management platforms

Third-Party Infrastructure

IT service management, and cloud/virtual and DevOps platforms

General Toolsets

Scripting/dev tools, system interfaces, data exchanges,
and messaging protocols

Safe Browsing Google
VirusTotal
radware
FARSIGHT SECURITY
POLARITY
Pulsedive

chronicle
Microsoft Security
Qualys.
SpyCloud
swimlane
Cyberprotect

IBM Security
servicenow
Gigamon
THREATQUOTIENT
TheHive
SHODAN

splunk>enterprise
splunk> phantom
Signal Sciences
urlscan.io
AbuseIPDB
';--have i been pwned?

aws
Microsoft Azure
Google Cloud
vmware
puppet
openstack.

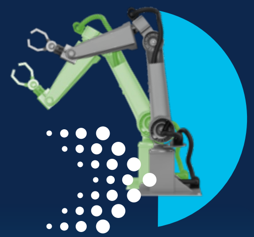
CHEF
ANSIBLE
OPENSHIFT
HTTP SMTP SNMP

Windows

cisco
DNA Center
Meraki
ACI
Cisco Webex
APPDYNAMICS
UCS Director
CloudCenter

...and more!

Introducing the 3 Pillars of SecureX



Detect and hunt For Threats

SOC Enablement

Integrate SecureX into your SOC while also benchmarking and improving your operational processes

Respond to Incidents

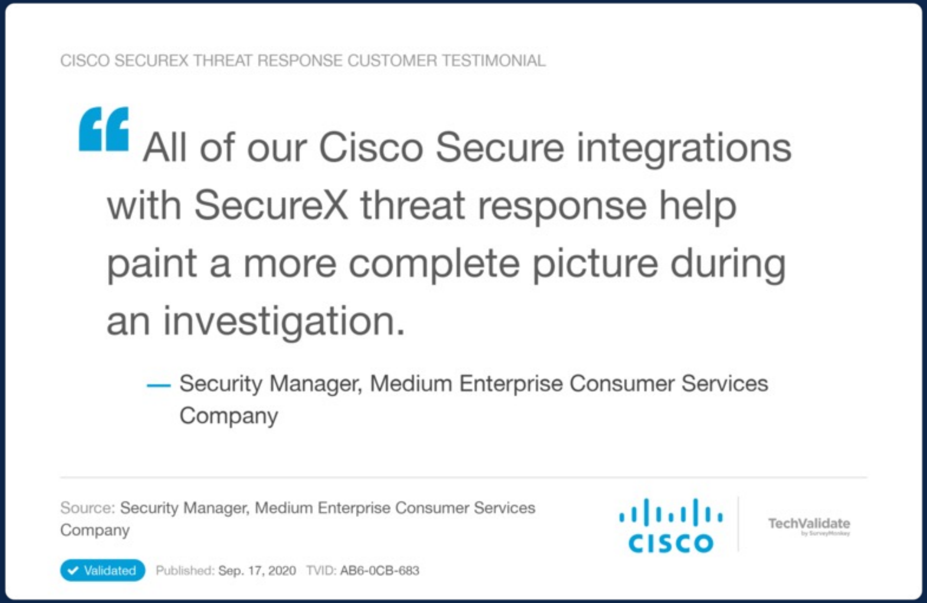
Incident Response

Plan, prepare and response to incidents identified through SecureX

Orchestrate and Automate Response

Automation and Orchestration

Identity automation opportunities and build custom playbooks across Cisco and multi-vendor solutions.



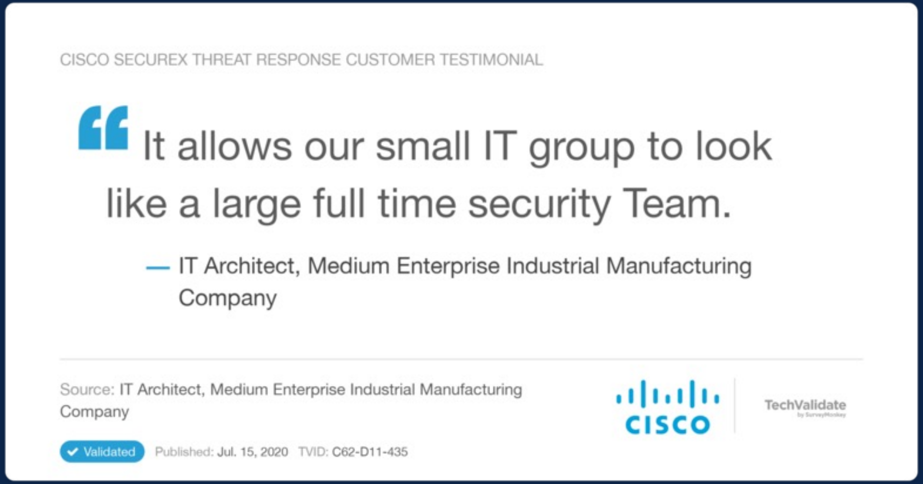
CISCO SECUREX THREAT RESPONSE CUSTOMER TESTIMONIAL

> “All of our Cisco Secure integrations with SecureX threat response help paint a more complete picture during an investigation.
>
> — Security Manager, Medium Enterprise Consumer Services Company

Source: Security Manager, Medium Enterprise Consumer Services Company

✓ Validated Published: Sep. 17, 2020 TVID: AB6-0CB-683

cisco
TechValidate



CISCO SECUREX THREAT RESPONSE CUSTOMER TESTIMONIAL

> “It allows our small IT group to look like a large full time security Team.
>
> — IT Architect, Medium Enterprise Industrial Manufacturing Company

Source: IT Architect, Medium Enterprise Industrial Manufacturing Company

✓ Validated Published: Jul. 15, 2020 TVID: C62-D11-435

cisco
TechValidate

Cisco SecureX customer insights

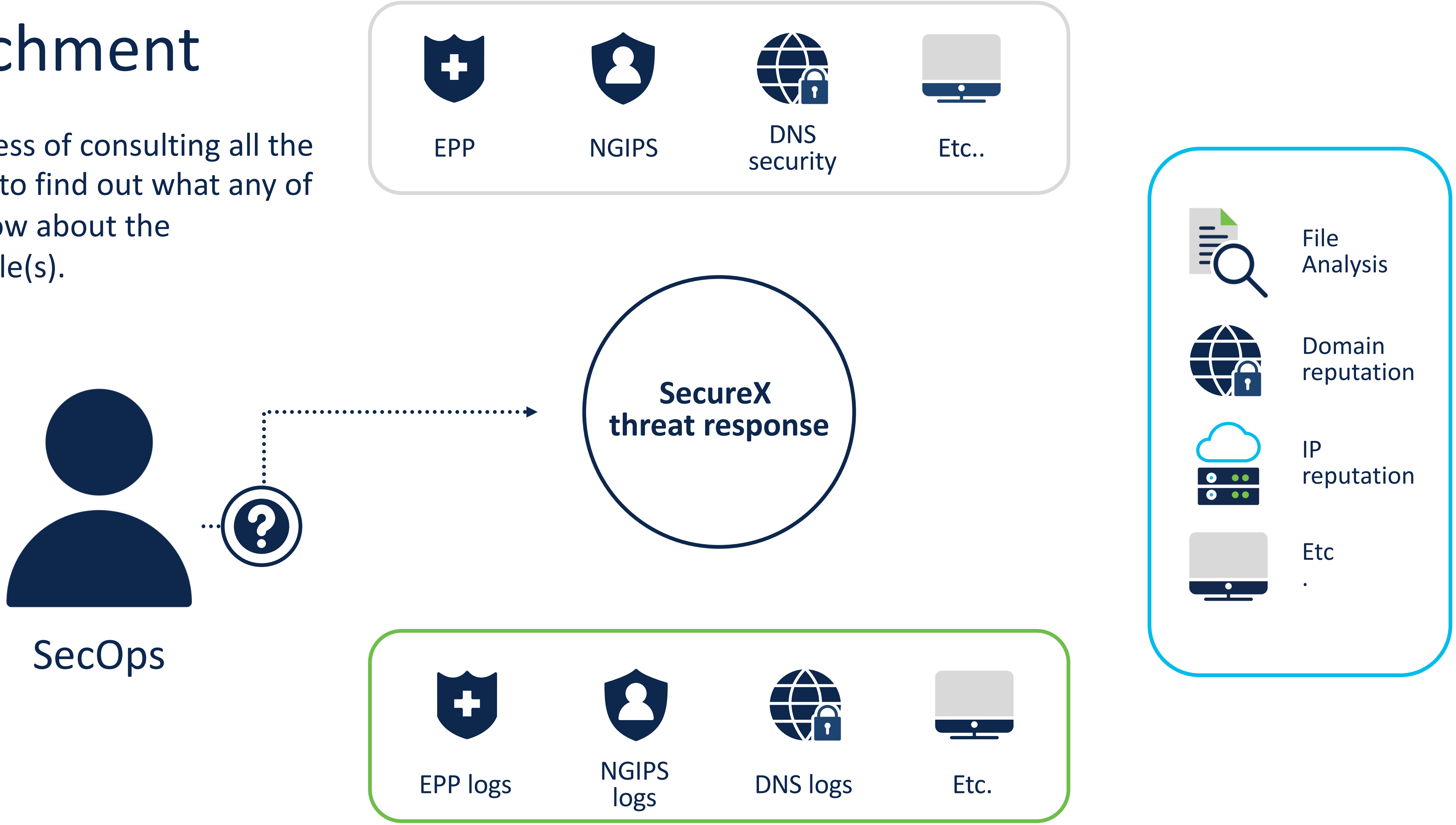
www.techvalidate.com/portals/securex-customer-insights

CX Cisco Customer Experience

Understanding SecureX

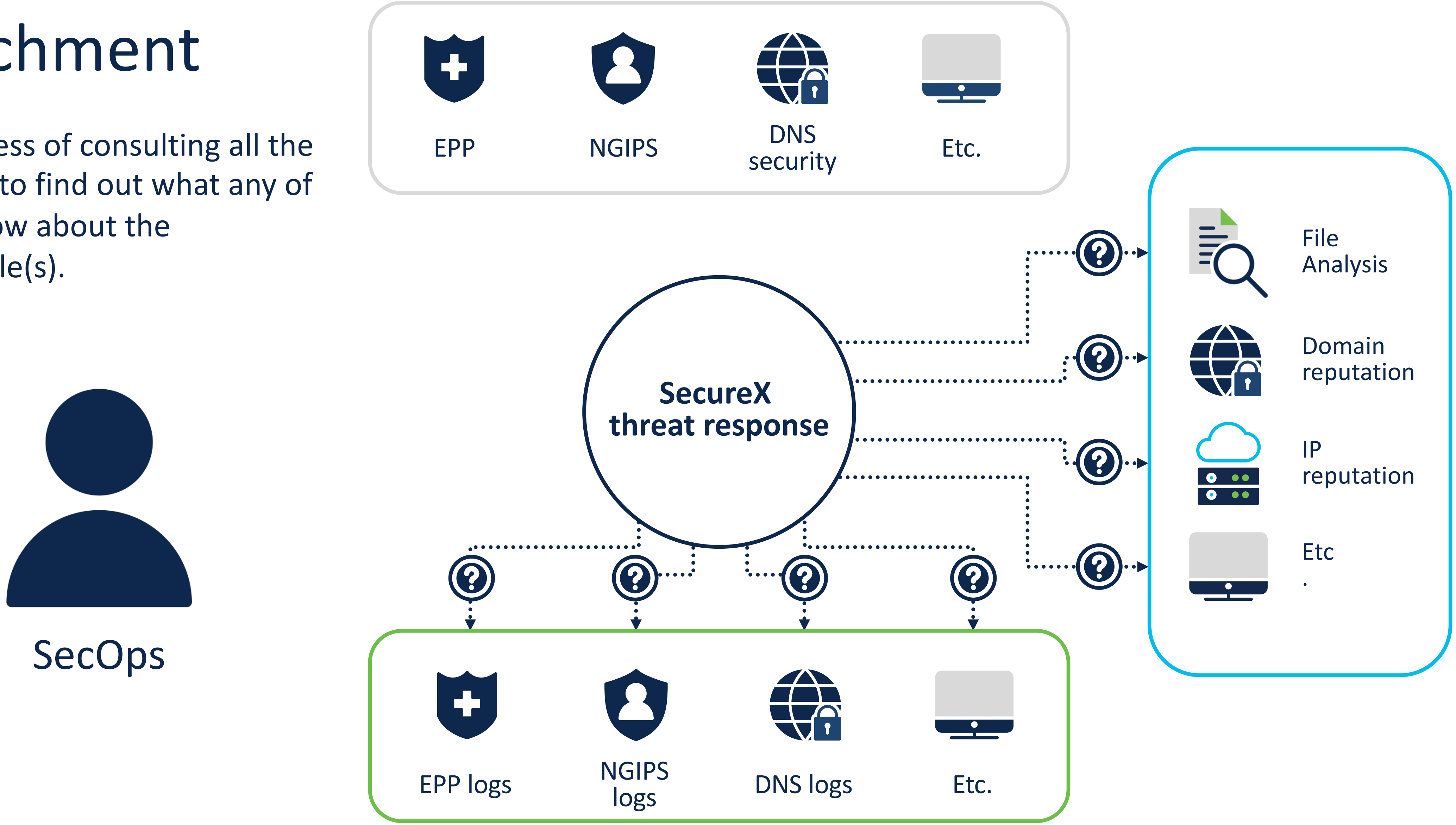
Enrichment

The process of consulting all the modules to find out what any of them know about the observable(s).



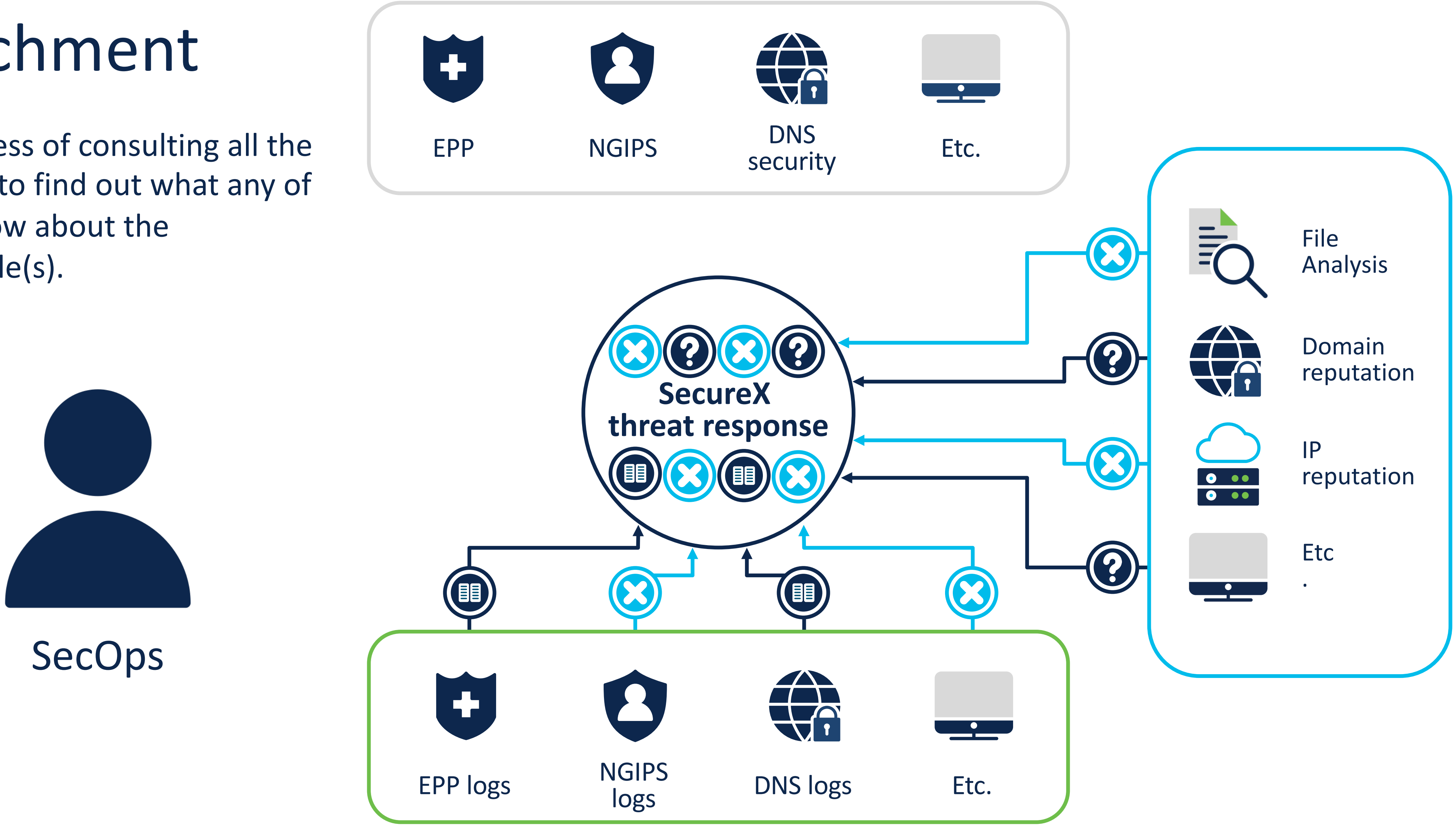
Enrichment

The process of consulting all the modules to find out what any of them know about the observable(s).



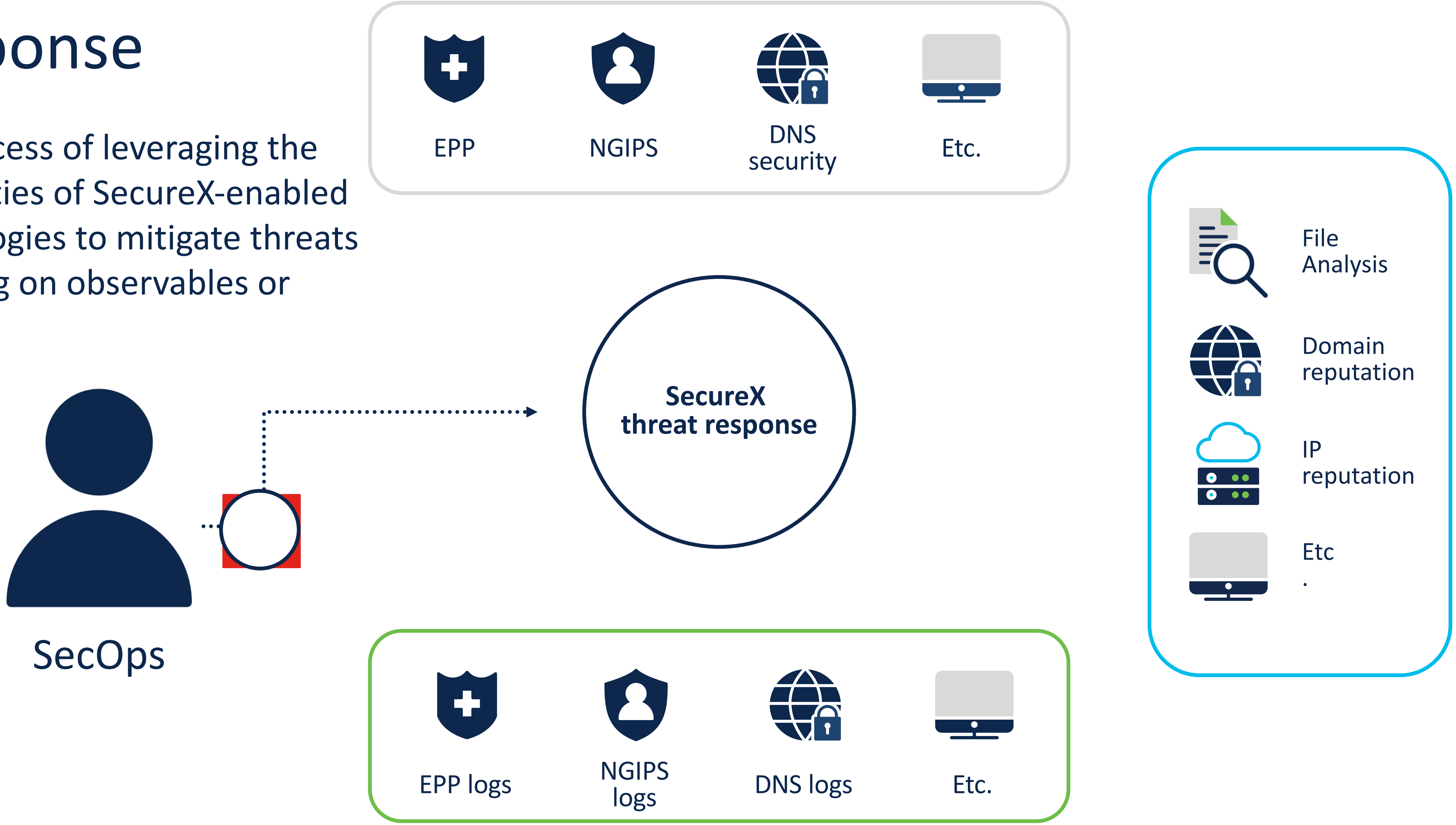
Enrichment

The process of consulting all the modules to find out what any of them know about the observable(s).



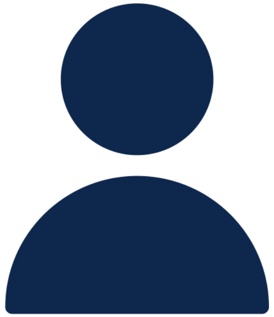
Response

The process of leveraging the capabilities of SecureX-enabled technologies to mitigate threats by acting on observables or targets

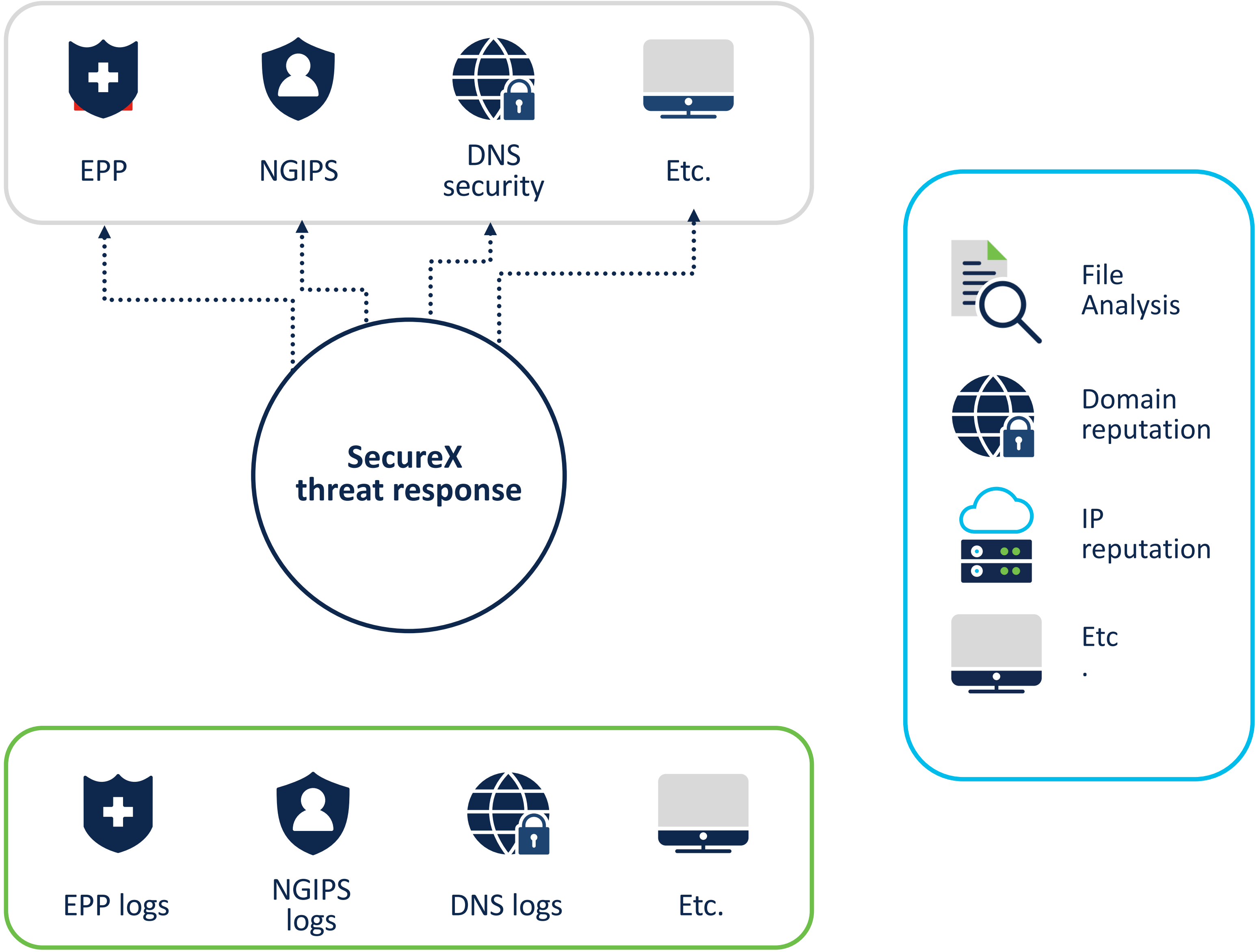


Response

The process of leveraging the capabilities of SecureX-enabled technologies to mitigate threats by acting on observables or targets



SecOps



SecureX Orchestration

I’m a Cisco Secure customer with SecureX threat response

My team can:

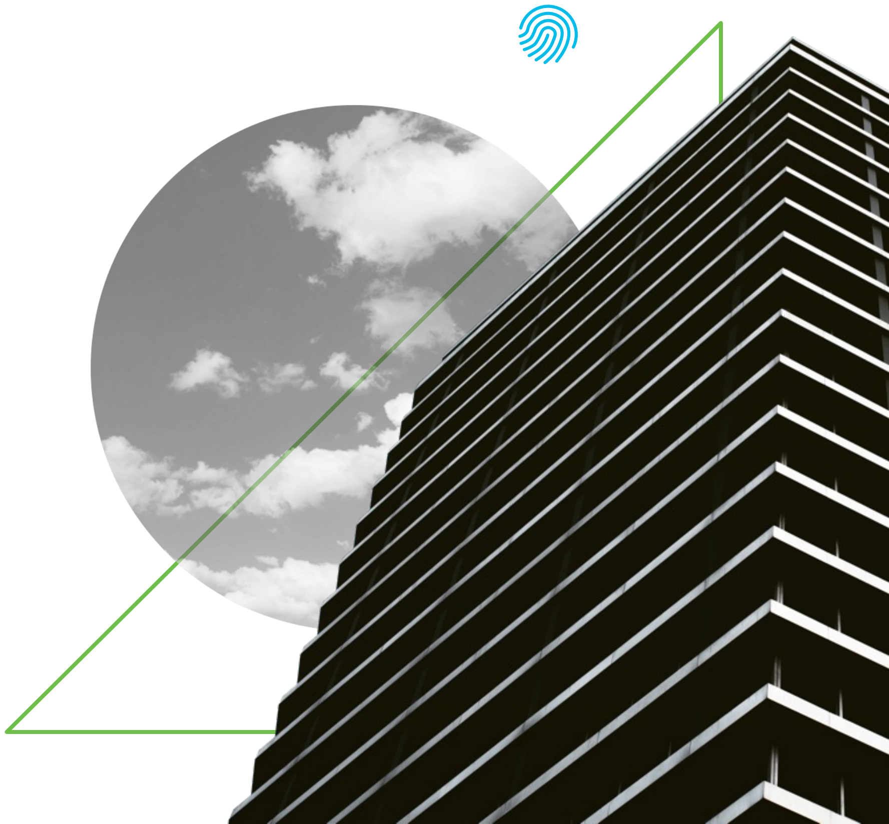
- Answer questions faster about observables.
- Block and unblock domains from threat response.
- Block and unblock file executions from threat response
- Isolate Hosts
- Hunt for an observable associated with a known actor and immediately see organizational impact.
- Save a point in time snapshot of our investigations for further analysis.
- Document our analysis in a cloud casebook from all integrated or web-accessible tools, via an API.
- Integrate threat response easily into existing processes and custom tools
- Store our own threat intel in threat response private intel for use in investigations
- See Incidents all in one place

Demo

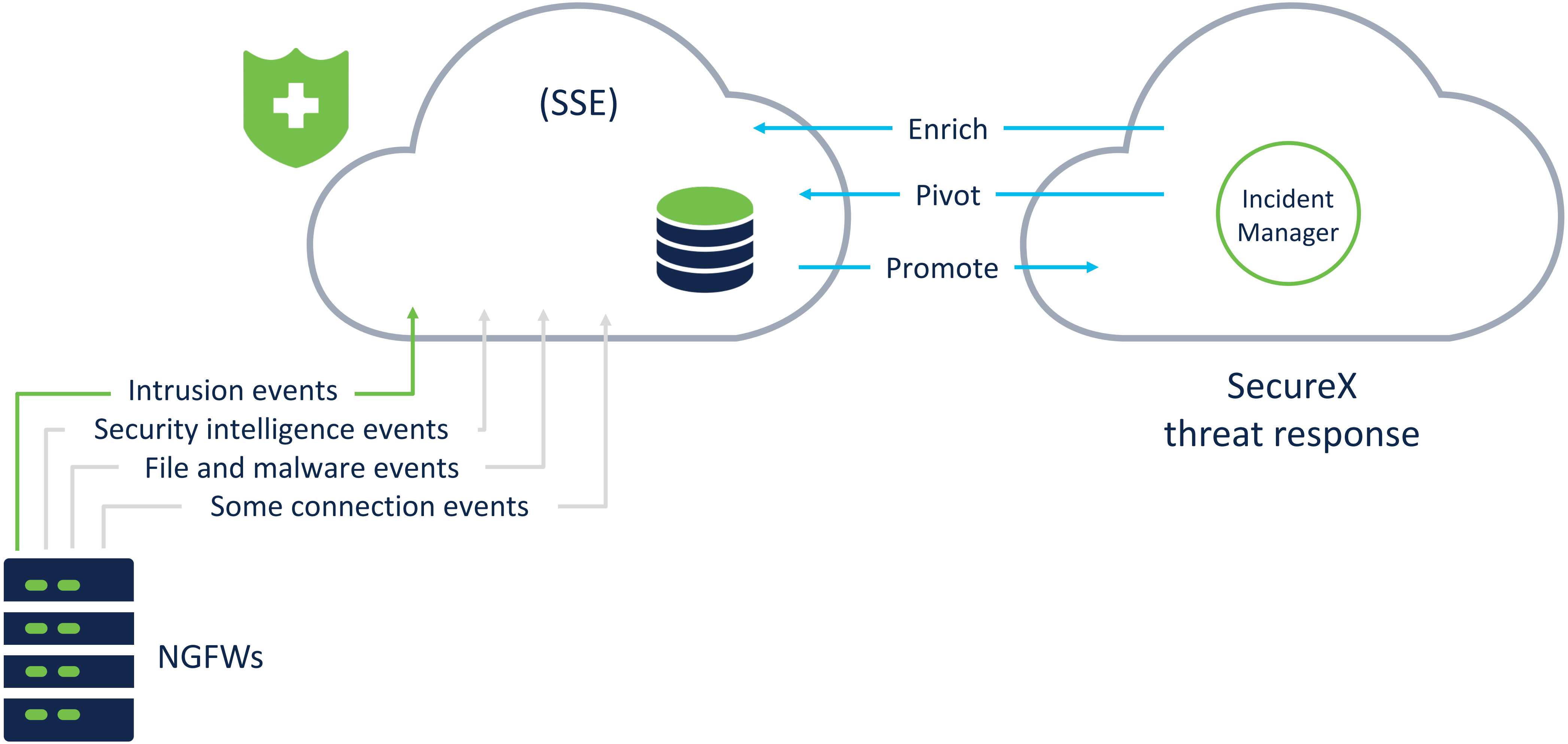
SecureX automated incident management

Retailer with multiple branches generate massive amounts of firewall incidents increasing complexity to effectively analyse and remediate them

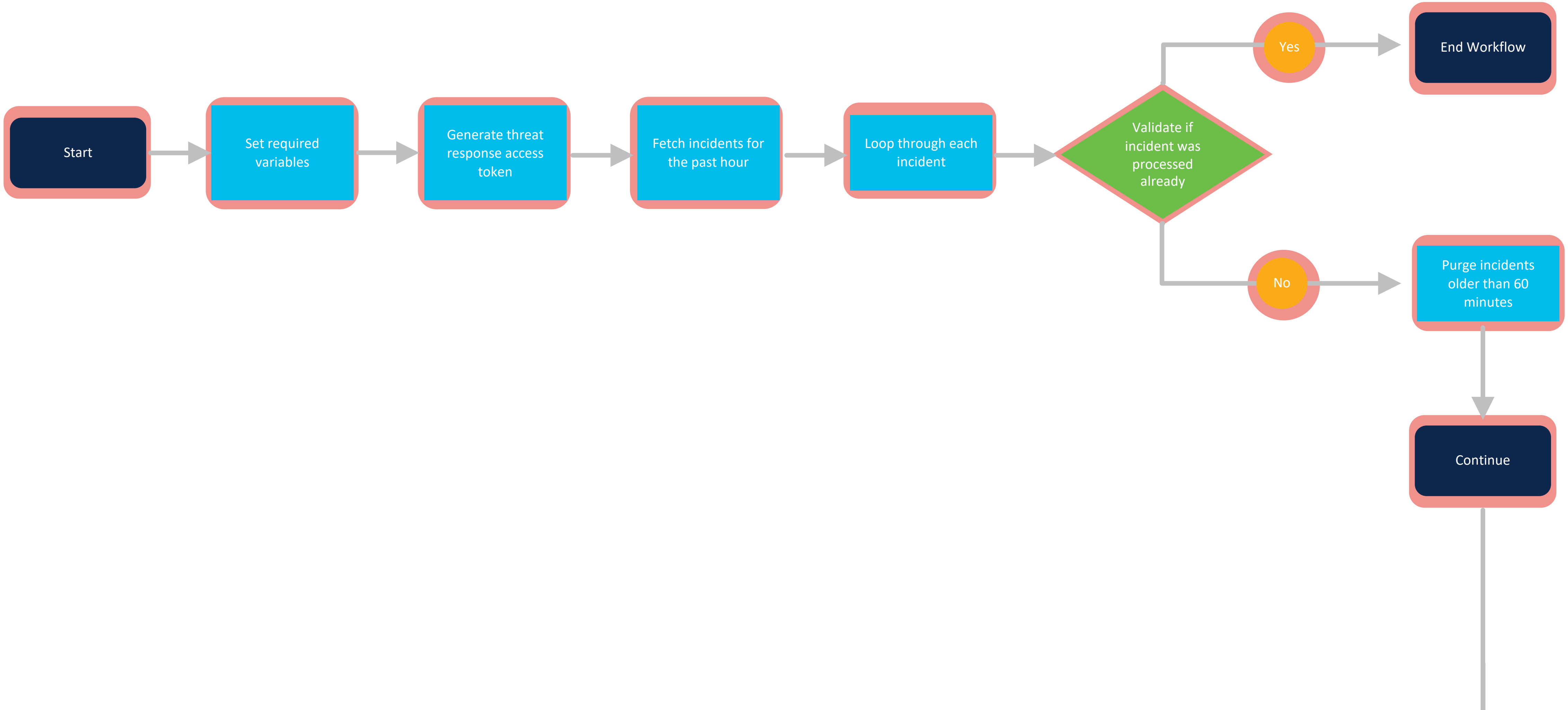
- Problem:
  - IT spends too much time analysing firewall incidents
- Solution:
  - Leverage SecureX detect, response and orchestration capabilties to analyse incidents from Firewalls
- Outcome:
  - Achieve consistency through automation
  - Reclaim headcount
  - Reduce mean time to detect (MTTD)



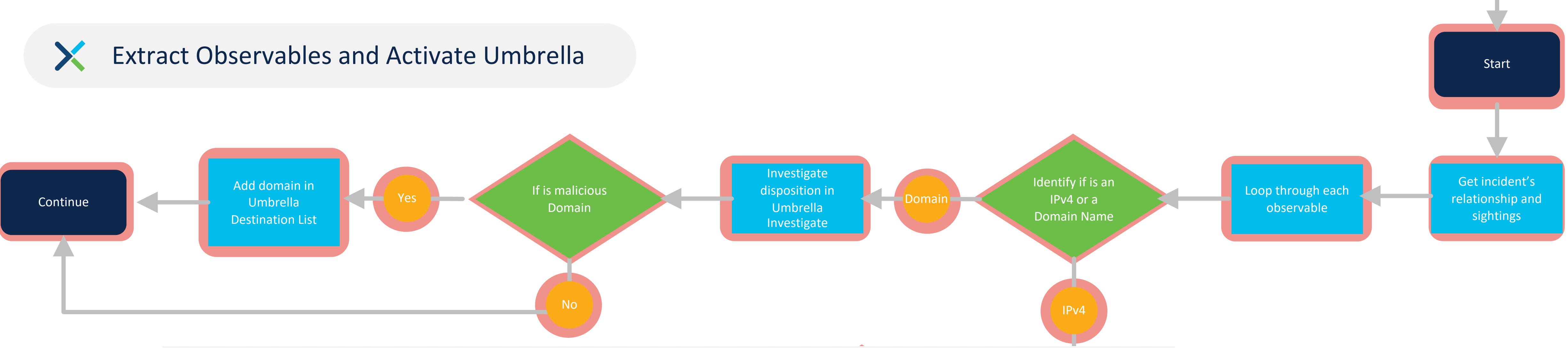
Cisco Secure Firewall Integration with SecureX



Instantiate Workflow and Validate Incident


Start
Set required variables
Generate threat response access token
Fetch incidents for the past hour
Loop through each incident
Validate if incident was processed already
Yes
End Workflow
No
Purge incidents older than 60 minutes
Continue

Extract Observables and Activate Umbrella



Start

Get incident's relationship and sightings

Loop through each observable

Identify if is an IPv4 or a Domain Name

Domain

IPv4

Investigate disposition in Umbrella Investigate

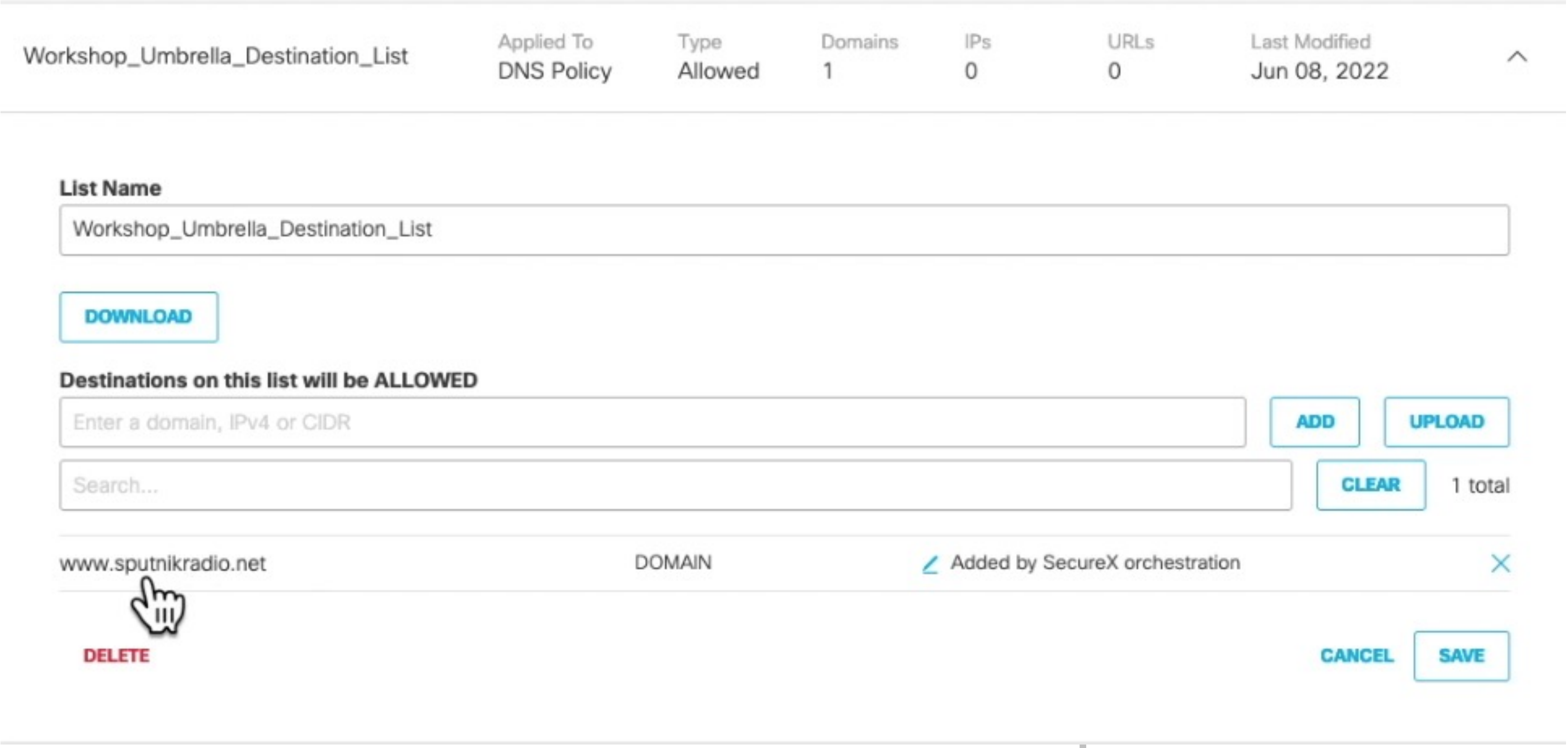
If is malicious Domain

Yes

No

Add domain in Umbrella Destination List

Continue



Workshop_Umbrella_Destination_List	Applied To	Type	Domains	IPs	URLs	Last Modified
	DNS Policy	Allowed	1	0	0	Jun 08, 2022

List Name

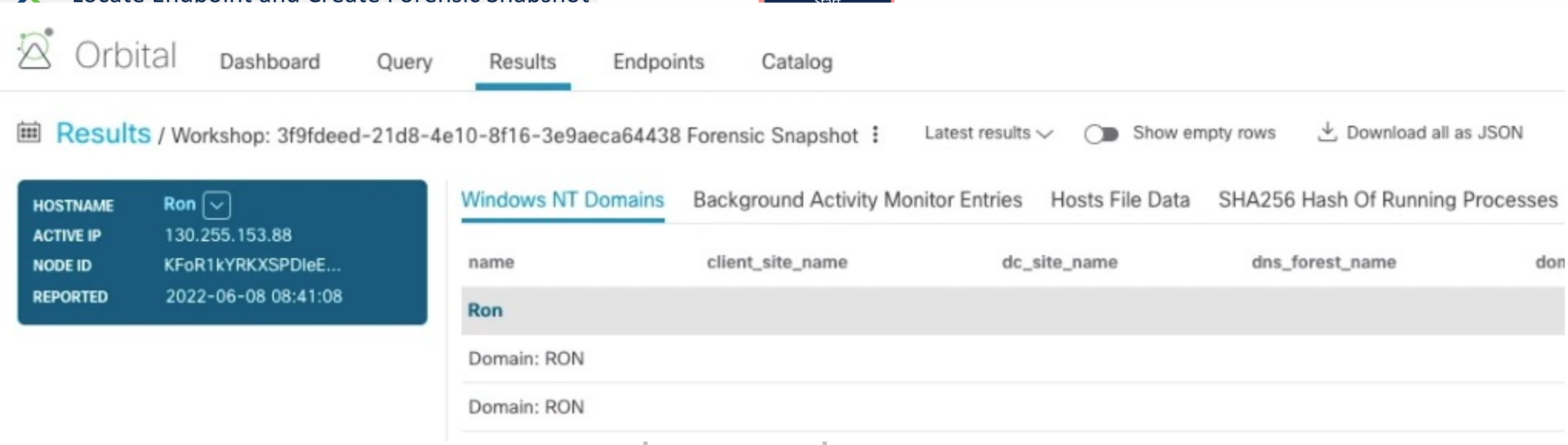
Workshop_Umbrella_Destination_List

Destinations on this list will be ALLOWED

1 total

www.sputnikradio.net DOMAIN Added by SecureX orchestration

Locate Endpoint and Create Forensic Snapshot



Orbital · Dashboard · Query · Results · Endpoints · Catalog

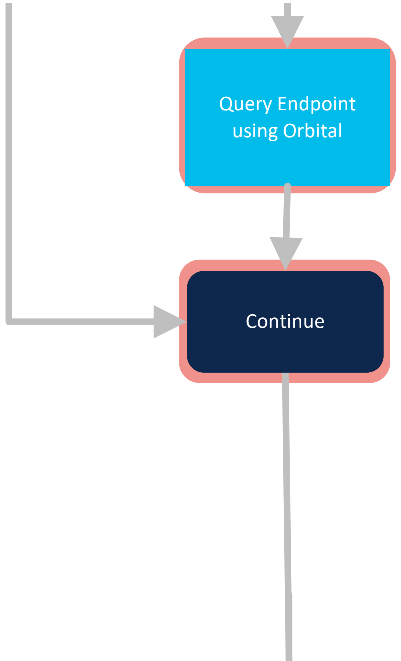
Results / Workshop: 3f9fdeed-21d8-4e10-8f16-3e9aeca64438 Forensic Snapshot

Latest results · Show empty rows · Download all as JSON

HOSTNAME	Ron
ACTIVE IP	130.255.153.88
NODE ID	KFoR1kYRKXSPDleE...
REPORTED	2022-06-08 08:41:08

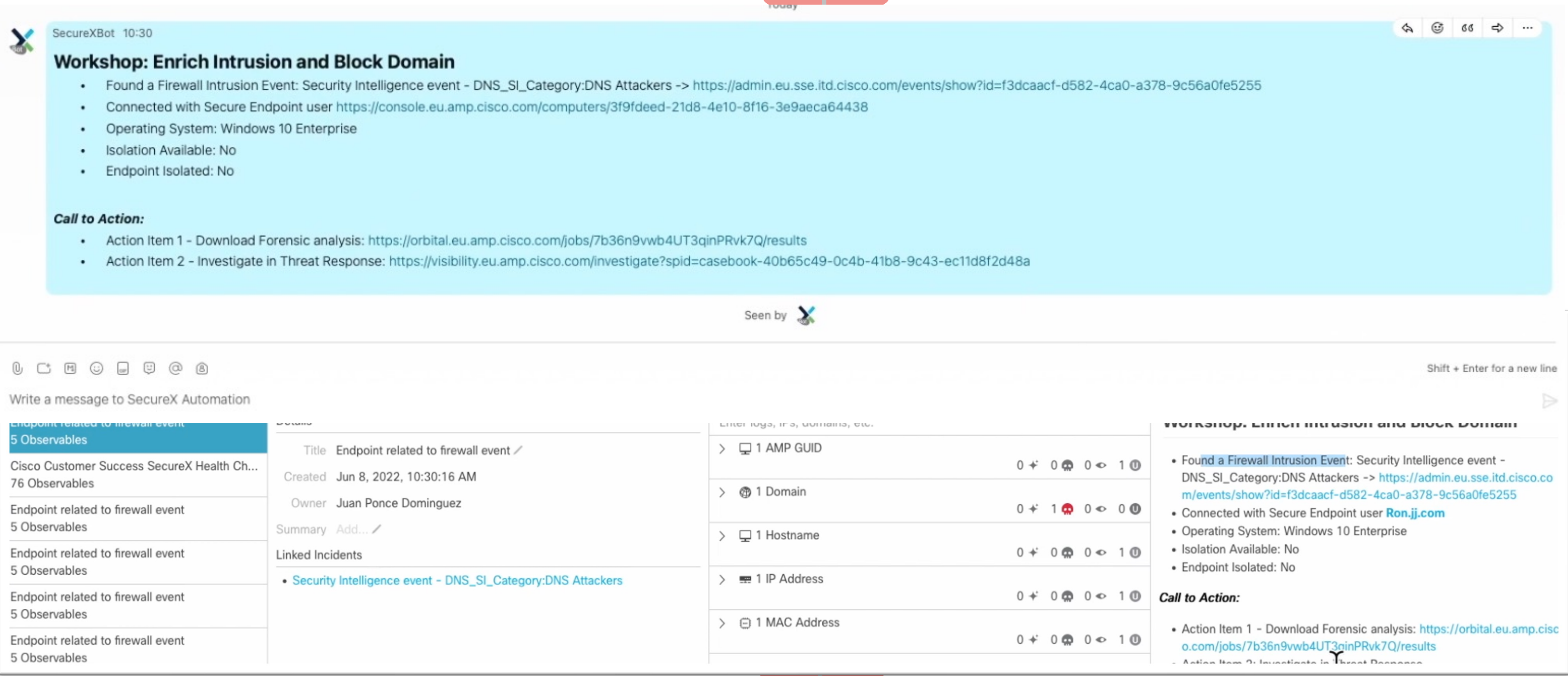
Windows NT Domains · Background Activity Monitor Entries · Hosts File Data · SHA256 Hash Of Running Processes

name	client_site_name	dc_site_name	dns_forest_name	don
Ron				
Domain: RON				
Domain: RON				



Notify SOC teams of Results

Start



SecureXBot 10:30

Workshop: Enrich Intrusion and Block Domain

- Found a Firewall Intrusion Event: Security Intelligence event - DNS_SI_Category:DNS Attackers -> https://admin.eu.sse.itd.cisco.com/events/show?id=f3dcaacf-d582-4ca0-a378-9c56a0fe5255
- Connected with Secure Endpoint user https://console.eu.amp.cisco.com/computers/3f9fdeed-21d8-4e10-8f16-3e9aeca64438
- Operating System: Windows 10 Enterprise
- Isolation Available: No
- Endpoint Isolated: No

Call to Action:

- Action Item 1 - Download Forensic analysis: https://orbital.eu.amp.cisco.com/jobs/7b36n9vwb4UT3qinPRvk7Q/results
- Action Item 2 - Investigate in Threat Response: https://visibility.eu.amp.cisco.com/investigate?spid=casebook-40b65c49-0c4b-41b8-9c43-ec11d8f2d48a

Seen by

Write a message to SecureX Automation

Endpoint related to firewall event
5 Observables

Cisco Customer Success SecureX Health Ch...
76 Observables

Endpoint related to firewall event
5 Observables

Endpoint related to firewall event
5 Observables

Endpoint related to firewall event
5 Observables

Endpoint related to firewall event
5 Observables

Details

Title	Endpoint related to firewall event
Created	Jun 8, 2022, 10:30:16 AM
Owner	Juan Ponce Dominguez
Summary	Add...

Linked Incidents

- Security Intelligence event - DNS_SI_Category:DNS Attackers

Enter logs, IPs, domains, etc.

```
> 1 AMP GUID      0 ✦  0 ☠  0 ⊂  1 ⓘ
> 1 Domain        0 ✦  1 ☠  0 ⊂  0 ⓘ
> 1 Hostname      0 ✦  0 ☠  0 ⊂  1 ⓘ
> 1 IP Address    0 ✦  0 ☠  0 ⊂  1 ⓘ
> 1 MAC Address   0 ✦  0 ☠  0 ⊂  1 ⓘ
```

Workshop: Enrich Intrusion and Block Domain

- Found a Firewall Intrusion Event: Security Intelligence event - DNS_SI_Category:DNS Attackers -> https://admin.eu.sse.itd.cisco.com/events/show?id=f3dcaacf-d582-4ca0-a378-9c56a0fe5255
- Connected with Secure Endpoint user Ron.jj.com
- Operating System: Windows 10 Enterprise
- Isolation Available: No
- Endpoint Isolated: No

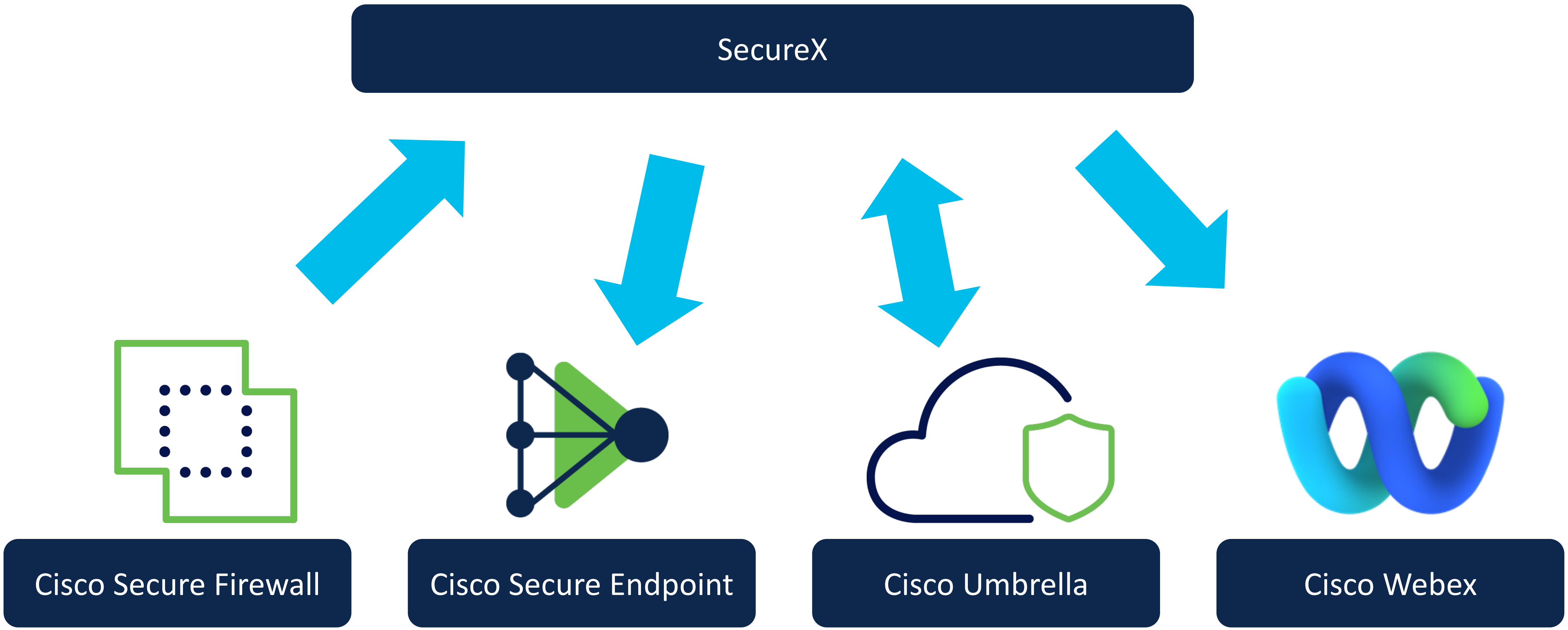
Call to Action:

- Action Item 1 - Download Forensic analysis: https://orbital.eu.amp.cisco.com/jobs/7b36n9vwb4UT3qinPRvk7Q/results
- Action Item 2: Investigate in Threat Response

End Workflow

SecureX Demo: Automated Incident Management

SECURE X



SecureX

Cisco Secure Firewall

Cisco Secure Endpoint

Cisco Umbrella

Cisco Webex

Want to try this workflow?:

https://cutt.ly/secx_june22

Safe trackable link that redirects to Github.com

CISCO SECURE