

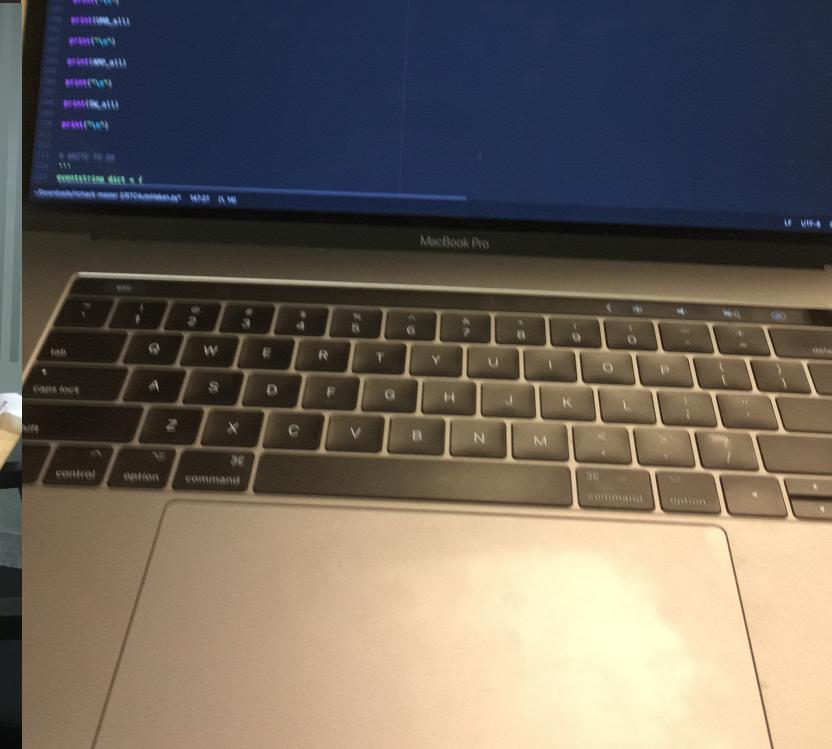
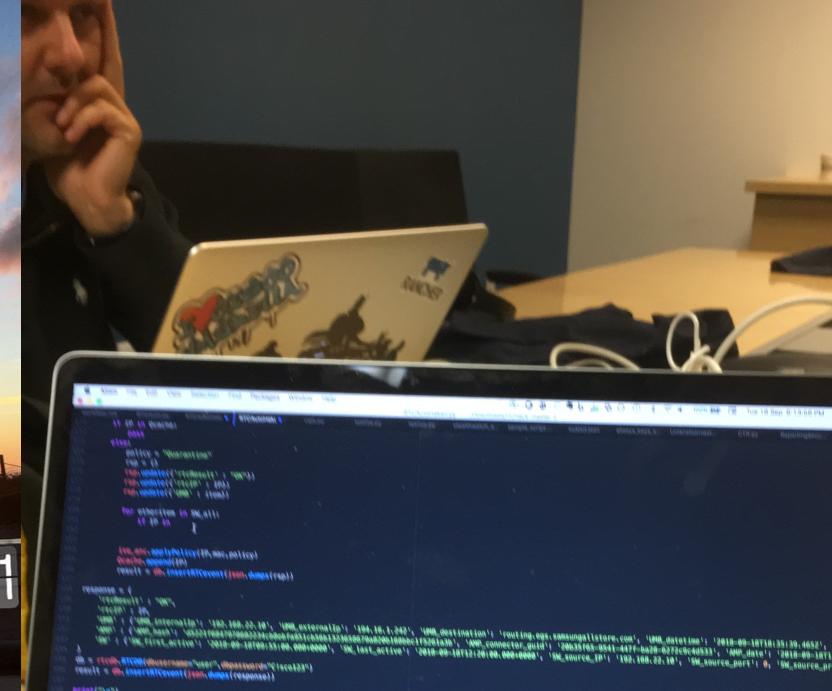
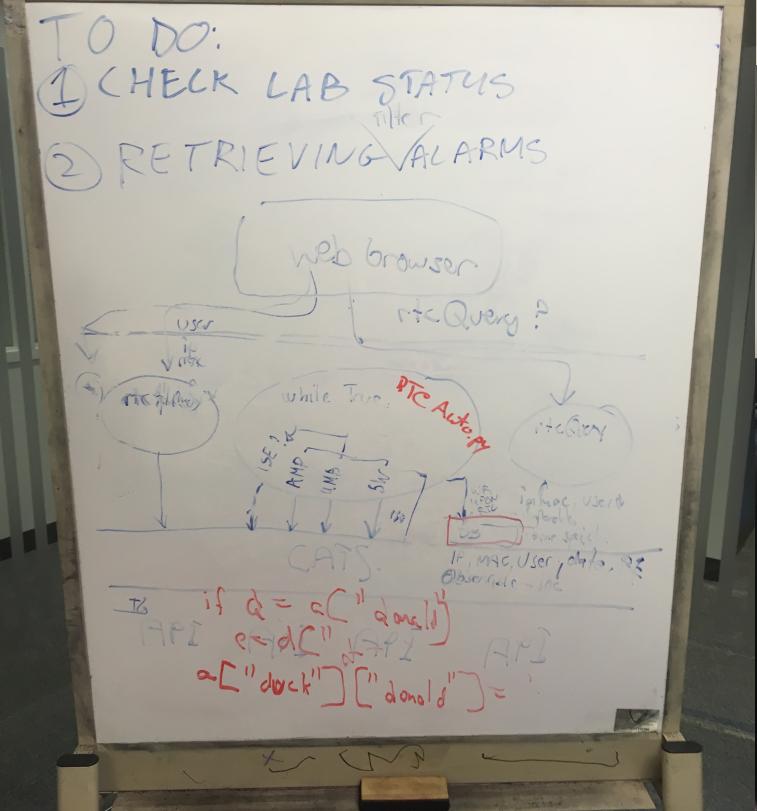
# SecureX Rapid Threat Containment

“RTC in da Cloud” “RTCAaaS”

*Multi-Domain Rapid Threat Containment without the False Positives*

Christopher van der Made and Håkan Nohre

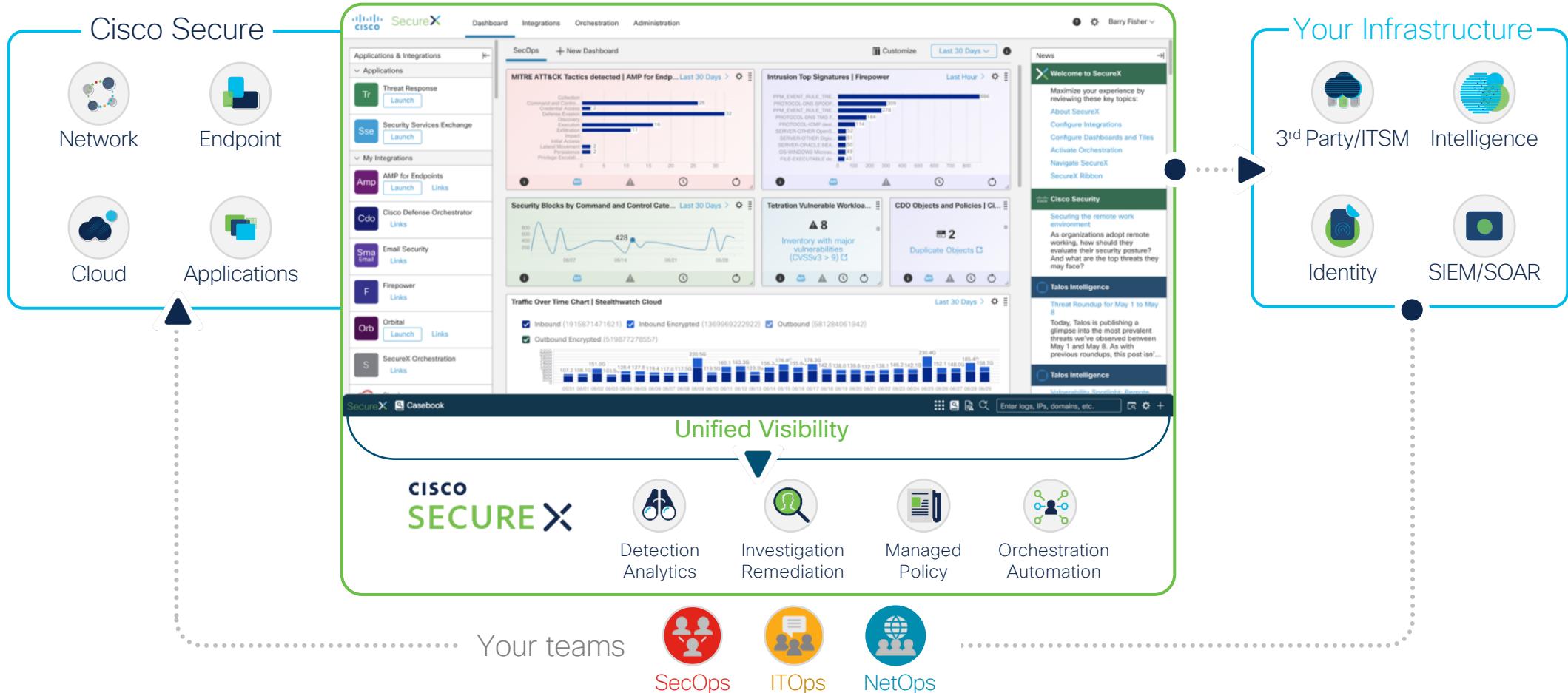




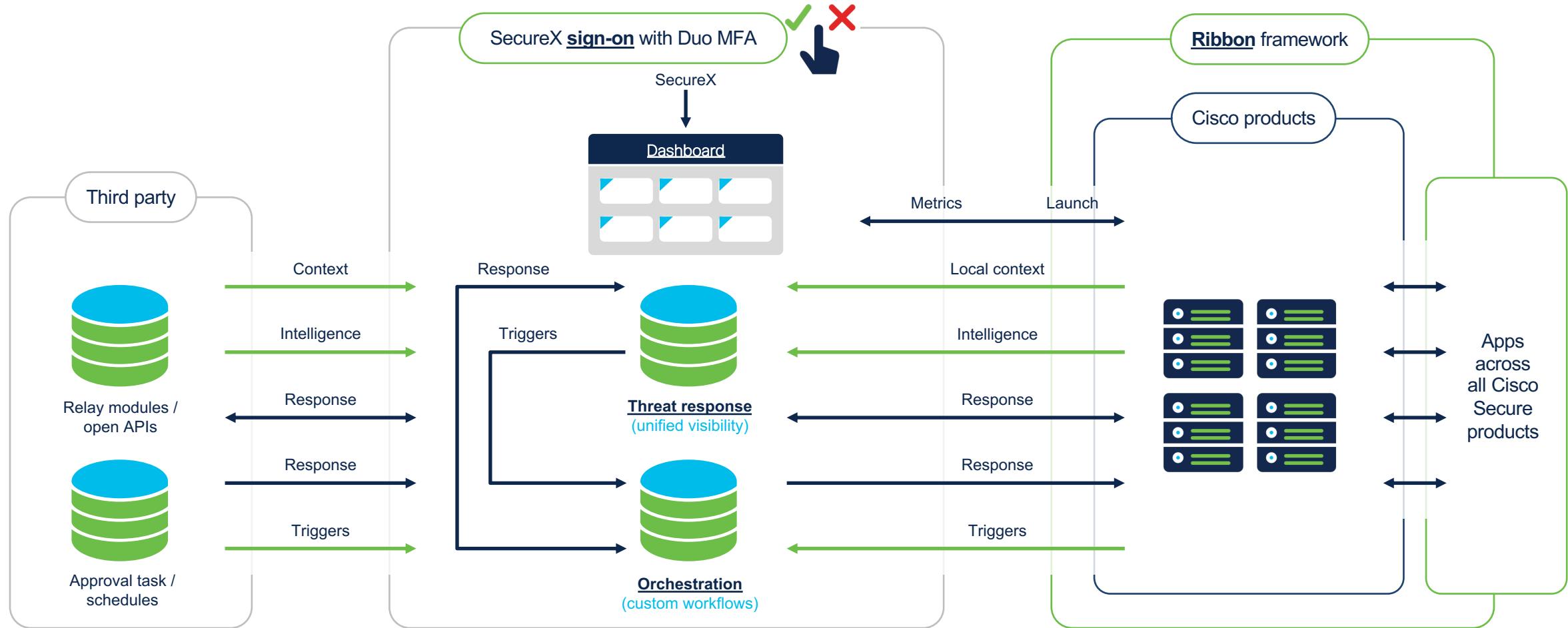
# Introduction to SecureX

# Introducing SecureX

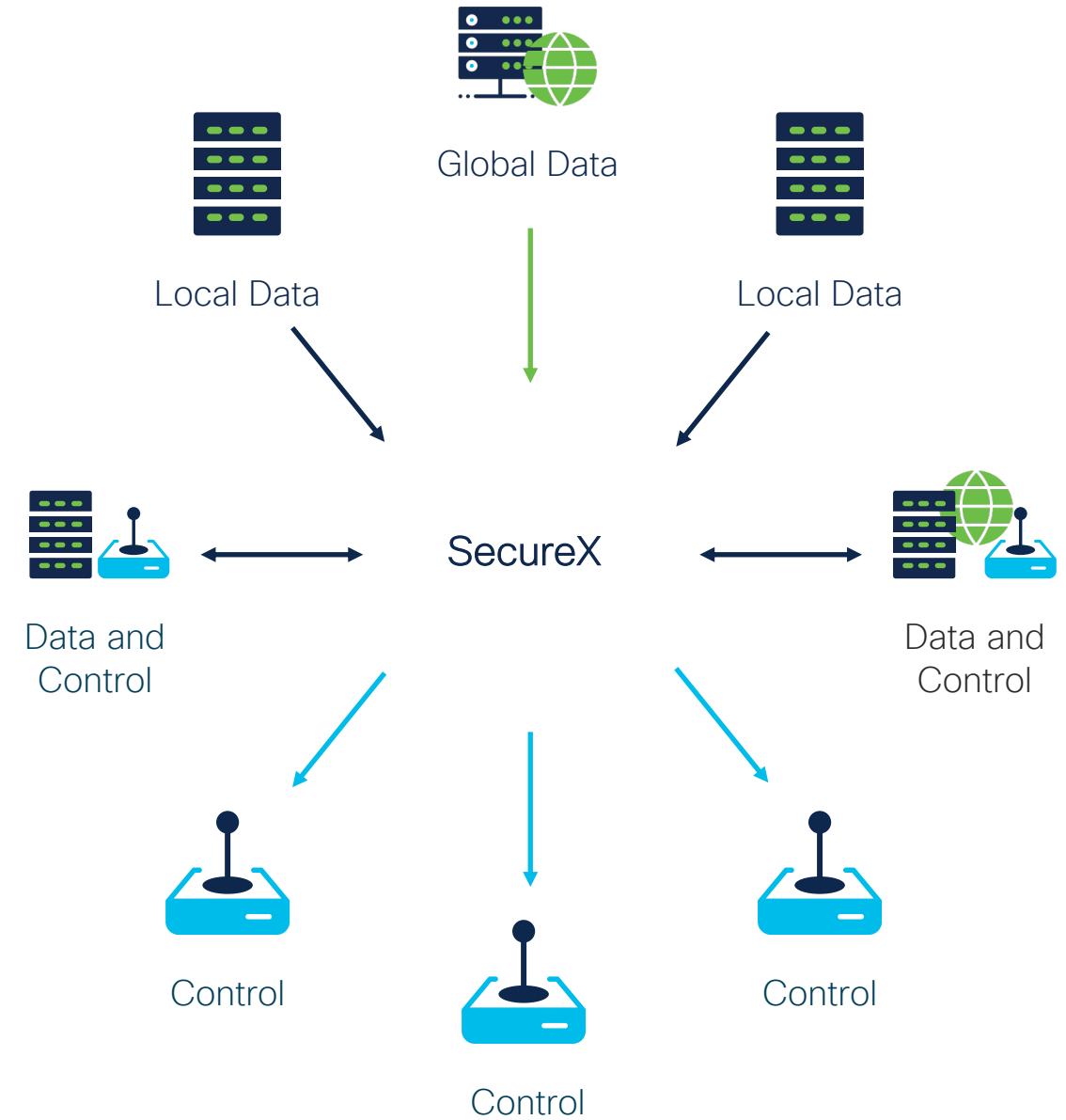
A cloud-native, built-in platform experience within our portfolio



# SecureX architecture



# API aggregation at work



# SecureX orchestration

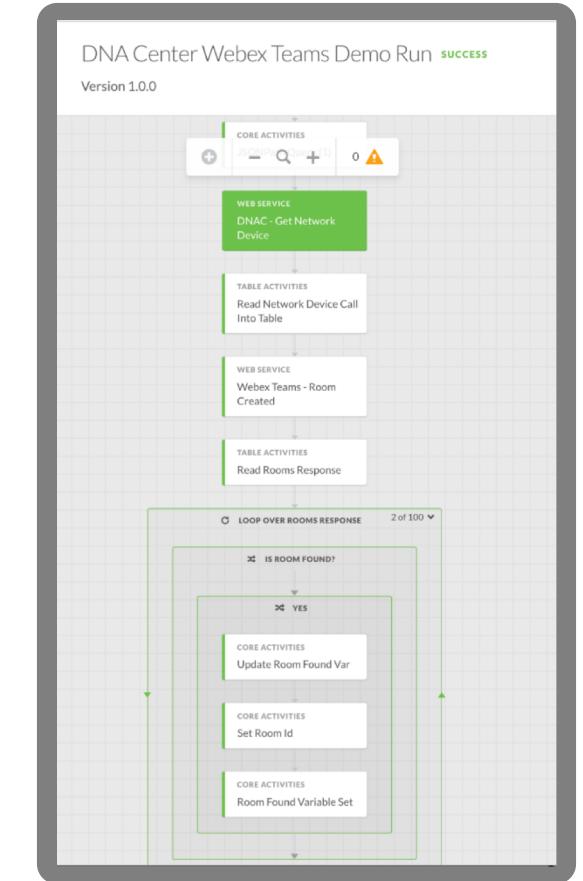
Cloud-Native, microservice architecture with “API-first” design

- Highly Performant, Scalable and Secure
- Reusable and Embeddable

Intuitive drag-drop UI with visual workflows

Combine flexible out of the box adapters to create new integrations

- Automate tasks according to schedules or external events such as email events

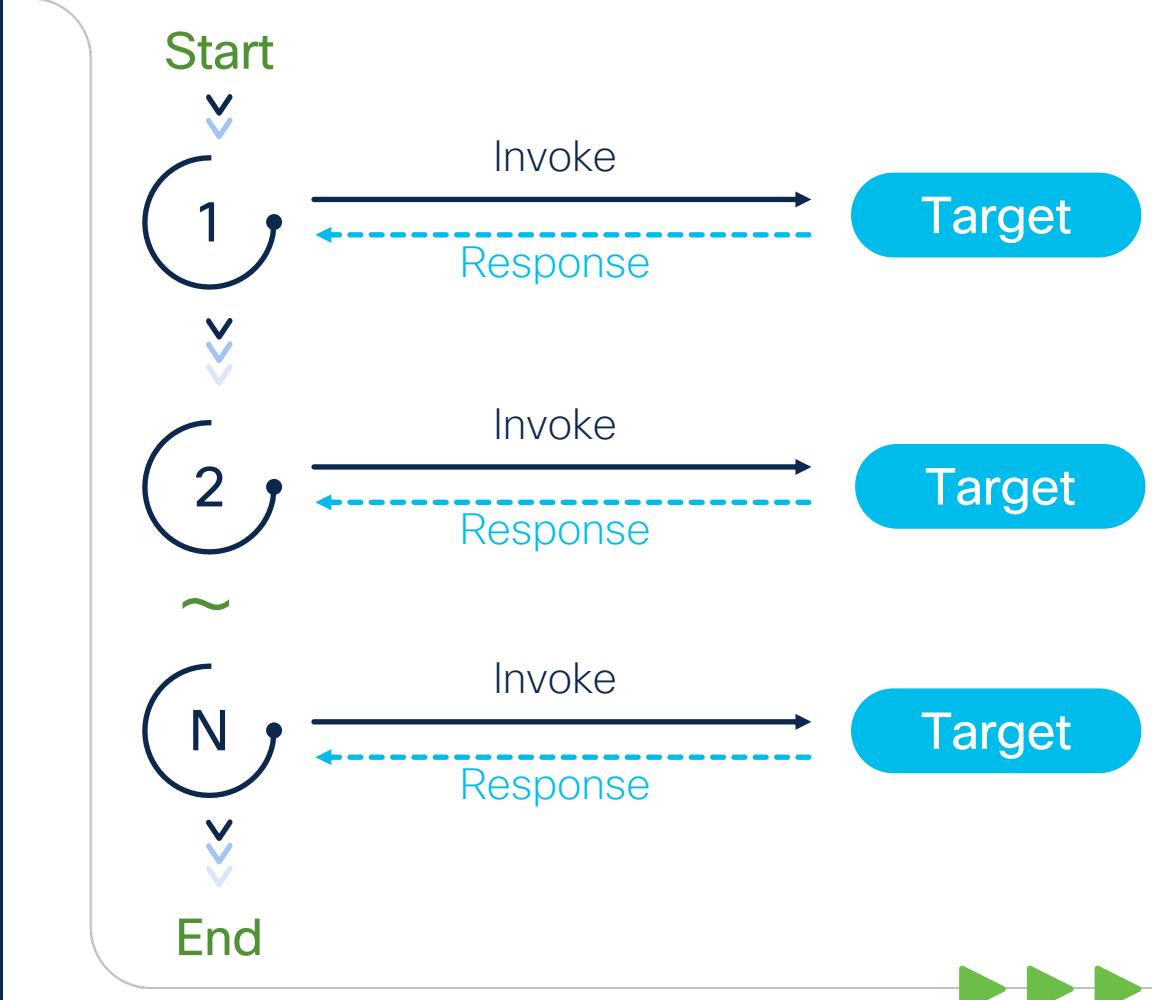


# SecureX orchestration

Ecosystem integration standardized using adapters and workflows

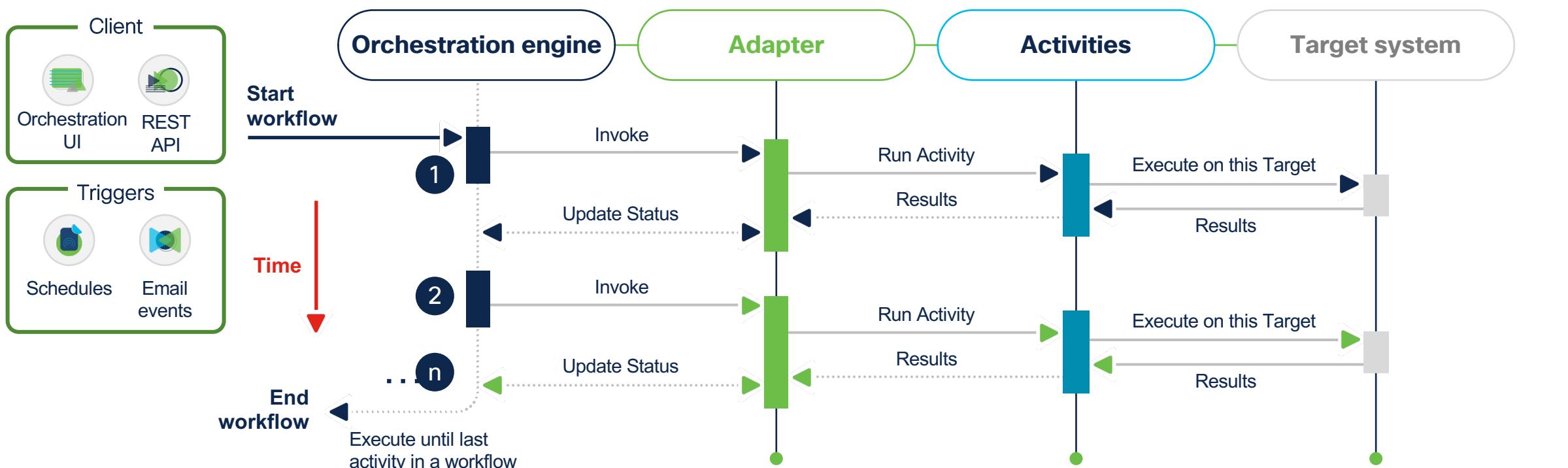
- Execute workflows with business and technical logic
- Use included adapters & activities  
... or create custom ones!

**Benefits:** Eliminate repetitive tasks and broaden scope of cloud orchestration, simplify business process and reduce human error



# SecureX orchestration workflow sequence

The orchestration engine invokes **adapters** to execute **activities** on the target systems, which returns results and **status**, then the next step in the workflow begins.



**Adapter:**  
Integration with a target system,  
provides activities to perform task  
automation

**Activity:**  
REST call, Run terminal,  
Send email ... etc.

**Target System:**  
The host/endpoint that  
executes an activity

**KEEP  
CALM  
IT IS  
DEMO  
TIME**

# Problem Statement



Wh

/ of

FA

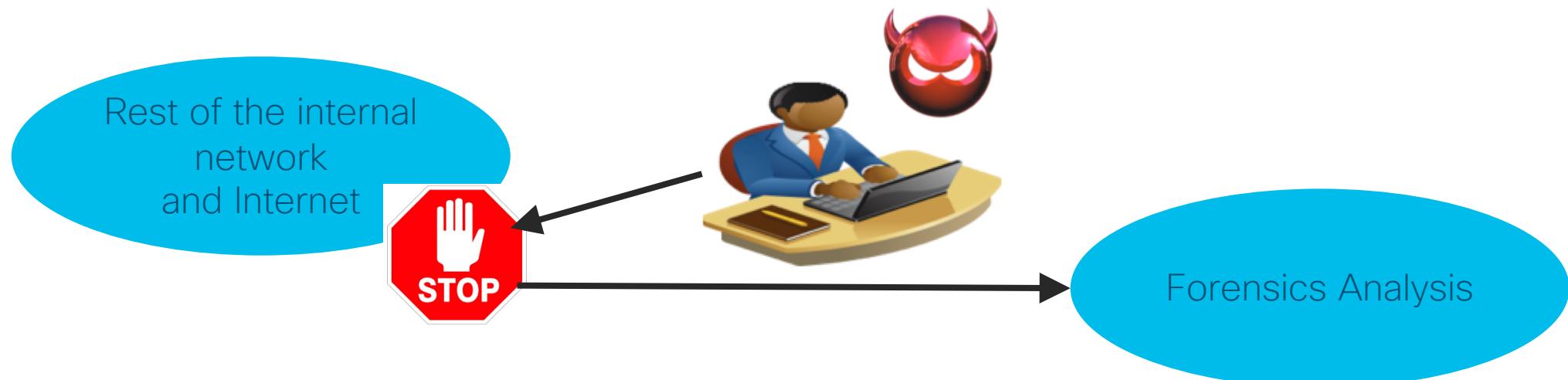
S!

# What is Threat Containment (Quarantine)?

- Blocking/minimizing network access for a host based on security event(s) by using:
  - Network Access Control solution (e.g. ISE, ClearPass...)
  - Reconfiguring access rules on Firewall/Router (Firepower, ISR)
  - Endpoint Security solutions (e.g. AMP, TrendMicro...)
- **Note:** Blocking access to a file on an endpoint can also be called quarantine.
- **Note:** Temporarily holding an email can also be called quarantine.
- **Note:** the customer must decide what it means!!!

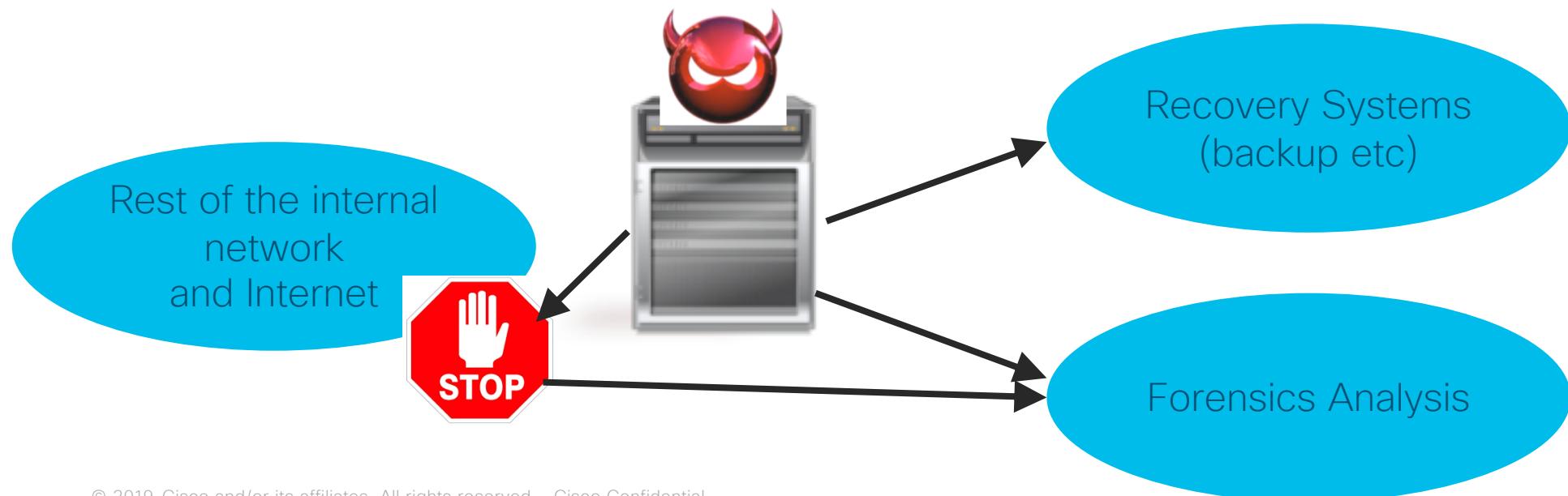
# Threat Containment Examples (1)

- A compromised client is discovered. Has been used by IT admin (with privileged credentials).
- Client is not allowed any network access **except system for forensic analysis**
- May involve traffic engineering of all traffic into systems for forensic analysis



# Threat Containment Examples (2)

- A compromised critical server is discovered. It must be reinstalled as soon as possible (reading last good backup etc.), but we cannot risk re-infection without knowing root cause.
- Allowed access to recovery-network and systems for forensics analysis



# What is **Rapid** Threat Containment (RTC)?

- To achieve Threat Containment : Now!
- You don't want to spend hours, days, weeks if there is a severe incident...
- Preparation is key!
- Knowledge of network is key!
- **Automation may help!!**
  - to perform action automatically
  - ...or to gather actionable intelligence automatically!
  - Note: the customer must decide what it means!!!

# Nuts we need to crack



# What Security Events are Relevant for RTC?

- ... IPS event that was blocked from the internet ??? **NO**
- ... Phishing mail blocked??? **NO**
- ... Malware file found and blocked by endpoint??? **NO**
- .... incoming connection from known bad IP blocked by FW ???? **NO**



Already Blocked!!!  
Does not indicate a compromise!!!!  
We don't care!!!

We are ONLY  
looking for signs of  
compromises!



# What Security Events are Relevant for RTC?

- ... IPS event from inside host.
- ....Malware file retrospectively found
- ... Outgoing Command and Control blocked
- ... DNS request for newly seen domain
- ... DNS with NXDOMAIN
- ... Network Anomalies
- ... Unusual login time

Yes

Yes

Yes

Maybe?

Maybe?

Maybe?

Maybe?

# What is a relevant Security Event?

- ... IPS event that was blocked from the internet ??? **NO points**
- ... IPS event from inside host??? **YES, 20 points**
- ... Command and Control blocked??? **YES, 20 points**
- ... Phishing mail blocked??? **NO points**
- ... DNS request for newly seen domain??? **YES, 10 points**
- ... DNS with NXDOMAIN??? **YES, 5 points**
- ... Malware file found and blocked by endpoint??? **NO points**
- ... Malware file retrospectivley found??? **YES, 25 points**

# Tracking the Targets under attack?

- Traditional Network Security (FW logs) track **IP address**
  - 10.1.33.10
- Traditional Network Security **may** track **MAC address**
  - 15:00:9d:01:67:04
- Endpoint security may track **Hostname**
  - (hakans-PC.labrats.se)
- Cloud security systems may track **Instance ID**
  - i-069b1c28365135ab4
- What about tracking the **user** ?
  - hakan, [hakan@labrats.se](mailto:hakan@labrats.se), CN=hakan,DC=Labrats,DC=se

Not Persistent  
DHCP etc.

Not Persistent  
New NIC  
MAC randomization.

Requires endpoint  
SW.

Cloud only.

How grab user info?

# Tracking the Targets under attack?

- Traditional Network Security (FW logs) track **IP address**

Not Persistent  
DHCP etc.

- Correlation and information grabbing needed
- when events occurs, grab as much tracking info as possible
- What about tracking the **user** ?
  - hakan, [hakan@labrats.se](mailto:hakan@labrats.se), CN=hakan

stent  
C  
nization.

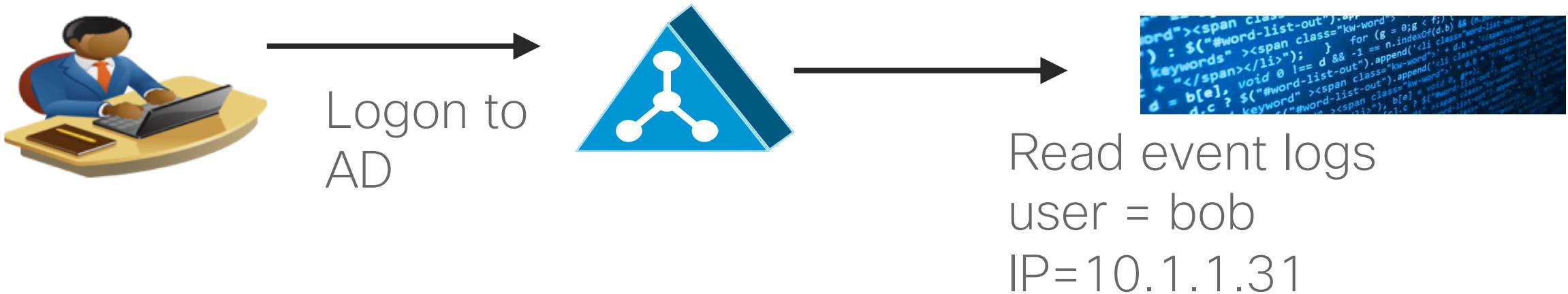
endpoint

only.

How grab user info?

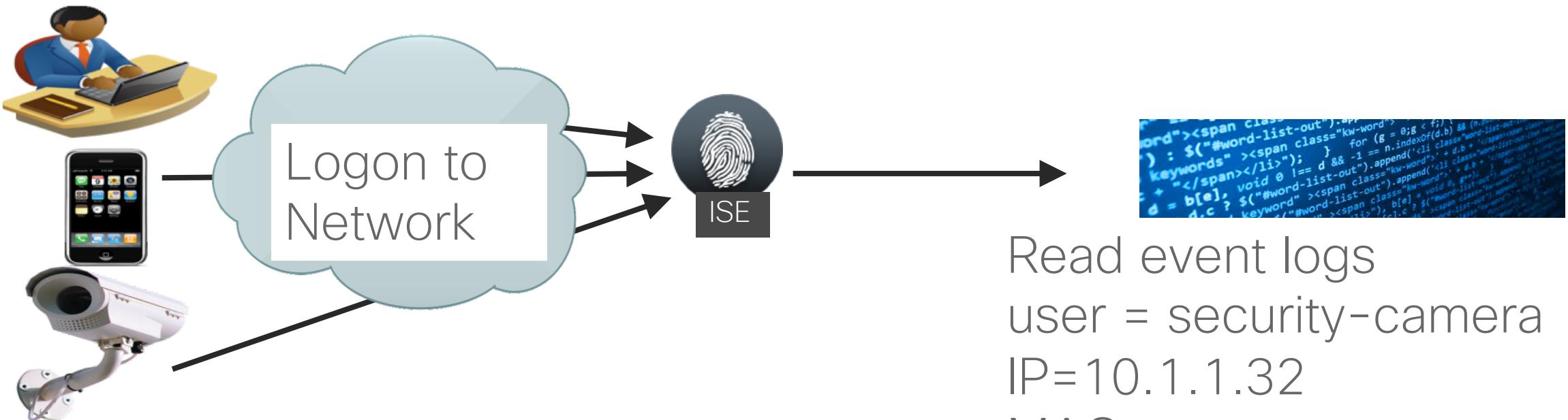
# How grab user info from IP address? (1)

- Parsing Active Directory logs – legacy Next Gen Firewall method
  - only works if there is an AD logon (not for IoT, BYOD etc)
  - tricky to detect when user takes laptop and leaves (no logoff)



# How grab user info from IP address? (2)

- Grab from Network Access Server
    - requires 802.1X/RADIUS logon
    - works with any device (also IoT, BYOD)
    - keeps track of devices leaving (senses link-down)



# How grab user info from IP address? (3)

- Ask Endpoint Security System
    - requires endpoint-security (Doh!)
    - works off-prem (home office etc)
    - can give more context, OS version, vulnerabilities etc.

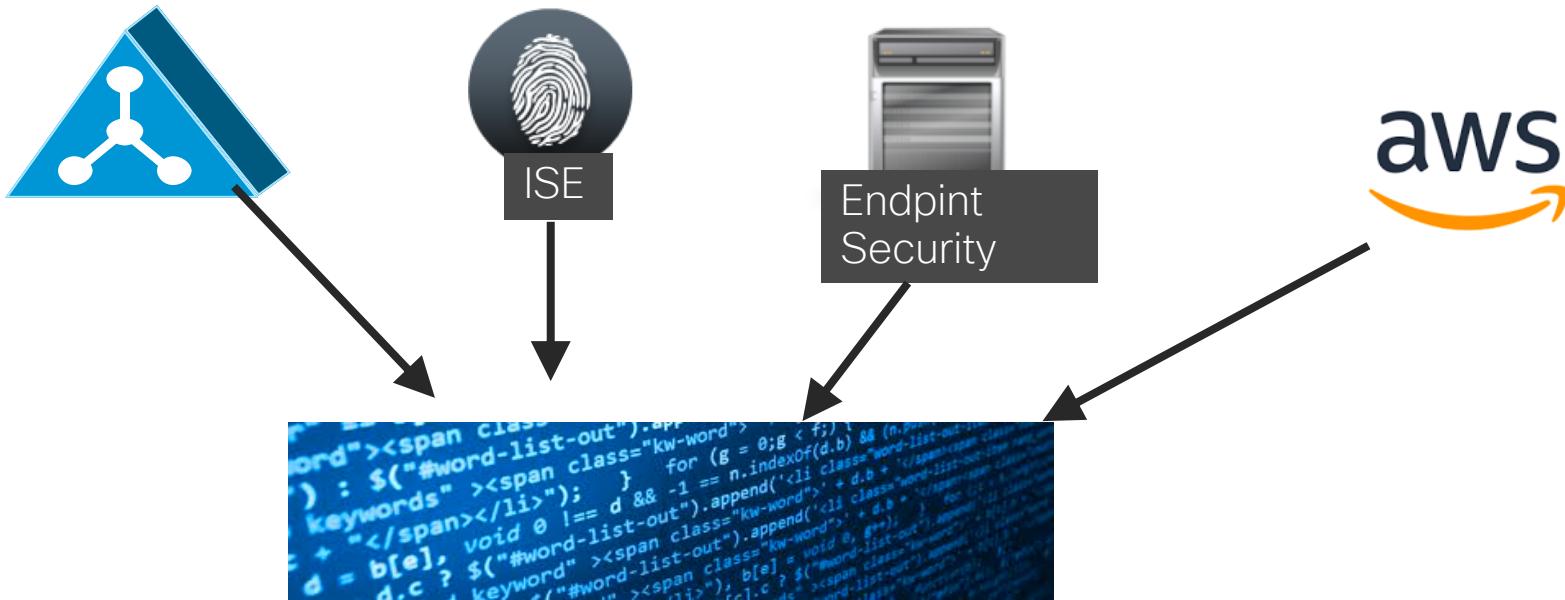


**ANSWER**

```
    "word") : $( "#word-list-out").append( "<li>" + keywords + "</span></li>" ); } for (b = 0; g < f;) { if (n.indexOf(d[b]) == -1) { d[b] = void 0; d[b] = c[b]; $( "#word-list-out").append( "<li class='kw-word'>" + d[b] + "</li>" ); } else { $( "#word-list-out").append( "<li class='kw-word'>" + d[b] + "</li>" ); } } } } );
```

Read from Endpoint Security  
user = hakan  
IP=10.1.1.32  
OS,version

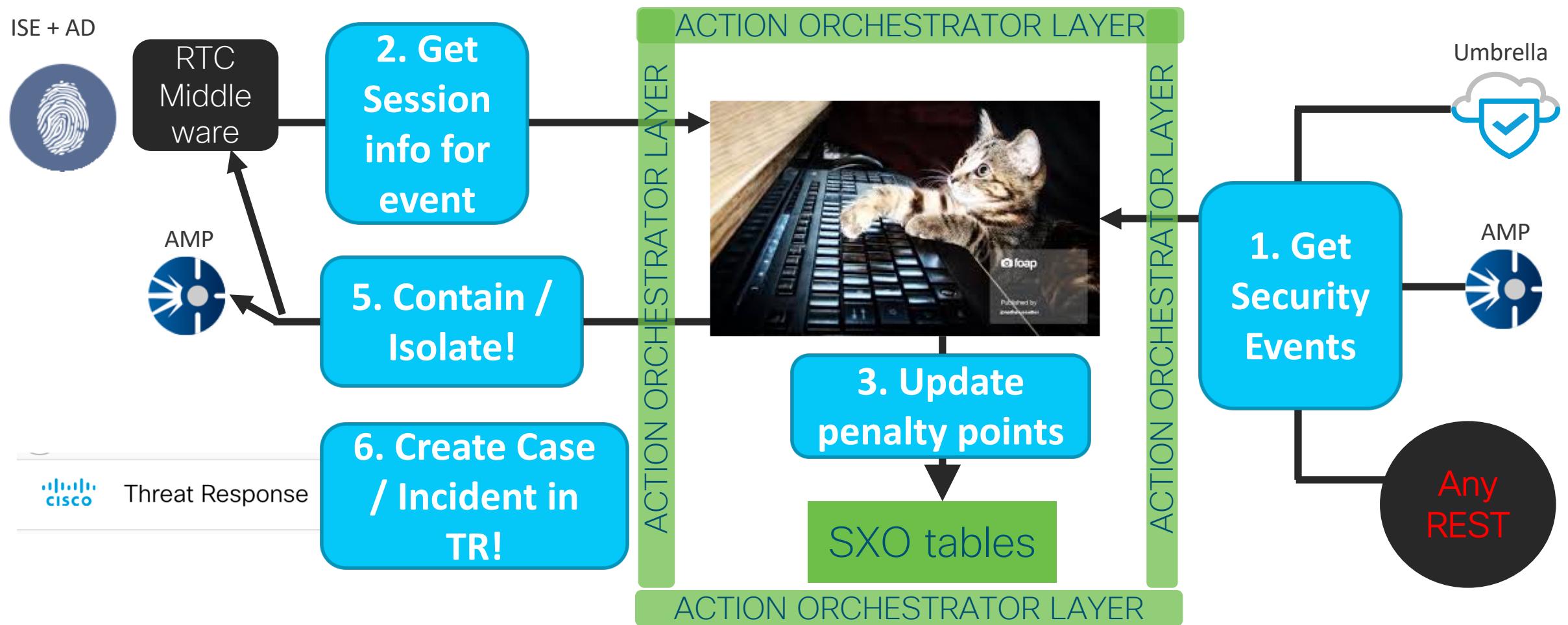
# Combining Multiple sources



IP	MAC	Hostname	Username	Instance ID	Event
					FW Event
					Endpoint Event
					Cloud Event

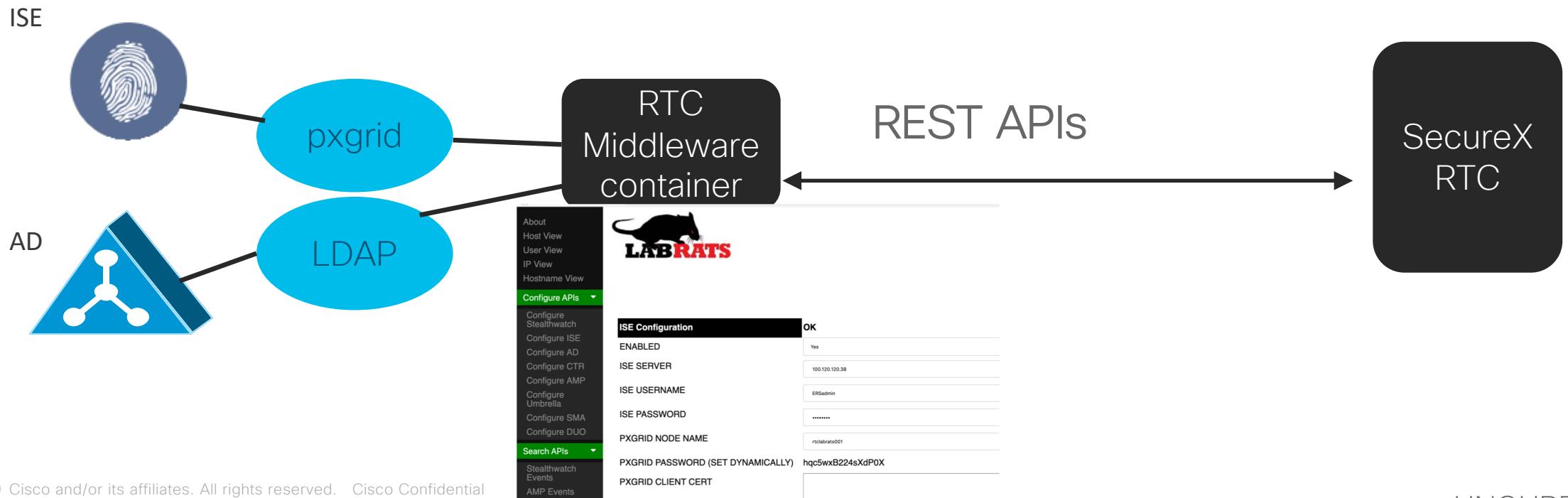
# Solution

# System Flow



# RTC Middleware

- Broker between SecureX RTC and ISE (and AD)
- REST API
  - rtc GetUserByIP. (retrieves username and MAC from IP from Cisco ISE)
  - rtcGetUserInfo (retrieves user info from AD: userPrincipalName, AD groups, Lastlogon...)
  - rtcANCapply



# SecureX Casebooks

The screenshot shows the Cisco SecureX Casebook interface. On the left, there's a sidebar with a search bar and a list of owned cases. The main area has tabs for Overview, Details, Observables, and Notes. The Overview tab is active, showing the title, creation date, owner, and summary of the selected case. The Observables tab shows two entries: a domain and a SHA-256 hash. The Notes tab contains a table with two rows: Title and Note.

Title	user:garfield
Note	garfield

Casebooks automatically  
created by IP, MAC, user  
and hostname

# SecureX Threat Response

Threat Response   **Investigate**   Snapshots   Incidents   Intelligence

New Investigation   Snapshots ...

Investigate   Clear   Reset   What can I search for?

5 Targets   2 Observables   5 Indicators   1 Domain   1 File Hash   0 IP Addresses   0 URLs

Relations Graph · Dispositions: All · Types: All · Mode: Simplified · Showing 14 of 79 nodes

The screenshot shows the Cisco SecureX Threat Response interface. At the top, there's a navigation bar with tabs for Threat Response, Investigate (which is selected), Snapshots, Incidents, and Intelligence. Below the navigation is a toolbar with buttons for New Investigation, Snapshots, Investigate, Clear, and Reset, along with a search bar labeled "What can I search for?". Further down are summary counts for Targets, Observables, Indicators, Domains, File Hashes, IP Addresses, and URLs. The main area is titled "Relations Graph" and displays a network of nodes representing different entities like hosts, domains, and files. A context menu is open over a node labeled "VMRAT32.labrats.se", which is highlighted with a red oval. The menu lists several RTC actions: Hostname, Investigate in Threat Response, AMP for Endpoints, Search for this hostname, SecureX Orchestration, RTC AMP Isolate Host, RTC AMP Stop Isolate Host, RTC Apply ANC, RTC Clear ANC, Perimeter Block, Internal Block, Talos Intelligence, Search for this hostname, Threat Grid, and Search VMRAT32.labrats.se. A large red callout bubble on the right side of the menu contains the text "RTC actions available".

3 Targets

- VMRAT32.labrats.se
- dac18b63-db80-4d50-9
- 10.1.33.32
- 00:0c:29:76:99:f8
- VMRAT10.labrats.se
- 7a145ad1-c773-48
- 10.1.33.10
- b4:96:91:41:43:d2
- vmrat13B.labrats.se
- 304b8777-0a5f-4642-8
- 10.1.33.13
- 00:0c:29:15:69:fa

23

3 Targets

2 Suspicious IPs

Target Endpoint  
0.1.33.33

14 Suspicious URLs

Malicious Domain  
sjpexaylsfjnop...

3 Clean IPs

4 IPs

Malicious IP  
209.126.127.231

Investigate in Threat Response

AMP for Endpoints

Search for this hostname

SecureX Orchestration

RTC AMP Isolate Host

RTC AMP Stop Isolate Host

RTC Apply ANC

RTC Clear ANC

Perimeter Block

Internal Block

Talos Intelligence

Search for this hostname

Threat Grid

Search VMRAT32.labrats.se

RTC actions available

CHRVAND

**KEEP  
CALM  
IT IS  
DEMO  
TIME**

# General Design

# RTC Event Table

Keep tracks on event observables per IP,MAC,Username,Hostname and the penalty incurred for that event-type

MAC_ADDRESS	PENALTY	TYPE	USER	VALUE
	init	0	init	value
.33.33	mac_address	25	domain	hffmzplu.com
.33.33	mac_address	25	domain	sjpexaylsfjnopolpg
.33.33	00:50:56:8b:95:4a	25	sha256	fa51a3bc680df330
.33.13	00:0c:29:15:69:fa	25	sha256	fa51a3bc680df330

observable type

observable value

# RTC Penalty Table

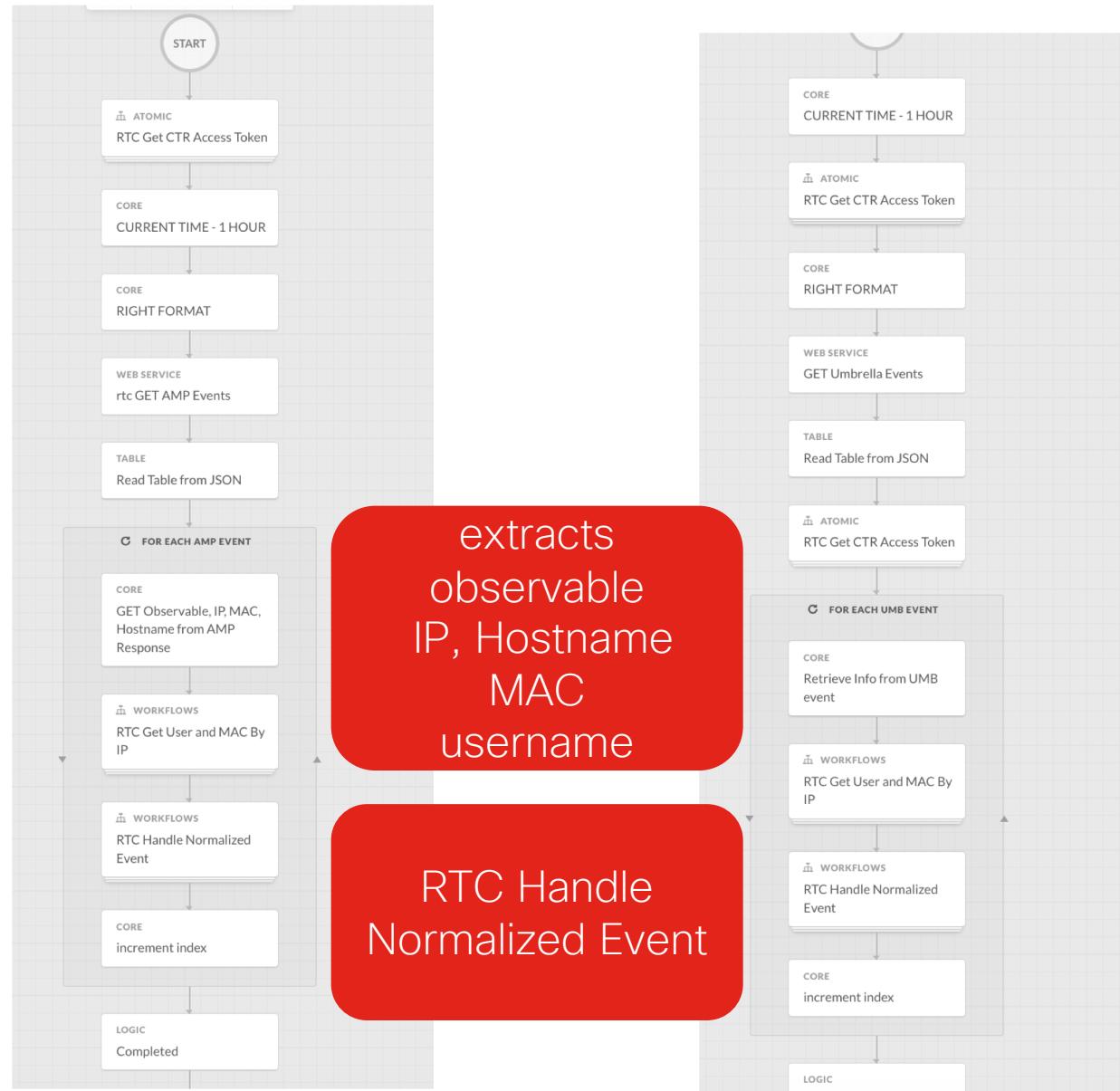
CASEBOOK_ID	ID	INCIDENT_ID	OBJECT_TYPE	PENALTY_POINTS	QUARANTINE_S
init	init	init	init	0	init
https://private.intel.	10.1.33.33	incident_id	ip	75	quarantine_
... and the casebook (so we can update later)	garfield	incident_id	user	25	quarantine_
vmrat33.labrats.se	incident_id	hostname	mac_address	25	quarantine_
casebook_id	00:50:56:8b:95:4a	incident_id	mac_address	25	quarantine_

Keep tracks of the Targets: users,  
hostnames, IPs, MACs

... and their accumulated Penalties

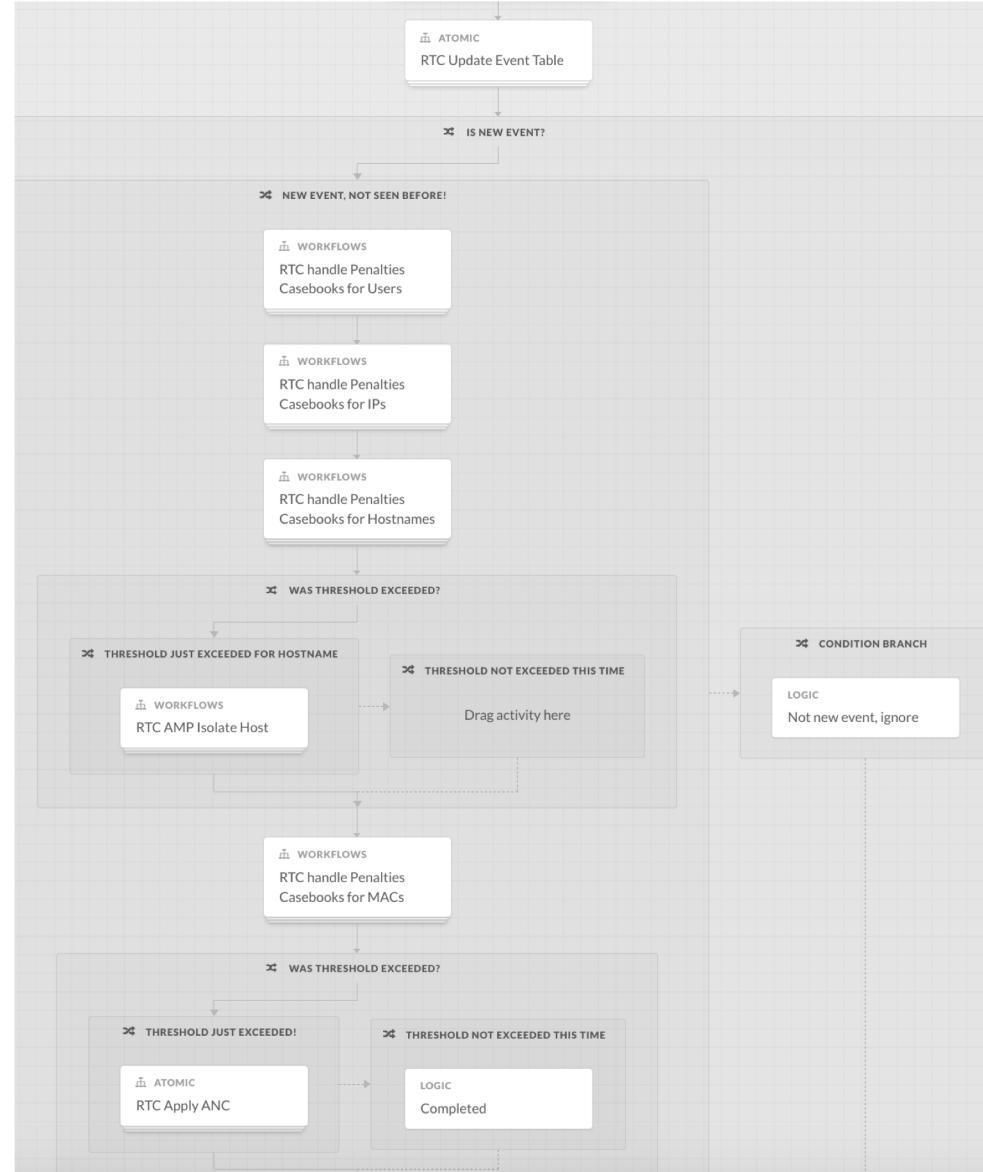
# RTC AMP Events, RTC UMB Events, RTC xyz

- Scheduled Workflows
- Retrieves CTR access token
- Retreives events from its API
- Loops through events
  - extracts observable
  - extracts IP, hostname of target
  - get username, MAC from ISE
  - calls **RTC Handle Normalized Event**



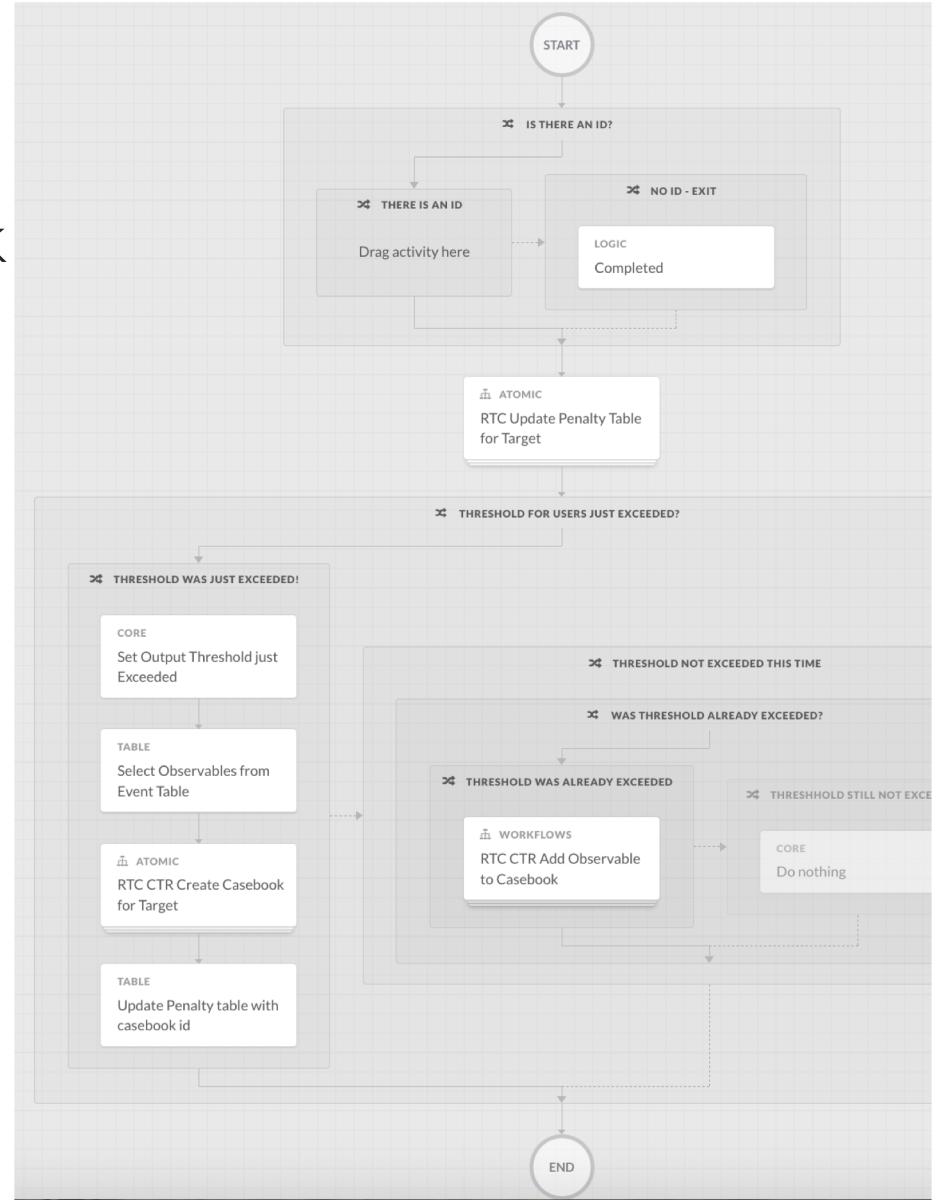
# RTC Handle Normalized Event

- Updates RTC Event Tables
- If new observable for target (user|hostname|ip|mac)
  - call RTC handle Penalties, Casebooks for target
  - if penalty threshold exceeded, perform RTC
    - (ANC or AMP Host Isolation)

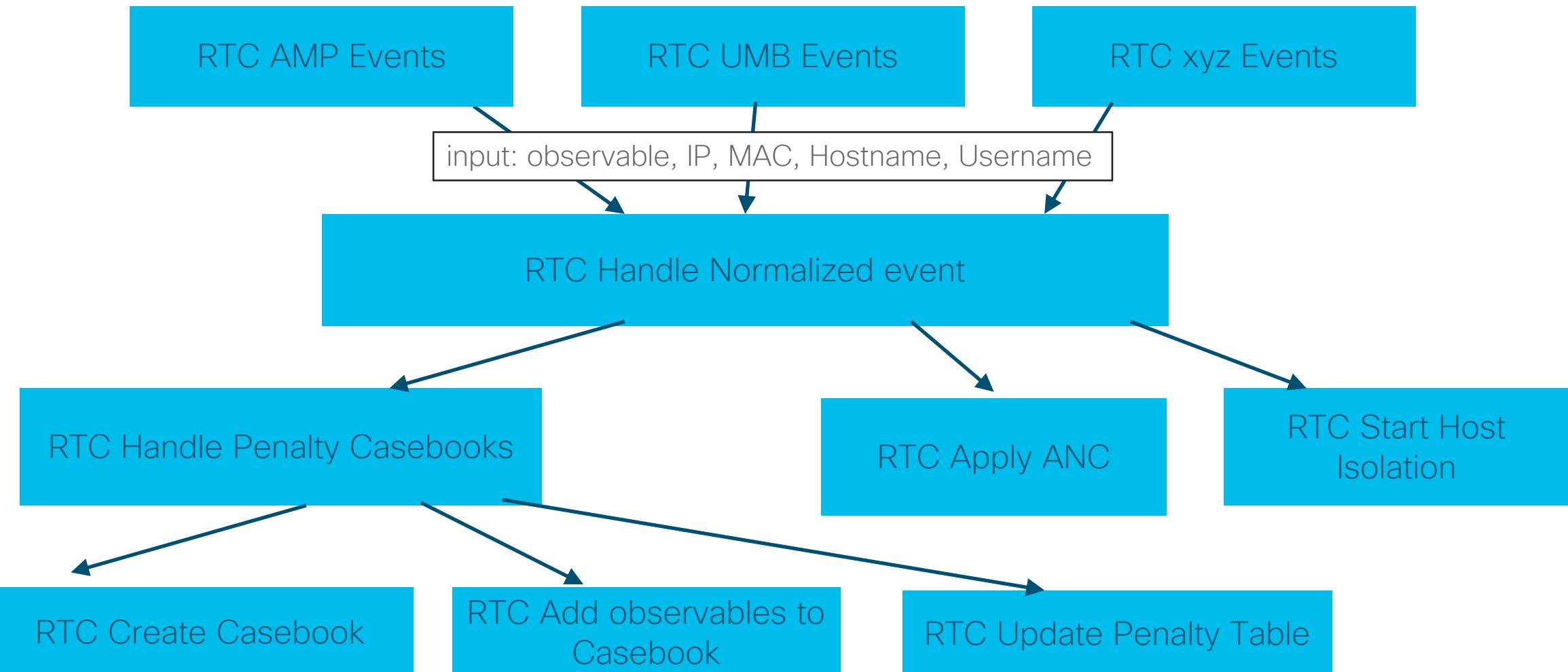


# RTC Hadle Penalties casebook for target

- Updates Penalty table for target
- If threshold just exceeded, create casebook
- If threshold was already exceeded, add observables to existing casebook



# Summary RTC Workflows



# Closing

# Roadmap [9 to 18 months, not committed] 😊

- Penalty Tile for uses etc. in Dashboards
- Add more sources for events (SWC, FP, Duo, Email)
- Optionally use external DB such as AWS RDS for better scalability
- Create and handle SecureX Incidents (not just SecureX Casebook)
- More granular configurable penalty points
  - per event type
  - per user (e.g. is it an IT admin with high privileges -> higher penalty points)
  - considering lateral movement (Stealthwatch)
  - MACHINE LEARNING!
- Please feel free to share more ideas / feedback!

# Road Map: Machine Learning!

- Ask SOC analysts whether the quarantine was a true positive.
  - ✓ If no: ask for feedback on security event points.
  - ✓ If yes: enforce security events and correlation more often.
- When enough data:
  - ✓ Calculate thresholds for specific host groups automagically.
  - ✓ Calculate penalty points for security events automagically.

Project is hosted here:  
<https://github.com/drnop/RTCaas>

Contact:  
[hnohre@cisco.com](mailto:hnohre@cisco.com)  
[chriivand@cisco.com](mailto:chriivand@cisco.com)

# Roadmap [9 to 18 months, not committed] 😊

- Penalty Tile foruses etc in Dashboards
- Add more sources for events (SWE, FP, Duo, Email)
- Optionally use external DB such as AWS RDS for better scalability
- Create and handle Incidents (not just casebooks)
- Configurable penalty points
  - per event type
  - per user (e.g. is it an IT admin with high privileges -> higher penalty points)
  - taking into account lateral movement (Stealthwatch)
- ...
- Please feel free to share more ideas / feedback!

# Installation Instructions

## RTCaaS

In SecureX

# 1a. Create Table Types in SecureX (names matter!!)

 Modify Variable Type

\* DISPLAY NAME  
RTC Penalty Table Type

DESCRIPTION

\*COLUMNS 1

REQUIRED	FIELD NAME	FIELD TITLE	FIELD TYPE	MAX LENGTH	MINIMUM
<input type="checkbox"/> NO	object_type	object_type	String	Max Length	Minimum
<input type="checkbox"/> NO	id	id	String	Max Length	Minimum
<input type="checkbox"/> NO	penalty_points	penalty_points	Integer	Max Length	Minimum
<input type="checkbox"/> NO	casebook_id	casebook_id	String	Max Length	Minimum
<input type="checkbox"/> NO	incident_id	incident_id	String	Max Length	Minimum

RTC Penalty Table Type

# 1b. Create Table Types in SecureX (names matter!!)

 Modify Variable Type

\* DISPLAY NAME  
RTC Event Table Type

DESCRIPTION

COLUMNS ⓘ

REQUIRED	FIELD NAME	FIELD TITLE	FIELD TYPE	MAX LENGTH	MINIMUM
NO	event_type	event_type	String	Max Length	Minimum
NO	user	user	String	Max Length	Minimum
NO	hostname	hostname	String	Max Length	Minimum
NO	ip	ip	String	Max Length	Minimum
NO	mac_address	mac_address	String	Max Length	Minimum
NO	type	type	String	Max Length	Minimum
NO	value	value	String	Max Length	Minimum
NO	penalty	penalty	Integer	Max Length	Minimum
NO	event_string	event_string	String	Max Length	Minimum

RTC Event Table Type

# 1c. Create Table Types in SecureX (names matter!!)

 Modify Variable Type

Table Type

General

\* DISPLAY NAME  
RTC Config

DESCRIPTION

\* COLUMNS ⓘ

REQUIRED	FIELD NAME	FIELD TITLE	FIELD TYPE	MAX LENGTH	MINIMUM
NO	AMPenalty	AMP Penalty	Integer	Max Length	Minimum
NO	UMBpenalty	UMB Penalty	Integer	Max Length	Minimum
NO	PenaltyThreshold	Penalty Threshold	Integer	Max Length	Minimum

RTC Config

## 2a. Create Penalty Table Variable

Modify Variable

Data Type

RTC Penalty Table Type

General

\* DISPLAY NAME  
RTC Penalty Table

DESCRIPTION

\* SCOPE  
Global

RTC Penalty Table

CASEBOOK_ID	ID	INCIDENT_ID	OBJECT_TYPE	PENALTY_POINTS	QUARANTINE
init	init	init	init	0	init

## 2b. Create Event Variable

 Modify Variable

Data Type

RTC Event Table Type

General

\* DISPLAY NAME  
RTC Events Table

DESCRIPTION

\* SCOPE  
Global

VALUE

EVENT_STRING	EVENT_TYPE	HOSTNAME	IP	MAC_ADDRESS	PENALTY
init	init	init	init	init	0

RTC Event Table

# 2c. Create Config Variables in SecureX

Modify Variable

Data Type: RTC Config

General

\* DISPLAY NAME: RTC Config var

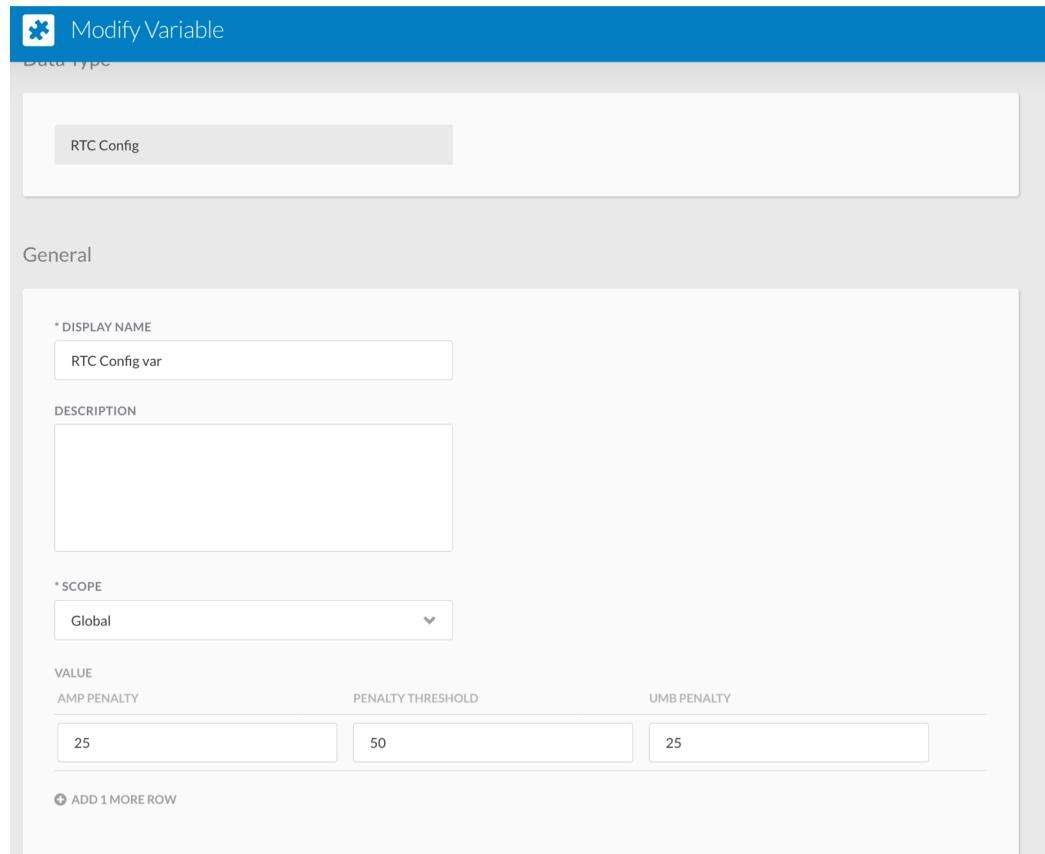
DESCRIPTION:

\* SCOPE: Global

VALUE

AMP PENALTY	PENALTY THRESHOLD	UMB PENALTY
25	50	25

[ADD 1 MORE ROW](#)



RTC Config

# 2d Create Variables for Authorizations strings

Modify Variable

Data Type

Secure String

General

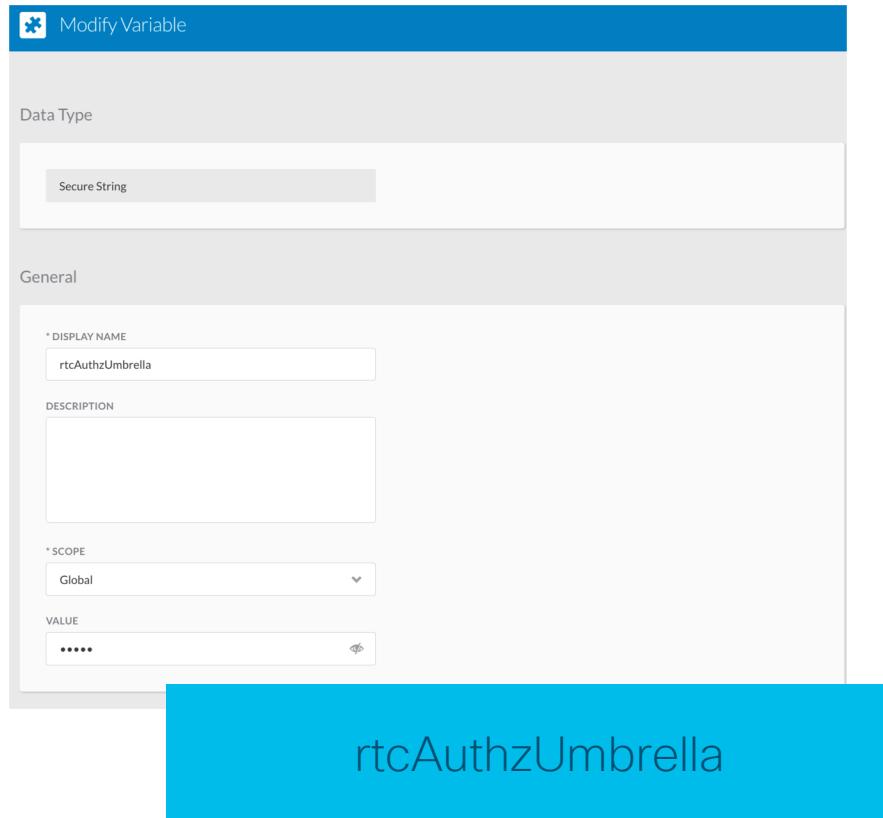
\* DISPLAY NAME  
rtcAuthzUmbrella

DESCRIPTION

\* SCOPE  
Global

VALUE  
\*\*\*\*\*

rtcAuthzUmbrella



Modify Variable

Data Type

Secure String

General

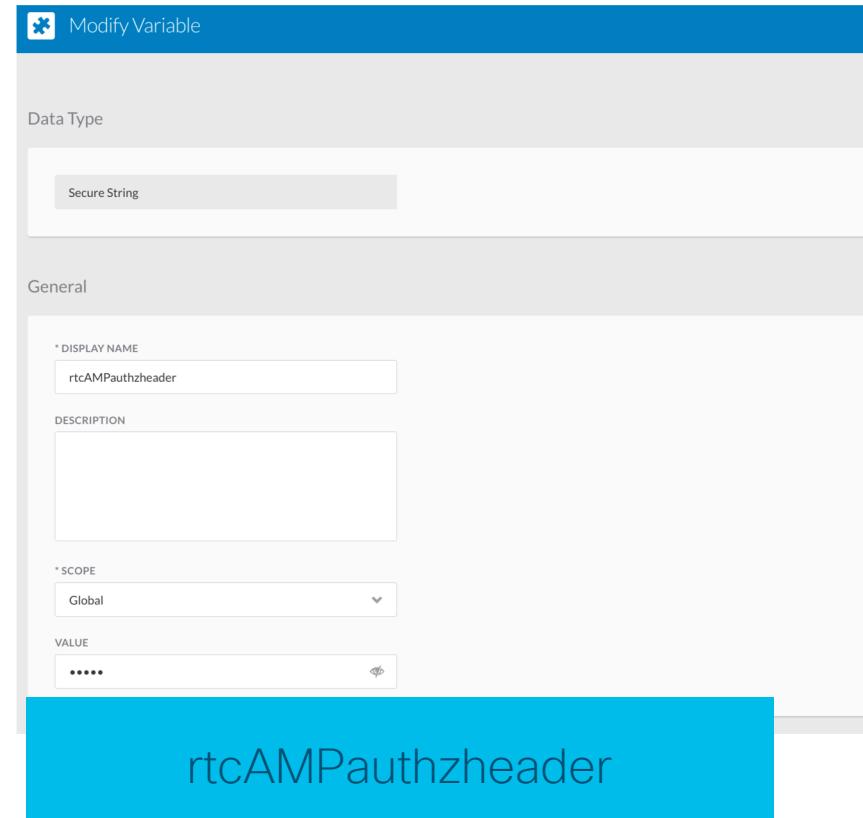
\* DISPLAY NAME  
rtcAMPauthzheader

DESCRIPTION

\* SCOPE  
Global

VALUE  
\*\*\*\*\*

rtcAMPauthzheader



# 2e Create Variables for Authorizations strings

Modify Variable

Data Type

Secure String

General

\* DISPLAY NAME  
RTC ISE Authz Secure String

DESCRIPTION

SCOPE  
Global

VALUE  
\*\*\*\*\*

RTC ISE Authz Secure String

©

# 3 Create Targets.....

RTC ISE. middleware

AMP Cloud (US, EU, SIA)

Umbrella Cloud (US, EU, SIA)

Modify Target

Account Keys

NO ACCOUNT KEYS ⓘ  
True

DEFAULT ACCOUNT KEYS  
Select

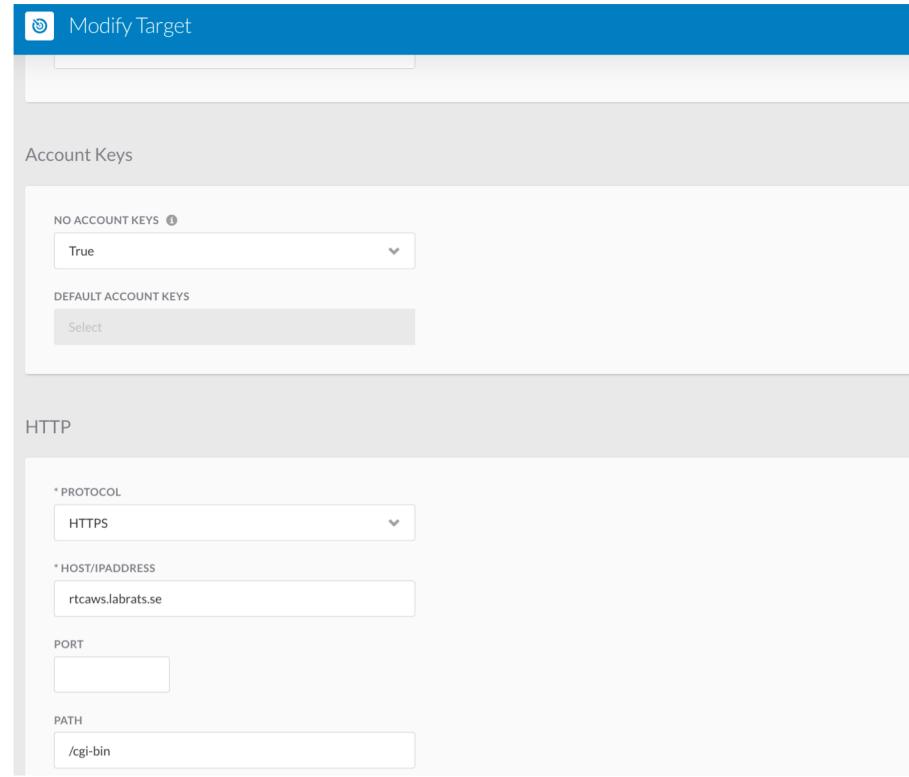
HTTP

\* PROTOCOL  
HTTPS

\* HOST/IPADDRESS  
rtcaws.labrats.se

PORT

PATH  
/cgi-bin



## 4. Download and Import the workflows