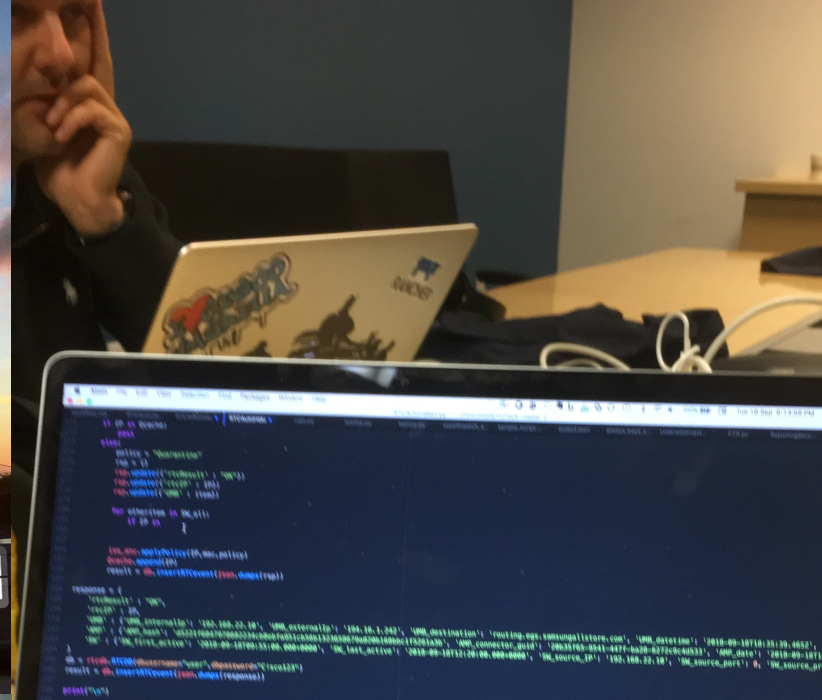
SecureX Rapid Threat Containment

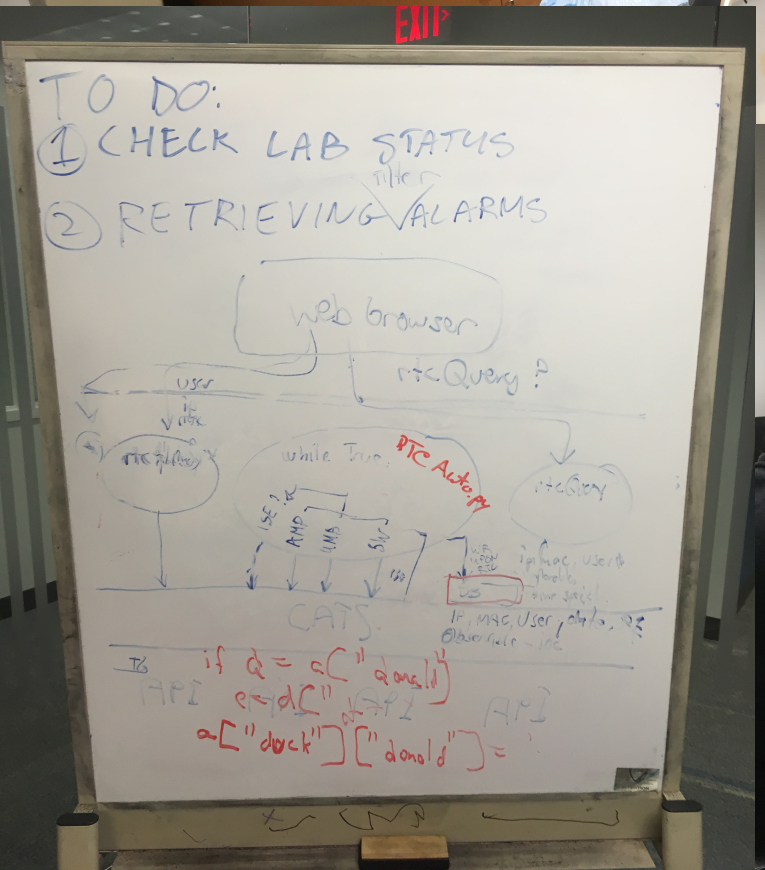
“RTC in da Cloud” “RTCaaS”

Multi-Domain Rapid Threat Containment without the False Positives

Christopher van der Made and Håkan Nohre


ON MY WAY
TO THE OFFICE
07 11



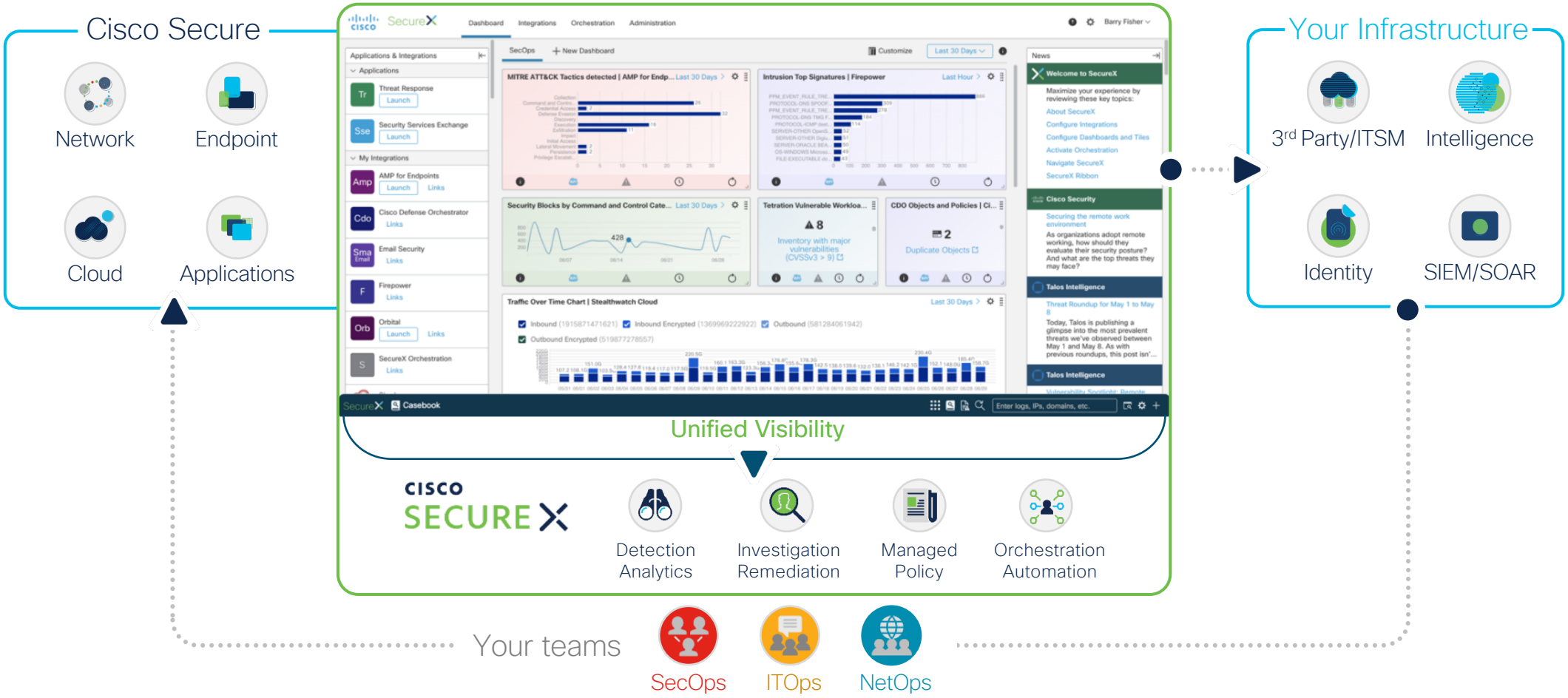

EXIT
TO DO:
1 CHECK LAB STATUS
2 RETRIEVING ALARMS
web browser
rtc.Query ?
while True:
PTC Auto-Pi
rtc.Query
CATS
API
API

MacBook Pro

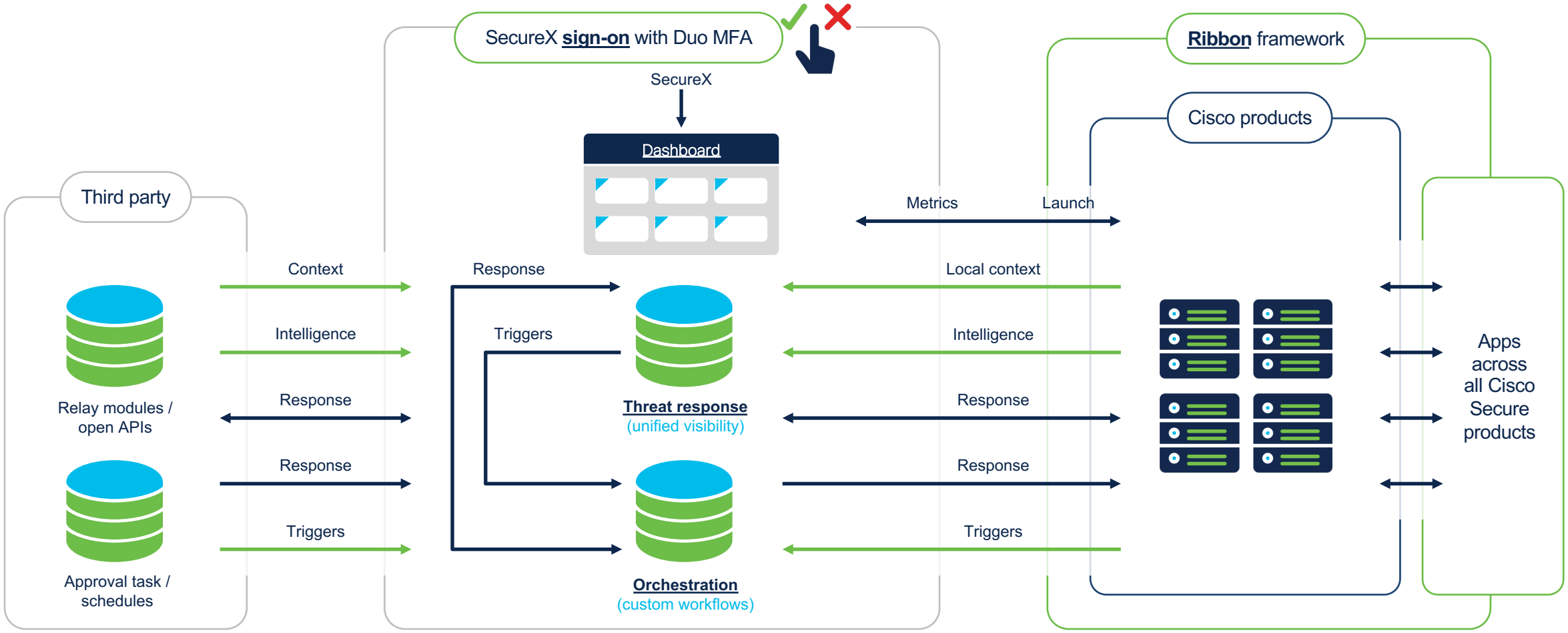
Introduction to SecureX

Introducing SecureX

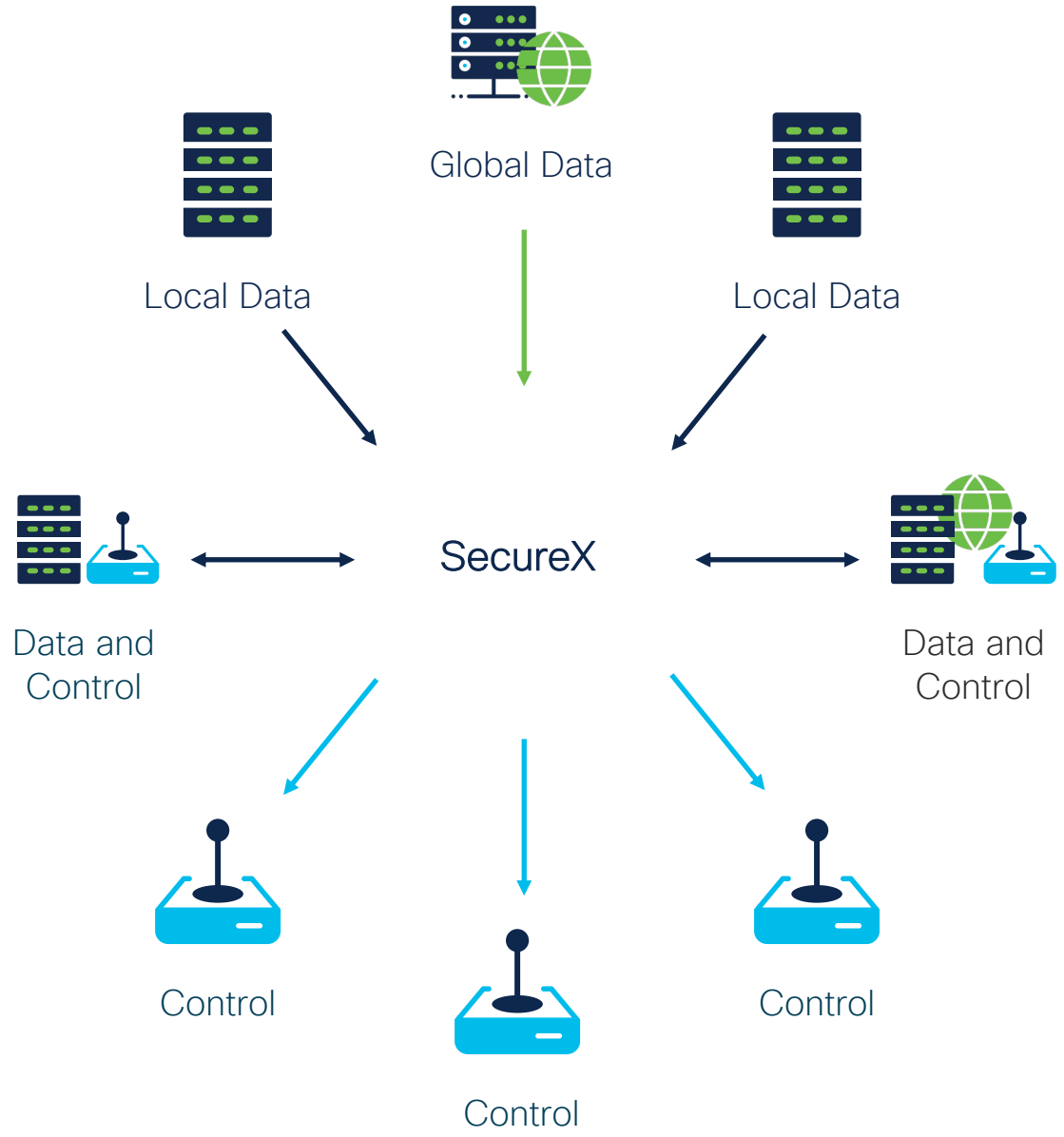
A cloud-native, **built-in platform** experience within our portfolio



SecureX architecture



API aggregation at work



SecureX orchestration

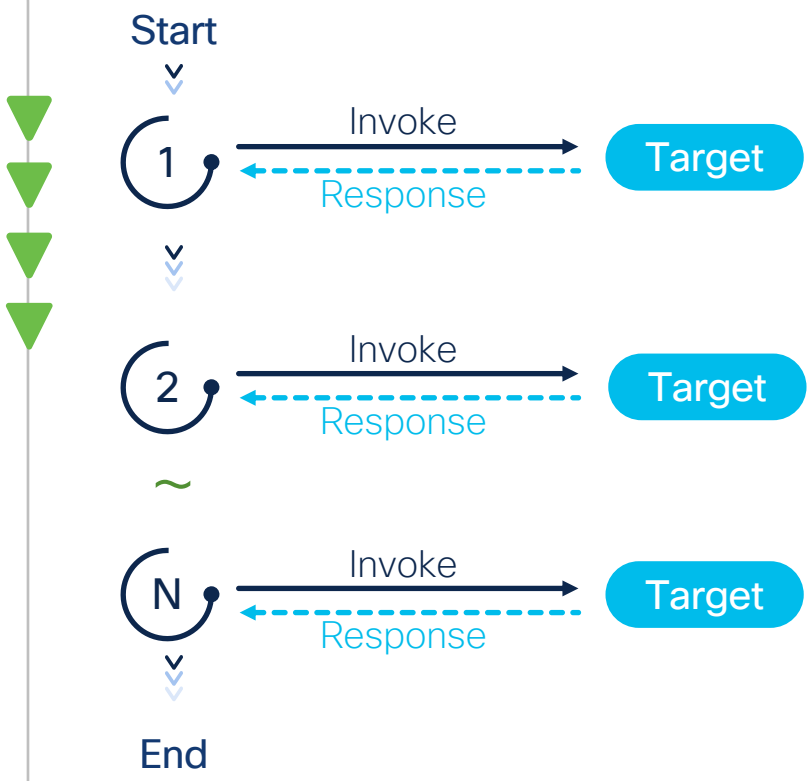
Cloud-Native, microservice architecture with “API-first” design

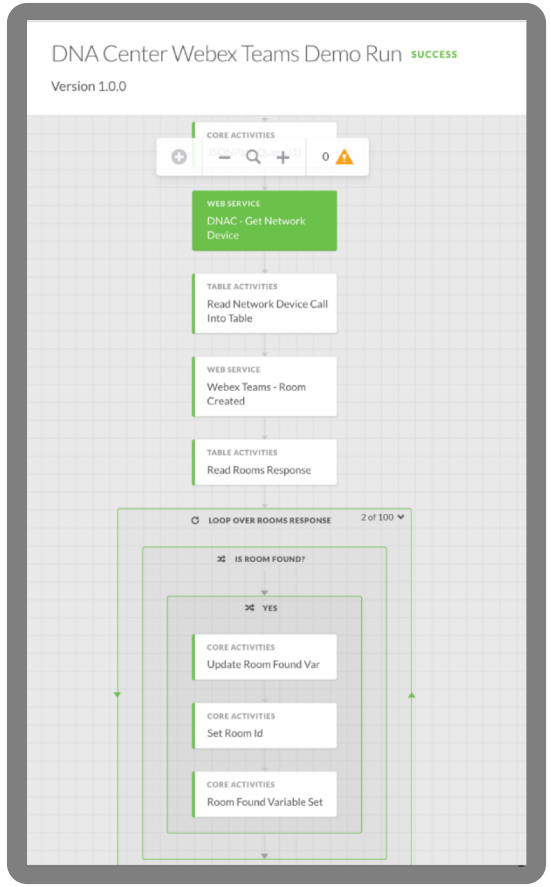
- Highly Performant, Scalable and Secure
- Reusable and Embeddable

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





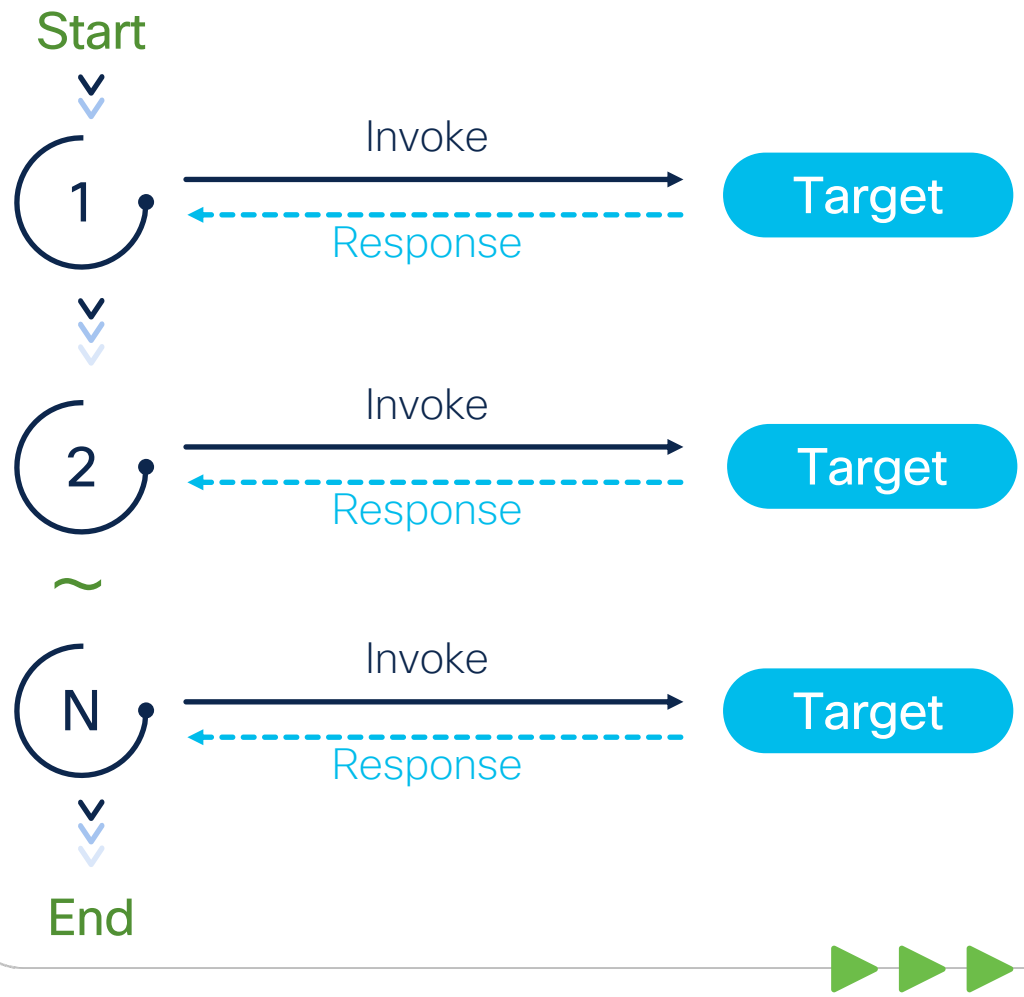
SecureX orchestration

Ecosystem integration standardized using adapters and workflows

- Execute workflows with business and technical logic
- Use included adapters & activities

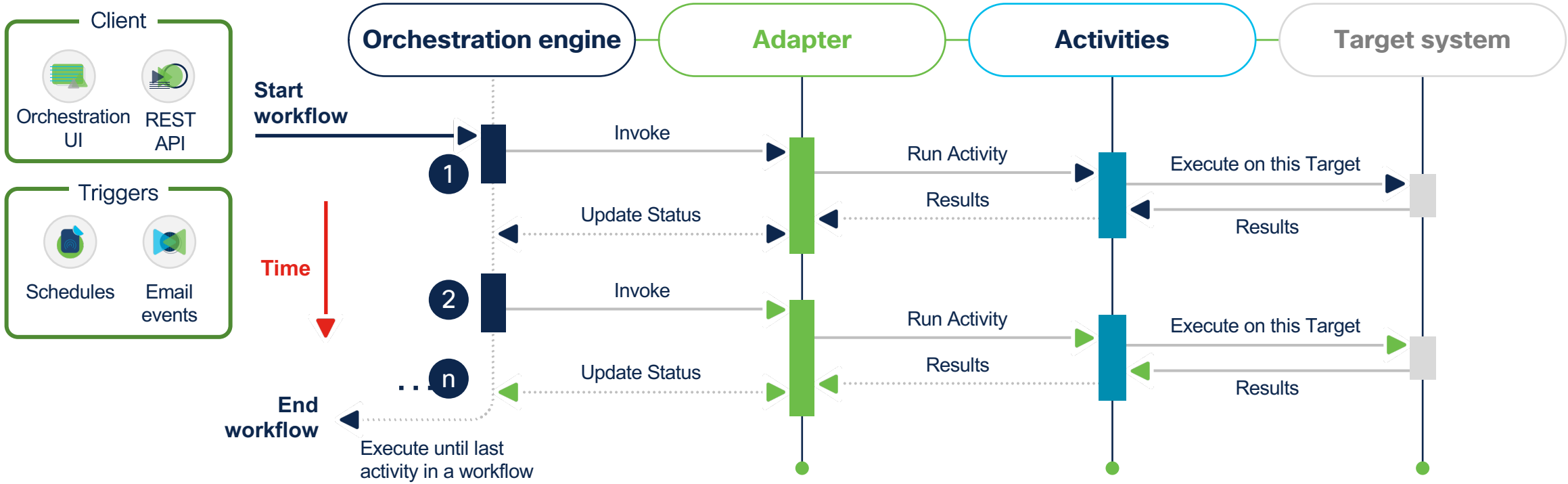
… or create custom ones!

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

Problem Statement

Wh / of

F S!


WARNING
ZOMBIE OUTBREAK
THIS AREA UNDER STRICT
QUARANTINE
AUTHORIZED PERSONNEL ONLY

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…)

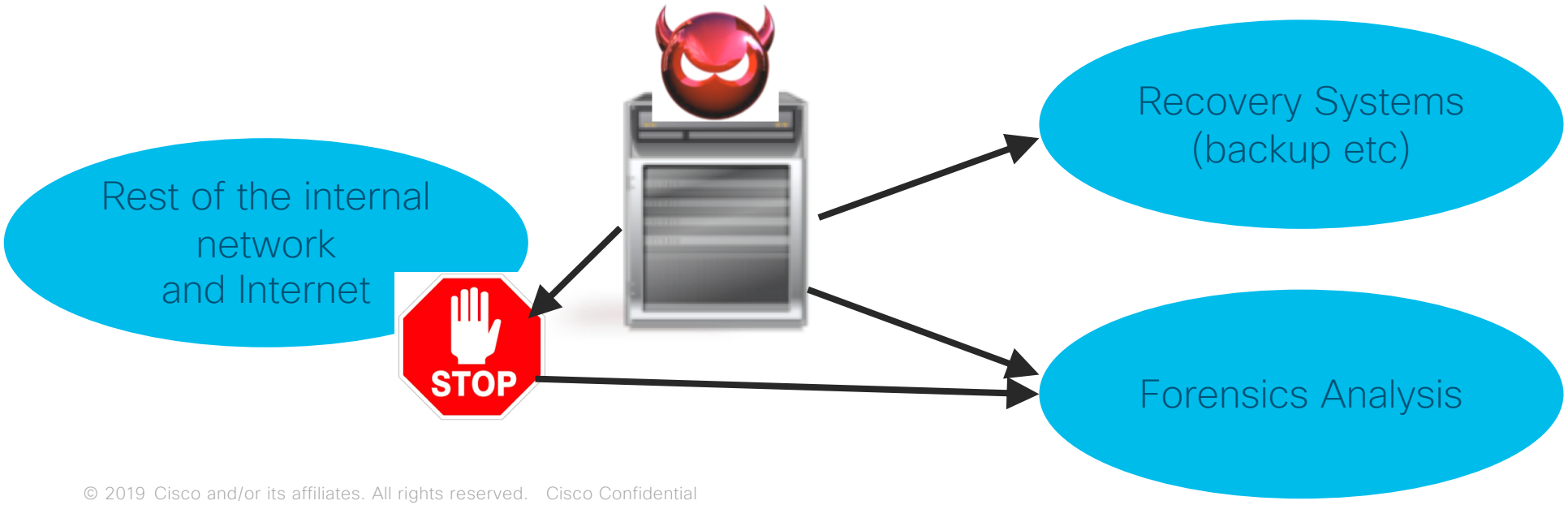
- **Note:** Blocking access to a file on an endpoint can also be called quarantine.
- **Note:** Temporarily holding an email can also be called quarantine.
- **Note:** the customer must decide what it means!!!

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!

CHRIVAND

What Security Events are Relevant for RTC?

- ... IPS event from inside host. — Yes
- ....Malware file retrospectively found — Yes
- ... Outgoing Command and Control blocked — Yes

- ... DNS request for newly seen domain — Maybe?
- ... DNS with NXDOMAIN — Maybe?
- ... Network Anomalies — Maybe?
- ... Unusual login time — 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, 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.

stent
IC
nization.

dpoint

nly.

How grab user info?

Correlation and information grabbing needed

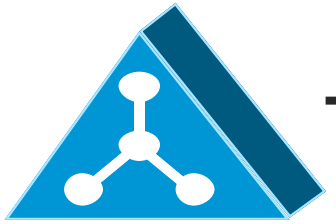
when events occurs, grab as much tracking info as possible

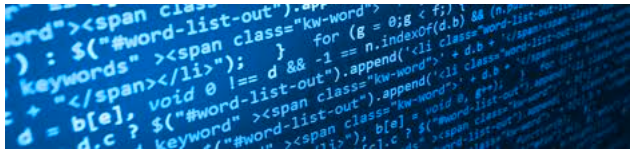
- What about tracking the user?
  - hakan, hakan@labrats.se, CN=hakan

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)

Logon to AD

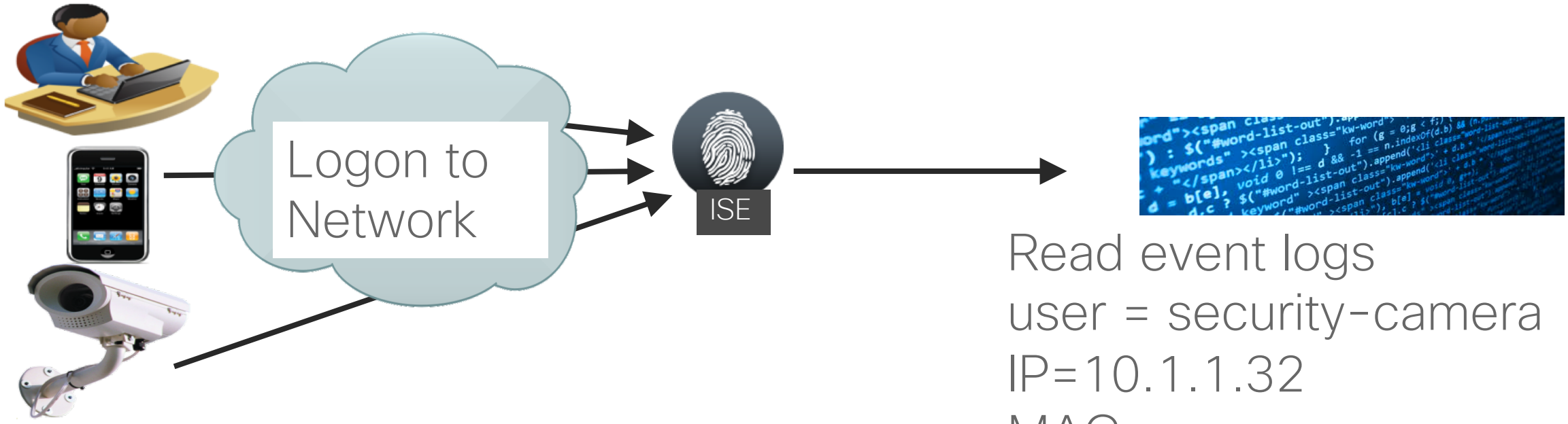




Read event logs
user = bob
IP=10.1.1.31

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)



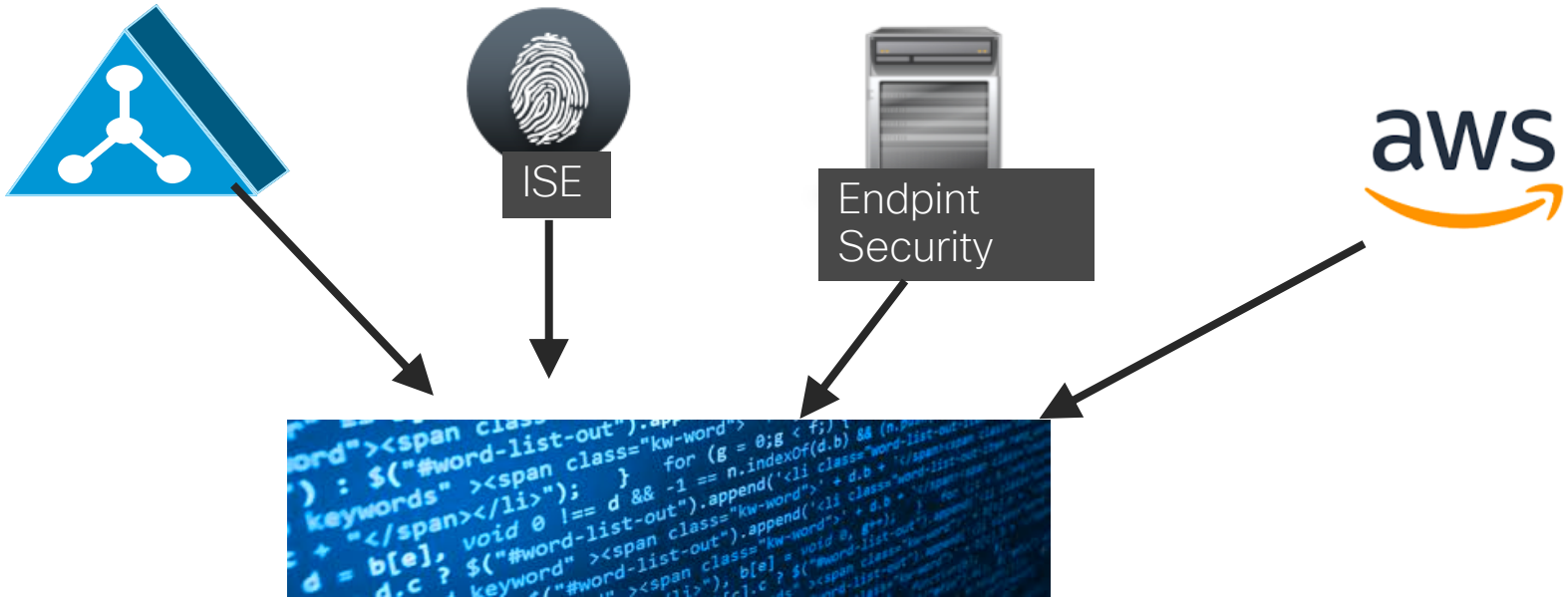
Read event logs
user = security-camera
IP=10.1.1.32
MAC=x.x.x.x.x.x

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.

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

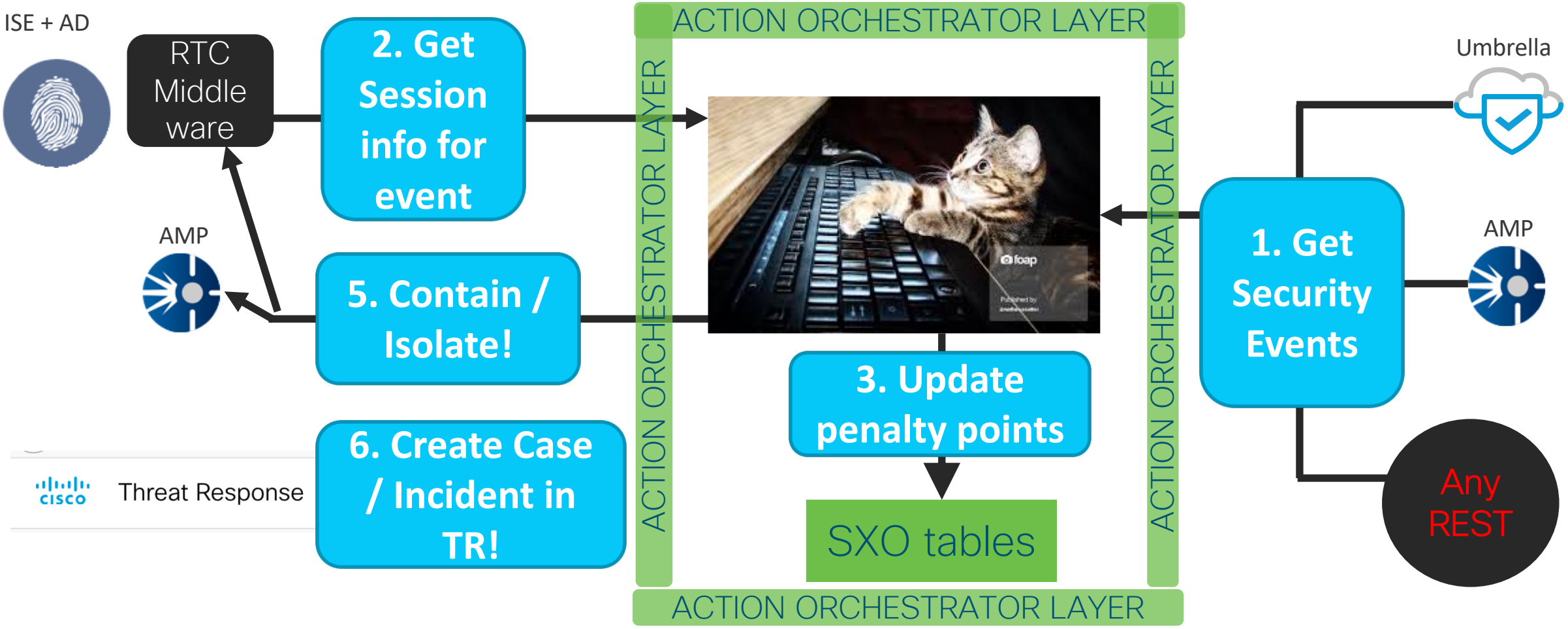
Combining Multiple sources



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

Solution

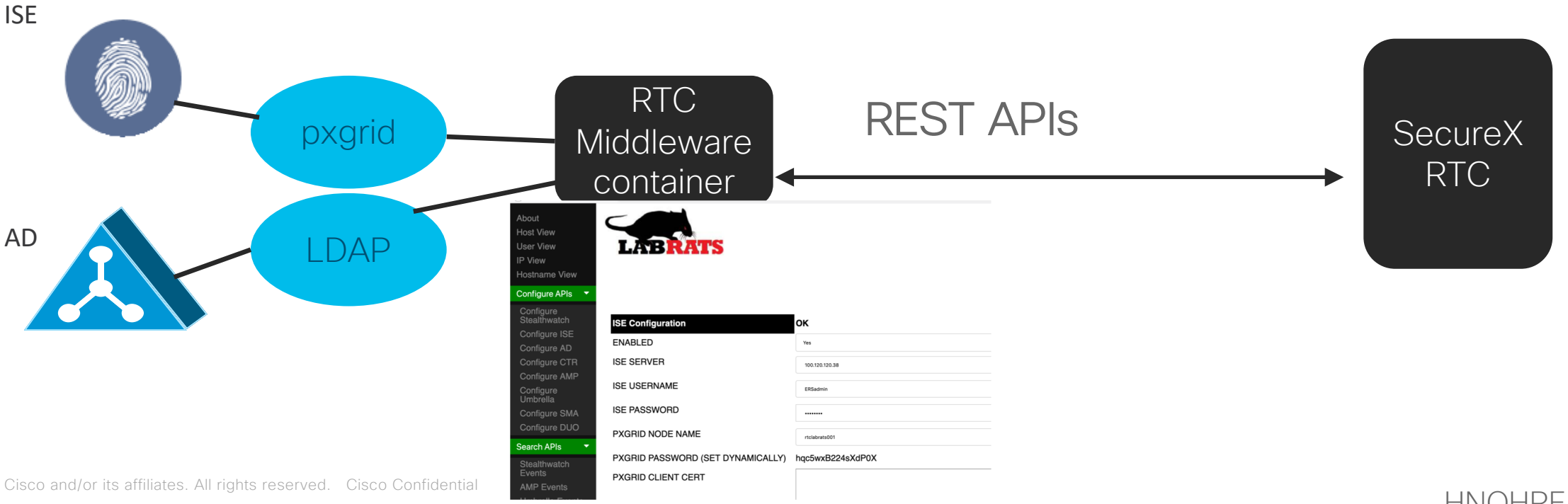
System Flow



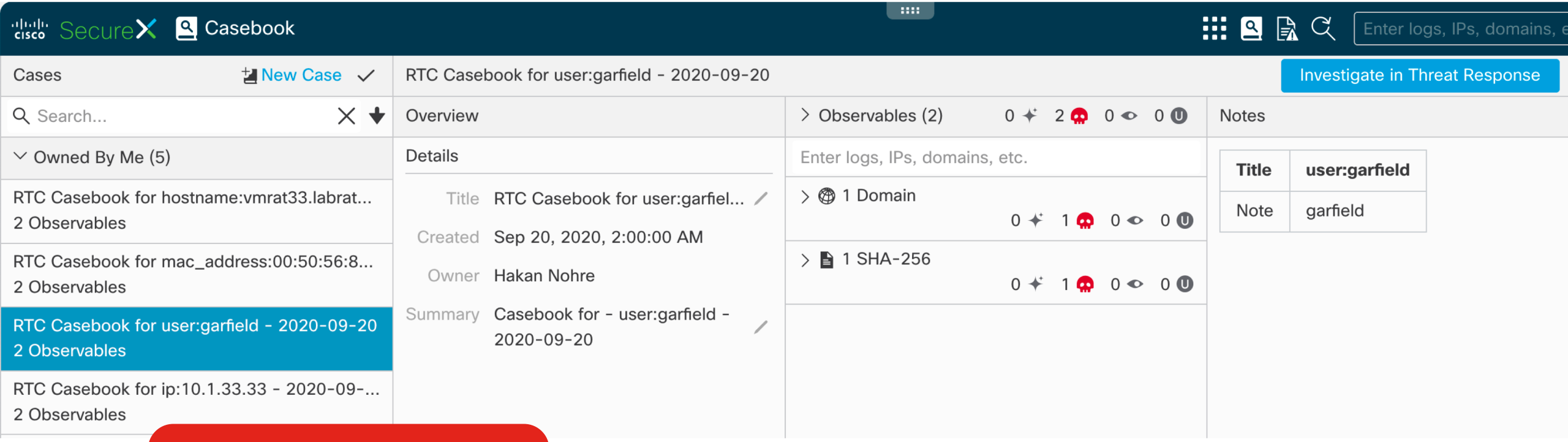
HNOHRE

RTC Middleware

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

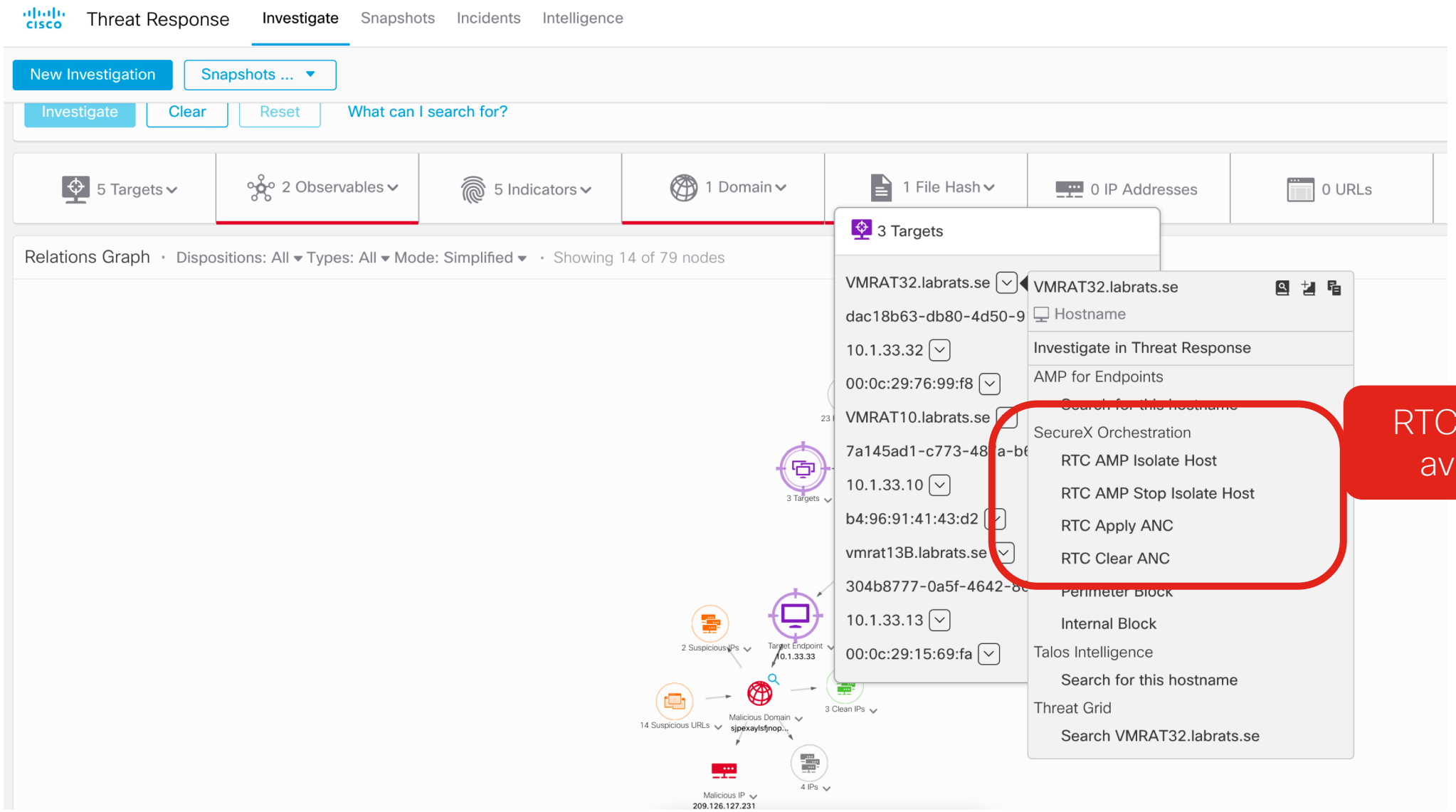


SecureX Casebooks



Casebooks automatically created by IP, MAC, user and hostname

SecureX Threat Response

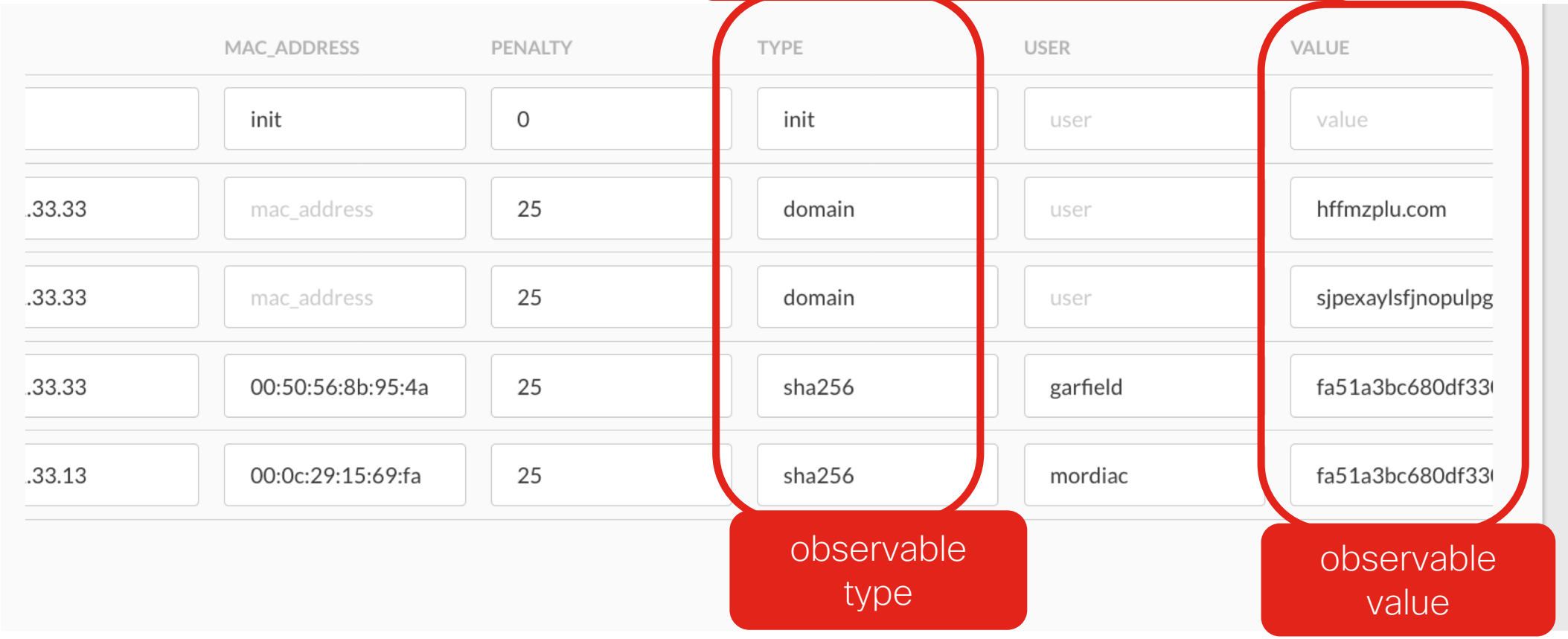


KEEP
CALM
IT IS
DEMO
TIME

General Design

RTC Event Table

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



	MAC_ADDRESS	PENALTY	TYPE	USER	VALUE
	init	0	init	user	value
.33.33	mac_address	25	domain	user	hffmzplu.com
.33.33	mac_address	25	domain	user	sjpexaylsfjnopulpg
.33.33	00:50:56:8b:95:4a	25	sha256	garfield	fa51a3bc680df33
.33.13	00:0c:29:15:69:fa	25	sha256	mordiac	fa51a3bc680df33

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_
	garfield	incident_id	user	25	quarantine_
	vmrat33.labrats.se	incident_id	hostname	25	quarantine_
casebook_id	00:50:56:8b:95:4a	incident_id	mac_address	25	quarantine_

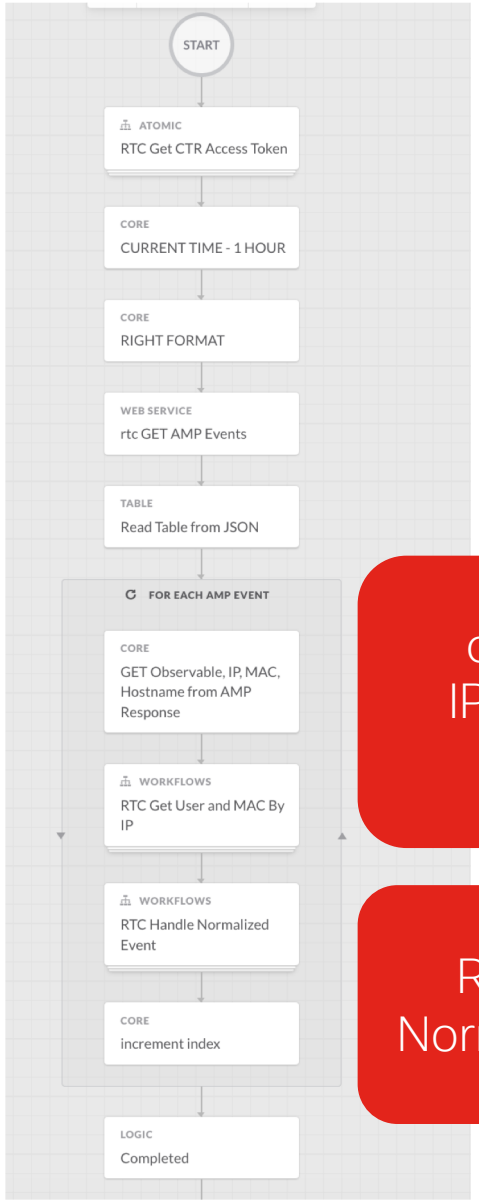
… and the casebook (so we can update later)

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

… and their accumulated Penalties

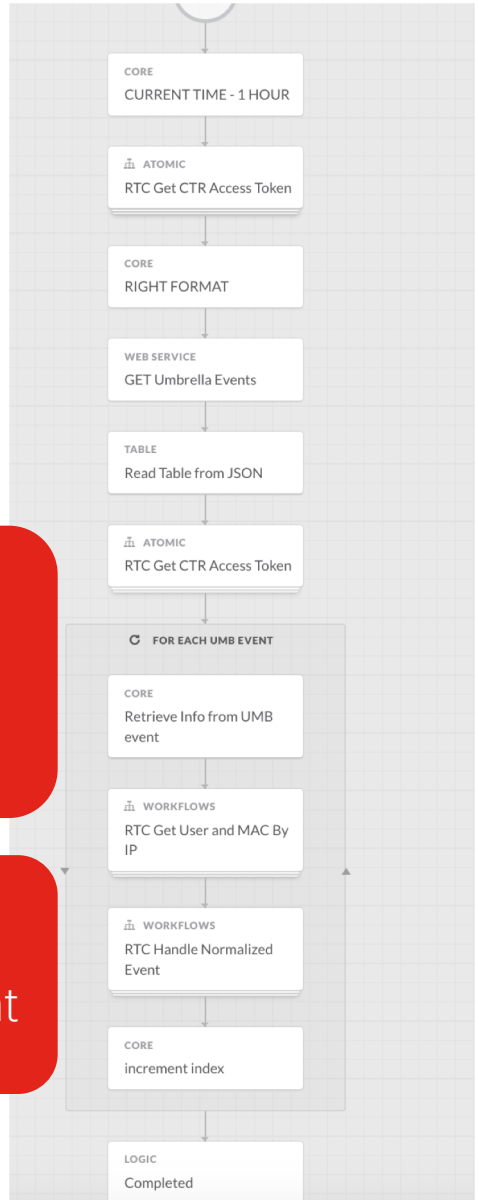
RTC AMP Events, RTC UMB Events, RTC xyz

- 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**



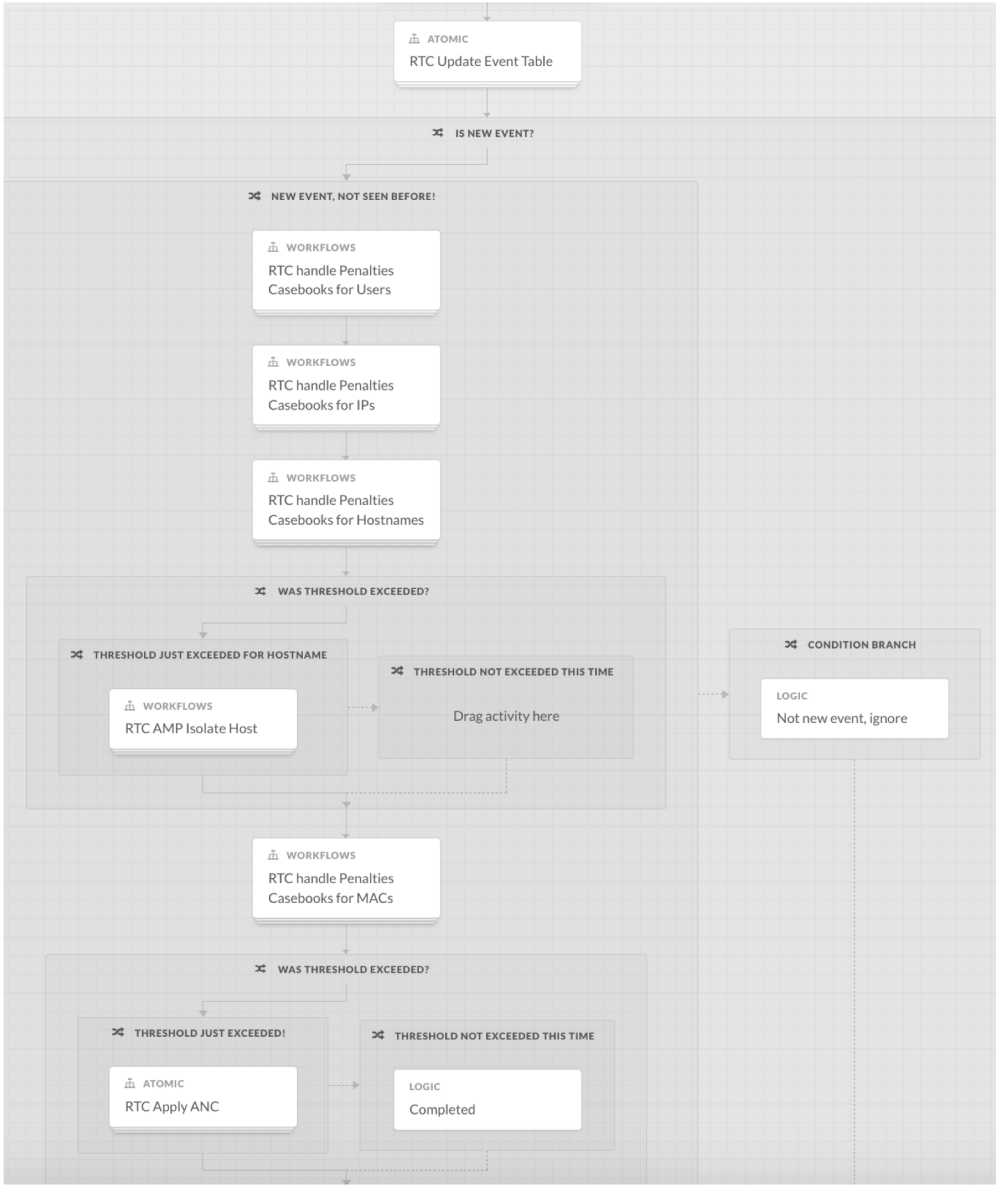
extracts observable IP, Hostname MAC username

RTC Handle Normalized Event



RTC Handle Normalized Event

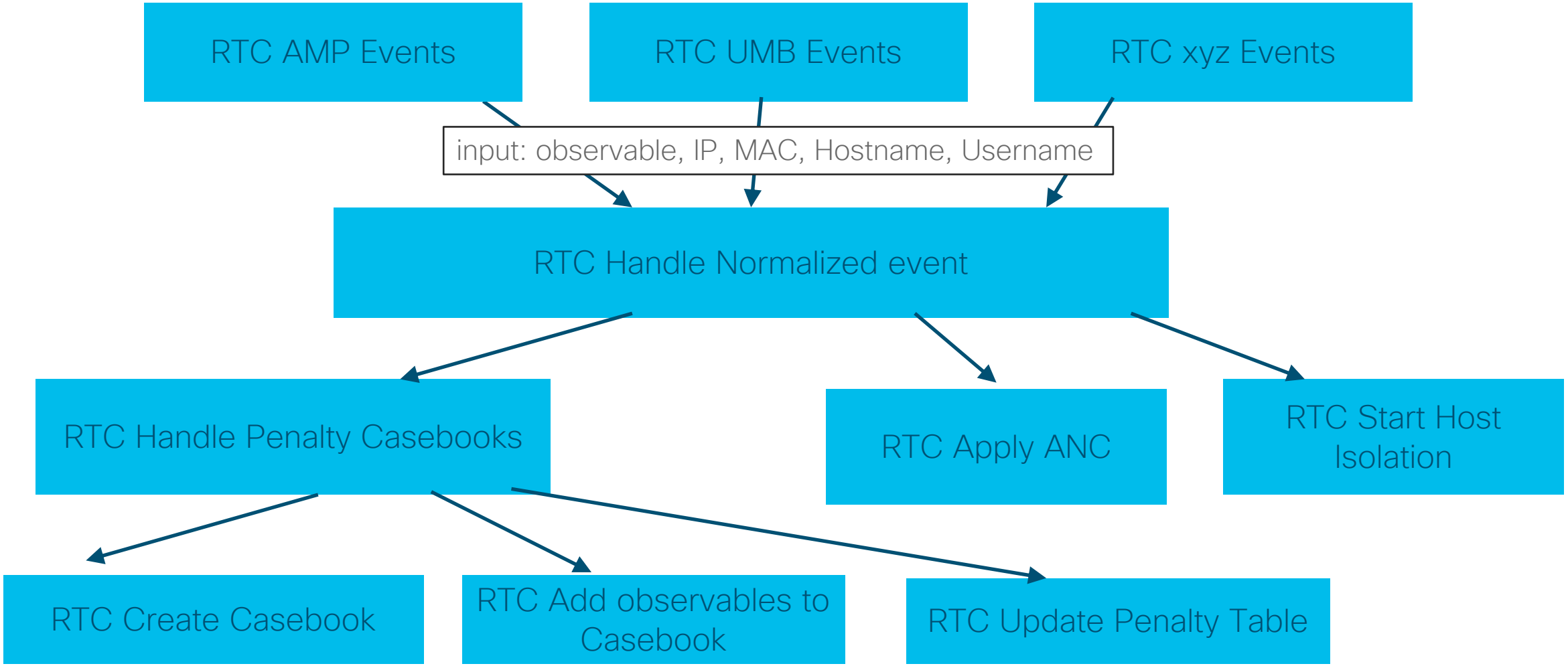
- Updates RTC Event Tables
- If new observable for target
  (user|hostname|ip|mac)
  - call **RTC handle Penalties, Casebooks for target**
  - if penalty threshold exceeded, perform RTC
    - (ANC or AMP Host Isolation)



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
chrivand@cisco.com

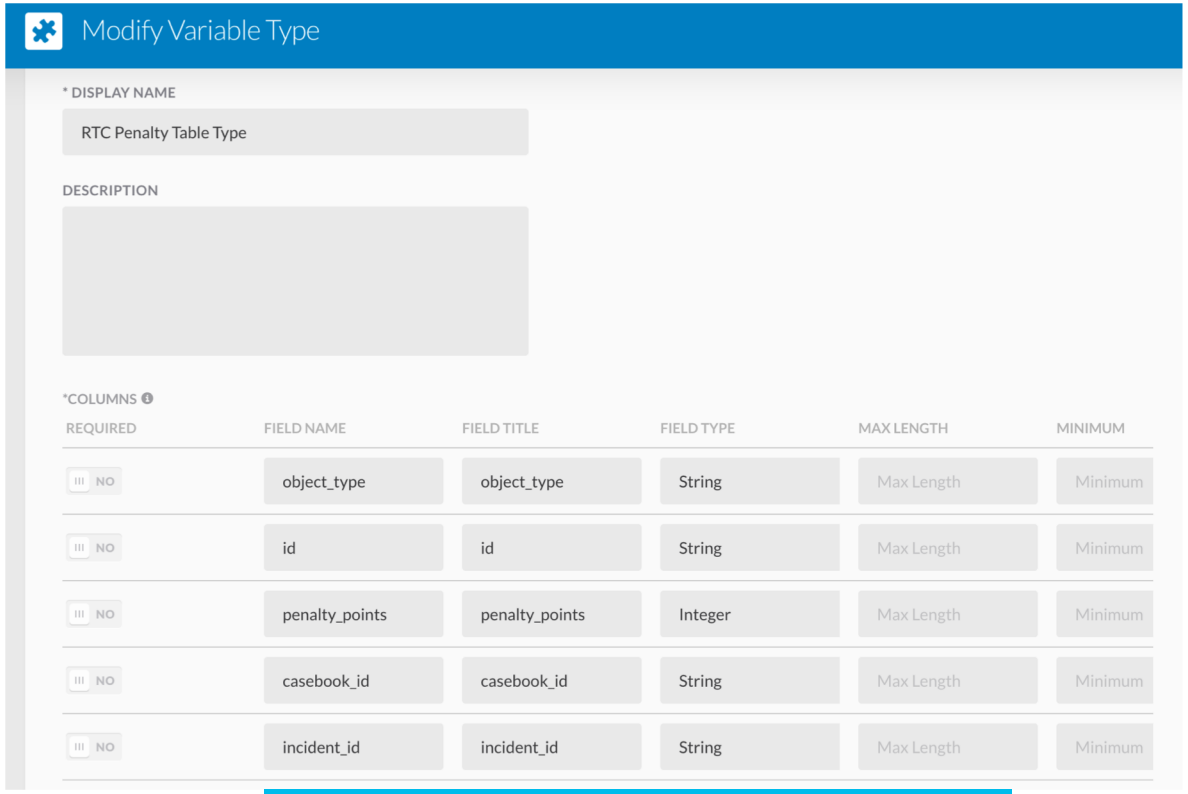
Roadmap [9 to 18 months, not committed] ☺

- Pentalty 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

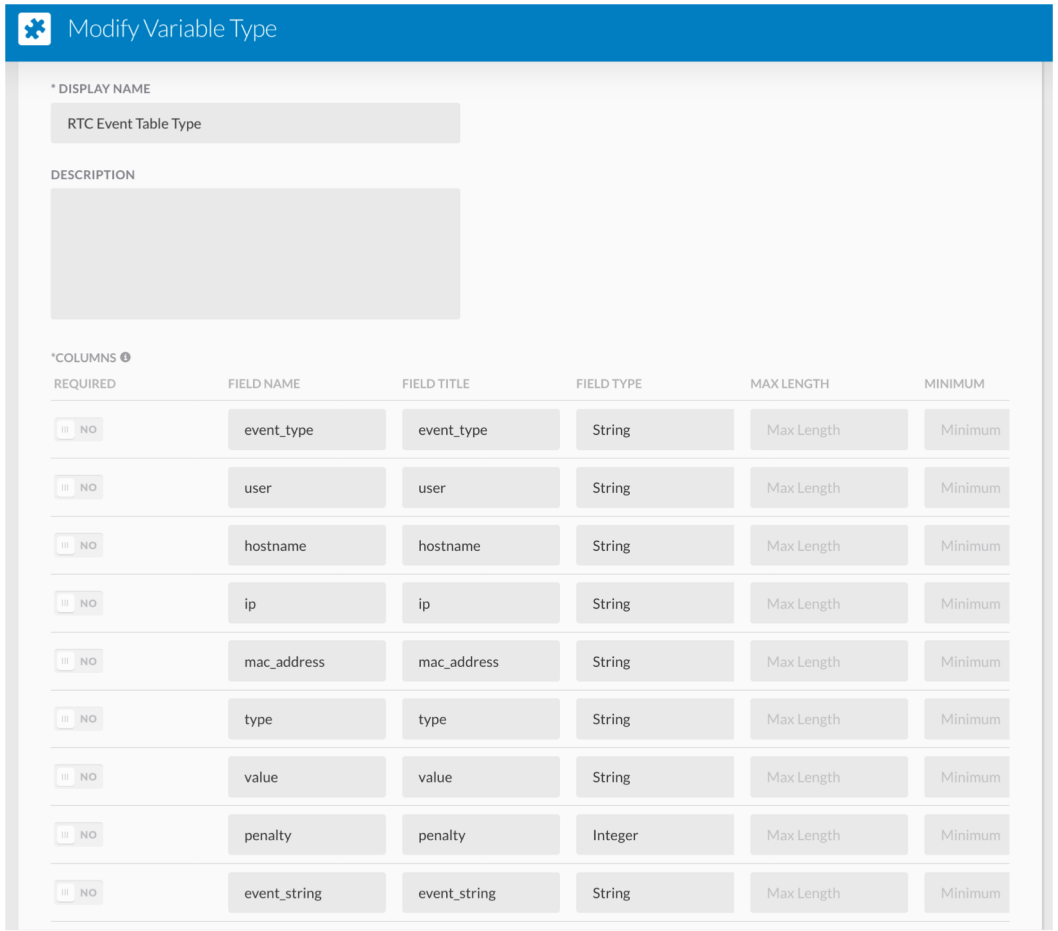
In SecureX

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



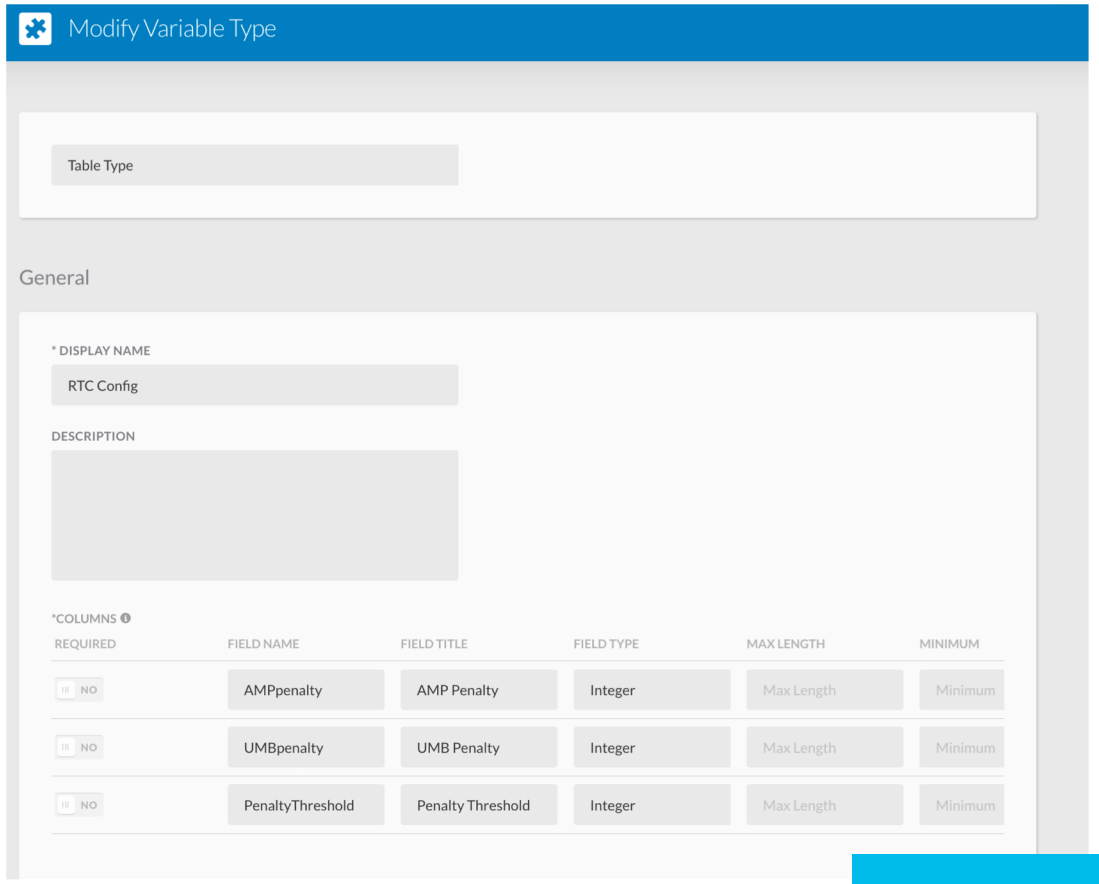
RTC Penalty Table Type

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



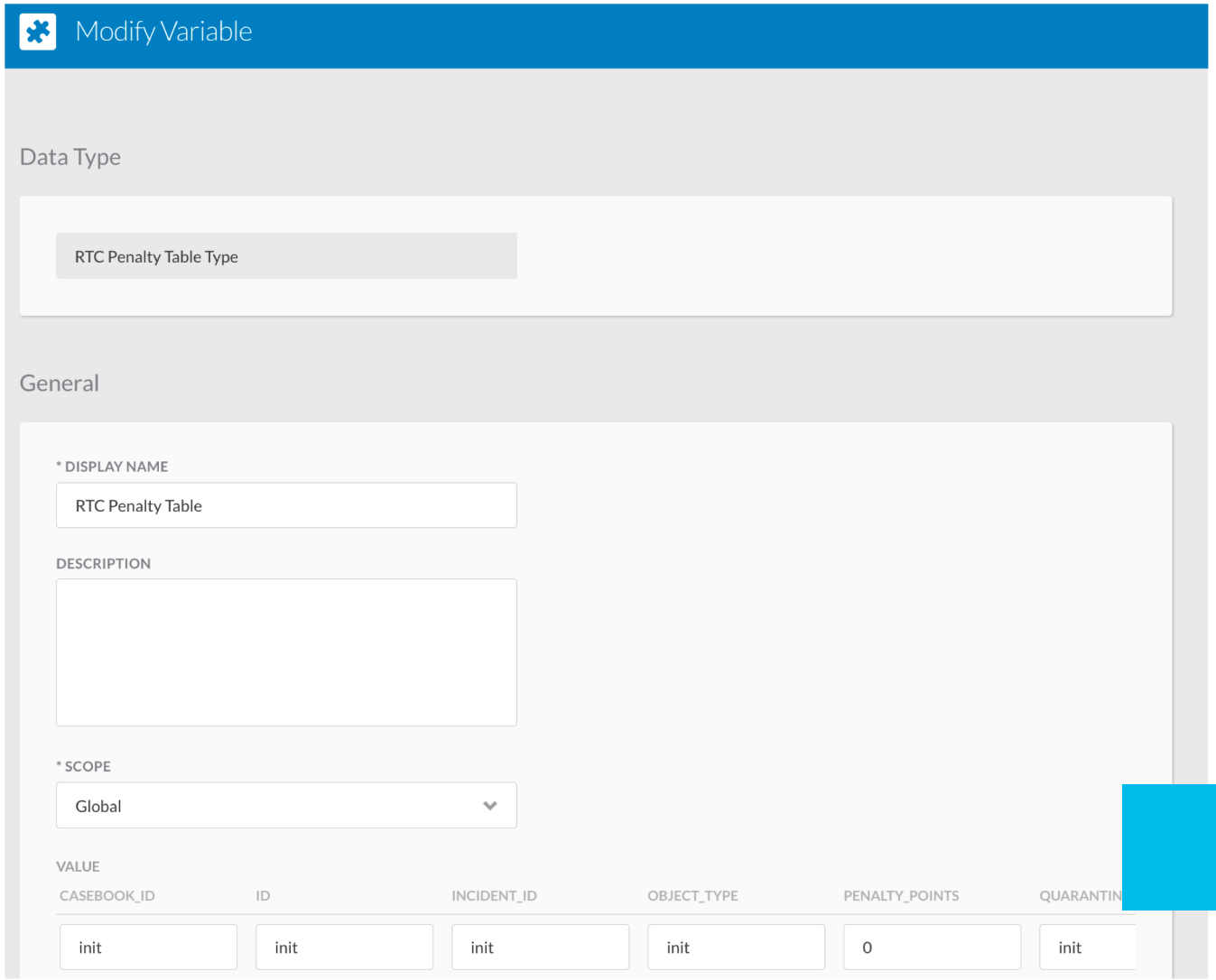
RTC Event Table Type

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



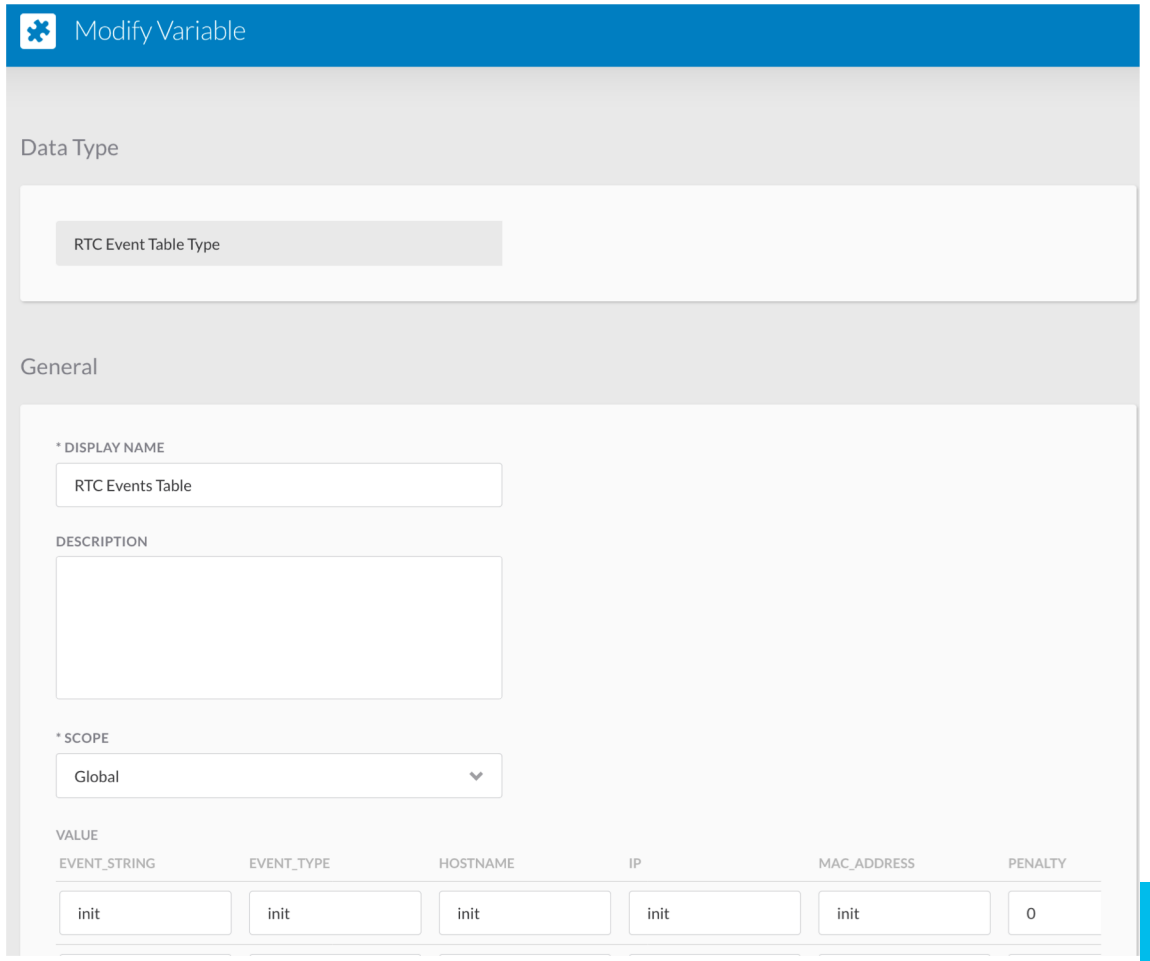
RTC Config

2a. Create Penalty Table Variable



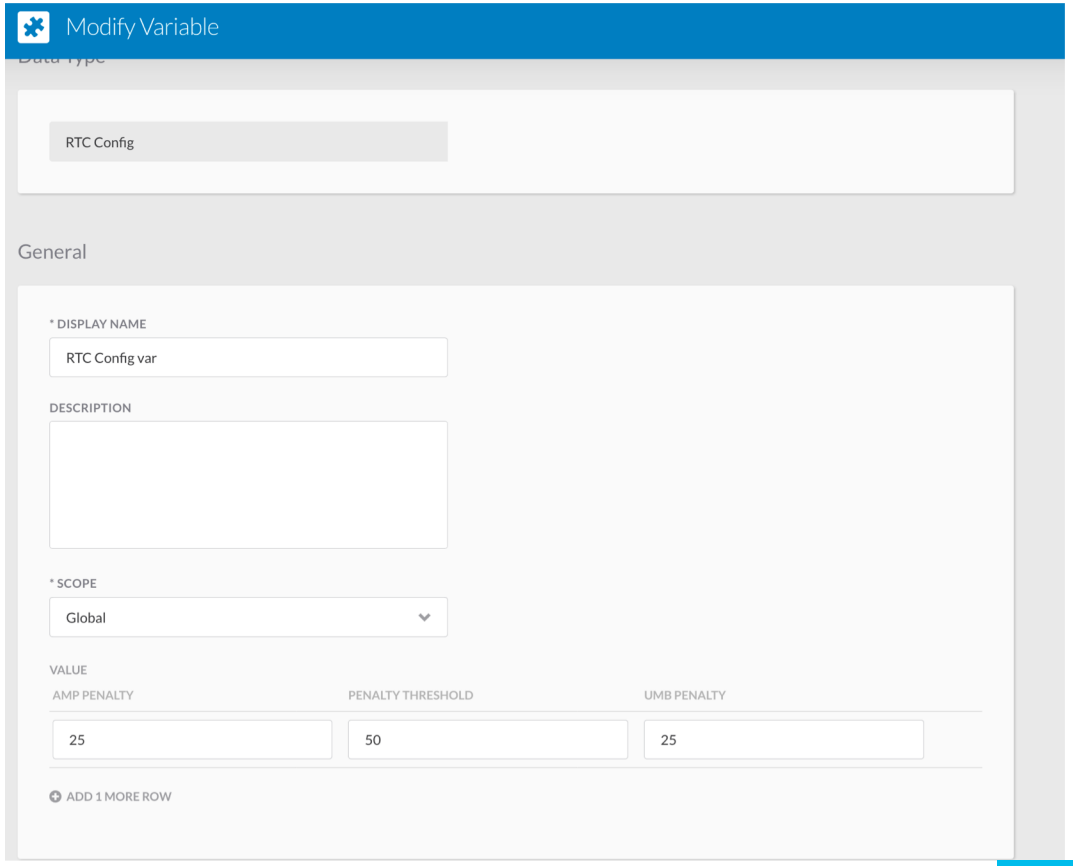
RTC Penalty Table

2b. Create Event Variable



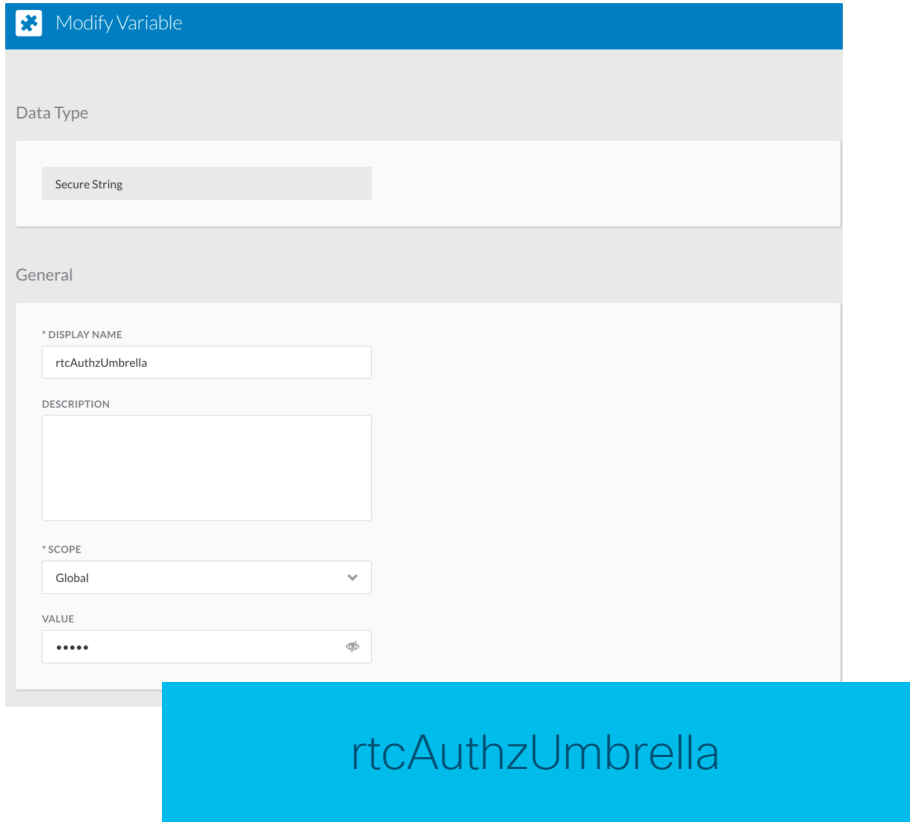
RTC Event Table

2c. Create Config Variables in SecureX

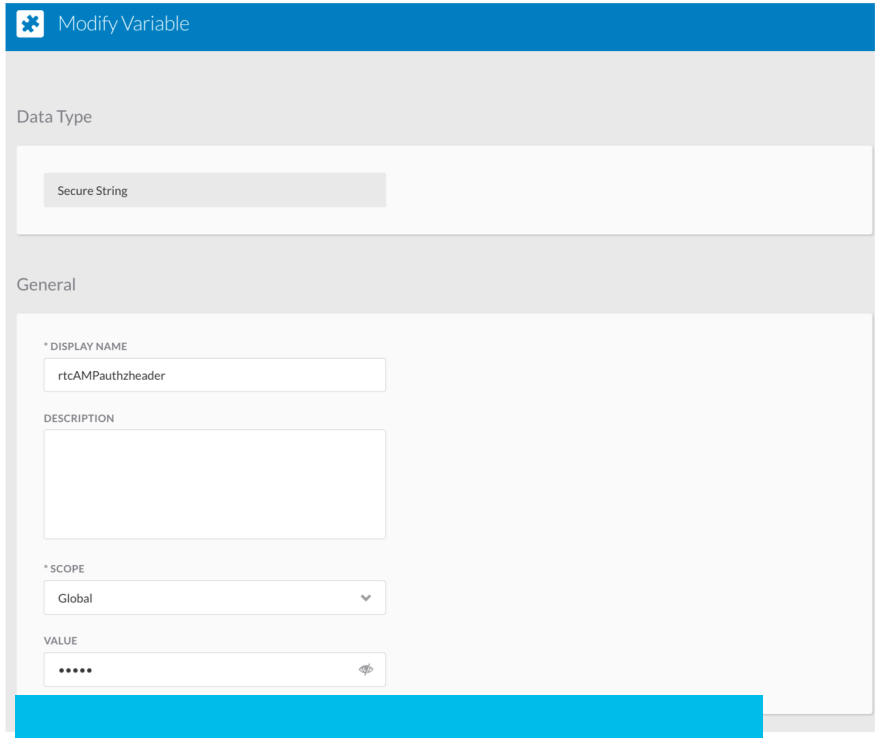


RTC Config

2d Create Variables for Authorizations strings

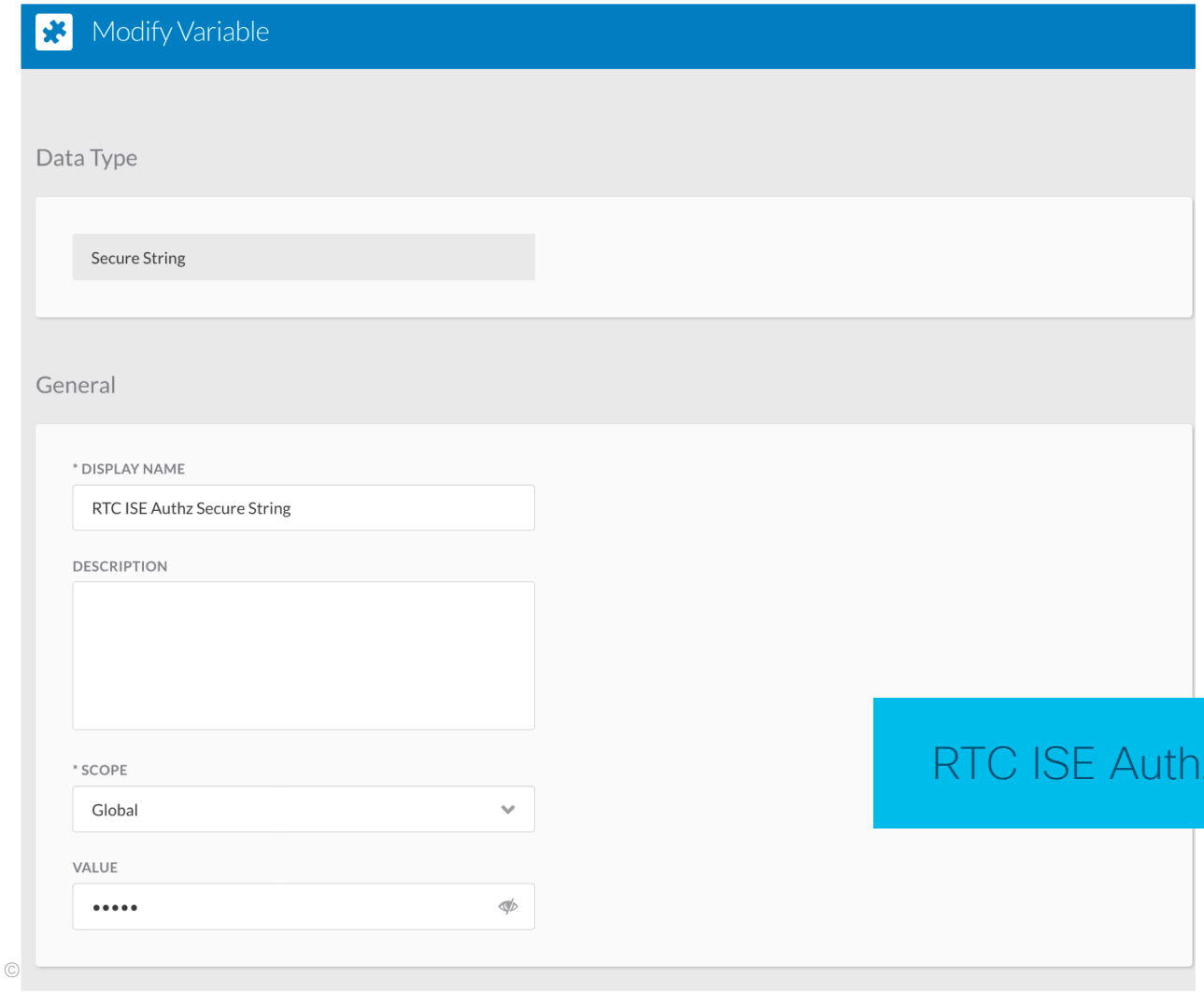


rtcAuthzUmbrella



rtcAMPauthzheader

2e Create Variables for Authorizations strings



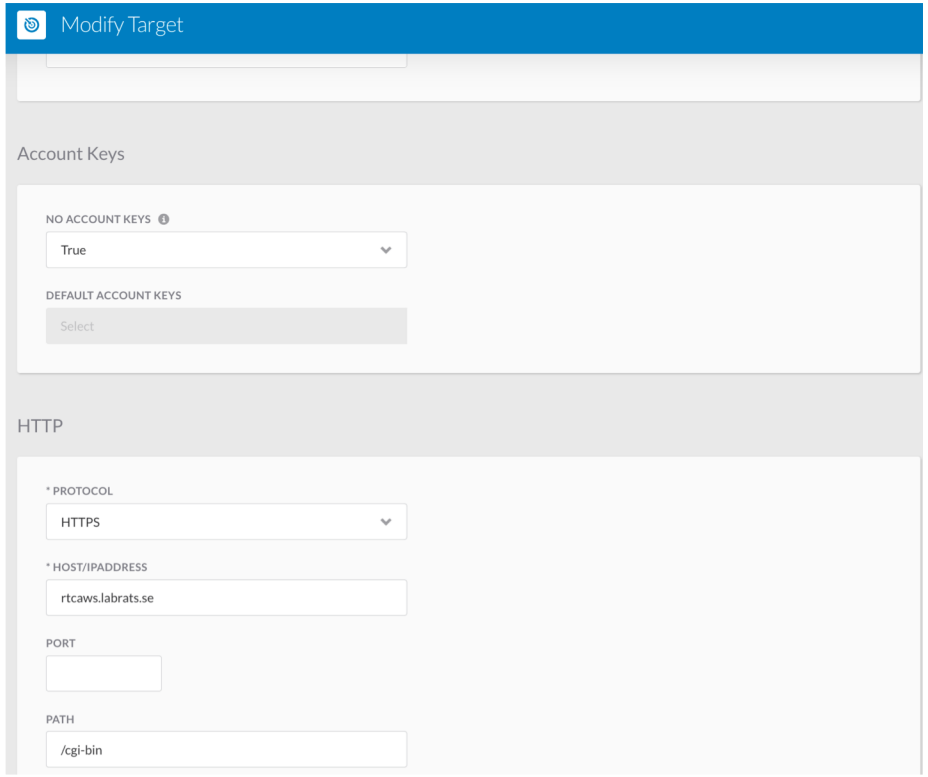
RTC ISE Authz Secure String

3 Create Targets.....

RTC ISE. middleware

AMP Cloud (US, EU, SIA)

Umbrella Cloud (US, EU, SIA)



4. Download and Import the workflows