CISCO
SECURE

cisco The bridge to possible

cisco SECURE X Orchestration Hackathon

American Frenchies

SecureX Orchestration Hackathon 2021

Alexandre Argeris, Cybersecurity TSA
Kevin C-Dubois, Cybersecurity TSS

Problem solved
Customer outcomes
Use Cases

Customer needs

Enrichment

Contextualize investigations, eliminate manual pivots, intelligence, verdicts / workflow catalog

"You really want [incidents/alerts] to be enriched with as much context as possible, so analysts don't have to pivot to a bunch of different systems." ***SOC Director, Insurance***

Response

Most demand for automated outcome is needed in email phishing, endpoint and malware / workflow catalog

"Users report phishing; automation might remove such email from everyone's inbox, remove file from endpoint, create a ticket for the desktop team." ***SOC Engineer, Healthcare***

Problem solved and customer outcomes

Secure Meter XD (written **SMXD**) is an **automated private security intelligence** framework to help automate internal observable judgements to **improve alert fidelity and automated response** inside of SecureX Orchestrator.

Use Cases

- Give the ability to security analyst to respond manually to a threat based on internal observable disposition.
  - Ex: before disabling a user in Cisco Secure Access by Duo the security analyst want to make sure more than 3 frauds authentication events has been received. (User observable = Suspicious)

- Let Cisco SecureX Orchestration respond automatically to a threat based on internal observable disposition.
  - Ex: Leverage Cisco Secure Endpoint isolation after 5 security events from any security event provider, Cisco Secure Endpoint, ISE, Duo, Secure Firewall, etc. (hostname observable = Malicious)

Innovation / Solution

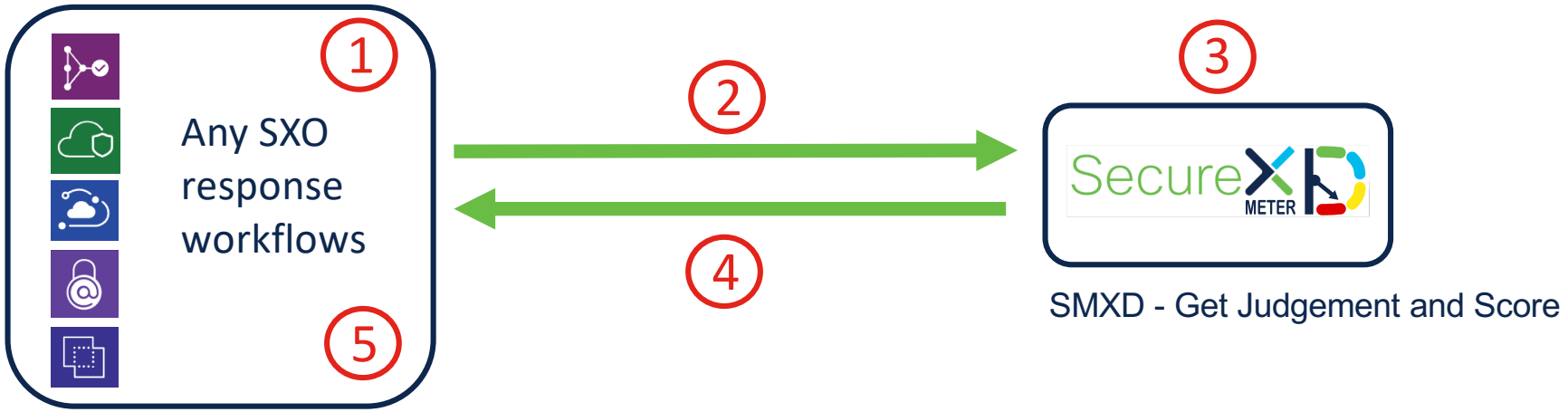
Secure Meter XD Framework

Inputs 1
- Observable (string)
- Increment / Decrement (integer)

Workflows 2
- Look for existing Judgement
- Create or Update Judgement based on the increment or decrement.

Output 3
- Observable (string)
- Current Judgement (string)

Secure Meter XD Framework

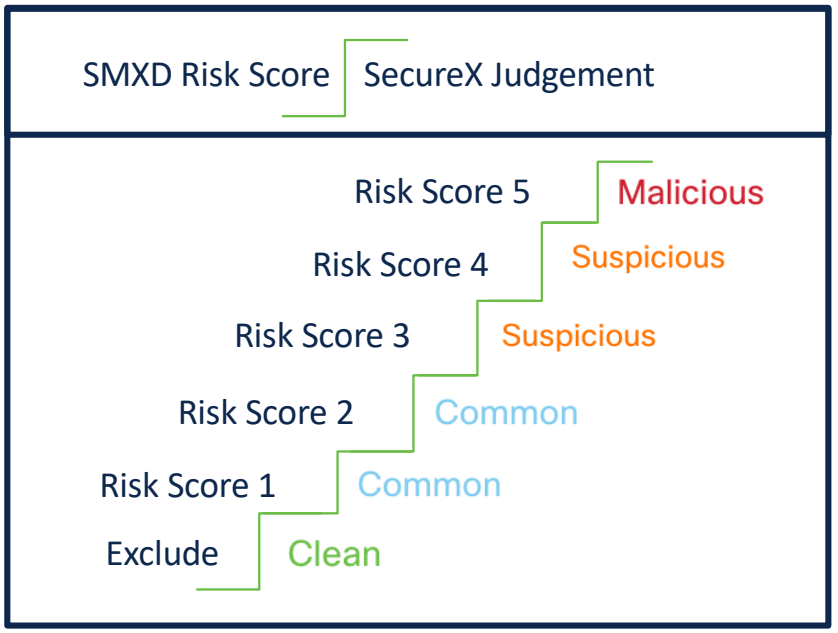


1. Customer Response Workflow need to identify the SMXD risk and disposition.
2. Workflow initiate a request to SMXD using the atomic action.
3. SMXD Atomic Action get the Judgement and Score for this observable.
4. Information are returned to the workflow.
5. Workflow can now choose automatically based on pre-config criteria the proper response action according to the current observable disposition.

Get SMXD disposition

Secure Meter XD Framework

- Secure Meter XD leverages SecureX private CTIA to store judgements on internal observable.
- Observable types are validated in all workflows
- Judgements are automatically created or updated based on the increment or decrement value.
- **“[Raise|Lower] Observable judgement”** workflows can be added to any exiting workflow or from the Pivot Menu.
- “**SMXD - Exclude Observable**” can be used to exclude an observable from the SMXD classification.



Supported Observable types

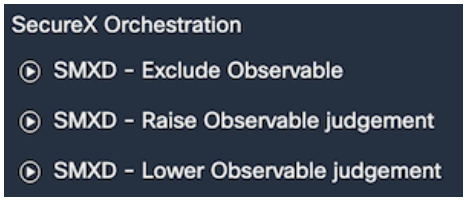
- ip (with validation for RFC 1918 for private IP)
- Hostname
- Username
- Email (with internal domains validation)
- amp_computer_guid
- mac_address

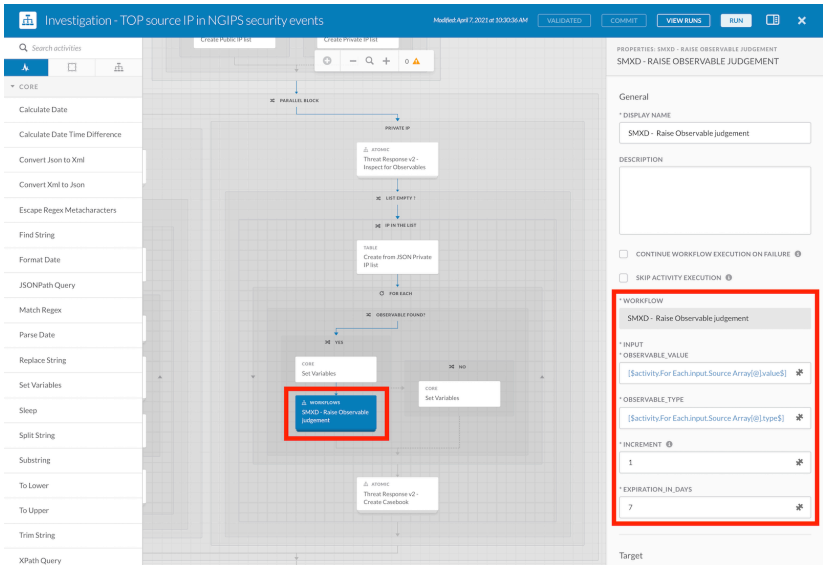
Secure Meter XD framework - Installation

- Secure Meter XD **does not** require any external component. ✔
- **No** database or SecureX Orchestration table required. 😀
- Only 4 workflows and 5 atomic actions.
- **No additonal target** to add. ✔
- Very **easy to add** to an existing workflows for input. ✔
- SMXD Response **workflow framework provided**. ✔
- SMXD atomic actions can be add to any response workflow. 😀
- All details in the README.md of the repo.

Secure Meter XD framework – How to use

Secure Meter XD can be use manually by clicking on "Exclude", "Raise" or "lower" workflows on the pivot menu of SecureX.

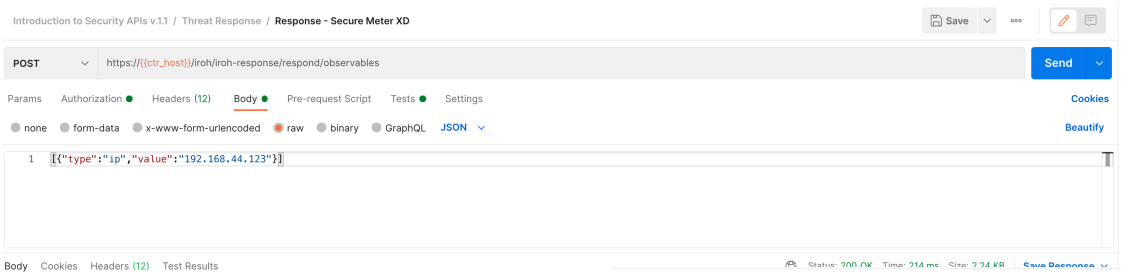


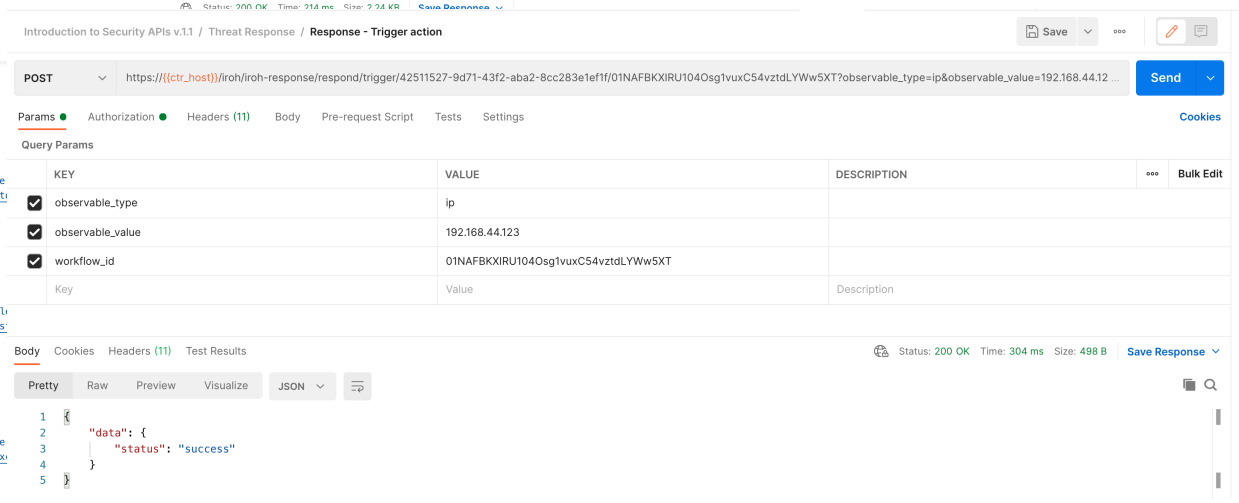


Secure Meter XD can also be added to any existing workflow where internal observables are collected or identified. The "Increment" variable can be modified from 1 to 5 to represent the criticality of the security events for the identified internal observable. The "Expiration_in_Days" set the expiration time frame for CTIA Judgement at the creation.

Secure Meter XD framework – How to use

Using Secure Meter XD with third-party SOAR

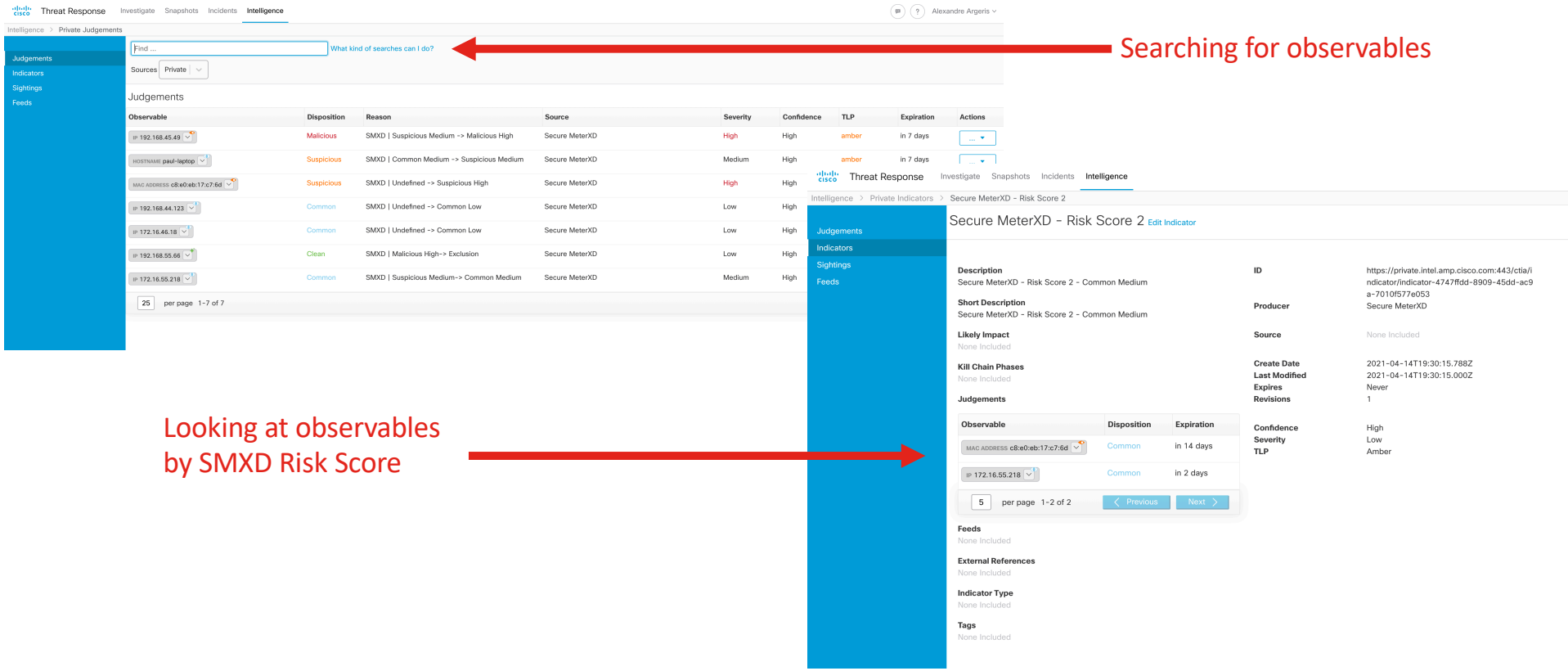




Ref: https://visibility.amp.cisco.com/iroh/iroh-response/index.html

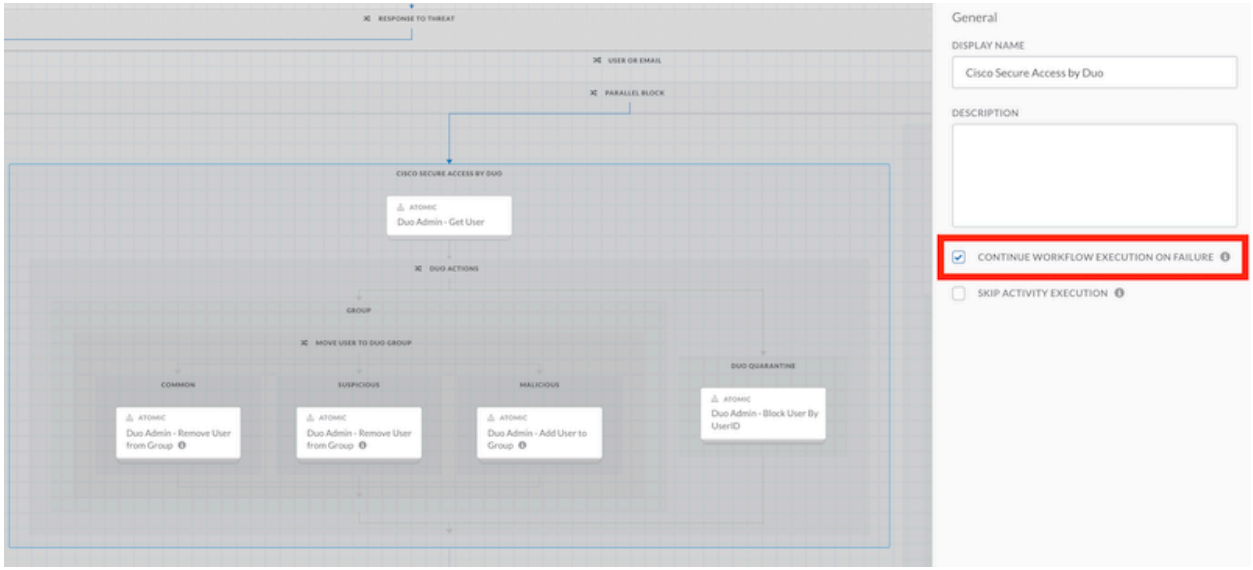
Secure Meter XD framework – How to use

Using Secure Meter XD is easy for the Security Analyst



Secure Meter XD framework – Optional Response workflow

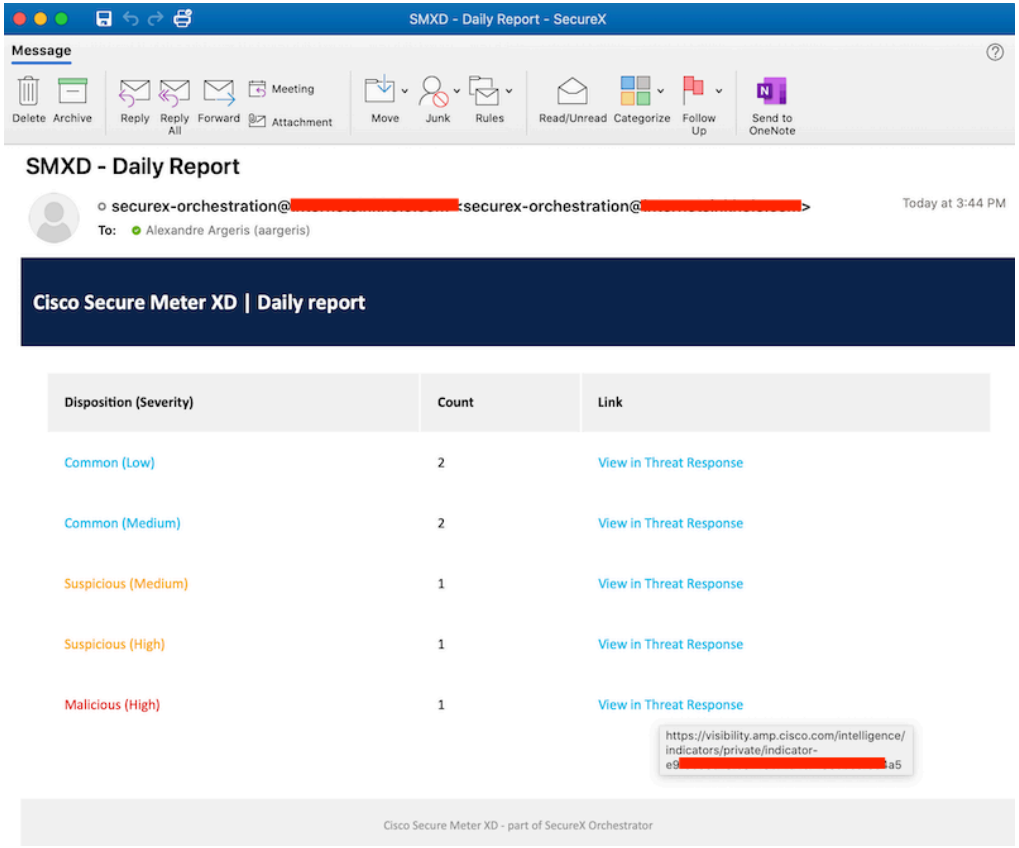
At the end of each SMXD workflow an optional response workflow can be added to response to threat based on the disposition of the internal observable.



"SMXD - Response actions based on disposition v2" workflow is a very flexible and will run even if you do not have a subscription for some of theses Cisco response action.

Secure Meter XD framework – Optional Report workflow

"SMXD – Email Report" workflow can be run to generate and email a daily report. The report include count of observables for each SMXD risk score and a link to the Cisco SecureX Indicator page.



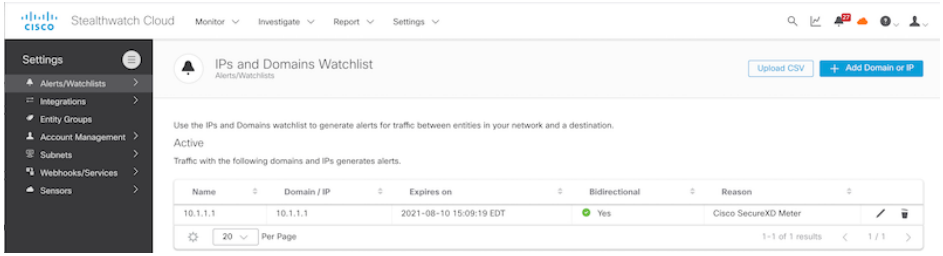
Secure Meter XD framework – Optional Response workflow

SMXD response to threat are based on the disposition of the internal observable. The appropriate action are initiate based on the risk of this observable within the customer environment.

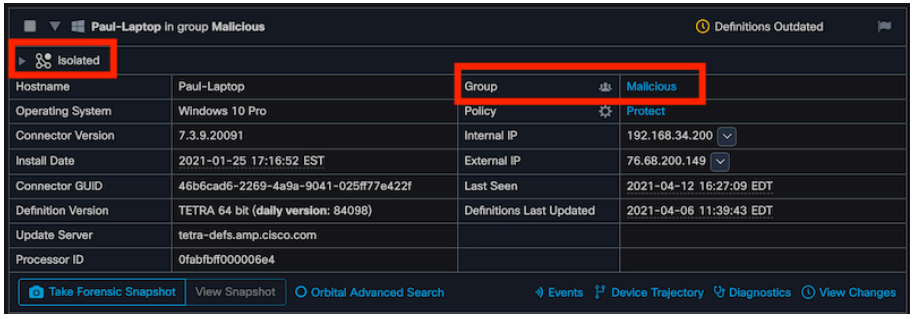
Secure Meter XD framework – Optional Response workflow

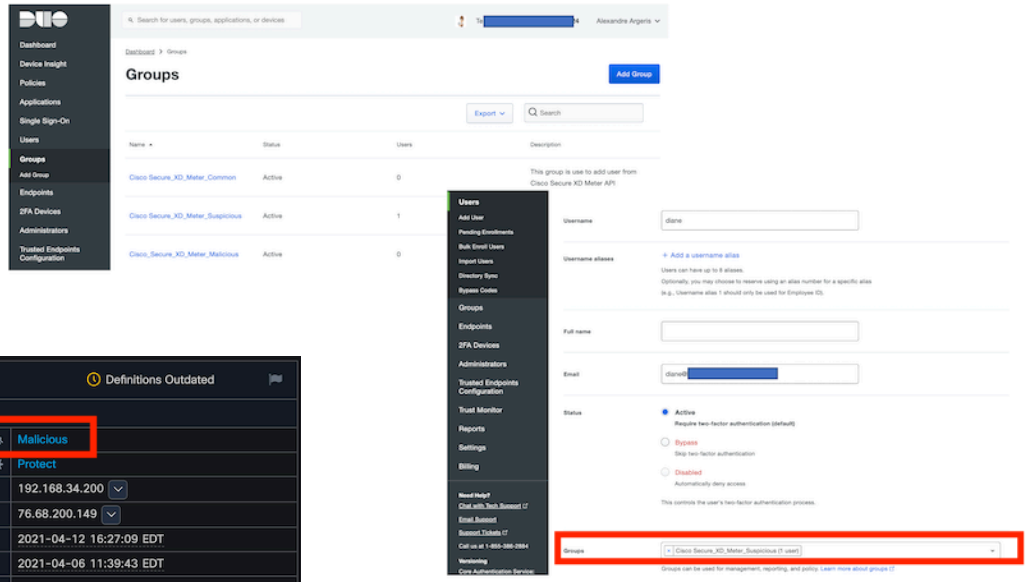
SMXD Response workflow come with pre-configured response actions based on disposition

Cisco Secure Cloud Analytics, add "IP" to IP watchlist



Cisco Secure Endpoint, move device to another group - isolate a device



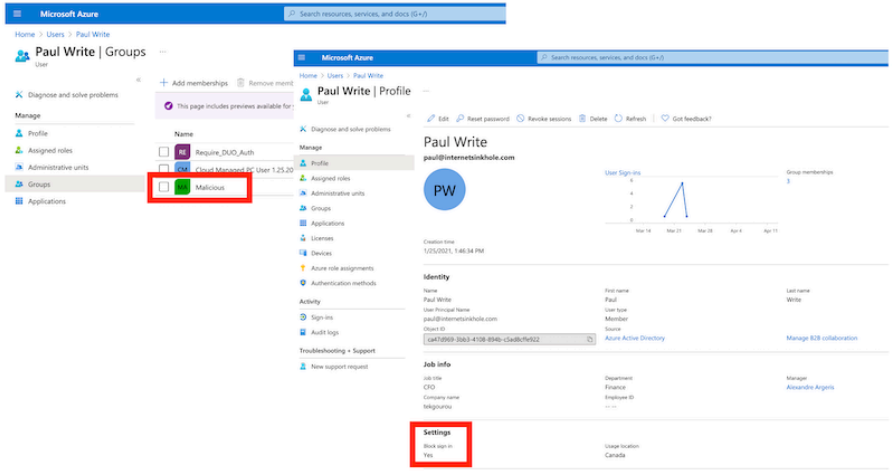


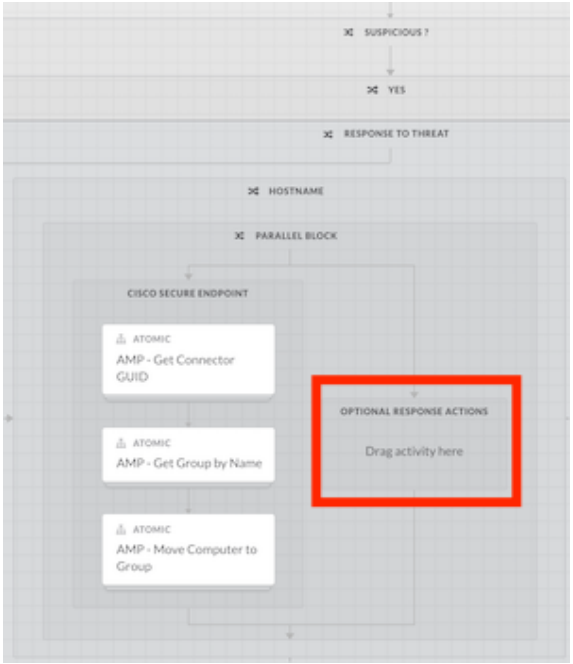
Cisco Secure Access by Duo, move user to a Duo local group - disable a user

Secure Meter XD framework – Optional Response workflow

SMXD Response workflow come with pre-configured **third-party** response actions

Microsoft Azure AD, add / remove user from group - Block sing in





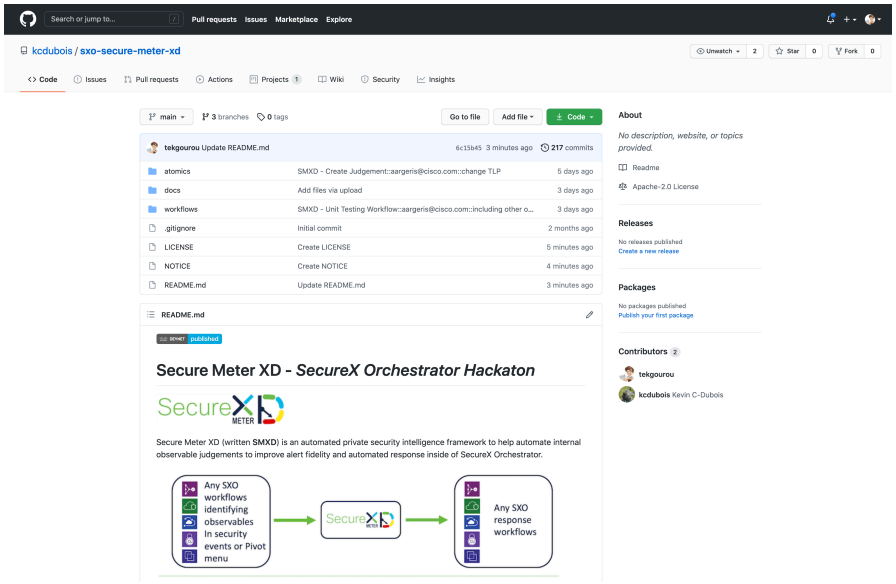
And it include section to add your own response action from a Third-party per example.

External references

(Github repo / youtube video)

Secure Meter XD framework - References

https://github.com/kcdubois/sxo-secure-meter-xd



https://www.youtube.com/watch?v=asXN3m9fV5U


CISCO


SecureX
METER