

CISCO
SECURE



American Frenchies

SecureX Orchestration Hackathon 2021

Alexandre Argeris, Cybersecurity TSA

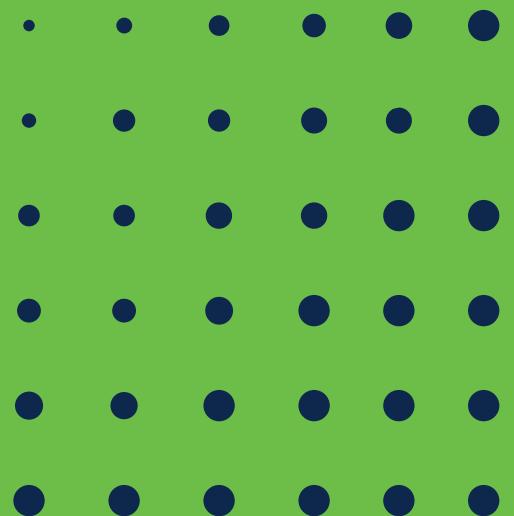
Kevin C-Dubois, Cybersecurity TSS

CISCO The bridge to possible



CISCO
SECURE X
Orchestration
Hackathon

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***

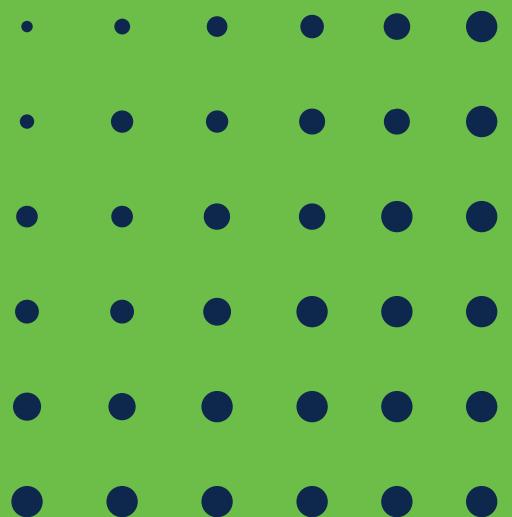
Problem solved and customer outcomes

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

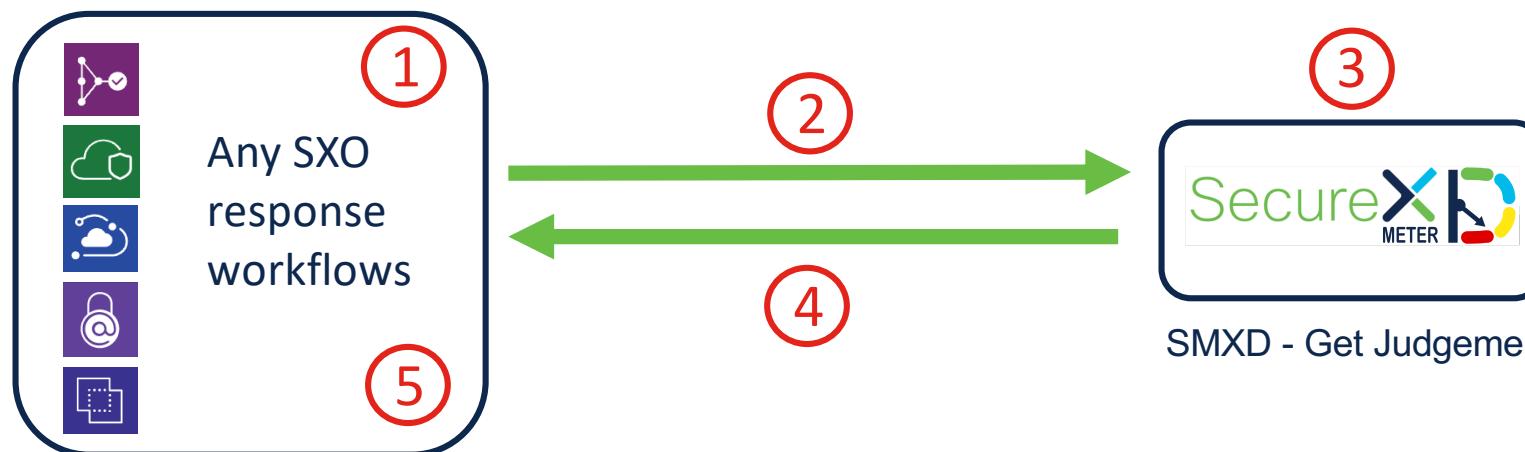


- Inputs **1**
- Observable (string)
 - Increment / Decrement (integer)

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

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

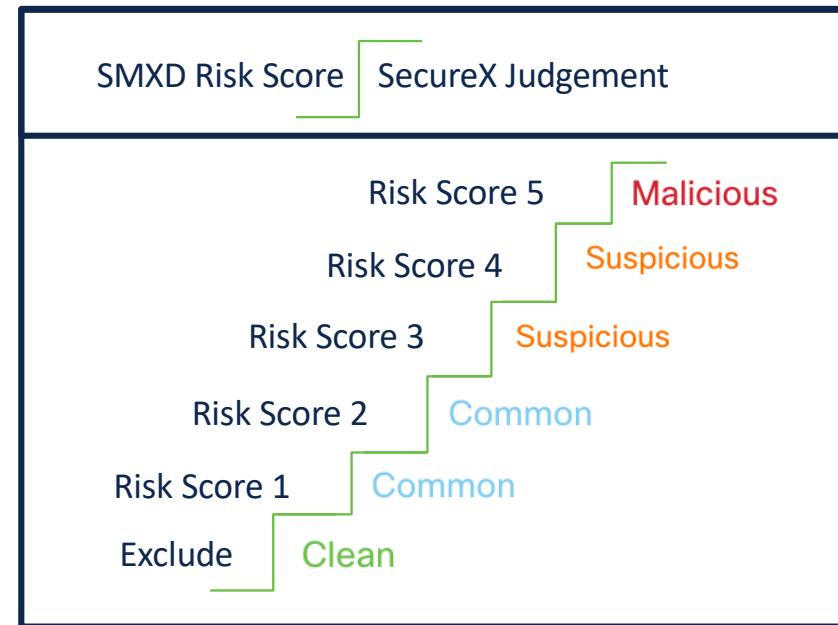
Secure Meter XD Framework



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

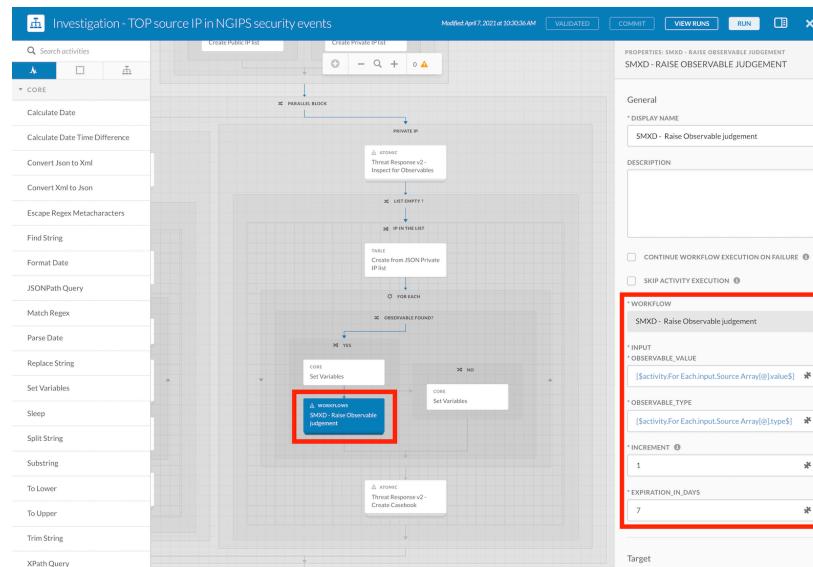
- Secure Meter XD **does not** require any external component. ✓
- **No** database or SecureX Orchestration table required. 😊
- Only 4 workflows and 5 atomic actions.
- **No additional target** to add. ✓
- Very **easy to add** to an existing workflows for input. ✓
- SMXD Response **workflow framework 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 used manually by clicking on "Exclude", "Raise" or "lower" workflows on the pivot menu of SecureX.

SecureX Orchestration

- ◎ SMXD - Exclude Observable
- ◎ SMXD - Raise Observable judgement
- ◎ SMXD - Lower Observable judgement



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

Introduction to Security APIs v.1.1 / Threat Response / Response - Secure Meter XD

POST https://((ctr_host))/iroh/iroh-response/respond/observables

Params Authorization Headers (12) Body Pre-request Script Tests Settings Cookies None form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 [{"type": "ip", "value": "192.168.44.123"}]
```

Save Send

Body Cookies Headers (12) Test Results

Pretty Raw Preview Visualize JSON

Status: 200 OK Time: 214 ms Size: 2.24 KB Save Response

Introduction to Security APIs v.1.1 / Threat Response / Response - Trigger action

POST https://((ctr_host))/iroh/iroh-response/respond/trigger/42511527-9d71-43f2-aba2-8cc283e1ef1f/01NAFBKXIRU104Osg1vuxC54vztdLYWw5XT?observable_type=ip&observable_value=192.168.44.123

Params Authorization Headers (11) Body Pre-request Script Tests Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION	Bulk Edit
<input checked="" type="checkbox"/> observable_type	ip		
<input checked="" type="checkbox"/> observable_value	192.168.44.123		
<input checked="" type="checkbox"/> workflow_id	01NAFBKXIRU104Osg1vuxC54vztdLYWw5XT		

Key Value Description

Body Cookies Headers (11) Test Results

Pretty Raw Preview Visualize JSON

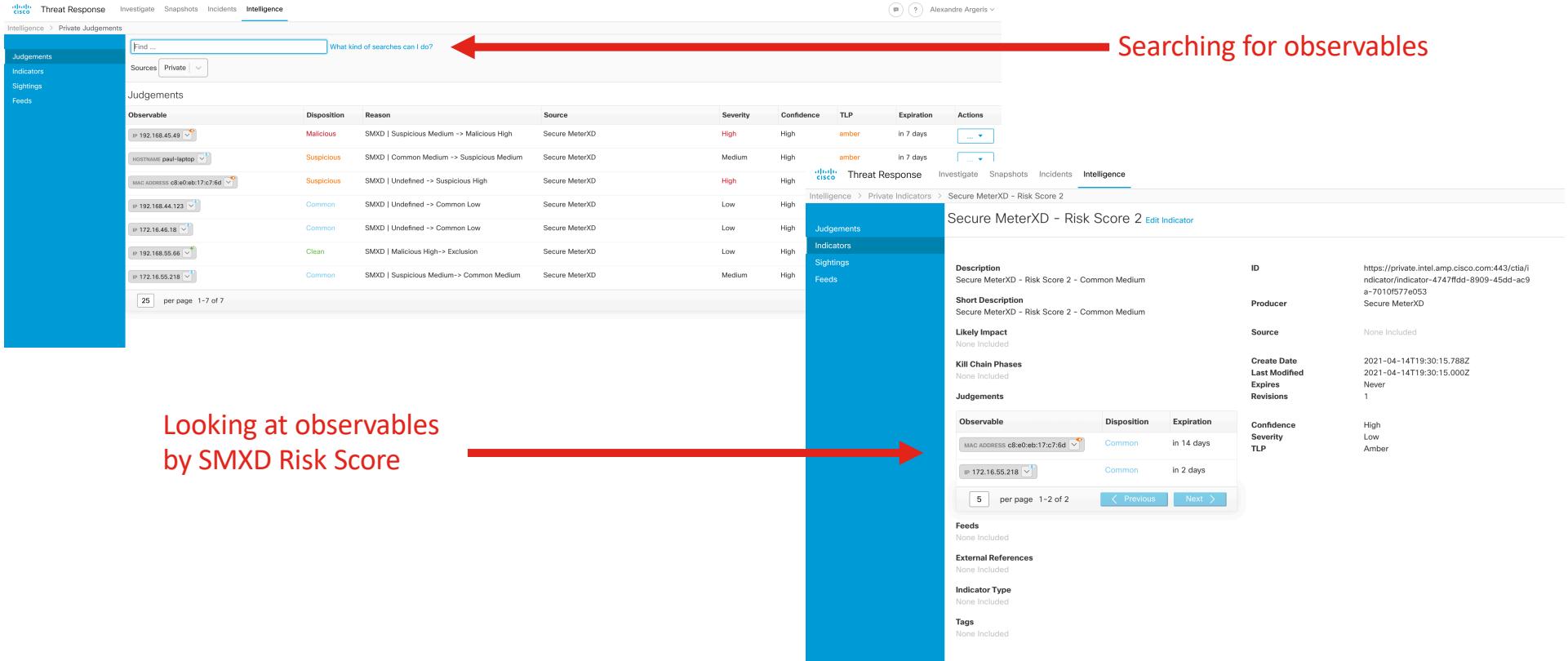
Status: 200 OK Time: 304 ms Size: 498 B Save Response

```
1 {"data": { "status": "success" }}
```

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



Intelligence > Private Judgements

Find ... What kind of searches can I do? ←

Sources: Private

Judgements

Observable	Disposition	Reason	Source	Severity	Confidence	TLP	Expiration	Actions
IP 192.168.45.49	Malicious	SMXD Suspicious Medium -> Malicious High	Secure MeterXD	High	High	amber	In 7 days	...
Hostname paul-laptop	Suspicious	SMXD Common Medium -> Suspicious Medium	Secure MeterXD	Medium	High	amber	In 7 days	...
MAC ADDRESS c8:e0:eb:17:c7:6d	Suspicious	SMXD Undefined -> Suspicious High	Secure MeterXD	High	High	amber	In 7 days	...
IP 192.168.44.123	Common	SMXD Undefined -> Common Low	Secure MeterXD	Low	High	amber	In 7 days	...
IP 172.16.46.18	Common	SMXD Undefined -> Common Low	Secure MeterXD	Low	High	amber	In 7 days	...
IP 192.168.55.66	Clean	SMXD Malicious High-> Exclusion	Secure MeterXD	Low	High	amber	In 7 days	...
IP 172.16.55.218	Common	SMXD Suspicious Medium-> Common Medium	Secure MeterXD	Medium	High	amber	In 7 days	...

25 per page 1-7 of 7

Intelligence > Private Indicators > Secure MeterXD - Risk Score 2

Secure MeterXD - Risk Score 2 [Edit Indicator](#)

Description: Secure MeterXD - Risk Score 2 - Common Medium ID: https://private.intel.amp.cisco.com:443/ctia/indicator/indicator-4747ffdd-8909-45dd-ac9a-7010f577e053 Producer: Secure MeterXD

Short Description: Secure MeterXD - Risk Score 2 - Common Medium Source: None Included

Likely Impact: None Included Create Date: 2021-04-14T19:30:15.788Z

Kill Chain Phases: None Included Last Modified: 2021-04-14T19:30:15.000Z

Expires: Never Revisions: 1

Judgements

Observable	Disposition	Expiration
MAC ADDRESS c8:e0:eb:17:c7:6d	Common	In 14 days
IP 172.16.55.218	Common	In 2 days

5 per page 1-2 of 2 < Previous Next >

Feeds: None Included

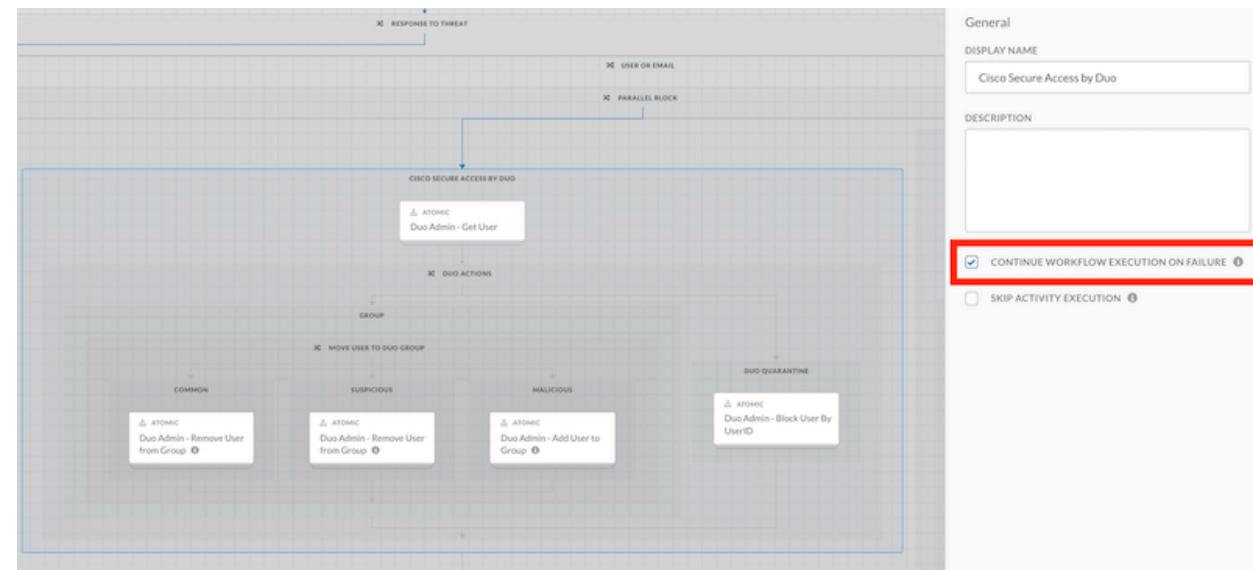
External References: None Included

Indicator Type: None Included

Tags: None Included

Secure Meter XD framework – Optional Response workflow

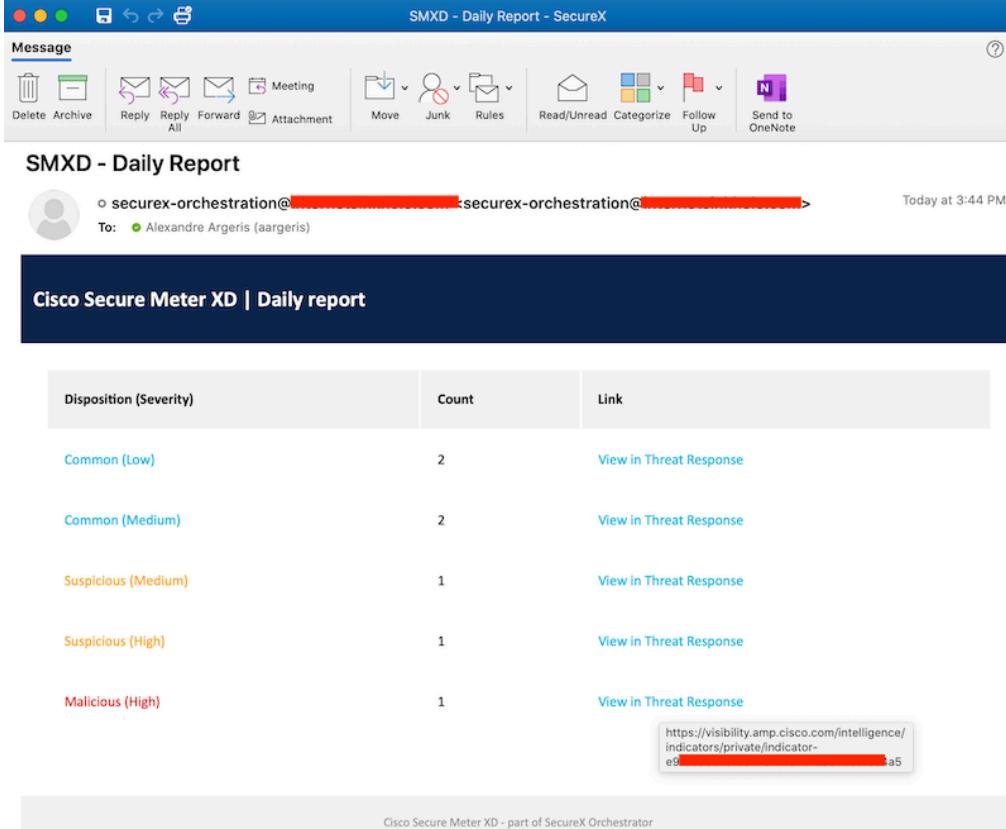
At the end of each SMXD workflow an optional response workflow can be added to response to threat based on the disposition of the internal observable.



"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.



SMXD - Daily Report

From: securex-orchestration@█████████████████████ To: Alexandre Argeris (aargeris) Today at 3:44 PM

Cisco Secure Meter XD | Daily report

Disposition (Severity)	Count	Link
Common (Low)	2	View in Threat Response
Common (Medium)	2	View in Threat Response
Suspicious (Medium)	1	View in Threat Response
Suspicious (High)	1	View in Threat Response
Malicious (High)	1	View in Threat Response

https://visibility.amp.cisco.com/intelligence/indicators/private/indicator-e9████████████████a5

Cisco Secure Meter XD - part of SecureX Orchestrator

Secure Meter XD framework – Optional Response workflow

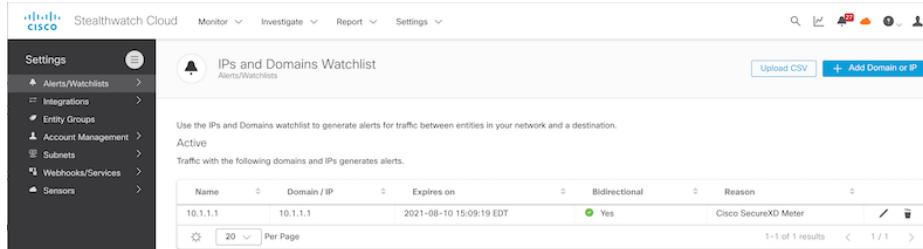
SMXD response to threat are based on the disposition of the internal observable. The appropriate action are initiate based on the risk of this observable within the customer environment.



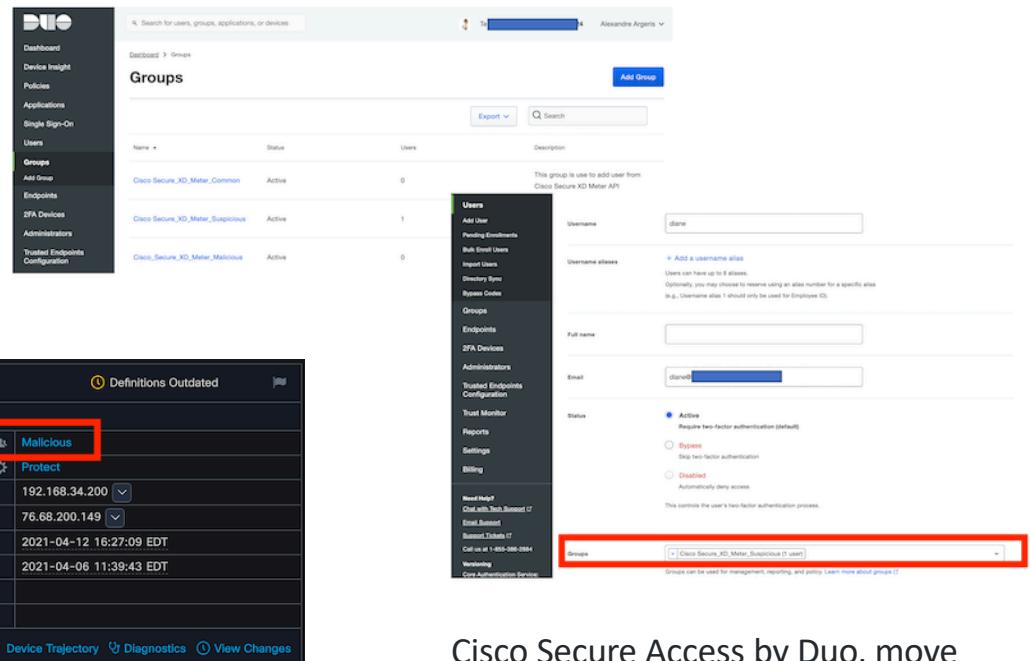
Secure Meter XD framework – Optional Response workflow

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

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

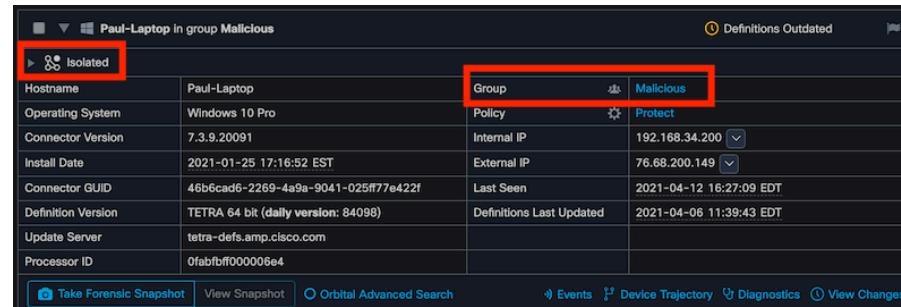


The screenshot shows the Cisco Secure Cloud Analytics interface under the 'Alerts/Watchlists' section. It displays a table with one row: Name: 10.1.1, Domain / IP: 10.1.1.1, Expires on: 2021-08-10 15:09:19 EDT, Bidirectional: Yes, Reason: Cisco SecureXD Meter. A red box highlights the 'Add Domain or IP' button.



The screenshot shows the Duo Groups management interface. It includes sections for Groups, Users, and Groups. A red box highlights the 'Groups' section where a new group 'Cisco_Secure_XD_Meter_Suspicious' is being created, assigned to the user Alexandre Argens. Another red box highlights the 'Groups' dropdown in the user creation form.

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



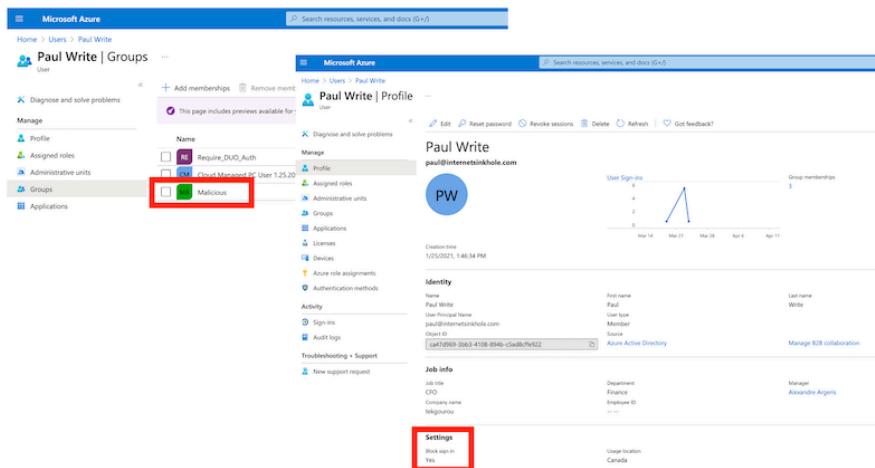
The screenshot shows the Cisco Secure Endpoint device details interface for 'Paul-Laptop'. A red box highlights the 'Isolated' status indicator. Another red box highlights the 'Group' field which is set to 'Malicious'.

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



The screenshot shows two pages from Microsoft Azure AD:

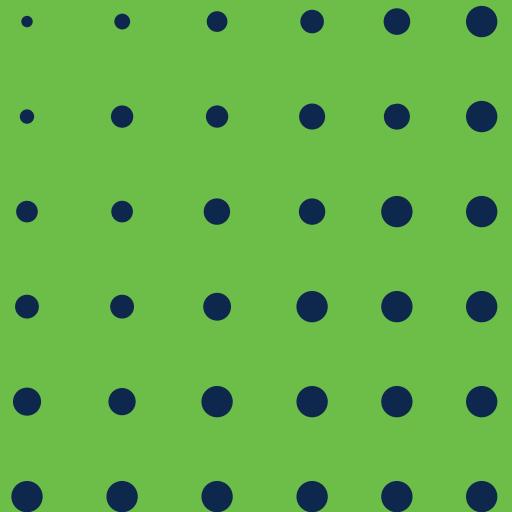
- Left Page (Groups):** Shows the 'Groups' section for a user named 'Paul Write'. A red box highlights the 'Malicious' checkbox under 'Administrative units'.
- Right Page (Profile):** Shows the 'Profile' page for the same user. A red box highlights the 'Settings' section at the bottom left, which includes a 'Block sign-in' link.



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

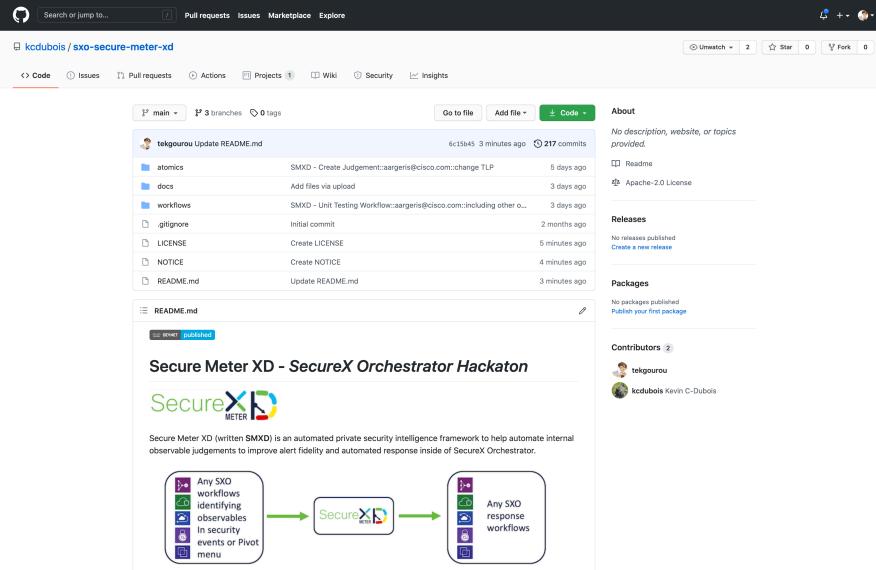
External references

(Github repo / youtube video)



Secure Meter XD framework - References

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



The screenshot shows the GitHub repository for "kcdubois / sxo-secure-meter-xd". The repository has 217 commits and 3 branches. The README.md file contains a diagram illustrating the integration of SecureX Orchestrator with Secure Meter XD. The diagram shows a flow from "Any SXO workflows, observables in security events or Pivot menu" through "SecureXD" to "Any SXO response workflows".

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



