The bridge to possible

Présentation de SecureX pour une Sécurité Maximale grâce à l'Automatisation

Community Live – Sécurité

Patrick Cardot - Technical Solution Architect | Internet Expert CCIE #1260
Xavier Crèvecœur - Network and Security Consultant | Security CCIE #11010 Firejumper Élite #135
30 Juin 2022

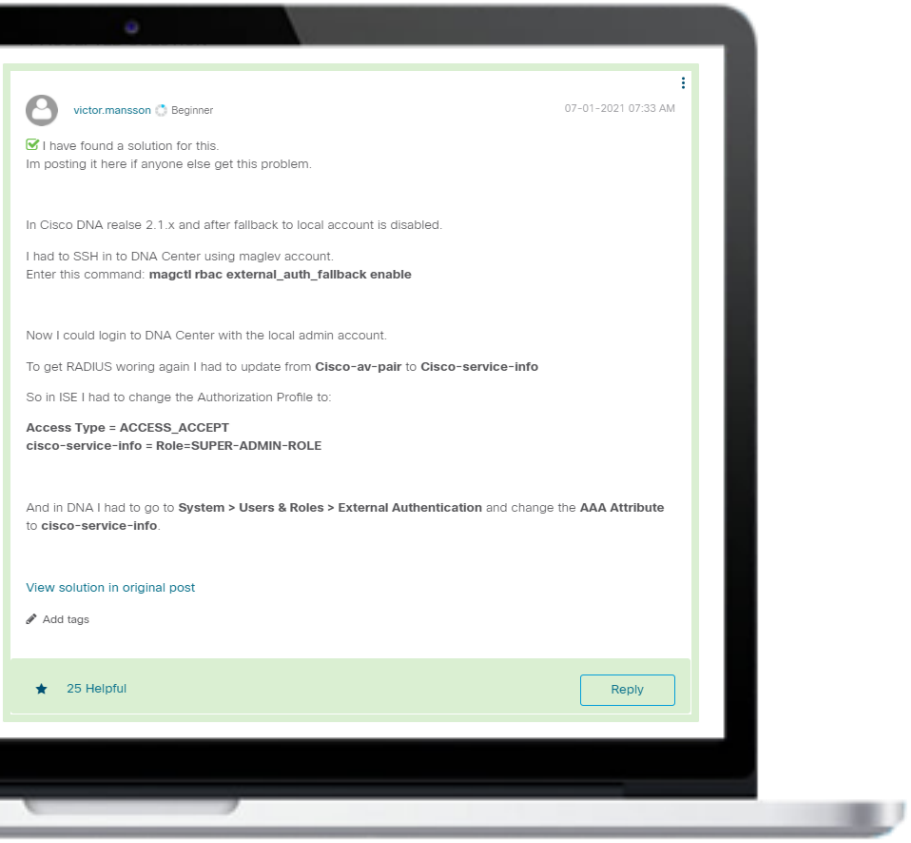
De grands changements arrivent dans la Communauté Cisco en juillet

En juillet, nous réimaginons la Communauté Cisco.

Nous travaillons pour vous procurer une expérience simplifiée et des ressources étape par étape pour vous guider dans l'adoption des produit et des technologies qui vous intéressent le plus !

[Des grandes choses arrivent dans la Communauté Cisco]

Connectez, Engagez, Collaborez !



Lorsque vous recevez une réponse correcte, **acceptez-la comme solution !**

Cela aide les autres utilisateurs à trouver des réponses correctes

Mettez en évidence les autres membres

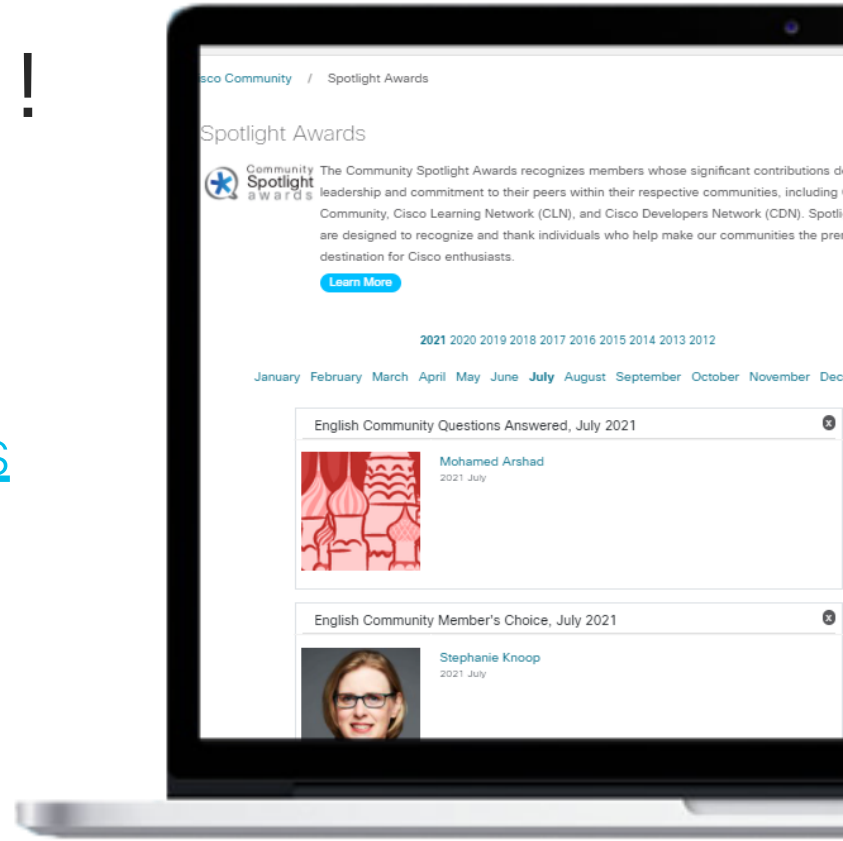
Les votes utiles motivent les membres enthousiastes en leur offrant **un signe de reconnaissance !**

Spotlight Awards

De nouveaux lauréats tous les mois !

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les Spotlight Awards sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat ! Cliquez ici



Notre Expert

Patrick Cardot
Présentateur

Xavier Crèvecœur
Question Manager

Jimena Saez
Modérateur

[Téléchargez la présentation !](https://bit.ly/WEB2sld-jun22)

https://bit.ly/WEB2sld-jun22

CISCO
SECURE

The bridge to possible

SecureX

Patrick Cardot
Technical Solutions Architect
2022-06-30

AMP4E

Firepower

CDO

Duo

E-mail Security

Web Security

Stealthwatch Cloud

Stealthwatch Enterprise

Threat Grid

Umbrella

Tetration

Integrate

SecureX

Orchestration

Dashboards

Threat Hunting

Enrichment

Incident Management

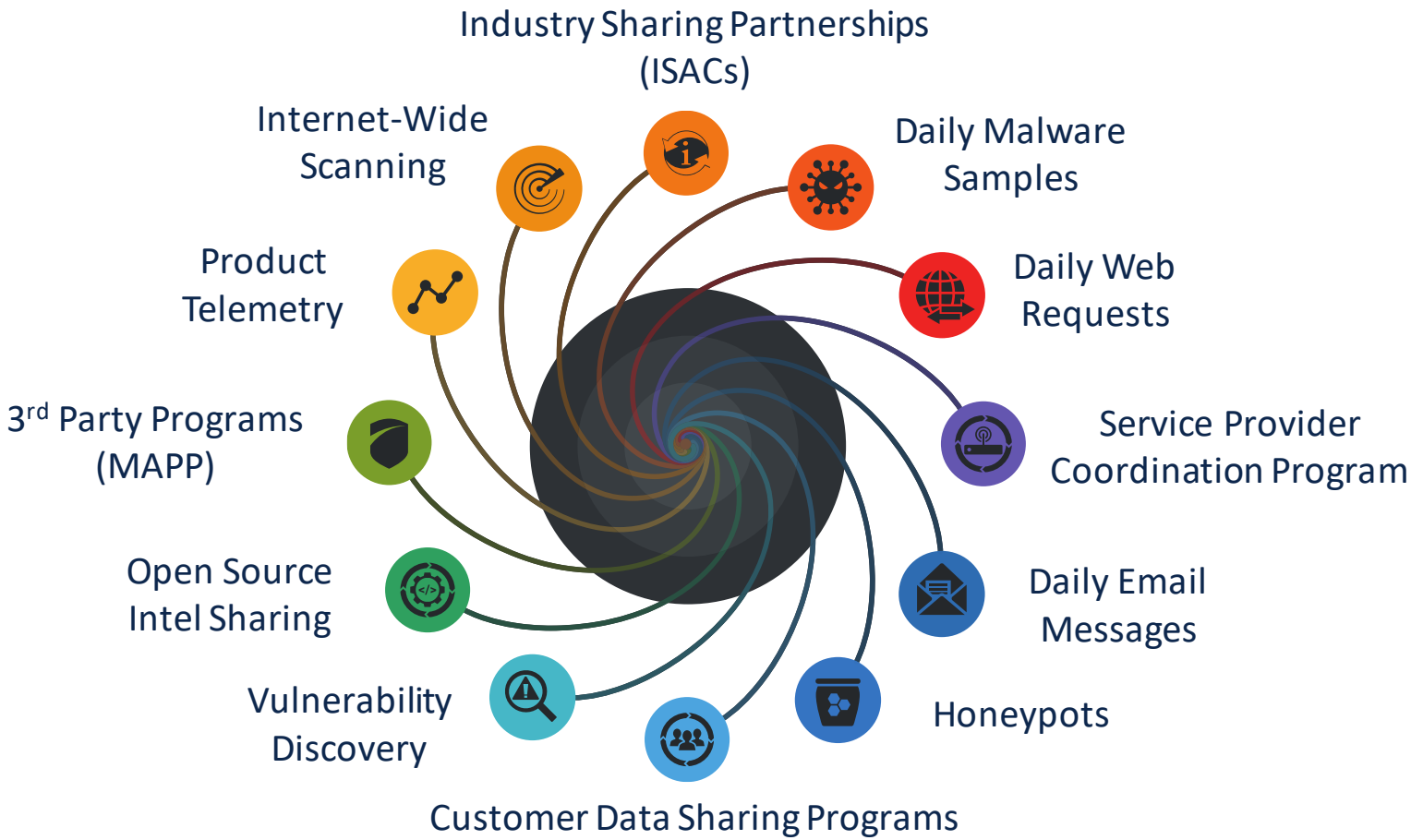
Response

TALOS

Cisco Security Research

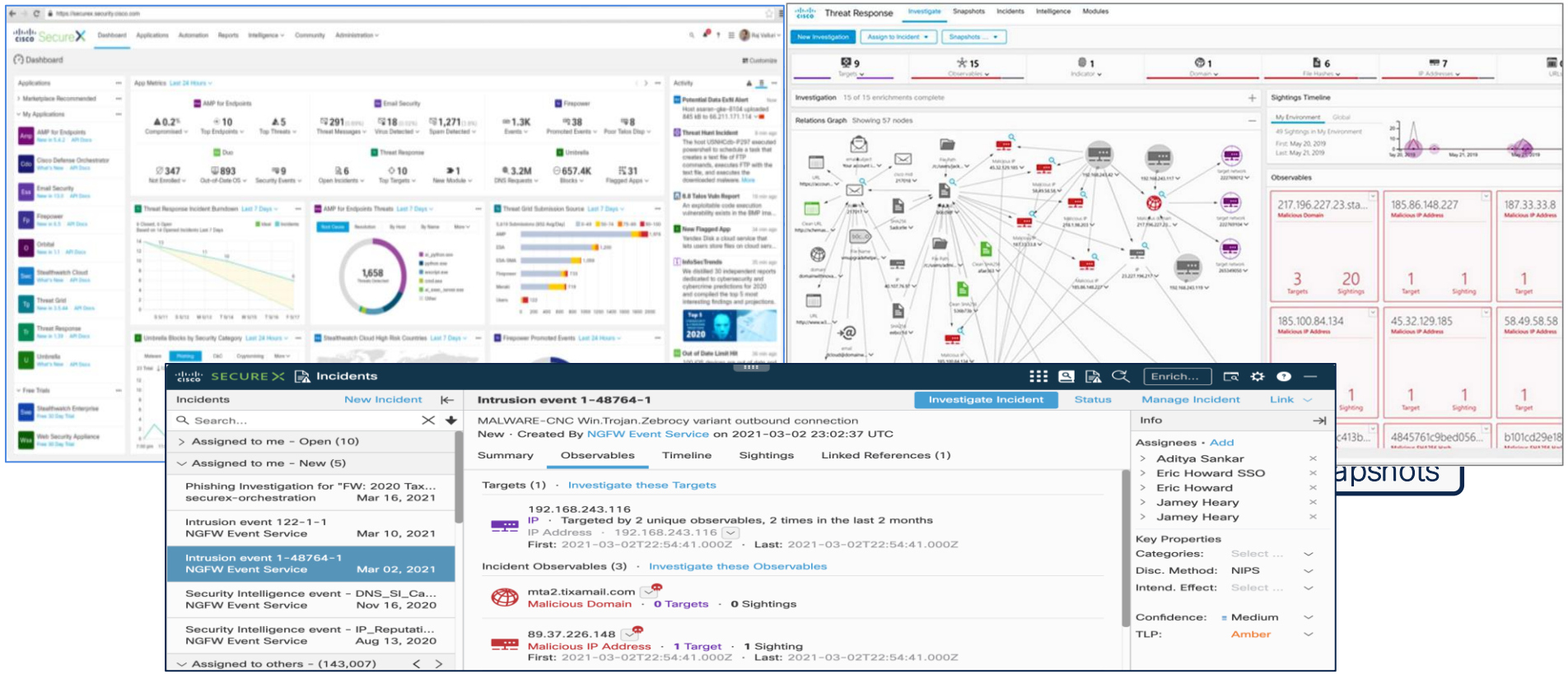
TALOSINTELLIGENCE.COM

Cisco Threat Intelligence

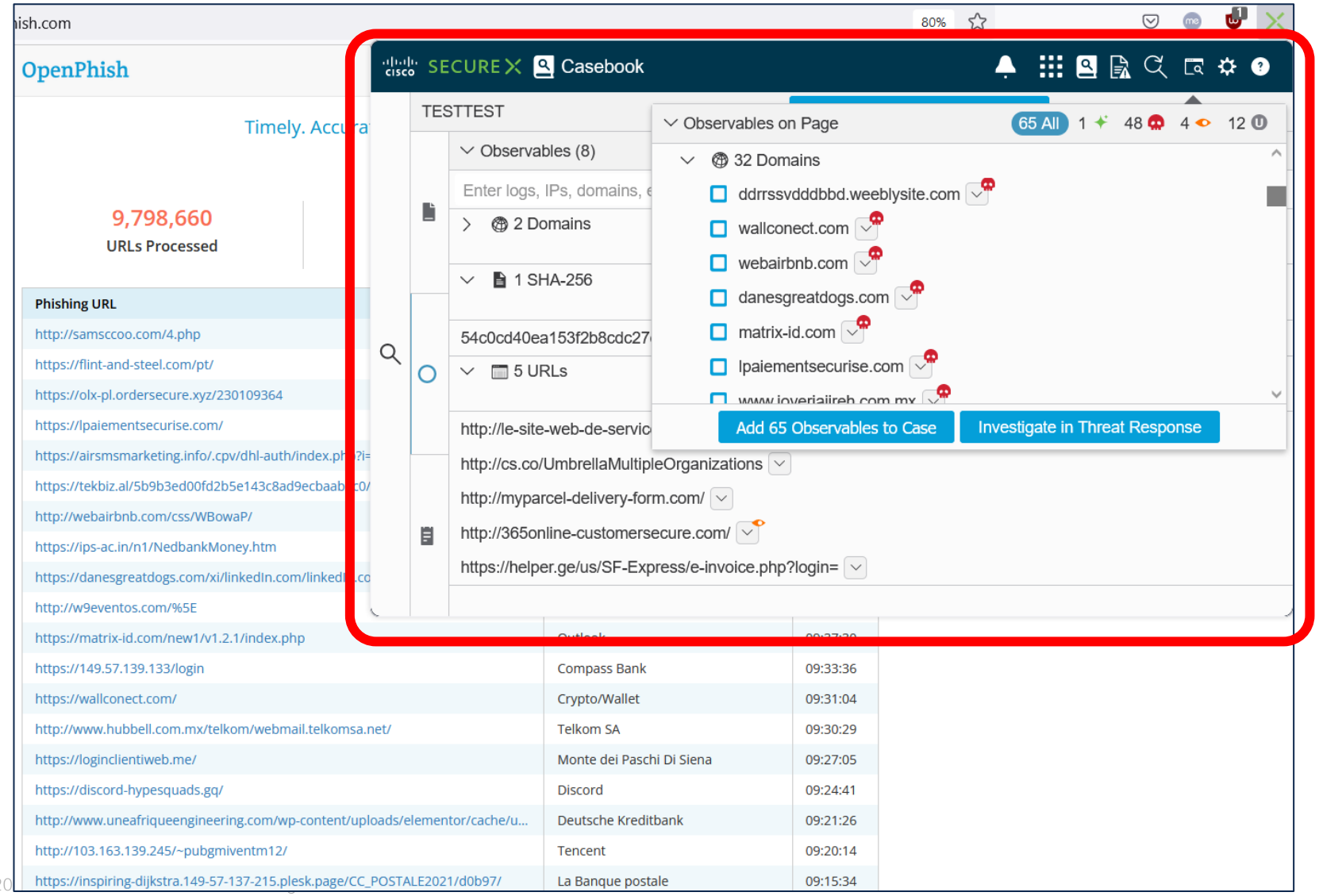


270+ Threat Researchers covering all timezones

SecureX : une plateforme de Threat Hunting

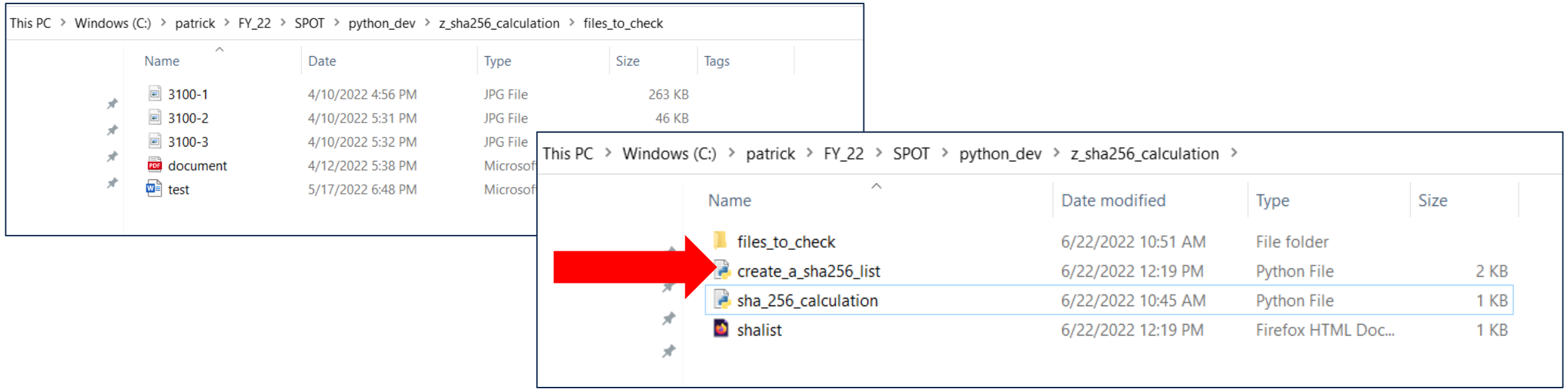


Plugin SecureX pour les navigateurs



Un Rapide Exemple

Je veux vérifier si des fichiers suspects sont malveillants ?



Script Python d'investigation

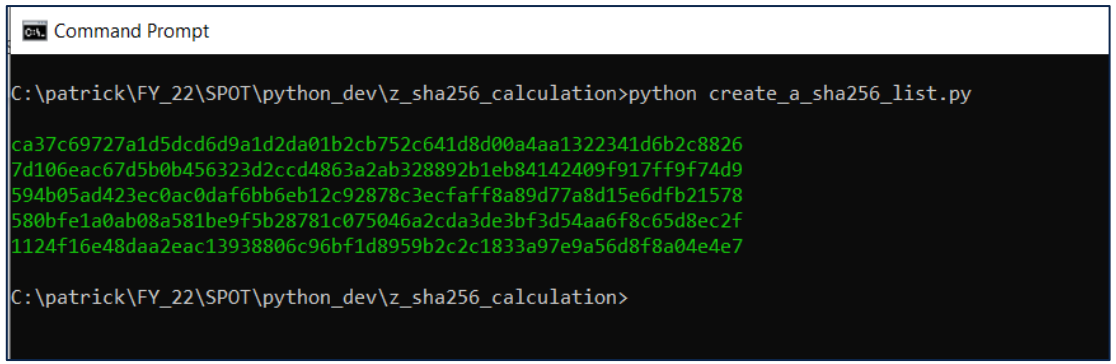
create_a_sha256_list.py

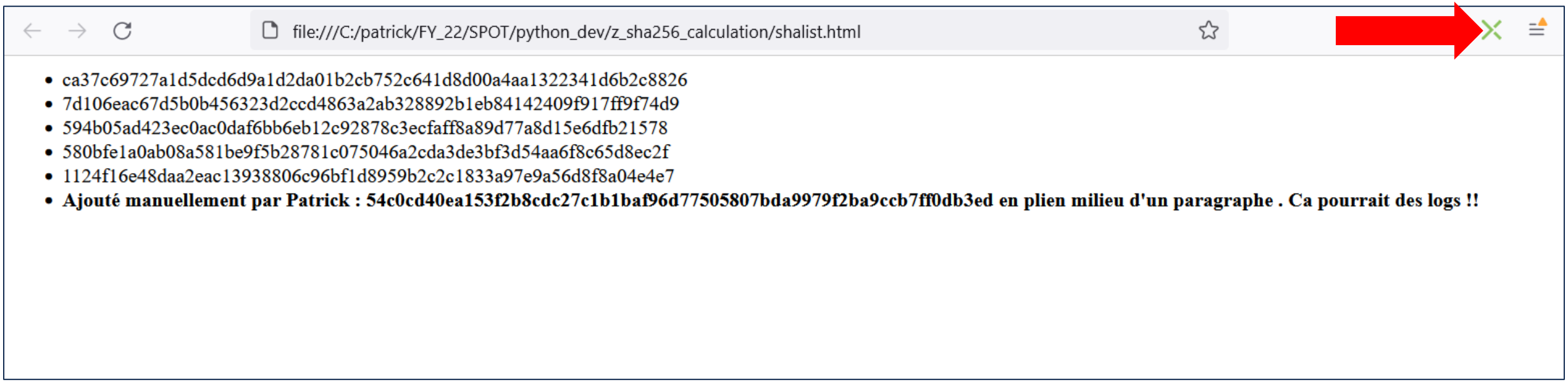
```
3  import hashlib
4
5  def sha256(filename):
6      sha256_hash = hashlib.sha256()
7      filename="./files_to_check/"+filename
8      with open(filename,"rb") as f:
9          # Read and update hash string value in blocks of 4K
10         for byte_block in iter(lambda: f.read(4096),b""):
11             sha256_hash.update(byte_block)
12         resultat=sha256_hash.hexdigest()
13     return(resultat)
14
15 if __name__=='__main__':
16     files =[file for file in os.listdir('./files_to_check')]
17     with open('shalist.html','w') as fichier:
18         fichier.write("<html><body><ul>")
19         print()
20         for file in files:
21             sha=sha256(file)
22             print(green(sha,bold=True))
23             fichier.write(f"<li>{sha}</li>")
24         fichier.write(f"<li><b> Ajout&eacute; manuellement par Patrick :
   54c0cd40ea153f2b8cdc27c1b1baf96d77505807bda9979f2ba9ccb7ff0db3ed en plien milieu d'un paragraphe . Ca pourrait des
   logs !!</></li>")
25         fichier.write("</ul></body></html>")
```

Calcul de sha256

- Parcours de tous les fichiers dans le répertoire
- Calcul de sha256 pour chacun
- Stockage des sha256 dans un fichier html

Script Python d’investigation

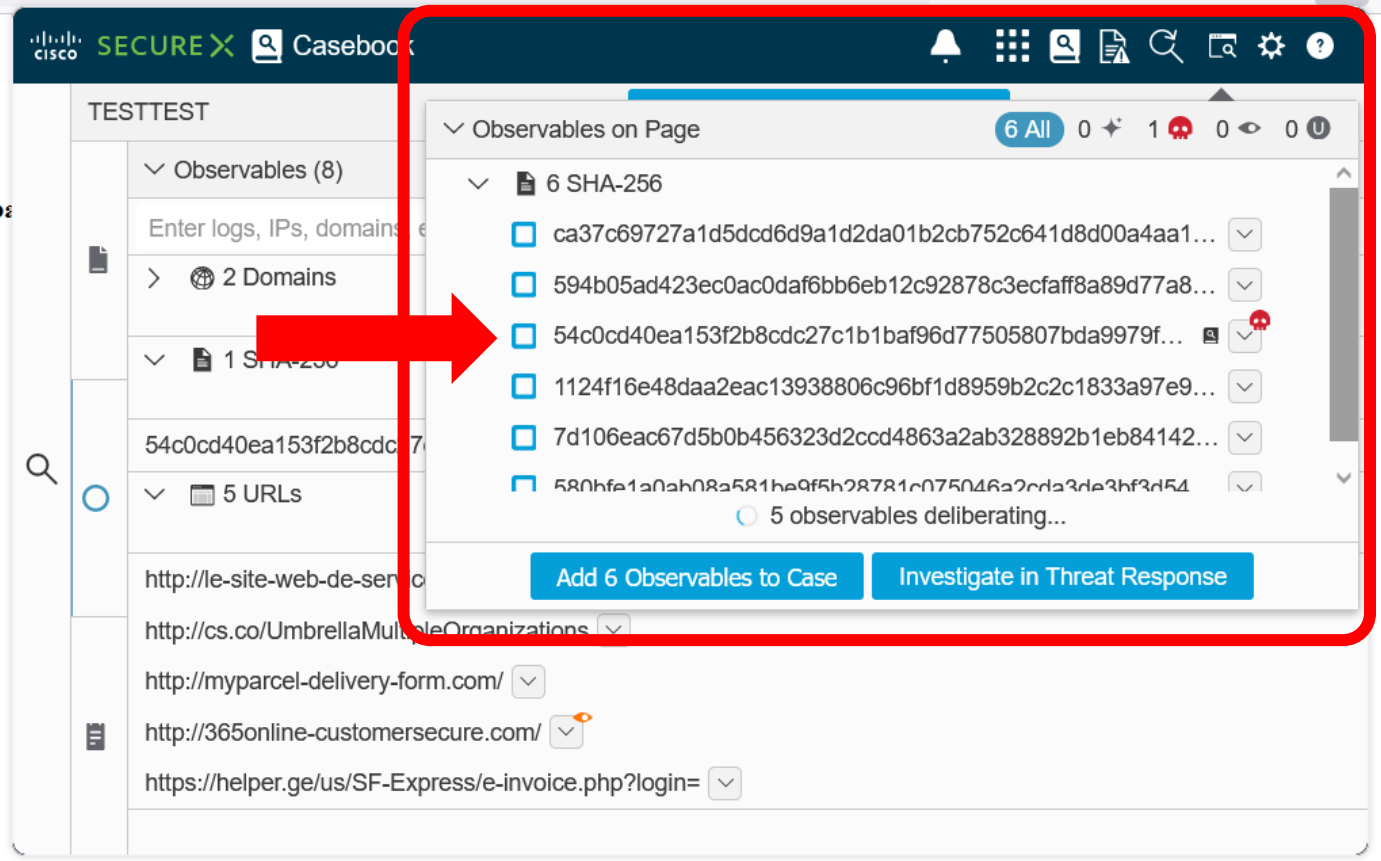




Le plugin SecureX en action

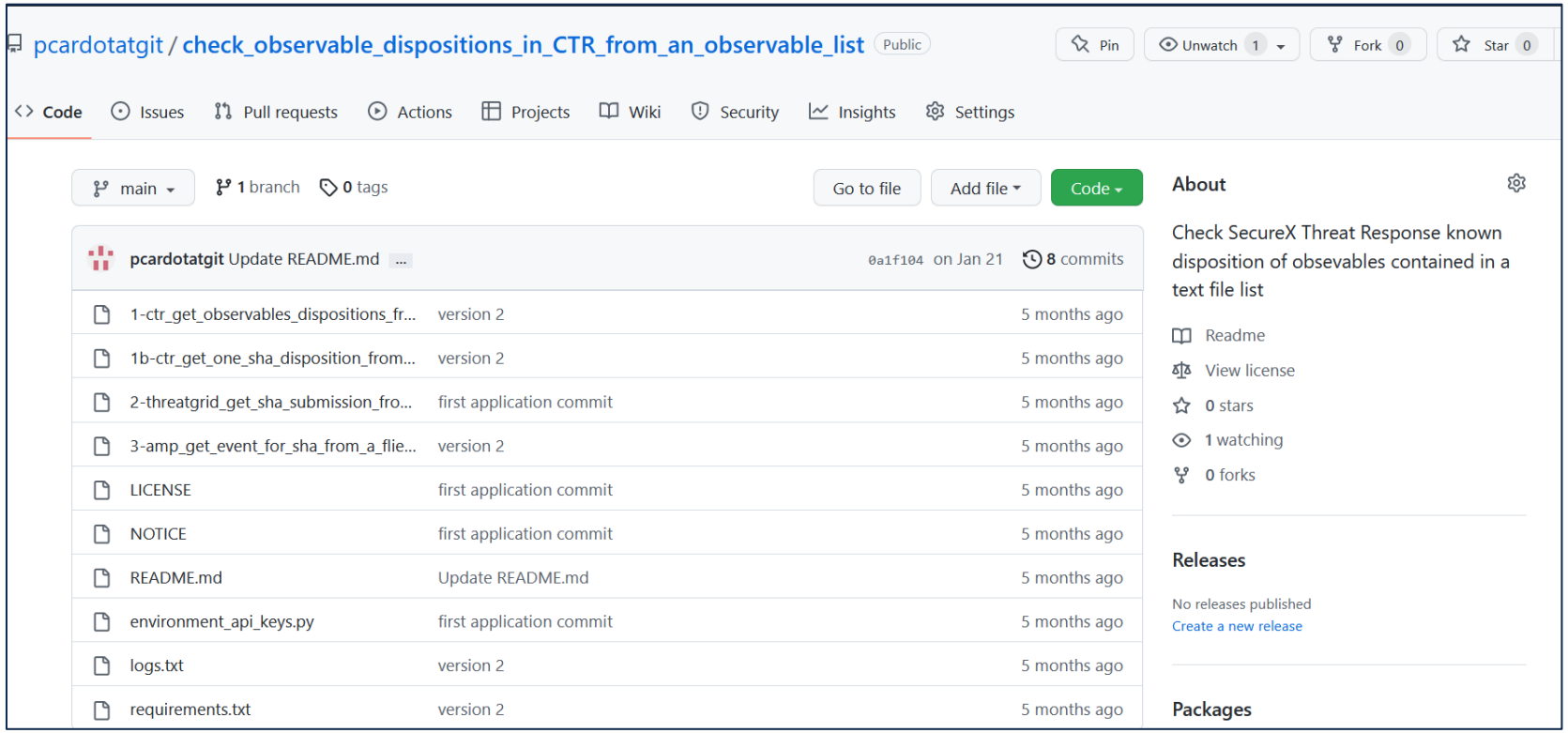
file:///C:/patrick/FY_22/SPOT/python_dev/z_sha256_calculation/shalist.html

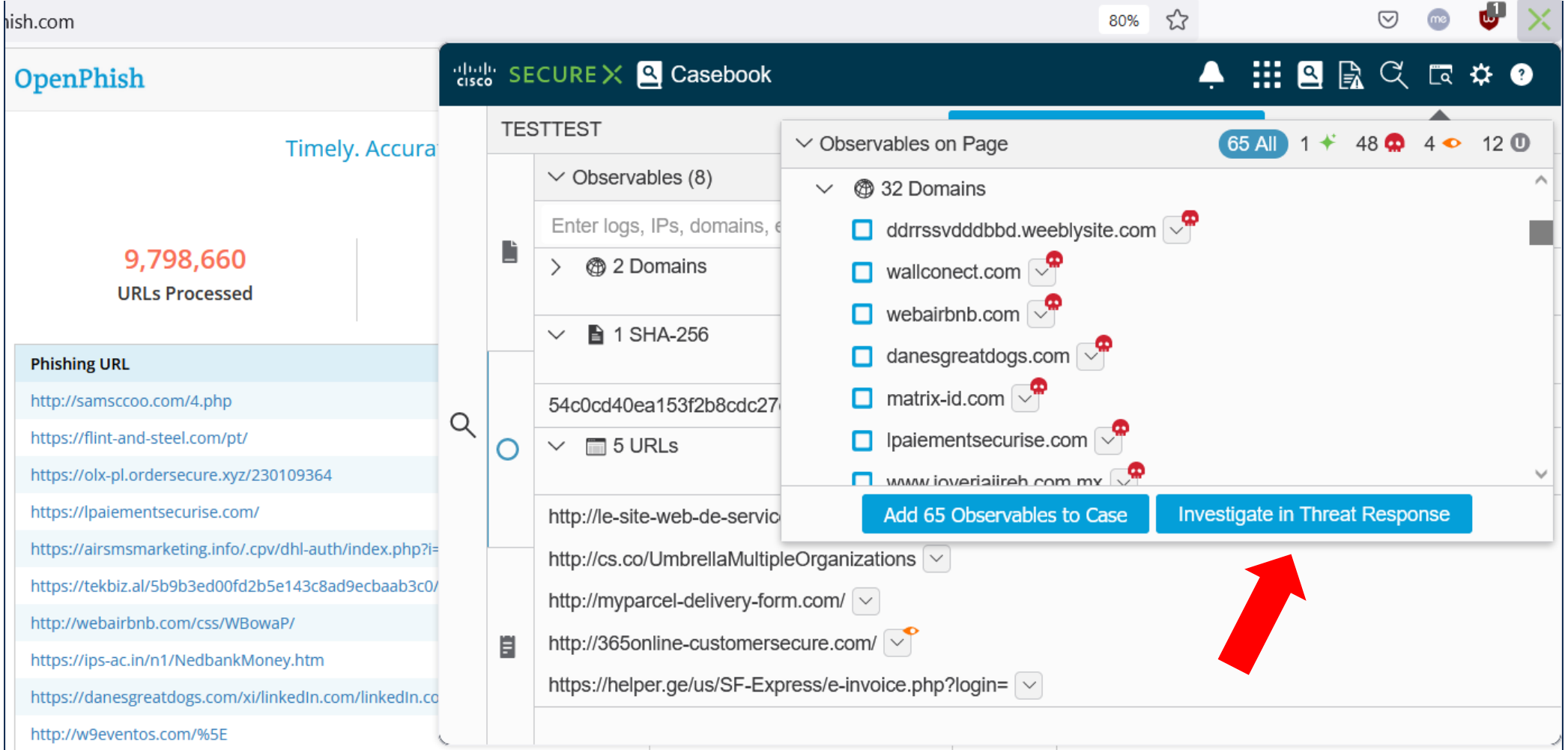
- ca37c69727a1d5dcd6d9a1d2da01b2cb752c641d8d00a4aa1322341d6b2c8826
- 7d106eac67d5b0b456323d2ccd4863a2ab328892b1eb84142409f917ff9f74d9
- 594b05ad423ec0ac0daf6bb6eb12c92878c3ecfaff8a89d77a8d15e6dfb21578
- 580bfe1a0ab08a581be9f5b28781c075046a2cda3de3bf3d54aa6f8c65d8ec2f
- 1124f16e48daa2eac13938806c96bf1d8959b2c2c1833a97e9a56d8f8a04e4e7
- **Ajouté manuellement par Patrick : 54c0cd40ea153f2b8cdc27c1b1baf96d77505807bda9979f2ba**



Investigation de logs de sécurité

- https://github.com/pcardotatgit/check_observable_dispositions_in_CTR_from_an_observable_list




ish.com
80%
OpenPhish
Timely. Accura
9,798,660
URLs Processed
Phishing URL
http://samsccoo.com/4.php
https://flint-and-steel.com/pt/
https://olx-pl.ordersecure.xyz/230109364
https://lpaiementsecurise.com/
https://airsmsmarketing.info/.cpv/dhl-auth/index.php?i=
https://tekbiz.al/5b9b3ed00fd2b5e143c8ad9ecbaab3c0/
http://webairbnb.com/css/WBowaP/
https://ips-ac.in/n1/NedbankMoney.htm
https://danesgreatdogs.com/xi/linkedIn.com/linkedIn.co
http://w9eventos.com/%5E
cisco SECURE X
Casebook
TESTTEST
Observables (8)
Enter logs, IPs, domains,
2 Domains
1 SHA-256
54c0cd40ea153f2b8cdc27
5 URLs
http://le-site-web-de-servic
http://cs.co/UmbrellaMultipleOrganizations
http://myparcel-delivery-form.com/
http://365online-customersecure.com/
https://helper.ge/us/SF-Express/e-invoice.php?login=
Observables on Page
65 All
1
48
4
12
32 Domains
ddrrssvdddbbd.weeblysite.com
wallconect.com
webairbnb.com
danesgreatdogs.com
matrix-id.com
lpaiementsecurise.com
Add 65 Observables to Case
Investigate in Threat Response
https://matrix-id.com/new1/v1.2.1/index.php
Outlook
09:37:30
https://149.57.139.133/login
Compass Bank
09:33:36
https://wallconect.com/
Crypto/Wallet
09:31:04
http://www.hubbell.com.mx/telkom/webmail.telkomsa.net/
Telkom SA
09:30:29
https://loginclientiweb.me/
Monte dei Paschi Di Siena
09:27:05
https://discord-hypesquads.gq/
Discord
09:24:41
http://www.uneafriqueengineering.com/wp-content/uploads/elementor/cache/u...
Deutsche Kreditbank
09:21:26
http://103.163.139.245/~pubgmiventm12/
Tencent
09:20:14
https://inspiring-dijkstra.149-57-137-215.plesk.page/CC_POSTALE2021/d0b97/
La Banque postale
09:15:34

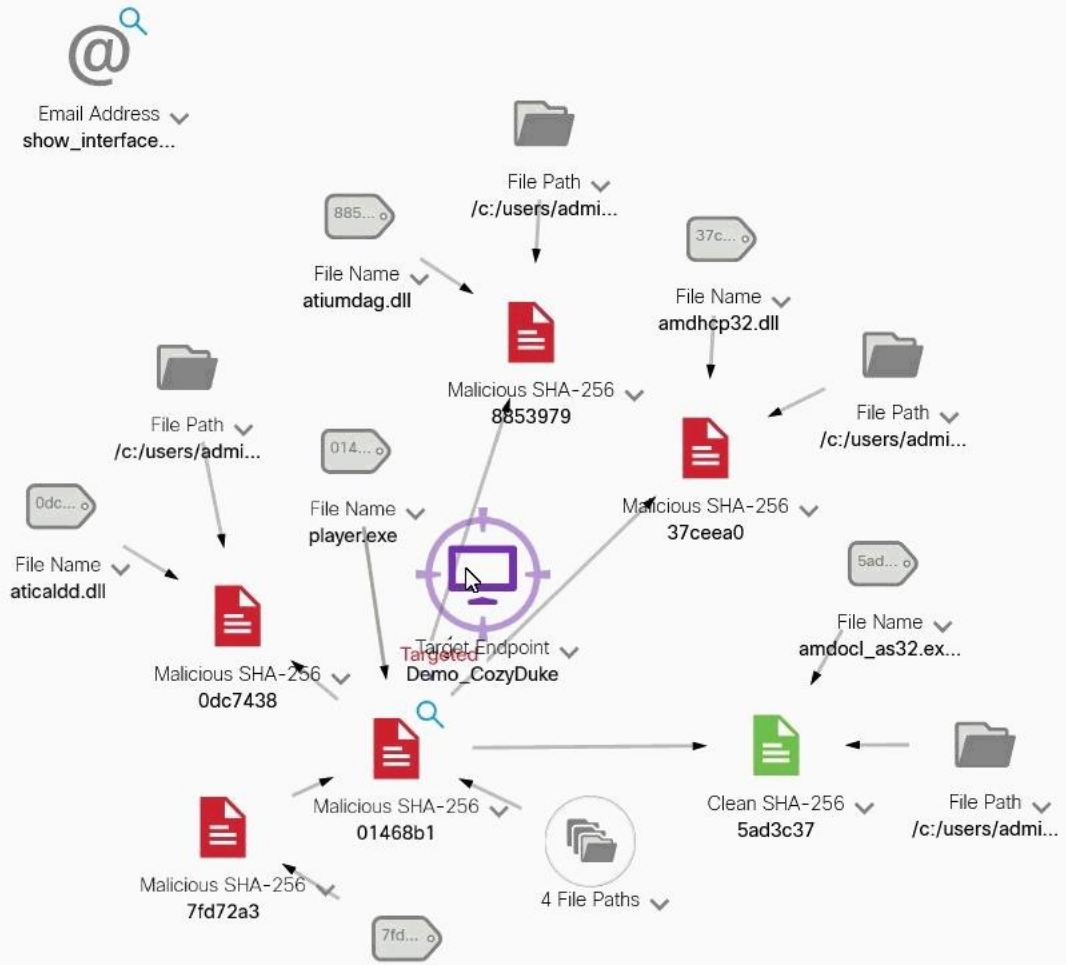
Cisco SecureX | Cisco Threat Response | Query | Orbital

https://visibility.eu.amp.cisco.com/investigate?q=sha256%3A"01468b1d3e089985a4ed255b6594d24863cfd94a647329c631e4f4e52759f8a9"%0Aemail%3A"show_interface_vlan2%40sxo.bot"

Threat Response | Investigate | Snapshots | Incidents | Intelligence | Patrick Cardot

New Investigation

Relations Graph · Dispositions: All · Types: All · Mode: Simplified · Showing 19 of 22 nodes



Casebook

Cisco SecureX | Query | Orbital

https://securex.eu.security.cisco.com

pcardot_SecureX_ALERTS
PAT_SECUREX_BOT
The Targeterd hosts are :
| (0) | Demo_CozyDuke | player.exe |

SECURE X

Dashboard | Integration Modules | Orchestration Beta | Administration

Applications & Integrations
- Applications
- My Integrations
  - AMP for Endpoints — Launch | Links
  - Orbital — Launch | Links
  - SecureX Orchestration — Links
  - SecureX Orchestrator — Links
  - Threat Grid — Launch | Links

ThreatGrid | AMP | patrick

Customize | Timeframe*

Compromises detected | AMP for Endpoints — Last 24 Hours

Critical (0) | High (0) | Medium (0) | Low (1)

Computers Summary | AMP for Endpoints

38 Computers
36 Seen > 7 days ago
1 Need AV Update
3 Out of Date Connectors

MITRE ATT&CK Tactics detected | AMP for Endpoints — Last 30 Days

Submission Source by Result | Threat Grid — Last 30 Days

News

Welcome to SecureX

Maximize your experience by reviewing these key topics:
- About SecureX
- Configure Integration Modules
- Configure Dashboards and Tiles
- Activate Orchestration
- Navigate SecureX
- SecureX Ribbon

SecureX Webinars in November

SecureX Webinars & Training Videos

Join Cisco experts in November for these live sessions: "Put your best foot forward with SecureX"

SECURE X | Casebook

Cases — New Case

Search...

Owned By Me (13)
- Case Nov 12, 2020, 2:59:03 PM — 2 Observables
- Casebook October 23, 2018 12:39 PM — 1 Observable
- Casebook October 3, 2018 11:18 AM — 4 Observables
- Casebook July 24, 2018 9:43 AM — 2 Observables
- Casebook June 22, 2018 11:46 AM — 15 Observables
- Casebook June 22, 2018 9:55 AM — 15 Observables

Case Nov 12, 2020, 2:59:03 PM

Overview

Details
- Title: Case Nov 12, 2020, 2:59:03 PM
- Created: Nov 12, 2020, 2:59:03 PM
- Owner: Patrick Cardot
- Summary: Add...

Observables (2) — 0 1 0 1

Enter logs, IPs, domains, etc.

1 Email — 0 0 0 1

show_interface_vlan2@sxo.bot

1 SHA-256 — 0 1 0 0

01468b1d3e089985a4ed255b6594d24863cfd94a647329c631e4f4e...

Link to Incident

01468b1d3e089985a4ed255b659...
Malicious SHA-256

Investigate in Threat Response
Create Judgement

AMP for Endpoints
- File trajectory
- Search for this SHA256
- Add SHA256 to custom detections ...
- Add SHA256 to custom detections t...

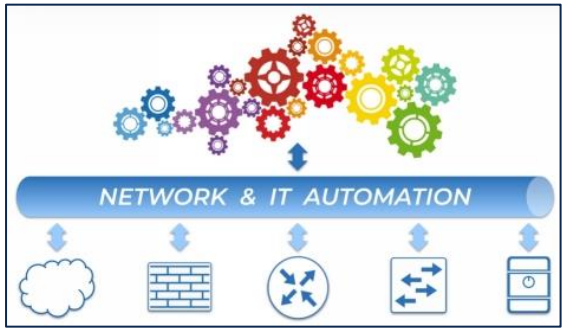
SecureX Orchestration
- SSH_to_ASA_and_do_show_interf...
- Which hosts are Targeted by this sh...
- Webex_Team_Send_Alert_to_SEC...
- PAT_ZTARGET
- pcardot_TEST
- Take Forensic Snapshot and Isolate

Success
Which hosts are Targeted by this sha256

Type here to search

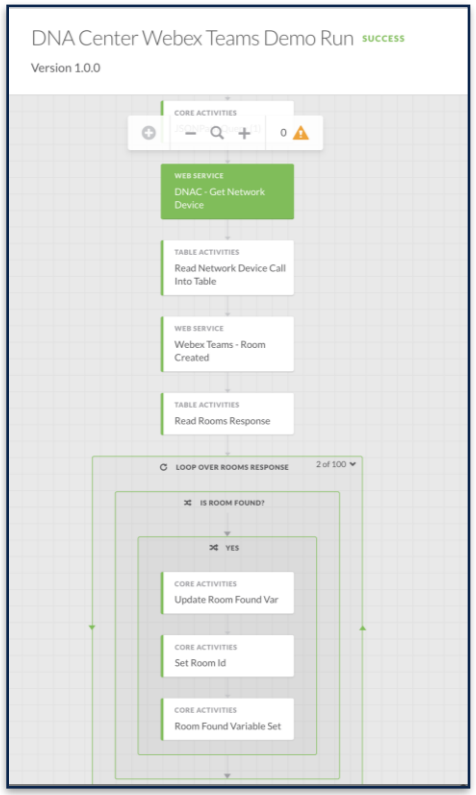
18:20
13/11/2020

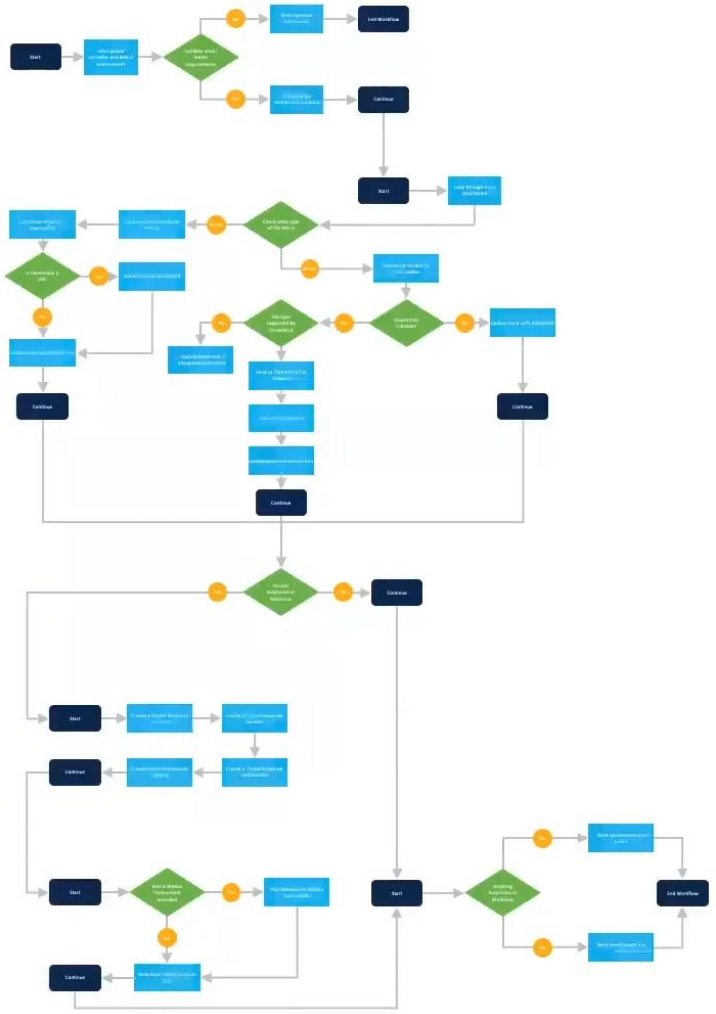
SecureX : Security ToolBox

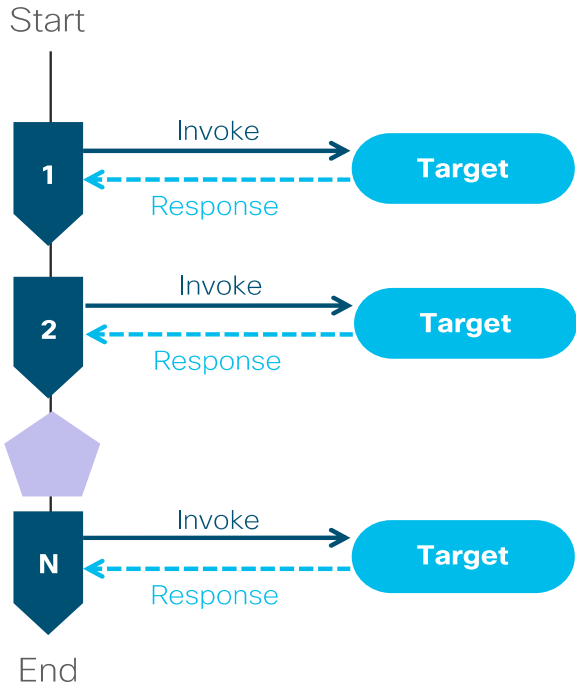


SecureX : Security Orchestration

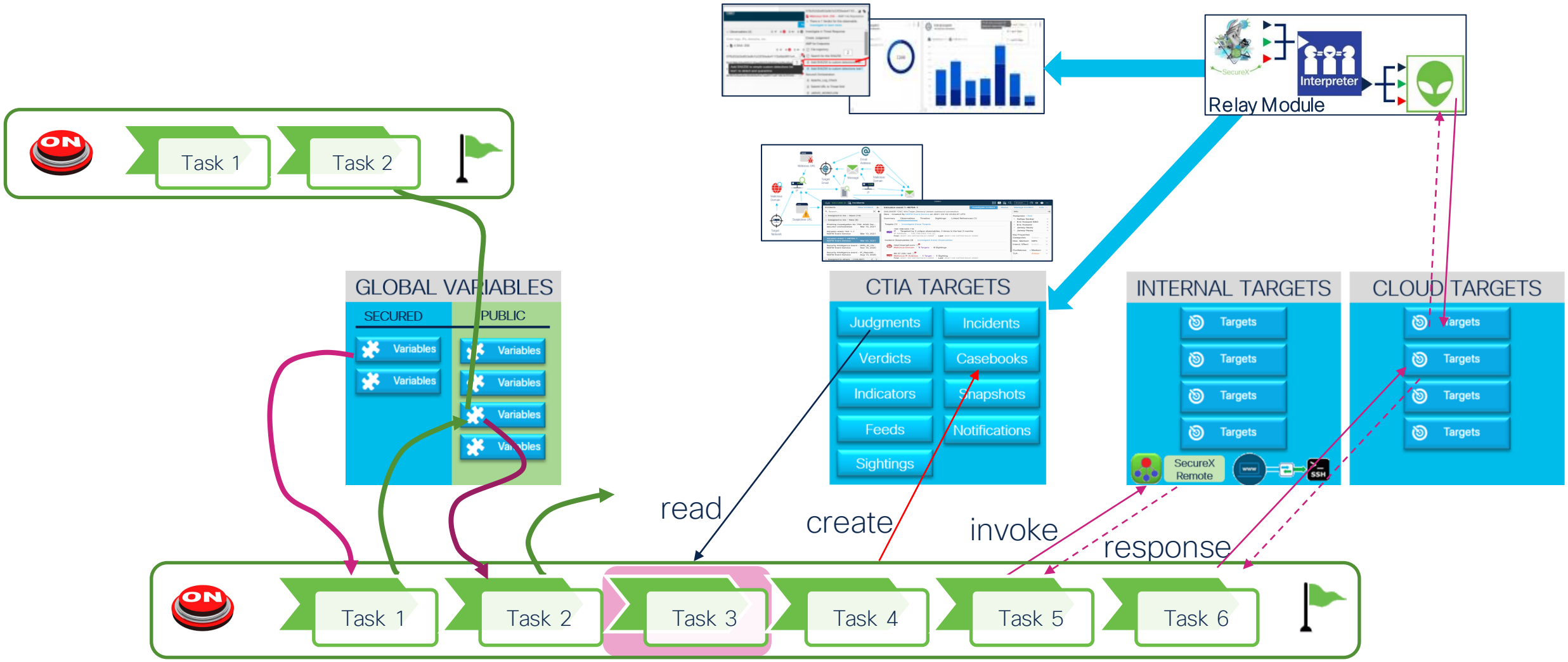
Workflows d’automatisation





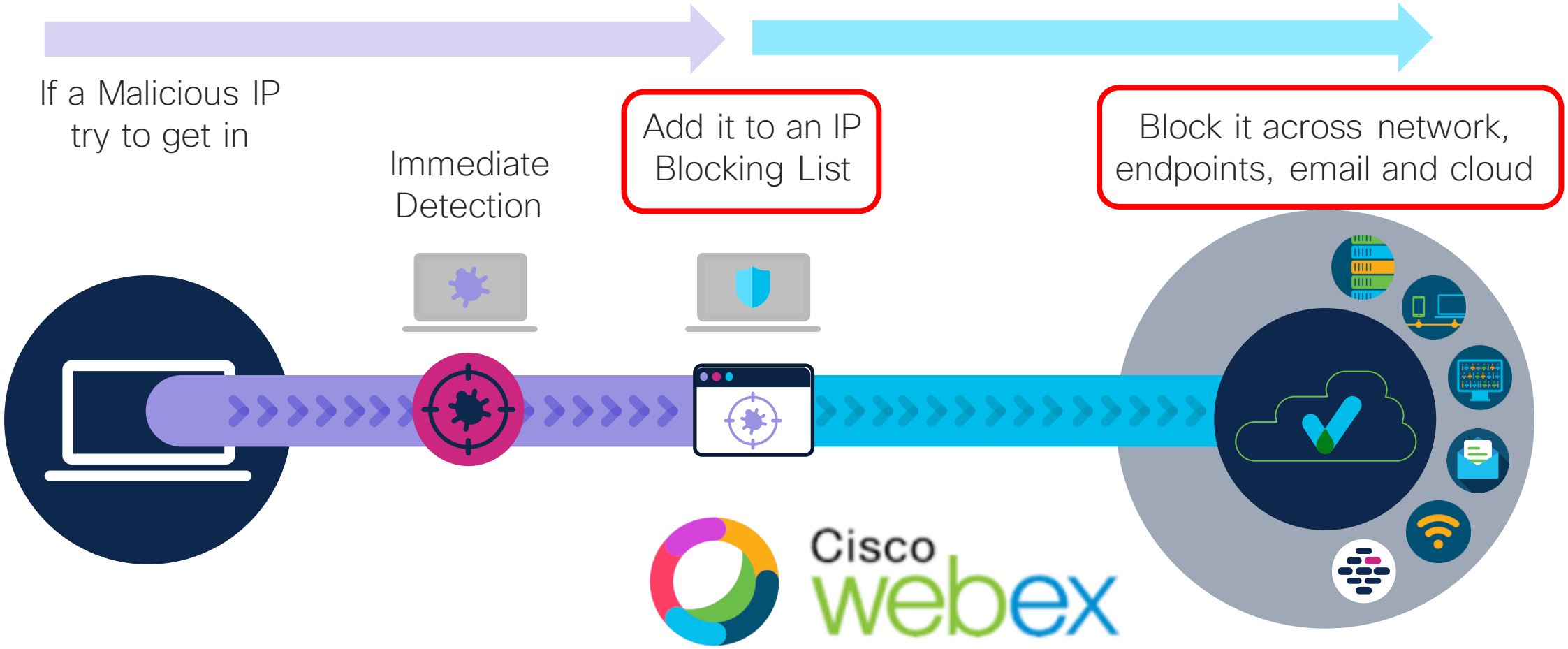


J’ai besoin d’une application de sécurité !

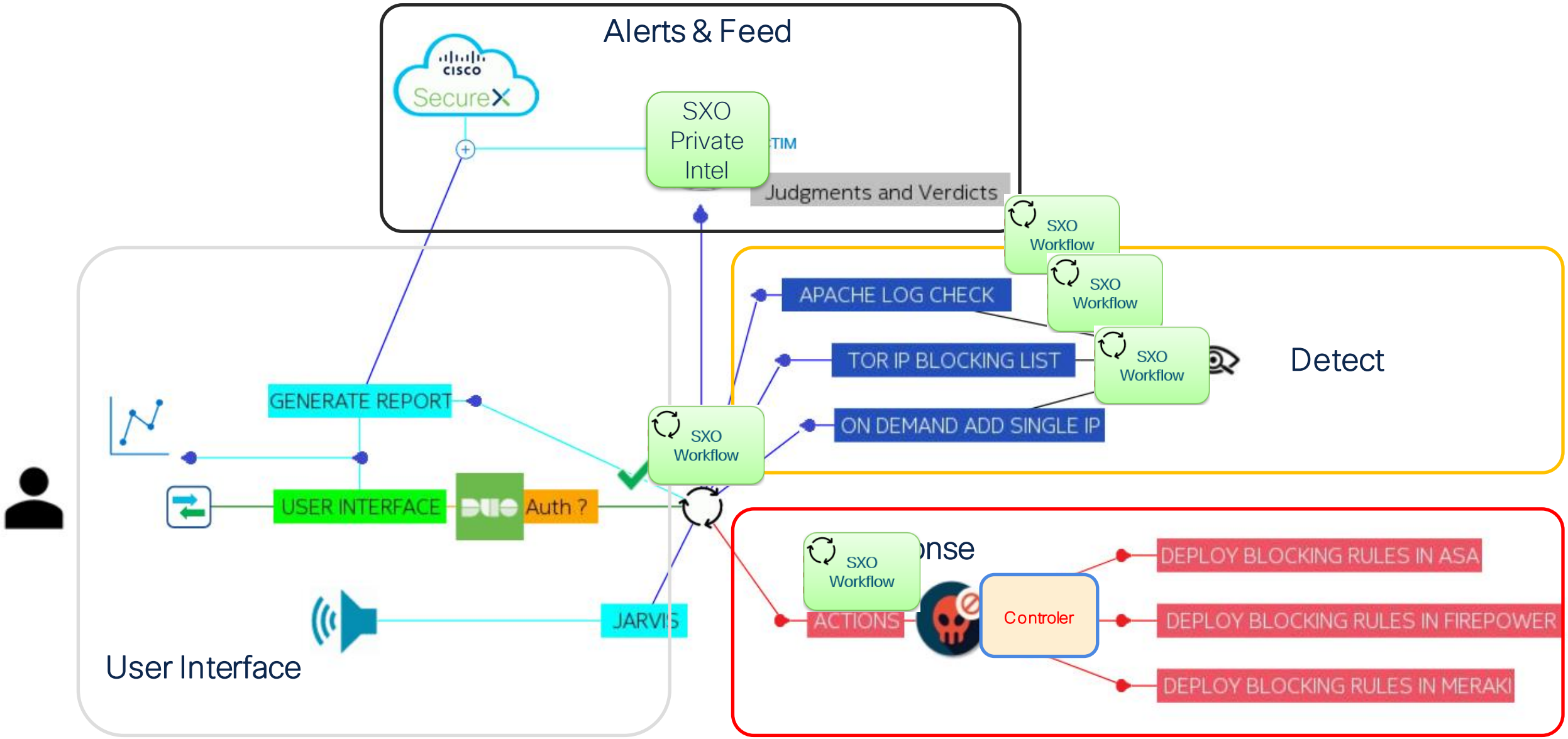


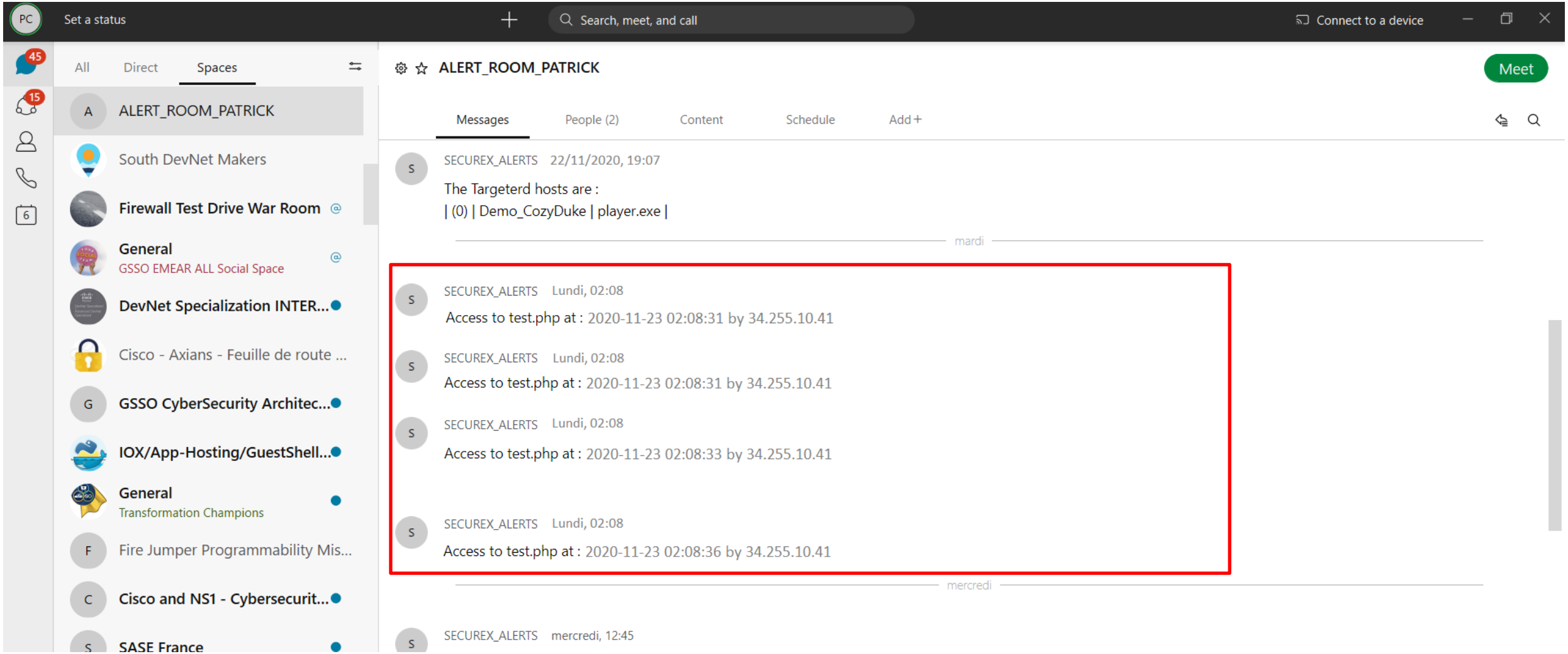
Quelques exemples concrets

Création de Feeds privées



Security Application

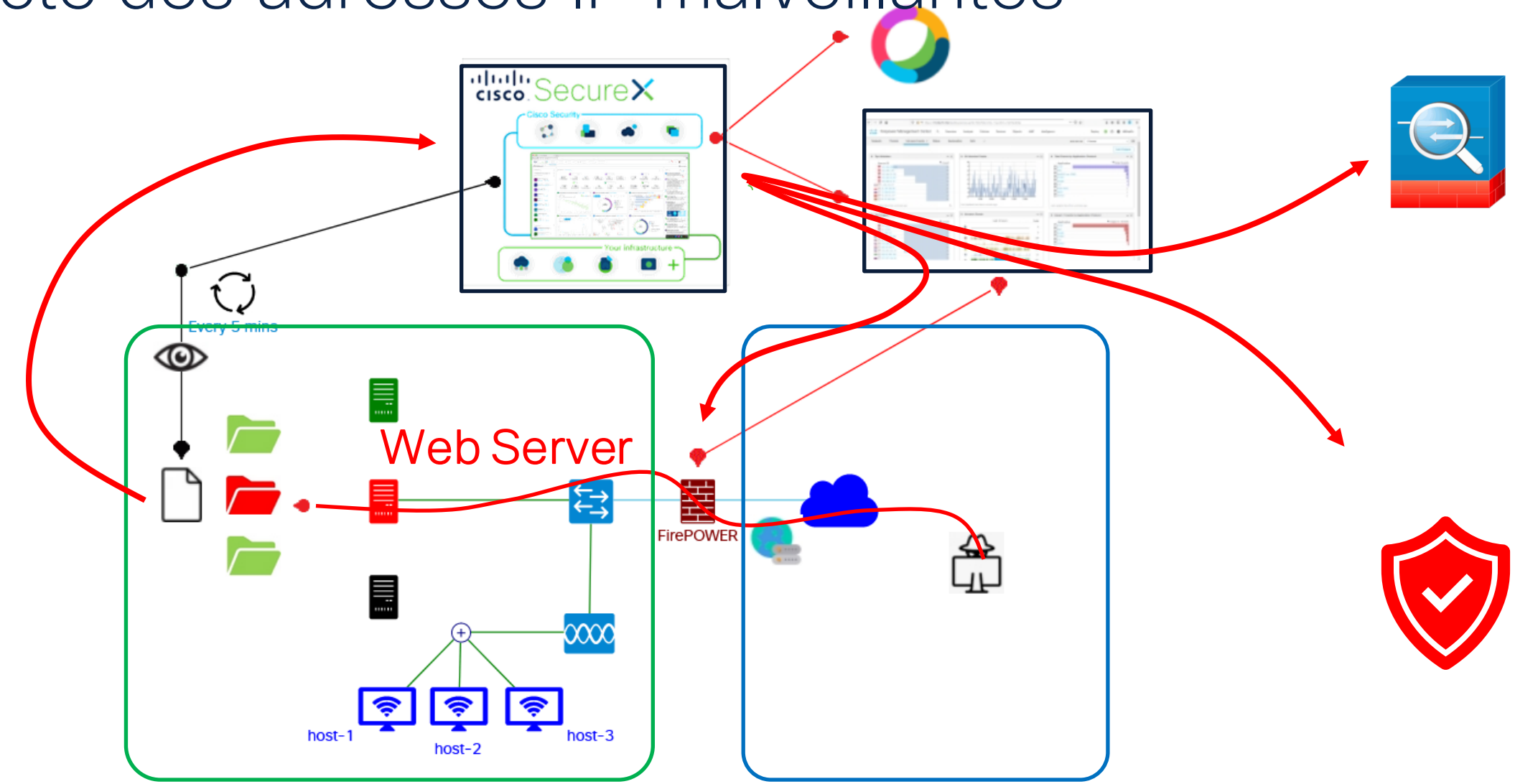




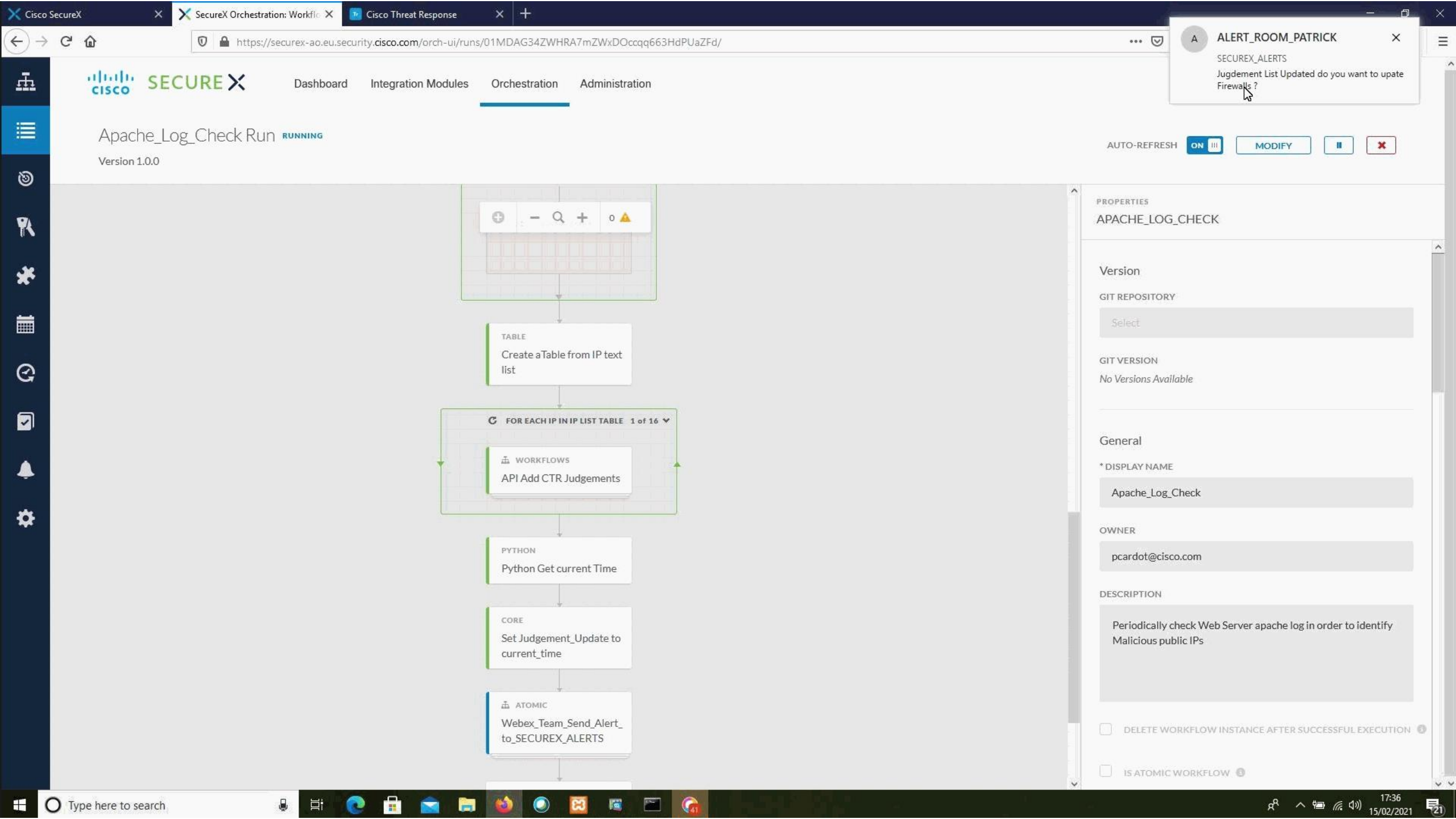
access.log

```
1556 185.239.242.162 - - [24/Jan/2021:10:07:46 +0100] "GET / HTTP/1.1" 200 209 "-" "Linux Gnu (cow)"
1557 198.98.61.98 - - [24/Jan/2021:10:40:53 +0100] "POST /boaform/admin/formLogin HTTP/1.1" 404 496
     "http://86.242.68.188:80/admin/login.asp" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0"
1558 75.32.238.202 - - [24/Jan/2021:11:38:10 +0100] "GET / HTTP/1.1" 200 190 "-" "-"
1559 83.97.20.30 - - [24/Jan/2021:12:30:54 +0100] "GET / HTTP/1.0" 200 209 "-" "-"
1560 88.73.96.161 - - [24/Jan/2021:13:04:37 +0100] "GET //proc/kcore HTTP/1.1" 404 459 "-" "Python-urllib/3.9"
1561 182.58.207.162 - - [24/Jan/2021:13:19:56 +0100] "GET /boaform/admin/formLogin?username=ec8&psd=ec8 HTTP/1.0" 404 458 "-" "-"
1562 188.131.172.48 - - [24/Jan/2021:13:33:14 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=456&server=1
     HTTP/1.1" 200 12750 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1563 188.131.172.48 - - [24/Jan/2021:13:33:21 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=root1&server=1
     HTTP/1.1" 200 12750 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1564 188.131.172.48 - - [24/Jan/2021:13:33:29 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=root12345&server=1
     HTTP/1.1" 200 12750 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1565 188.131.172.48 - - [24/Jan/2021:13:33:33 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=root@123&server=1
     HTTP/1.1" 200 12750 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1566 188.131.172.48 - - [24/Jan/2021:13:33:34 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=admin@123&server=1
     HTTP/1.1" 200 12749 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1567 188.131.172.48 - - [24/Jan/2021:13:33:35 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=p1O5oemS76C&server=1
     HTTP/1.1" 200 12749 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1568 188.131.172.48 - - [24/Jan/2021:13:33:37 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=Abcd1234&server=1
     HTTP/1.1" 200 12749 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1569 188.131.172.48 - - [24/Jan/2021:13:33:41 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=admin123456&server=1
     HTTP/1.1" 200 12749 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1570 188.131.172.48 - - [24/Jan/2021:13:33:45 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=lenovo&server=1
     HTTP/1.1" 200 12749 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1571 188.131.172.48 - - [24/Jan/2021:13:33:47 +0100] "GET /phpmyadmin/index.php?pma_username=root&pma_password=q1w2e3&server=1
     HTTP/1.1" 200 12749 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0"
1572 181.143.101.194 - - [24/Jan/2021:14:12:32 +0100] "POST /cgi-bin/ViewLog.asp HTTP/1.1" 404 492 "-" "Hello, World"
```

Collecte des adresses IP malveillantes



Démo


Cisco SecureX
SecureX Orchestration: Workfl
Cisco Threat Response
https://securex-ao.eu.security.cisco.com/orch-ui/runs/01MDAG34ZWHRA7mZWxDOccqq663HdPUaZFd/
ALERT_ROOM_PATRICK
SECUREX_ALERTS
Jugdement List Updated do you want to upate Firewalls ?
SECURE X
Dashboard
Integration Modules
Orchestration
Administration
Apache_Log_Check Run RUNNING
Version 1.0.0
AUTO-REFRESH
ON
MODIFY
TABLE
Create aTable from IP text list
FOR EACH IP IN IP LIST TABLE 1 of 16
WORKFLOWS
API Add CTR Judgements
PYTHON
Python Get current Time
CORE
Set Judgement_Update to current_time
ATOMIC
Webex_Team_Send_Alert_ to_SECUREX_ALERTS
PROPERTIES
APACHE_LOG_CHECK
Version
GIT REPOSITORY
Select
GIT VERSION
No Versions Available
General
* DISPLAY NAME
Apache_Log_Check
OWNER
pcardot@cisco.com
DESCRIPTION
Periodically check Web Server apache log in order to identify Malicious public IPs
DELETE WORKFLOW INSTANCE AFTER SUCCESSFUL EXECUTION
IS ATOMIC WORKFLOW
Type here to search
17:36
15/02/2021

Cisco SecureX | SecureX Orchestration: Workflo | Cisco Threat Response

https://visibility.eu.amp.cisco.com/intelligence/judgements/private

Threat Response | Investigate | Snapshots | Incidents | Intelligence | Patrick Cardot

Intelligence > Private Judgements

- Judgements
- Indicators
- Sightings
- Feeds

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

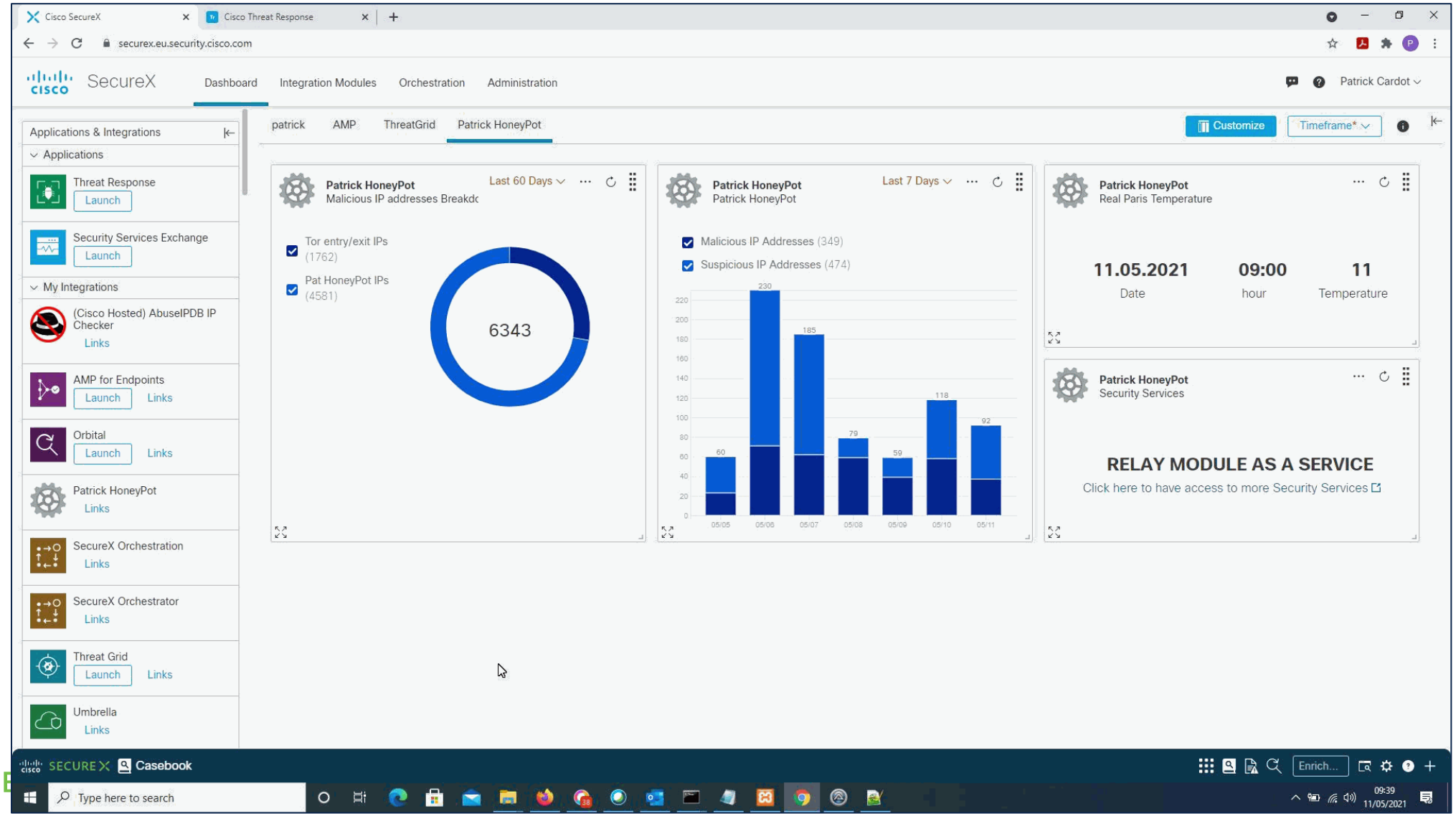
Sources: Private

Judgements

Observable	Disposition	Reason	Source	Severity	Confidence	TLP	Expiration	Actions
IP 45.77.247.72	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 139.224.72.224	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 39.86.62.165	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 125.141.5.251	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 186.179.112.254	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 81.71.120.65	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 123.52.87.40	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 78.179.218.141	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 54.83.23.109	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 192.241.219.140	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 222.186.136.150	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 68.197.33.124	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 128.199.43.195	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...
IP 211.247.5.96	Malicious		Patrick HoneyPot	Medium	Medium	red	in 7 days	...

Casebook

Besoin d'un dashboard ?



Cisco SecureX | Cisco Threat Response

securex.eu.security.cisco.com

SecureX

Dashboard | Integration Modules | Orchestration | Administration

Patrick Cardot

Applications & Integrations

Applications

- Threat Response — Launch
- Security Services Exchange — Launch

My Integrations

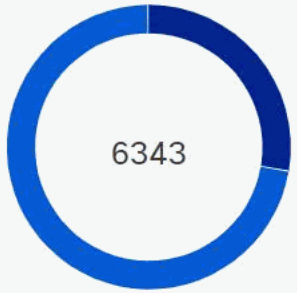
- (Cisco Hosted) AbuseIPDB IP Checker — Links
- AMP for Endpoints — Launch | Links
- Orbital — Launch | Links
- Patrick HoneyPot — Links
- SecureX Orchestration — Links
- SecureX Orchestrator — Links
- Threat Grid — Launch | Links
- Umbrella — Links

patrick | AMP | ThreatGrid | Patrick HoneyPot

Customize | Timeframe*

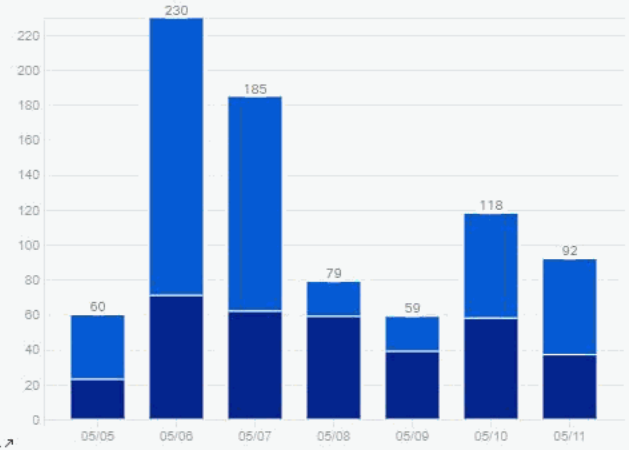
Patrick HoneyPot
Malicious IP addresses Breakdc
Last 60 Days

- Tor entry/exit IPs (1762)
- Pat HoneyPot IPs (4581)



Patrick HoneyPot
Patrick HoneyPot
Last 7 Days

- Malicious IP Addresses (349)
- Suspicious IP Addresses (474)



Patrick HoneyPot
Real Paris Temperature

11.05.2021	09:00	11
Date	hour	Temperature

Patrick HoneyPot
Security Services

RELAY MODULE AS A SERVICE

Click here to have access to more Security Services

SECURE X | Casebook | Enrich...

Type here to search

09:39
11/05/2021

Cisco SecureX | localhost:6060/focus/focus.php? | Cisco Threat Response

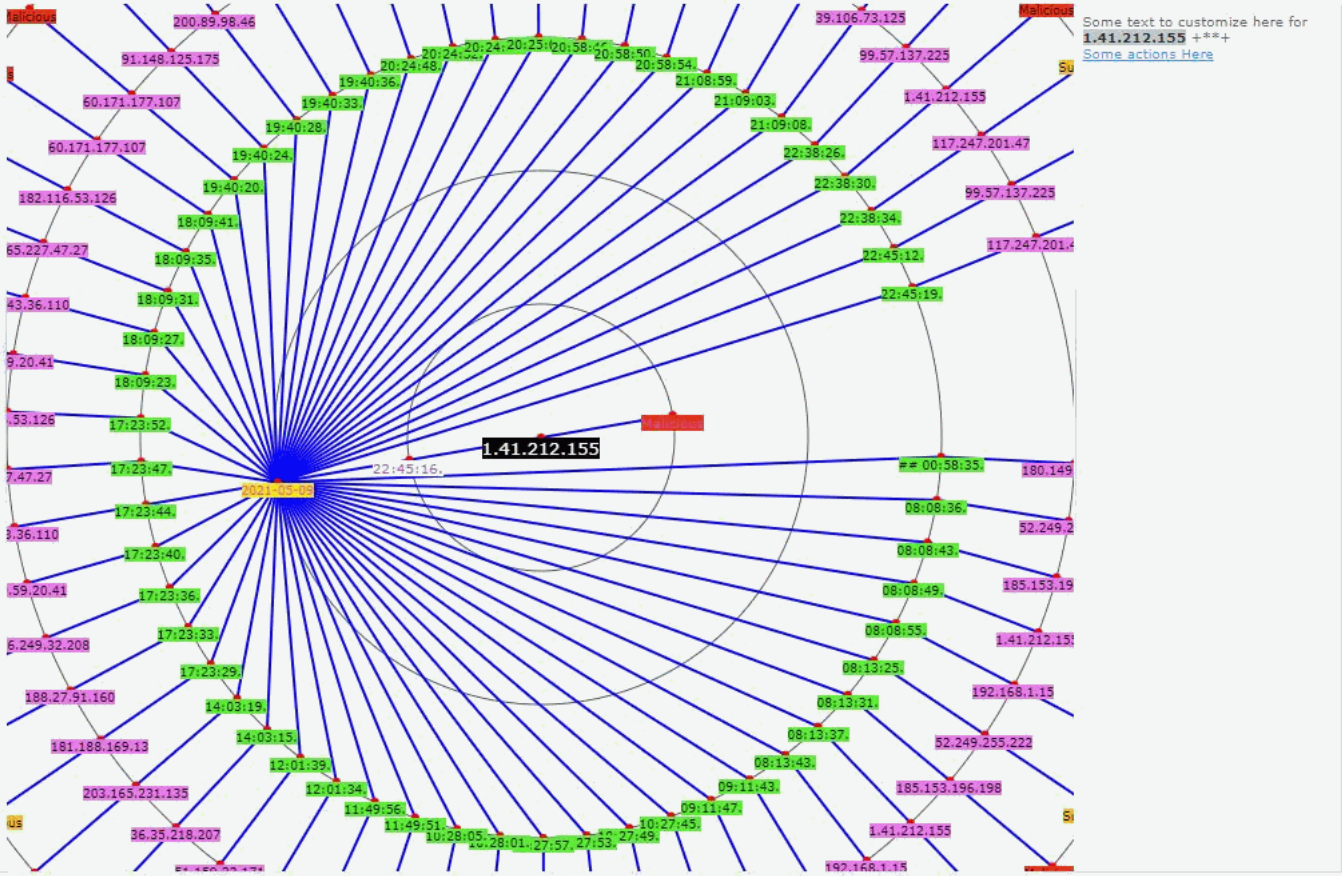
localhost:6060/focus/focus.php?date=2021-05-09

focus on [ ] back

Clickable Relation Graph

Click on objects in order to focus on them

Some actions Here



Some text to customize here for **1.41.212.155** +**+

Some actions Here

1.41.212.155

Malicious IP Address - Private Intelligence

There are 3 Verdicts for this observable.

Investigate to learn more.

Webex_Team_Send_Alert_to_SECUREX_ALE...

Copy-Apache_Log_Check

Copy-Pat_Talk_To_SecureX

API_TRIGGERED_TEST

PAT_IP_TO_GEOLOC

Lookup this IP on Talos Intelligence

Talos Intelligence

Search for this IP

Threat Grid

Browse 1.41.212.155

Search 1.41.212.155

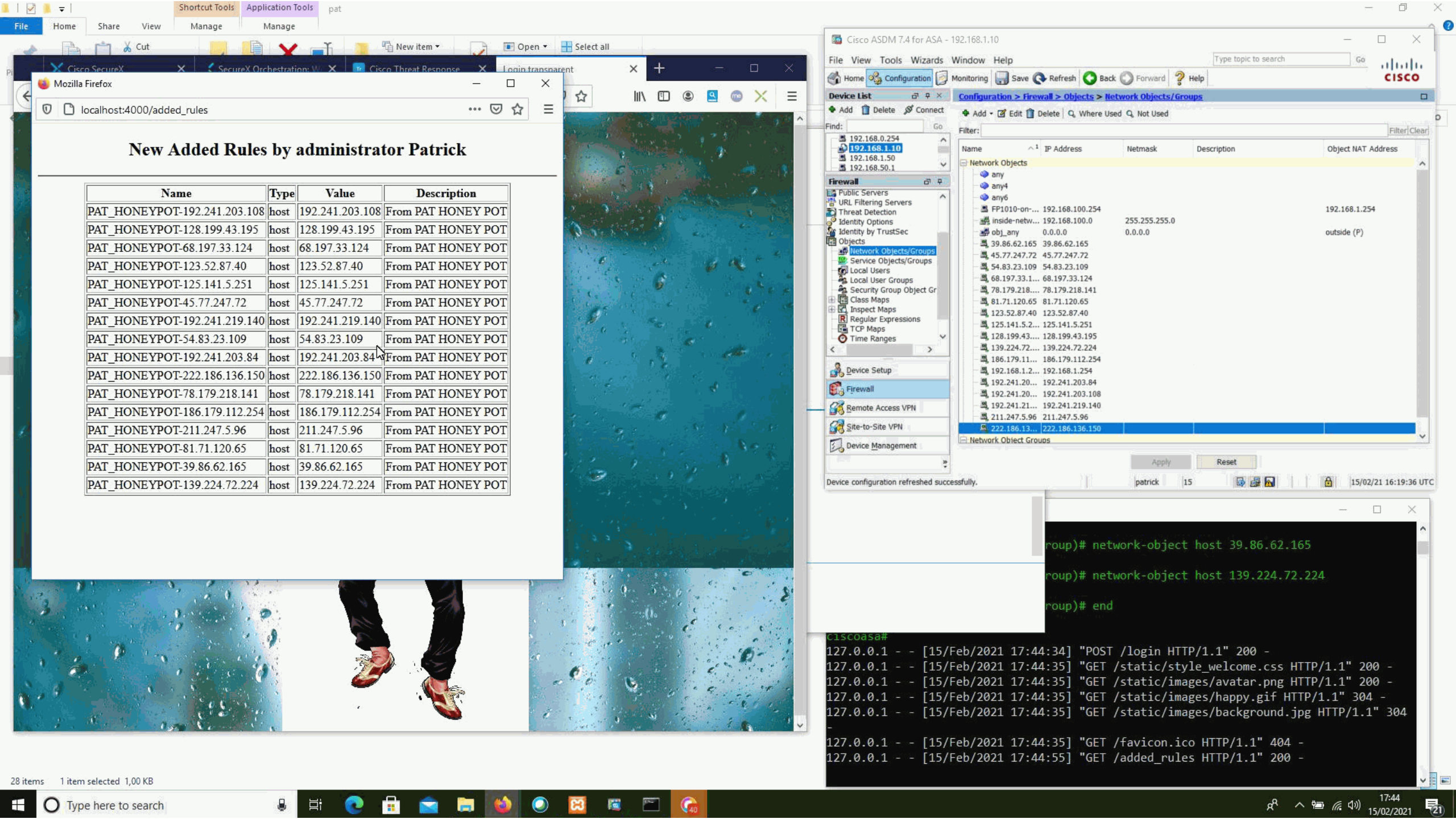
Umbrella

IP view for 1.41.212.155

Type here to search

09:41

11/05/2021


Mozilla Firefox
localhost:4000/added_rules
New Added Rules by administrator Patrick
Name | Type | Value | Description
PAT_HONEYPOT-192.241.203.108 | host | 192.241.203.108 | From PAT HONEY POT
PAT_HONEYPOT-128.199.43.195 | host | 128.199.43.195 | From PAT HONEY POT
PAT_HONEYPOT-68.197.33.124 | host | 68.197.33.124 | From PAT HONEY POT
PAT_HONEYPOT-123.52.87.40 | host | 123.52.87.40 | From PAT HONEY POT
PAT_HONEYPOT-125.141.5.251 | host | 125.141.5.251 | From PAT HONEY POT
PAT_HONEYPOT-45.77.247.72 | host | 45.77.247.72 | From PAT HONEY POT
PAT_HONEYPOT-192.241.219.140 | host | 192.241.219.140 | From PAT HONEY POT
PAT_HONEYPOT-54.83.23.109 | host | 54.83.23.109 | From PAT HONEY POT
PAT_HONEYPOT-192.241.203.84 | host | 192.241.203.84 | From PAT HONEY POT
PAT_HONEYPOT-222.186.136.150 | host | 222.186.136.150 | From PAT HONEY POT
PAT_HONEYPOT-78.179.218.141 | host | 78.179.218.141 | From PAT HONEY POT
PAT_HONEYPOT-186.179.112.254 | host | 186.179.112.254 | From PAT HONEY POT
PAT_HONEYPOT-211.247.5.96 | host | 211.247.5.96 | From PAT HONEY POT
PAT_HONEYPOT-81.71.120.65 | host | 81.71.120.65 | From PAT HONEY POT
PAT_HONEYPOT-39.86.62.165 | host | 39.86.62.165 | From PAT HONEY POT
PAT_HONEYPOT-139.224.72.224 | host | 139.224.72.224 | From PAT HONEY POT
Cisco ASDM 7.4 for ASA - 192.168.1.10
Configuration > Firewall > Objects > Network Objects/Groups
Device configuration refreshed successfully.
roup)# network-object host 39.86.62.165
roup)# network-object host 139.224.72.224
roup)# end
ciscoasa#
127.0.0.1 - - [15/Feb/2021 17:44:34] "POST /login HTTP/1.1" 200 -
127.0.0.1 - - [15/Feb/2021 17:44:35] "GET /static/style_welcome.css HTTP/1.1" 200 -
127.0.0.1 - - [15/Feb/2021 17:44:35] "GET /static/images/avatar.png HTTP/1.1" 200 -
127.0.0.1 - - [15/Feb/2021 17:44:35] "GET /static/images/happy.gif HTTP/1.1" 304 -
127.0.0.1 - - [15/Feb/2021 17:44:35] "GET /static/images/background.jpg HTTP/1.1" 304 -
127.0.0.1 - - [15/Feb/2021 17:44:35] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [15/Feb/2021 17:44:55] "GET /added_rules HTTP/1.1" 200 -

Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
RADIUS Server Group
Route Map
Security Group Tag
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set

Network

Add Network | Filter

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	::/0	Host	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	::ffff:0.0.0.0/96	Network	
IPv6-Link-Local	fe80::/10	Network	
IPv6-Private-Unique-Local-Addresses	fc00::/7	Network	
IPv6-to-IPv4-Relay-Anycast	192.88.99.0/24	Network	

Displaying 1 - 14 of 14 rows Page 1 of 1

How To

Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
RADIUS Server Group
Route Map
Security Group Tag
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set

Network

Add Network | Filter

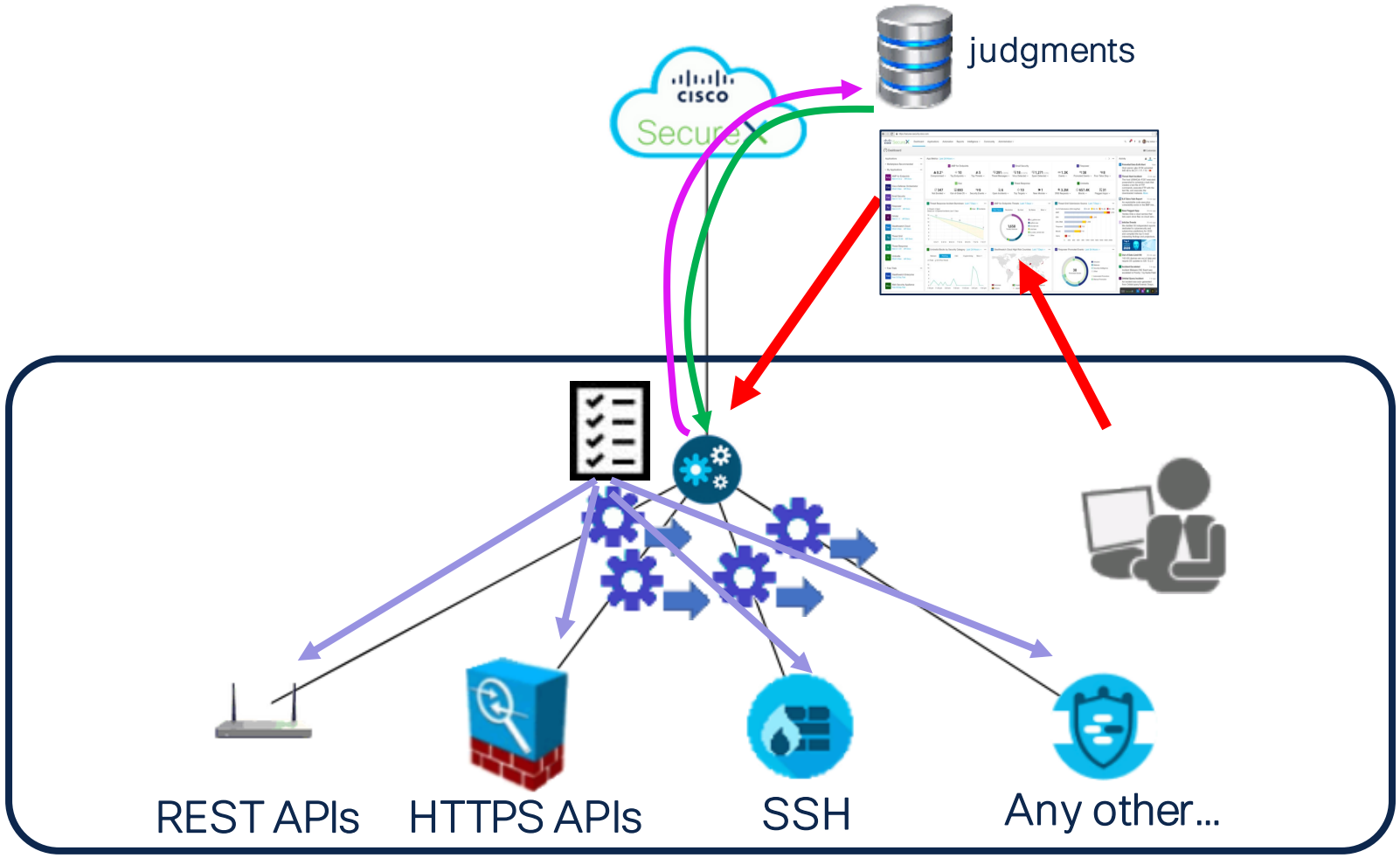
A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Domain	Value	Type	Default Domain	Description	Override
any		0.0.0.0/0 ::/0		Group		
any-ipv4		0.0.0.0/0		Network		
any-ipv6		::/0		Host		
IPv4-Benchmark-Tests		198.18.0.0/15		Network		
IPv4-Link-Local		169.254.0.0/16		Network		
IPv4-Multicast		224.0.0.0/4		Network		
IPv4-Private-10.0.0.0-8		10.0.0.0/8		Network		
IPv4-Private-172.16.0.0-12		172.16.0.0/12		Network		
IPv4-Private-192.168.0.0-16		192.168.0.0/16		Network		
IPv4-Private-All-RFC1918		10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		Group		
IPv6-IPv4-Mapped		::ffff:0.0.0.0/96		Network		
IPv6-Link-Local		fe80::/10		Network		
IPv6-Private-Unique-Local-Addresses		fc00::/7		Network		
IPv6-to-IPv4-Relay-Anycast		192.88.99.0/24		Network		
PAT_HONEY_POT-121.5.113.11		121.5.113.11		Host		
PAT_HONEY_POT-121.5.226.36		121.5.226.36		Host		
PAT_HONEY_POT-165.232.136.24		165.232.136.24		Host		
PAT_HONEY_POT-178.175.30.253		178.175.30.253		Host		
PAT_HONEY_POT-192.168.1.14		192.168.1.14		Host		

Displaying 1 - 20 of 22 rows Page 1 of 2

How To

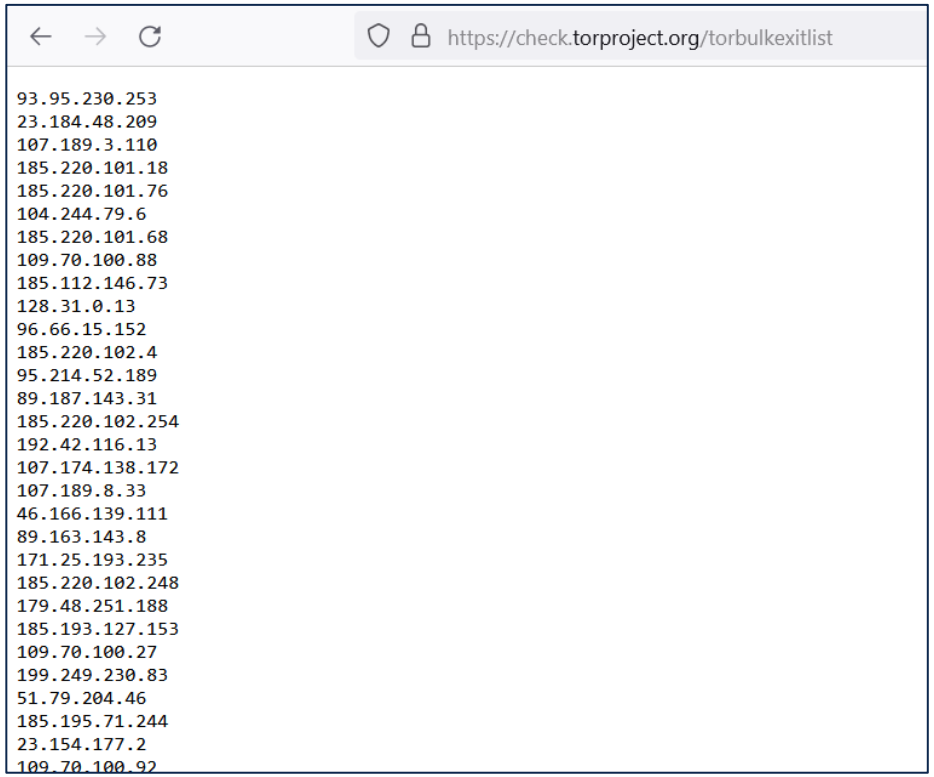
Architecture de la solution



Tor IP Blocking List

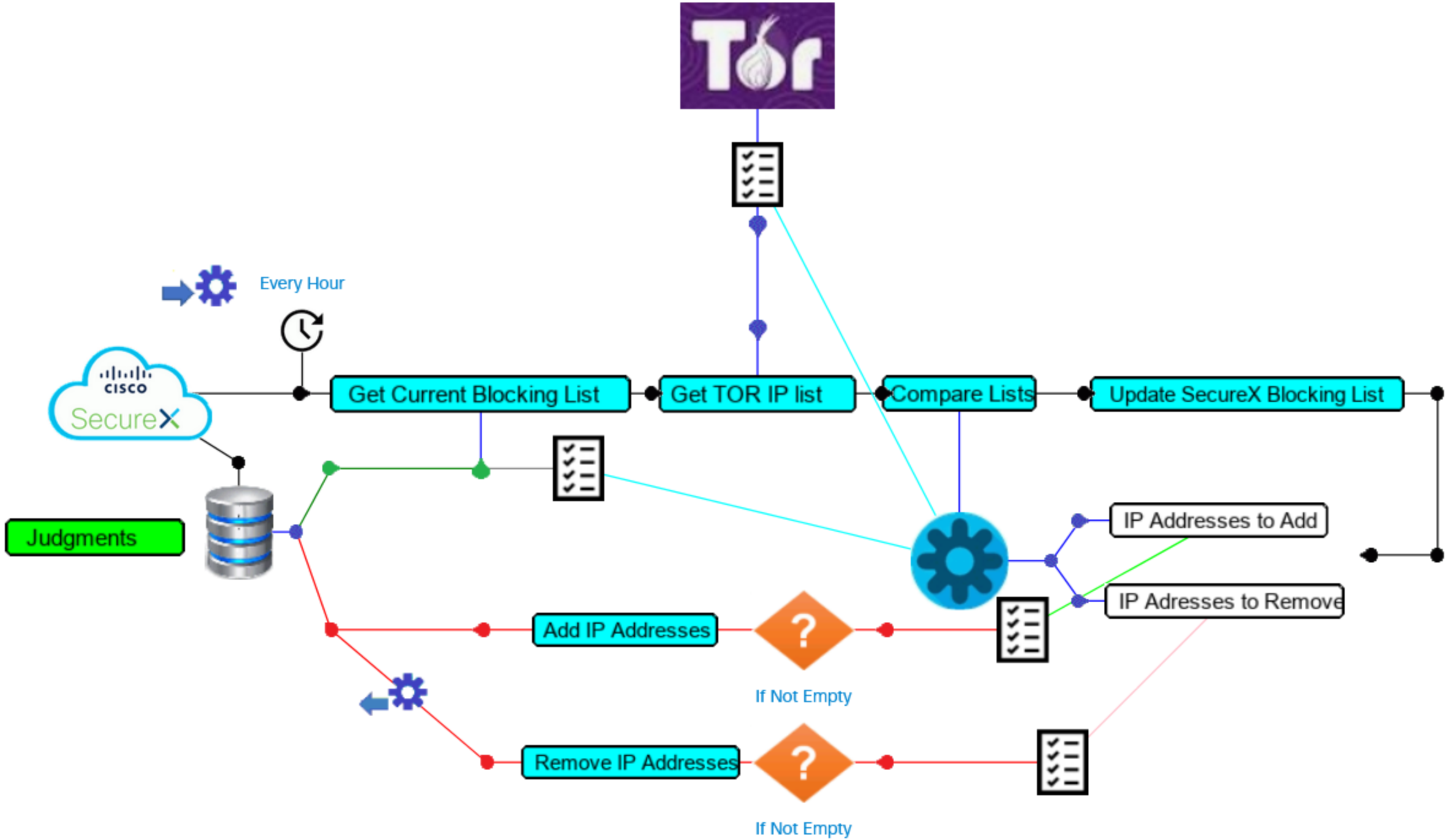
TOR : Adresses IP entrées et sorties

- https://check.torproject.org/torbulkexitlist

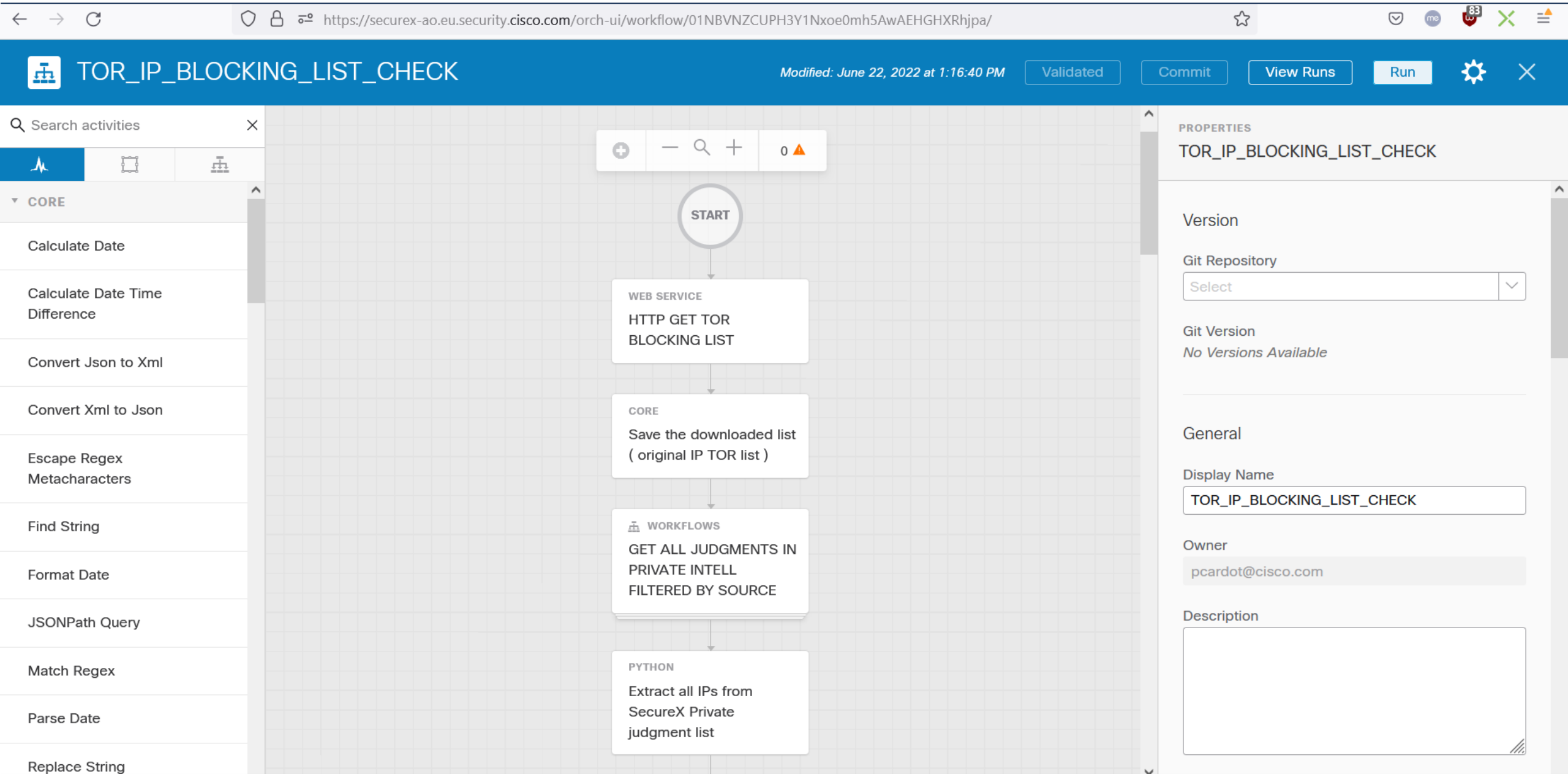


- Les recommandations de Sécurité sont :

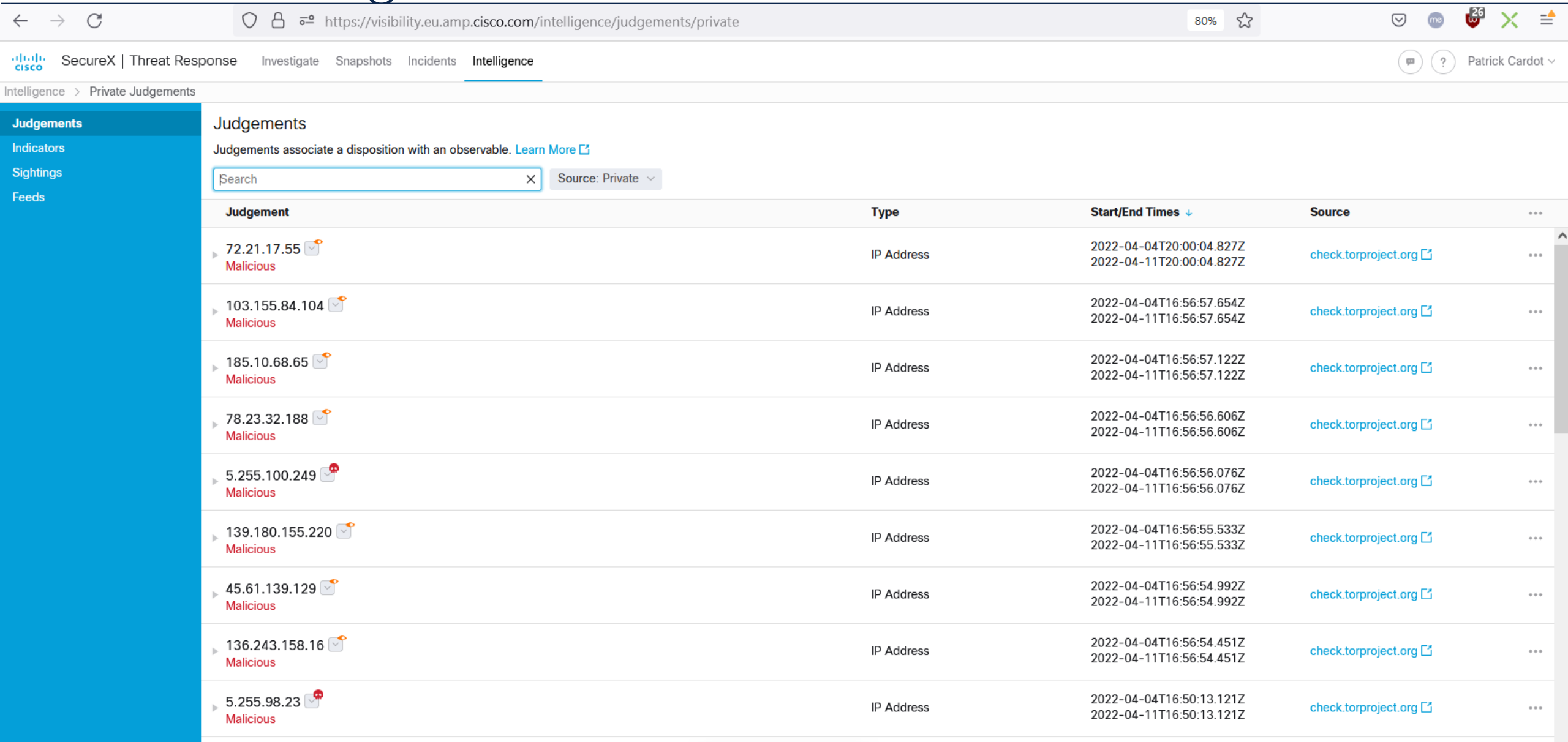
- Télécharger la liste toutes les heures
- Et bloquer les adresses IP
  - En entrée
  - En sortie
  - Dans tous les firewalls INTERNET


Every Hour
Get Current Blocking List
Get TOR IP list
Compare Lists
Update SecureX Blocking List
Judgments
IP Addresses to Add
IP Adresses to Remove
Add IP Addresses
If Not Empty
Remove IP Addresses
If Not Empty

Workflow SecureX



La blocking List



What else ?

CERT France to blocking list

https://cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-005/

le 06 décembre 2021

INDICATEURS DE COMPROMISSION DU CERT-FR

Objet: Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium

GESTION DU DOCUMENT

Référence	CERTFR-2021-IOC-005
Titre	Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium
Date de la première version	06 décembre 2021
Date de la dernière version	06 décembre 2021
Source(s)	

Objet: 🇫🇷/🇬🇧 Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium

GESTION DU DOCUMENT

Référence	CERTFR-2021-IOC-005
Titre	🇫🇷/🇬🇧 Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium
Date de la première version	06 décembre 2021
Date de la dernière version	06 décembre 2021
Source(s)	
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

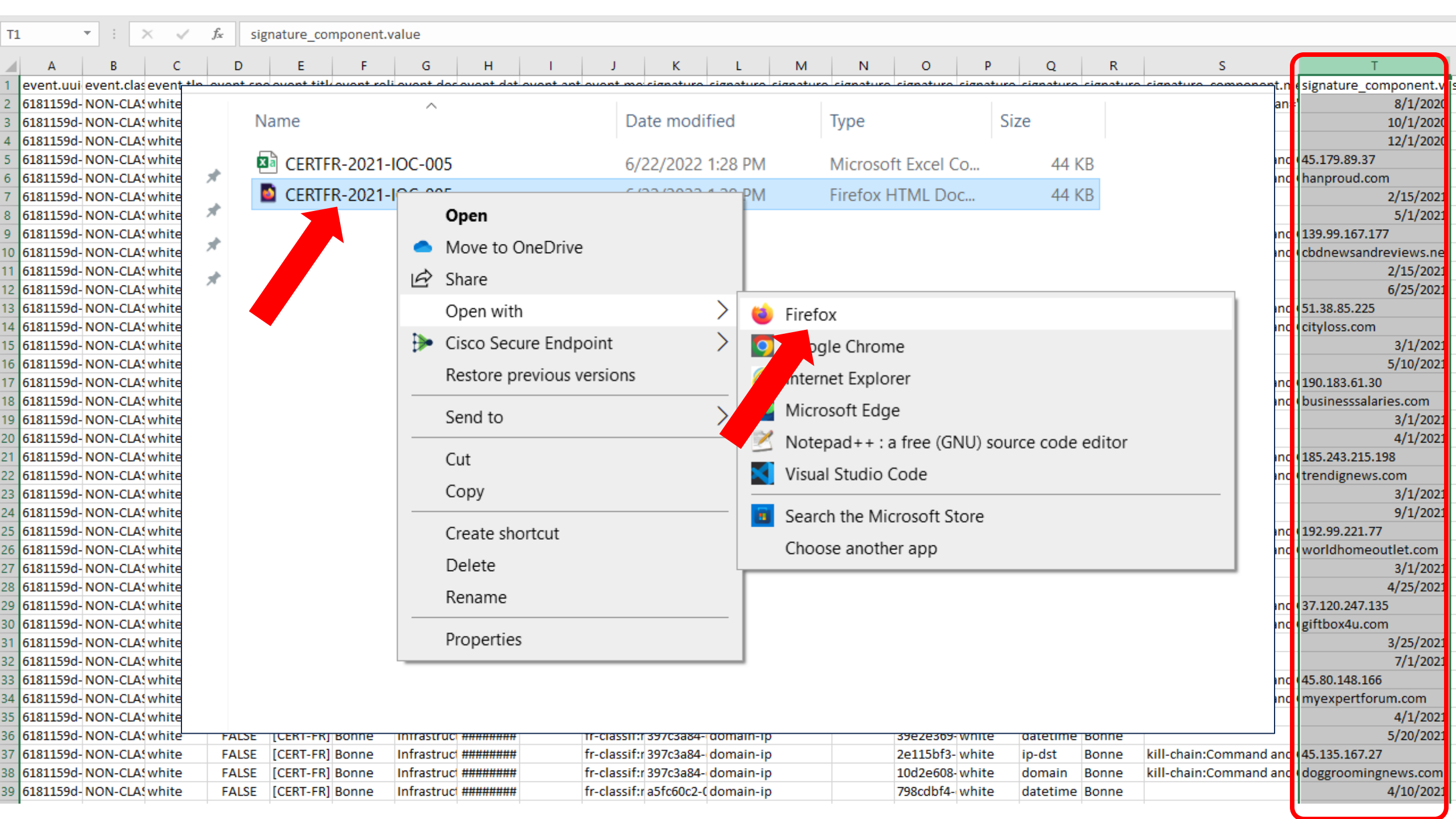
Une gestion de version détaillée se trouve à la fin de ce document.

🇫🇷 Les marqueurs techniques suivants sont associés aux campagnes d'hameçonnage du mode opératoire Nobelium décrites dans la publication CERTFR-2021-CTI-010. Ils peuvent être utilisés à des fins de recherche de compromission dans des journaux historiques ou de détection.

🇬🇧 The following indicators of compromise are associated with the phishing campaigns by the Nobelium intrusion set described in the CERTFR-2021-CTI-011 report. These technical elements are provided to help detecting malicious activities in logs or inside live network trafic.

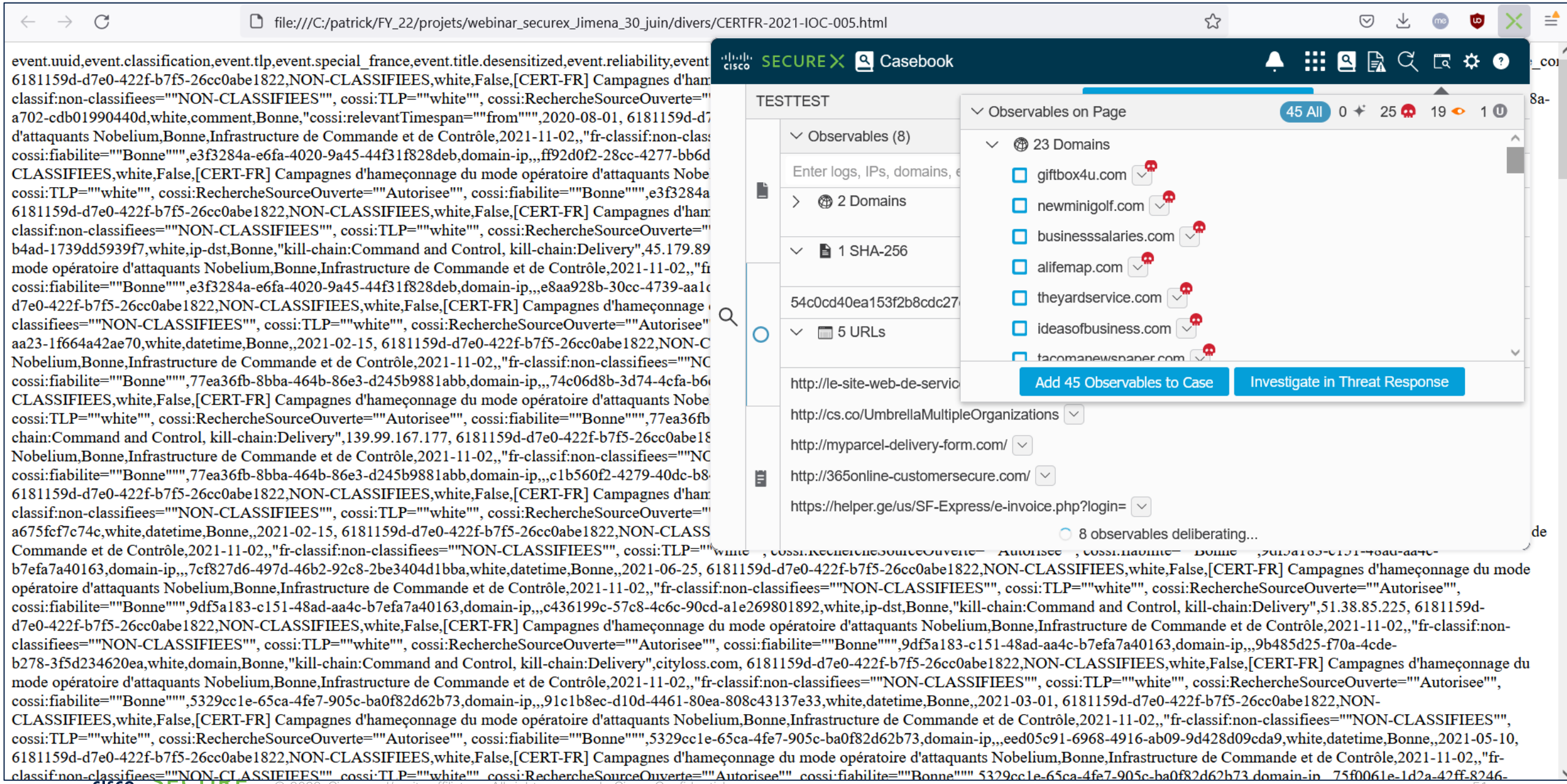
TÉLÉCHARGER LES MARQUEURS (JSON MISP)
🇬🇧 DOWNLOAD IOCs (JSON MISP)

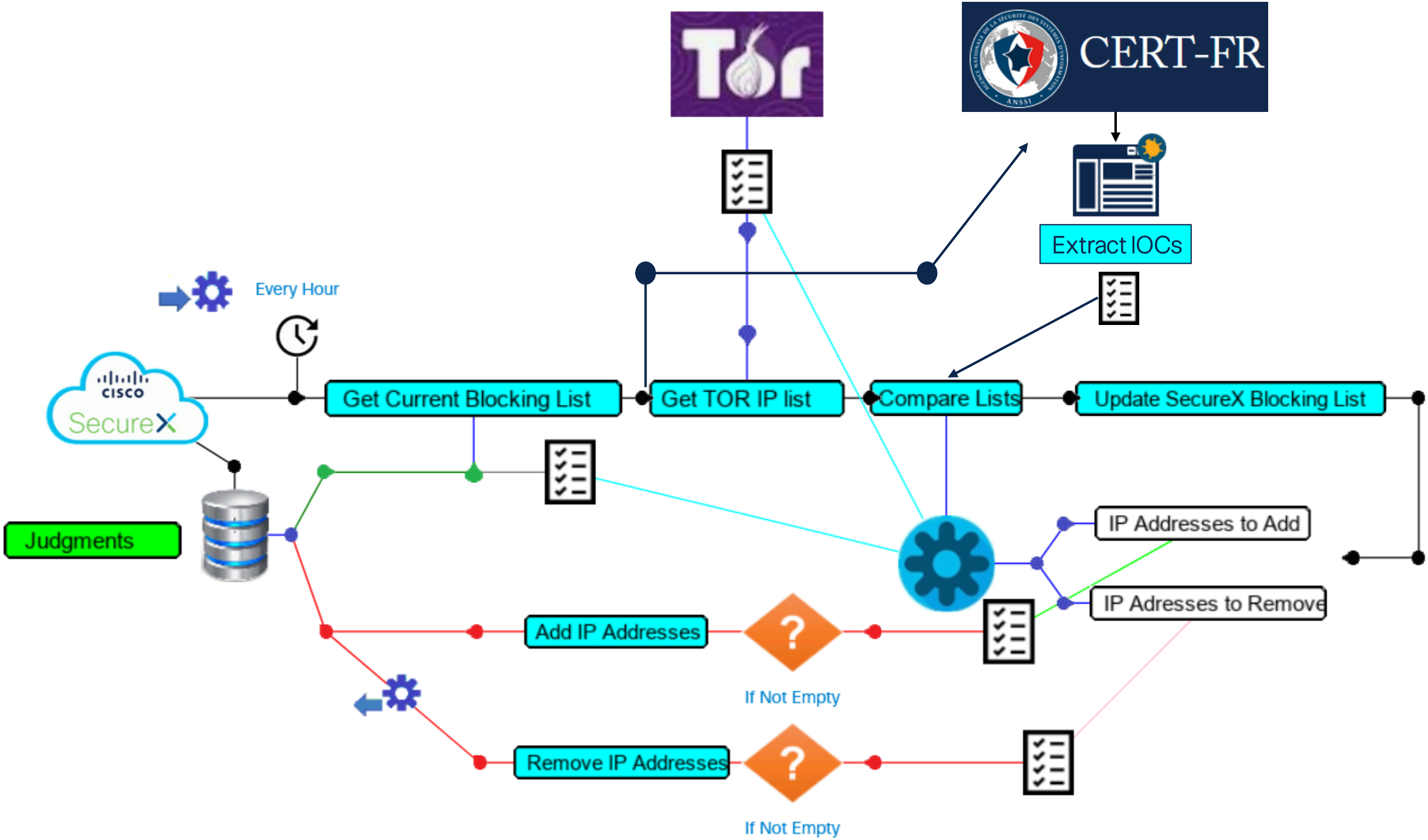
TÉLÉCHARGER LES MARQUEURS (CSV MISP)
🇬🇧 DOWNLOAD IOCs (CSV MISP)


T1
signature_component.value
Name
Date modified
Type
Size
CERTFR-2021-IOC-005
6/22/2022 1:28 PM
Microsoft Excel Co...
44 KB
Firefox HTML Doc...
44 KB
Open
Move to OneDrive
Share
Open with
Cisco Secure Endpoint
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Firefox
Google Chrome
Internet Explorer
Microsoft Edge
Notepad++ : a free (GNU) source code editor
Visual Studio Code
Search the Microsoft Store
Choose another app

file:///C:/patrick/FY_22/projets/webinar_securex_Jimena_30_juin/divers/CERTFR-2021-IOC-005.html

event.uuid,event.classification,event.tlp,event.special_france,event.title.desensitized,event.reliability,event.description,event.date,event.apts,event.metadata,signature.uuid,signature.type,signature.description,signature.value,signature_co
6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",e63dbf73-7e56-468a-a702-cdb01990440d,comment,,2020-08-01,e63dbf73-7e56-468a-a702-cdb01990440d,white,comment,Bonne,"cossi:relevantTimespan=""from""",2020-08-01, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",e3f3284a-e6fa-4020-9a45-44f31f828deb,domain-ip,,,ff92d0f2-28cc-4277-bb6d-1cdc5c2f7315,white,datetime,Bonne,,2020-10-01, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",e3f3284a-e6fa-4020-9a45-44f31f828deb,domain-ip,,,f2aa70f1-8c6a-4968-a3da-4bdb36fbc6a1,white,datetime,Bonne,,2020-12-01, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",e3f3284a-e6fa-4020-9a45-44f31f828deb,domain-ip,,,8ed8b9a2-f95e-47f2-b4ad-1739dd5939f7,white,ip-dst,Bonne,"kill-chain:Command and Control, kill-chain:Delivery",45.179.89.37, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",e3f3284a-e6fa-4020-9a45-44f31f828deb,domain-ip,,,e8aa928b-30cc-4739-aa1d-f78364f618c7,white,domain,Bonne,"kill-chain:Command and Control, kill-chain:Delivery",hanproud.com, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",77ea36fb-8bba-464b-86e3-d245b9881abb,domain-ip,,,690bd55c-c8ea-4c69-aa23-1f664a42ae70,white,datetime,Bonne,,2021-02-15, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",77ea36fb-8bba-464b-86e3-d245b9881abb,domain-ip,,,74c06d8b-3d74-4cfa-b6cc-64b76260adf2,white,datetime,Bonne,,2021-05-01, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",77ea36fb-8bba-464b-86e3-d245b9881abb,domain-ip,,,f0816314-14bf-4349-84cf-272c9ba17443,white,ip-dst,Bonne,"kill-chain:Command and Control, kill-chain:Delivery",139.99.167.177, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",77ea36fb-8bba-464b-86e3-d245b9881abb,domain-ip,,,c1b560f2-4279-40dc-b847-80fc0cf7ef7e,white,domain,Bonne,"kill-chain:Command and Control, kill-chain:Delivery",cbdnewsandreviews.net, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",9df5a183-c151-48ad-aa4c-b7efa7a40163,domain-ip,,,c87fe1af-4133-4a8b-9fc9-a675fcf7c74c,white,datetime,Bonne,,2021-02-15, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",9df5a183-c151-48ad-aa4c-b7efa7a40163,domain-ip,,,7cf827d6-497d-46b2-92c8-2be3404d1bba,white,datetime,Bonne,,2021-06-25, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",9df5a183-c151-48ad-aa4c-b7efa7a40163,domain-ip,,,c436199c-57c8-4c6c-90cd-a1e269801892,white,ip-dst,Bonne,"kill-chain:Command and Control, kill-chain:Delivery",51.38.85.225, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",9df5a183-c151-48ad-aa4c-b7efa7a40163,domain-ip,,,9b485d25-f70a-4cde-b278-3f5d234620ea,white,domain,Bonne,"kill-chain:Command and Control, kill-chain:Delivery",cityloss.com, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",5329cc1e-65ca-4fe7-905c-ba0f82d62b73,domain-ip,,,91c1b8ec-d10d-4461-80ea-808c43137e33,white,datetime,Bonne,,2021-03-01, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",5329cc1e-65ca-4fe7-905c-ba0f82d62b73,domain-ip,,,eed05c91-6968-4916-ab09-9d428d09cda9,white,datetime,Bonne,,2021-05-10, 6181159d-d7e0-422f-b7f5-26cc0abe1822,NON-CLASSIFIEES,white,False,[CERT-FR] Campagnes d'hameçonnage du mode opératoire d'attaquants Nobelium,Bonne,Infrastructure de Commande et de Contrôle,2021-11-02,,"fr-classif:non-classifiees=""NON-CLASSIFIEES"", cossi:TLP=""white"", cossi:RechercheSourceOuverte=""Autorisee"", cossi:fiabilite=""Bonne""",5329cc1e-65ca-4fe7-905c-ba0f82d62b73,domain-ip,,,75f0061e-1d2a-42ff-8246-




Tor
CERT-FR
Extract IOCs
Every Hour
cisco
SecureX
Get Current Blocking List
Get TOR IP list
Compare Lists
Update SecureX Blocking List
Judgments
IP Addresses to Add
IP Adresses to Remove
Add IP Addresses
?
If Not Empty
Remove IP Addresses
?
If Not Empty

Détection et Réaction

Stratégie de défense SecureX

SecureX Device Insight : Inventaire des biens critiques

https://securex.eu.security.cisco.com/endpoints

SecureX | Dashboard | Integration Modules | Orchestration | Insights | Administration | Patrick Cardot

Device Insights

- Inventory Overview
- Sources
- Source Settings

Source Health

75%

2 Devices

Types
- Server (0)
- Desktop (2)
- Virtual (0)
- Mobile (0)

Status
- Managed (0)
- Unmanaged (2)

OS

Other				
0	0	0	0	
0	0	0	0	

Basic Search: Select Saved Filter

Text Search: User, IP, hostname...

Managed Status: Select

Operating System: Select

OS Support: Select

Type: Select

Sources: Select

Policies: Select

Has Faults (0) | AV Definitions out of date (0) | Clear Filters | Save Filters

2 Devices found | Export to CSV | Edit Columns

Device Name	OS	OS Version	OS Support	Users Seen	Sources	Managed	Compromised
DESKTOP-1MNPTK4	Windows	10 Pro			AMP for Endpoints Secure Endpoint - Cisco - pcardot	No	
Cedric	Windows	8.1 Connected			AMP for Endpoints Secure Endpoint - Cisco - pcardot	No	

SECURE X Home | Enrich...

https://securex.eu.security.cisco.com/endpoints/endpoint/0fe49ed9-55f0-46ad-ab2c-fcb354d1d488

SecureX | Dashboard | Integration Modules | Orchestration | Insights | Administration | Patrick Cardot

Device Insights
- Inventory Overview
- Sources
- Source Settings

Inventory / Cedric

Windows 8.1 Connected

Managed: No

Details

Associated Users	
Last Active	2022-05-30T14:33:23.000Z
Location	NA
Hostname	Cedric
Local IPs	192.168.201.15 , 10.0.0.2
Public IPs	85.172.214.53
Macs	d0:53:49:07:e6:d5, 0a:00:27:00:00:07
Hardware Id	bfebfbff00030678
Serial Number	

Vulnerabilities

Vulnerabilities

47

Security Products

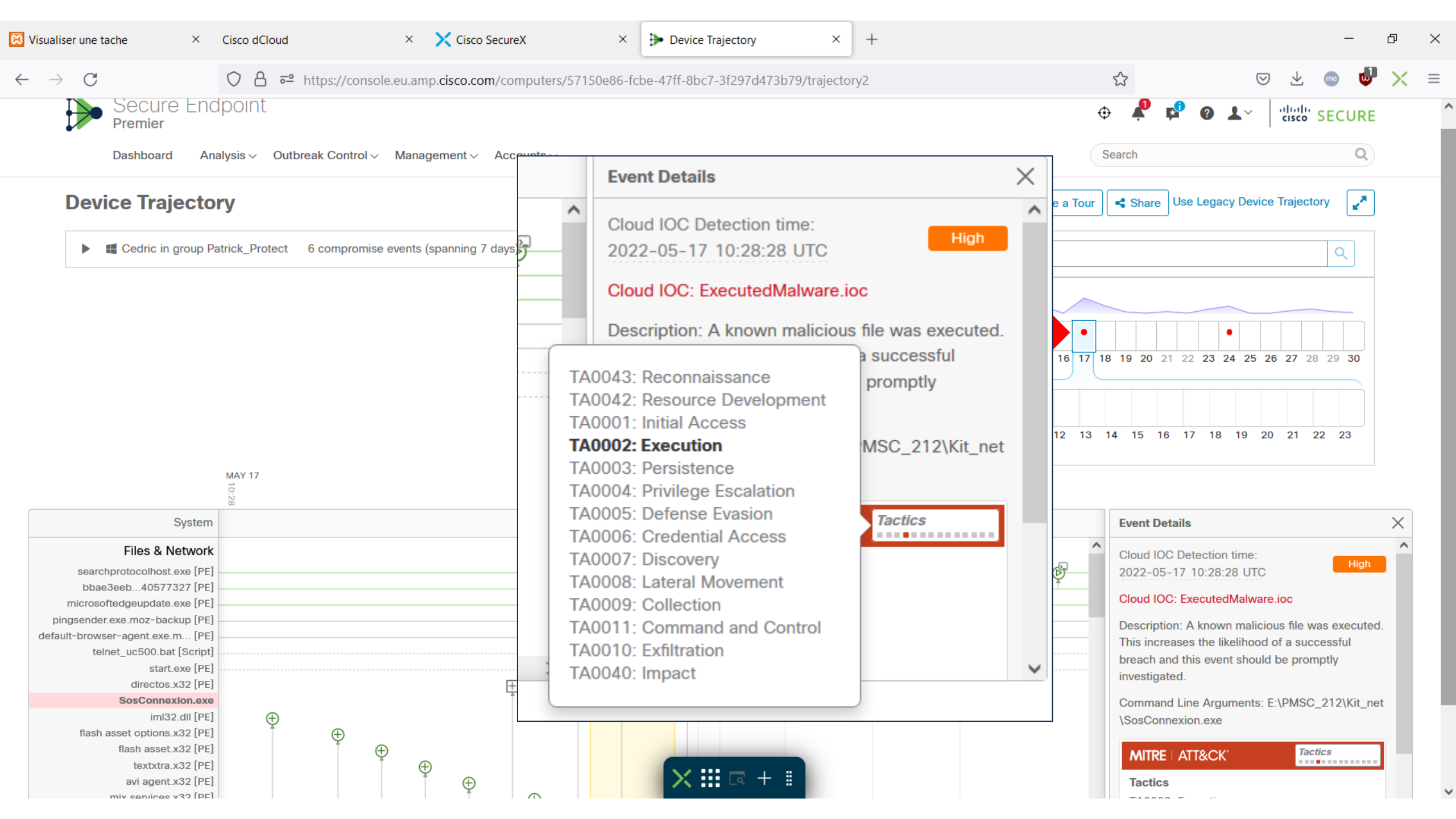
Firewall	Cisco Secure Endpoint
NA	Enabled
Disk Encryption	Automatic Updates
NA	NA

Cisco Secure Endpoint (AMP)

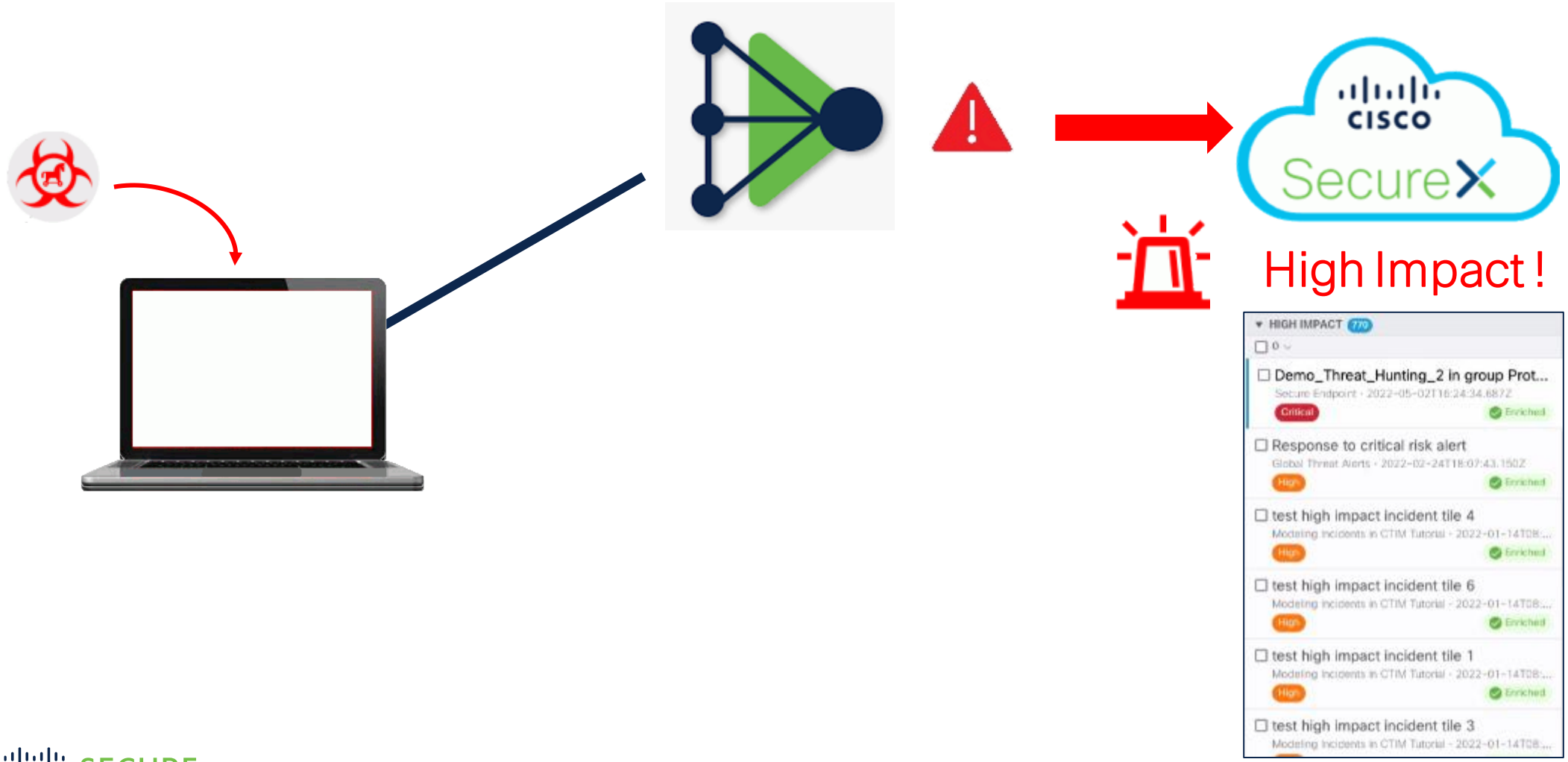
Definitions	Definitions Up To Date
Isolation	Not Isolated
Orbital	Not Enabled
Compromised	Endpoint has a Compromised Artifact

Connector GUID:
57150e86-fcbe-47ff-8bc7-3f297d473b79

SECURE X | Incidents | Enrich...


Visualiser une tache
Cisco dCloud
Cisco SecureX
Device Trajectory
https://console.eu.amp.cisco.com/computers/57150e86-fcbe-47ff-8bc7-3f297d473b79/trajectory2
Secure Endpoint
Premier
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Device Trajectory
Cedric in group Patrick_Protect
6 compromise events (spanning 7 days)
Share
Use Legacy Device Trajectory
Event Details
Cloud IOC Detection time:
2022-05-17 10:28:28 UTC
High
Cloud IOC: ExecutedMalware.ioc
Description: A known malicious file was executed.
successful
promptly
MSC_212\Kit_net
TA0043: Reconnaissance
TA0042: Resource Development
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0008: Lateral Movement
TA0009: Collection
TA0011: Command and Control
TA0010: Exfiltration
TA0040: Impact
Tactics
MAY 17
System
Files & Network
searchprotocolhost.exe [PE]
bbae3eeb...40577327 [PE]
microsoftedgeupdate.exe [PE]
pingsender.exe.moz-backup [PE]
default-browser-agent.exe.m... [PE]
telnet_uc500.bat [Script]
start.exe [PE]
directos.x32 [PE]
SosConnexion.exe
iml32.dll [PE]
flash asset options.x32 [PE]
flash asset.x32 [PE]
textxtra.x32 [PE]
avi agent.x32 [PE]
Event Details
Cloud IOC Detection time:
2022-05-17 10:28:28 UTC
High
Cloud IOC: ExecutedMalware.ioc
Description: A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.
Command Line Arguments: E:\PMSC_212\Kit_net\SosConnexion.exe
MITRE | ATT&CK
Tactics
Tactics

SecureX High Impact Incidents



Cisco SecureX | Dashboard

https://console.eu.amp.cisco.com/dashboard

Secure Endpoint
Premier

Dashboard | Analysis | Outbreak Control | Management | Accounts

Search

Dashboard

Dashboard | Inbox | Overview | Events | iOS Clarity

Refresh All | Auto-Refresh | Reset | New Filter | 30 days | 2022-05-24 13:46 | 2022-06-23 13:46 | UTC

0% compromised

Inbox Status

0 Require Attention | 0 In Progress | 0 Resolved

Global Threat Alerts

unresolved threats
0

Compromises

Inbox

Top | 0 / 42

Protect

Triage

Audit

Quarantined Detections

Quarantine Events

Top | 0 / 42

Triage

Audit

Vulnerabilities

View

Top | 0 / 42

Protect

Triage

Audit

24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
MAY JUN

Secure Malware Analytics

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

46.6K Files Scanned
2.42K Network Connections Logged

Connectors

42 Connectors
0 Installs
0 Install Failures

Significant Compromise Observables

Compromise Event Types

Type here to search

80°F Mostly sunny

ENG FR 3:57 PM 6/23/2022

Cisco SecureX | Dashboard

https://console.eu.amp.cisco.com/dashboard

Refresh All | Auto-Refresh | Reset | New Filter | 30 days | 2022-05-24 14:00 | 2022-06-23 14:00 | UTC

2.4% compromised

Inbox Status

1 Requires Attention | 0 In Progress | 0 Resolved

Global Threat Alerts

unresolved threats
0

Compromises

Inbox

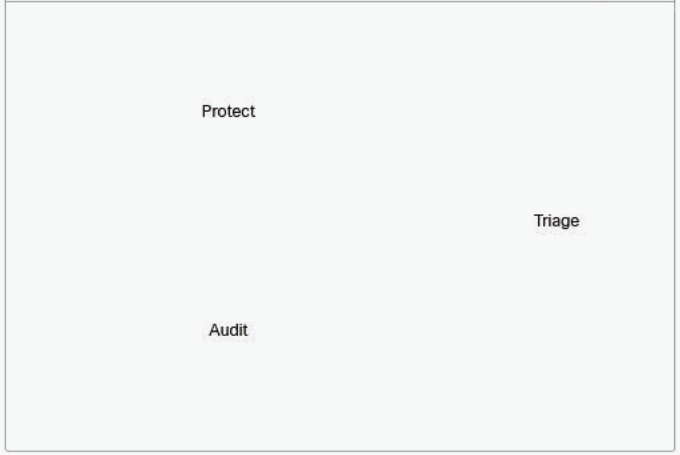
Top 1 / 42

24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
MAY JUN

Quarantined Detections

Quarantine Events

Top 0 / 42

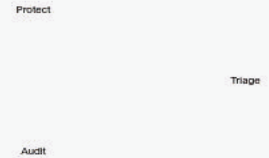


24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
MAY JUN

Vulnerabilities

View

Top 0 / 42



Secure Malware Analytics

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

46.6K Files Scanned
2.42K Network Connections Logged

Connectors

42 Connectors
0 Installs
0 Install Failures

Quick Start

Set Up Windows Connector
Set Up Mac Connector
Set Up Linux Connector

Significant Compromise Observables

FILE	21524672...082ce585 SosConnexion.exe	1

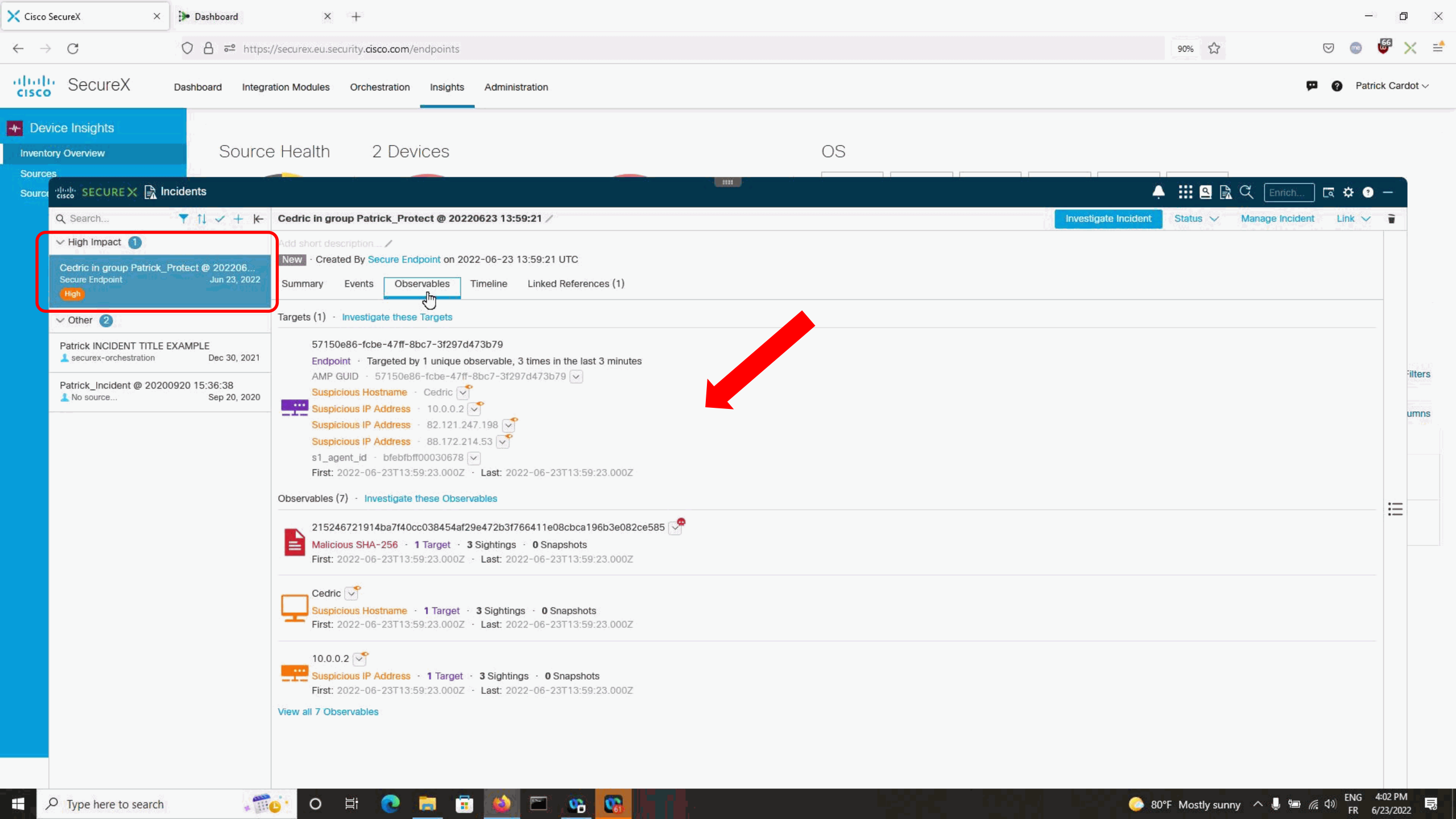
Compromise Event Types

High	ExecutedMalware.ioc	1
Medium	Threat Detected	1
Medium	Quarantine Failure	1

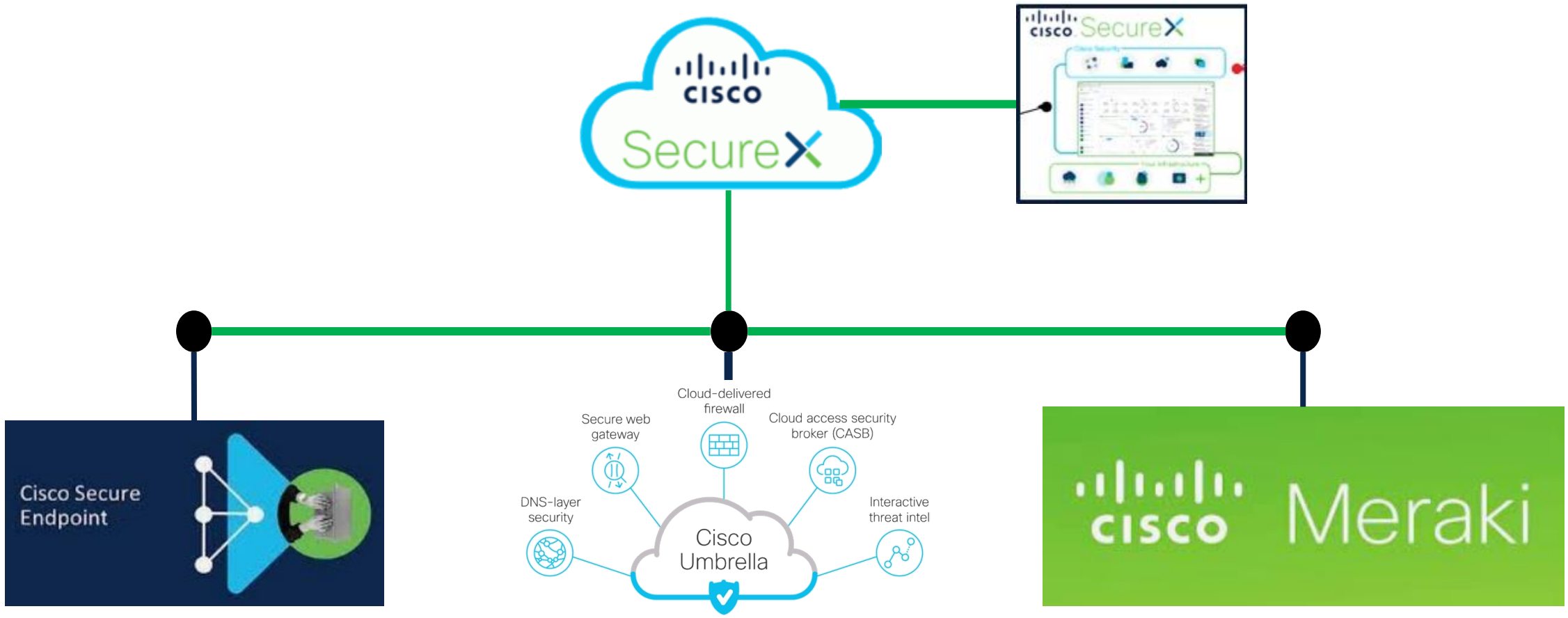
Type here to search

80°F Mostly sunny

ENG FR 4:00 PM 6/23/2022


Cisco SecureX
Dashboard
https://securex.eu.security.cisco.com/endpoints
SecureX
Dashboard
Integration Modules
Orchestration
Insights
Administration
Patrick Cardot
Device Insights
Inventory Overview
Sources
Source Health
2 Devices
OS
SECURE X
Incidents
Search...
High Impact 1
Cedric in group Patrick_Protect @ 202206...
Secure Endpoint
Jun 23, 2022
High
Other 2
Patrick INCIDENT TITLE EXAMPLE
securex-orchestration
Dec 30, 2021
Patrick_Incident @ 20200920 15:36:38
No source...
Sep 20, 2020
Cedric in group Patrick_Protect @ 20220623 13:59:21
Investigate Incident
Status
Manage Incident
Link
Add short description ...
New · Created By Secure Endpoint on 2022-06-23 13:59:21 UTC
Summary
Events
Observables
Timeline
Linked References (1)
Targets (1) · Investigate these Targets
57150e86-fcbe-47ff-8bc7-3f297d473b79
Endpoint · Targeted by 1 unique observable, 3 times in the last 3 minutes
AMP GUID · 57150e86-fcbe-47ff-8bc7-3f297d473b79
Suspicious Hostname · Cedric
Suspicious IP Address · 10.0.0.2
Suspicious IP Address · 82.121.247.198
Suspicious IP Address · 88.172.214.53
s1_agent_id · bfebfbff00030678
First: 2022-06-23T13:59:23.000Z · Last: 2022-06-23T13:59:23.000Z
Observables (7) · Investigate these Observables
2152467219l4ba7f40cc038454af29e472b3f766411e08cbca196b3e082ce585
Malicious SHA-256 · 1 Target · 3 Sightings · 0 Snapshots
First: 2022-06-23T13:59:23.000Z · Last: 2022-06-23T13:59:23.000Z
Cedric
Suspicious Hostname · 1 Target · 3 Sightings · 0 Snapshots
First: 2022-06-23T13:59:23.000Z · Last: 2022-06-23T13:59:23.000Z
10.0.0.2
Suspicious IP Address · 1 Target · 3 Sightings · 0 Snapshots
First: 2022-06-23T13:59:23.000Z · Last: 2022-06-23T13:59:23.000Z
View all 7 Observables
Type here to search
80°F Mostly sunny
ENG FR
4:02 PM 6/23/2022

Multi Tenant Use case



Cisco SecureX

https://securex.eu.security.cisco.com

90%

SecureX

Dashboard | Integration Modules | Orchestration | Insights | Administration

Patrick Cardot

CUSTOMERS | Umbrella | Secure Endpoint New | Global Dashboard | AMP | ThreatGrid | Customer's Dashboard

Customize | Timeframe*

MSSP Dashboard

Clients List

SAFE ! ALERT !

CLIENT	STATUS	Selected
ACME COMPANY	SAFE	
STAR IN THE SKY	SAFE	
MAGICAL BUSINESS	! ALERT !	YES
INTERNATIONAL BUSINESS	! ALERT !	

SECURE X Incidents

Enrich...

Type here to search

Rain coming

ENG FR

9:55 AM 6/19/2022

Cisco SecureX

https://securex.eu.security.cisco.com

90%

ALERT_ROOM_PATRICK
SECUREX_ALERTS
Alert Assigned to Expert : Patrick !
Critical Asset Targeted by a Malware...

SecureX

Dashboard | Integration Modules | Orchestration | Insights | Administration

CUSTOMERS | Umbrella | Secure Endpoint New | Global Dashboard | AMP | ThreatGrid | Customer's Dashboard

Customize | Timeframe*

MSSP Dashboard
Customer Information

ACME COMPANY
Customer

! ALERT !
Threat Risk

50/100
Risk Meter

MSSP Dashboard
Alertes Critiques

Last Hour

Severity	Description	Status	Source	Date and Time
High	MALWARE ALERT	NEW	Secure EndPoint	2022-06-19T07:58:29.759695Z

MSSP Dashboard
Secure Endpoint Alerts

Last Hour

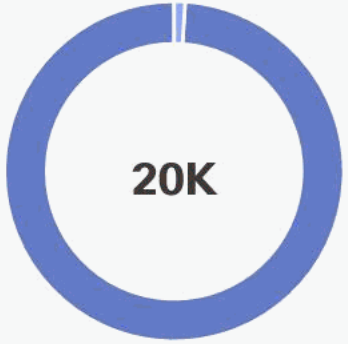
High

Endpoint	Internal IP	Earlist Activity	Latest Activity	Severity	Status
ZenConnect Demo Endpoint	192.168.8.14	2022-06-19T07:58:29.776Z	2022-06-19T07:58:29.776Z	High	Unresolved

MSSP Dashboard
Umbrella DNS Requests Breakdown

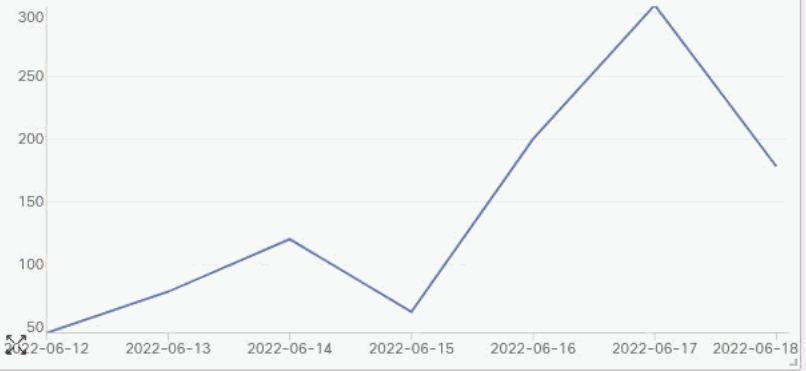
Last 7 Days

Items
Allowed (20.3k)
blocked (100)



MSSP Dashboard
Umbrella Blocked Requests

Last 7 Days



SECURE X Incidents

Enrich...

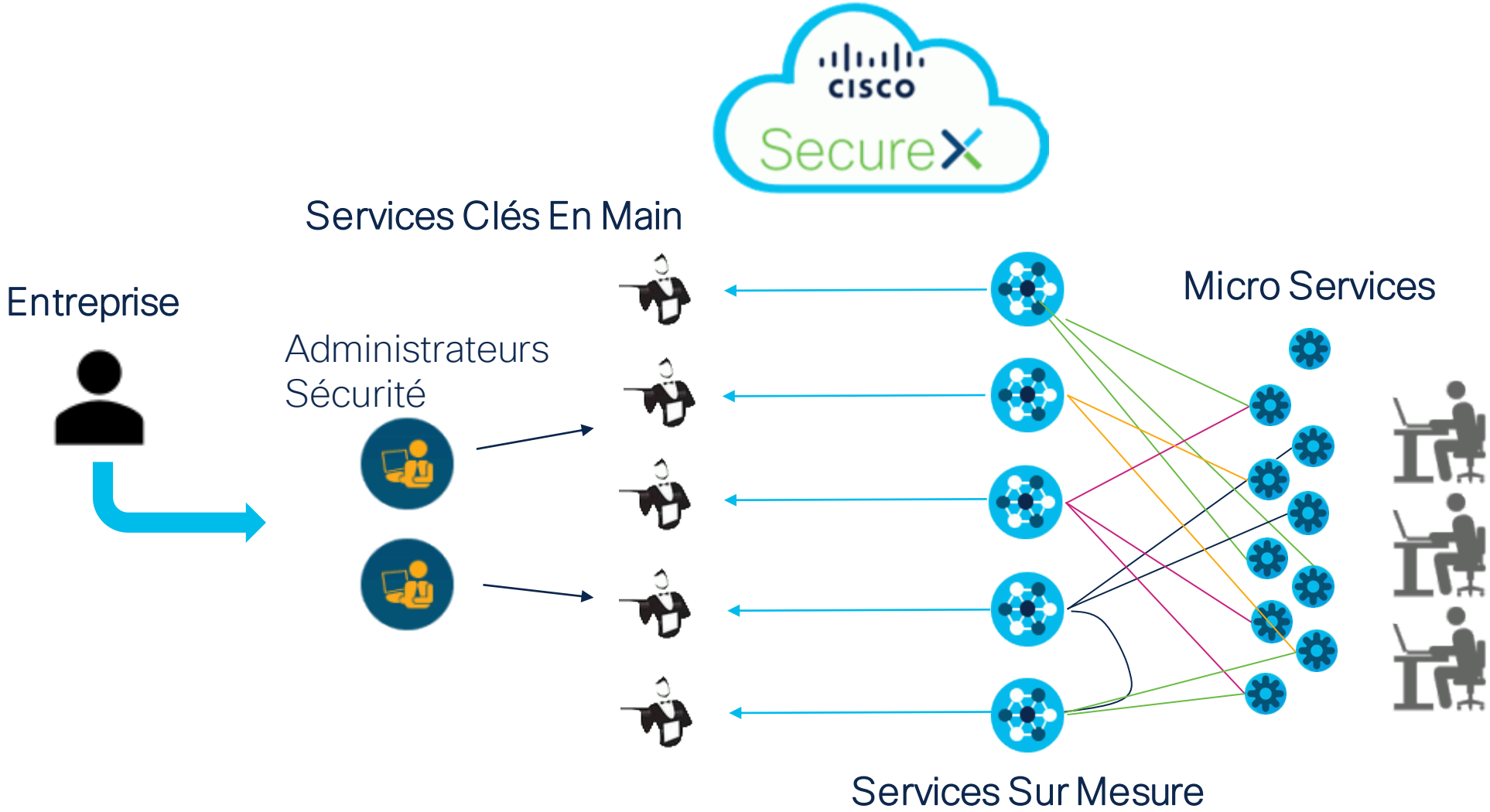
Type here to search

67°F Sunny

ENG FR

10:21 AM 6/19/2022

SecureX : Une Architecture de Services de Sécurité



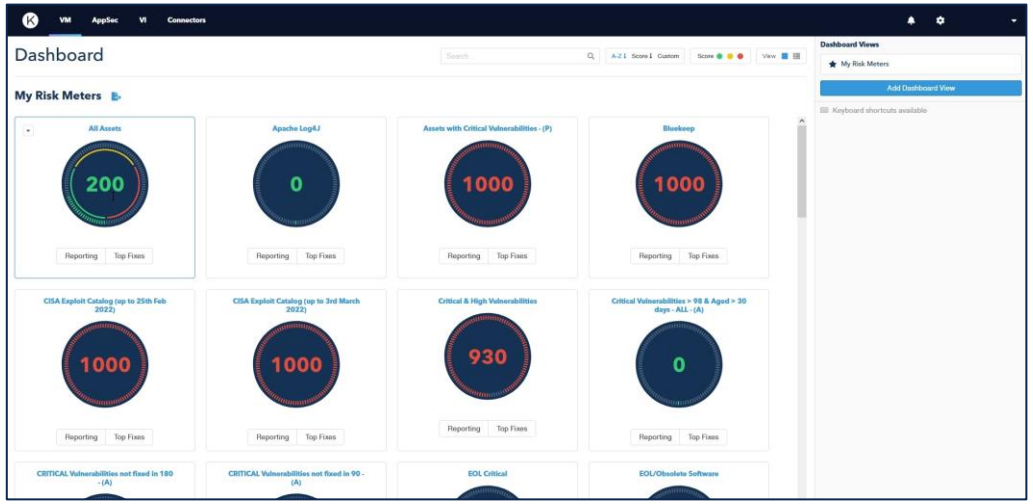
Vulnerability Risk Management Driven Security

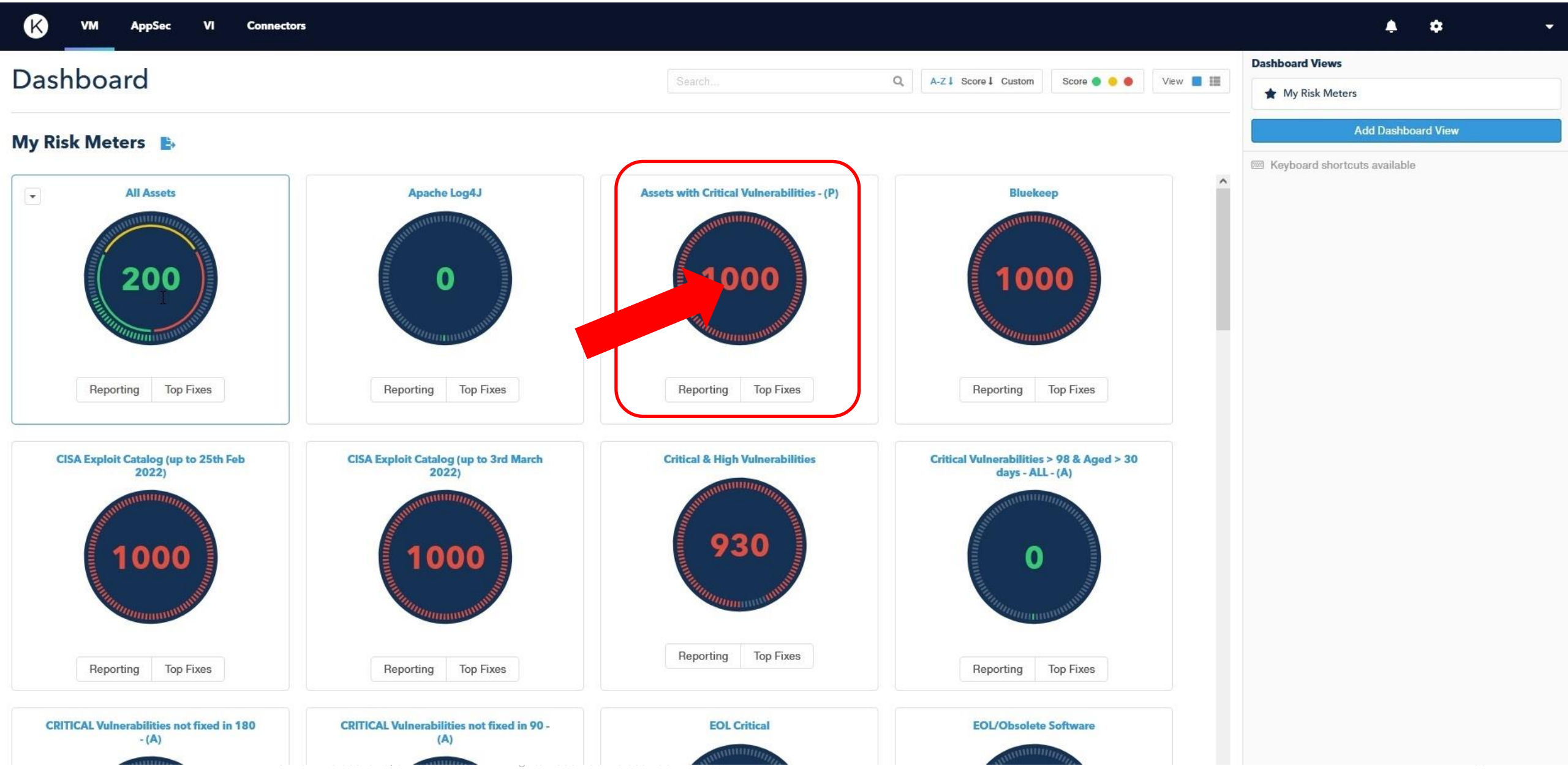
Kenna Security

Vulnerability Scanner Solutions

beyond SECURITY AVDS
CROWDSTRIKE
tripwire API
OpenVAS
Outpost24 Outscan/HIAB
Outpost24 SWAT
Outpost24 XML
Qualys. VM
RAPID7 Nexpose
RAPID7 NexposeXML
TANIUM Comply
nessus Importer
nessus XML
tenable.sc
tenable.io
BETA PRISMA CLOUD (TWISTLOCK)

CISCO™
KENNA
Security




VM
AppSec
VI
Connectors
Dashboard
Search...
A-Z
Score
Custom
Score
View
My Risk Meters
All Assets
200
Reporting
Top Fixes
Apache Log4J
0
Reporting
Top Fixes
Assets with Critical Vulnerabilities - (P)
1000
Reporting
Top Fixes
Bluekeep
1000
Reporting
Top Fixes
CISA Exploit Catalog (up to 25th Feb 2022)
1000
Reporting
Top Fixes
CISA Exploit Catalog (up to 3rd March 2022)
1000
Reporting
Top Fixes
Critical & High Vulnerabilities
930
Reporting
Top Fixes
Critical Vulnerabilities > 98 & Aged > 30 days - ALL - (A)
0
Reporting
Top Fixes
CRITICAL Vulnerabilities not fixed in 180 - (A)
CRITICAL Vulnerabilities not fixed in 90 - (A)
EOL Critical
EOL/Obsolete Software
Dashboard Views
My Risk Meters
Add Dashboard View
Keyboard shortcuts available

Assets with Critical Vulnerabilities - (P)

View Report | Explore

1000

Top Fix Groups

1000 → 906 | 1000 → 956 | 1000 → 971 | 1000 → 995

Group 1

Risk Score Reduction of 94, 1 Fix

Send via email | Export CSV

PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

1 Vulns Affected

Diagnosis | Solution | CVEs Addressed 1 | ets Affected 1 | Scanner IDs 1

Alternate Fixes Available

According to its banner, the version of [illegible] the remote web server is prior to 7.1.33, 7.2.x prior to 7.2.24, or 7.3.x prior to 7.3.11. It is, therefore, affected by a remote code execution vulnerability due to insufficient va[illegible]r input. An unauthenticated, remote attacker can exploit this, by sending a specially crafted request, to cause the execution of arbitrary code by breaking the fastcgi_split_path_in[illegible]rective.

See Also:

- https://www.php.net/ChangeLog-7.php#7.3.11 https://www.php.net/ChangeLog-7.php#7.2.24 https://www.php.net/ChangeLog-7.php#7.1.33 https://bugs.php.net/bug.php?id=78599

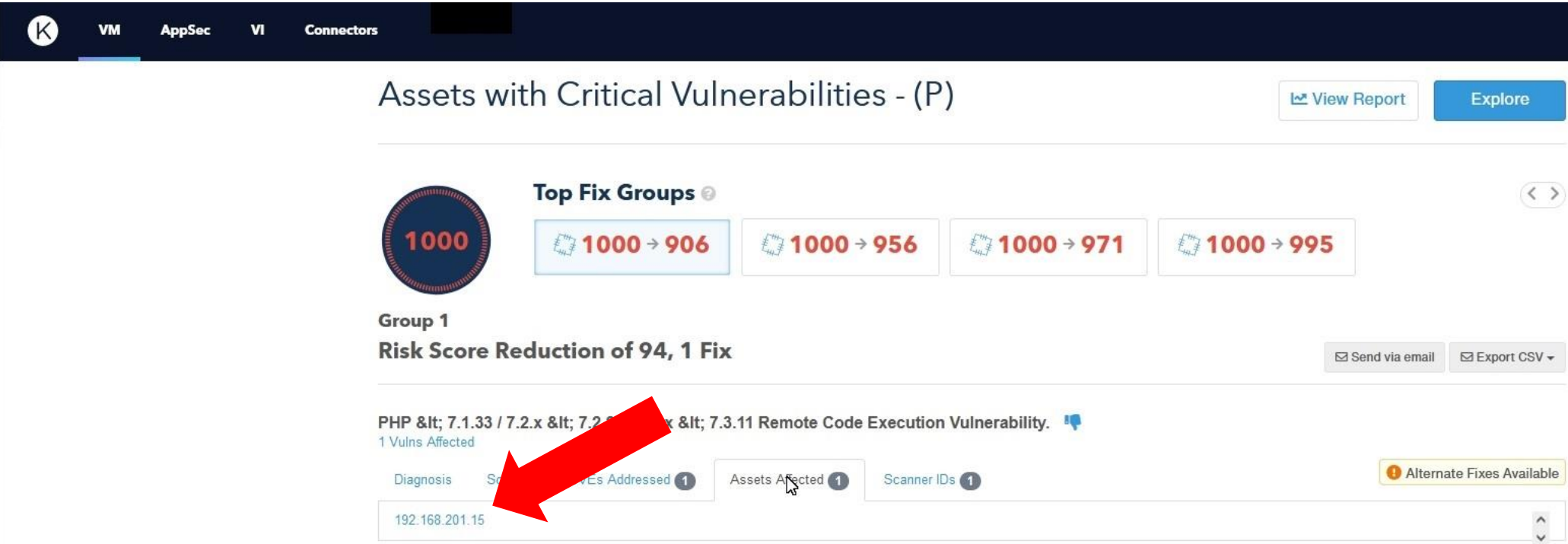
Related CVE IDs:

- CVE-2019-11043

Other Security Standard Reference IDs:

- CISA-KNOWN-EXPLOITED:2022/04/15
- IAVA:2019-A-0399-S

Kenna Fix ID: 2081096



192.168.201.15

Score: 1,000 / 1,000

Vulnerabilities 47

Edit Display

Score	Name
100 / 100 CVSS 2: 8 CVSS 3: 9.8	CVE-2019-11043 In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution. Nessus XML Fix Available Remote Code Execution
45 / 100 CVSS 2: 5	CVE-2004-2761 The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate. Nessus XML Fix Available
24 / 100 CVSS 2: 4 CVSS 3: 5.3	CVE-2019-20372 NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer. Nessus XML Fix Available
8 / 100 CVSS 2: 0	CVE-1999-0524 ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts. Nessus XML Fix Available
0 / 100 CVSS 2:	Patch Report Nessus XML Fix Available
0 / 100 CVSS 2:	JQuery Detection Nessus XML
0 / 100 CVSS 2:	PHP < 7.3.24 Multiple Vulnerabilities Nessus XML Fix Available
0 / 100 CVSS 2:	PHP < 7.3.28 Email Header Injection Nessus XML Fix Available
0 / 100 CVSS 2:	Web Server robots.txt Information Disclosure Nessus XML Fix Available

VULNERABILITY FILTERS

Status

- [ ] all
- [x] open 47

ASSET DETAILS

There are fixes available for this asset.

DETAILS

IP ADDRESS
192.168.201.15

LAST SEEN TIME
about a month ago

CREATED
10 days ago

OPERATING SYSTEM
Linux Kernel 2.6

TYPE

OPEN PORTS
22 (TCP)
80 (TCP)
443 (TCP)
8082 (TCP)

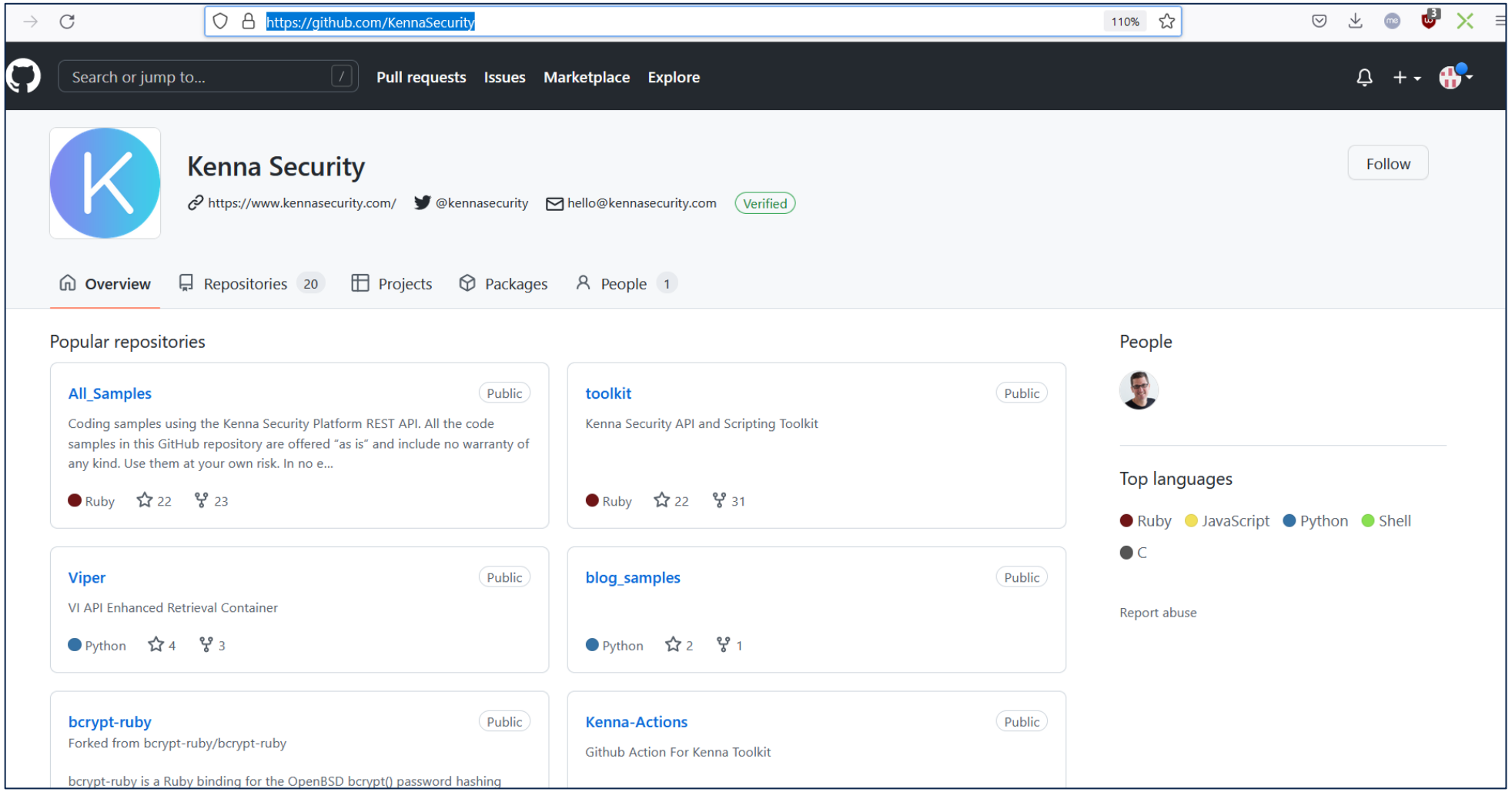
EXPIRATION DATE
07/27/2022

TAGS


KENNA
Security
SecureX
Device Insights

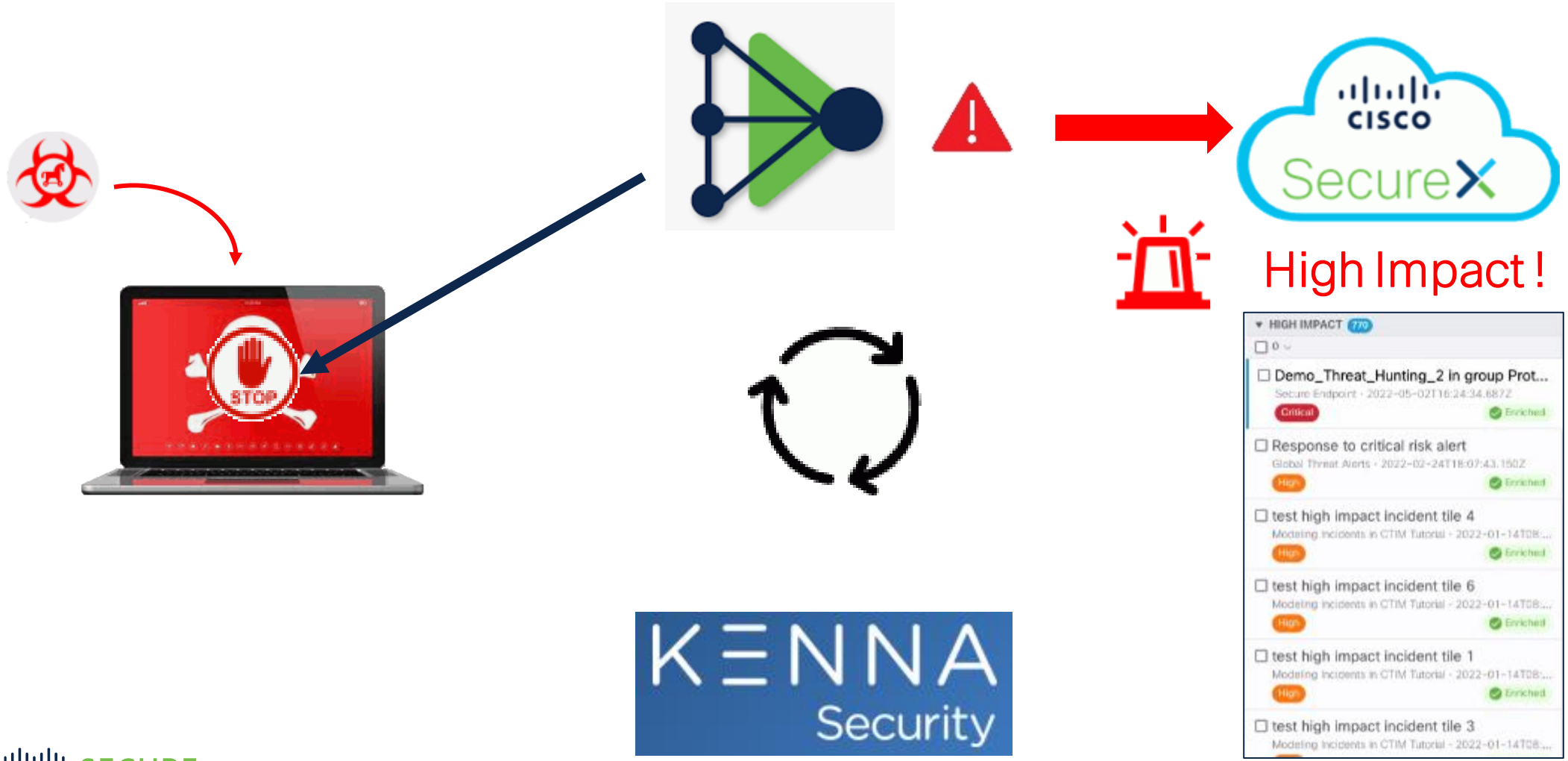
Kenna APIs

https://github.com/KennaSecurity



Vulnerability Risk Management Driven Security

SecureX + Secure EndPoint + Kenna



Cisco SecureX

https://securex.eu.security.cisco.com

SecureX

Dashboard | Integration Modules | Orchestration | Insights | Administration

Patrick Cardot

Kenna Assets | Kenna Asset Details | Kenna CVE Vue | Umbrella | Secure Endpoint New | AMP | ThreatGrid

Customize | Timeframe*

Patrick Kenna Dashboard

Assets

100 400 600 700 800 999 500 200 300

Asset ID	Asset Name	Risk Meter
3274193	10.10.3.2	100
3273443	10.10.3.1	100
3253303	192.46.26.9	400
3251925	156.81.219.51	100
3251001	156.81.217.141	
3249506	156.81.249.197	
3248899	169.225.178.56	800
3248853	169.225.176.34	700
18323888	dendesktop	100

Patrick Kenna Dashboard

Risk Score Month over Month

Proof Of Concept Demo

SECURE X Incidents

Enrich...

Type here to search

77°F Sunny

ENG FR 3:42 PM 6/28/2022

Cisco SecureX

https://securex.eu.security.cisco.com

SecureX

Dashboard | Integration Modules | Orchestration | Insights | Administration

Patrick Cardot

Kenna Assets | Kenna Asset Details | Kenna CVE Vue | Umbrella | Secure Endpoint New | AMP | ThreatGrid

Customize | Timeframe*

Patrick Kenna Dashboard
Asset information

Identifier	**api-dev.community.scl3.acmeinc.com**
Asset ID	18323858
OS	HP - embedded - embedded
IP address	63.245.223.32
Status	active
Risk Score	**999 ACTION REQUIRED !!**

ALERT IMEDIATE ACTION REQUIRED !

This asset had been targeted by an attack related to CVE-2021-44228 And this asset is vulnerable to it !

Patrick Kenna Dashboard
Asset Vulnerabilities

9 8

CVE ID	severity	Risk Meter Score	Closed
CVE-2021-44228	9	100	0
CVE-2011-3192	8	100	0

Patrick Kenna Dashboard
Risk Meter

Items

Risk Score (999)

Proof Of Concept Demo

Last Hour

High Impact Alerts

Severity	Description	Status	Source	Date and Time
CRITICAL	MALWARE ALERT	NEW	Secure EndPoint	2022-05-26T14:52:58.000Z

SECURE X Incidents

Enrich...

Type here to search

77°F Sunny

ENG FR 3:43 PM 6/28/2022

Cisco SecureX

https://securex.eu.security.cisco.com

ALERT_ROOM_PATRICK
SECUREX_ALERTS
You Selected Asset : 18322960

SecureX

Dashboard | Integration Modules | Orchestration | Insights | Administration

Kenna Assets | Kenna Asset Details | Kenna CVE Vue | Umbrella | Secure Endpoint New | AMP | ThreatGrid

Customize | Timeframe*

Patrick Kenna Dashboard
CVE Details

CVE : **CVE-2021-44228**

Details :

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Solution :

The vendor has released patch. Please visit <a href="https://support.broadcom.com/web/ecx/suppor
2-CVE-2021-44228-Vulnerability/SYMSA19793">SYMSA19793 (Symantec Endpoint Protection Man
on Broadcom Dow
/article?legacyId=TECH103088">here for download instruction.Workaround:
Please refer to SYMSA19793 (Symantec Endpoint Protection Manager) for mitigation information. Patch:
 Following are links for downloading patches to fix the vulnerabilities:

<a href="https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/Symantec-Security-Advisory-for-Log4j-2-CVE-2021-44228-Vulnerability
/SYMSA19793">SYMSA19793 (Symantec Endpoint Protection Manager)

Patrick Kenna Dashboard
All Assets vulnerable to this CVE

999

Asset ID	Asset Name	Risk Meter
18322569	bamboo1.metrics.scl3.acmeinc.com	999
18322864	ganglia1.private.scl3.acmeinc.com	999
18322960	BYOB-KEYMASTER1	999
18323858	api-dev.community.scl3.acmeinc.com	999

Proof Of Concept Demo

https://0595-88-172-214-53.ngrok.io/asset?asset_id=18322960

Type here to search

77°F Sunny

ENG FR 3:44 PM 6/28/2022

Qu'elle Stratégie de Défense

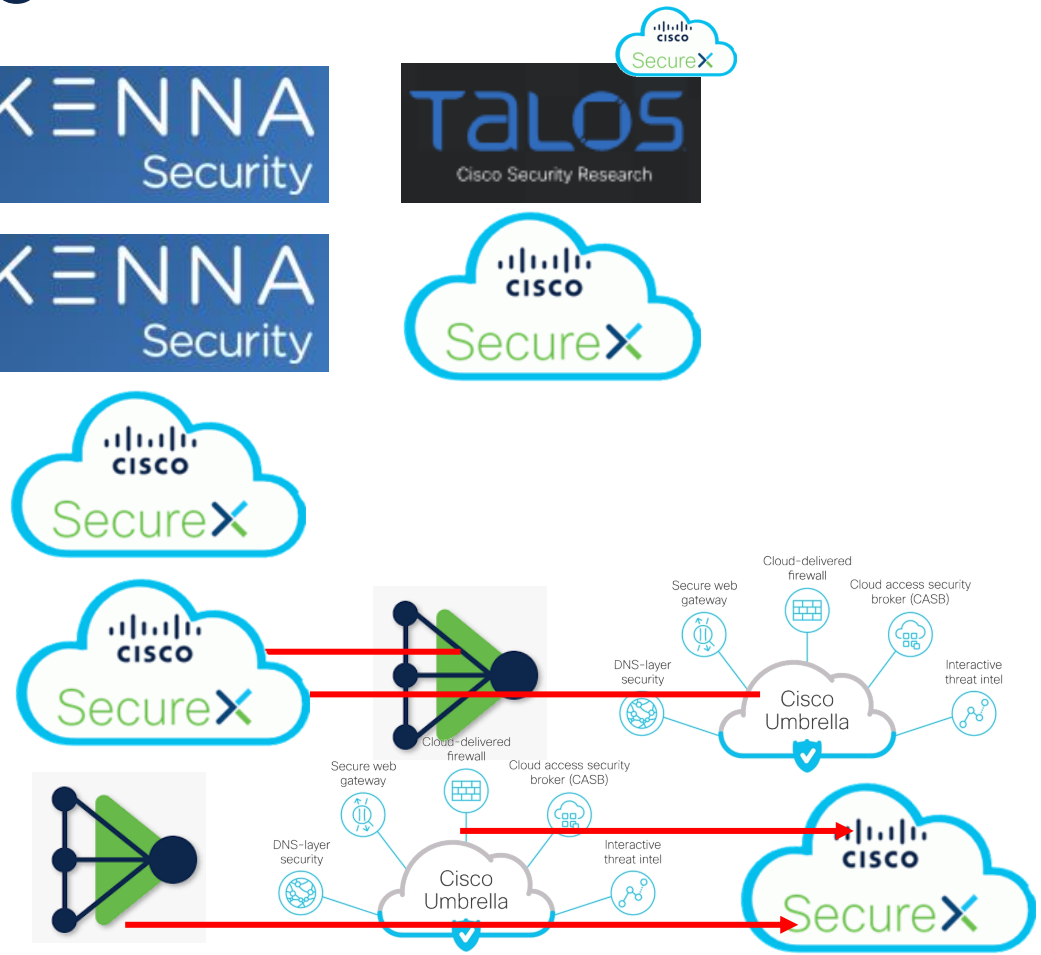
Une menace existe ?

J'ai des assets vulnérables ?

Les protections sont en place ?

Surveillance – Signaux Faibles

Détection & Réaction



Avez-vous encore des questions ?

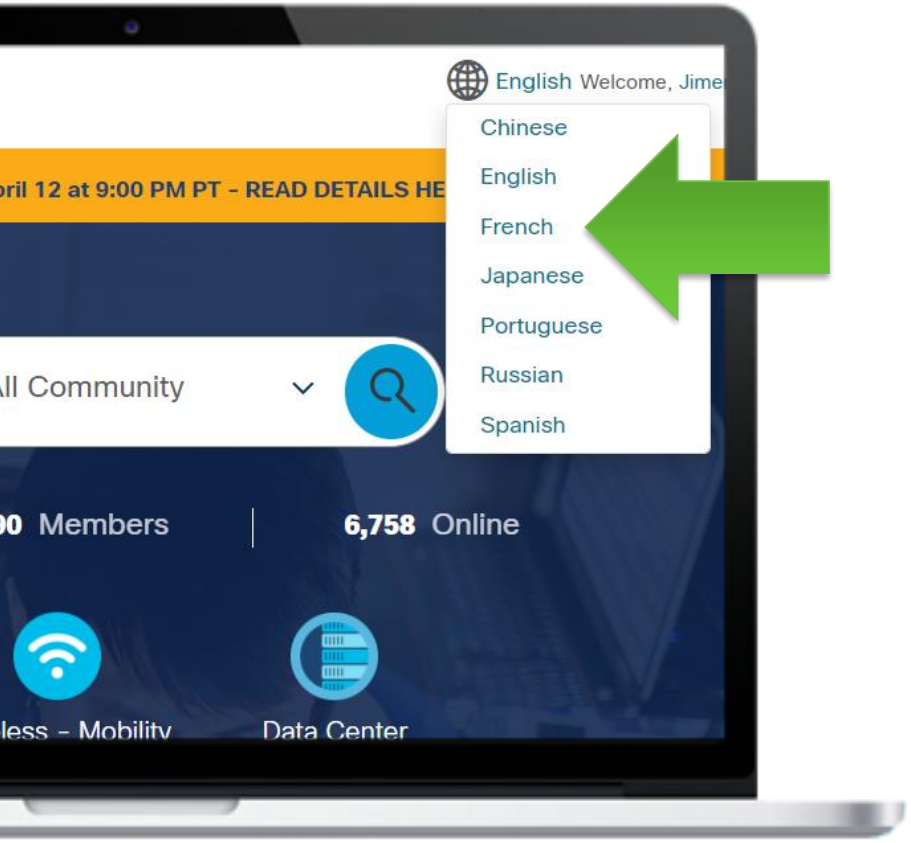
Forum Ask Me Anything

Retrouvez notre expert sur la page de Discussion

Toutes les nouvelles questions sur le sujet de ce webinaire seront répondues par la suite jusqu'à la semaine prochaine: 8 juillet, 2022.

Postez une question ici
https://bit.ly/AMA2d-jun22

Où que vous soyez restez connecté…



- Facebook [CiscoSupportCommunity]
- Twitter [@cisco_support]
- YouTube [CiscoSupportChannel]
- LinkedIn [Cisco Community]
- Instagram [CiscoSupportCommunity]

Avez-vous des commentaires ?
Répondez à notre enquête !

The bridge to possible