PHOENI2X - A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation and Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange

George Daniil

University of Patras

12/11/2024

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No101070586

Outline

- Introduction to the PHOENI2X framework
- Validation
- Highlights
- PHOENI2X in action

Outline

- Introduction to the PHOENI2X framework
- Validation
- Highlights
- PHOENI2X in action

PHOENI2X framework overview

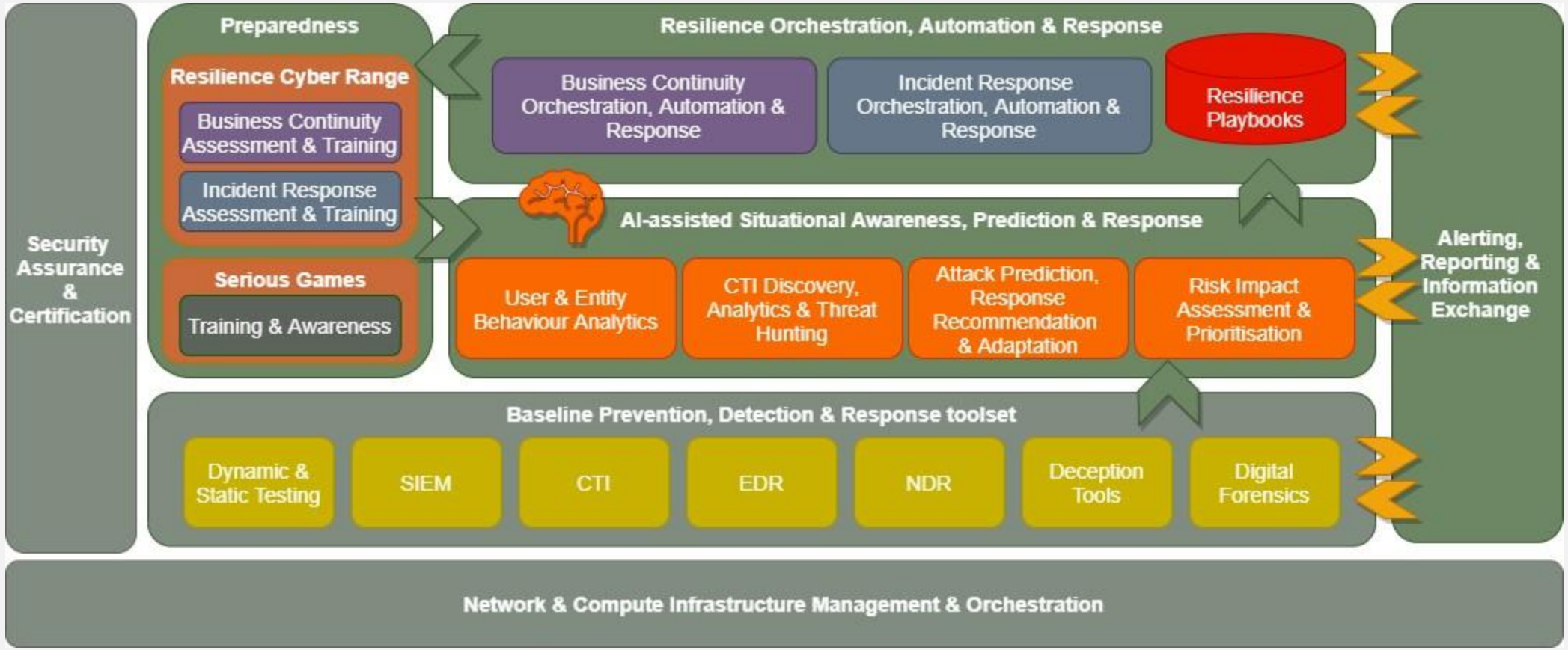
- PHOENI2X aims to design, develop, and deliver a Cyber Resilience Framework providing Artificial Intelligence (AI) - assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange
- Tailored to the needs of Operators of Essential Services (OES) and of the EU Member State (MS) National Authorities entrusted with cybersecurity.
- Aligned with the pertinent EU initiatives, such as the recommendations provided in the European Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ("Cyber Blueprint") & supporting the newly launched Cyber Crisis Liaison Organization Network (CyCLONe).

PHOENI2X will assist operators of critical sectors achieve cyber resilience & also support EU MS authorities in enhancing national cybersecurity capabilities, cross-border collaboration, and national supervision of their critical sectors, per the NIS Directive's requirements.

Key approach objectives

- Through PHOENI2X Cyber Resilience Centres (**PHOENI2X CRCs**), OES will gain:
  1) Enhanced Situational Awareness with AI-assisted Prediction, Prevention, Detection & Response capabilities, and business risk impact assessment-based prioritisation
  2) Proactive & reactive Resilience Automation, Orchestration, and Response (ROAR) mechanisms, providing Business Continuity, Recovery and Cyber & Physical Incident Response
  3) Increased Preparedness through relevant Serious Games and realistic Resilience Cyber Range (RCR) Assessment & Training
  4) Timely and actionable Information Exchange between OES, National Authorities and EU actors, leveraging interoperable and standardised alerting and reporting mechanisms and processes

PHOENI2X conceptual architecture



Baseline prevention, detection and response toolset

- Dynamic and static vulnerability testing
- Security Information and Event Management
- CTI management and sharing
- Endpoint Detection and Response
- Network Detection and Response
- Deception tools
- Forensics tools

Outline

- Introduction to the PHOENI2X framework
- Validation
- Highlights
- PHOENI2X in action

Validation

PHOENi²X CRCs validated in the context of 3 OES use cases [Objective 5]:

1. **Energy use case**, based in **Greece**, directly involving an OES (**PPC**) as well a supporting telecom provider (**COSMOTE**), and the National Authority (**NCSA**) overseeing the OES;
2. **Transport use case**, based in **Spain**, directly involving an OES (**FGC**), supported by an IoT provider (**WSE**) and;
3. **Healthcare use case**, based in **Cyprus**, involving an essential provider (**NODALPOINT**) in the supply chain of an OES (the General Healthcare System of Cyprus), and the National Authority (**DSA**) overseeing the OES.

Outline

- Introduction to the PHOENI2X framework
- Validation
- Highlights
- PHOENI2X in action

Highlights

- Integration of ≥10 prevention and detection technologies and tools, covering all the following categories: (i) Dynamic testing; (ii) Static testing; (iii) Endpoint Detection and Response (EDR); (iv) Network Detection and Response (NDR); (v) Deception tools; (vi) Digital Forensics; (vii) SIEM; (viii) CTI
  - **Completed:** 12 tools integrated, covering all categories
- Integration of CTI tools and methods collecting ≥10 technical, tactical, operational, and strategic intelligence sources
  - **Completed:** Deployment of MISP CTI platform integrating ~70 CTI sources, covering all levels of CTI information.

Highlights

- Definition of four (4) types of Business Continuity -focused RPs: (i) Proactive Business Continuity Plan (pBCP) Playbooks; (ii) Business Continuity Scenario (BCS) Playbooks; (iii) Reactive Business Continuity Plan (rBCP) Playbooks; and (iv) Disaster Recovery Plan (DRP) Playbooks.
  - **Completed:** Business Continuity Workshops to define Use Case-specific BC intricacies; Definition of high-level Business Continuity Plan activation process playbook.
- Definition of seven (7) types of Incident Response -focused RPs: (i) Prevention Playbooks; (ii) Incident Response Scenario (IRS) Playbooks; (iii) Security Assessment Playbooks; (iv) Detection Playbooks; (v) Mitigation Playbooks; (vi) Remediation Playbooks; and (vii) Investigation Playbooks.
  - **Completed:** Delivery & demonstration of first set of IR playbooks, covering categories (i)-(vi) above.

Highlights

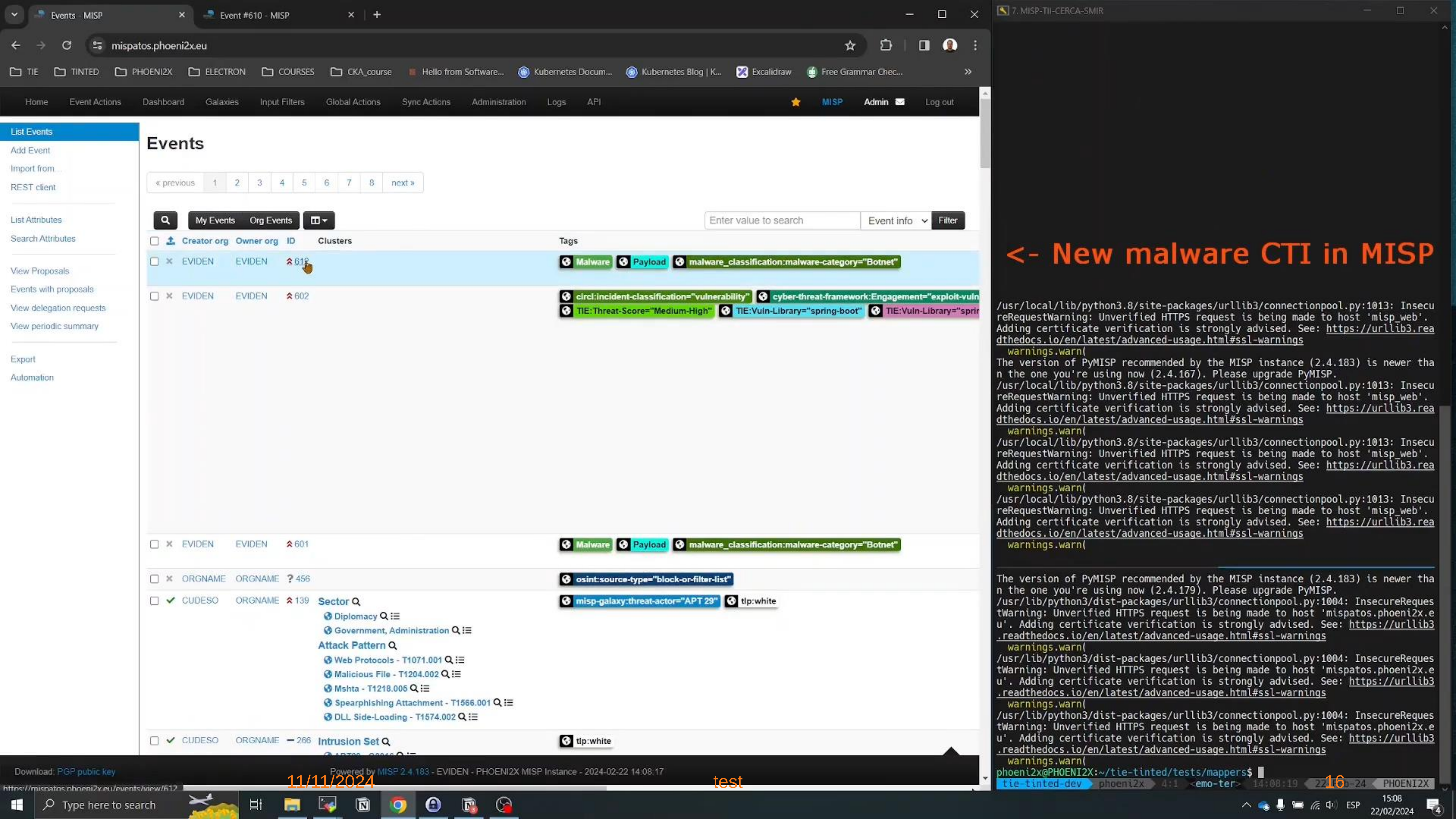
- Integration of Serious Gaming toolset for training & awareness targeting the human factor.
  - **Completed:** Development of new SG features to support integration with PHOENI2X components, also offering improvements in terms of robustness and performance; identification of relevant training scenarios for each of the use cases.
  - **Planned:** Integration of SG into PHOENI2X; Development, delivery & demonstration of PHOENI2X SG content.

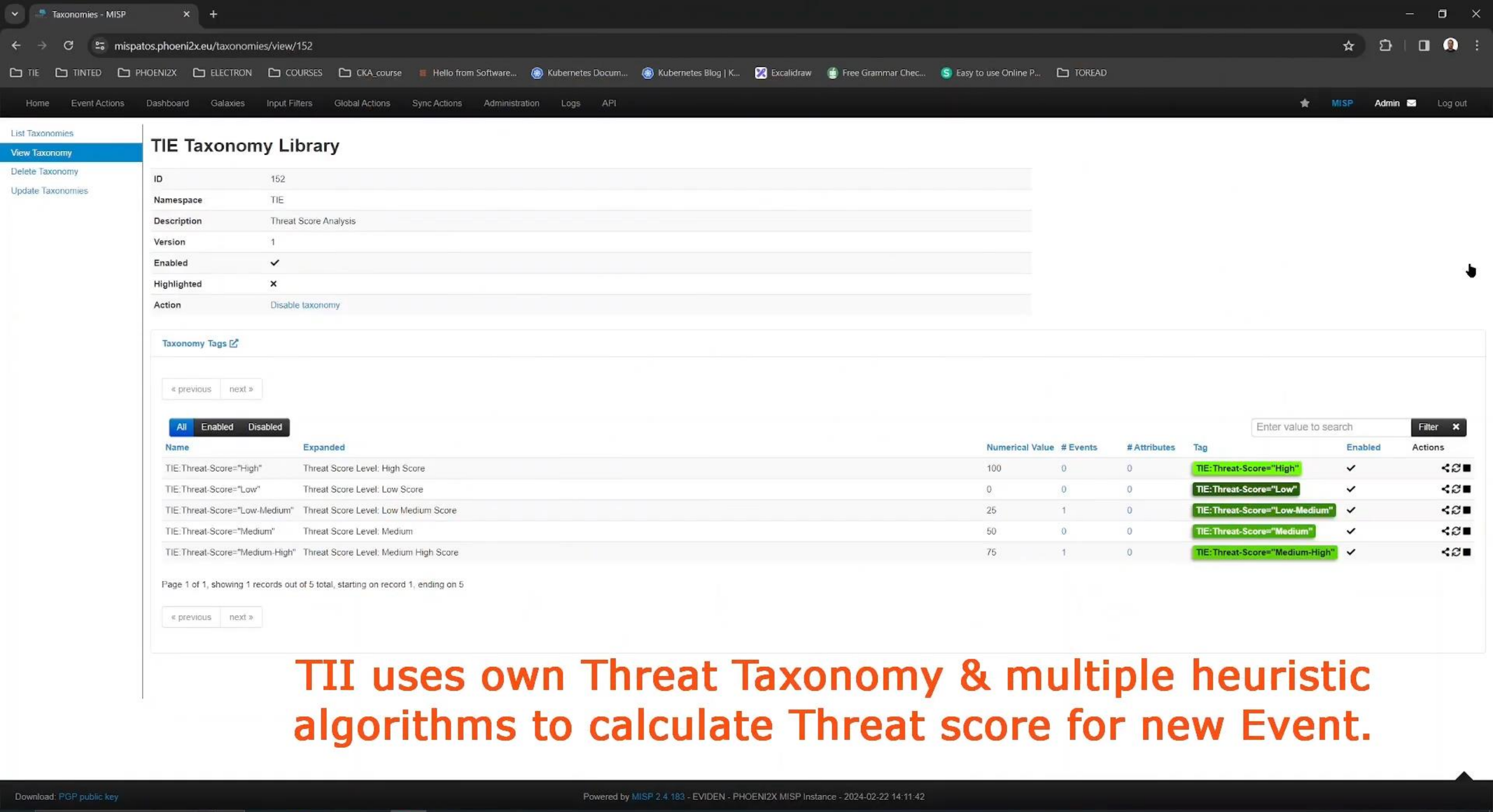
Highlights

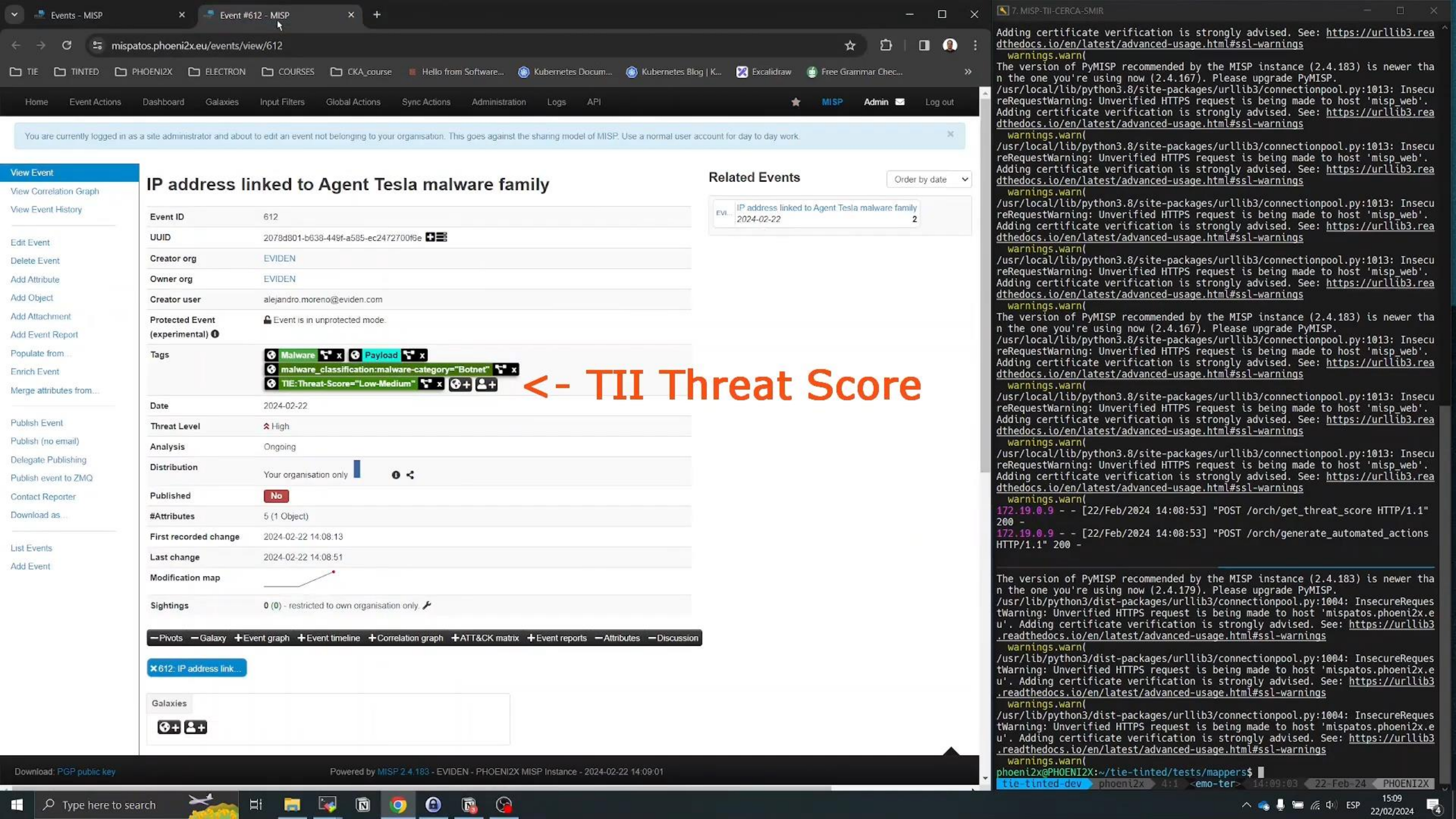
- Delivery of reporting mechanisms enabling the generation of CyCLO reports, facilitating the production of the corresponding CyCLONe national situational awareness report.
  - **Completed:** Delivery of PoC of Reporting component that can be customized to the generation of structured reports (e.g., CyCLONe report in MISP format).
  - **Planned:** (Delivery of two versions of said reporting component, demonstrating its capacity to support the generation of CyCLONe reports**.**

Outline

- Introduction to the PHOENI2X framework
- Validation
- Highlights
- PHOENI2X in action


Events - MISP
Event #610 - MISP
mispatos.phoeni2x.eu
TIE
TINTED
PHOENI2X
ELECTRON
COURSES
CKA_course
Hello from Software...
Kubernetes Docum...
Kubernetes Blog | K...
Excalidraw
Free Grammar Chec...
Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Logs
API
MISP
Admin
Log out
List Events
Add Event
Import from...
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
View periodic summary
Export
Automation
Events
« previous
1
2
3
4
5
6
7
8
next »
My Events
Org Events
Enter value to search
Event info
Filter
Creator org
Owner org
ID
Clusters
Tags
EVIDEN
EVIDEN
612
Malware
Payload
malware_classification:malware-category="Botnet"
EVIDEN
EVIDEN
602
circl:incident-classification="vulnerability"
cyber-threat-framework:Engagement="exploit-vuln
TIE:Threat-Score="Medium-High"
TIE:Vuln-Library="spring-boot"
TIE:Vuln-Library="sprir
EVIDEN
EVIDEN
601
Malware
Payload
malware_classification:malware-category="Botnet"
ORGNAME
ORGNAME
456
osint:source-type="block-or-filter-list"
CUDESO
ORGNAME
139
Sector
Diplomacy
Government, Administration
Attack Pattern
Web Protocols - T1071.001
Malicious File - T1204.002
Mshta - T1218.005
Spearphishing Attachment - T1566.001
DLL Side-Loading - T1574.002
misp-galaxy:threat-actor="APT 29"
tlp:white
CUDESO
ORGNAME
266
Intrusion Set
tlp:white
Download: PGP public key
Powered by MISP 2.4.183 - EVIDEN - PHOENI2X MISP Instance - 2024-02-22 14:08:17
https://mispatos.phoeni2x.eu/events/view/612
7. MISP-TII-CERCA-SMIR
<- New malware CTI in MISP
/usr/local/lib/python3.8/site-packages/urllib3/connectionpool.py:1013: InsecureRequestWarning: Unverified HTTPS request is being made to host 'misp_web'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
The version of PyMISP recommended by the MISP instance (2.4.183) is newer than the one you're using now (2.4.167). Please upgrade PyMISP.
/usr/local/lib/python3.8/site-packages/urllib3/connectionpool.py:1013: InsecureRequestWarning: Unverified HTTPS request is being made to host 'misp_web'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
/usr/local/lib/python3.8/site-packages/urllib3/connectionpool.py:1013: InsecureRequestWarning: Unverified HTTPS request is being made to host 'misp_web'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
/usr/local/lib/python3.8/site-packages/urllib3/connectionpool.py:1013: InsecureRequestWarning: Unverified HTTPS request is being made to host 'misp_web'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
The version of PyMISP recommended by the MISP instance (2.4.183) is newer than the one you're using now (2.4.179). Please upgrade PyMISP.
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1004: InsecureRequestWarning: Unverified HTTPS request is being made to host 'mispatos.phoeni2x.eu'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1004: InsecureRequestWarning: Unverified HTTPS request is being made to host 'mispatos.phoeni2x.eu'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1004: InsecureRequestWarning: Unverified HTTPS request is being made to host 'mispatos.phoeni2x.eu'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
phoeni2x@PHOENI2X:~/tie-tinted/tests/mappers$
tie-tinted-dev
phoeni2x
<emo-ter>
14:08:19
PHOENI2X
Type here to search
ESP
15:08
22/02/2024


Taxonomies - MISP
mispatos.phoeni2x.eu/taxonomies/view/152
Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Logs
API
MISP
Admin
Log out
List Taxonomies
View Taxonomy
Delete Taxonomy
Update Taxonomies
TIE Taxonomy Library
ID 152
Namespace TIE
Description Threat Score Analysis
Version 1
Enabled
Highlighted
Action Disable taxonomy
Taxonomy Tags
« previous
next »
All
Enabled
Disabled
Enter value to search
Filter
Name
Expanded
Numerical Value
Events
Attributes
Tag
Enabled
Actions
TIE:Threat-Score="High" Threat Score Level: High Score 100 0 0 TIE:Threat-Score="High"
TIE:Threat-Score="Low" Threat Score Level: Low Score 0 0 0 TIE:Threat-Score="Low"
TIE:Threat-Score="Low-Medium" Threat Score Level: Low Medium Score 25 1 0 TIE:Threat-Score="Low-Medium"
TIE:Threat-Score="Medium" Threat Score Level: Medium 50 0 0 TIE:Threat-Score="Medium"
TIE:Threat-Score="Medium-High" Threat Score Level: Medium High Score 75 1 0 TIE:Threat-Score="Medium-High"
Page 1 of 1, showing 1 records out of 5 total, starting on record 1, ending on 5
« previous
next »
TII uses own Threat Taxonomy & multiple heuristic algorithms to calculate Threat score for new Event.
Download: PGP public key
Powered by MISP 2.4.183 - EVIDEN - PHOENI2X MISP Instance - 2024-02-22 14:11:42
Type here to search
ESP
15:11
22/02/2024


Events - MISP
Event #612 - MISP
mispatos.phoeni2x.eu/events/view/612
TIE
TINTED
PHOENI2X
ELECTRON
COURSES
CKA_course
Hello from Software...
Kubernetes Docum...
Kubernetes Blog | K...
Excalidraw
Free Grammar Chec...
Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Logs
API
MISP
Admin
Log out
You are currently logged in as a site administrator and about to edit an event not belonging to your organisation. This goes against the sharing model of MISP. Use a normal user account for day to day work.
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...
Publish Event
Publish (no email)
Delegate Publishing
Publish event to ZMQ
Contact Reporter
Download as...
List Events
Add Event
IP address linked to Agent Tesla malware family
Event ID 612
UUID 2078d801-b638-449f-a585-ec2472700f6e
Creator org EVIDEN
Owner org EVIDEN
Creator user alejandro.moreno@eviden.com
Protected Event (experimental) Event is in unprotected mode.
Tags Malware Payload
malware_classification:malware-category="Botnet"
TIE:Threat-Score="Low-Medium"
<- TII Threat Score
Date 2024-02-22
Threat Level High
Analysis Ongoing
Distribution Your organisation only
Published No
#Attributes 5 (1 Object)
First recorded change 2024-02-22 14:08:13
Last change 2024-02-22 14:08:51
Modification map
Sightings 0 (0) - restricted to own organisation only
Pivots
Galaxy
Event graph
Event timeline
Correlation graph
ATT&CK matrix
Event reports
Attributes
Discussion
612: IP address link...
Galaxies
Related Events
Order by date
IP address linked to Agent Tesla malware family
2024-02-22
2
Download: PGP public key
Powered by MISP 2.4.183 - EVIDEN - PHOENI2X MISP Instance - 2024-02-22 14:09:01
7. MISP-TII-CERCA-SMIR
Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
The version of PyMISP recommended by the MISP instance (2.4.183) is newer than the one you're using now (2.4.167). Please upgrade PyMISP.
/usr/local/lib/python3.8/site-packages/urllib3/connectionpool.py:1013: InsecureRequestWarning: Unverified HTTPS request is being made to host 'misp_web'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
172.19.0.9 - - [22/Feb/2024 14:08:53] "POST /orch/get_threat_score HTTP/1.1" 200 -
172.19.0.9 - - [22/Feb/2024 14:08:53] "POST /orch/generate_automated_actions HTTP/1.1" 200 -
The version of PyMISP recommended by the MISP instance (2.4.183) is newer than the one you're using now (2.4.179). Please upgrade PyMISP.
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1004: InsecureRequestWarning: Unverified HTTPS request is being made to host 'mispatos.phoeni2x.eu'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings
warnings.warn(
phoeni2x@PHOENI2X:~/tie-tinted/tests/mappers$
tie-tinted-dev phoeni2x 4:1 <emo-ter> 14:09:03 22-Feb-24 PHOENI2X
Type here to search
ESP
15:09
22/02/2024

BAITING

- You find a USB drive labeled 'Employee Salary Info' in the parking lot of your energy facility
- Curiosity prompts you to plug the drive into your work computer
- The drive contains malware that immediately infects your system and spreads across the network

DEFENSE

- Do not use unknown USB drives or other media devices found in public places
- Report the found device to your IT security department
- Always have up-to-date antivirus software on your system

DEFENSE

- Never share sensitive information over the phone with unverified callers
- Request the caller's name and contact them through an official number
- Report the incident to your cybersecurity team immediately

DEFENSE

- Stop and ask the person who they are
- Ask the person to open the door with their own key card or ask for an access authorization
- If the person cannot provide evidence, ask the head office if the person is known

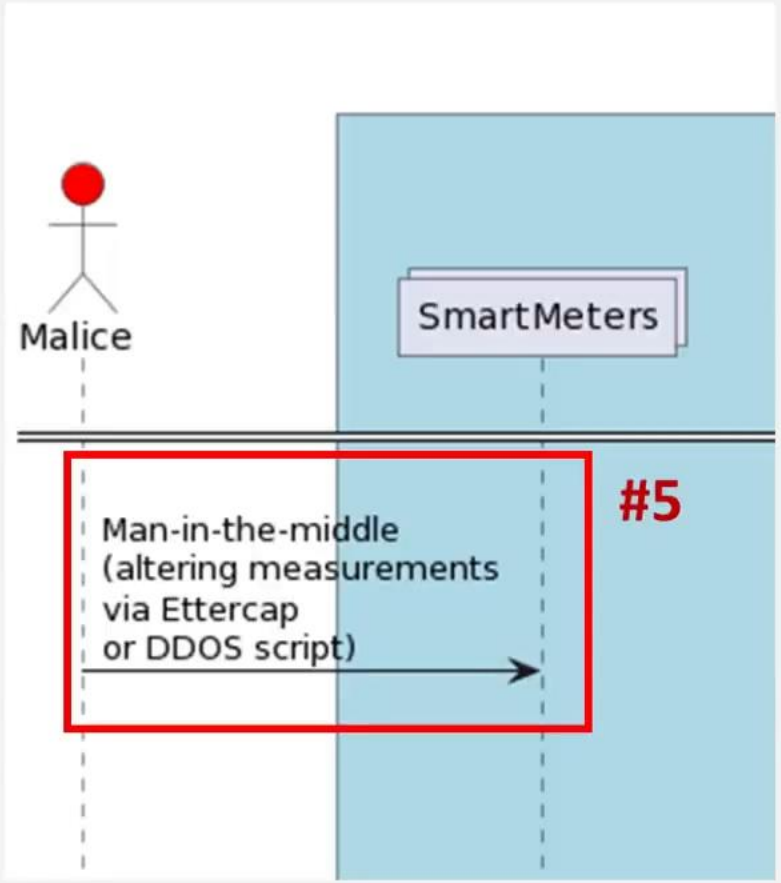
DEFENSE

- Verify the sender's email address for authenticity
- Never click on links or attachments from unsolicited emails
- Contact your energy provider through official channels if in doubt

PROTECT

Social Engineering Academy

Sub-scenario 2 – During the Attack Phase

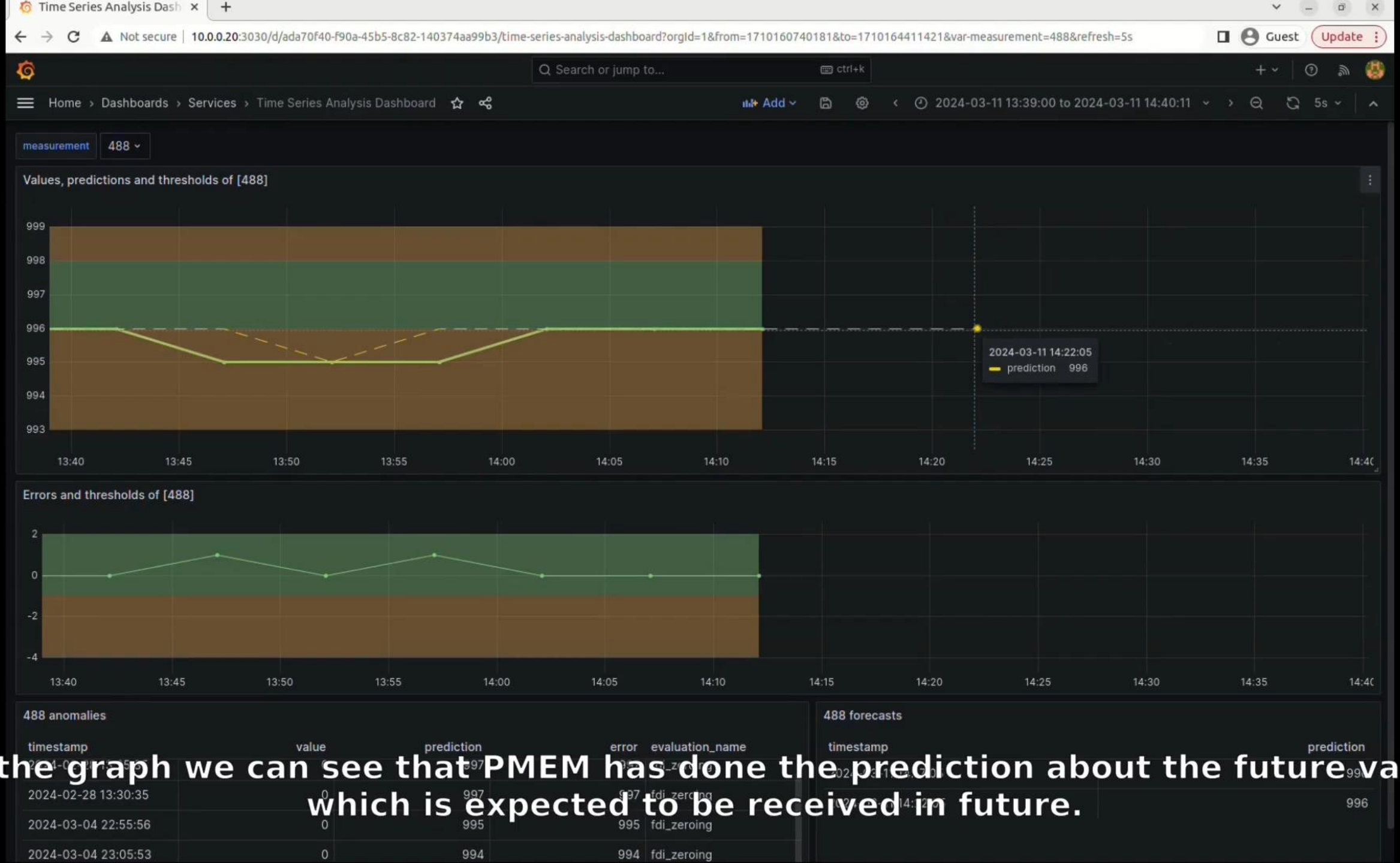


Step #5

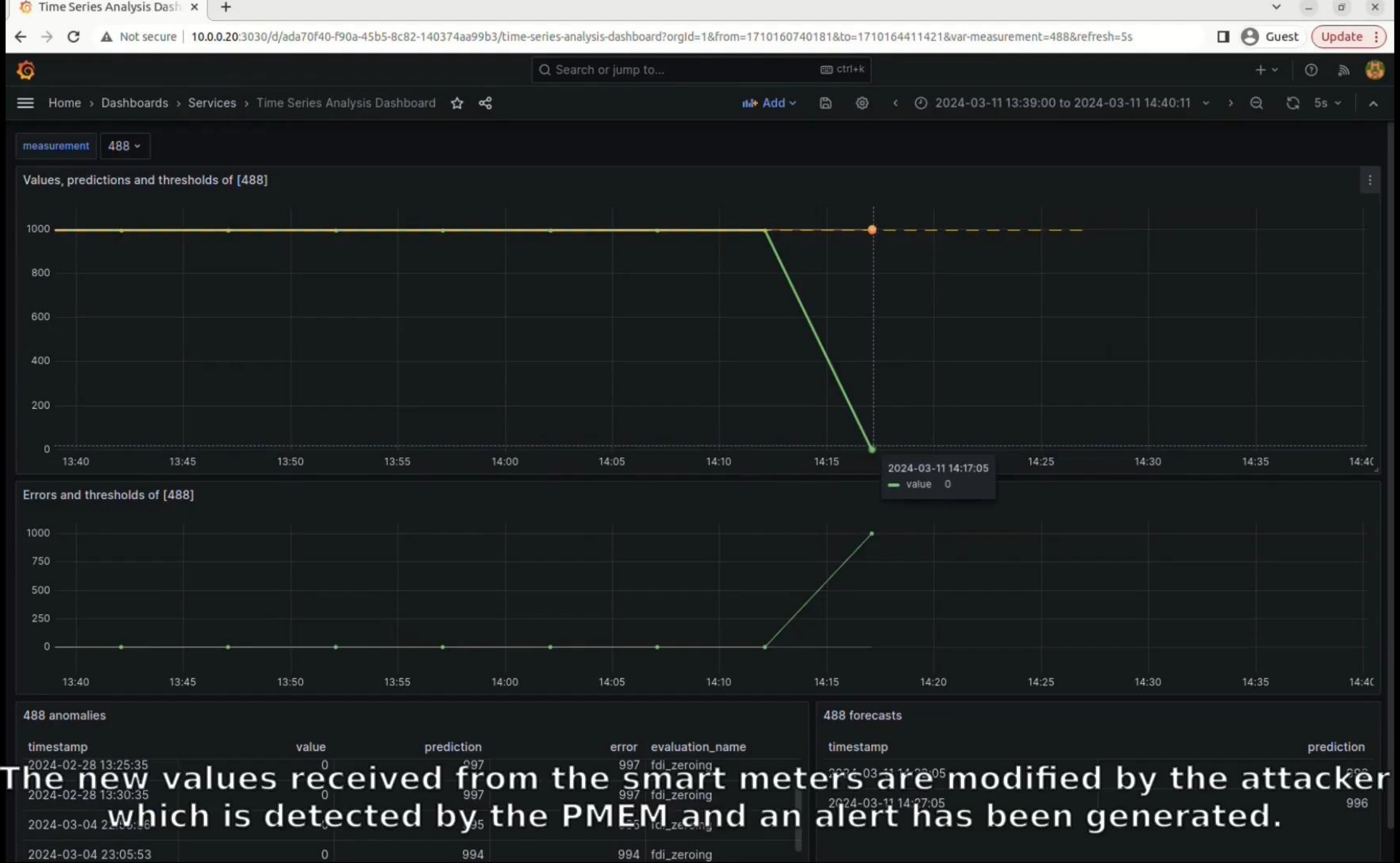
The cyberattack is implemented:

a. DLMS/COSEM ReadRequests - Switch with Heartbeat
b. DLMS/COSEM ReadRequests - Switch with other measurements
c. DLMS/COSEM ReadResponses zeroing

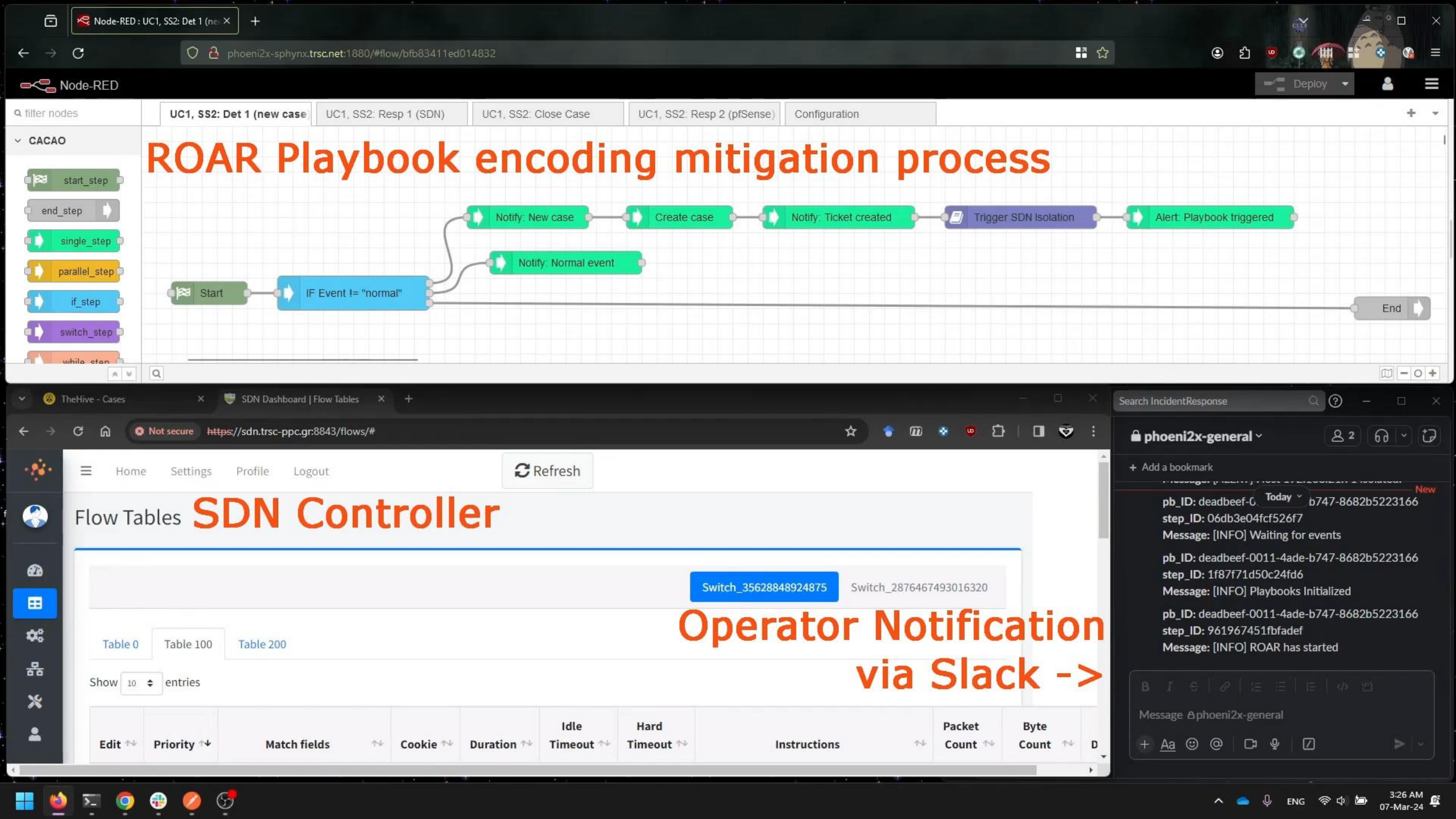
PHOENIIX

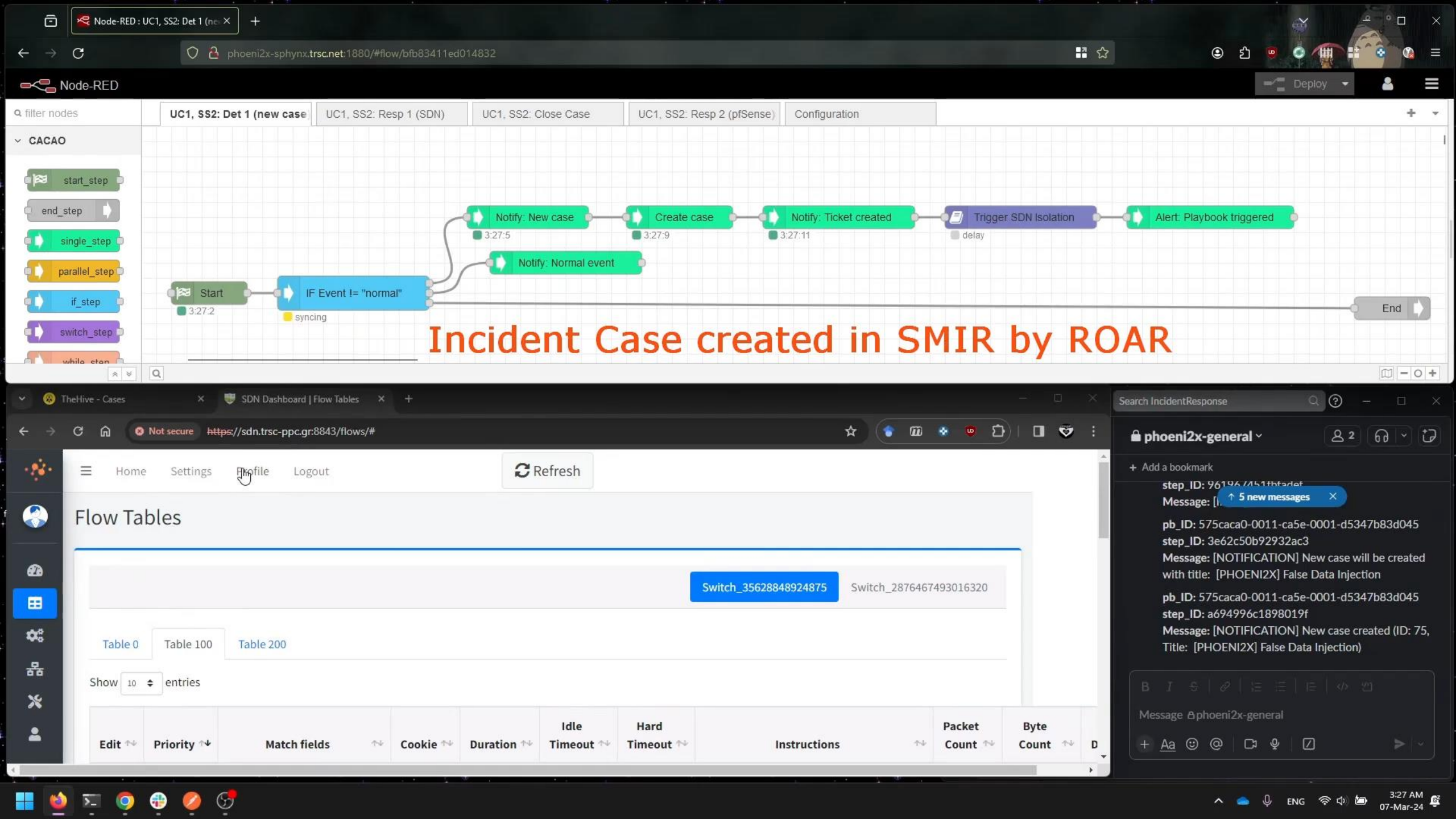


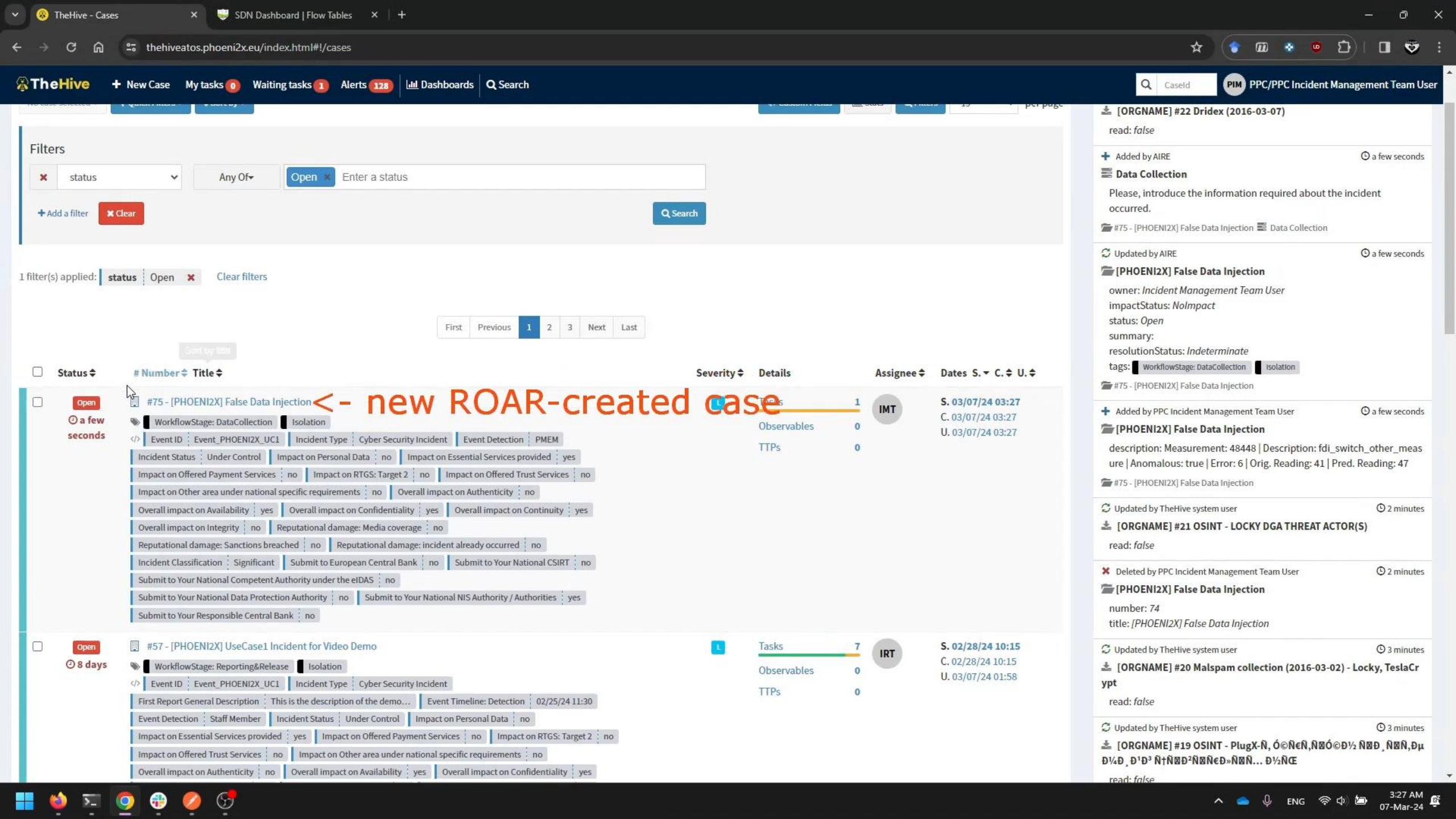
On the graph we can see that PMEM has done the prediction about the future value which is expected to be received in future.



The new values received from the smart meters are modified by the attacker which is detected by the PMEM and an alert has been generated.


Node-RED : UC1, SS2: Det 1 (ne
phoeni2x-sphynx.trsc.net:1880/#flow/bfb83411ed014832
Node-RED
Deploy
filter nodes
UC1, SS2: Det 1 (new case
UC1, SS2: Resp 1 (SDN)
UC1, SS2: Close Case
UC1, SS2: Resp 2 (pfSense)
Configuration
CACAO
start_step
end_step
single_step
parallel_step
if_step
switch_step
ROAR Playbook encoding mitigation process
Notify: New case
Create case
Notify: Ticket created
Trigger SDN Isolation
Alert: Playbook triggered
Notify: Normal event
Start
IF Event != "normal"
End
TheHive - Cases
SDN Dashboard | Flow Tables
Not secure
https://sdn.trsc-ppc.gr:8843/flows/#
Home
Settings
Profile
Logout
Refresh
Flow Tables
SDN Controller
Switch_35628848924875
Switch_2876467493016320
Table 0
Table 100
Table 200
Show 10 entries
Edit
Priority
Match fields
Cookie
Duration
Idle Timeout
Hard Timeout
Instructions
Packet Count
Byte Count
Search IncidentResponse
phoeni2x-general
Add a bookmark
Today
New
pb_ID: deadbeef-0
b747-8682b5223166
step_ID: 06db3e04fcf526f7
Message: [INFO] Waiting for events
pb_ID: deadbeef-0011-4ade-b747-8682b5223166
step_ID: 1f87f71d50c24fd6
Message: [INFO] Playbooks Initialized
pb_ID: deadbeef-0011-4ade-b747-8682b5223166
step_ID: 961967451fbfadef
Message: [INFO] ROAR has started
Operator Notification via Slack ->
Message phoeni2x-general
ENG
3:26 AM
07-Mar-24


Node-RED : UC1, SS2: Det 1 (ne
phoeni2x-sphynx.trsc.net:1880/#flow/bfb83411ed014832
Node-RED
Deploy
filter nodes
UC1, SS2: Det 1 (new case
UC1, SS2: Resp 1 (SDN)
UC1, SS2: Close Case
UC1, SS2: Resp 2 (pfSense)
Configuration
CACAO
start_step
end_step
single_step
parallel_step
if_step
switch_step
Notify: New case
3:27:5
Create case
3:27:9
Notify: Ticket created
3:27:11
Trigger SDN Isolation
delay
Alert: Playbook triggered
Notify: Normal event
Start
3:27:2
IF Event != "normal"
syncing
End
Incident Case created in SMIR by ROAR
TheHive - Cases
SDN Dashboard | Flow Tables
Not secure
https://sdn.trsc-ppc.gr:8843/flows/#
Home
Settings
Profile
Logout
Refresh
Flow Tables
Switch_35628848924875
Switch_2876467493016320
Table 0
Table 100
Table 200
Show 10 entries
Edit
Priority
Match fields
Cookie
Duration
Idle Timeout
Hard Timeout
Instructions
Packet Count
Byte Count
Search IncidentResponse
phoeni2x-general
Add a bookmark
5 new messages
pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: 3e62c50b92932ac3
Message: [NOTIFICATION] New case will be created with title: [PHOENI2X] False Data Injection
pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: a694996c1898019f
Message: [NOTIFICATION] New case created (ID: 75, Title: [PHOENI2X] False Data Injection)
Message phoeni2x-general
ENG
3:27 AM
07-Mar-24


TheHive - Cases
SDN Dashboard | Flow Tables
thehiveatos.phoeni2x.eu/index.html#!/cases
TheHive
New Case
My tasks 0
Waiting tasks 1
Alerts 128
Dashboards
Search
CaseId
PIM PPC/PPC Incident Management Team User
Filters
status
Any Of
Open
Enter a status
Add a filter
Clear
Search
1 filter(s) applied: status Open
Clear filters
First Previous 1 2 3 Next Last
Status
Number
Title
Severity
Details
Assignee
Dates S. C. U.
Open
a few seconds
#75 - [PHOENI2X] False Data Injection
<- new ROAR-created case
WorkflowStage: DataCollection
Isolation
Event ID Event_PHOENI2X_UC1
Incident Type Cyber Security Incident
Event Detection PMEM
Incident Status Under Control
Impact on Personal Data no
Impact on Essential Services provided yes
Impact on Offered Payment Services no
Impact on RTGS: Target 2 no
Impact on Offered Trust Services no
Impact on Other area under national specific requirements no
Overall impact on Authenticity no
Overall impact on Availability yes
Overall impact on Confidentiality yes
Overall impact on Continuity yes
Overall impact on Integrity no
Reputational damage: Media coverage no
Reputational damage: Sanctions breached no
Reputational damage: incident already occurred no
Incident Classification Significant
Submit to European Central Bank no
Submit to Your National CSIRT no
Submit to Your National Competent Authority under the eIDAS no
Submit to Your National Data Protection Authority no
Submit to Your National NIS Authority / Authorities yes
Submit to Your Responsible Central Bank no
Tasks 1
Observables 0
TTPs 0
IMT
S. 03/07/24 03:27
C. 03/07/24 03:27
U. 03/07/24 03:27
Open
8 days
#57 - [PHOENI2X] UseCase1 Incident for Video Demo
WorkflowStage: Reporting&Release
Isolation
Event ID Event_PHOENI2X_UC1
Incident Type Cyber Security Incident
First Report General Description This is the description of the demo...
Event Timeline: Detection 02/25/24 11:30
Event Detection Staff Member
Incident Status Under Control
Impact on Personal Data no
Impact on Essential Services provided yes
Impact on Offered Payment Services no
Impact on RTGS: Target 2 no
Impact on Offered Trust Services no
Impact on Other area under national specific requirements no
Overall impact on Authenticity no
Overall impact on Availability yes
Overall impact on Confidentiality yes
Tasks 7
Observables 0
TTPs 0
IRT
S. 02/28/24 10:15
C. 02/28/24 10:15
U. 03/07/24 01:58
[ORGNAME] #22 Dridex (2016-03-07)
read: false
Added by AIRE
a few seconds
Data Collection
Please, introduce the information required about the incident occurred.
#75 - [PHOENI2X] False Data Injection
Data Collection
Updated by AIRE
a few seconds
[PHOENI2X] False Data Injection
owner: Incident Management Team User
impactStatus: NoImpact
status: Open
summary:
resolutionStatus: Indeterminate
tags: WorkflowStage: DataCollection
Isolation
#75 - [PHOENI2X] False Data Injection
Added by PPC Incident Management Team User
a few seconds
[PHOENI2X] False Data Injection
description: Measurement: 48448 | Description: fdi_switch_other_measure | Anomalous: true | Error: 6 | Orig. Reading: 41 | Pred. Reading: 47
#75 - [PHOENI2X] False Data Injection
Updated by TheHive system user
2 minutes
[ORGNAME] #21 OSINT - LOCKY DGA THREAT ACTOR(S)
read: false
Deleted by PPC Incident Management Team User
2 minutes
[PHOENI2X] False Data Injection
number: 74
title: [PHOENI2X] False Data Injection
Updated by TheHive system user
3 minutes
[ORGNAME] #20 Malspam collection (2016-03-02) - Locky, TeslaCrypt
read: false
Updated by TheHive system user
3 minutes
[ORGNAME] #19 OSINT - PlugX-Ñ, Ó©Ñ€Ñ,ÑØÓ©Đ½ ÑØĐ¸ÑØÑ,Đµ Đ¼Đ¸Đ³ Ñ†ÑØĐ²ÑØÑ€Đ»ÑØÑ... Đ½ÑŒ
read: false
ENG
3:27 AM
07-Mar-24

TheHive - Case #75: [PHOENI2X] | SDN Dashboard | Flow Tables

thehiveatos.phoeni2x.eu/index.html#!/case/~~2009817208/details

TheHive | + New Case | My tasks 0 | Waiting tasks 1 | Alerts 128 | Dashboards | Search | CaseId | PIM PPC/PPC Incident Management Team User

Case # 75 - [PHOENI2X] False Data Injection

PPC Incident Management Team User | 03/07/24 03:27 | a few seconds | Sharing (0) | Close | Flag | Merge | Remove | Export (0)

Details | Tasks 1 | Observables 0 | TTPs

Basic Information

Title	[PHOENI2X] False Data Injection
Severity	L
TLP	TLP:WHITE
PAP	PAP:WHITE
Assignee	Incident Management Team User
Date	03/07/24 03:27
Tags	WorkflowStage: DataCollection, Isolation

Additional information

+Add | Layout

Event ID	Event_PHOENI2X_UC1	**Incident Type**	Cyber Security Incident	**Event Detection**	PMEM
Incident Status	Under Control	**Impact on Personal Data**	no	**Impact on Essential Services ...**	yes
Impact on Offered Payment ...	no	**Impact on RTGS: Target 2**	no	**Impact on Offered Trust Serv...**	no
Impact on Other area under ...	no	**Overall impact on Authenticity**	no	**Overall impact on Availability**	yes
Overall impact on Confidenti...	yes	**Overall impact on Continuity**	yes	**Overall impact on Integrity**	no
Reputational damage: Media...	no	**Reputational damage: Sancti...**	no	**Reputational damage: incide...**	no
Incident Classification	Significant	**Submit to European Central ...**	no	**Submit to Your National CSIRT**	no
Submit to Your National Com...	no	**Submit to Your National Data...**	no	**Submit to Your National NIS ...**	yes

Open in new window | Hide

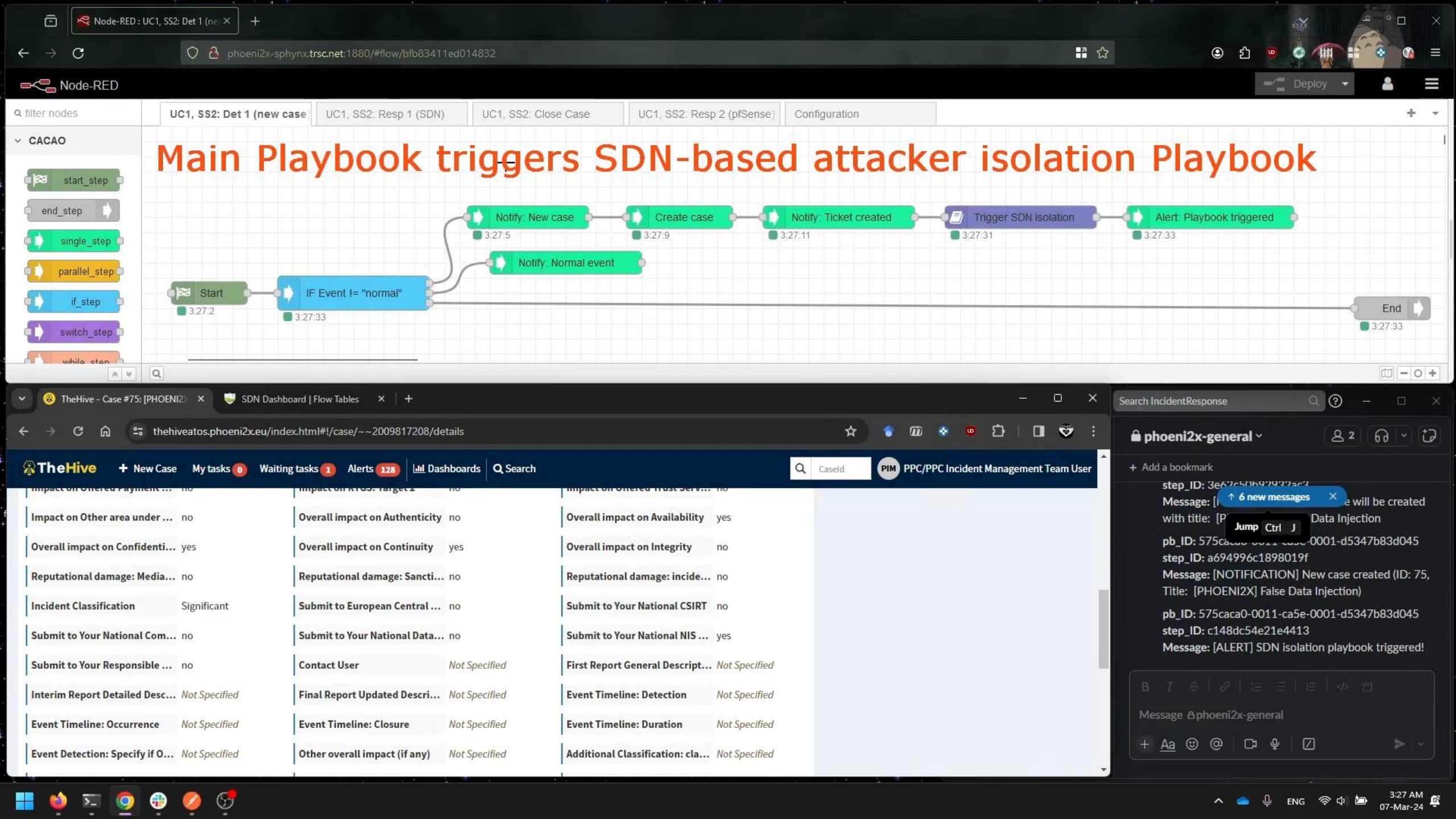
Updated by AIRE — a few seconds
[PHOENI2X] False Data Injection
owner: *Incident Management Team User*
impactStatus: *NoImpact*
status: *Open*
summary:
resolutionStatus: *Indeterminate*
tags: WorkflowStage: DataCollection, Isolation
#75 - [PHOENI2X] False Data Injection

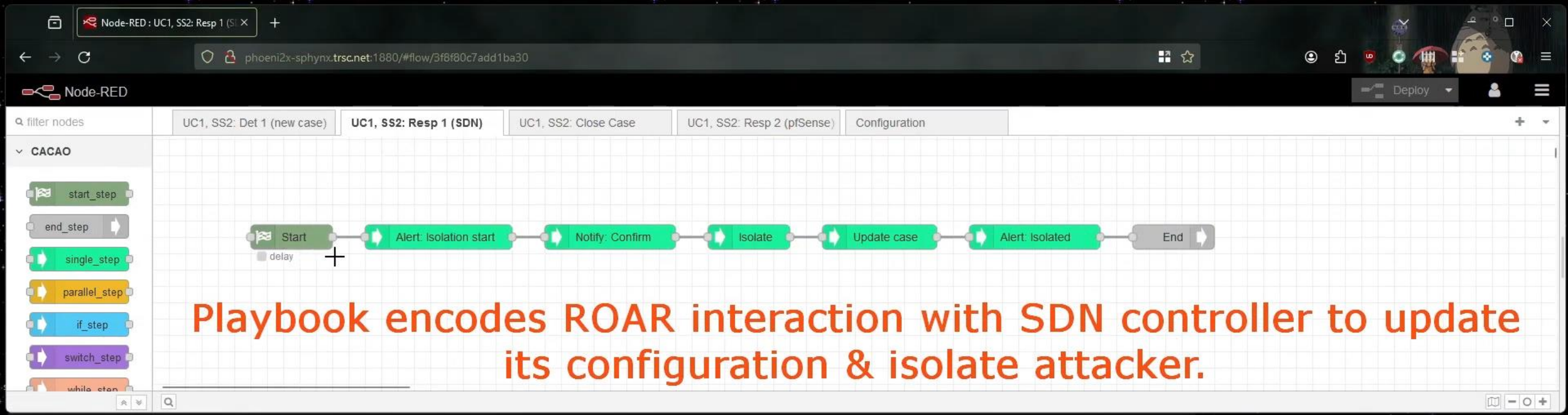
Added by AIRE — a few seconds
Data Collection
Please, introduce the information required about the incident occurred.
#75 - [PHOENI2X] False Data Injection | Data Collection

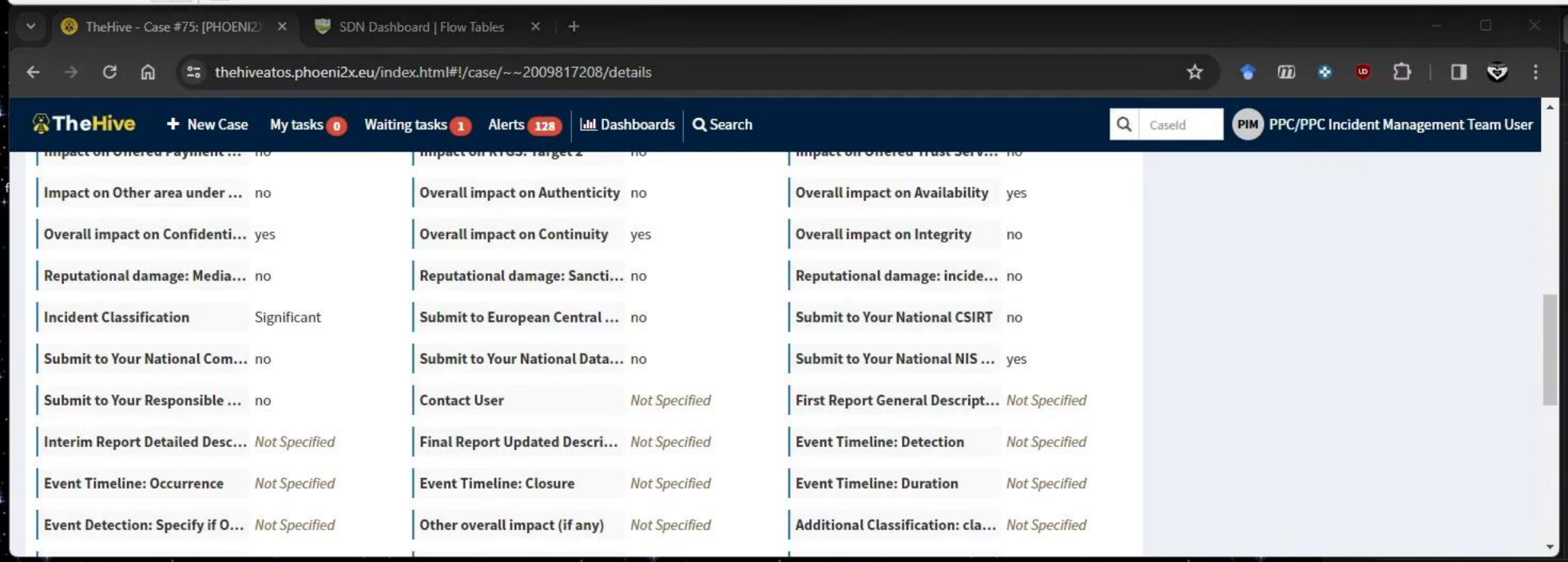
Added by PPC Incident Management Team User — a few seconds
[PHOENI2X] False Data Injection
description: Measurement: 48448 | Description: fdi_switch_other_measure | Anomalous: true | Error: 6 | Orig. Reading: 41 | Pred. Reading: 47
#75 - [PHOENI2X] False Data Injection

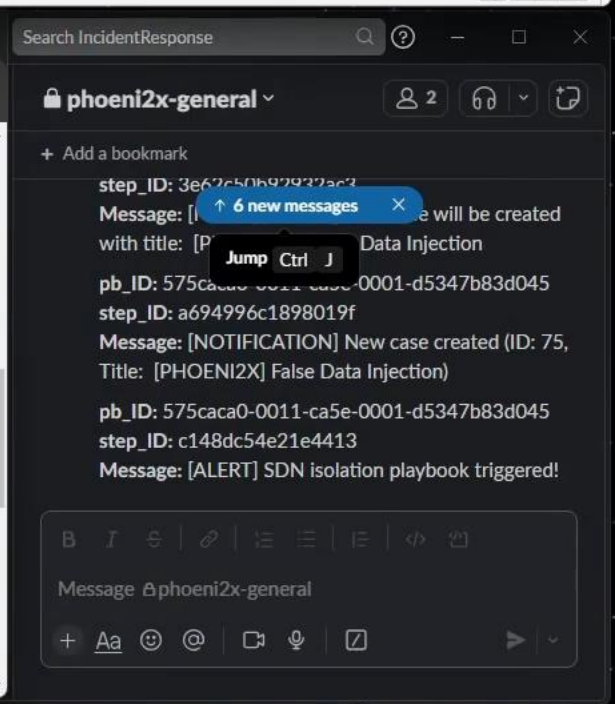
Viewing Incident Case details in SMIR (as encoded by ROAR)

ENG 3:27 AM 07-Mar-24


Node-RED : UC1, SS2: Det 1 (ne
phoeni2x-sphynx.trsc.net:1880/#flow/bfb83411ed014832
Node-RED
Deploy
filter nodes
UC1, SS2: Det 1 (new case
UC1, SS2: Resp 1 (SDN)
UC1, SS2: Close Case
UC1, SS2: Resp 2 (pfSense)
Configuration
CACAO
start_step
end_step
single_step
parallel_step
if_step
switch_step
Main Playbook triggers SDN-based attacker isolation Playbook
Notify: New case
3:27:5
Create case
3:27:9
Notify: Ticket created
3:27:11
Trigger SDN Isolation
3:27:31
Alert: Playbook triggered
3:27:33
Notify: Normal event
Start
3:27:2
IF Event != "normal"
3:27:33
End
3:27:33
TheHive - Case #75: [PHOENI2
SDN Dashboard | Flow Tables
thehiveatos.phoeni2x.eu/index.html#!/case/~~2009817208/details
TheHive
New Case
My tasks 0
Waiting tasks 1
Alerts 128
Dashboards
Search
CaseId
PIM
PPC/PPC Incident Management Team User
Impact on Other area under ... no
Overall impact on Authenticity no
Overall impact on Availability yes
Overall impact on Confidenti... yes
Overall impact on Continuity yes
Overall impact on Integrity no
Reputational damage: Media... no
Reputational damage: Sancti... no
Reputational damage: incide... no
Incident Classification Significant
Submit to European Central ... no
Submit to Your National CSIRT no
Submit to Your National Com... no
Submit to Your National Data... no
Submit to Your National NIS ... yes
Submit to Your Responsible ... no
Contact User Not Specified
First Report General Descript... Not Specified
Interim Report Detailed Desc... Not Specified
Final Report Updated Descri... Not Specified
Event Timeline: Detection Not Specified
Event Timeline: Occurrence Not Specified
Event Timeline: Closure Not Specified
Event Timeline: Duration Not Specified
Event Detection: Specify if O... Not Specified
Other overall impact (if any) Not Specified
Additional Classification: cla... Not Specified
Search IncidentResponse
phoeni2x-general
Add a bookmark
6 new messages
Jump Ctrl J
Data Injection
pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: a694996c1898019f
Message: [NOTIFICATION] New case created (ID: 75, Title: [PHOENI2X] False Data Injection)
pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: c148dc54e21e4413
Message: [ALERT] SDN isolation playbook triggered!
Message phoeni2x-general
ENG
3:27 AM
07-Mar-24


Node-RED : UC1, SS2: Resp 1 (SDN)
phoeni2x-sphynx.trsc.net:1880/#flow/3f8f80c7add1ba30
Node-RED
Deploy
filter nodes
UC1, SS2: Det 1 (new case)
UC1, SS2: Resp 1 (SDN)
UC1, SS2: Close Case
UC1, SS2: Resp 2 (pfSense)
Configuration
CACAO
start_step
end_step
single_step
parallel_step
if_step
switch_step
Start
delay
Alert: Isolation start
Notify: Confirm
Isolate
Update case
Alert: Isolated
End
Playbook encodes ROAR interaction with SDN controller to update its configuration & isolate attacker.


TheHive - Case #75: [PHOENI2
SDN Dashboard | Flow Tables
thehiveatos.phoeni2x.eu/index.html#!/case/~~2009817208/details
TheHive
New Case
My tasks 0
Waiting tasks 1
Alerts 128
Dashboards
Search
CaseId
PIM
PPC/PPC Incident Management Team User
Impact on Other area under ... no
Overall impact on Confidenti... yes
Reputational damage: Media... no
Incident Classification Significant
Submit to Your National Com... no
Submit to Your Responsible ... no
Interim Report Detailed Desc... Not Specified
Event Timeline: Occurrence Not Specified
Event Detection: Specify if O... Not Specified
Overall impact on Authenticity no
Overall impact on Continuity yes
Reputational damage: Sancti... no
Submit to European Central ... no
Submit to Your National Data... no
Contact User Not Specified
Final Report Updated Descri... Not Specified
Event Timeline: Closure Not Specified
Other overall impact (if any) Not Specified
Overall impact on Availability yes
Overall impact on Integrity no
Reputational damage: incide... no
Submit to Your National CSIRT no
Submit to Your National NIS ... yes
First Report General Descript... Not Specified
Event Timeline: Detection Not Specified
Event Timeline: Duration Not Specified
Additional Classification: cla... Not Specified


Search IncidentResponse
phoeni2x-general
Add a bookmark
6 new messages
Jump Ctrl J
step_ID: 3e62c50b92932ac3
Message: [e will be created with title: [P Data Injection
pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: a694996c1898019f
Message: [NOTIFICATION] New case created (ID: 75, Title: [PHOENI2X] False Data Injection)
pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: c148dc54e21e4413
Message: [ALERT] SDN isolation playbook triggered!
Message phoeni2x-general

Search IncidentResponse

IncidentResponse

Drafts & sent

Channels
- general
- intelliot-general
- intelliot-reports
- **ir-bot**
- jcop-general
- jcop-reports
- phoeni2x-general
- phoeni2x-reports
- random
- sts-cyber-range
- **sts-general**
- sts-reports

Add channels

Direct messages

Apps

Home DMs Activity More

phoeni2x-general

2 Canvas

Add a bookmark

Today

pb_ID: deadbeef-0011-4ade-b747-8682b5223166
step_ID: 06db3e04fcf526f7
Message: [INFO] Waiting for events

pb_ID: deadbeef-0011-4ade-b747-8682b5223166
step_ID: 1f87f71d50c24fd6
Message: [INFO] Playbooks Initialized

pb_ID: deadbeef-0011-4ade-b747-8682b5223166
step_ID: 961967451fbfadef
Message: [INFO] ROAR has started

New

pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: 3e62c50b92932ac3
Message: [NOTIFICATION] New case will be created with title: [PHOENI2X] False Data Injection

pb_ID: 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: a694996c1898019f
Message: [NOTIFICATION] New case created (ID: 75, Title: [PHOENI2X] False Data Injection)

3:27 **pb_ID:** 575caca0-0011-ca5e-0001-d5347b83d045
step_ID: c148dc54e21e4413
Message: [ALERT] SDN isolation playbook triggered!

pb_ID: 575caca0-0011-ca5e-0001-31cde725836f
step_ID: 9f58642ec0feadba
Message: [ALERT] Host isolation has started (SDN)

pb_ID: 575caca0-0011-ca5e-0001-31cde725836f
step_ID: 81db2c2282693331
Message: [NOTIFICATION] Host 192.168.21.91 will be isolated

pb_ID: 575caca0-0011-ca5e-0001-31cde725836f
step_ID: 1fa77e910834c77c
Message: [ALERT] Case updated!

pb_ID: 575caca0-0011-ca5e-0001-31cde725836f
step_ID: 1fa77e910834c77c
Message: [ALERT] Host 192.168.21.91 isolated!

Message phoeni2x-general

Detailed notification for all actions on Operator's Slack Channel

ENG 3:28 AM 07-Mar-24

Assets Aggregated Statistics

Alerts	Playbooks	Smart Meter Logs	PMEM events
17	1	3691	632117

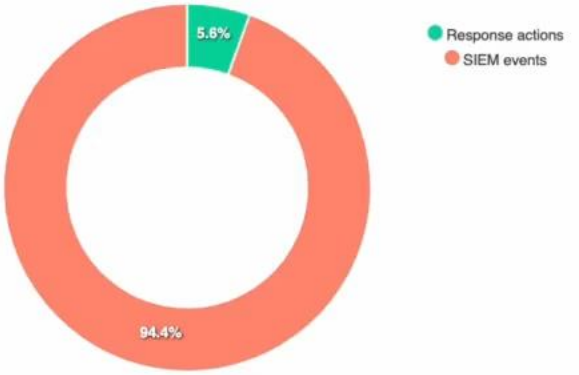
SIEM monitoring (Latest)

Filter

Agent_name	Rule_description	Timestamp	Actions
phoeni2x-siem	System user successfully logged to the system.	19/03/2024, 17:40:24	
phoeni2x-siem	System user successfully logged to the system.	19/03/2024, 17:40:24	
phoeni2x-siem	System user successfully logged to the system.	19/03/2024, 17:40:24	
phoeni2x-siem	sshd: Attempt to login using a non-existent user	19/03/2024, 17:40:06	
phoeni2x-siem	sshd: Attempt to login using a non-existent user	19/03/2024, 17:40:00	

Items per page: 5 1 – 5 of 500

Mitigation actions

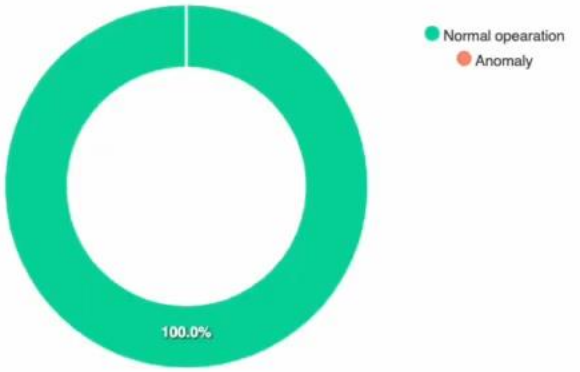


Predictive Maintenance Events (Latest)

Filter

Ami_measurement	Prediction	Original	Description	Timestamp
13208	1120270376	1179470661	normal	23/02/2024, 07:23:41
12504	106875310	106875310	normal	23/02/2024, 07:23:41
9872	778743693	842710733	normal	23/02/2024, 07:23:41
9696	673701542	737104651	normal	23/02/2024, 07:23:41
9520	58116955	58116955	normal	23/02/2024, 07:23:41

Overal Operation (%)



PHOENIIX

Overview | Incident Handling | Use Case 1: Energy

Overview & Features | Internal Incidents Insights | External Incidents Insights | FVT

> Feature: 3 | **Incident Response**

Filters Bar

Severity: Select Severity(ies)

Choose start date: 01/06/2023, 15:21:19

Choose end date: 19/03/2024, 17:42:03

Search | Get Latest

Widgets Bar

Viewing ROAR events (playbook actions) on FVT

Temporal Representation (Playbook execution) ⓘ Alert Message

Playbook start · Playbook step · Playbook finish

	2023							2024		
	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
Playbooks								PLAYBOOK_START STEP_TRIGGERED STEP_EXECUTING STEP_TRIGGERED STEP_FINISHED Step on: 1000 ms del...		

Temporal Representation (Event) ⓘ

Filter

Playbook	Step	Step_id	Level	Message	Timestamp	Related_threat	Actions
575caca0-0011-ca5e-0001-d5347b83d045	Start	26de81f14625771c	1	PLAYBOOK_START	25/01/2024, 11:32:25	Threat	
575caca0-0011-ca5e-0001-d5347b83d045	Start	26de81f14625771c	1	STEP_TRIGGERED	25/01/2024, 11:32:25	Threat	
575caca0-0011-ca5e-0001-d5347b83d045	Start	26de81f14625771c	1	STEP_EXECUTING	25/01/2024, 11:32:25	Threat	
575caca0-0011-ca5e-0001-d5347b83d045	Notify: New case	3e62c50b92932ac3	1	STEP_TRIGGERED	25/01/2024, 11:32:25	Threat	

(irt_ppc@dei.gr)

User Profile | Incident Management | Incidents Additional Info | Reports | Help

Converting information to pre-defined formats/templates

Incident Reports registered in the Incident Reporting Smart Engine:

Summary | Ready ManagerialJudgement | Ready DataConversion | Ready Green-lightReporting | Ready Reporting | Reported | All

Incident	Type	Status	Phase	IR Workflow	Registration Date
2020_365_ENTITY_001	Unknown	In progress	M1	DataCollection	Feb. 26, 2024, 11:57 a.m.
2020_365_ENTITY_001	Unknown	In progress	M1	DataCollection	Feb. 26, 2024, 12:12 p.m.
Event_PHOENI2X_UC1	Cyber Security Incident	In progress	M1	DataConversion	Feb. 28, 2024, 8:15 a.m.
PHOENI2X_UC2_1	Cyber Security Incident	In progress	M1	DataConversion	Jan. 18, 2024, 8:26 a.m.
2020_365_ENTITY_001	Unknown	In progress	M1	DataCollection	Jan. 18, 2024, 12:05 p.m.
2020_365_ENTITY_001	Unknown	In progress	M1	DataCollection	Jan. 18, 2024, 12:07 p.m.

following definition applies, inter alia:

> *"**Event**": any incident that actually has an adverse effect on the security of network systems and information*

1. My Contact Information

I am:

(•) The impacted user ( ) Reporting on behalf of the impacted user

First Name:

Dimitrios

Last Name:

Merkouris

* Email:

d.merkouris@dei.gr

2. My Organization

What type of organization are you?

( ) Government (•) Private Sector

SMIR-generated structured report of specific incident

Consortium

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

Sphynx Analytics

Public Power Corporation

COSMOTE

FGC
Ferrocarrils de la Generalitat de Catalunya

WORLD SENSING

NATIONAL CSIRT-CY

Nodalpoint

Atos

SOCIAL ENGINEERING ACADEMY

AEGIS IT RESEARCH

APIROPLUS SOLUTIONS

Eunomia Ltd.
Consulting Services

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UiO : University of Oslo

PHOENIIX

Thank you for your attention!

Phoeni2x.eu

gdaniil@ece.upatras.gr

This project has received funding from the Horizon Europe Research and Innovation programme under Grant Agreement No101070586