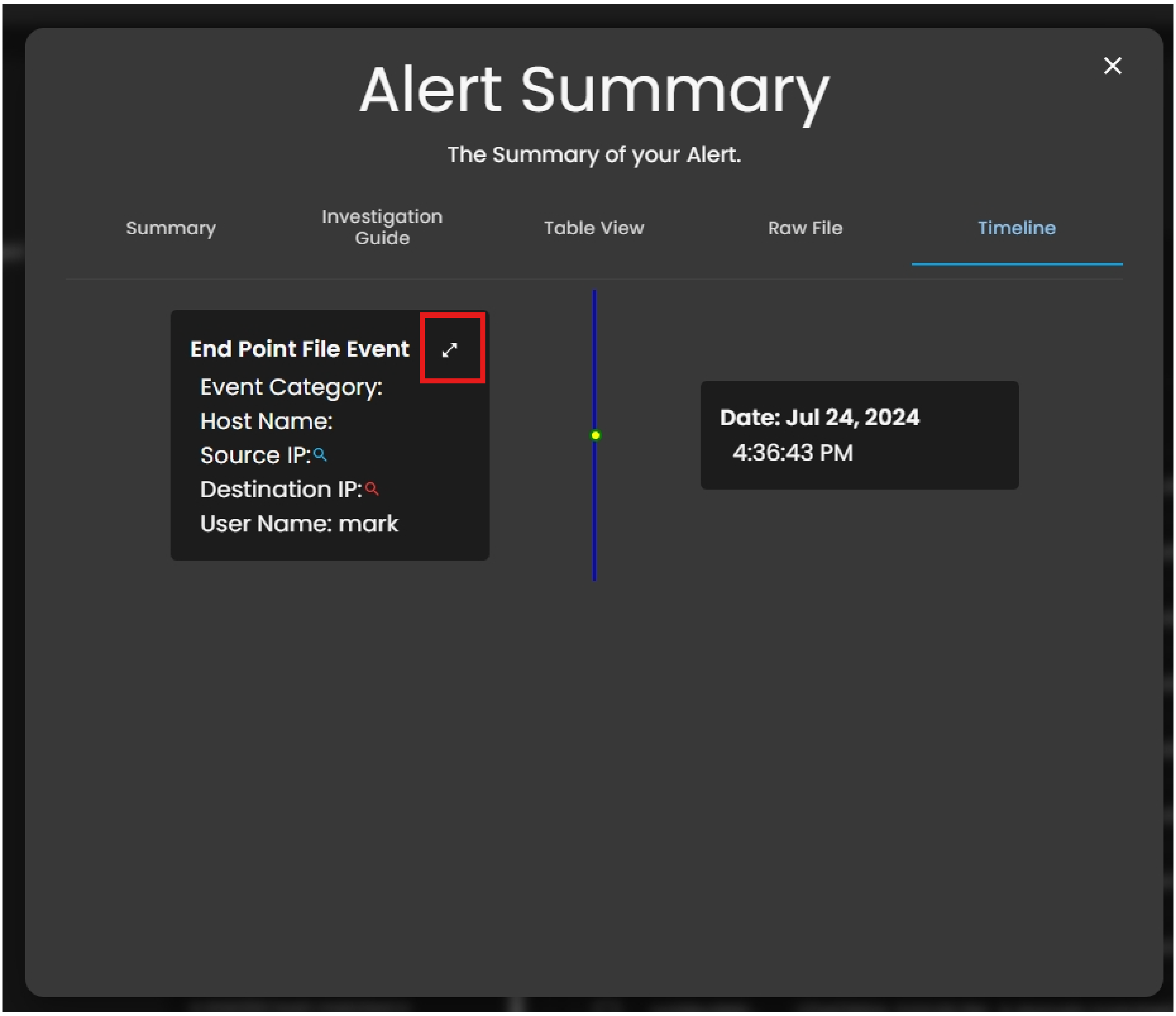
Daily Update: July 26

Here are the main updates of the CISO Workplace:

CIM Updates:

Alert Timeline more information:



End Point File Event

Event Category:

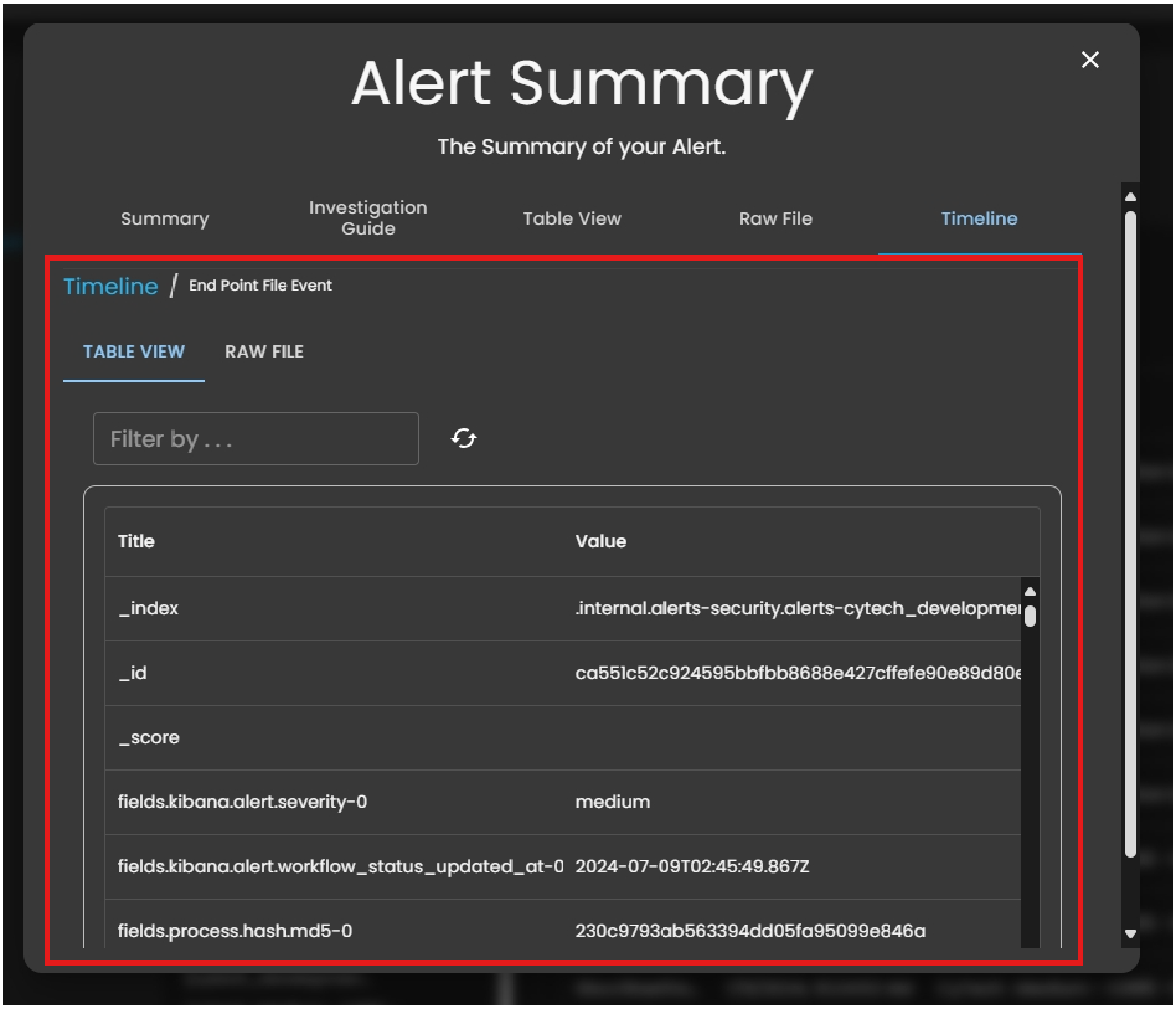
Host Name:

Source IP:

Destination IP:

User Name: mark

Date: Jul 24, 2024 4:36:43 PM

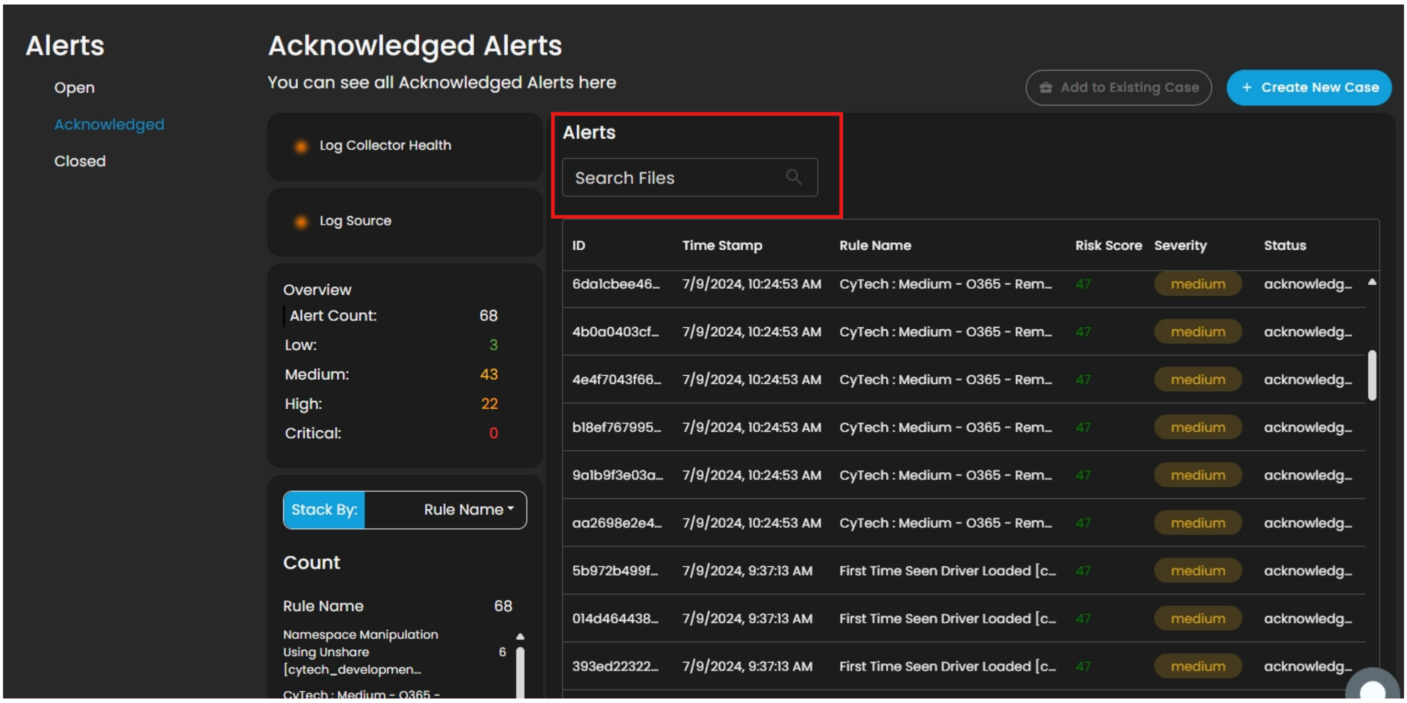


Alert Summary

The Summary of your Alert.

Title	Value
_index	.internal.alerts-security.alerts-cytech_developme
_id	ca551c52c924595bbfbb8688e427cffefe90e89d80
_score	
fields.kibana.alert.severity-0	medium
fields.kibana.alert.workflow_status_updated_at-0	2024-07-09T02:45:49.867Z
fields.process.hash.md5-0	230c9793ab563394dd05fa95099e846a

Added Search in Alerts Page



You can see all Acknowledged Alerts here

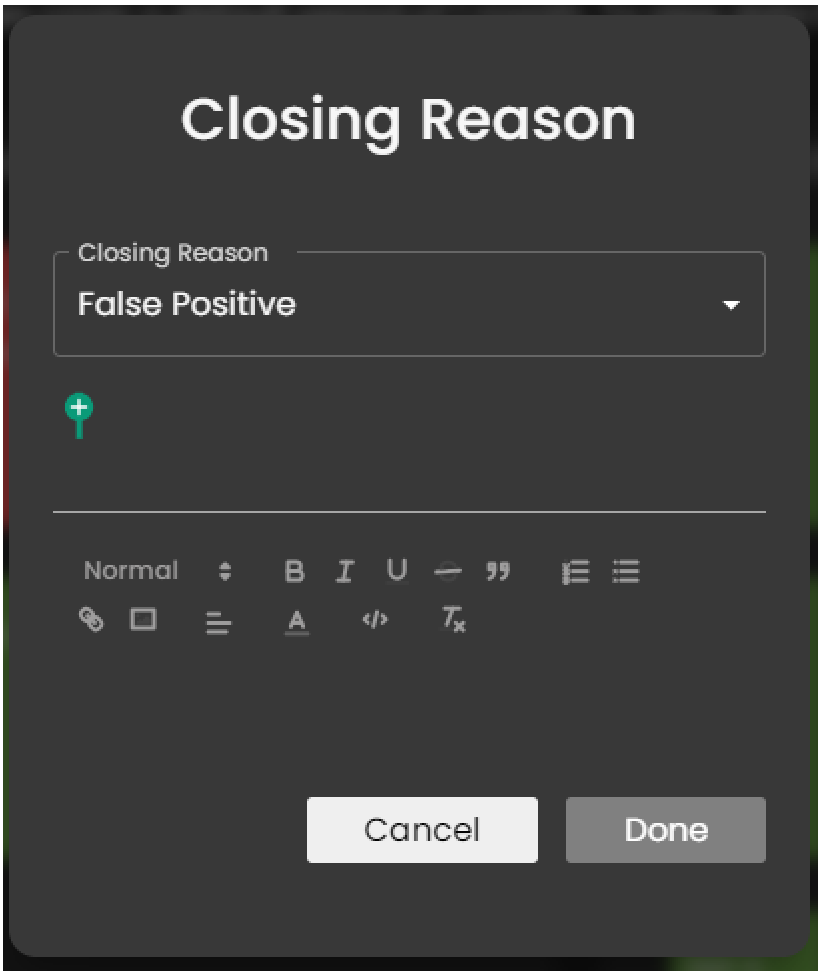
Overview	
Alert Count:	68
Low:	3
Medium:	43
High:	22
Critical:	0

Count	
Rule Name	68
Namespace Manipulation Using Unshare [cytech_developmen…	6
CyTech : Medium - O365 -	

Alerts

ID	Time Stamp	Rule Name	Risk Score	Severity	Status
6da1cbee46…	7/9/2024, 10:24:53 AM	CyTech : Medium - O365 - Rem…	47	medium	acknowledg…
4b0a0403cf…	7/9/2024, 10:24:53 AM	CyTech : Medium - O365 - Rem…	47	medium	acknowledg…
4e4f7043f66…	7/9/2024, 10:24:53 AM	CyTech : Medium - O365 - Rem…	47	medium	acknowledg…
b18ef767995…	7/9/2024, 10:24:53 AM	CyTech : Medium - O365 - Rem…	47	medium	acknowledg…
9a1b9f3e03a…	7/9/2024, 10:24:53 AM	CyTech : Medium - O365 - Rem…	47	medium	acknowledg…
aa2698e2e4…	7/9/2024, 10:24:53 AM	CyTech : Medium - O365 - Rem…	47	medium	acknowledg…
5b972b499f…	7/9/2024, 9:37:13 AM	First Time Seen Driver Loaded [c…	47	medium	acknowledg…
014d464438…	7/9/2024, 9:37:13 AM	First Time Seen Driver Loaded [c…	47	medium	acknowledg…
393ed22322…	7/9/2024, 9:37:13 AM	First Time Seen Driver Loaded [c…	47	medium	acknowledg…

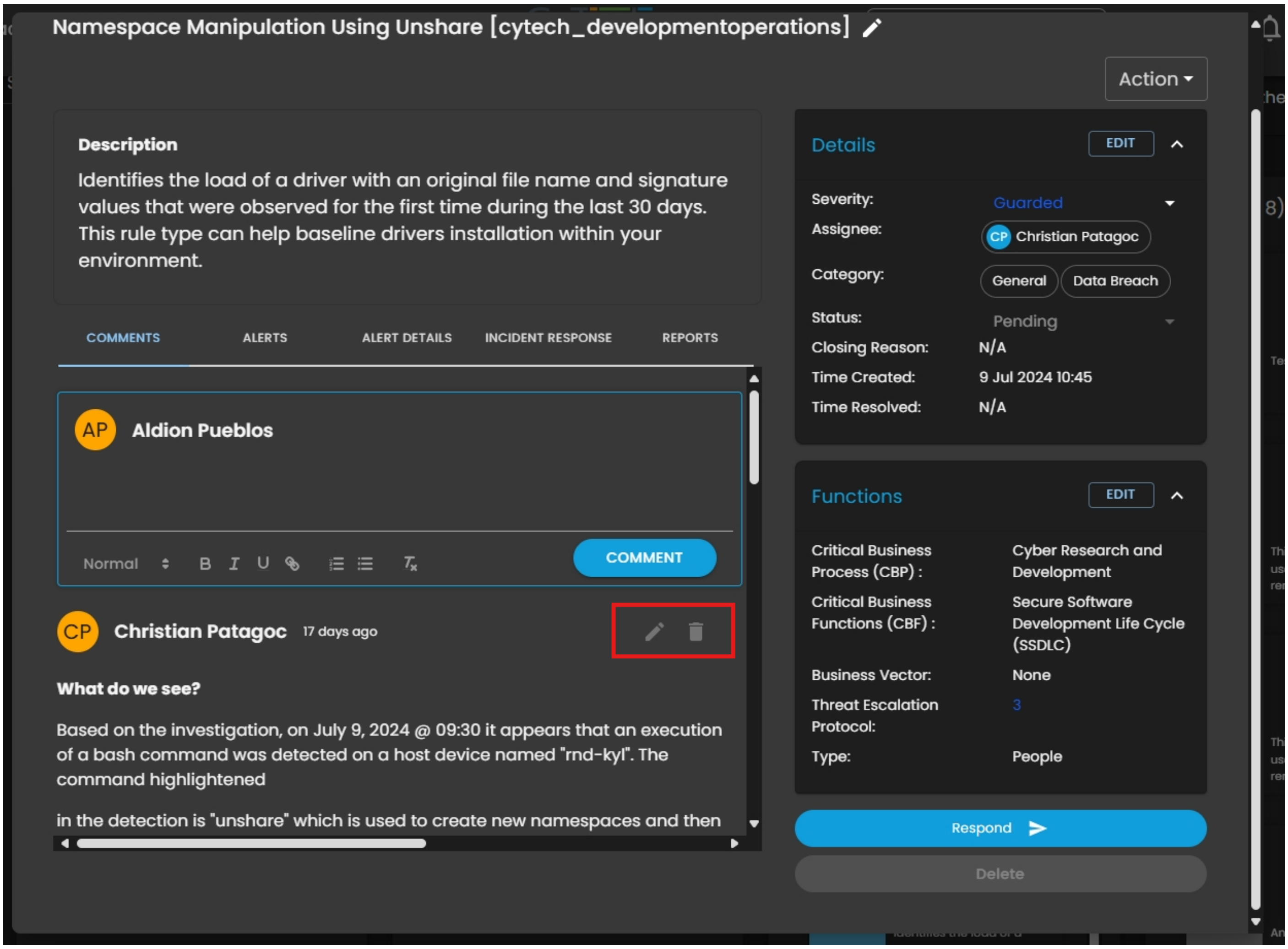
Set Closing Reason Description as Optional:



Closing Reason: False Positive

CIM Bug Fixes:

Cannot Delete / Modify comments not belonging to user



Namespace Manipulation Using Unshare [cytech_developmentoperations]

Description

Identifies the load of a driver with an original file name and signature values that were observed for the first time during the last 30 days. This rule type can help baseline drivers installation within your environment.

CP Christian Patagoc 17 days ago

What do we see?

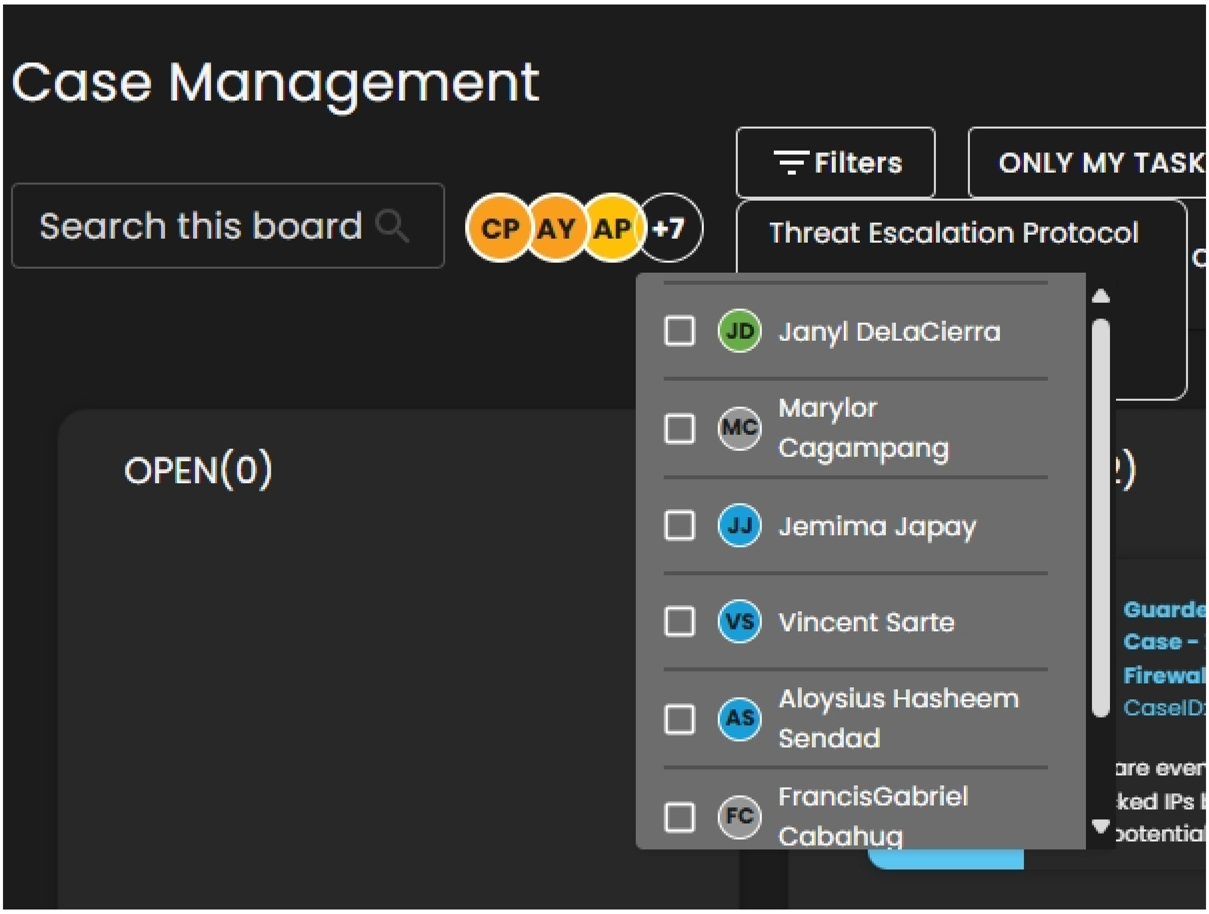
Based on the investigation, on July 9, 2024 @ 09:30 it appears that an execution of a bash command was detected on a host device named "rnd-kyl". The command highlighted

in the detection is "unshare" which is used to create new namespaces and then

Severity:	Guarded
Assignee:	CP Christian Patagoc
Category:	General Data Breach
Status:	Pending
Closing Reason:	N/A
Time Created:	9 Jul 2024 10:45
Time Resolved:	N/A

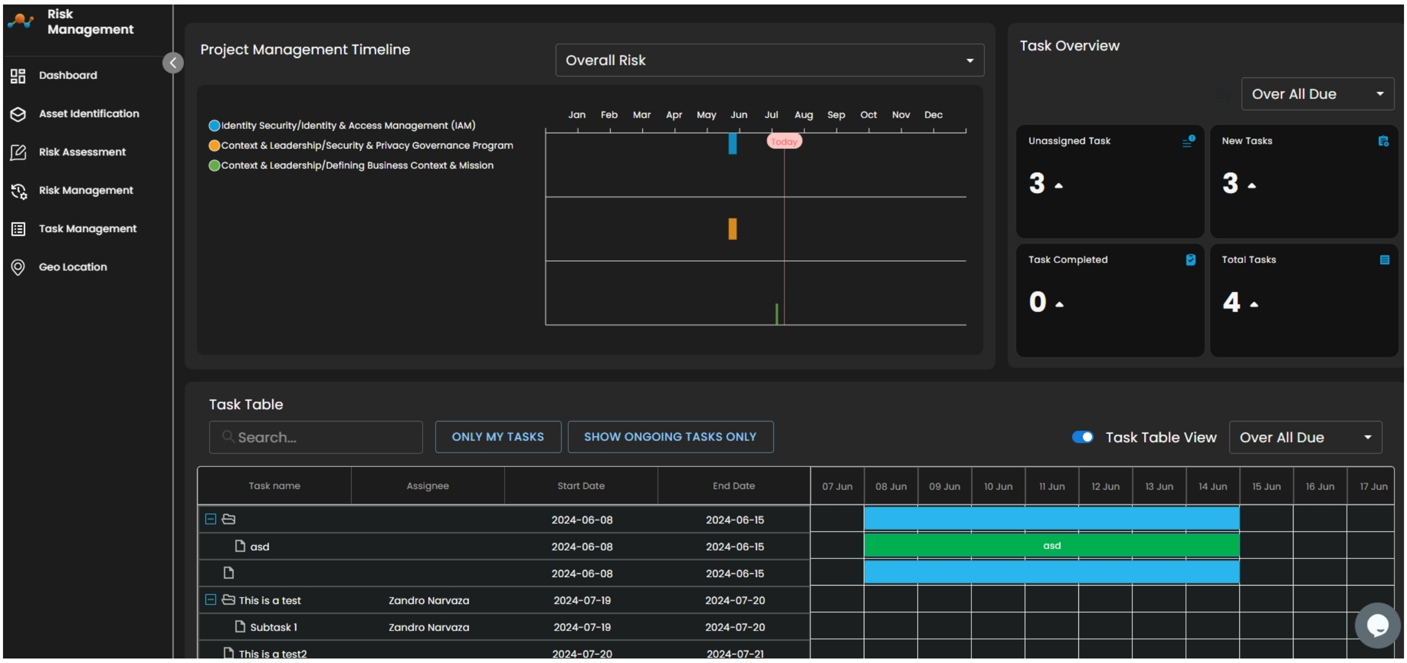
Critical Business Process (CBP) :	Cyber Research and Development
Critical Business Functions (CBF) :	Secure Software Development Life Cycle (SSDLC)
Business Vector:	None
Threat Escalation Protocol:	3
Type:	People

User Filter in cases is closed automatically when mouse is out



RM Updates

Task Management Overview component
Mitigation Proposal Timeline Gantt Chart
Assignee Full name displayed in Timeline
Improvement in Task management timeline search



Unassigned Task 3

New Tasks 3

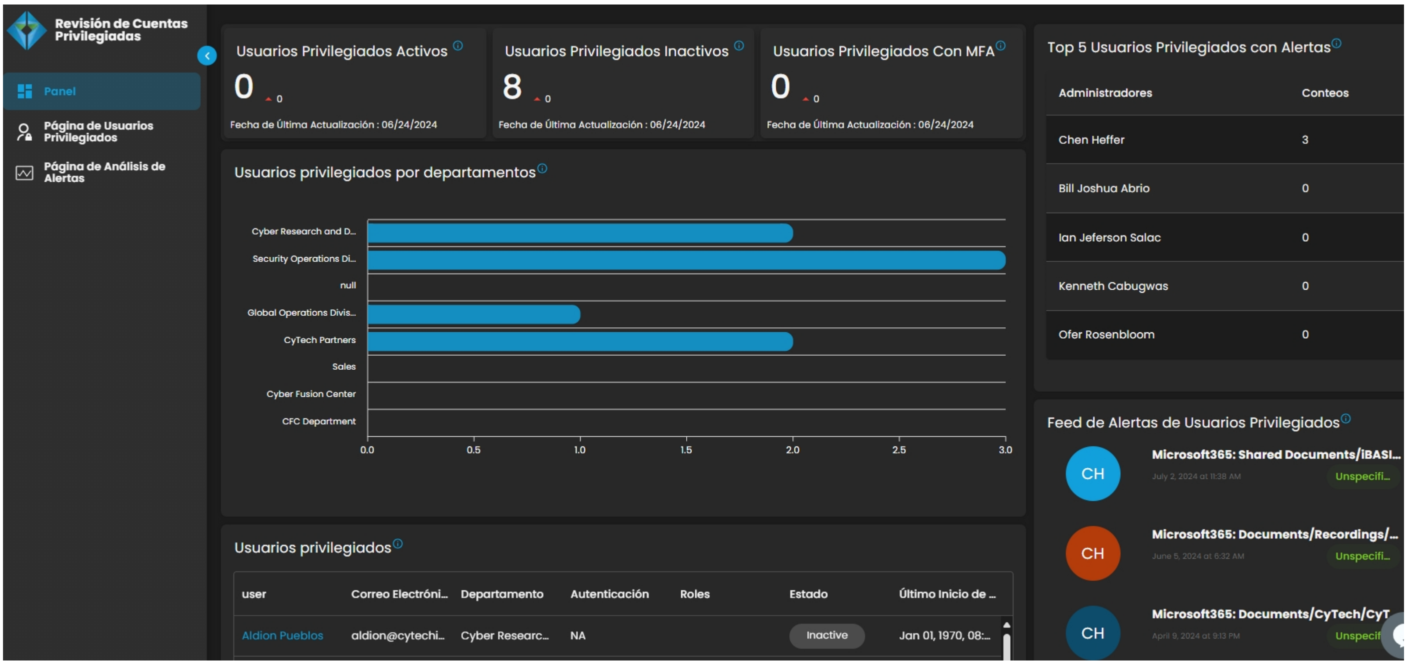
Task Completed 0

Total Tasks 4

Task name	Assignee	Start Date	End Date
		2024-06-08	2024-06-15
asd		2024-06-08	2024-06-15
		2024-06-08	2024-06-15
This is a test	Zandro Narvaza	2024-07-19	2024-07-20
Subtask 1	Zandro Narvaza	2024-07-19	2024-07-20
This is a test2		2024-07-20	2024-07-21

Privileged Account Review Updates:

Spanish Translation Support



Revisión de Cuentas Privilegiadas
Panel
Página de Usuarios Privilegiados
Página de Análisis de Alertas

Usuarios Privilegiados Activos

0 ▲ 0

Fecha de Última Actualización : 06/24/2024

Usuarios Privilegiados Inactivos

8 ▲ 0

Fecha de Última Actualización : 06/24/2024

Usuarios Privilegiados Con MFA

0 ▲ 0

Fecha de Última Actualización : 06/24/2024

Top 5 Usuarios Privilegiados con Alertas

Administradores	Conteos
Chen Heffer	3
Bill Joshua Abrio	0
Ian Jeferson Salac	0
Kenneth Cabugwas	0
Ofer Rosenbloom	0

Usuarios privilegiados por departamentos

Feed de Alertas de Usuarios Privilegiados

CH Microsoft365: Shared Documents/iBASI... July 2, 2024 at 11:38 AM Unspecifi...

CH Microsoft365: Documents/Recordings/... June 5, 2024 at 6:32 AM Unspecifi...

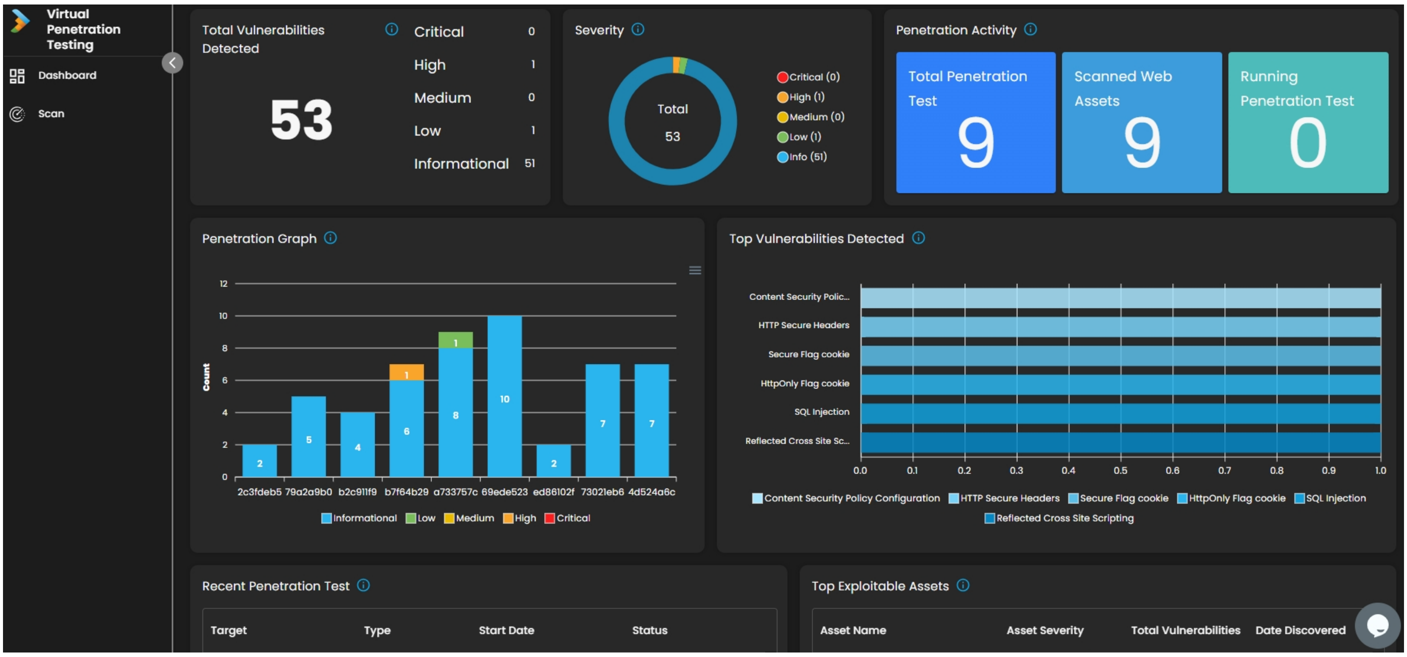
CH Microsoft365: Documents/CyTech/CyT April 9, 2024 at 9:13 PM Unspecif

Usuarios privilegiados

user	Correo Electróni...	Departamento	Autenticación	Roles	Estado	Último Inicio de ...
Aldion Pueblos	aldion@cytechi...	Cyber Researc...	NA		Inactive	Jan 01, 1970, 08:...

Virtual Penetration Testing Updates:

Updated dashboard with some "Rabbit Hole" support



Total Vulnerabilities Detected

53

Critical	0
High	1
Medium	0
Low	1
Informational	51

Severity

Penetration Activity

Total Penetration Test 9

Scanned Web Assets 9

Running Penetration Test 0

Penetration Graph

Top Vulnerabilities Detected

Recent Penetration Test

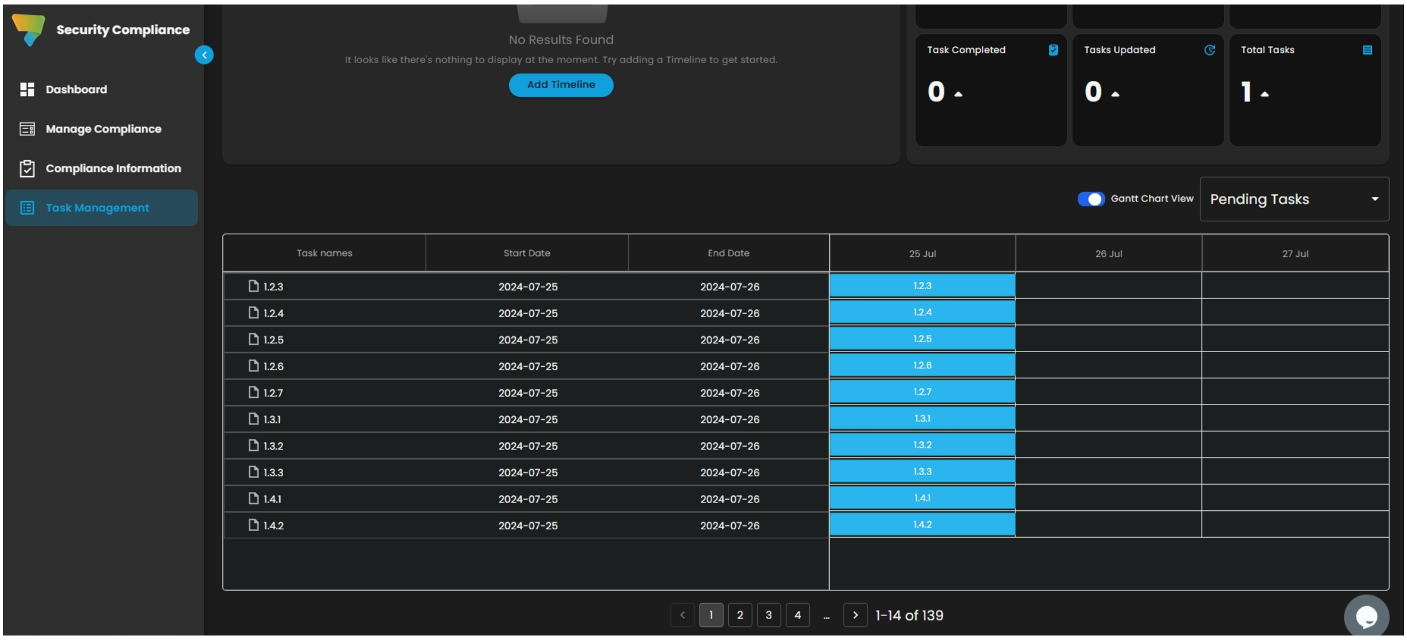
Target	Type	Start Date	Status

Top Exploitable Assets

Asset Name	Asset Severity	Total Vulnerabilities	Date Discovered

Security and Privacy Compliance Updates:

Updated Timeline Gantt Chart



No Results Found

It looks like there's nothing to display at the moment. Try adding a Timeline to get started.

Task Completed 0

Tasks Updated 0

Total Tasks 1

Pending Tasks

Task names	Start Date	End Date	25 Jul	26 Jul	27 Jul
1.2.3	2024-07-25	2024-07-26	1.2.3		
1.2.4	2024-07-25	2024-07-26	1.2.4		
1.2.5	2024-07-25	2024-07-26	1.2.5		
1.2.6	2024-07-25	2024-07-26	1.2.6		
1.2.7	2024-07-25	2024-07-26	1.2.7		
1.3.1	2024-07-25	2024-07-26	1.3.1		
1.3.2	2024-07-25	2024-07-26	1.3.2		
1.3.3	2024-07-25	2024-07-26	1.3.3		
1.4.1	2024-07-25	2024-07-26	1.4.1		
1.4.2	2024-07-25	2024-07-26	1.4.2		

< 1 2 3 4 ... > 1-14 of 139

Revision #2
Created 26 July 2024 11:32:55 by Aldion Pueblos
Updated 26 July 2024 12:50:54 by Aldion Pueblos