

Daily Update: July 26

Here are the main updates of the CISO Workplace:

CIM Updates:

Alert Timeline more information:

Alert Summary

The Summary of your Alert.

Summary

Investigation Guide

Table View

Raw File

Timeline

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.

Summary

Investigation
Guide

Table View

Raw File

Timeline

Timeline / End Point File Event

TABLE VIEW

RAW FILE

Filter by ...



Title

Value

_index

.internal.alerts-security.alerts-cytech_developme

_id

ca551c52c924595bbfbb8688e427cffe90e89d80e

_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

Namespace Manipulation Using Unshare [cytech_developmentoperations]

Action

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.

COMMENTS

ALERTS

ALERT DETAILS

INCIDENT RESPONSE

REPORTS

AP Aldion Pueblos

Normal B I U

COMMENT

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 highlightened

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

Details

EDIT

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

Functions

EDIT

Critical Business Process (CBP): Cyber Research and Development

Critical Business Functions (CBF): Secure Software Development Life Cycle (SSDLC)

Business Vector: None

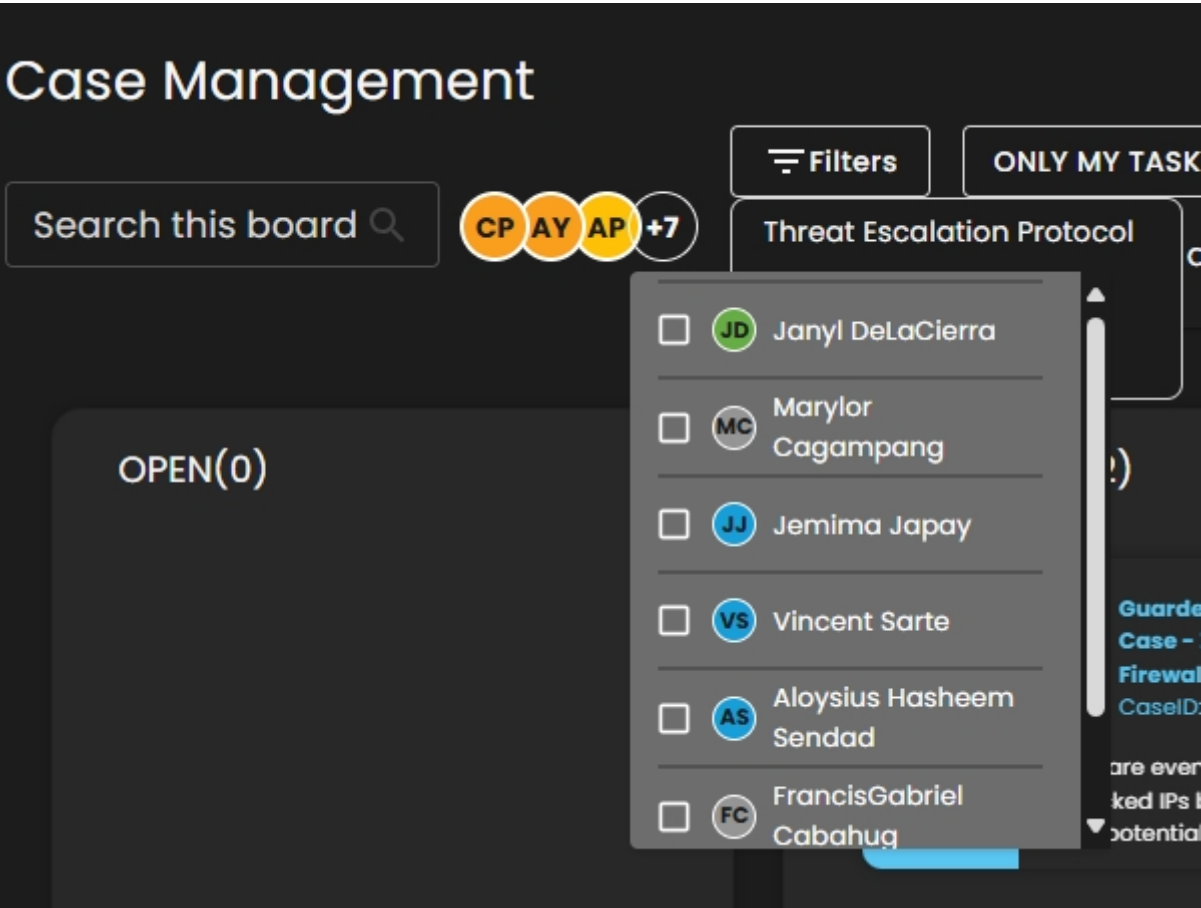
Threat Escalation Protocol: 3

Type: People

Respond

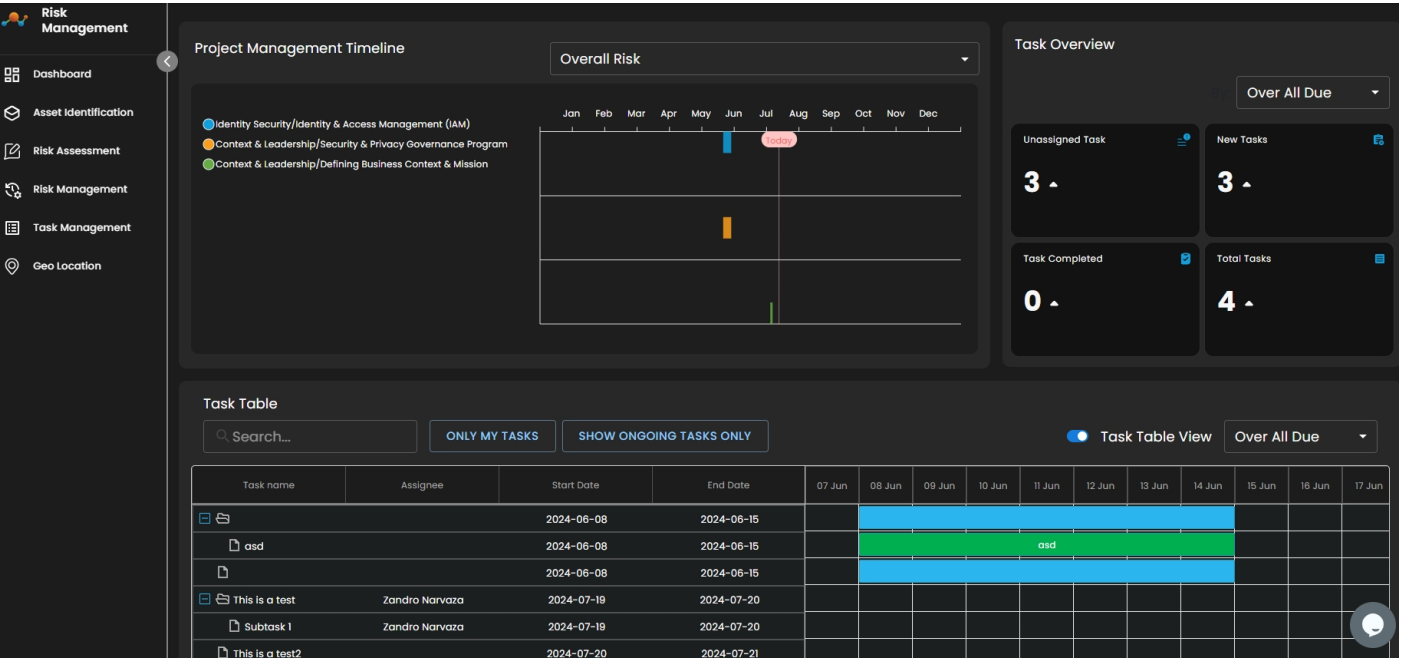
Delete

User Filter in cases is closed automatically when mouse is out



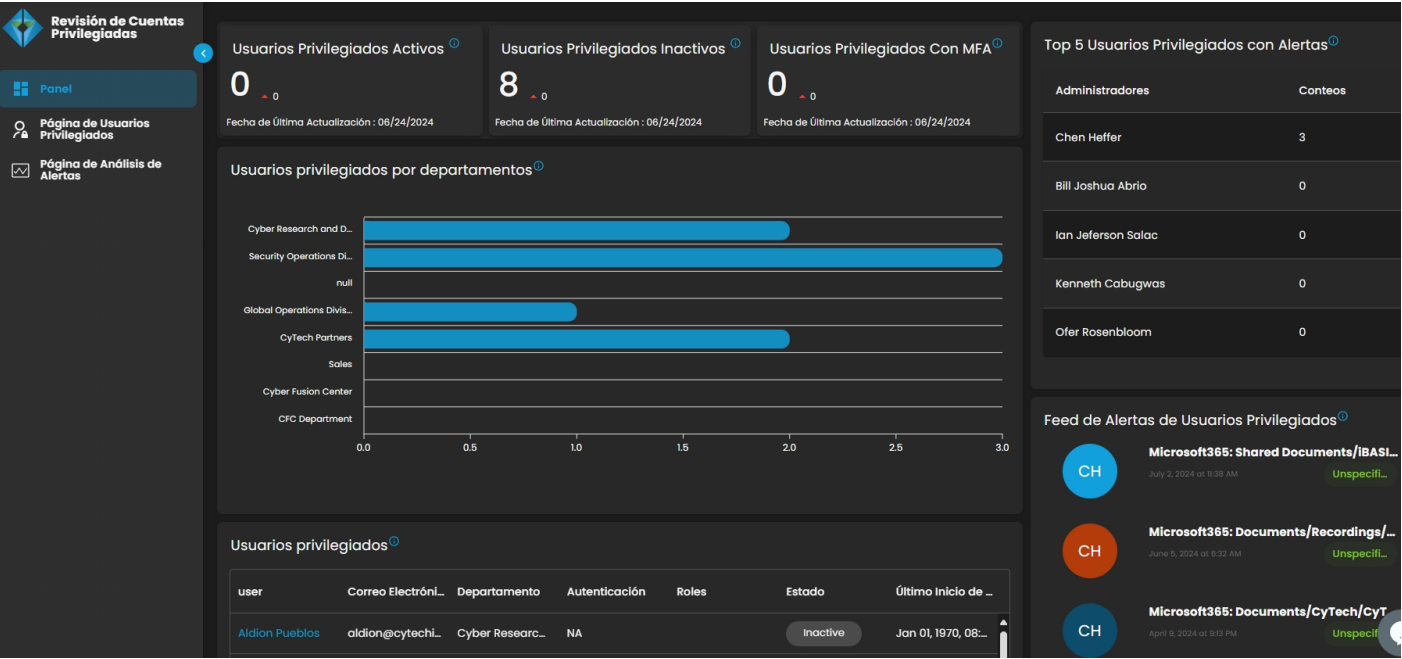
RM Updates

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



Privileged Account Review Updates:

Spanish Translation Support



Virtual Penetration Testing Updates:

Updated dashboard with some "Rabbit Hole" support



Security and Privacy Compliance Updates:

Updated Timeline Gantt Chart

Security Compliance

Dashboard

Manage Compliance

Compliance Information

Task Management

No Results Found

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

Add Timeline

Task Completed0

Tasks Updated0

Total Tasks1

Gantt Chart View

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		

<1234-

>

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