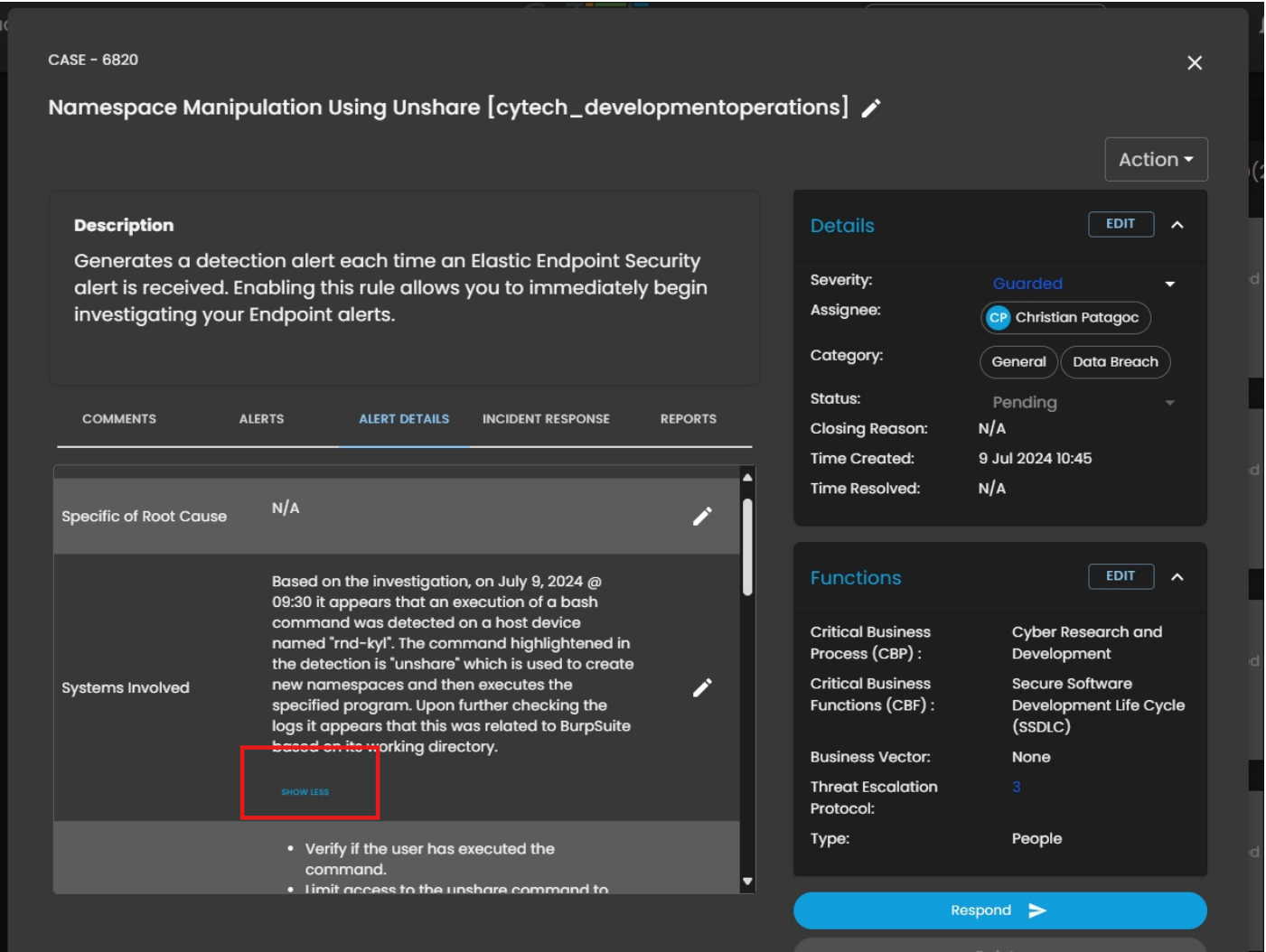


Daily Update: July 30

Here are the main updates of the CISO Workplace:

CIM Updates:

In Alert Details, added "show less" and "show more"



In Alert Details, updated the display formatting:

CASE - 6820

Namespaces Manipulation Using Unshare [cytech_developmentoperations]

Action

Description

Generates a detection alert each time an Elastic Endpoint Security alert is received. Enabling this rule allows you to immediately begin investigating your Endpoint alerts.

COMMENTS

ALERTS

ALERT DETAILS

INCIDENT RESPONSE

REPORTS

Location of Vulnerable system

- Verify if the user has executed the command.
- Limit access to the unshare command to authorized users only.
- Implement proper access controls and permissions to prevent unauthorized execution.
- Regularly review and audit user privileges to ensure they align with the principle of least privilege. If your application runs in containers (e.g., Docker), ensure that container security measures are in place. Use container runtime security tools to detect and prevent privilege escalation attempts.
- Consider using tools like SELinux or AppArmor to enforce security policies.

Details

EDIT

Severity: Guarded

Assignee: 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)

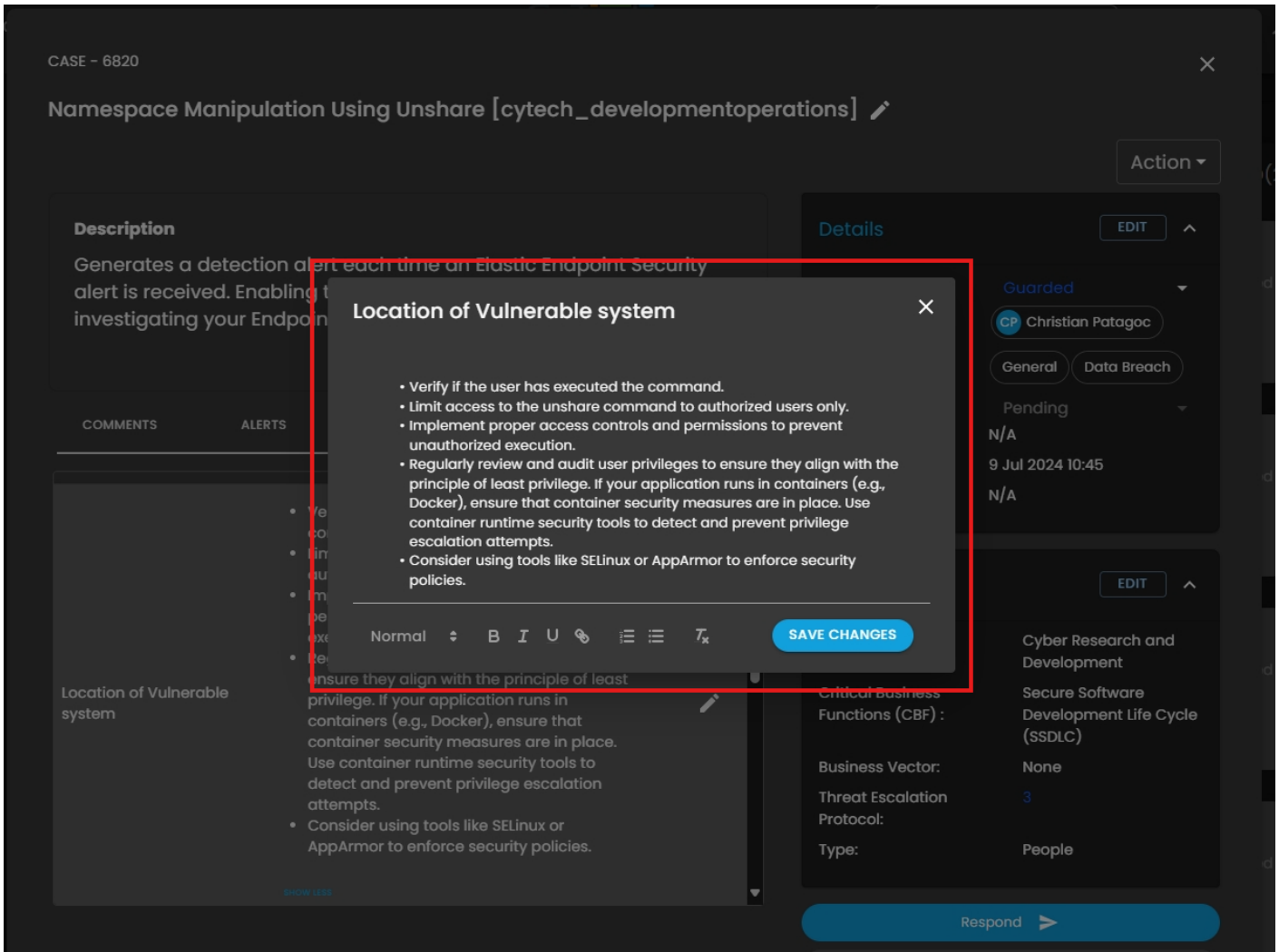
Business Vector: None

Threat Escalation Protocol: 3

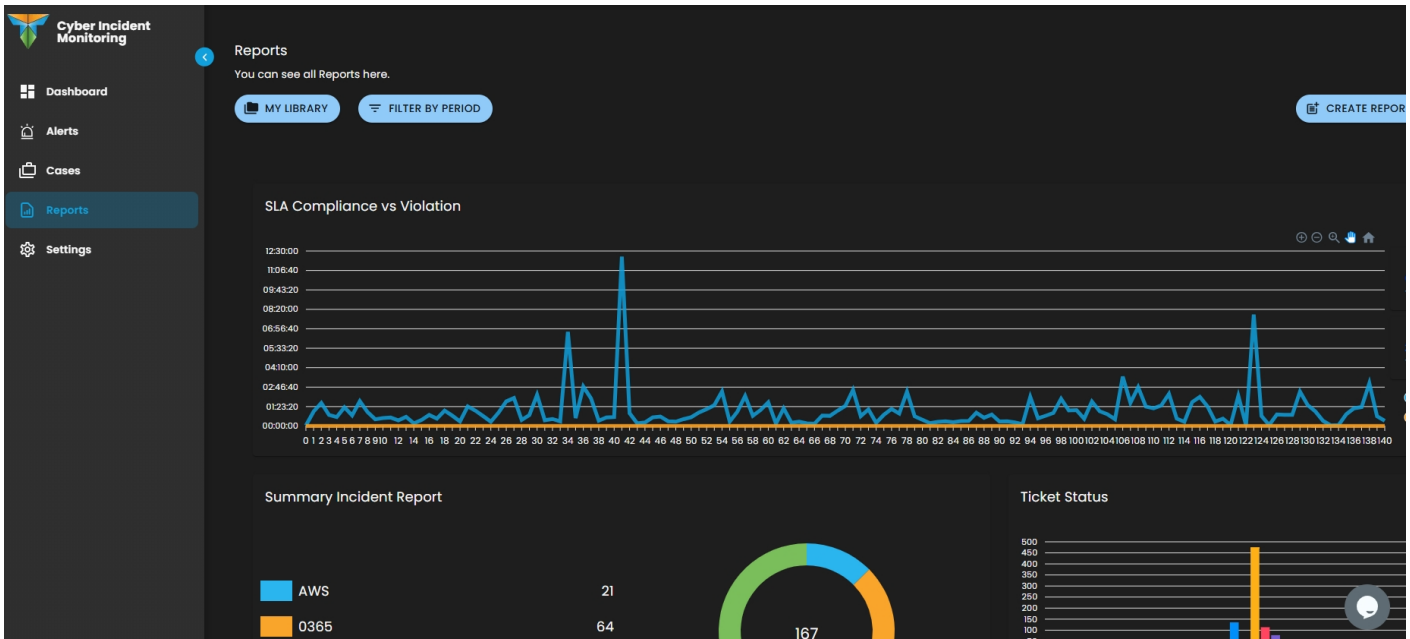
Type: People

Respond

In Alert Details, updated the improvement for editing an alert detail:

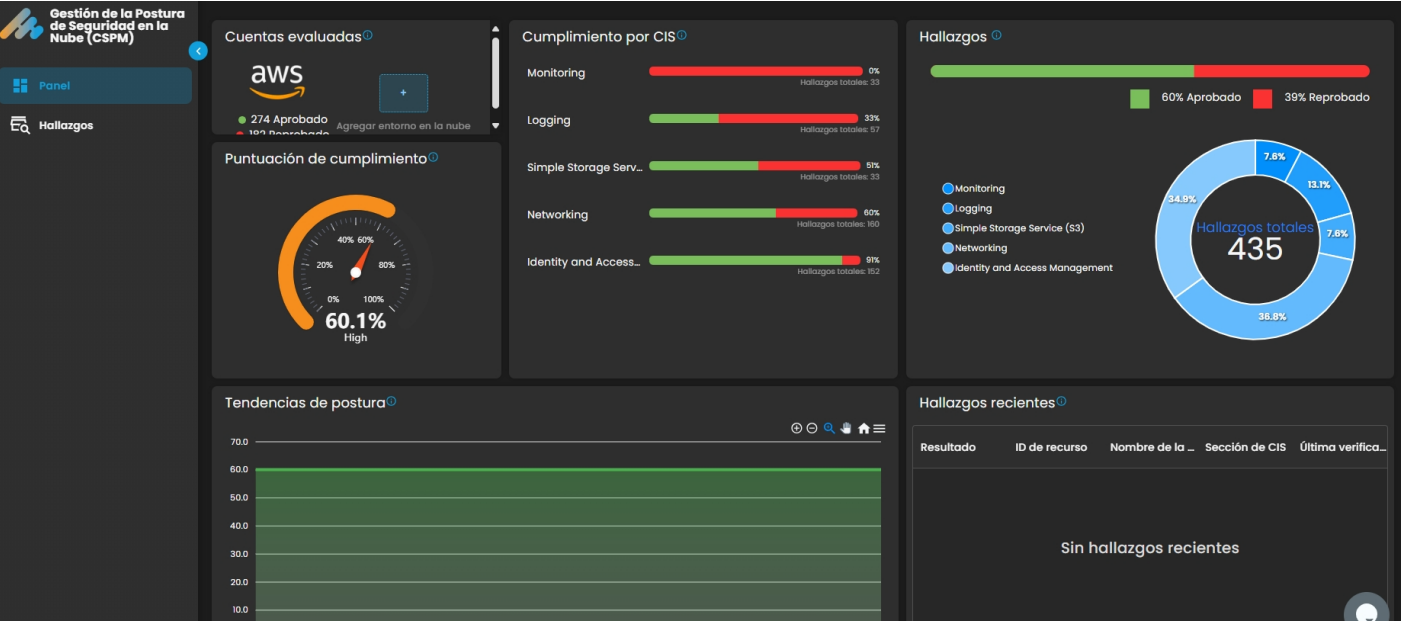


Bug Fixes in graph display for Quarterly and Annual Report:



Cloud Security Posture Management Updates:

Spanish Translation



Revision #1

Created 30 July 2024 11:16:35 by Aldion Pueblos

Updated 30 July 2024 11:39:07 by Aldion Pueblos