

# Daily Update: July 30

Here are the main updates of the CISO Workplace:

## CIM Updates:

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

The screenshot displays the 'Alert Details' view for Case 6820, titled 'Namespace Manipulation Using Unshare [cytech\_developmentoperations]'. The interface is dark-themed and includes a navigation bar with tabs for 'COMMENTS', 'ALERTS', 'ALERT DETAILS' (selected), 'INCIDENT RESPONSE', and 'REPORTS'. A top right 'Action' dropdown is visible. The main content area is divided into several sections:

- 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.
- Details:** A panel containing metadata such as Severity (Guarded), Assignee (Christian Patagoc), Category (General, Data Breach), Status (Pending), Closing Reason (N/A), Time Created (9 Jul 2024 10:45), and Time Resolved (N/A).
- Functions:** A table listing business processes and vectors, such as Cyber Research and Development, Secure Software Development Life Cycle (SSDLC), and People.
- Alert Content:** A scrollable area with a 'Specific of Root Cause' (N/A) and 'Systems Involved' section. The 'Systems Involved' text describes an investigation on July 9, 2024, at 09:30, identifying a 'unshare' command on a host named 'rnd-kyl'. A red box highlights a 'SHOW LESS' link at the bottom of this section.

At the bottom of the alert details, there is a prominent blue 'Respond' button with a right-pointing arrow.

In Alert Details, updated the display formatting:

CASE - 6820

## Namespace 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.

SHOW LESS

**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)

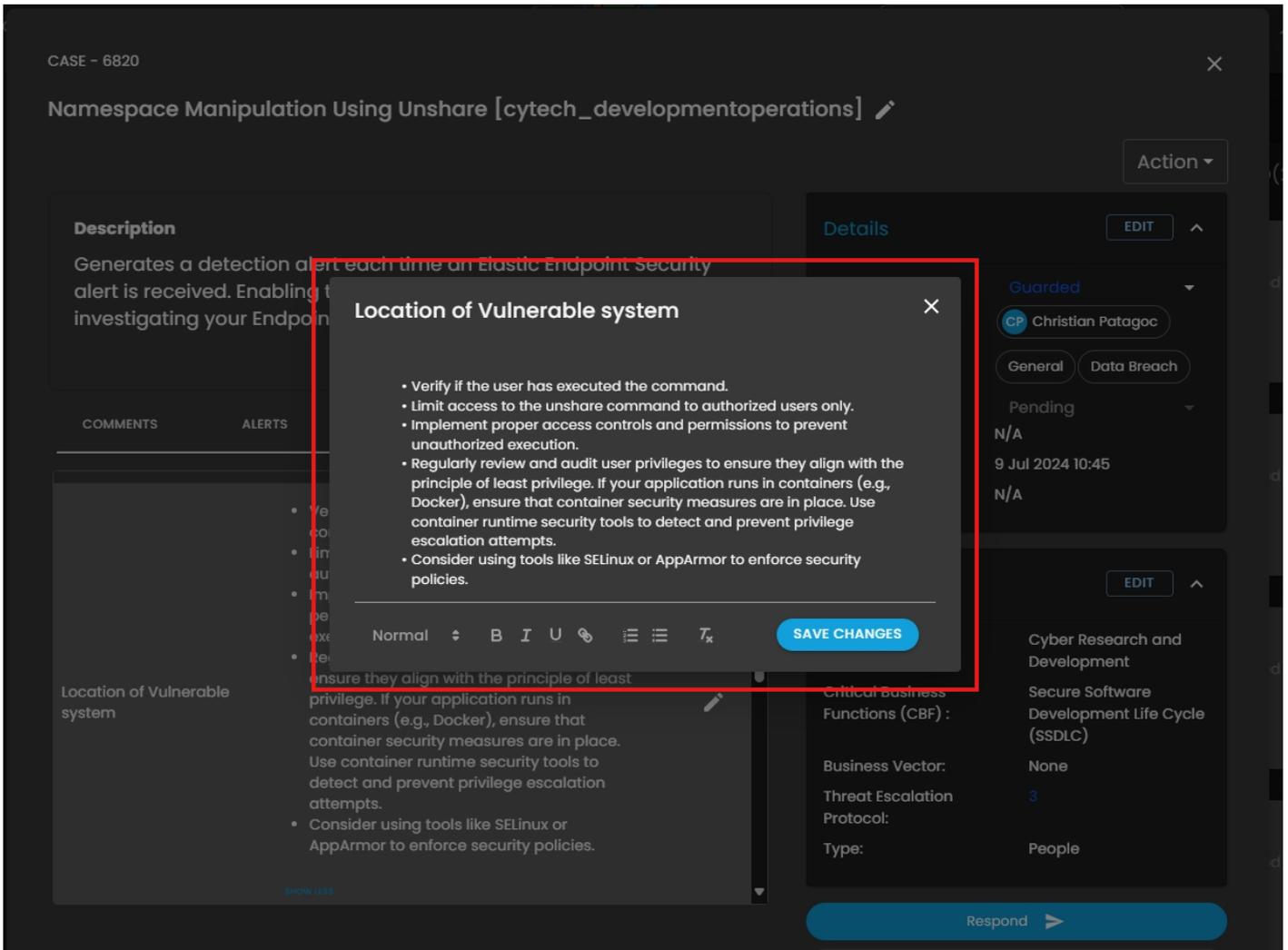
Business Vector: None

Threat Escalation Protocol: 3

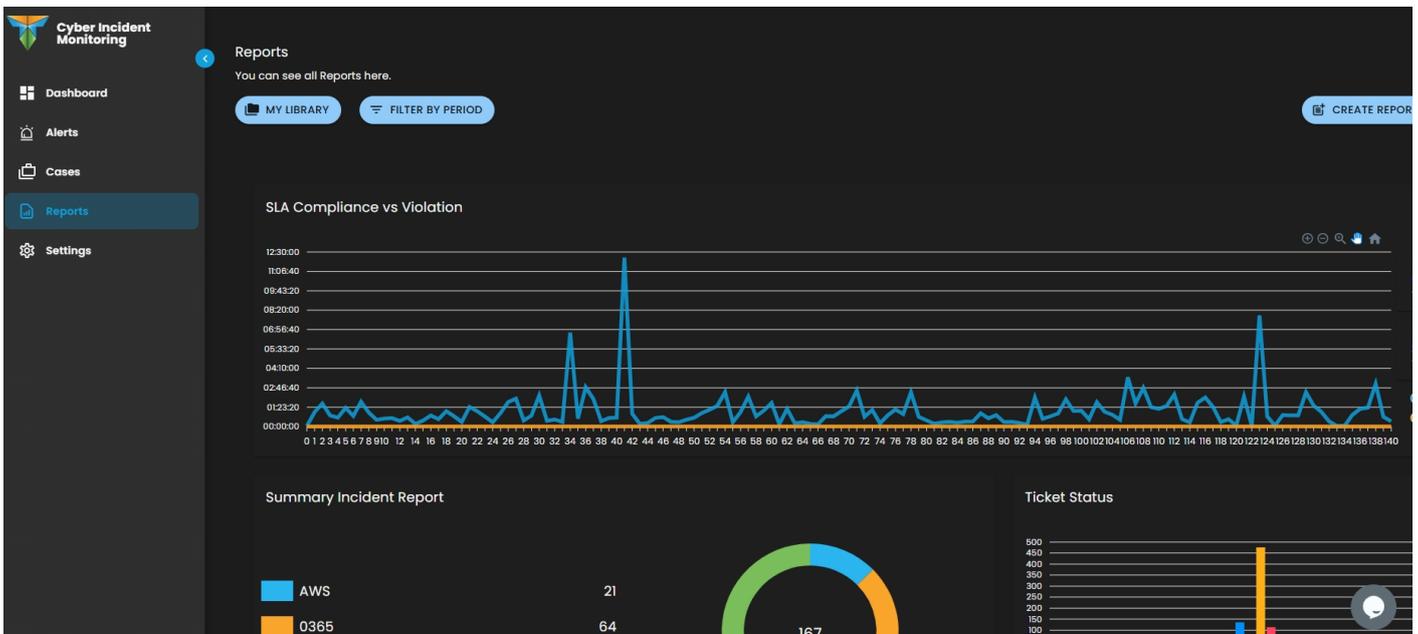
Type: People

Respond ➤

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

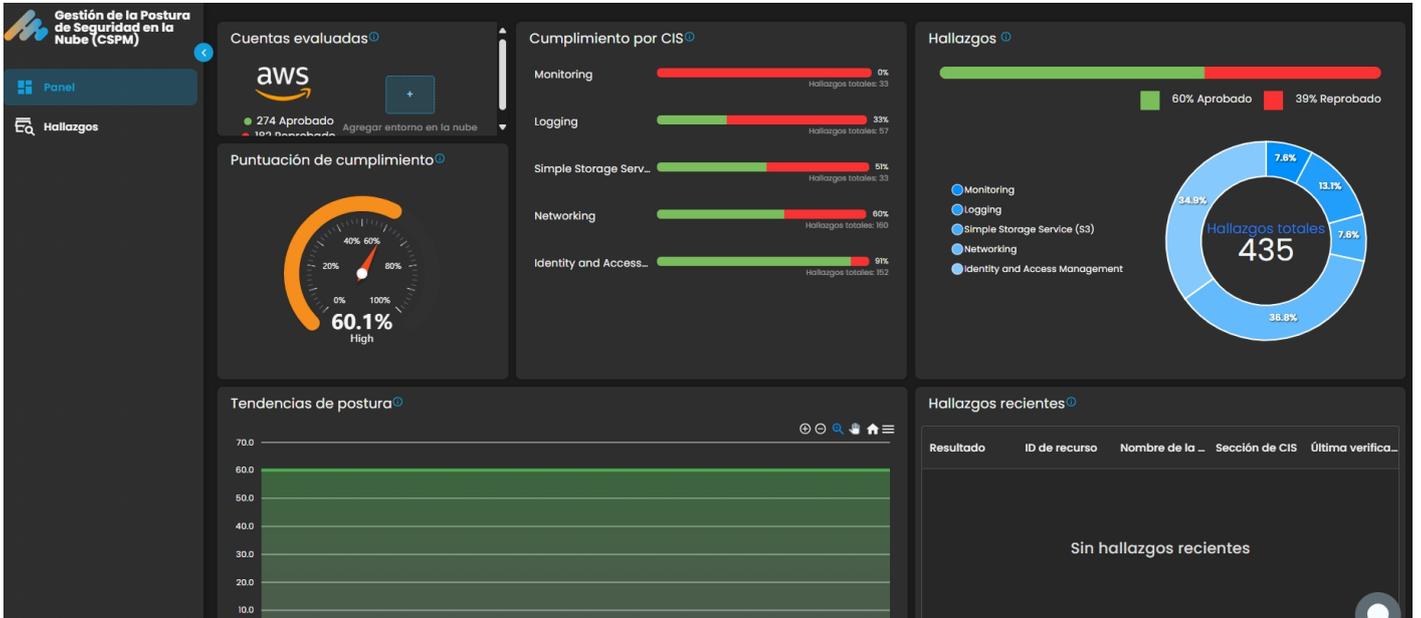


Bug Fixes in graph display for Quarterly and Annual Report:



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