

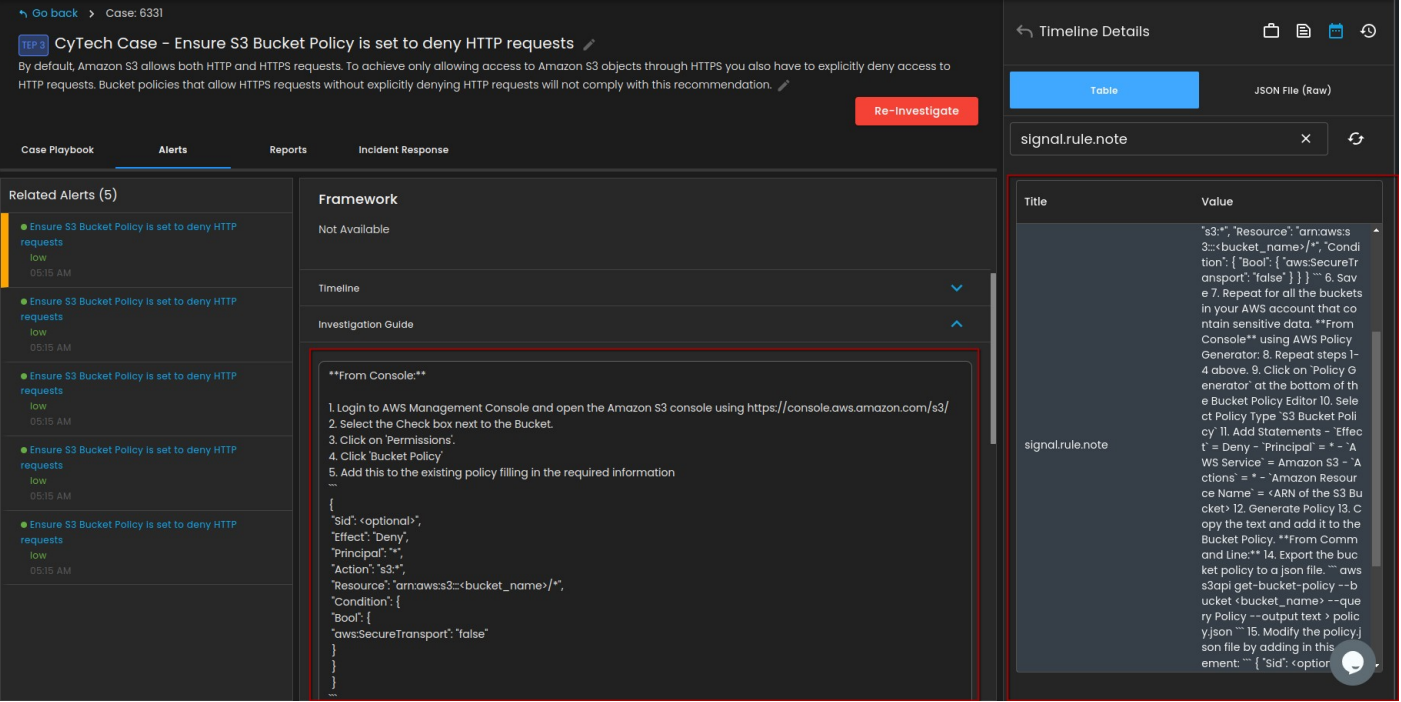
Daily Update: September 16

Here are the main updates of the CISO Workplace:

CIM Updates:

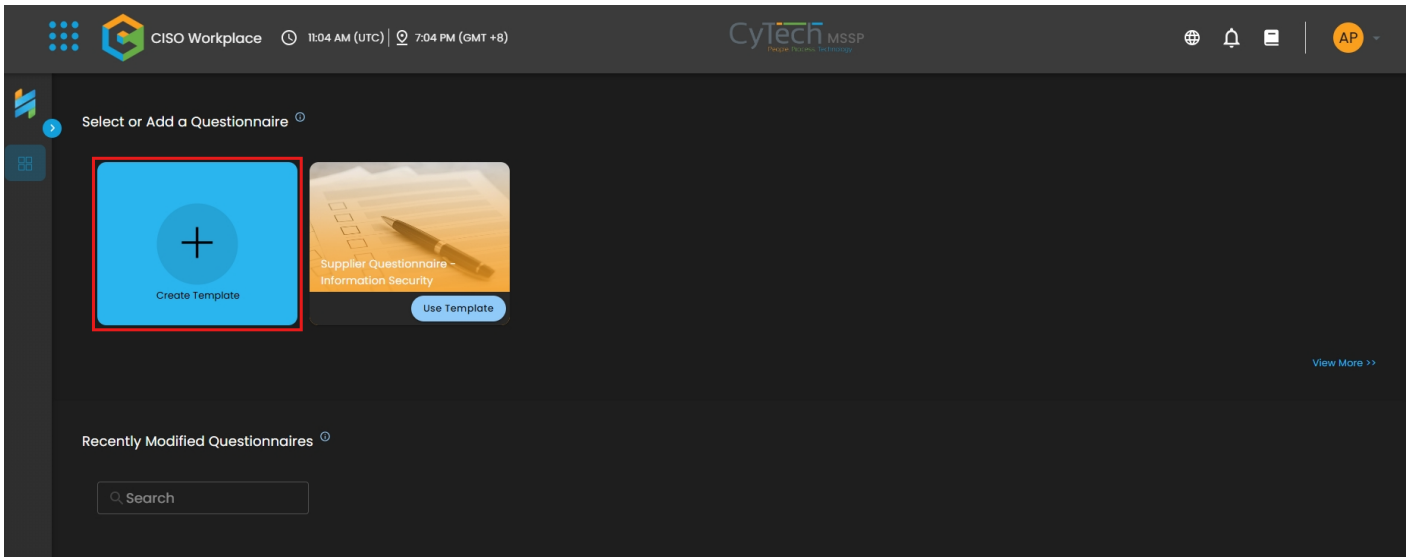
Improvement of the display of timeline elements

Fix in the display of Investigation Guide in Alerts



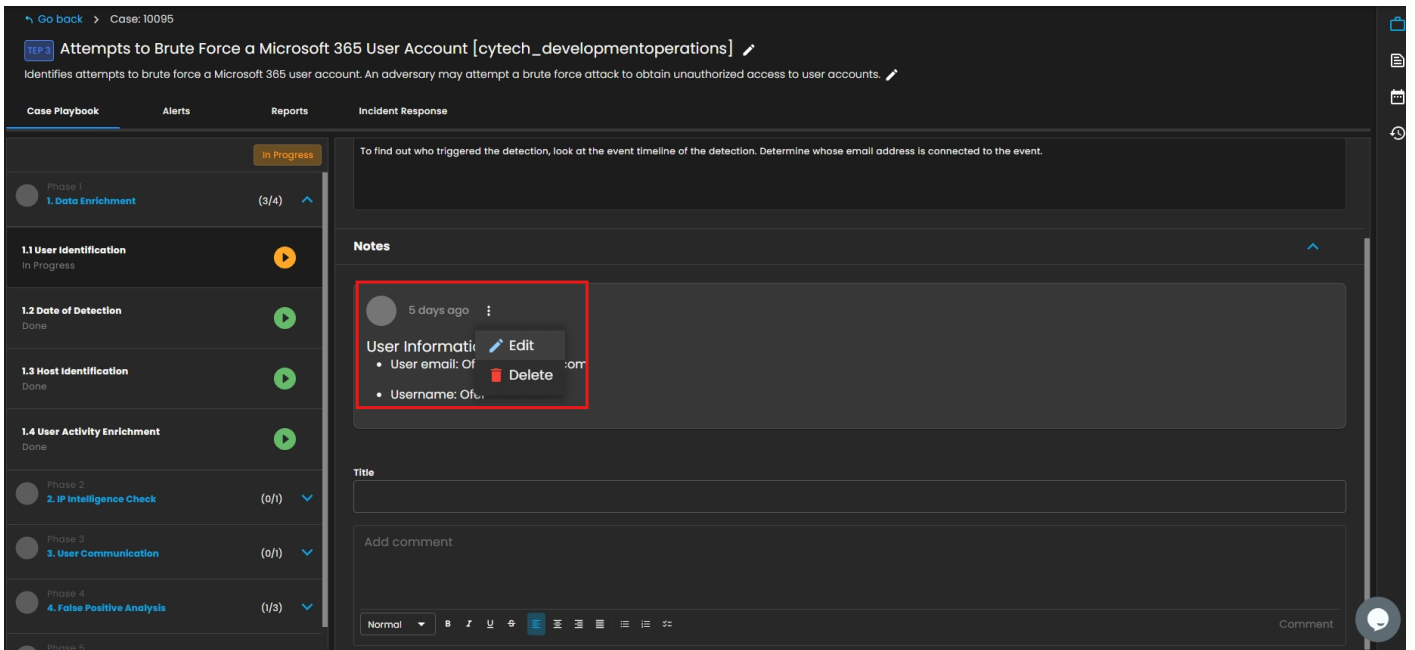
Security Assessment Questionnaires Updates

Support for Create Template Feature



CIM Updates

Support for Edit/Delete in Playbook Notes



Go back > Case: 10095

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]

Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack to obtain unauthorized access to user accounts.

Case Playbook Alerts Reports Incident Response

Phase 1: 1. Data Enrichment (4/4)

1.1 User Identification Done

1.2 Date of Detection Done

1.3 Host Identification Done

1.4 User Activity Enrichment Done

Phase 2: 2. IP Intelligence Check (0/1)

Phase 3: 3. User Communication (0/1)

Phase 4: 4. False Positive Analysis (1/3)

Edit Note

Title

test update

test update desc

Normal B I U + E X Y Z []

Cancel Save

5 days ago

User Information

- User email: Ofer@cytechint.com
- Username: Ofer

Edvir Davin 3 days ago

test update

Edit Delete

Title

Go back > Case: 10095

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]

Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack to obtain unauthorized access to user accounts.

Case Playbook Alerts Reports Incident Response

Phase 1: 1. Data Enrichment (4/4)

1.1 User Identification Done

1.2 Date of Detection Done

1.3 Host Identification Done

1.4 User Activity Enrichment Done

Phase 2: 2. IP Intelligence Check (0/1)

Phase 3: 3. User Communication (0/1)

Phase 4: 4. False Positive Analysis (1/3)

Description

To find out who triggered the detection, look at the event timeline of the detection. Determine whose email address is connected to the event.

Notes

5 days ago

User Information

- User email: Ofer@cytechint.com
- Username: Ofer

Edvir Davin a few seconds ago

test update

test update desc

Title

Go back > Case: 10095

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]

Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack to obtain unauthorized access to user accounts.

Case Playbook Alerts Reports Incident Response

Phase 1: 1. Data Enrichment (4/4)

1.1 User Identification Done

1.2 Date of Detection Done

1.3 Host Identification Done

1.4 User Activity Enrichment Done

Phase 2: 2. IP Intelligence Check (0/1)

Phase 3: 3. User Communication (0/1)

Phase 4: 4. False Positive Analysis (1/3)

Description

To find out who triggered the detection, look at the event timeline of the detection. Determine whose email address is connected to the event.

Notes

5 days ago

User Information

- User email: Ofer@cytechint.com
- Username: Ofer

Edvir Davin a minute ago

test update

test update desc

Confirm Deletion

Are you sure you want to delete this note?

Cancel Delete

Title

Go back > Case: 10095

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]

Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack to obtain unauthorized access to user accounts.

Case PlaybookAlertsReportsIncident Response

In Progress

Phase 1

1. Data Enrichment (4/4)

1.1 User Identification Done

1.2 Date of Detection Done

1.3 Host Identification Done

1.4 User Activity Enrichment Done

Phase 2

2. IP Intelligence Check (0/1)

Phase 3

3. User Communication (0/1)

Phase 4

4. False Positive Analysis (1/3)

Description

To find out who triggered the detection, look at the event timeline of the detection. Determine whose email address is connected to the event.

Notes

5 days ago

User Information

- User email: Ofer@cytechint.com
- Username: Ofer

Title

Add comment

CSPM Updates

Bug fixes in the Misconfigurations Table in Findings Menu

Revision #1
Created 16 September 2024 11:00:49 by Aldion Pueblos
Updated 16 September 2024 11:23:30 by Aldion Pueblos