

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

The screenshot displays the CISO Workplace interface for a specific case (Case: 6331). The main alert is titled "CyTech Case - Ensure S3 Bucket Policy is set to deny HTTP requests" and is categorized as "low" severity. The alert description states: "By default, Amazon S3 allows both HTTP and HTTPS requests. To achieve only allowing access to Amazon S3 objects through HTTPS you also have to explicitly deny access to HTTP requests. Bucket policies that allow HTTPS requests without explicitly denying HTTP requests will not comply with this recommendation." A "Re-investigate" button is visible next to the alert.

The interface is divided into several sections:

- Related Alerts (5):** A list of five alerts, all with the same title and severity, dated 05:15 AM.
- Framework:** Shows "Not Available" for the current alert.
- Timeline:** A section for viewing the alert's history.
- Investigation Guide:** A detailed guide for resolving the issue, starting with "From Console:" and listing steps: 1. Login to AWS Management Console... 2. Select the Check box next to the Bucket. 3. Click on 'Permissions'. 4. Click 'Bucket Policy'. 5. Add this to the existing policy filling in the required information. Below the steps is a JSON policy snippet:

```
{  "Sid": "<optional>",  "Effect": "Deny",  "Principal": "**",  "Action": "s3*",  "Resource": "arn:aws:s3::<bucket_name>/*",  "Condition": {    "Bool": {      "aws:SecureTransport": "false"    }  }  }
```
- Timeline Details:** A panel on the right showing a "Table" view of the alert's details, including a "signal.rule.note" field with a detailed explanation of the S3 bucket policy configuration and steps for remediation.

Security Assessment Questionnaires Updates

Support for Create Template Feature

Go back > Case: 10095

STEP 3 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

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

6 days ago

User Information

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

Edvir Davin 3 days ago

test update

test update desc

Normal B I U +

Cancel Save

Title

Go back > Case: 10095

STEP 3 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

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

6 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

STEP 3 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

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

6 days ago

User Information

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

Edvir Davin a minute ago

test update

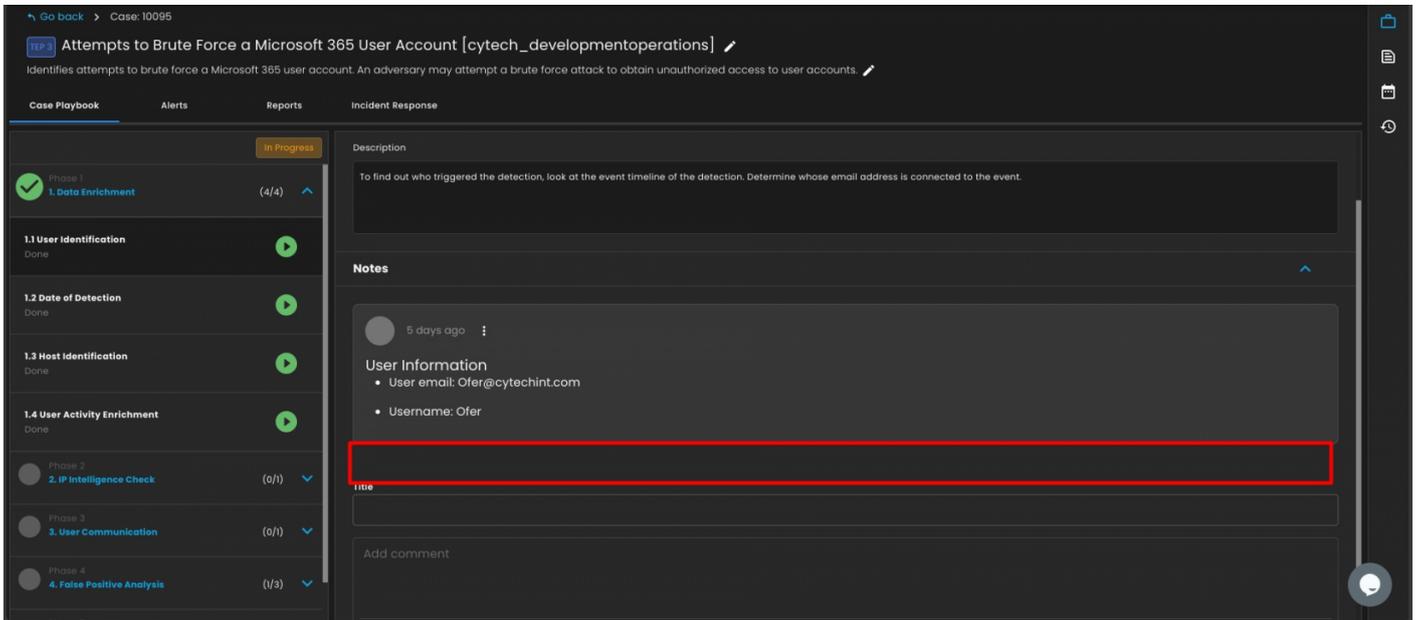
test update desc

Confirm Deletion

Are you sure you want to delete this note?

Cancel Delete

Title



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