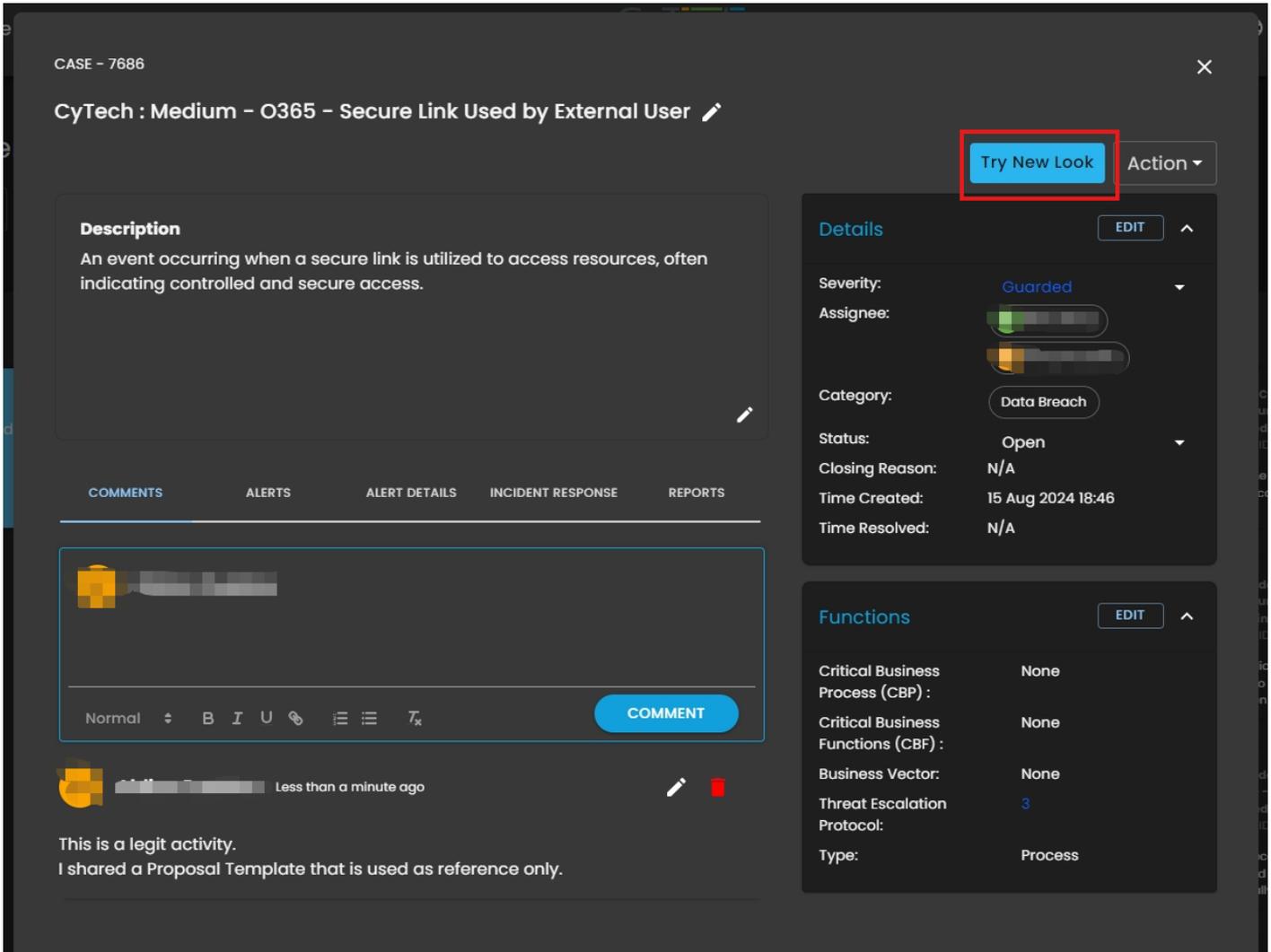


# Daily Update: August 15

Here are the main updates of the CISO Workplace:

**CIM** Updates:

CIM v3 New Look (Preview Version)



The screenshot displays a case detail view for 'CASE - 7686' titled 'CyTech : Medium - O365 - Secure Link Used by External User'. A red box highlights a 'Try New Look' button in the top right corner. The interface is divided into several sections:

- Description:** An event occurring when a secure link is utilized to access resources, often indicating controlled and secure access.
- Details:** A panel containing fields for Severity (Guarded), Assignee, Category (Data Breach), Status (Open), Closing Reason (N/A), Time Created (15 Aug 2024 18:46), and Time Resolved (N/A).
- Functions:** A panel with fields for Critical Business Process (CBP), Critical Business Functions (CBF), Business Vector, Threat Escalation Protocol (3), and Type (Process).
- Comments:** A section with a text input area, a 'COMMENT' button, and a recent comment from a user stating, 'This is a legit activity. I shared a Proposal Template that is used as reference only.'

Improved Case and Alerts Look and Feel

Go back

STEP 3 CyTech : Medium - O365 - Secure Link Used by External User ✎

An event occurring when a secure link is utilized to access resources, often indicating controlled and secure access. ✎

Case Playbook Alerts Reports Incident Response

Related Alerts (1)

- CyTech : Medium - O365 - Secure Link Used by External User  
medium  
04:38 PM

Overview

Specific Root Cause

N/A ✎

System Involved

o365 ✎

Location of Vulnerable System

None ✎

Users Involved

Case Details

Information  
Provides you with a brief overview of the case.

Severity  
guarded

Assignee  
Bon Zituny  
Vincent Sarte Assign...

Status  
Open

Time Created  
15 August 2024 18:46

Time Resolve  
Invalid date

Closing Reason  
Closing Reason

CRAM™ Details  
Provides you the information about the affected business processes.

Notes (1)  
Communicate and Collaborate here.

Semi-automated Alerts Details (Best effort) Auto-fill in the following fields:

- Systems Involved
- User Involved
- Location of Vulnerabilities
- Location of Threat
- Indicators

Go back

STEP 3 CyTech Case - Sharing Set & Added To Secure Link ✎

This event records when a user is added to a secure link, potentially providing them with secure access to resources. ✎

Case Playbook Alerts Reports Incident Response

Related Alerts (7)

- CyTech : Medium - O365 - Sharing Set  
medium  
04:30 PM
- CyTech : Medium - O365 - Added To Secure Link  
medium  
03:14 PM
- CyTech : Medium - O365 - Added To Secure Link  
medium  
03:14 PM
- CyTech : Medium - O365 - Sharing Set  
medium  
03:14 PM
- CyTech : Medium - O365 - Sharing Set  
medium  
03:14 PM
- CyTech : Medium - O365 - Sharing Set  
medium  
03:14 PM
- CyTech : Medium - O365 - Sharing Set  
medium  
03:14 PM

Overview

Specific Root Cause

The user had added the users into a secure link to access a file resource located on SharePoint that is related to a multimedia recording of a meeting. ✎

Show less

System Involved

SharePoint - Microsoft 365 ✎

Location of Vulnerable System

https://cytechco-my.sharepoint.com/personal/michillenem\_cytechint\_com/Documents/Recordings/Marketing Agenda Updates-20240815\_135906-Meeting Recording.mp4 ✎

Users Involved

Timeline Details

Table Json File (Raw)

No Timeline Selected

To view details, please select a timeline from the alert  
> related alerts > timeline.

Improved Timeline View

Go back

**STEP 2** CyTech : Medium - O365 - Secure Link Used by External User [↗](#)

An event occurring when a secure link is utilized to access resources, often indicating controlled and secure access. [↗](#)

Case Playbook Alerts Reports Incident Response

Related Alerts (1)

- CyTech : Medium - O365 - Secure Link Used by External User
  - External User
  - medium
  - 04:38 PM

Alert Details

Timeline

Jump to Change layout Change density

15 Aug, 2024 @ 16:38:19

localhost.localdomain 15 Aug, 2024 @ 16:38:19

SecureLinkUsed

User Name: urn:spa:guest#garay.val [↗](#)

Host Name: icloud.com

Source IP:49.147.122.168 [↗](#)

Destination IP:[↗](#)

Event Category: web

Event Outcome: success

Investigation Guide

Go back

**STEP 3** CyTech : Medium - O365 - Secure Link Used by External User [↗](#)

An event occurring when a secure link is utilized to access resources, often indicating controlled and secure access. [↗](#)

Case Playbook Alerts Reports Incident Response

Related Alerts (1)

- CyTech : Medium - O365 - Secure Link Used by External User
  - External User
  - medium
  - 04:38 PM

Alert Details

Timeline

Jump to Change layout Change density

15 Aug, 2024 @ 16:38:19

localhost.localdomain 15 Aug, 2024 @ 16:38:19

SecureLinkUsed

User Name: urn:spa:guest#garay.val [↗](#)

Host Name: icloud.com

Source IP:49.147.122.168 [↗](#)

Destination IP:[↗](#)

Event Category: web

Event Outcome: success

Investigation Guide

Timeline Details

Table Json File (Raw)

Filter by ... [↻](#)

Title	Value
_index	.internal.alerts-security.alerts-cytech_developmentoperations-000008
_id	7532854ce020484e61a7d65315af3289b61220e12551c25b8eb377daf0d21fa
_score	
fields.kibana.alert.severity-0	medium
fields.kibana.alert.workflow_status_updated_at-0	2024-08-15T10:46:18.985Z
fields.kibana.alert.rule.updated_by-0	elastic
fields.signal.ancestors.depth-0	
fields.event.category-0	web
fields.elastic_agent.version-0	8.12.0
fields.o365.audit.CorrelationId-0	ad7146a1-f013-9000-8e95-1e58aa23db9c
fields.user_agent.original.text-0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0

SHOW MORE

## Known Bugs:

- Error when Alert Details are modified/updated

## Limitations:

- Update of Case Details is not yet supported

## Revision #2

Created 15 August 2024 10:42:46 by Aldion Pueblos

Updated 15 August 2024 14:16:25 by Aldion Pueblos