

Daily Update: August 16

Here are the main updates of the CISO Workplace:

CIM v3 Updates:

Update in Editable Case Details:

The screenshot displays the 'Case Details' view for a 'CyTech Case - Sharing Set & Added To Secure Link'. The interface is dark-themed and includes a navigation bar at the top with 'Go back' and a breadcrumb trail. Below the breadcrumb, there are tabs for 'Case Playbook', 'Alerts', 'Reports', and 'Incident Response'. The main content area is divided into two columns. The left column shows 'Related Alerts (7)' with a list of alerts, each with a 'medium' severity and a timestamp of '03:14 PM'. The right column shows the 'Case Details' for the selected case. The 'Information' section is highlighted with a red box and contains the following details: Severity: Low; Status: In Progress; Assignee: Fredrik Dacer and Vincent Sarto; Category: Data Breach; Time Created: 15 August 2024 18:10; Time Resolve: ---; Closing Reason: Closing Reason. Below the 'Information' section, there are sections for 'CRAM™ Details' and 'Notes'.

Bug Fix in Editable Alert Details:

The screenshot displays the 'Case Details' view for a 'CyTech Case - Sharing Set & Added To Secure Link'. The interface is dark-themed and includes a navigation bar at the top with 'Go back' and a breadcrumb trail. Below the breadcrumb, there are tabs for 'Case Playbook', 'Alerts', 'Reports', and 'Incident Response'. The main content area is divided into two columns. The left column shows 'Related Alerts (7)' with a list of alerts, each with a 'medium' severity and a timestamp of '03:14 PM'. The right column shows the 'Case Details' for the selected case. The 'Overview' section is highlighted with a red box and contains the following details: Specific of 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; Systems 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. Below the 'Overview' section, there is a section for 'Users Involved'.

Update in Case Activity Details:

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 of 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

Systems 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

Activity Logs

Activity Type

- Case Activity: Edvir Davin modified a CaseKanban to In Progress status with id: 7685 2024-08-16 11:04:09.154810
- Case Activity: Edvir Davin modified a CaseKanban to Open status with id: 7685 2024-08-16 11:03:14.319781
- Case Activity: Fredrik Dacer modified a Case Title with id: 7685 2024-08-15 10:29:36.377923

Rich Text Support for Notepad

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

Alert Details

Details	Table	Json File (Row)
ID:214840cd19d0f16ea4e29285b79a8574756df22d2463255b9a2 beef0alees7ef		08-15-2024 04:30 PM

• CyTech : Medium - O365 - Sharing Set

This event is generated when sharing permissions or access is granted to users or entities, that is not Cytechint.com and outside the Office IP

Reason

web event with file Proposal_Contractor_Reference.docx, source 180.190.10.242 by urnspaguest#catilyn.jandog on

Notepad

Writing Notes with Rich Text

RM Updates

Support for Task Milestone

Milestone

Title *

Description

Date *

mm/dd/yyyy

SAVE

Task Table

Risk ID	Task ID	Task Title	Risk Owner	Assignee
RM27	4	Enabled AWS Cloudtrail	No Risk Owner	
RM27	5	Credentials Security Training	No Risk Owner	
RM60	20	This is a test		Zandra Narvaza
RM60	21	This is a test2		Zandra Narvaza

Task Completed: 0

Total Tasks: 4

Task Milestone: + CREATE MILESTONE

No Results Found

It looks like there's nothing to display at the moment. Try adding a milestone.

Task Gantt Chart

Search...

ONLY MY TASKS

SHOW ONGOING TASKS ONLY

Milestone

Overall Due

Task Name	Assignee	Start Date	End Date
milestone_title_nl		2024-08-14	2024-08-14
milestone_title_nl_1		2024-08-18	2024-08-18
milestone_title_nl_2		2024-08-25	2024-08-25
milestone_title_nl_3		2024-08-29	2024-08-29
wewwww		2024-09-29	2024-08-29
maaka kol		2024-08-15	2024-08-15
wowers		2024-08-15	2024-08-15
nge		2024-08-16	2024-08-16

Milestone

All Category

Project

Task

Milestone

15 Aug 16 Aug 17 Aug 18 Aug 19 Aug 20 Aug 21 Aug 22 Aug 23 Aug 24 Aug 25 Aug

Project Management Timeline

Overall Risk

- Context & Leadership/Defining Business Context & Mission
- Security eDiscovery and Forensic/Security & Privacy Attributes
- Data Security/Data Handling Procedures
- Network & Infrastructure Security/Endpoint Protection
- Security Threat Detection/Unauthorized Network Services

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

Task Overview

+ CREATE TASK

Overall Due

Unassigned Task: 5

New Tasks: 5

The screenshot displays a project management interface. At the top, a Gantt chart shows a timeline from August 13th to 25th, 2024. Below it is a table of tasks with columns for Task Name, Assignee, Start Date, and End Date. A modal window titled 'Milestone' is open, allowing the user to edit the title and date of a milestone.

Task Name	Assignee	Start Date	End Date
milestone_title_ni		2024-08-14	2024-08-14
milestone_title_ni_1		2024-08-18	2024-08-18
milestone_title_ni_2		2024-08-25	2024-08-25
milestone_title_ni_3		2024-08-29	2024-08-29
weewwww		2024-08-29	2024-08-29
maaka kol		2024-08-15	
wowers		2024-08-15	
nge		2024-08-16	

Milestone Modal Form:

Title: milestone_title_ni
 Date: 08/14/2024

Task Overview:

- Unassigned Task: 5
- New Tasks: 5
- Task Completed: 0
- Total Tasks: 7

Risk Assessment Drawer Updates

The screenshot shows a risk assessment interface. On the left, a 'Risk Details' drawer is open, displaying information about a risk with ID R260. On the right, a 'Mitigation Recommendation Form' is visible, which is highlighted with a red border. The form includes fields for 'Evaluation & Direction', 'Task', and 'Control Effectiveness'.

Risk Details:

- Risk ID: R260
- Risk Description: The organization lacks a structured approach for integrating security measures into the software development process, leaving systems vulnerable to security flaws and vulnerabilities.
- Risk Type: Administrative
- Method of Detection: Expert Judgment
- Risk Owner: Keith Gamana
- Risk Score: Very High
- Risk Tolerance: Very High
- Probability and Impact: Very High
- Level of Probability: Very High
- Level of Impact: Very High
- CIA Impact: asdasdasdasdasdasda: Very High
- Other Assets Affected

Mitigation Recommendation Form:

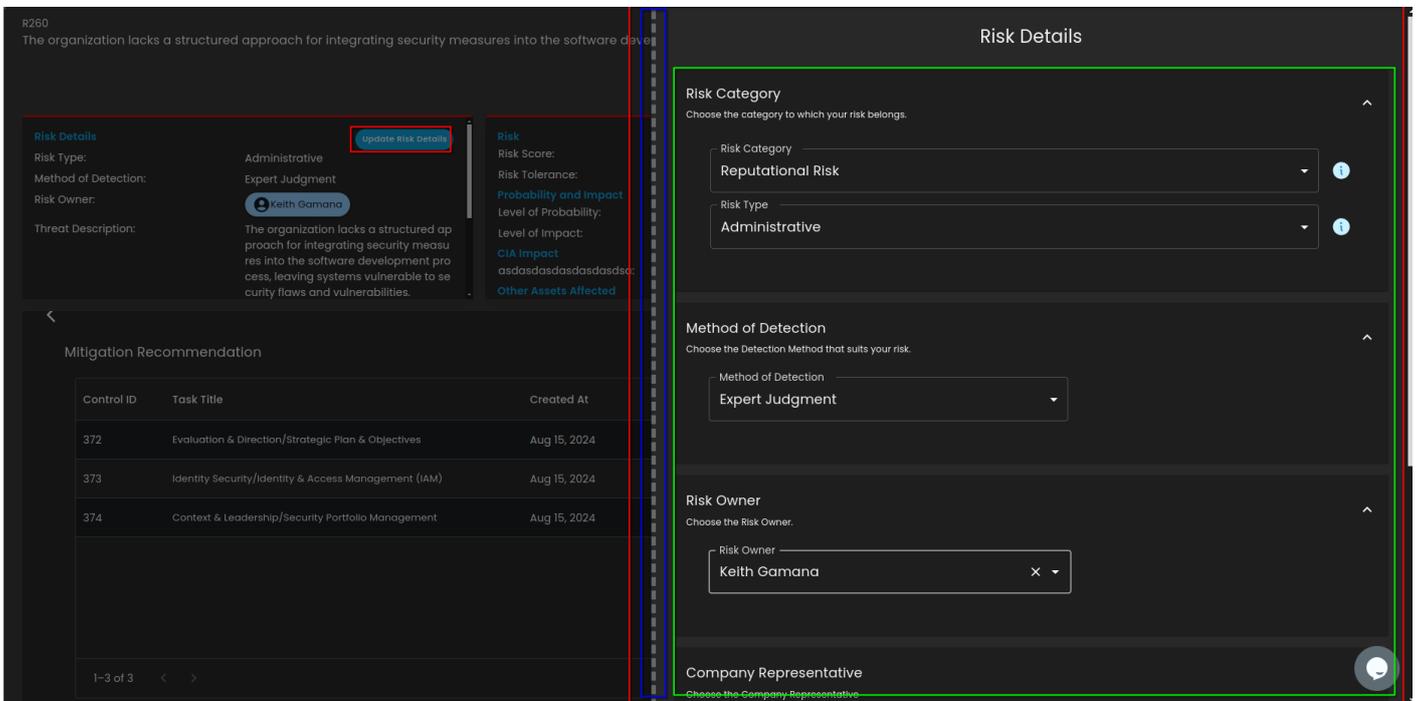
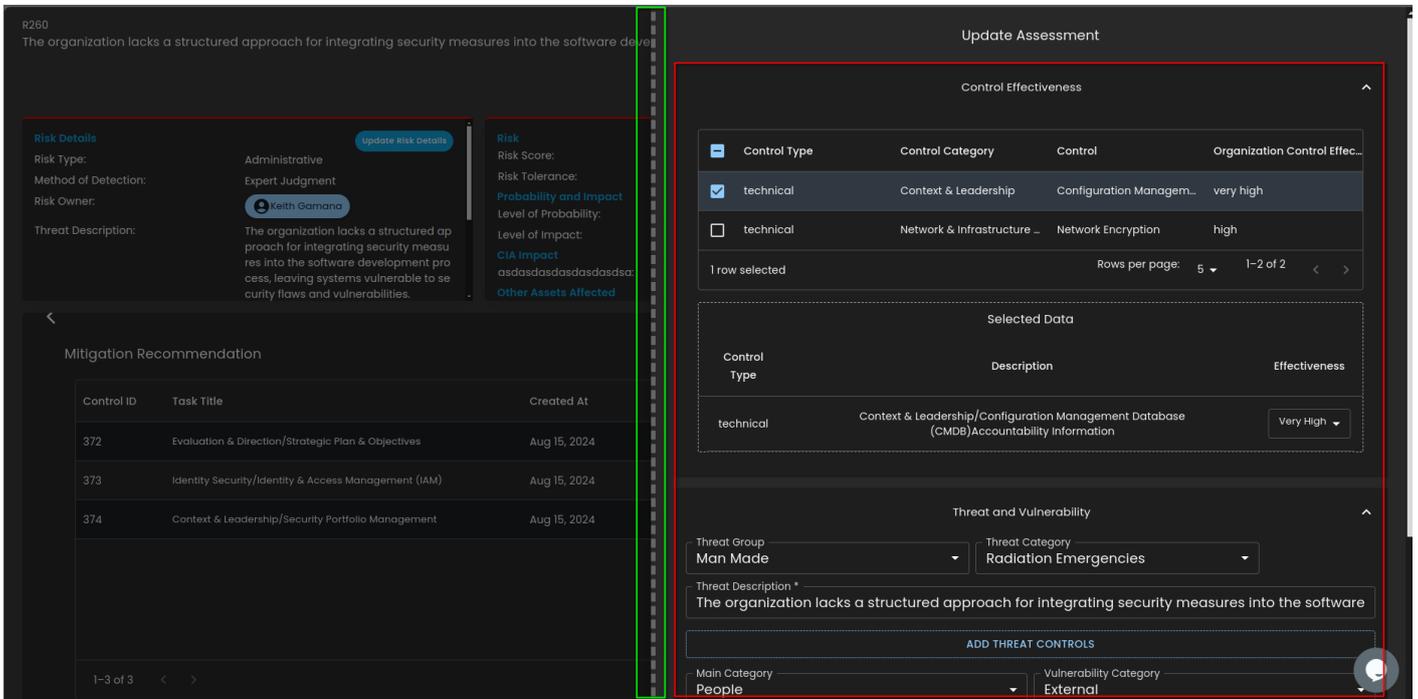
Prepare and reduce the impact of negative events by giving recommendations.

Evaluation & Direction:

- Controls Category: Evaluation & Direction
- Controls: Strategic Plan & Objectives
- Task: asdasd
- Task: asdasdasd
- Control Effectiveness: Very Low

Mitigation Recommendation Table:

Control ID	Task Title	Created At	Task Title
372	Evaluation & Direction/Strategic Plan & Objectives	Aug 15, 2024	very low
373	Identity Security/Identity & Access Management (IAM)	Aug 15, 2024	very low
374	Context & Leadership/Security Portfolio Management	Aug 15, 2024	high



Revision #1

Created 16 August 2024 11:07:35 by Aldion Pueblos

Updated 16 August 2024 11:34:45 by Aldion Pueblos