

Daily Update: August 30

Here are the main updates of the CISO Workplace:

CIM Updates:

Playbook Support in Cases

Limitation: Only 1 Playbook is currently defined: *Attempts to Brute force Alerts*

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

Playbooks: Attempts L Use Playbook

Phase 1

1. Data Enrichment

1.1 User Identification

1.2 Date of Detection

1.3 Host Identification

1.4 User Activity Enrichment

Phase 2

2. IP Intelligence Check

Phase 3

3. User Communication

Phase 4

4. False Positive Analysis

Phase 5

5. Escalation

1. Data Enrichment

1.1 User Identification

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.

1.2 Date of Detection

Description

Check for event timestamps in the detection or other relevant date and time values to potentially identify the exact date of when did the events had occurred.

1.3 Host Identification

Description

Relevant tags include user agent related values. These are tags related to the device used by the user to execute the said events.

1.4 User Activity Enrichment

Timeline Details

Table Json File (Raw)

Filter by ...

Title	Value
_index	.internal.alerts-security.alerts-cytech_developmentoperations-000008
_id	ddb2eefa6b3c3aa9d3e347c2ef617753c1654e7e430b671fb5024241c3945e76
_score	
fields.kibana.alert.severity-0	medium
fields.kibana.alert.workflow_status_updated_at-0	2024-08-30T03:55:32.140Z
fields.kibana.alert.rule.update_d_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	d5f04aa1-c07b-9000-92df-ab09d0034701
fields.user_agent.original.text-0	Mozilla/5.0 (Linux; Android; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0

Go back Case: 8871

STEP 3 CyTech : Medium - O365 - Remove-Mailbox

This event is generated when a mailbox is removed or deleted.

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)

Case Playbook

Phase

1.1 User Identification

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

Title

Add comment

Case Details

Information

Provides you with a brief overview of the case.

Severity Low Status Pending

Assignee Juniele Galbe +1 Assignees

Category General Categories

Time Created 28 August 2024 08:59 Time Resolve - - - -

Closing Reason Closing Reason

CRAM™ Details

Provides you the information about the affected business process

Notes

Communicate and Collaborate here.

Bug Fix for Notification Setting based on Case Notification

RM Updates

Size Adjustment to Risk Details

R69

The organization lacks a formal process for managing the termi

Risk Details

Risk Type: Technological

Method of Detection: Competitive Analysis

Risk Owner: Aldian Pueblos

Threat Description: --

Vulnerability Description: --

Company representative: Aldian Pueblos

Identified By: Aldian Pueblos

Update Risk

Recommendation Timeline

Control Name	Start Date	End Date	28 Aug
Context &	2024-08-29	2024-08-30	
Sample	2024-08-29	2024-08-30	

Accessor Response :

Prepare and reduce the impact of negative events by g

Risk Details

Risk Category

Choose the category to which your risk belongs.

Risk Category

Health Hazard Risk

Risk Type

Technological

Method of Detection

Choose the Detection Method that suits your risk.

Method of Detection

Competitive Analysis

Risk Owner

Choose the Risk Owner.

Risk Owner

Aldian Pueblos

Company Representative

Choose the Company Representative

Layout and component adjustments in the Task Management

Task Gantt Chart

Search...

Task Name	Assignee	Start Date	End Date	27 Jun	28 Jun	29 Jun	30 Jun	1 Jul	2 Jul	3 Jul	4 Jul	5 Jul	6 Jul	7 Jul	8 Jul	9 Jul	10 Jul	11 Jul	12 Jul	13 Jul	14 Jul	15 Jul	16 Jul	17 Jul	18 Jul	19 Jul	20 Jul	21 Jul	22 Jul	23 Jul	24 Jul	25 Jul	26 Jul	27 Jul	28 Jul	29 Jul	30 Jul	31 Jul
Enabled AWS Cloudtrail	Zandro Navassa	2024-06-08	2024-06-15	Enabled AWS Cloudtrail																																		
Credential Security Tr	Zandro Navassa	2024-06-08	2024-06-15	Credential Security Training																																		
This is a test	Zandro Navassa	2024-07-19	2024-07-20																																			
This is a test2	Zandro Navassa	2024-07-20	2024-07-21																																			
Enabled AWS Cloudtrail	Zandro Navassa	2024-06-09	2024-06-09																																			
Enabled AWS Cloudtrail	Zandro Navassa	2024-07-27	2024-07-27																																			

Task Table

Search...

Risk ID	Task ID	Task Title	Risk Owner	Assignee	Start Date	End Date	Status
RM27	4	Enabled AWS Cloudtrail	No Risk Owner	Zandro Navassa	Jun 8, 2024	Jun 15, 2024	not started
RM27	5	Credential Security Training	No Risk Owner	No Assignee	Jun 8, 2024	Jun 15, 2024	not started
RM60	20	This is a test	Zandro Navassa	Zandro Navassa	Jul 19, 2024	Jul 20, 2024	In progress
RM60	21	This is a test2	Zandro Navassa	No Assignee	Jul 20, 2024	Jul 21, 2024	not started
RM27	27	Enabled AWS Cloudtrail	No Risk Owner	Zandro Navassa	Jun 9, 2024	Jun 9, 2024	not started
RM27	28	Enabled AWS Cloudtrail	No Risk Owner	Zandro Navassa	Jul 27, 2024	Jul 27, 2024	not started

1-6 of 6

Task Overview

CREATE TASK

Overall Due

Unassigned Task

2

New Tasks

5

Task Completed

0

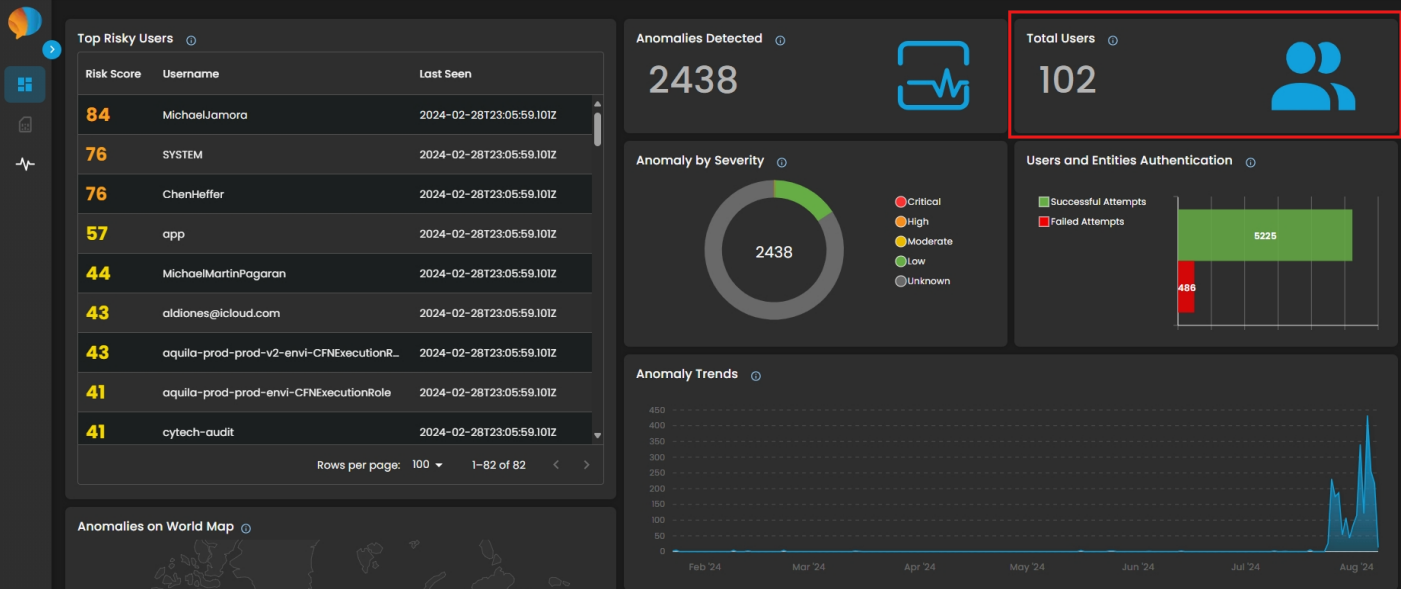
Total Tasks

6

UEBA Updates

Bug Fix for the detecting Total Users

Bug Fixes in Dashboard



Revision #1
Created 30 August 2024 05:07:33 by Aldion Pueblos
Updated 30 August 2024 11:37:22 by Aldion Pueblos