November 2024

The daily updates for the month of November 2024

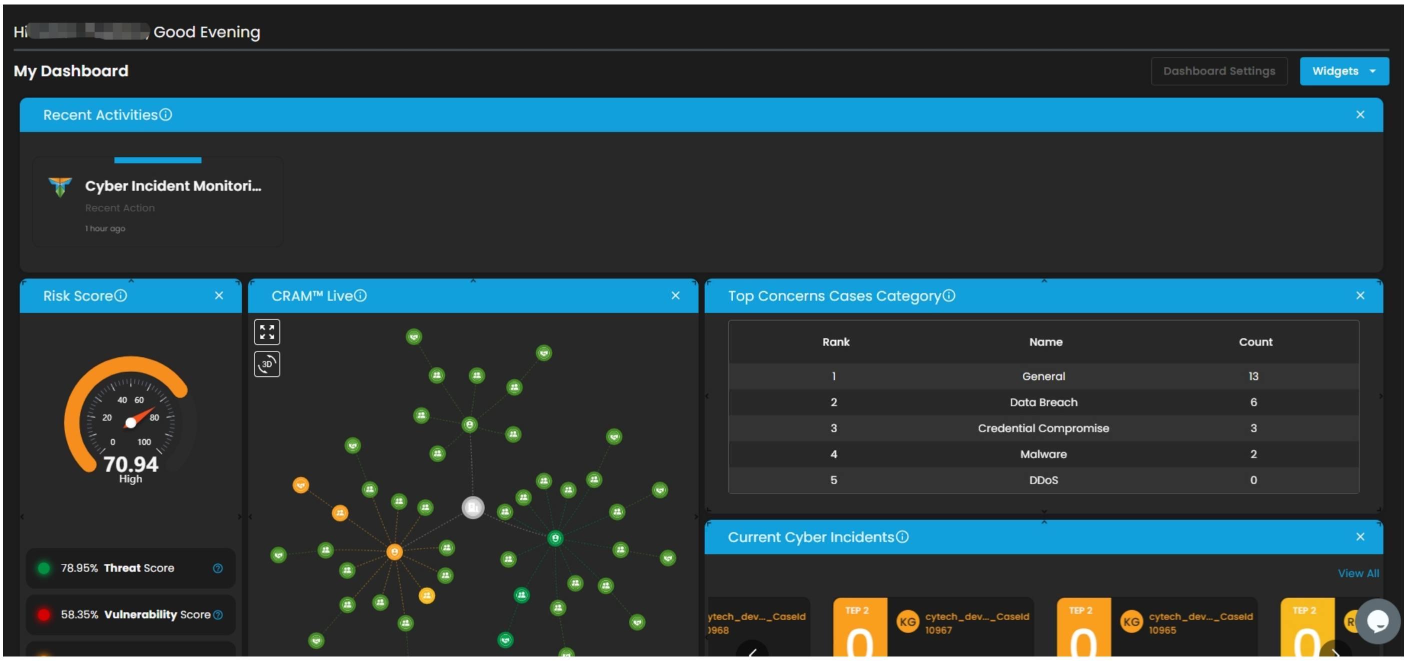
- Daily Update: November 4
- Daily Update: November 6
- Daily Update: November 8

Daily Update: November 4

Here are the main updates of the CISO Workplace:

General Updates:

Redirect to Home on Switch Client



Hi [redacted], Good Evening

My Dashboard

Recent Activities

Cyber Incident Monitori...

Recent Action

1 hour ago

Risk Score

70.94 High

78.95% **Threat** Score

58.35% **Vulnerability** Score

CRAM™ Live

Top Concerns Cases Category

Rank	Name	Count
1	General	13
2	Data Breach	6
3	Credential Compromise	3
4	Malware	2
5	DDoS	0

Current Cyber Incidents

ytech_dev..._CaseId)968

TEP 2 0 KG cytech_dev..._CaseId 10967

TEP 2 0 KG cytech_dev..._CaseId 10965

TEP 2 0 R

Bug fixes:

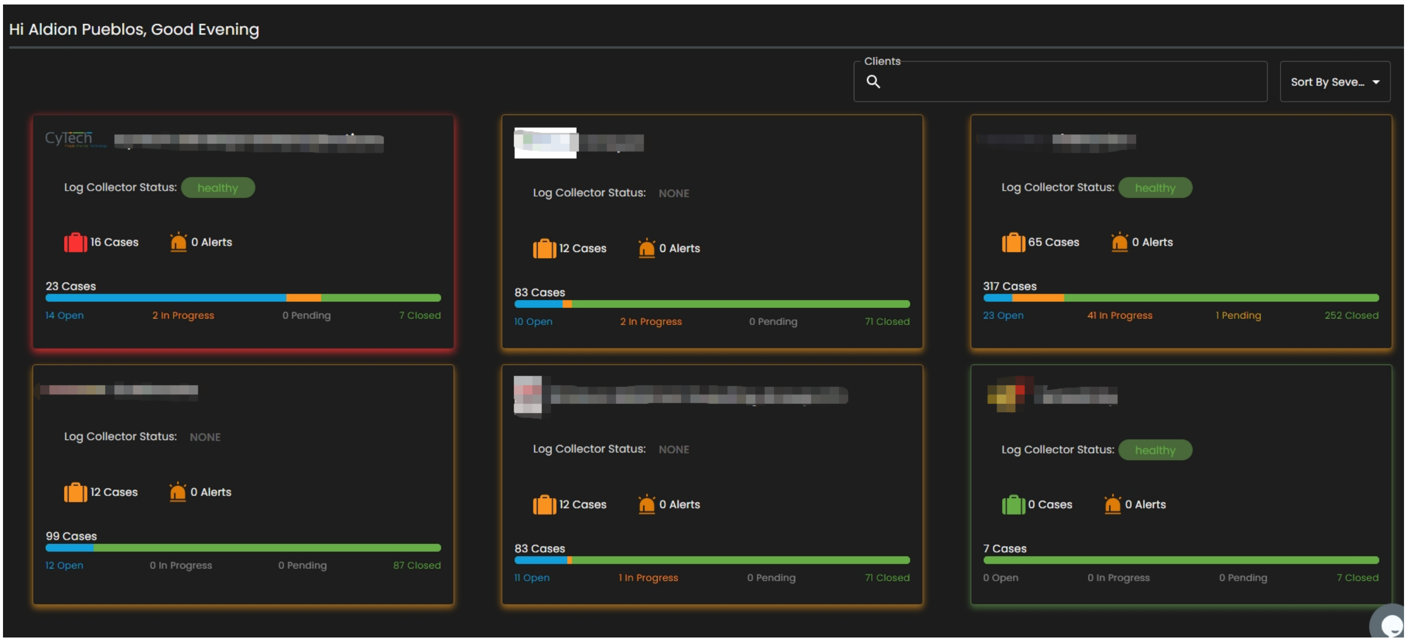
1. Missing Requirements in Compliance Gap Analysis
2. Updated the Severity Filter in CIM Kanban

Daily Update: November 6

Here are the main updates of the CISO Workplace:

General Updates:

Support for MSSP Dashboard



Hi Aldion Pueblos, Good Evening

CyTech [redacted]

Log Collector Status: healthy

16 Cases 0 Alerts

23 Cases

14 Open 2 In Progress 0 Pending 7 Closed

[redacted]

Log Collector Status: NONE

12 Cases 0 Alerts

83 Cases

10 Open 2 In Progress 0 Pending 71 Closed

[redacted]

Log Collector Status: healthy

65 Cases 0 Alerts

317 Cases

23 Open 41 In Progress 1 Pending 252 Closed

[redacted]

Log Collector Status: NONE

12 Cases 0 Alerts

99 Cases

12 Open 0 In Progress 0 Pending 87 Closed

[redacted]

Log Collector Status: NONE

12 Cases 0 Alerts

83 Cases

11 Open 1 In Progress 0 Pending 71 Closed

[redacted]

Log Collector Status: healthy

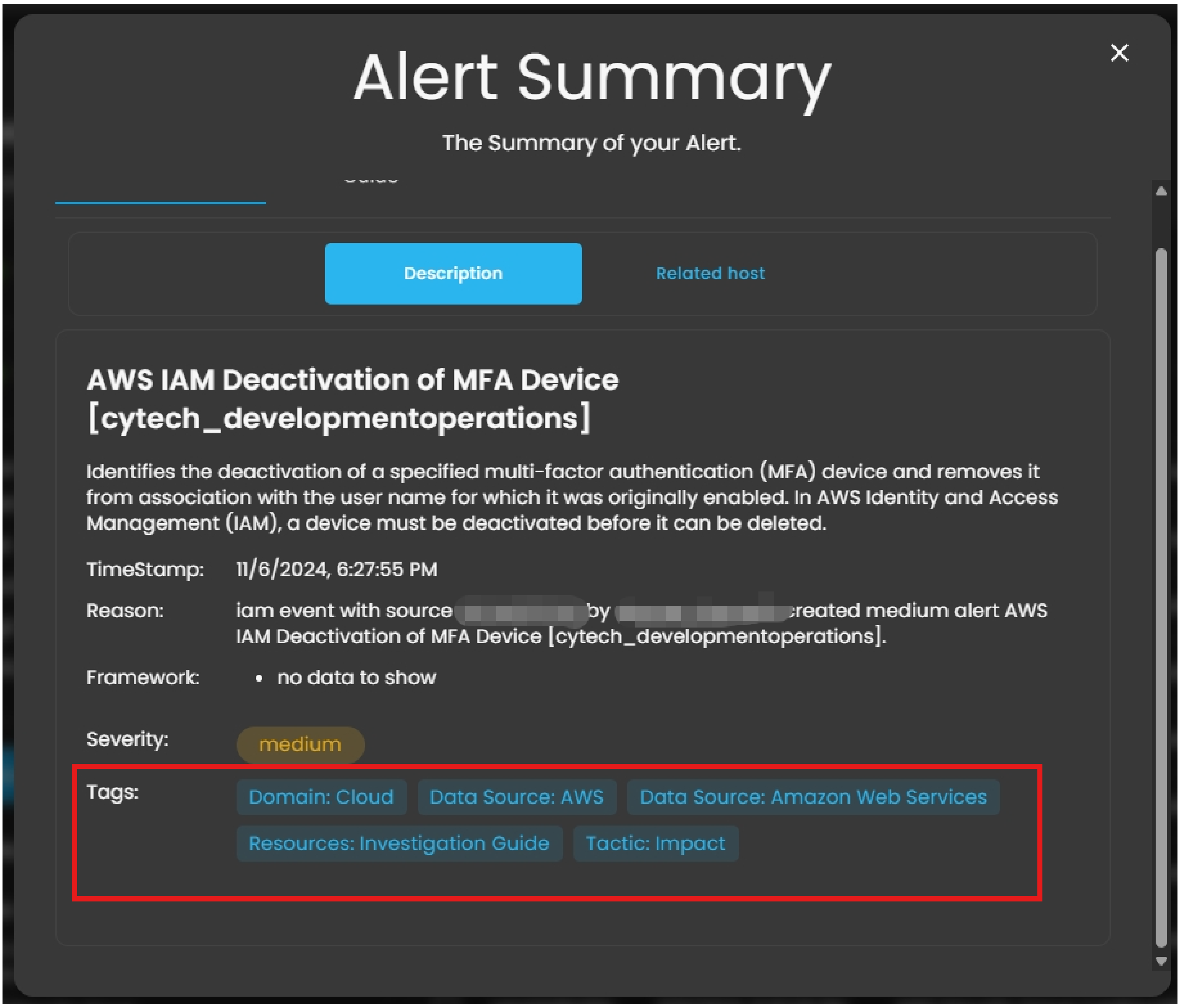
0 Cases 0 Alerts

7 Cases

0 Open 0 In Progress 0 Pending 7 Closed

CIM Updates:

Indicate Log Source in Alerts



Alert Summary

The Summary of your Alert.

AWS IAM Deactivation of MFA Device [cytech_developmentoperations]

Identifies the deactivation of a specified multi-factor authentication (MFA) device and removes it from association with the user name for which it was originally enabled. In AWS Identity and Access Management (IAM), a device must be deactivated before it can be deleted.

TimeStamp: 11/6/2024, 6:27:55 PM

Reason: iam event with source [redacted] by [redacted] created medium alert AWS IAM Deactivation of MFA Device [cytech_developmentoperations].

Framework:
- no data to show

Severity: medium

Tags: Domain: Cloud | Data Source: AWS | Data Source: Amazon Web Services | Resources: Investigation Guide | Tactic: Impact

Bug fix Updates:

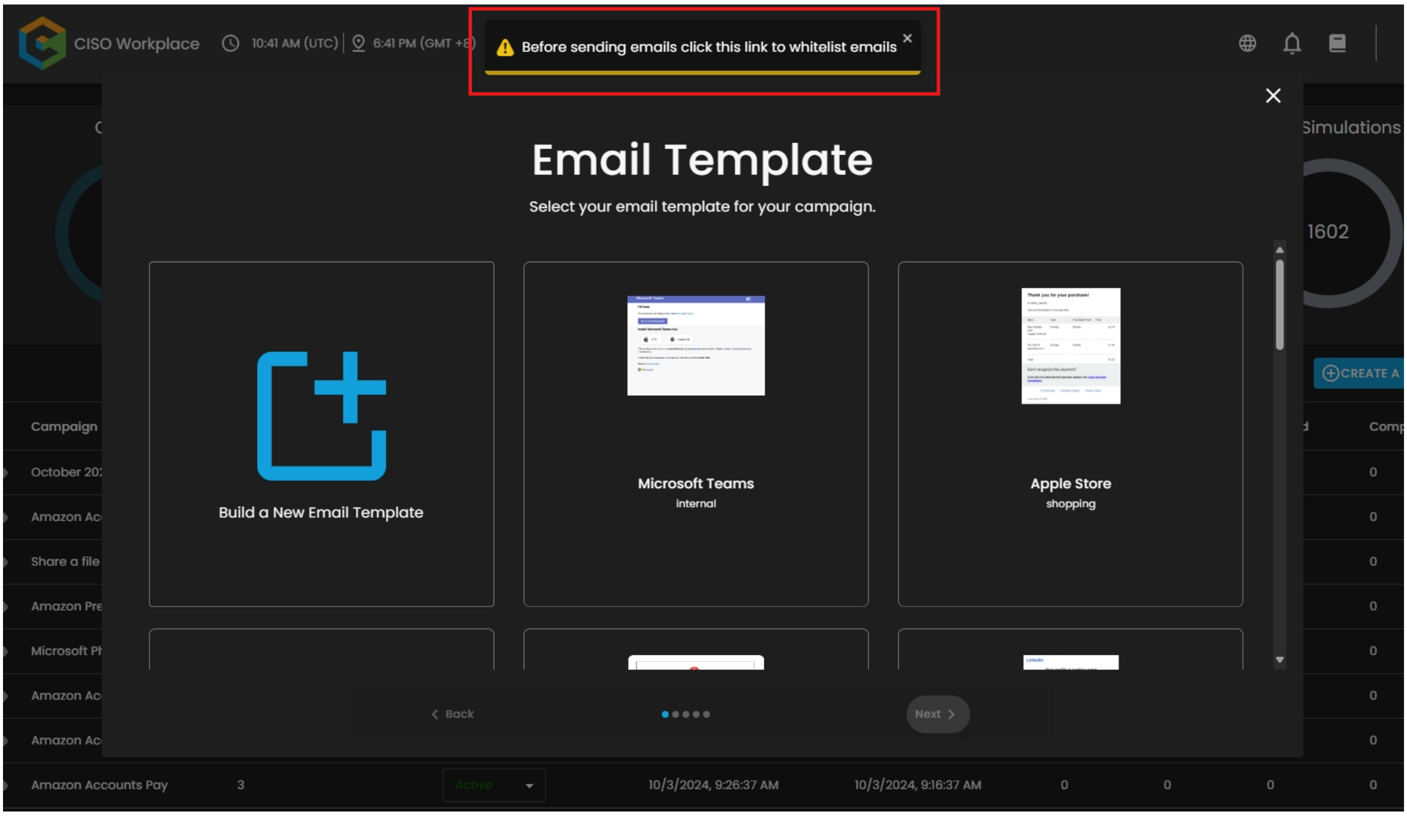
1) Bug Fixes in CISO Workplan Module

Daily Update: November 8

Here are the main updates of the CISO Workplace:

Phishing Simulation Updates:

Added link to Whitelist Manual



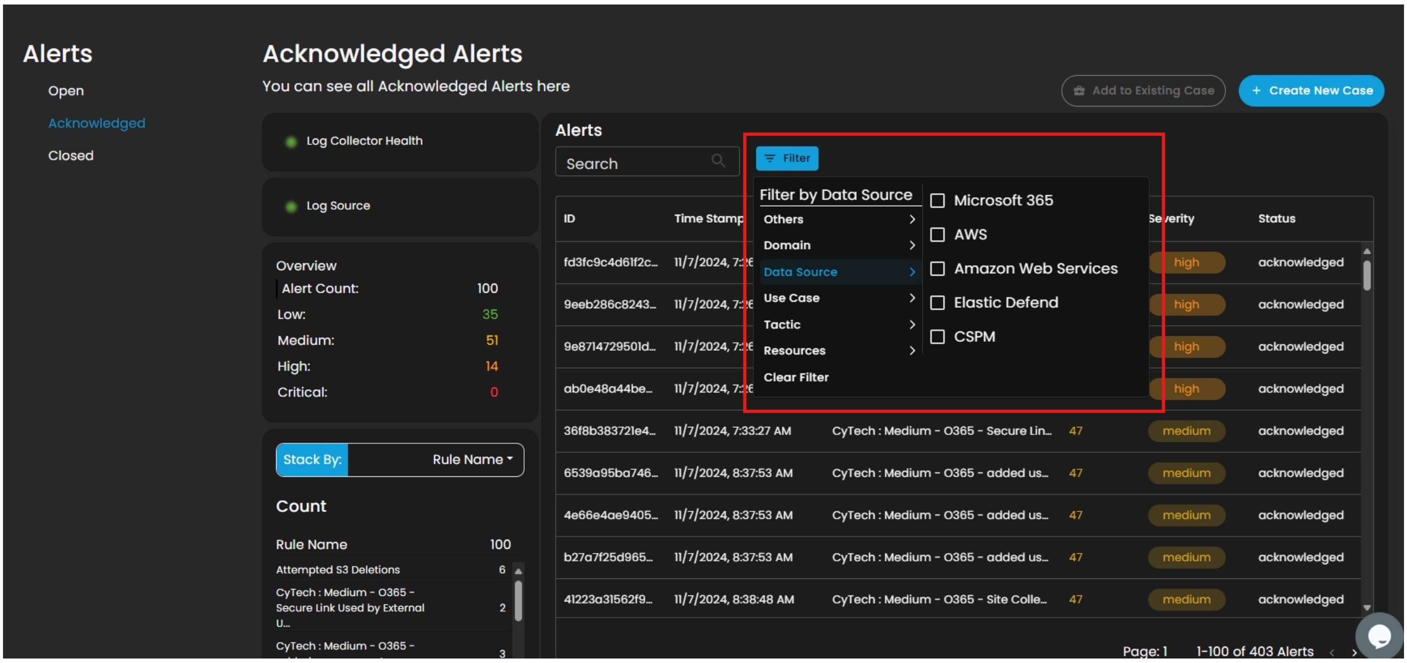
Before sending emails click this link to whitelist emails

Email Template

Select your email template for your campaign.

CIM Updates:

Filter alerts by tags such as Data Source



Alerts

Open

Acknowledged

Closed

Acknowledged Alerts

You can see all Acknowledged Alerts here

Add to Existing Case

+ Create New Case

Log Collector Health

Log Source

Overview

Alert Count:	100
Low:	35
Medium:	51
High:	14
Critical:	0

Stack By: Rule Name

Count

Rule Name	100
Attempted S3 Deletions	6
CyTech : Medium - O365 - Secure Link Used by External U...	2
CyTech : Medium - O365 -	3

Alerts

Search

Filter

Filter by Data Source

- Others >
- Domain >
- Data Source >
- Use Case >
- Tactic >
- Resources >
- Clear Filter

□ Microsoft 365

□ AWS

□ Amazon Web Services

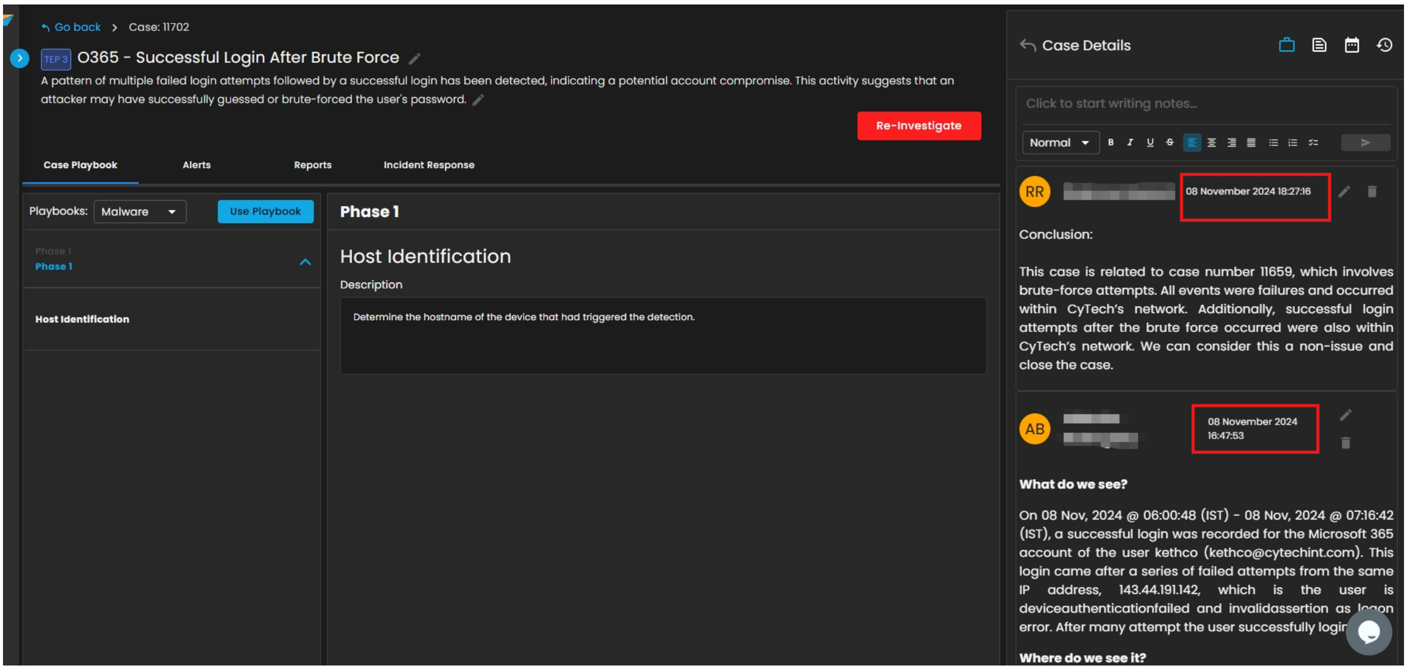
□ Elastic Defend

□ CSPM

ID	Time Stamp			Severity	Status
fd3fc9c4d61f2c...	11/7/2024, 7:26			high	acknowledged
9eeb286c8243...	11/7/2024, 7:26			high	acknowledged
9e8714729501d...	11/7/2024, 7:26			high	acknowledged
ab0e48a44be...	11/7/2024, 7:26			high	acknowledged
36f8b383721e4...	11/7/2024, 7:33:27 AM	CyTech : Medium - O365 - Secure Lin...	47	medium	acknowledged
6539a95ba746...	11/7/2024, 8:37:53 AM	CyTech : Medium - O365 - added us...	47	medium	acknowledged
4e66e4ae9405...	11/7/2024, 8:37:53 AM	CyTech : Medium - O365 - added us...	47	medium	acknowledged
b27a7f25d965...	11/7/2024, 8:37:53 AM	CyTech : Medium - O365 - added us...	47	medium	acknowledged
41223a31562f9...	11/7/2024, 8:38:48 AM	CyTech : Medium - O365 - Site Colle...	47	medium	acknowledged

Page: 1   1-100 of 403 Alerts

Comments sorted in Descending Order



Go back > Case: 11702

TEP 3 O365 - Successful Login After Brute Force

A pattern of multiple failed login attempts followed by a successful login has been detected, indicating a potential account compromise. This activity suggests that an attacker may have successfully guessed or brute-forced the user's password.

Re-Investigate

Case Playbook | Alerts | Reports | Incident Response

Playbooks: Malware

Use Playbook

Phase 1

Phase 1

Host Identification

Phase 1

Host Identification

Description

Determine the hostname of the device that had triggered the detection.

Case Details

Click to start writing notes...

Normal

RR [redacted] 08 November 2024 18:27:16

Conclusion:

This case is related to case number 11659, which involves brute-force attempts. All events were failures and occurred within CyTech's network. Additionally, successful login attempts after the brute force occurred were also within CyTech's network. We can consider this a non-issue and close the case.

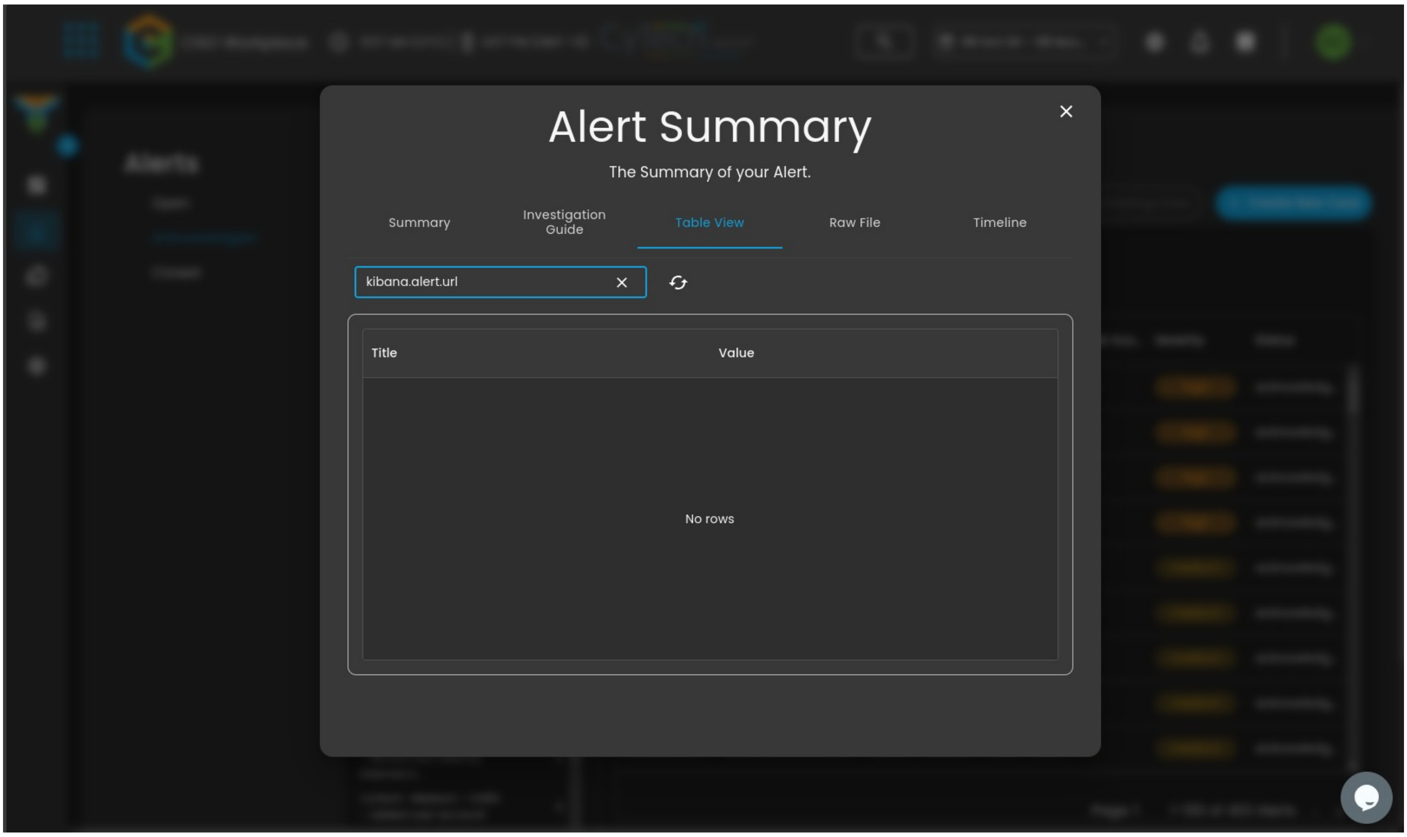
AB [redacted] 08 November 2024 16:47:53

What do we see?

On 08 Nov, 2024 @ 06:00:48 (IST) - 08 Nov, 2024 @ 07:16:42 (IST), a successful login was recorded for the Microsoft 365 account of the user kethco (kethco@cytechint.com). This login came after a series of failed attempts from the same IP address, 143.44.191.142, which is the user is deviceauthenticationfailed and invalidassertion as logon error. After many attempt the user successfully login

Where do we see it?

Omit Alerts Fields with Elastic URLs



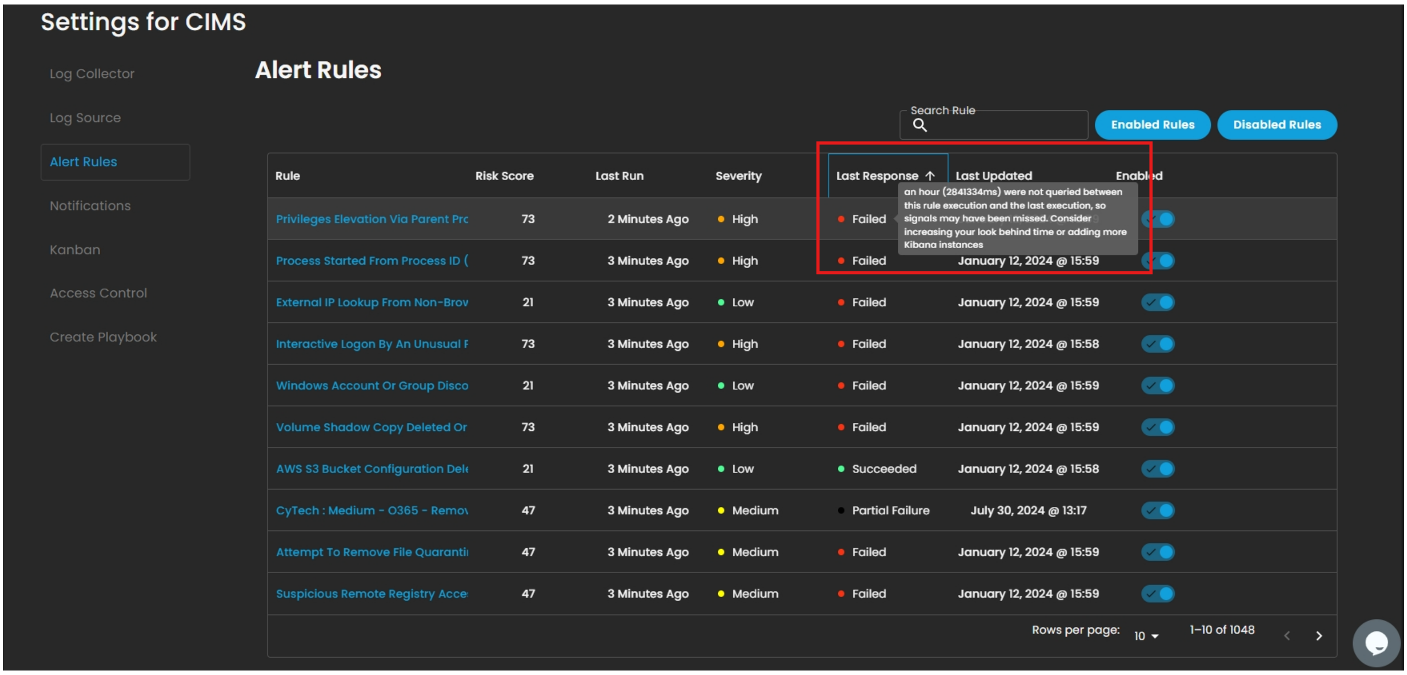
Alert Summary

The Summary of your Alert.

kibana.alert.url

Title	Value
No rows	

Provide more message to Alerts Last Response



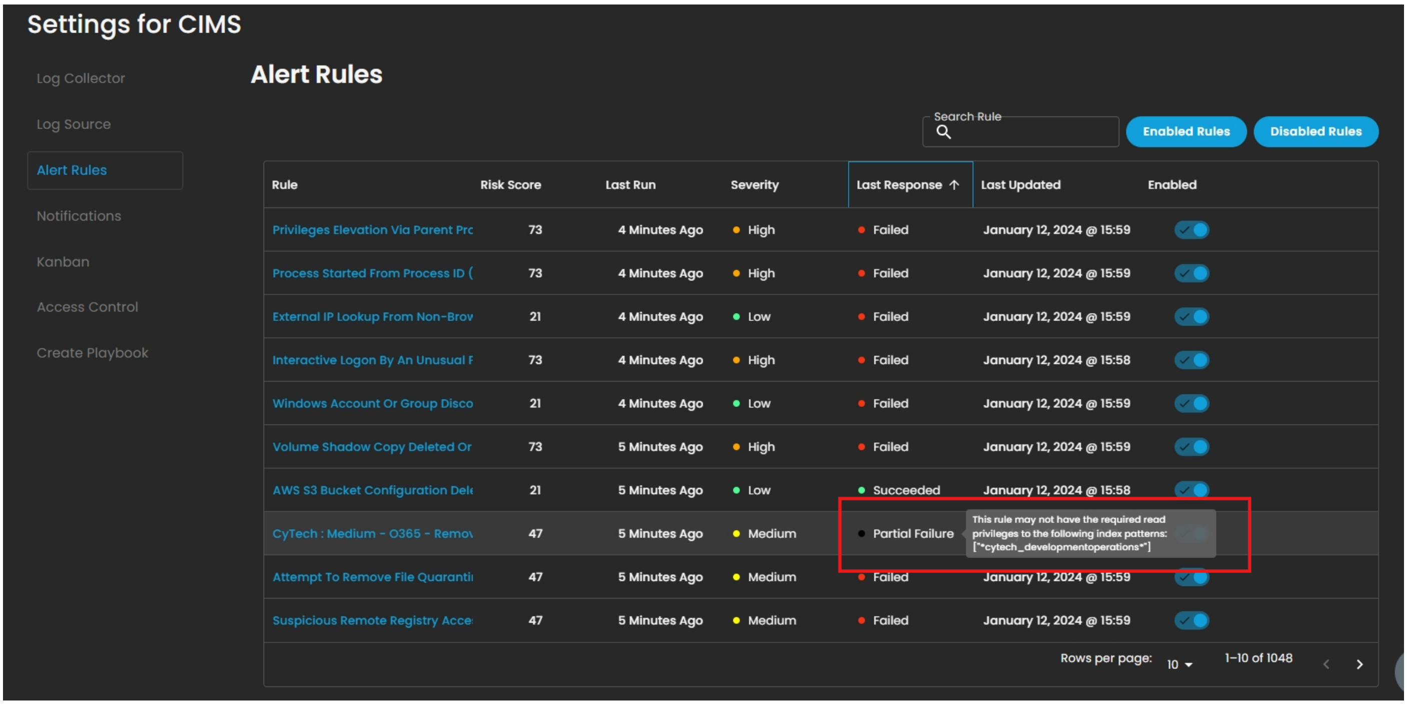
Settings for CIMS

Alert Rules

an hour (2841334ms) were not queried between this rule execution and the last execution, so signals may have been missed. Consider increasing your look behind time or adding more Kibana instances

Rule	Risk Score	Last Run	Severity	Last Response ↑	Last Updated	Enabled
Privileges Elevation Via Parent Prc	73	2 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:59	✓
Process Started From Process ID (	73	3 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:59	✓
External IP Lookup From Non-Brov	21	3 Minutes Ago	● Low	● Failed	January 12, 2024 @ 15:59	✓
Interactive Logon By An Unusual F	73	3 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:58	✓
Windows Account Or Group Disco	21	3 Minutes Ago	● Low	● Failed	January 12, 2024 @ 15:59	✓
Volume Shadow Copy Deleted Or	73	3 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:59	✓
AWS S3 Bucket Configuration Dele	21	3 Minutes Ago	● Low	● Succeeded	January 12, 2024 @ 15:58	✓
CyTech : Medium - O365 - Remo\	47	3 Minutes Ago	● Medium	● Partial Failure	July 30, 2024 @ 13:17	✓
Attempt To Remove File Quaranti	47	3 Minutes Ago	● Medium	● Failed	January 12, 2024 @ 15:59	✓
Suspicious Remote Registry Acce	47	3 Minutes Ago	● Medium	● Failed	January 12, 2024 @ 15:59	✓

Rows per page: 10 ▾ 1–10 of 1048 ‹ ›



Settings for CIMS

Alert Rules

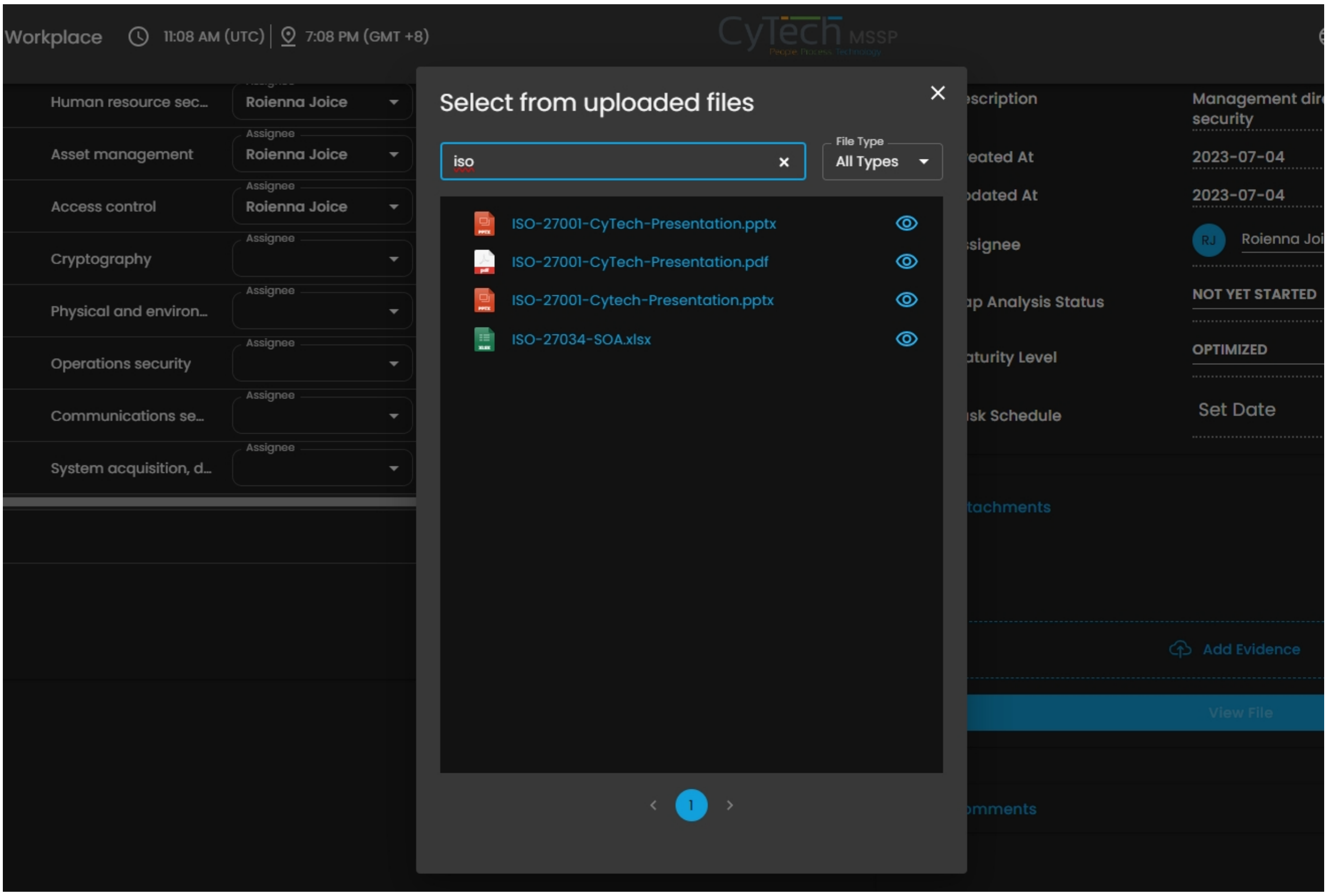
Rule	Risk Score	Last Run	Severity	Last Response ↑	Last Updated	Enabled
Privileges Elevation Via Parent Prc	73	4 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:59	✓
Process Started From Process ID (	73	4 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:59	✓
External IP Lookup From Non-Brov	21	4 Minutes Ago	● Low	● Failed	January 12, 2024 @ 15:59	✓
Interactive Logon By An Unusual F	73	4 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:58	✓
Windows Account Or Group Disco	21	4 Minutes Ago	● Low	● Failed	January 12, 2024 @ 15:59	✓
Volume Shadow Copy Deleted Or	73	5 Minutes Ago	● High	● Failed	January 12, 2024 @ 15:59	✓
AWS S3 Bucket Configuration Dele	21	5 Minutes Ago	● Low	● Succeeded	January 12, 2024 @ 15:58	✓
CyTech : Medium - O365 - Remov	47	5 Minutes Ago	● Medium	● Partial Failure		
Attempt To Remove File Quarantii	47	5 Minutes Ago	● Medium	● Failed	January 12, 2024 @ 15:59	✓
Suspicious Remote Registry Acce	47	5 Minutes Ago	● Medium	● Failed	January 12, 2024 @ 15:59	✓

This rule may not have the required read privileges to the following index patterns: ["*cytech_developmentoperations*"]

Rows per page: 10 ▾ 1–10 of 1048 ‹ ›

Compliance Updates

Improvement in the Evidence List Modal



	Assignee
Human resource sec...	Roienna Joice
Asset management	Roienna Joice
Access control	Roienna Joice
Cryptography	
Physical and environ...	
Operations security	
Communications se...	
System acquisition, d...	

Select from uploaded files

iso ×

File Type: All Types ▾

- ISO-27001-CyTech-Presentation.pptx
- ISO-27001-CyTech-Presentation.pdf
- ISO-27001-Cytech-Presentation.pptx
- ISO-27034-SOA.xlsx

‹ 1 ›

escription: Management dir security
eated At: 2023-07-04
pdated At: 2023-07-04
ssignee: RJ Roienna Joi
ap Analysis Status: NOT YET STARTED
aturity Level: OPTIMIZED
isk Schedule: Set Date