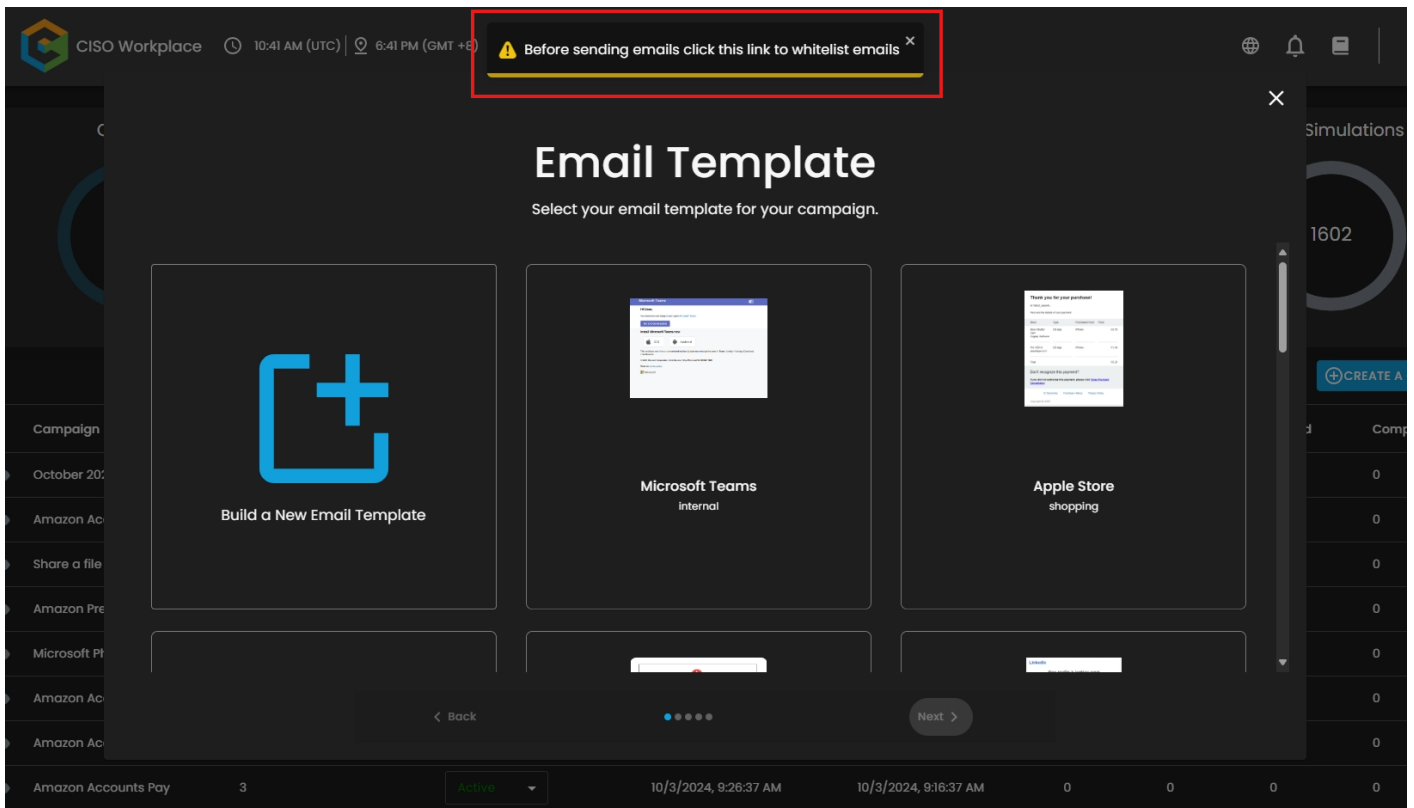


Daily Update: November 8

Here are the main updates of the CISO Workplace:

Phishing Simulation Updates:

Added link to Whitelist Manual



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

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, 7:06 | high | acknowledged |
| 9eeb286c8243... | 11/7/2024, 7:06 | high | acknowledged |
| 9e8714729501d... | 11/7/2024, 7:06 | high | acknowledged |
| ab0e48a44be... | 11/7/2024, 7:06 | high | acknowledged |
| 36f8b383721e4... | 11/7/2024, 7:33:27 AM | medium | acknowledged |
| 6539a95ba746... | 11/7/2024, 8:37:53 AM | medium | acknowledged |
| 4e66e4ae9405... | 11/7/2024, 8:37:53 AM | medium | acknowledged |
| b27a7f25d965... | 11/7/2024, 8:37:53 AM | medium | acknowledged |
| 41223a31562f9... | 11/7/2024, 8:38:48 AM | medium | acknowledged |

Page: 1 1-100 of 403 Alerts

Comments sorted in Descending Order

Go back > Case: 11702

STEP 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 B I U L Link Image Bold Italic Underline Link Image Bold Italic Underline Link Image Bold Italic Underline Link Image Bold Italic Underline

RR

08 November 2024 18:27:18

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

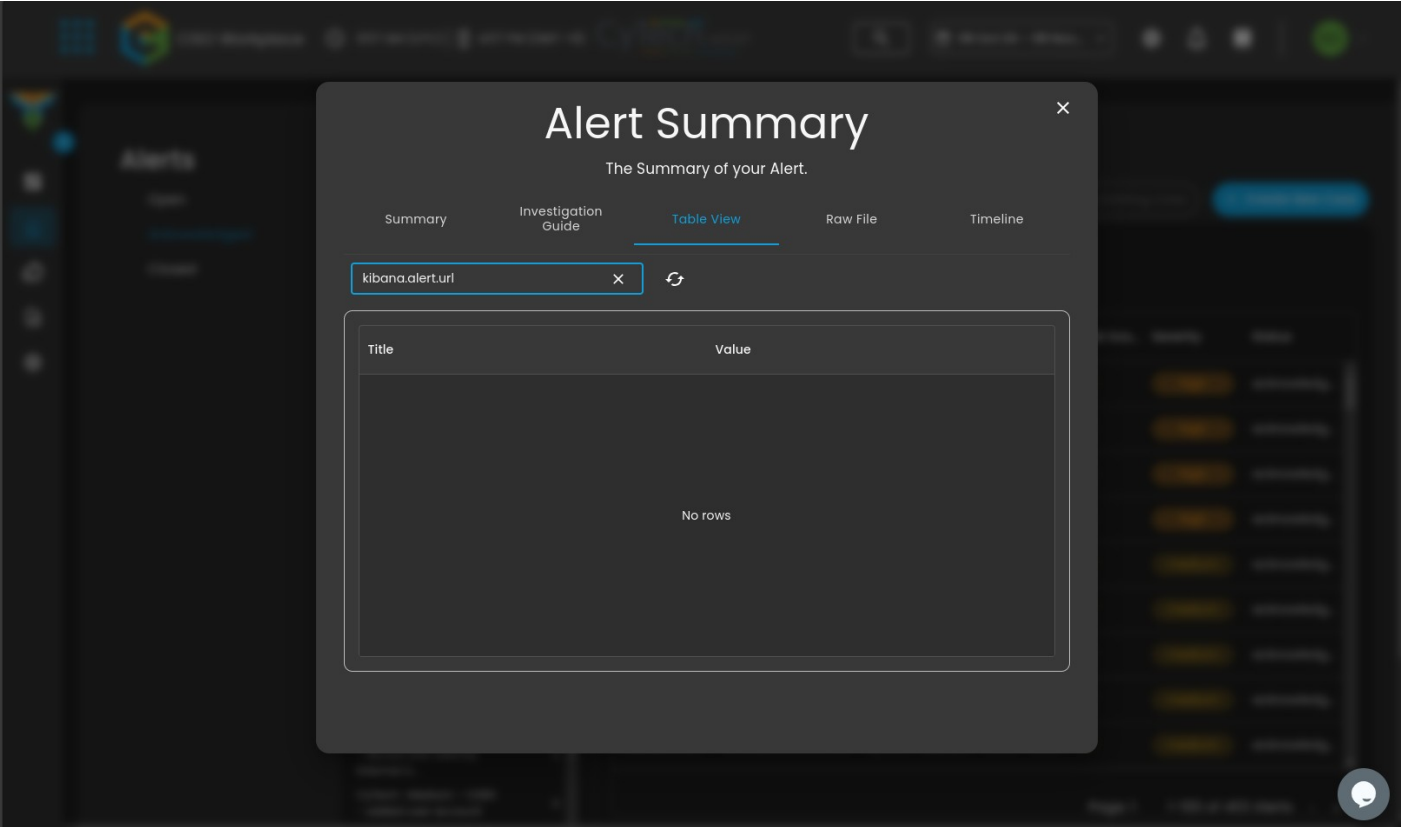
08 November 2024 18:47:53

What do we see?

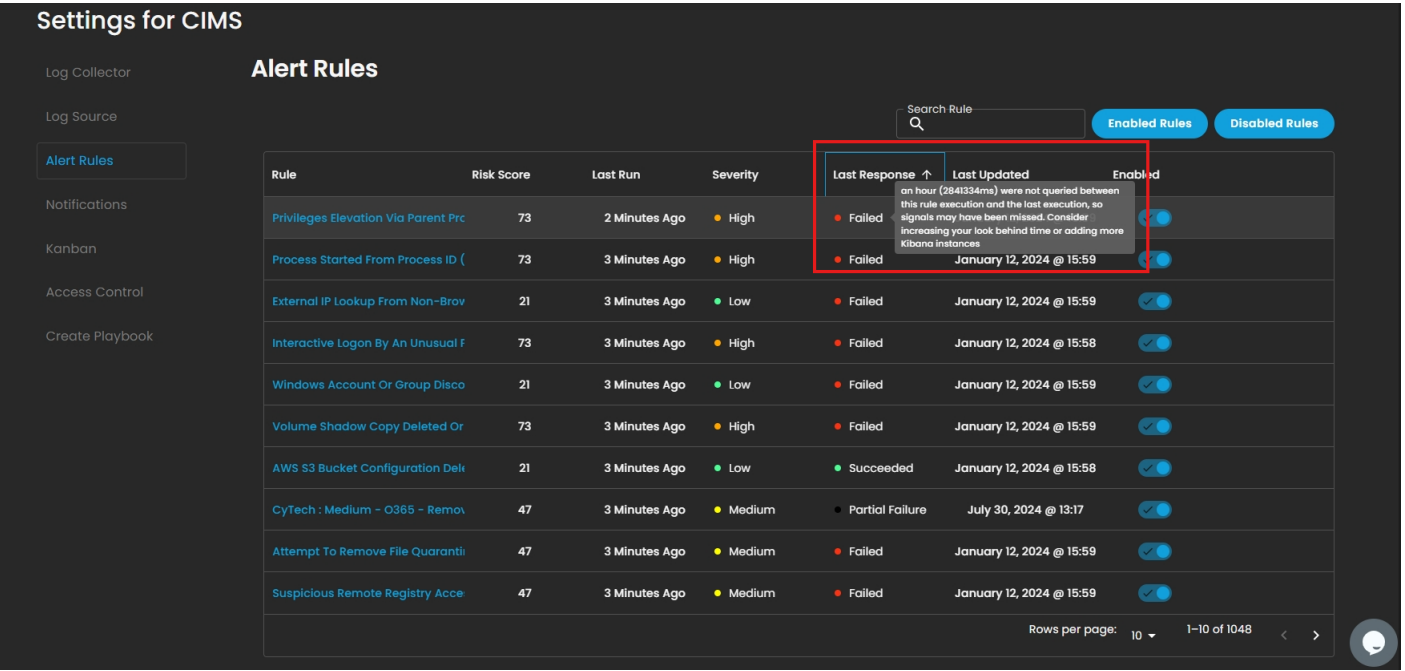
On 08 Nov, 2024 @ 06:00:48 (IST) - 08 Nov, 2024 @ 07:16:42 (IST), a successful login was recorded for the Microsoft 365 account of the user kethco (kethco@cytechint.com). This login came after a series of failed attempts from the same IP address, 143.44.191.142, which is the user is deviceauthenticationfailed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

Where do we see it?

Omit Alerts Fields with Elastic URLs



Provide more message to Alerts Last Response



Settings for CIMS

Log Collector

Log Source

Alert Rules

Notifications

Kanban

Access Control

Create Playbook

Alert Rules

Search Rule

Enabled Rules

Disabled 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 | <input checked="" type="checkbox"/> |
| Process Started From Process ID (| 73 | 4 Minutes Ago | High | Failed | January 12, 2024 @ 15:59 | <input checked="" type="checkbox"/> |
| External IP Lookup From Non-Brov | 21 | 4 Minutes Ago | Low | Failed | January 12, 2024 @ 15:59 | <input checked="" type="checkbox"/> |
| Interactive Logon By An Unusual F | 73 | 4 Minutes Ago | High | Failed | January 12, 2024 @ 15:58 | <input checked="" type="checkbox"/> |
| Windows Account Or Group Disco | 21 | 4 Minutes Ago | Low | Failed | January 12, 2024 @ 15:59 | <input checked="" type="checkbox"/> |
| Volume Shadow Copy Deleted Or | 73 | 5 Minutes Ago | High | Failed | January 12, 2024 @ 15:59 | <input checked="" type="checkbox"/> |
| AWS S3 Bucket Configuration Del | 21 | 5 Minutes Ago | Low | Succeeded | January 12, 2024 @ 15:58 | <input checked="" type="checkbox"/> |
| CyTech : Medium - O365 - Remov | 47 | 5 Minutes Ago | Medium | Partial Failure | | <input checked="" type="checkbox"/> |
| Attempt To Remove File Quaranti | 47 | 5 Minutes Ago | Medium | Failed | January 12, 2024 @ 15:59 | <input checked="" type="checkbox"/> |
| Suspicious Remote Registry Acce | 47 | 5 Minutes Ago | Medium | Failed | January 12, 2024 @ 15:59 | <input checked="" type="checkbox"/> |

Rows per page: 10 1-10 of 1048

Compliance Updates

Improvement in the Evidence List Modal

Workplace 11:08 AM (UTC) 7:08 PM (GMT +8)

CyTech MSSP

People. Process. Technology.

Human resource sec...

Asset management

Access control

Cryptography

Physical and environ...

Operations security

Communications se...

System acquisition, d...

Roienna Joice

Assignee

Roienna Joice

Assignee

Roienna Joice

Assignee

Assignee

Assignee

Assignee

Assignee

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

description

Management dir...

security

2023-07-04

2023-07-04

Assignee

NOT YET STARTED

OPTIMIZED

Set Date

Attachments

Add Evidence

View File

Comments

1

Revision #2

Created 8 November 2024 10:42:05 by Aldion Pueblos

Updated 8 November 2024 11:22:03 by Aldion Pueblos