

Daily Update: August 22

Here are the main updates of the CISO Workplace:

CIM Updates:

Support for Table Format Timeline

[Go back](#)

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

Generates a detection alert each time an Elastic Endpoint Security alert is received. Enabling this rule allows you to immediately begin investigating your Endpoint alerts.

Case Playbook Alerts Reports Incident Response

Related Alerts (8)

- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
06:12 PM
- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
06:12 PM
- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
06:12 PM
- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
06:12 PM
- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
06:12 PM
- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
05:55 PM
- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
05:54 PM
- Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job
high
05:54 PM

Timeline

⏪ ⏴ ⏵ ⏩

Jump to Change layout Change density

20 Aug, 2024 @ 17:33:46

rule_detection

User Name: romeijhon
Host Name: crnd-romel
Source IP:
Destination IP:
Event Category: malware intrusion_detection
Event Outcome: success

Investigation Guide

Timeline Details

Table Json File (Raw)

Filter by ...

Title	Value
fields.Events.process.group_id	981
fields.Events.process.group_leader.supplemental_groups.id-0	3
fields.Events.process.group_leader.supplemental_groups.id-1	981
fields.Events.process.group_leader.supplemental_groups.id-2	998
fields.Events.group.id-0	1000
fields.kibana.alert.ancestors.id-0	adchb5EBPIRg3WZCpPh6
fields.process.name.text-0	notepadqq-bin
fields.kibana.alert.original_event.code-0	behavior
fields.Events.process.session_loader.user.id-0	1000
fields.kibana.alert.rule.description-0	Generates a detection alert each time an Elastic Endpoint Security alert is received. Enab...
fields.signal.rule.id-0	b1e85cbe-11b3-468f-9b-a7fec2654

Go Back

STEP 3 Attempts to Brute Force a Microsoft 365 User Account

Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack to obtain unauthorized access to user accounts.

Case Playbook

Alerts

Reports

Incident Response

Related Alerts (10)

CyTech: High - o365 - Attempts to Brute Force a Microsoft 365 User Account
high
12:07 AM

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]
high
01:55 PM

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]
high
01:20 AM

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]
high
05:27 PM

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]
high
08:09 AM

Potential Password Spraying of Microsoft 365 User Accounts [cytech_developmentoperations]
high
08:07 AM

Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]
high

Framework

MITRE ATT&CK: -> Credential Access -> Brute Force

Timeline

Search

Table Timeline

Agent Name	User Name	Host Name	Source Ip	Destinati...	Event Categ...	Event Outco...	@Timestamp
✓ -----	NataliaT	cytechint.c...	2804:14...	-----	web	success	2024-08-1...
✓ -----	NataliaT	cytechint.c...	2804:14...	-----	web	success	2024-08-1...
✓ -----	NataliaT	cytechint.c...	2804:14...	-----	web	success	2024-08-1...
✓ -----	NataliaT	cytechint.c...	2804:14...	-----	web	success	2024-08-1...
✓ -----	NataliaT	cytechint.c...	2804:14...	-----	web	success	2024-08-1...

1-5 of 10 < >

Investigation Guide

Timeline Details

Table

Json File (Raw)

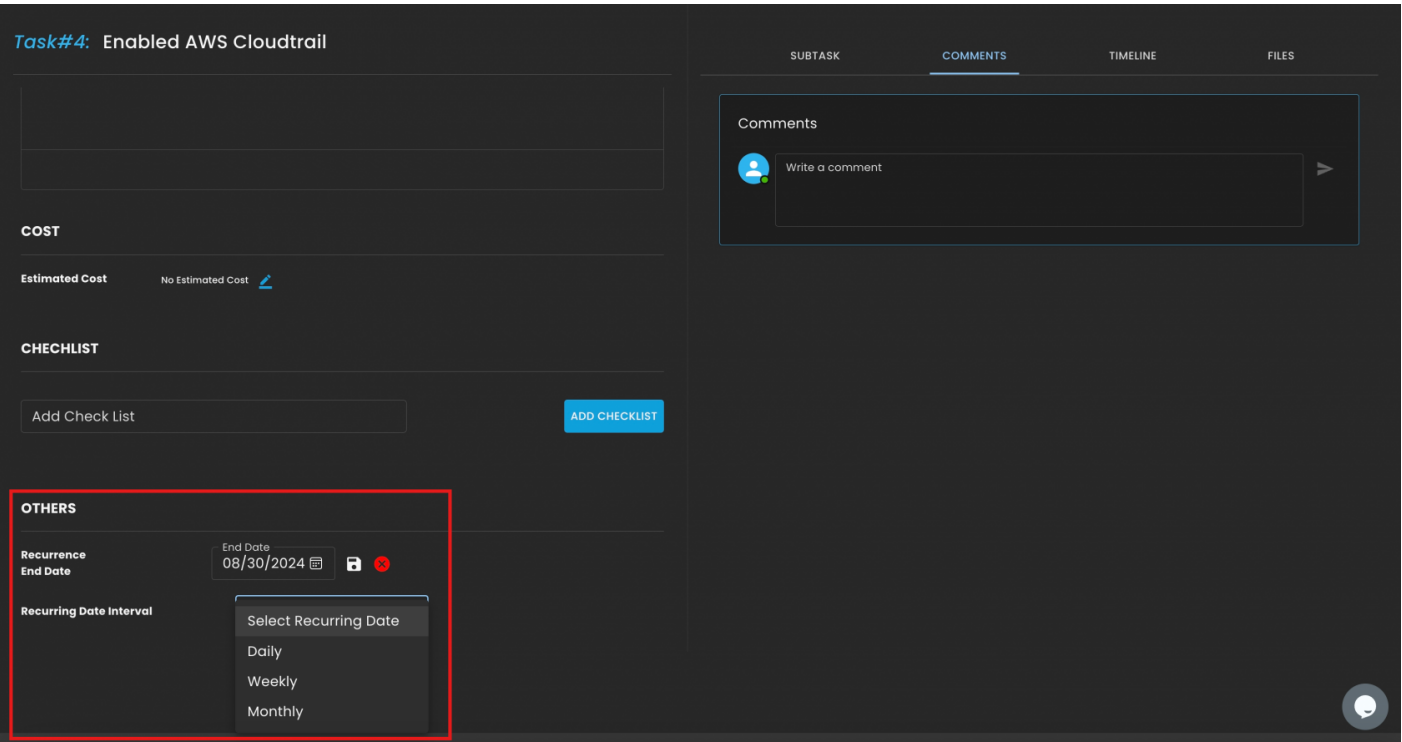
Filter by ...

Title	Value
_index	.ds-logs-o365.audit-cytech_d... developmentoperations-2024_0... 7.26-000564
_id	ktpPawZWPjuju5le4aldxFgeclE... =
_score	
fields.o365.audit.SupportTicketI...	d-0
fields.elastic._agent.version-0	8.12.0
fields.event.category-0	web
fields.event.category-1	authentication
fields.o365.audit.UserId-0	NataliaT@cytechint.com
fields.o365.audit.ApplicationId-0	8c59ead7-d703-4a27-9e55-c... 98a0054c8d2
fields.user._agent.original.text-0	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3... 6 (KHTML, like Gecko) Chrome...
fields.o365.audit.DevicePropert...	OS
fields.o365.audit.DevicePropert...	BrowserType

Kanban Filter Bug Fix for Search Field

RM Updates

Support Recurring Tasks



Bug fixes in the Task Management

Security and Privacy Compliance Updates

Task Modal Layout Improvement

TaskID56731: 1.1.1

CLOSE

Requirements

All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. ...

Not Started

Started at: Tuesday, March 19, 2024 Created at: Tuesday, March 19, 2024

Applicable

PEOPLE

Assignee

AlliahGrace Canillo

DETAILS

ID

56731

Name

1.1.1

Created At

2024-03-19

Updated At

2024-03-19

Description

All security policies and operational procedures are i...

Maturity Level

INITIAL

Task Schedule

June 10, 2024 to September 28, 2024

SUBTASK

COMMENTS

FILES

Task ID	Task Name	Status
9	Analysis for minimum requirements	Not Done
10	Analysis for minimum requirements	Not Done

1-2 of 2

1.1.1 > Task Activity

CLOSE

Analysis for minimum requirements

Description:

The analysis of minimum requirements focuses on identifying the essential compliance standards and regulations necessary for our operations. This includes evaluating legal, industry-specific, and internal compliance criteria to ensure our practices meet all required guidelines and maintain regulatory adherence.

Assignees

Chen Helfer

Assignees

Task Framework

PCI DSS Version 4.0 - SAQ A-EP

Date

07/22/2024

11/23/2024

Reoccurrence

Daily

Status

In-progress

Affected Framework

ASFI Bolivia - Title VII Minimum Safety Requirements

Affected Fra...

SAVE

COMMENTS

UPDATES

FILES

Add Comment Here

Revision #1

Created 22 August 2024 14:45:05 by Aldion Pueblos

Updated 22 August 2024 15:10:28 by Aldion Pueblos