

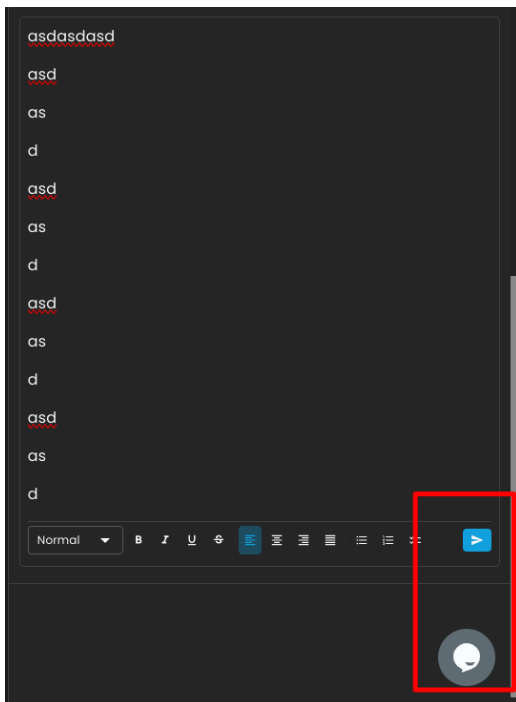
Daily Update: August 20

Here are the main updates of the CISO Workplace:

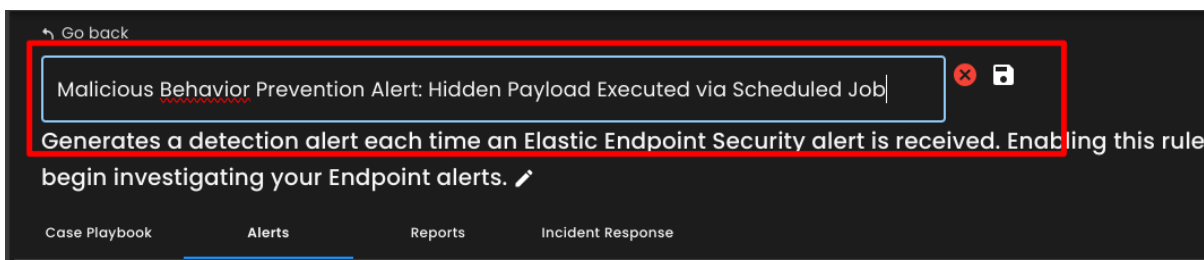
CIM Updates:

Bug Fixes

Making sure Submit Button is displayed and can be clicked in Notepad



Case Title is displayed on update



Fix in Save and Close Button in Alert Details

Overview

Specific of Root Cause

N/A

Normal

B

I

U

Systems Involved

endpoint

Normal

B

I

U

Updated Activity Logs

- Added "See changes" for modifications in Alert Details

Go back

ESP-3

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 PlaybookAlertsReportsIncident Response

Related Alerts (8)

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

high

08:12 PM

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

high

08:12 PM

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

high

08:12 PM

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

high

08:12 PM

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

high

08:12 PM

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

high

08:55 PM

Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job

high

08:54 PM

Overview

Specific of Root Cause

N/A

Systems Involved

endpoint

Location of Vulnerable System

Endpoint

Users Involved

Activity Logs

Activity Type

Case Activity: Aidion Pueblos modified a Case Analyst, and Location Of Vulnerable System with id: 7791

2024-08-20 07:24 PM

SEE CHANGES

Case Activity: Juniele Gaibe modified a CaseKanban to in Progress status with id: 7791

2024-08-20 08:23 PM

Case Activity: Juniele Gaibe added a Case titled 'Malicious Behavior Prevention Alert: Hidden Payload Executed via Scheduled Job' with id: 7791

2024-08-20 08:58 PM

Visual Updates in Report - Summary Incident Report

Summary Incident Report

FILTER

Date	Case ID	Severity	Status	Description
01-18-2024	2633	Elevated	Closed	Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack L...
01-18-2024	2634	Guard...	Closed	This rule uses alert data to determine when multiple different alerts involving the same user are triggered. Analys...
01-18-2024	2637	Guard...	Closed	Identifies the load of a driver with an original file name and signature values that were observed for the first time ...
01-18-2024	2638	Elevated	Closed	Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack L...
01-18-2024	2639	Guard...	Closed	Identifies potential malicious file download and execution from Google Drive. The rule checks for download activit...

1-5 of 894 < >

RM Updates:

Added Milestone in Tasks

Task#4: Enabled AWS Cloudtrail

TaskTypeTask

ComplexityNormal

PriorityNormal

MilestoneSelect Milestone

DateSelect Milestone24-06-15

Affected ControlsIdentity Security/Identity & Access Management (IAM)

COST

SUBTASK

COMMENTS

TIMELINE

FILES

Comments

Write a comment

Security and Privacy Compliance Updates:

Security Improvements (Authorization)

Revision #2
Created 20 August 2024 10:37:33 by Aldion Pueblos
Updated 20 August 2024 11:44:00 by Aldion Pueblos