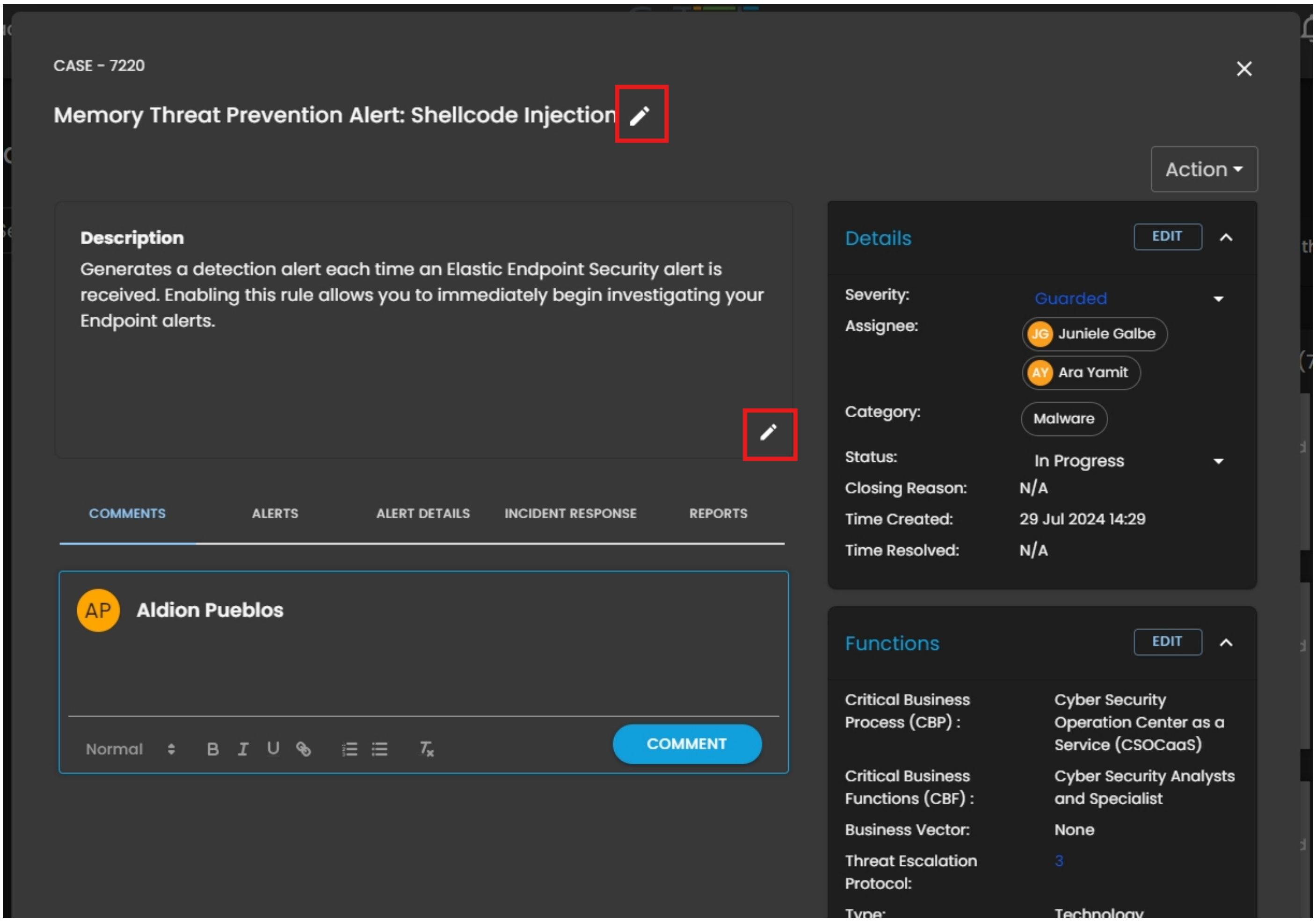
Daily Update: August 1

Here are the main updates of the CISO Workplace:

CIM Updates:

Added Edit Functionality for Case Description:



CASE - 7220

Memory Threat Prevention Alert: Shellcode Injection

Description

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.

AP Aldion Pueblos

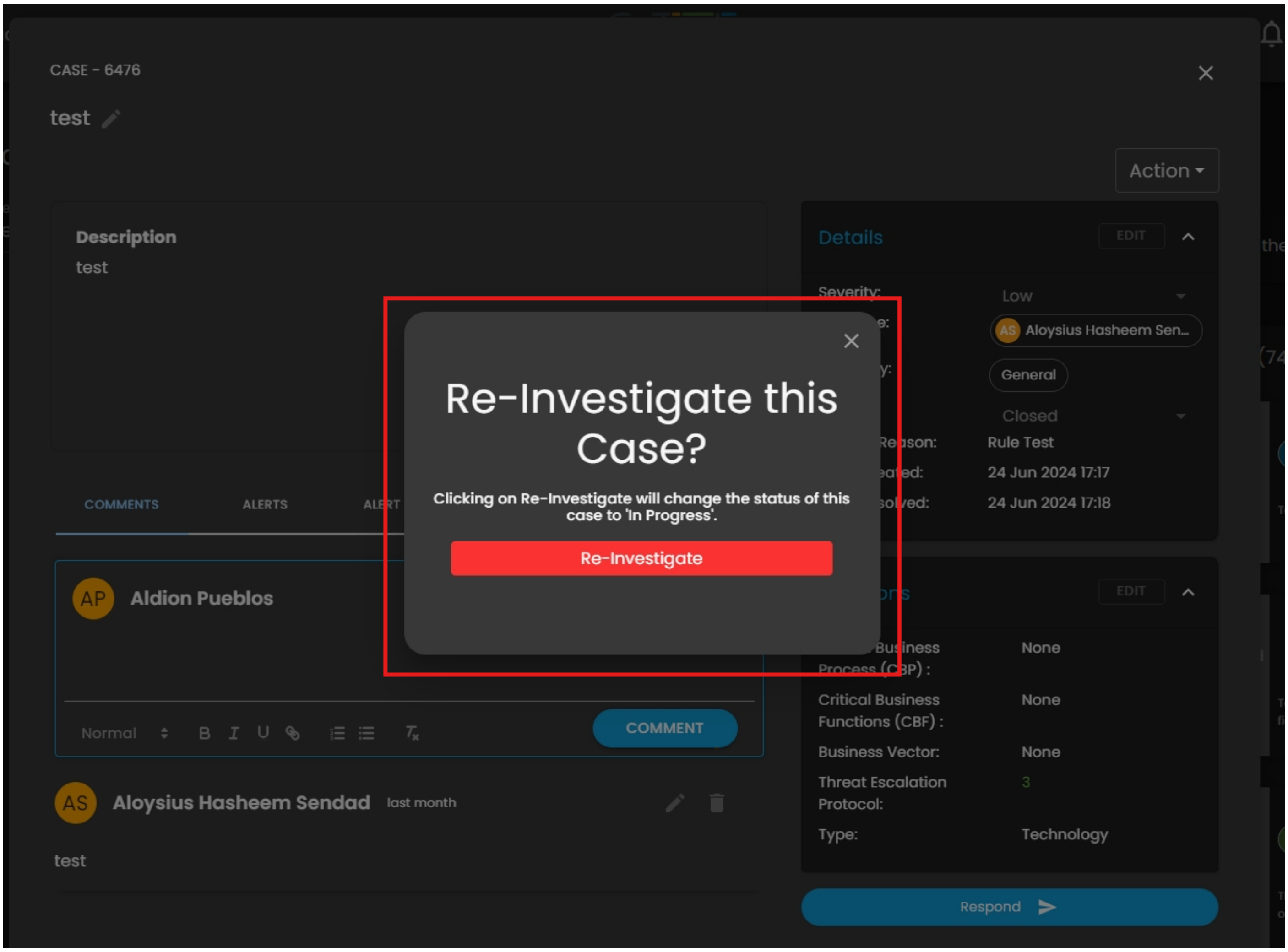
Details

Severity:	Guarded
Assignee:	JG Juniele Galbe AY Ara Yamit
Category:	Malware
Status:	In Progress
Closing Reason:	N/A
Time Created:	29 Jul 2024 14:29
Time Resolved:	N/A

Functions

Critical Business Process (CBP) :	Cyber Security Operation Center as a Service (CSOCaaS)
Critical Business Functions (CBF) :	Cyber Security Analysts and Specialist
Business Vector:	None
Threat Escalation Protocol:	3
Type:	Technology

"Re-investigate" Closed Cases. When cases are re-investigated, they are automatically set to "In-Progress".



Description
test

Re-Investigate this Case?

Clicking on Re-Investigate will change the status of this case to 'In Progress'.

Severity:	Low
	Aloysius Hasheem Sen...
	General
	Closed
Reason:	Rule Test
Created:	24 Jun 2024 17:17
Resolved:	24 Jun 2024 17:18

Business Process (CBP) :	None
Critical Business Functions (CBF) :	None
Business Vector:	None
Threat Escalation Protocol:	3
Type:	Technology

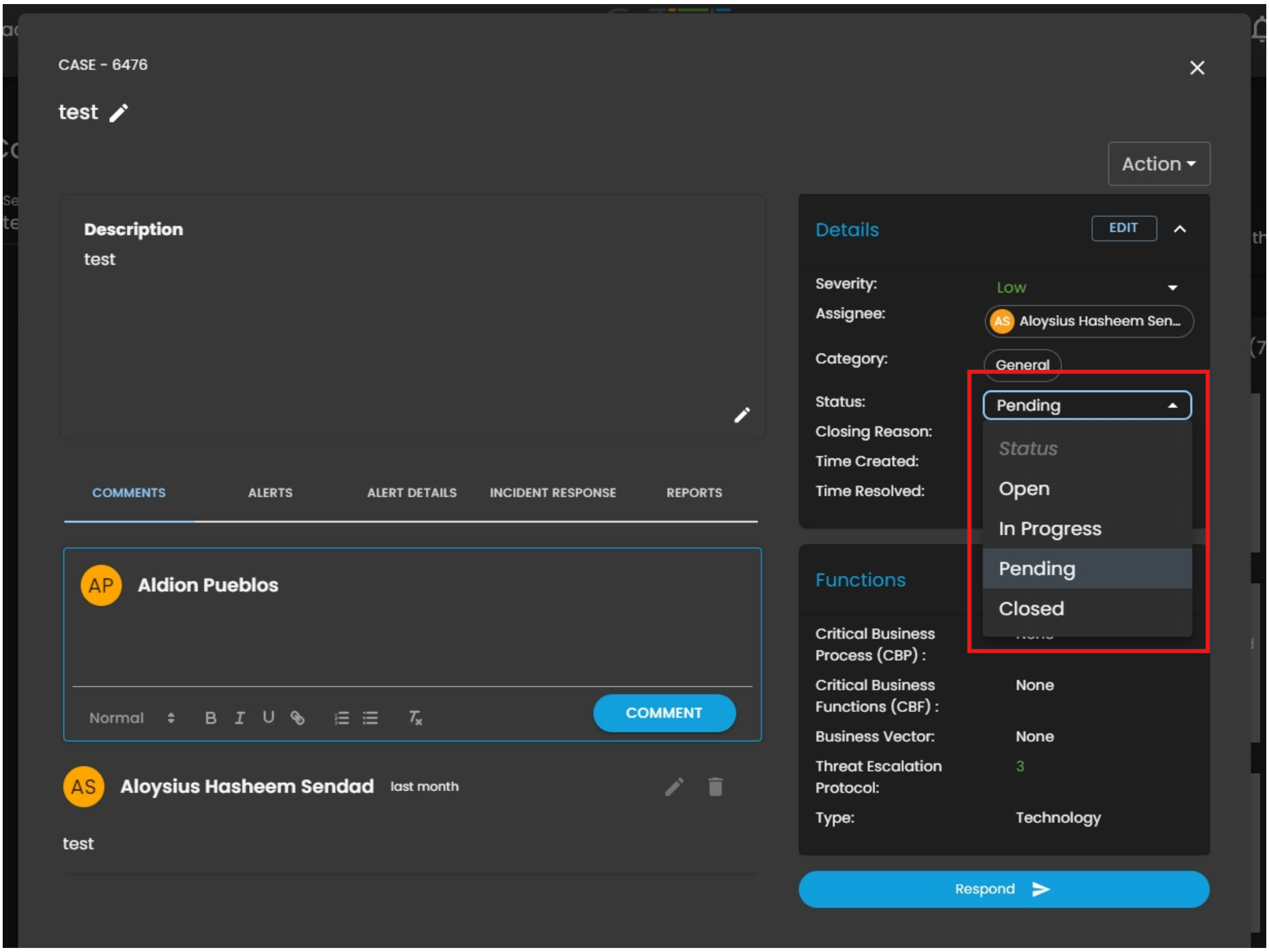
AS Aloysius Hasheem Sendad last month

test

Streamlined changing of Case status. Changing of case status is now removed from "Edit". Changing of status is now only in 2 ways:

1) Kanban Board

2) Case Window


CASE - 6476

test

Description

test

Severity: Low

Assignee: Aloysius Hasheem Sen...

Category: General

Status: Pending

Closing Reason:

Time Created:

Time Resolved:

Critical Business Process (CBP) : None

Critical Business Functions (CBF) : None

Business Vector: None

Threat Escalation Protocol: 3

Type: Technology

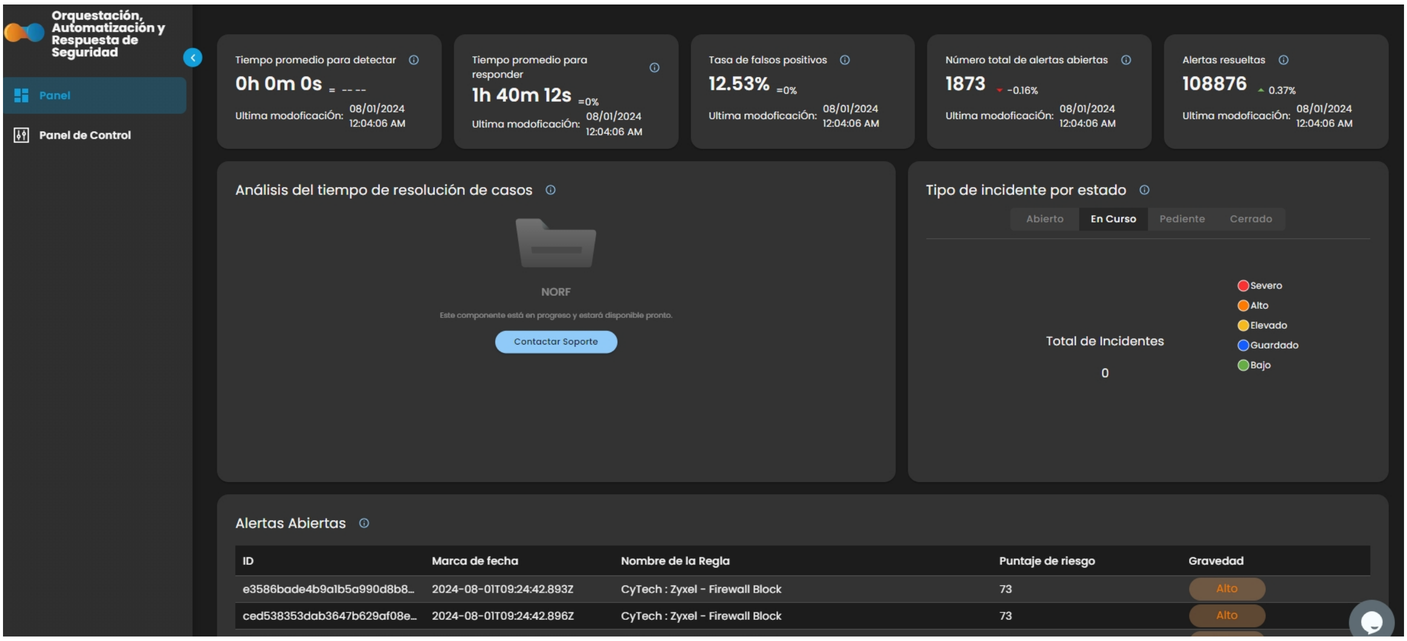
Aldion Pueblos

Aloysius Hasheem Sendad last month

test

SOAR Updates:

- Spanish Translation


Orquestación, Automatización y Respuesta de Seguridad

Tiempo promedio para detectar: 0h 0m 0s = -- --
Ultima modoficaciÓn: 08/01/2024 12:04:06 AM

Tiempo promedio para responder: 1h 40m 12s =0%
Ultima modoficaciÓn: 08/01/2024 12:04:06 AM

Tasa de falsos positivos: 12.53% =0%
Ultima modoficaciÓn: 08/01/2024 12:04:06 AM

Número total de alertas abiertas: 1873 -0.16%
Ultima modoficaciÓn: 08/01/2024 12:04:06 AM

Alertas resueltas: 108876 0.37%
Ultima modoficaciÓn: 08/01/2024 12:04:06 AM

Análisis del tiempo de resolución de casos

NORF

Este componente está en progreso y estará disponible pronto.

Tipo de incidente por estado

Total de Incidentes 0

Alertas Abiertas

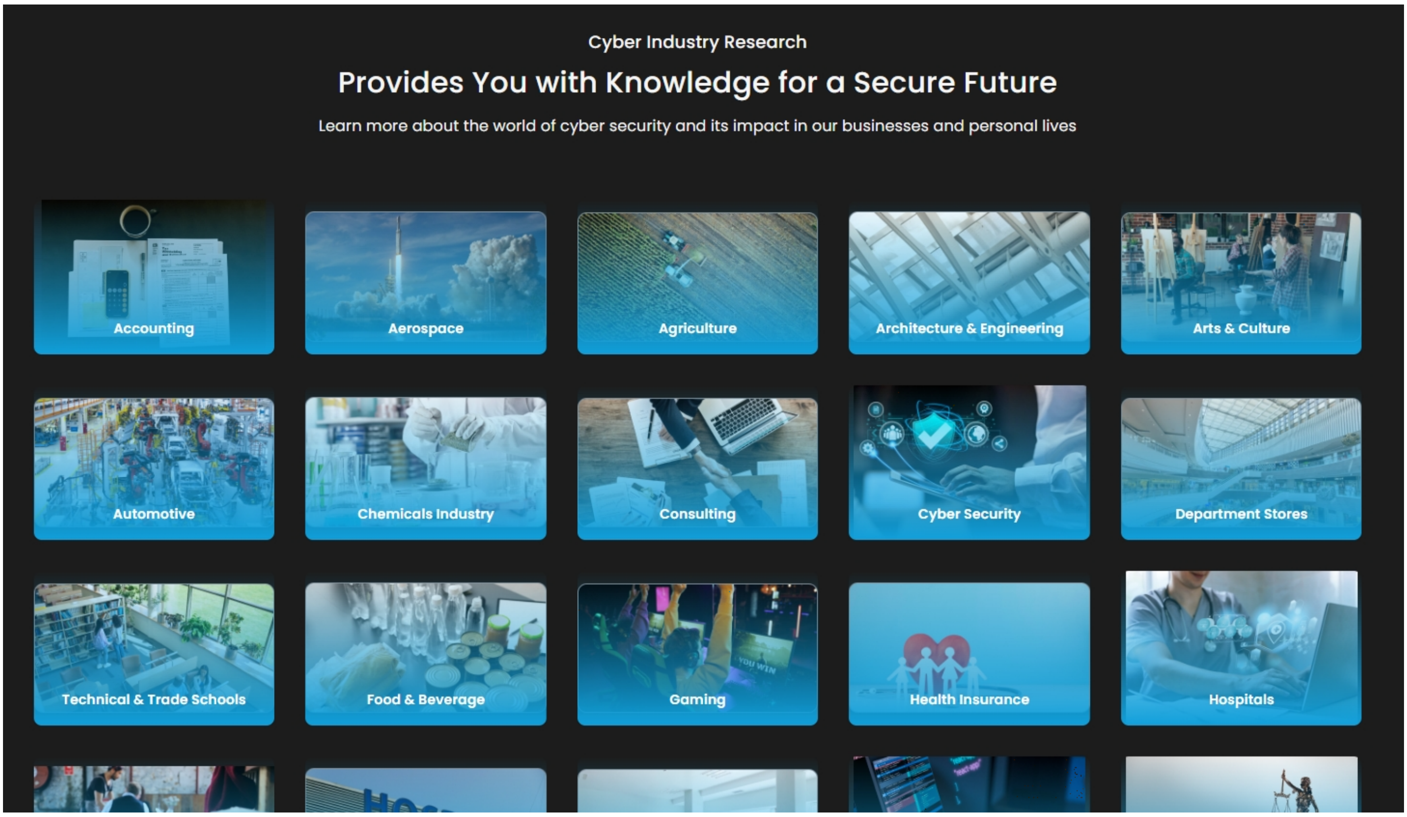
ID	Marca de fecha	Nombre de la Regla	Puntaje de riesgo	Gravedad
e3586bade4b9a1b5a990d8b8...	2024-08-01T09:24:42.893Z	CyTech : Zyxel - Firewall Block	73	Alto
ced538353dab3647b629af08e...	2024-08-01T09:24:42.896Z	CyTech : Zyxel - Firewall Block	73	Alto

Phishing Simulation Updates:

- Bug Fixes in Recipient and Dashboard

CISO Enrichments Updates:

- Updated to be able retrieve data from Wordpress



Cyber Industry Research

Provides You with Knowledge for a Secure Future

Learn more about the world of cyber security and its impact in our businesses and personal lives

Revision #1
Created 1 August 2024 10:17:17 by Aldion Pueblos
Updated 1 August 2024 11:07:21 by Aldion Pueblos