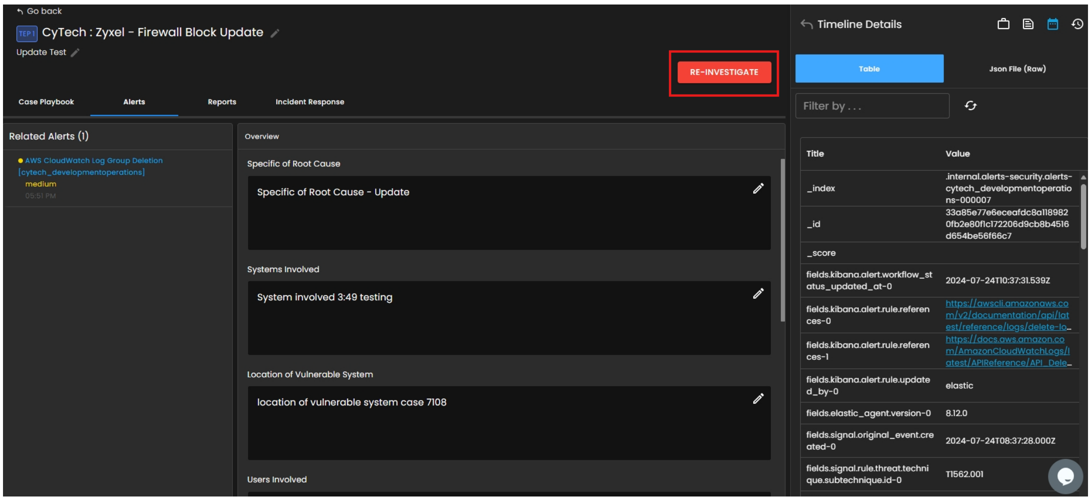
Daily Update: August 21

Here are the main updates of the CISO Workplace:

CIMS v3 Updates:

Support for "Re-investigate" and Reason



CyTech : Zyxel - Firewall Block Update

Update Test

Related Alerts (1)

- AWS CloudWatch Log Group Deletion [cytech_developmentoperations]
  medium
  05:51 PM

Overview

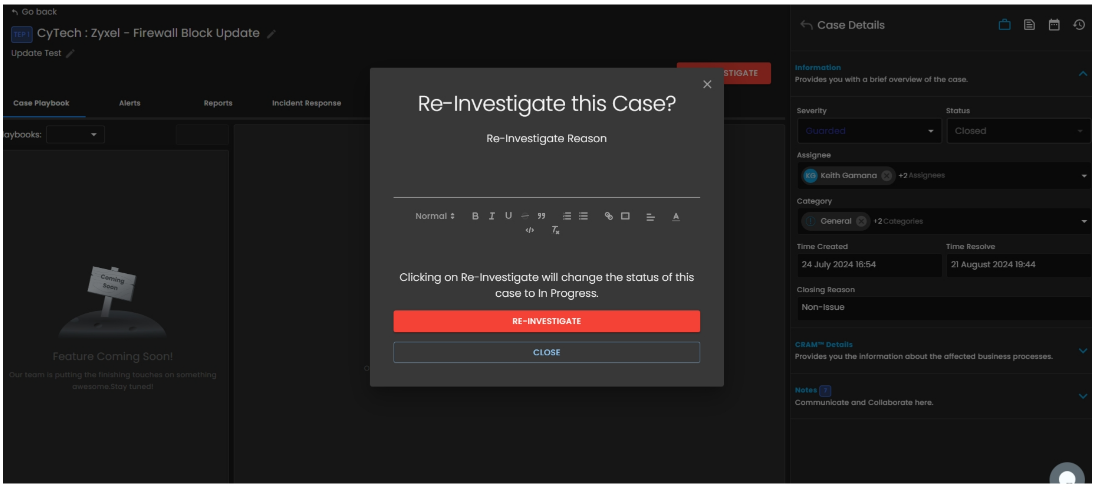
Specific of Root Cause: Specific of Root Cause - Update

Systems Involved: System involved 3:49 testing

Location of Vulnerable System: location of vulnerable system case 7108

Users Involved

Title	Value
_index	.internal.alerts-security.alerts-cytech_developmentoperations-000007
_id	33a85e77e6eceafdc8a118982 0fb2e80f1c172206d9cb8b4516 d654be56f66c7
_score	
fields.kibana.alert.workflow_status_updated_at-0	2024-07-24T10:37:31.539Z
fields.kibana.alert.rule.references-0	https://awscli.amazonaws.com/v2/documentation/api/latest/reference/logs/delete-lo...
fields.kibana.alert.rule.references-1	https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API_Dele...
fields.kibana.alert.rule.updated_by-0	elastic
fields.elastic_agent.version-0	8.12.0
fields.signal.original_event.created-0	2024-07-24T08:37:28.000Z
fields.signal.rule.threat.technique.subtechnique.id-0	T1562.001



CyTech : Zyxel - Firewall Block Update

Update Test

Feature Coming Soon!

Our team is putting the finishing touches on something awesome.Stay tuned!

Re-Investigate this Case?

Re-Investigate Reason

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

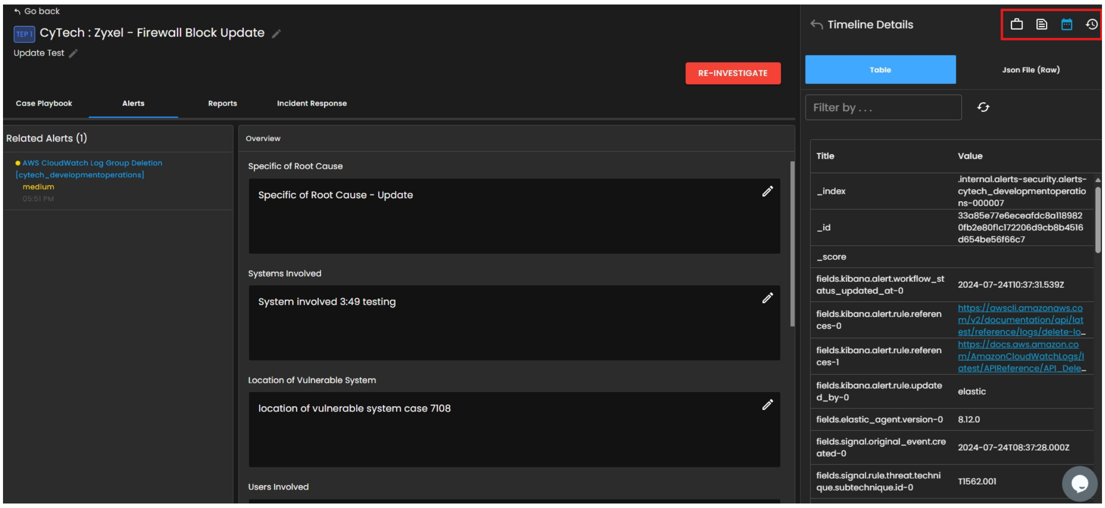
Information
Provides you with a brief overview of the case.

Severity: Guarded
Status: Closed
Assignee: Keith Gamana +2 Assignees
Category: General +2 Categories
Time Created: 24 July 2024 16:54
Time Resolve: 21 August 2024 19:44
Closing Reason: Non-Issue

CRAM™ Details
Provides you the information about the affected business processes.

Notes 7
Communicate and Collaborate here.

Added Tabs Links



Go back

CyTech : Zyxel - Firewall Block Update

Update Test

Related Alerts (1)

AWS CloudWatch Log Group Deletion [cytech_developmentoperations]
medium
05:51 PM

Overview

Specific of Root Cause

Specific of Root Cause - Update

Systems Involved

System involved 3:49 testing

Location of Vulnerable System

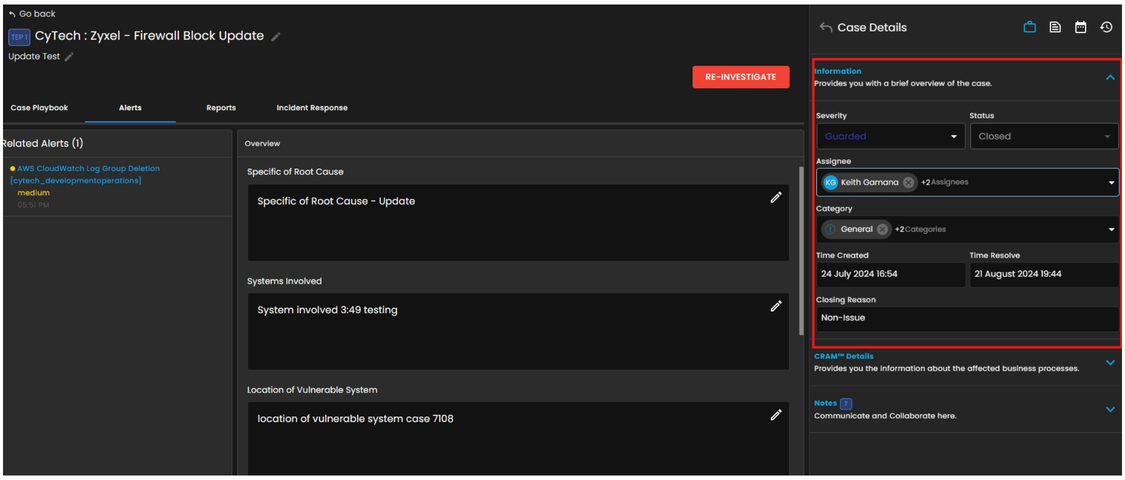
location of vulnerable system case 7108

Users Involved

Timeline Details

Title	Value
_index	.internal.alerts-security.alerts-cytech_developmentoperations-000007
_id	33a85e77e6eceafdc8a1189820fb2e80f1c172206d9cb8b4516d654be56f66c7
_score	
fields.kibana.alert.workflow_status_updated_at-0	2024-07-24T10:37:31.539Z
fields.kibana.alert.rule.references-0	https://awscli.amazonaws.com/v2/documentation/api/latest/reference/logs/delete-lo…
fields.kibana.alert.rule.references-1	https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API_Dele…
fields.kibana.alert.rule.updated_by-0	elastic
fields.elastic_agent.version-0	8.12.0
fields.signal.original_event.created-0	2024-07-24T08:37:28.000Z
fields.signal.rule.threat.technique.subtechnique.id-0	T1562.001

Case Details Update Support



Go back

CyTech : Zyxel - Firewall Block Update

Update Test

Related Alerts (1)

AWS CloudWatch Log Group Deletion [cytech_developmentoperations]
medium
05:51 PM

Overview

Specific of Root Cause

Specific of Root Cause - Update

Systems Involved

System involved 3:49 testing

Location of Vulnerable System

location of vulnerable system case 7108

Case Details

Information

Provides you with a brief overview of the case.

Severity: Guarded

Status: Closed

Assignee: Keith Gamana +2Assignees

Category: General +2Categories

Time Created: 24 July 2024 16:54

Time Resolve: 21 August 2024 19:44

Closing Reason: Non-Issue

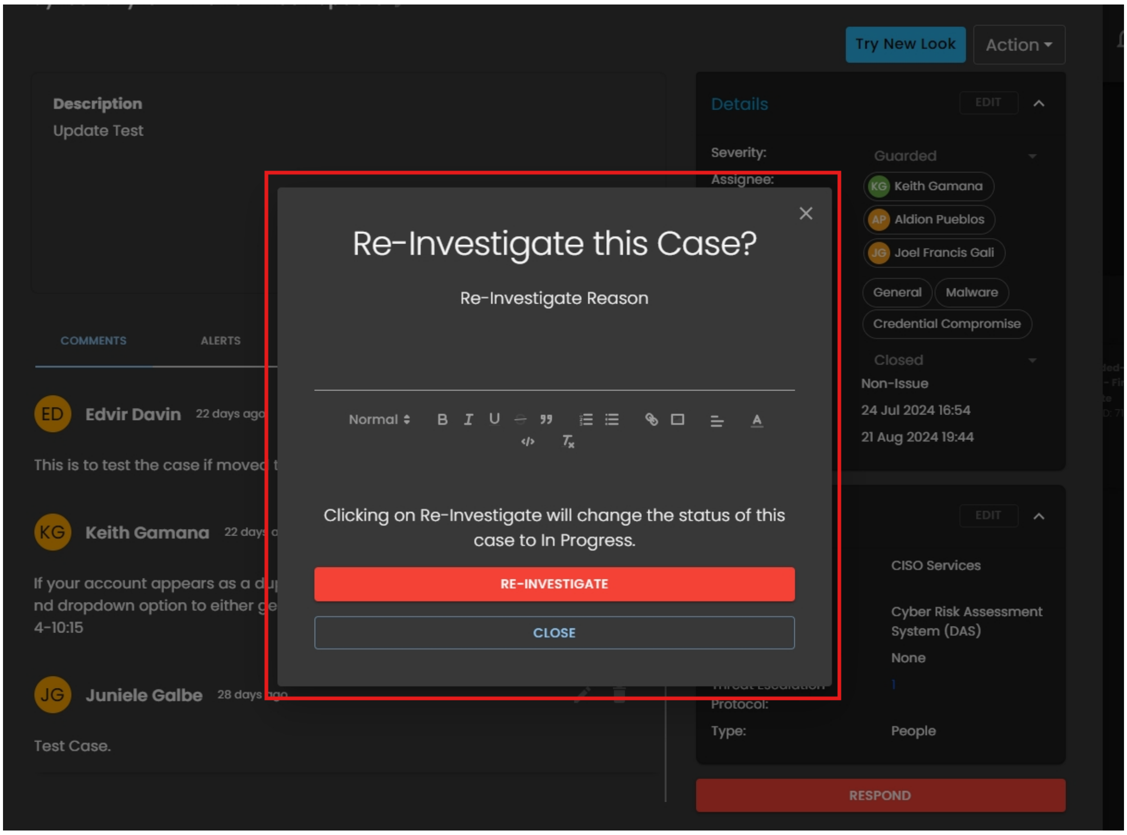
CRAM™ Details

Provides you the information about the affected business processes.

Notes 7

Communicate and Collaborate here.

Added Reason for Re-investigation (in CIM v2 Look)



Description
Update Test

Edvir Davin 22 days ago

This is to test the case if moved t

Keith Gamana 22 days

If your account appears as a du
nd dropdown option to either g
4-10:15

Juniele Galbe 28 days ago

Test Case.

Re-Investigate this Case?

Re-Investigate Reason

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

Details

Severity: Guarded

Assignee: Keith Gamana, Aldion Pueblos, Joel Francis Gali

General, Malware, Credential Compromise

Closed

Non-Issue

24 Jul 2024 16:54

21 Aug 2024 19:44

CISO Services

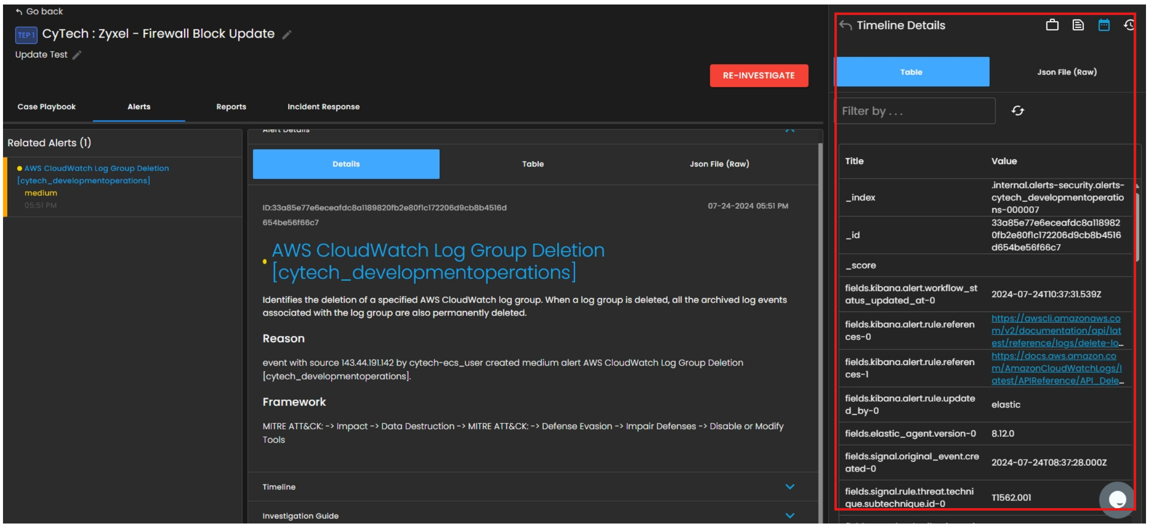
Cyber Risk Assessment System (DAS)

None

Protocol:

Type: People

Right-side details are not closed when opening other areas



CyTech : Zyxel - Firewall Block Update

Update Test

Related Alerts (1)

AWS CloudWatch Log Group Deletion [cytech_developmentoperations]
medium
05:51 PM

ID:33a85e77e6eceafdc8a1189820fb2e80f1c172206d9cb8b4516d654be56f66c7

07-24-2024 05:51 PM

AWS CloudWatch Log Group Deletion [cytech_developmentoperations]

Identifies the deletion of a specified AWS CloudWatch log group. When a log group is deleted, all the archived log events associated with the log group are also permanently deleted.

Reason

event with source 143.44.191.142 by cytech-ecs_user created medium alert AWS CloudWatch Log Group Deletion [cytech_developmentoperations].

Framework

MITRE ATT&CK: -> Impact -> Data Destruction -> MITRE ATT&CK: -> Defense Evasion -> Impair Defenses -> Disable or Modify Tools

Timeline Details

Title	Value
_index	.internal.alerts-security.alerts-cytech_developmentoperations-000007
_id	33a85e77e6eceafdc8a1189820fb2e80f1c172206d9cb8b4516d654be56f66c7
_score	
fields.kibana.alert.workflow_status_updated_at-0	2024-07-24T10:37:31.539Z
fields.kibana.alert.rule.references-0	https://awscli.amazonaws.com/v2/documentation/api/latest/reference/logs/delete-lo...
fields.kibana.alert.rule.references-1	https://docs.aws.amazon.com/AmazonCloudWatchLogs/latest/APIReference/API_Dele...
fields.kibana.alert.rule.updated_by-0	elastic
fields.elastic_agent.version-0	8.12.0
fields.signal.original_event.created-0	2024-07-24T08:37:28.000Z
fields.signal.rule.threat.technique.subtechnique.id-0	T1562.001

BIA Updates

Update for MSSP Support

Revision #1
Created 21 August 2024 11:03:44 by Aldion Pueblos
Updated 21 August 2024 12:09:31 by Aldion Pueblos