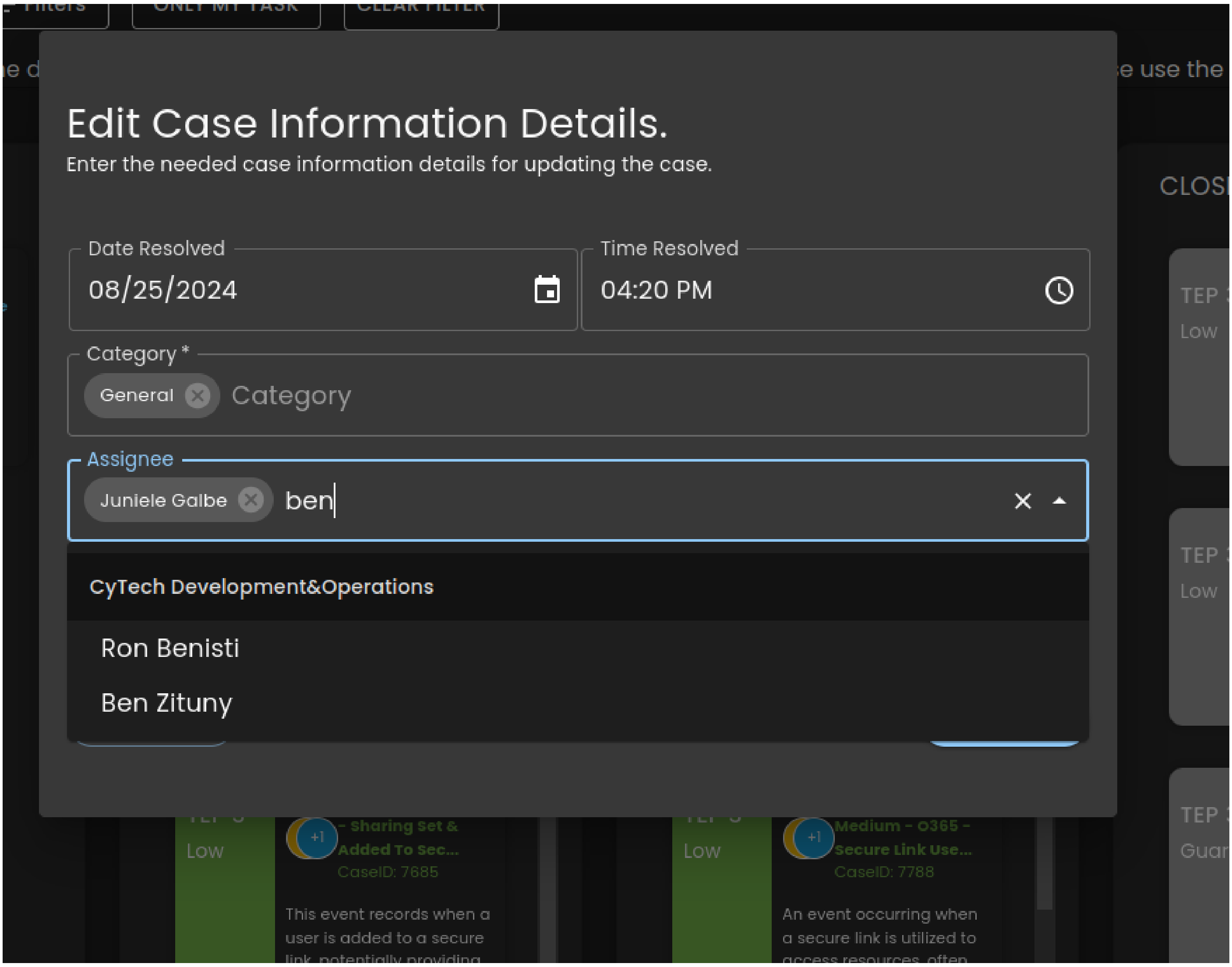
Daily Update: August 27

Here are the main updates of the CISO Workplace:

CIM Updates:

Fix on Case Assignee



Edit Case Information Details.

Enter the needed case information details for updating the case.

Date Resolved: 08/25/2024

Time Resolved: 04:20 PM

Category *: General

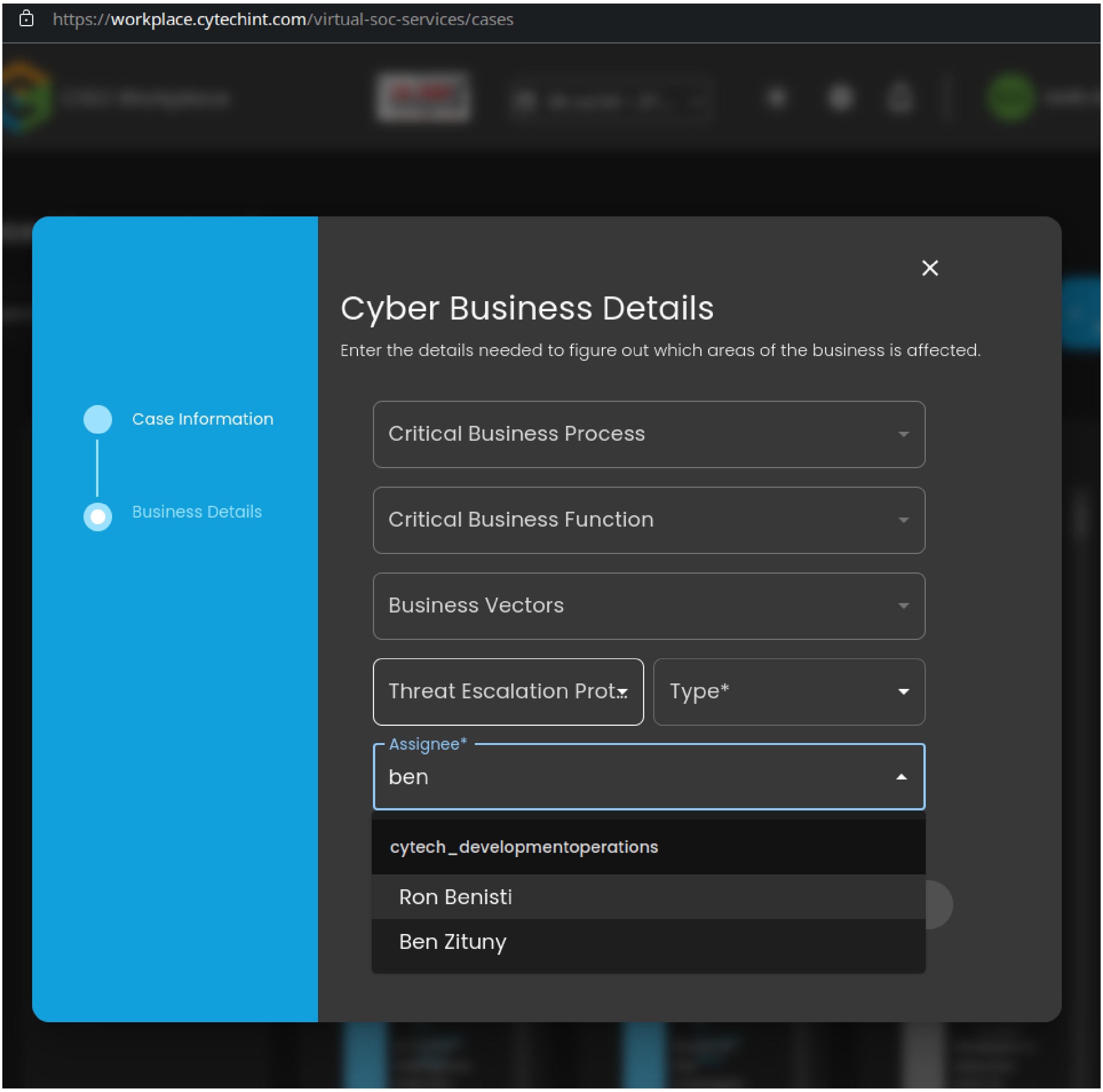
Assignee: Juniele Galbe ben

CyTech Development&Operations

Ron Benisti

Ben Zituny

Filters
ONLY MY TASK
CLEAR FILTER
CLOSE
TEP
Low
Low
- Sharing Set & Added To Sec...
CaseID: 7685
This event records when a user is added to a secure link, potentially providing
Low
Medium - O365 - Secure Link Use...
CaseID: 7788
An event occurring when a secure link is utilized to access resources, often
Guar



https://workplace.cytechint.com/virtual-soc-services/cases

Cyber Business Details

Enter the details needed to figure out which areas of the business is affected.

Critical Business Process

Critical Business Function

Business Vectors

Threat Escalation Prot

Type*

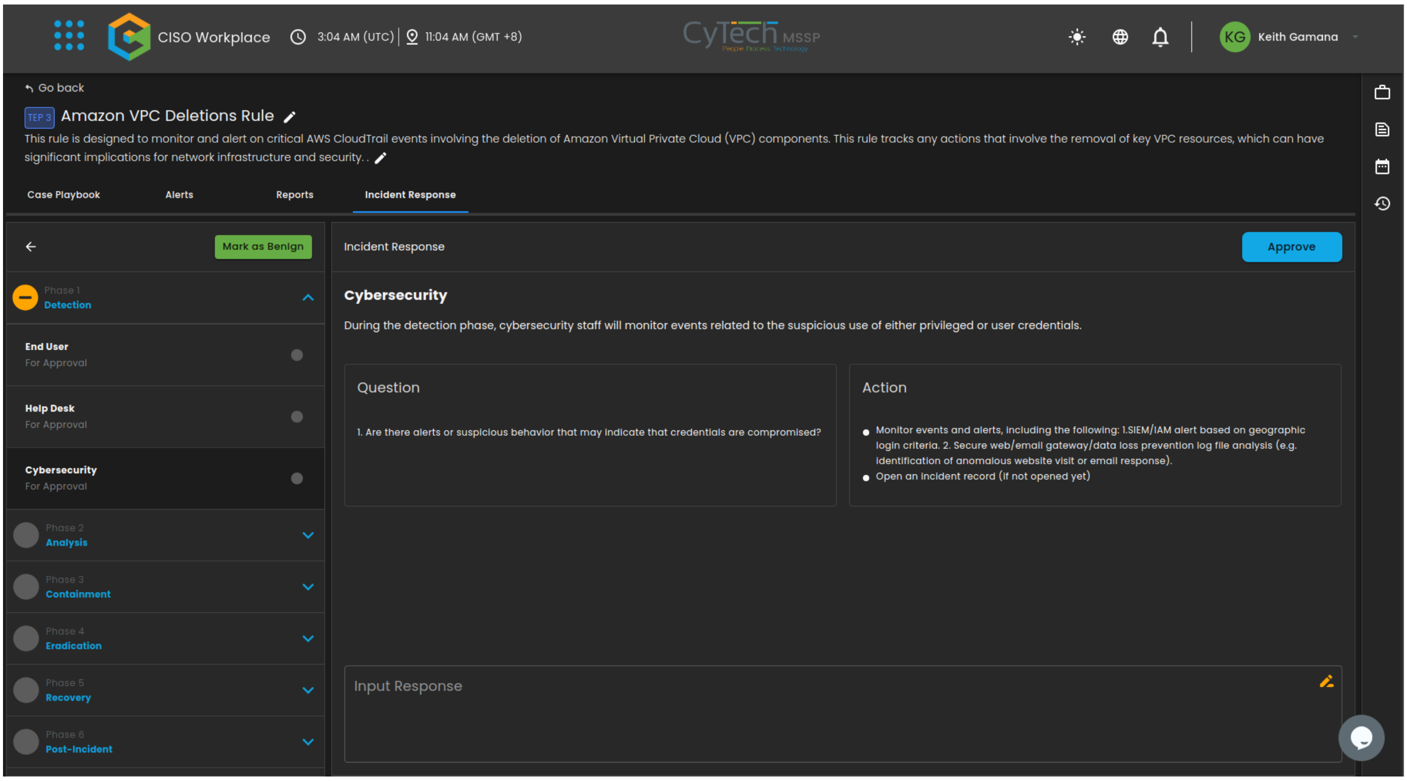
Assignee*: ben

cytech_developmentoperations

Ron Benisti

Ben Zituny

Support on Incident Response in CIM v3



TEP 3 Amazon VPC Deletions Rule

This rule is designed to monitor and alert on critical AWS CloudTrail events involving the deletion of Amazon Virtual Private Cloud (VPC) components. This rule tracks any actions that involve the removal of key VPC resources, which can have significant implications for network infrastructure and security. .

Phase 1 Detection

End User
For Approval

Help Desk
For Approval

Cybersecurity
For Approval

Phase 2 Analysis

Phase 3 Containment

Phase 4 Eradication

Phase 5 Recovery

Phase 6 Post-Incident

Incident Response

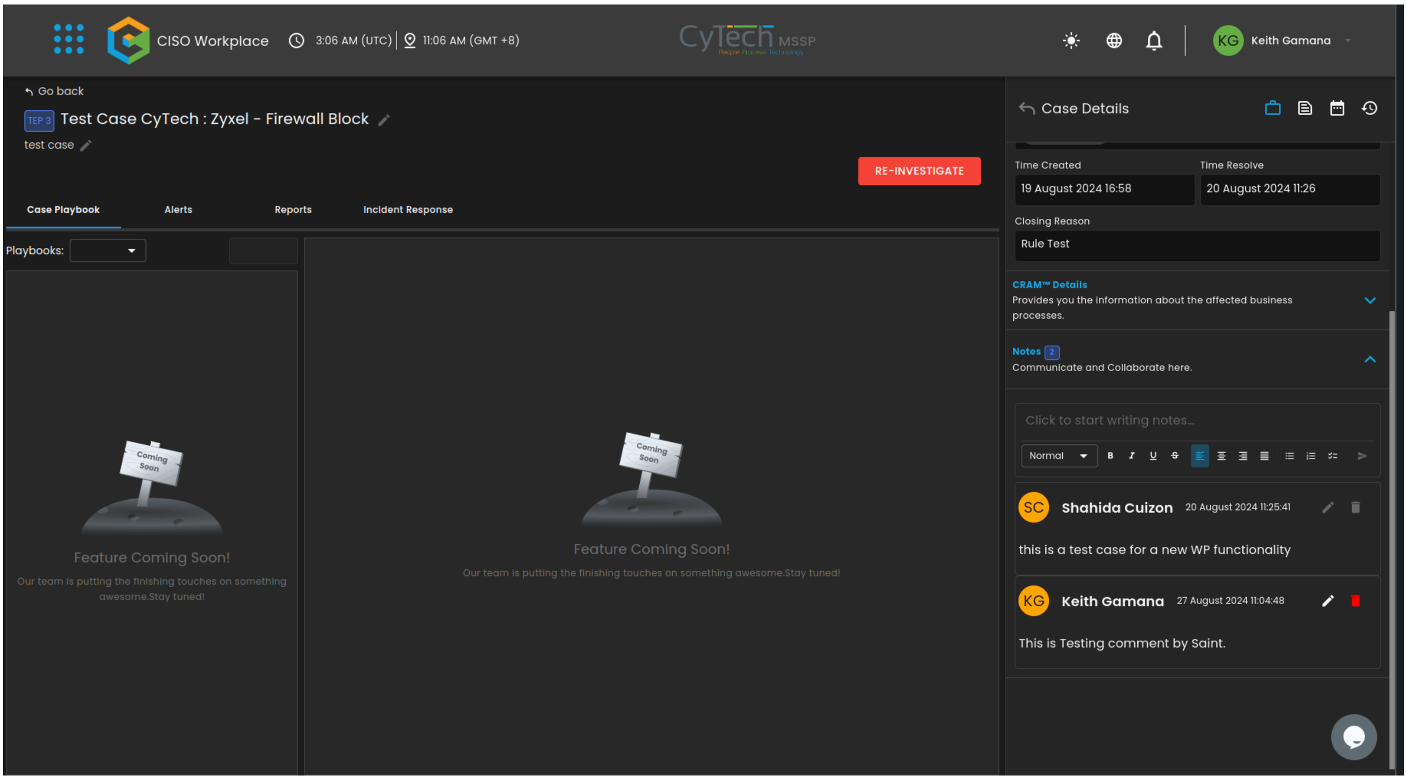
Cybersecurity

During the detection phase, cybersecurity staff will monitor events related to the suspicious use of either privileged or user credentials.

Question	Action
1. Are there alerts or suspicious behavior that may indicate that credentials are compromised?	● Monitor events and alerts, including the following: 1.SIEM/IAM alert based on geographic login criteria. 2. Secure web/email gateway/data loss prevention log file analysis (e.g. identification of anomalous website visit or email response). ● Open an incident record (if not opened yet)

Input Response

Bug Fix on Details Note



TEP 3 Test Case CyTech : Zyxel - Firewall Block

test case

Feature Coming Soon!

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

Feature Coming Soon!

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

Time Created	Time Resolve
19 August 2024 16:58	20 August 2024 11:26

Closing Reason: Rule Test

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

Notes 2
Communicate and Collaborate here.

Click to start writing notes...

SC Shahida Cuizon 20 August 2024 11:25:41
this is a test case for a new WP functionality

KG Keith Gamana 27 August 2024 11:04:48
This is Testing comment by Saint.

Revision #1
Created 27 August 2024 10:52:25 by Aldion Pueblos
Updated 29 August 2024 10:47:15 by Aldion Pueblos