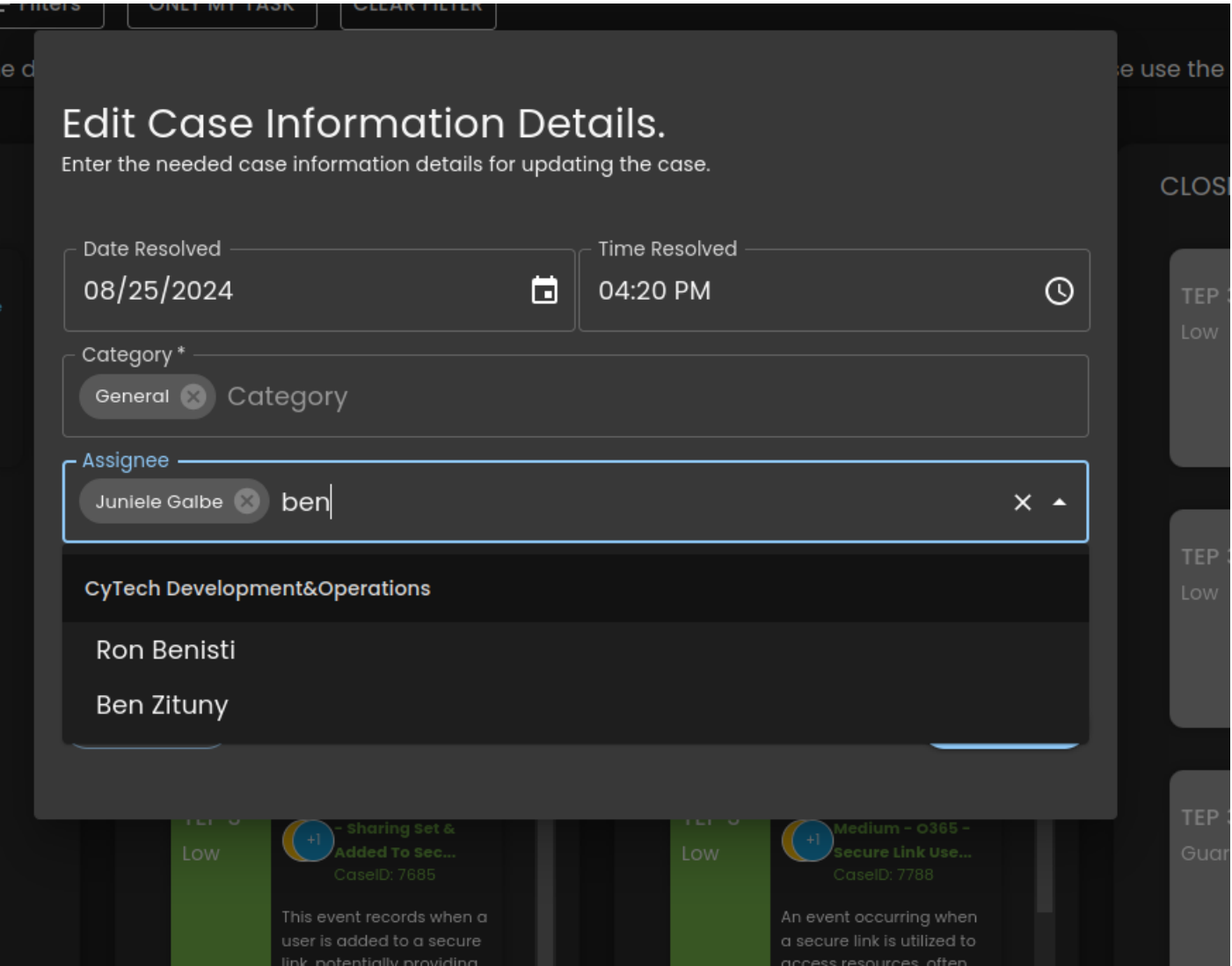


Daily Update: August 27

Here are the main updates of the CISO Workplace:

CIM Updates:

Fix on Case Assignee



Case Information

Business Details

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*

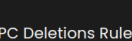
Assignee*
ben

cytech_developmentoperations



Ron Benisti


Ben Zituny




Support on Incident Response in CIM v3




CISO Workplace

 3:04 AM (UTC) |
  11:04 AM (GMT +8)



 Keith Gamana

Go back

STEP 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.

Case Playbook

Alerts

Reports

Incident Response

←

Mark as Benign

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

Approve

Cybersecurity

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


Question



1. Are there alerts or suspicious behavior that may indicate that credentials are compromised?


Action





- 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



 3:06 AM (UTC)
  11:06 AM (GMT +8)






 Keith Gamana

Go back

STEP 3

Test Case CyTech : Zyxel - Firewall Block

test case

RE-INVESTIGATE

Case Playbook

Alerts

Reports

Incident Response

Playbooks:

Coming Soon

Feature Coming Soon!

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

Coming Soon

Feature Coming Soon!

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

Case Details

Time Created

19 August 2024 16:58

Time Resolve

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...

Normal

B I U L G

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.