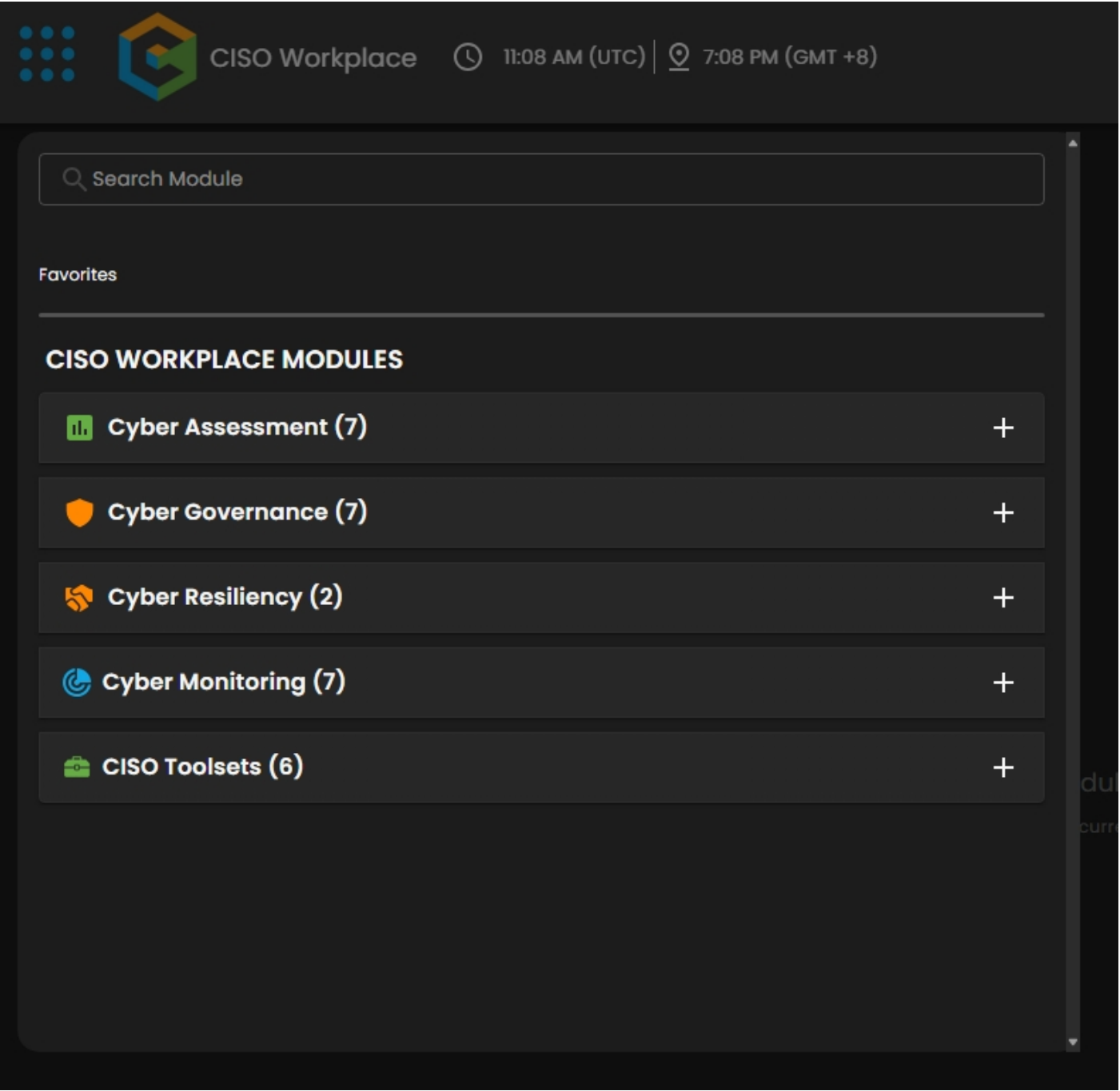


Daily Update: October 8

Here are the main updates of the CISO Workplace:

Overall Updates:

Workplace Menu Update

















Favorites Support in Menu

Search Module

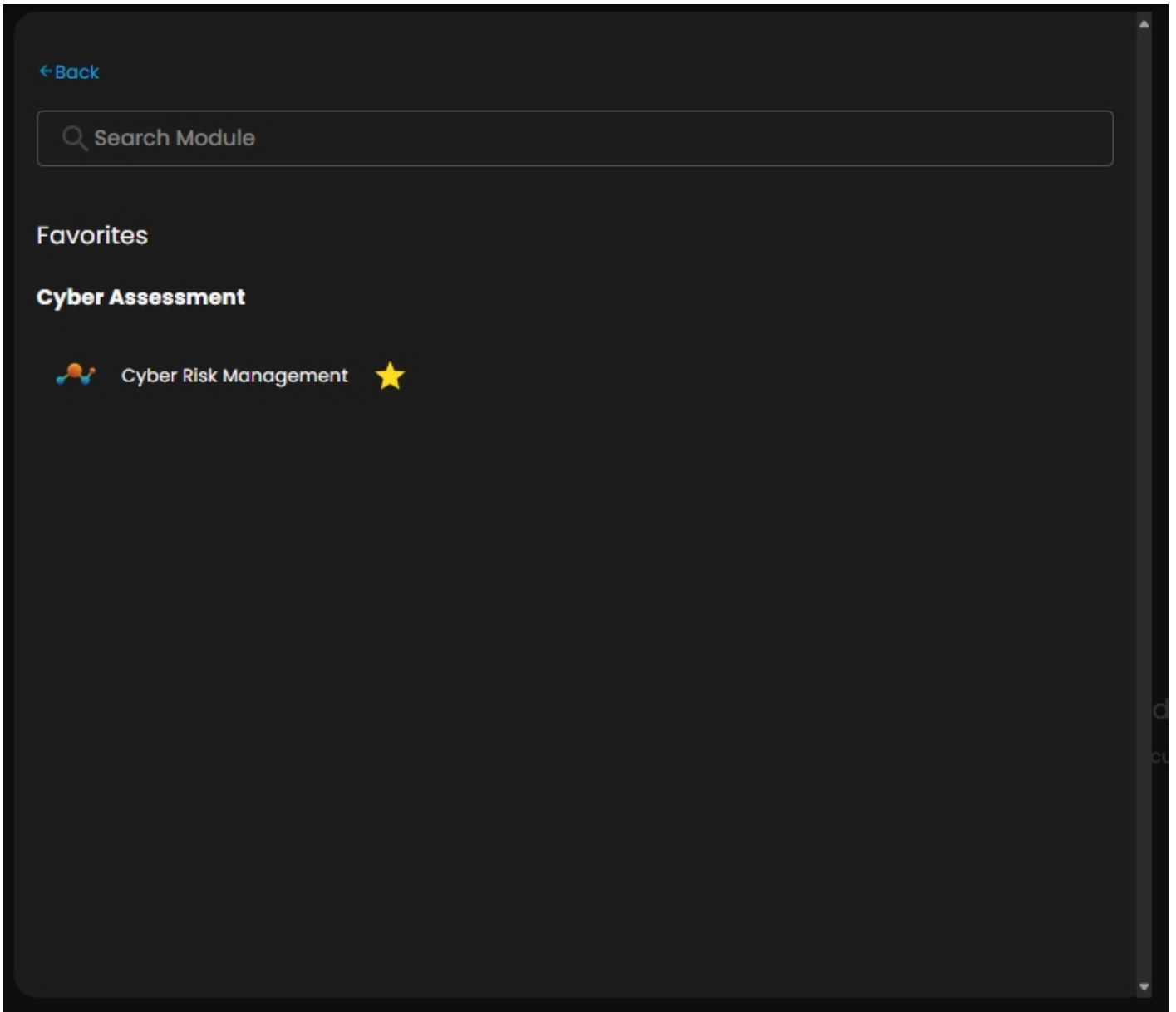
Favorites

CISO WORKPLACE MODULES

Cyber Assessment (7)

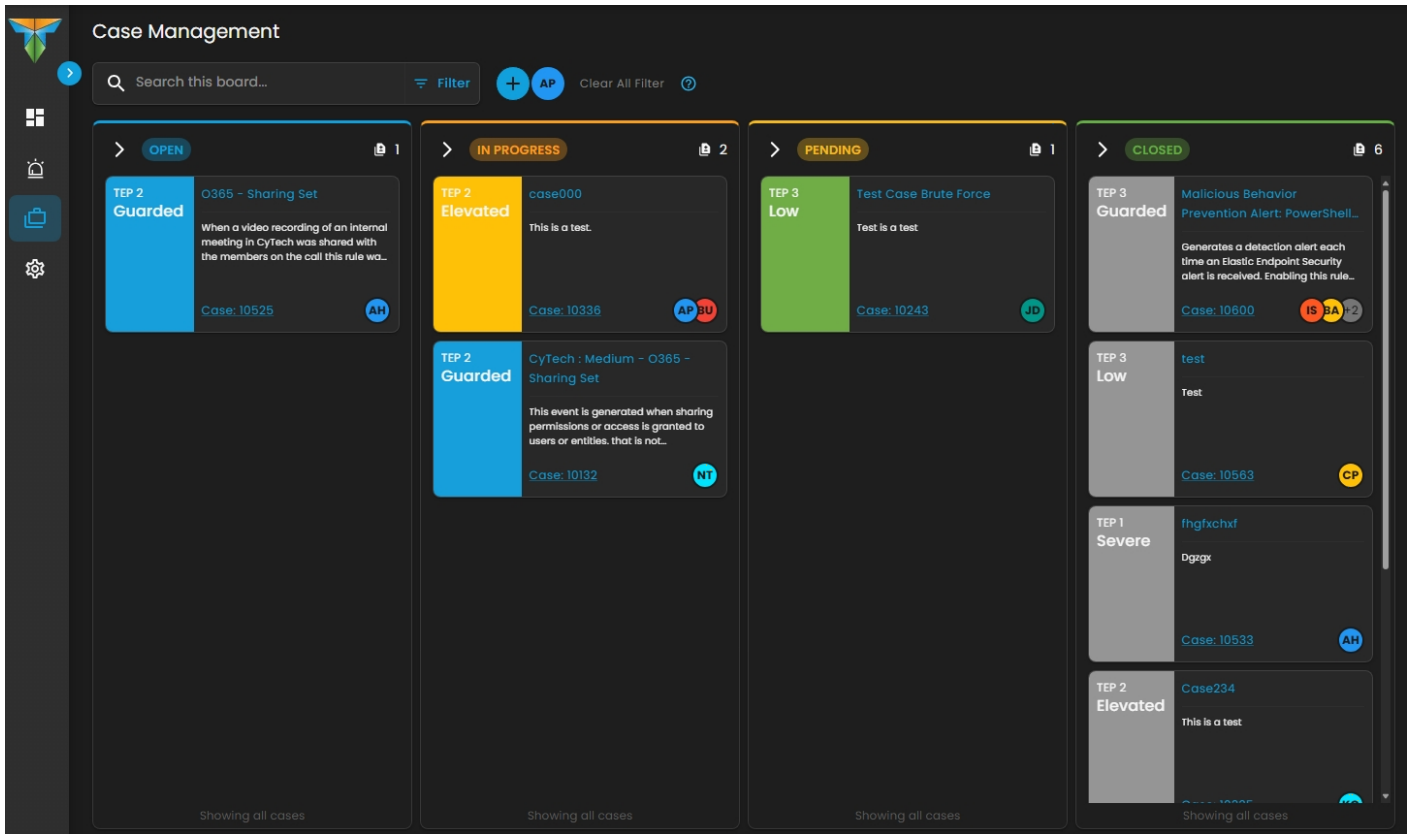
-  Cyber Risk Management 
-  Supply Chain Risk Management 
-  Cloud Security Posture Management (CSPM)(CSPM) 
-  Vulnerability Assessment and Management 
-  Threat Intelligence(TI) 
-  Virtual Penetration Testing 
-  Phishing Simulations 

Cyber Governance (7)

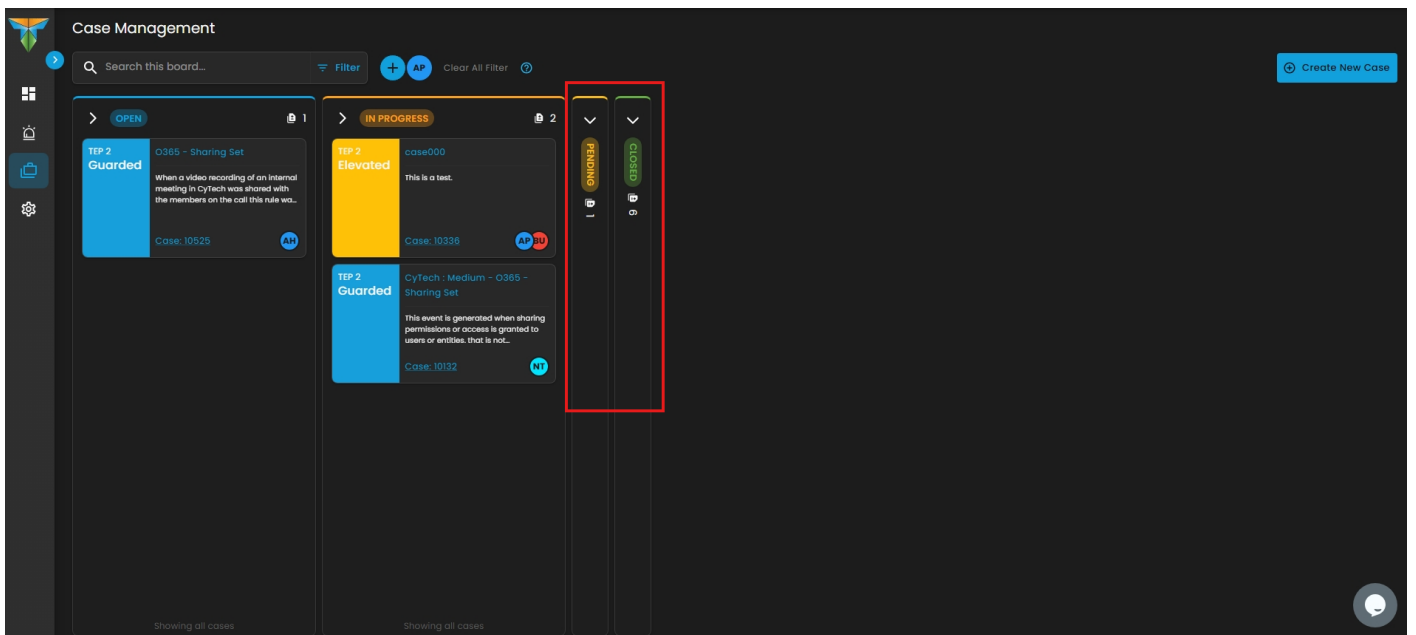


CIM Updates:

Kanban Board Improvements



Foldable column support



Case Page Improvements

Go back > Case: 10243

Test Case Brute Force

Test is a test

Case PlaybookAlertsReportsIncident Response

Related Alerts (6)

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Alert Details

DetailsTableJSON File (Raw)

ID:005d274157e2d7dd9548a92935f3ca36eb4e2bcd9e19cdd84678a005e4270bd09-16-2024 10:35 PM

Test Successful Brute Force

A pattern of multiple failed login attempts followed by a successful login has been detected, indicating a potential account compromise. This activity suggests that an attacker may have successfully guessed or brute-forced the user's password.

Reason

web, authentication event with source created high alert Test Successful Brute Force.

Framework

Not Available

Timeline

Case Details

Information

Provides you with a brief overview of the case.

SeverityLowStatusPending

AssigneeAssignees

CategoryCredential CompromiseCategories

Time CreatedTime Resolve

Closing ReasonNon-Issue

CRAM™ Details

Provides you the information about the affected business processes.

Notes

Communicate and Collaborate here.

Image Preview in Case Comments

Go back > Case: 10243

Test Case Brute Force

Test is a test

Case PlaybookAlertsReportsIncident Response

Playbooks: Malware Use Playbook

Phase 1

Phase 1

Host Identification

Description

Determine the hostname of the device that had triggered the detection.

Case Details

Non-Issue

CRAM™ Details

Provides you the information about the affected business processes.

Notes

Communicate and Collaborate here.

Click to start writing notes...

NormalB I U G

AP08 October 2024 19:20:59

Test Case Brute Force

Test is a test

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

AH02 October 2024 08:08:48

This was a Brute Force test

Go back > Case: 10243

Test Case Brute Force

Test is a test

Case PlaybookAlertsReportsIncident Response

Related Alerts (6)

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Test Successful Brute Force

high

10:35 PM

Alert Details

DetailsTableJSON File (Raw)

ID:005d274157e2d7dd9548a92935f3ca36eb4e2bcd9e19cdd84678a005e4270bd09-16-2024 10:35 PM

Test Successful Brute Force

A pattern of multiple failed login attempts followed by a successful login has been detected, indicating a potential account compromise. This activity suggests that an attacker may have successfully guessed or brute-forced the user's password.

Reason

web, authentication event with source created high alert Test Successful Brute Force.

Framework

Not Available

Timeline

Case Details

Information

Provides you with a brief overview of the case.

SeverityLowStatusPending

AssigneeAssignees

CategoryCredential CompromiseCategories

Time CreatedTime Resolve

Closing ReasonNon-Issue

CRAM™ Details

Provides you the information about the affected business processes.

Notes

Communicate and Collaborate here.

Revision #2

Created 8 October 2024 11:08:58 by Aldion Pueblos

Updated 8 October 2024 11:43:17 by Aldion Pueblos