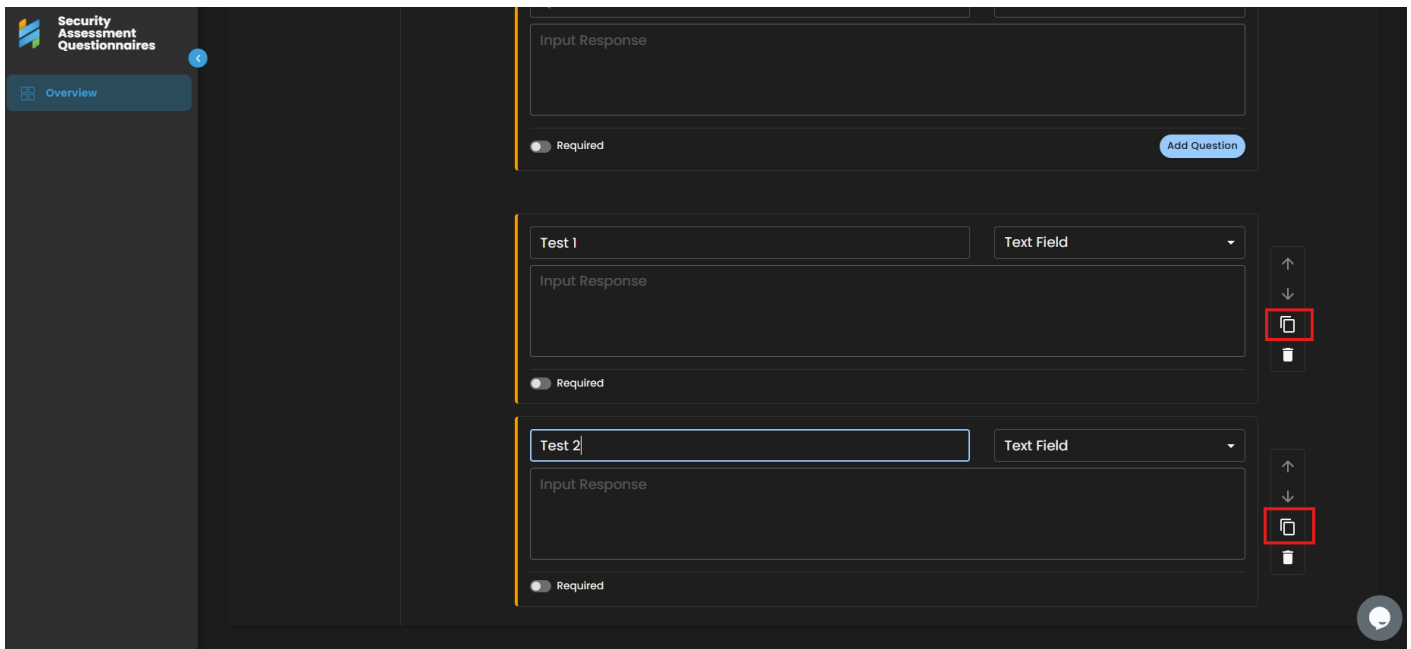


Daily Update: September 27

Here are the main updates of the CISO Workplace:

Security Assessment and Questionnaires Updates:

Duplicate Question Feature



The screenshot displays the 'Security Assessment Questionnaires' interface. On the left, there is a sidebar with a logo and an 'Overview' button. The main area shows a list of questions. The first question is 'Test 1' with a 'Text Field' input type. Below it is a 'Test 2' question, also with a 'Text Field' input type. Each question has an 'Input Response' field and a 'Required' toggle switch. A red box highlights the 'Duplicate' icon (two overlapping document icons) in the right-hand action menu of each question. The 'Add Question' button is visible at the top right of the question list.

TI Updates:

Show Previous Scans and Prompt Spear Fishing

⚙

Social Footprint

Go beyond the surface. Discover the hidden connections.

🔍 AndreiLM@cytechint.com

👤 Username AndreiLM@cytechint.com has found 48 Results ✓

High Social Exposure Risk Detected

This user's social exposure puts them at an increased risk of phishing attacks

Would you like to initiate a targeted spear-phishing simulation for this user?

Start Phishing Simulation



Scout an Employee

🔍

Show Scanned Users ☐

AM Andrei Madale

Scan User

FD Fredrik Dacer

Scan User

KT Kyla Theresa Martinito

Scan User

Scout an Employee

Close

🔍

Show Scanned Users ☒

AM Andrei Madale

Rescan User

Show Previous Result

FD Fredrik Dacer

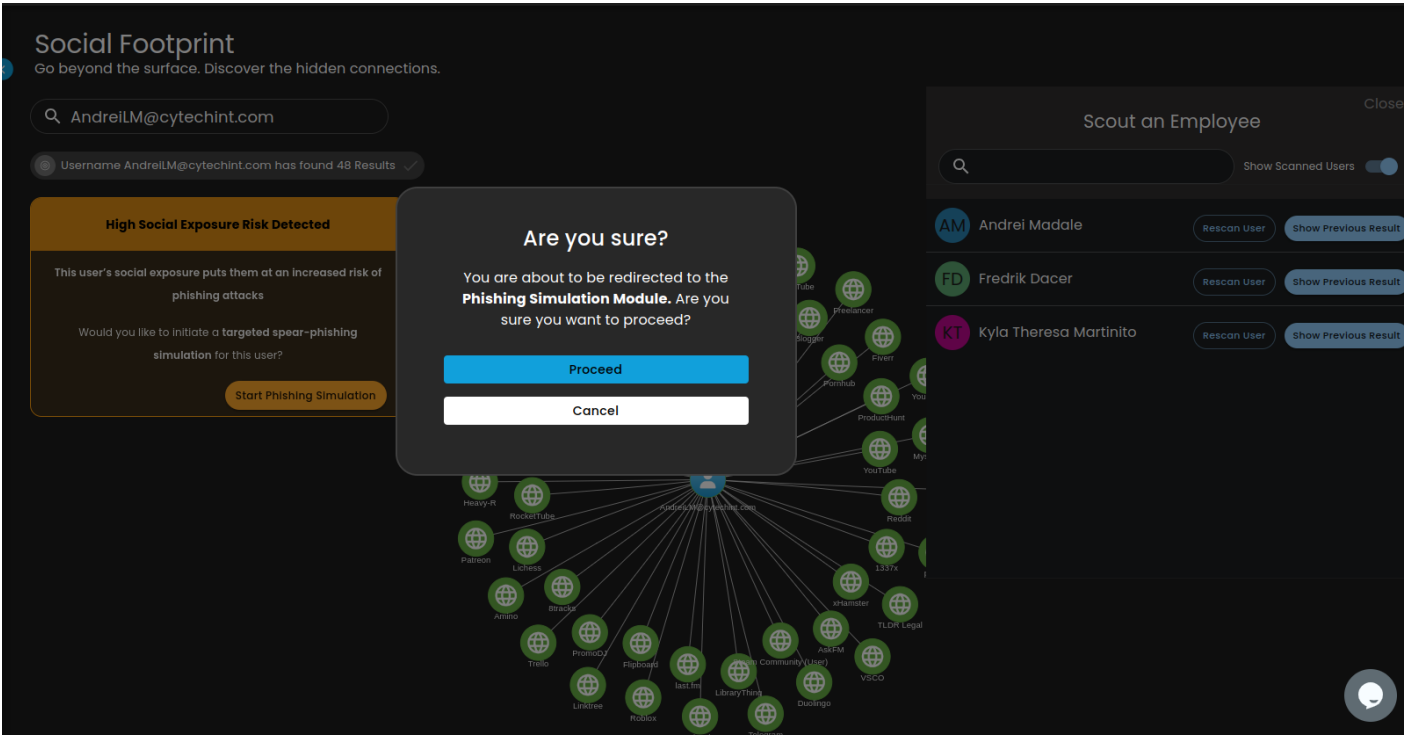
Rescan User

Show Previous Result

KT Kyla Theresa Martinito

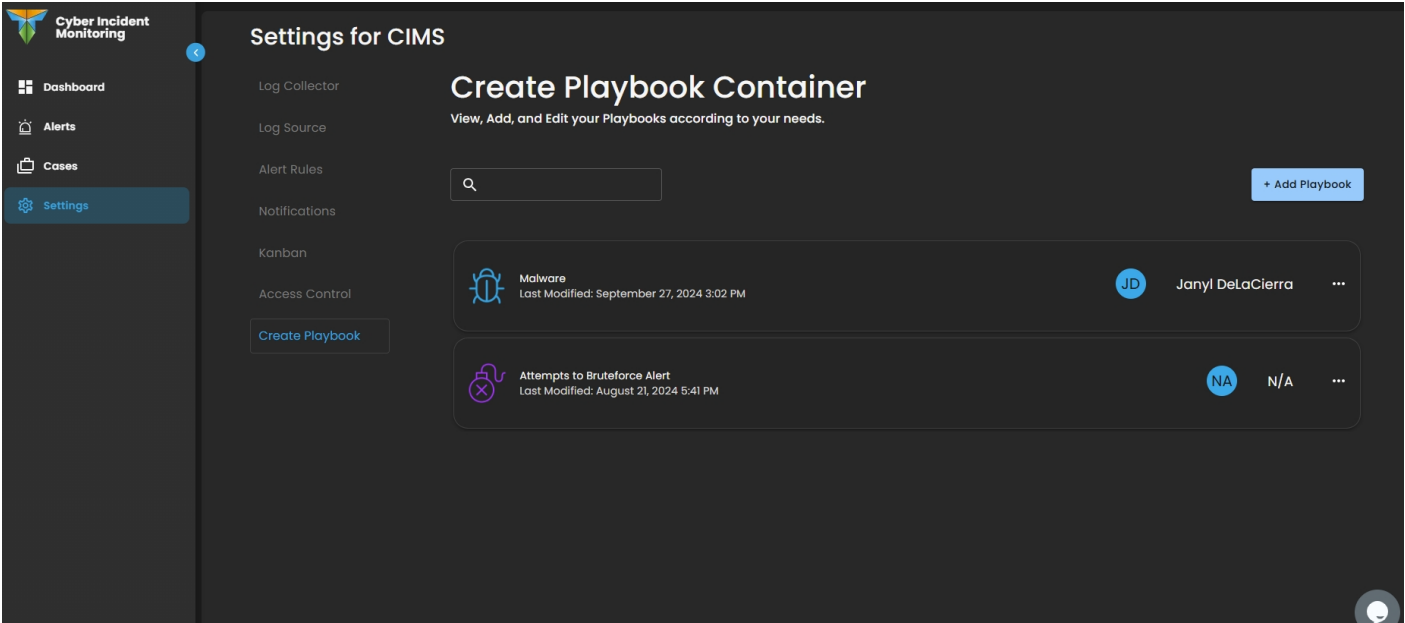
Rescan User

Show Previous Result



CIM Updates

Create Playbook Template Menu in Settings



Edit Playbook

Go back > Playbook: Attempts to Bruteforce Alert

Attempts to Bruteforce Alert

Add Phase

Phase 1

1. Data Enrichment **Add Task**

1.1 User Identification

1.2 Date of Detection

1.3 Host Identification

1.4 User Activity Enrichment

Phase 2

2. IP Intelligence Check **Add Task**

Phase 3

3. User Communication **Add Task**

Phase 4

4. False Positive Analysis **Add Task**

Phase 5

5. Escalation **Add Task**

1. Data Enrichment

1.1 User Identification **Edit**

To find out who triggered the detection, look at the event timeline of the detection. Determine whose email address is connected to the event.

1.2 Date of Detection **Edit**

Check for event timestamps in the detection or other relevant date and time values to potentially identify the exact date of when did the events had occurred.

1.3 Host Identification **Edit**

Relevant tags include user agent related values. These are tags related to the device used by the user to execute the said events.

1.4 User Activity Enrichment **Edit**

Confirm the results or outcome of the login events. How many login attempts occurred and are those events related to user/password attempts or MFA.

Website Updates

Website Contact Us

Platform ▾ Products ▾ Services ▾ Resources ▾

Start your free trial of our CISO Workplace™

Log me into my CISO Workplace™

Contact our sales team

Please fill out this form with your contact information.
A Sales Representative will contact you.
* Field is required

First Name *

Last Name *

Business Email *

Company Name *

Company Size *

Country *

Message

☐ I agree to the use or processing of my personal information by CyTech for the purpose of fulfilling this request and in accordance with CyTech Privacy Policy.

Submit

People. Process. Technology.

Bug Fixes Updates

1. [SAQ] Bug Fixes in Questionnaires Section
2. [CIM] Bug Fixes in the CIM v3

Revision #1

Created 27 September 2024 06:44:51 by Aldion Pueblos

