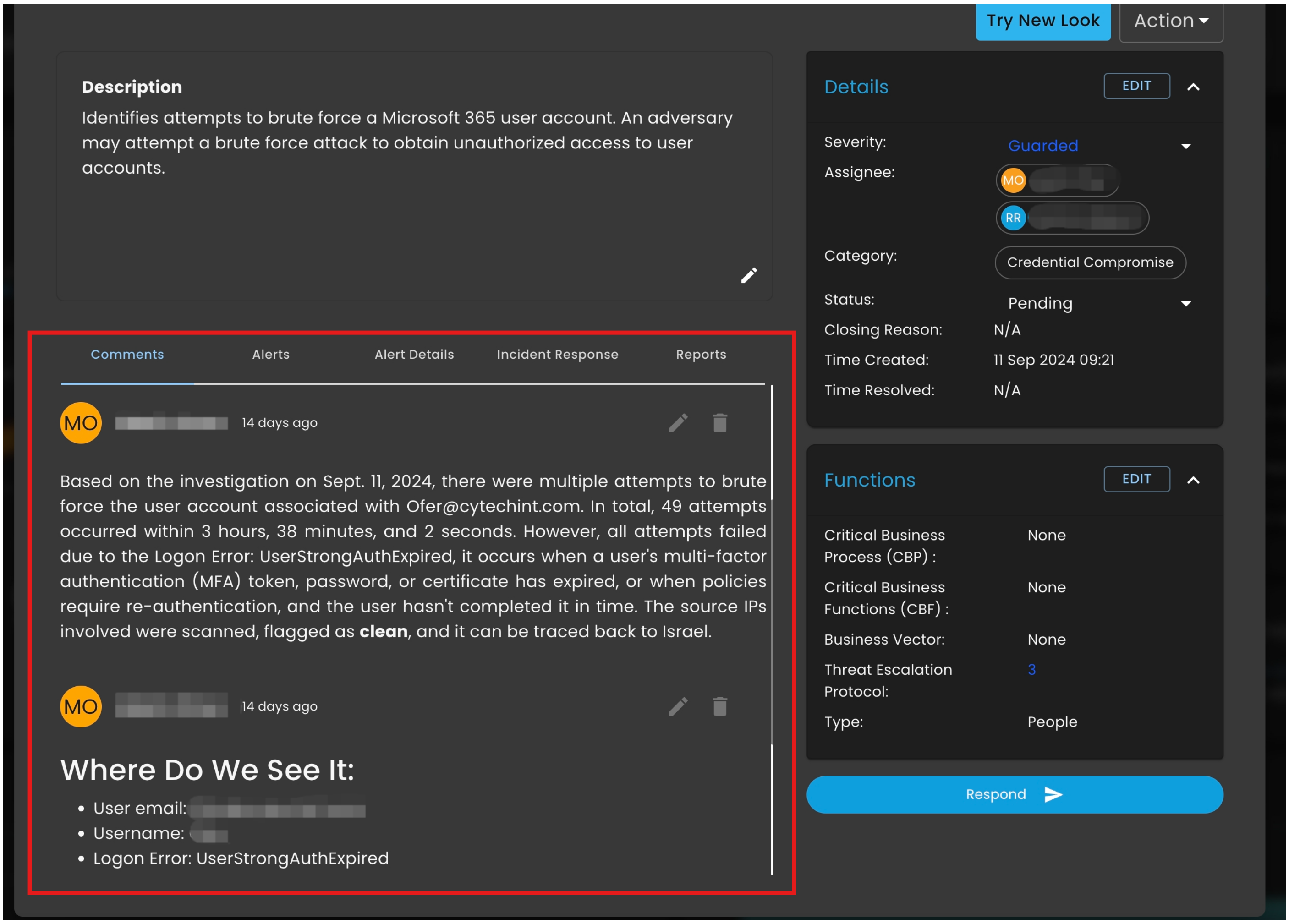
Daily Update: September 25

Here are the main updates of the CISO Workplace:

CIM Updates:

Bug Fix in Case Modal Comments (Old Look)



Description

Identifies attempts to brute force a Microsoft 365 user account. An adversary may attempt a brute force attack to obtain unauthorized access to user accounts.

MO [redacted] 14 days ago

Based on the investigation on Sept. 11, 2024, there were multiple attempts to brute force the user account associated with Ofer@cytechint.com. In total, 49 attempts occurred within 3 hours, 38 minutes, and 2 seconds. However, all attempts failed due to the Logon Error: UserStrongAuthExpired, it occurs when a user's multi-factor authentication (MFA) token, password, or certificate has expired, or when policies require re-authentication, and the user hasn't completed it in time. The source IPs involved were scanned, flagged as **clean**, and it can be traced back to Israel.

MO [redacted] 14 days ago

Where Do We See It:

- User email: [redacted]
- Username: [redacted]
- Logon Error: UserStrongAuthExpired

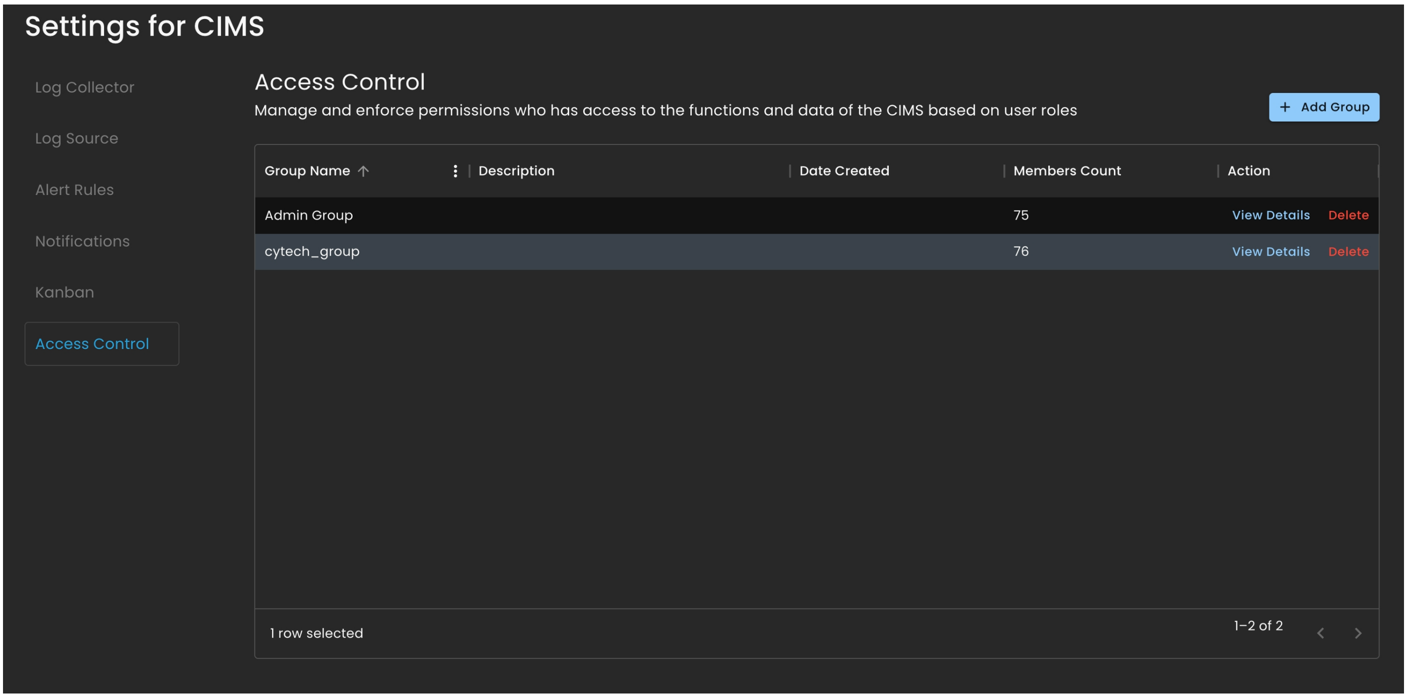
Details

Severity:	Guarded
Assignee:	MO [redacted] RR [redacted]
Category:	Credential Compromise
Status:	Pending
Closing Reason:	N/A
Time Created:	11 Sep 2024 09:21
Time Resolved:	N/A

Functions

Critical Business Process (CBP) :	None
Critical Business Functions (CBF) :	None
Business Vector:	None
Threat Escalation Protocol:	3
Type:	People

Access Control Support



Settings for CIMS

Access Control

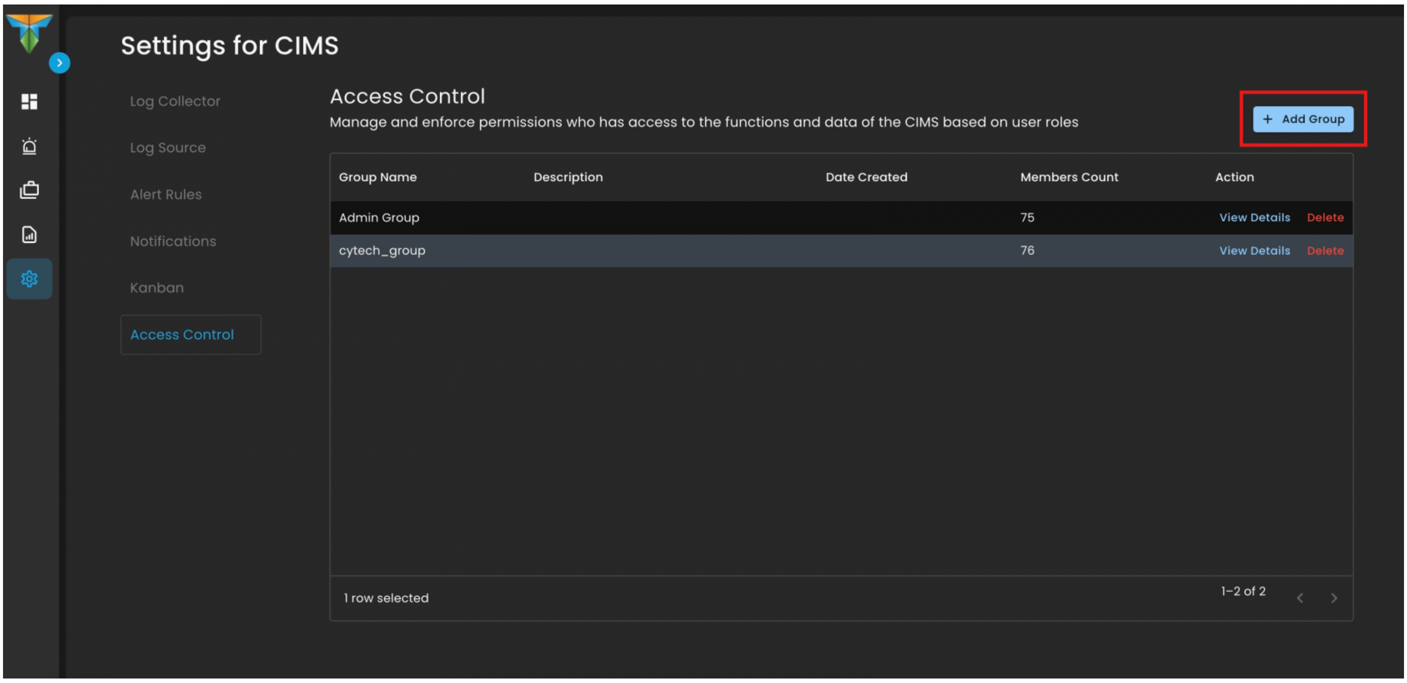
Manage and enforce permissions who has access to the functions and data of the CIMS based on user roles

Group Name	Description	Date Created	Members Count	Action
Admin Group			75	View Details Delete
cytech_group			76	View Details Delete

1 row selected

1–2 of 2

Support for Access Control Group



Settings for CIMS

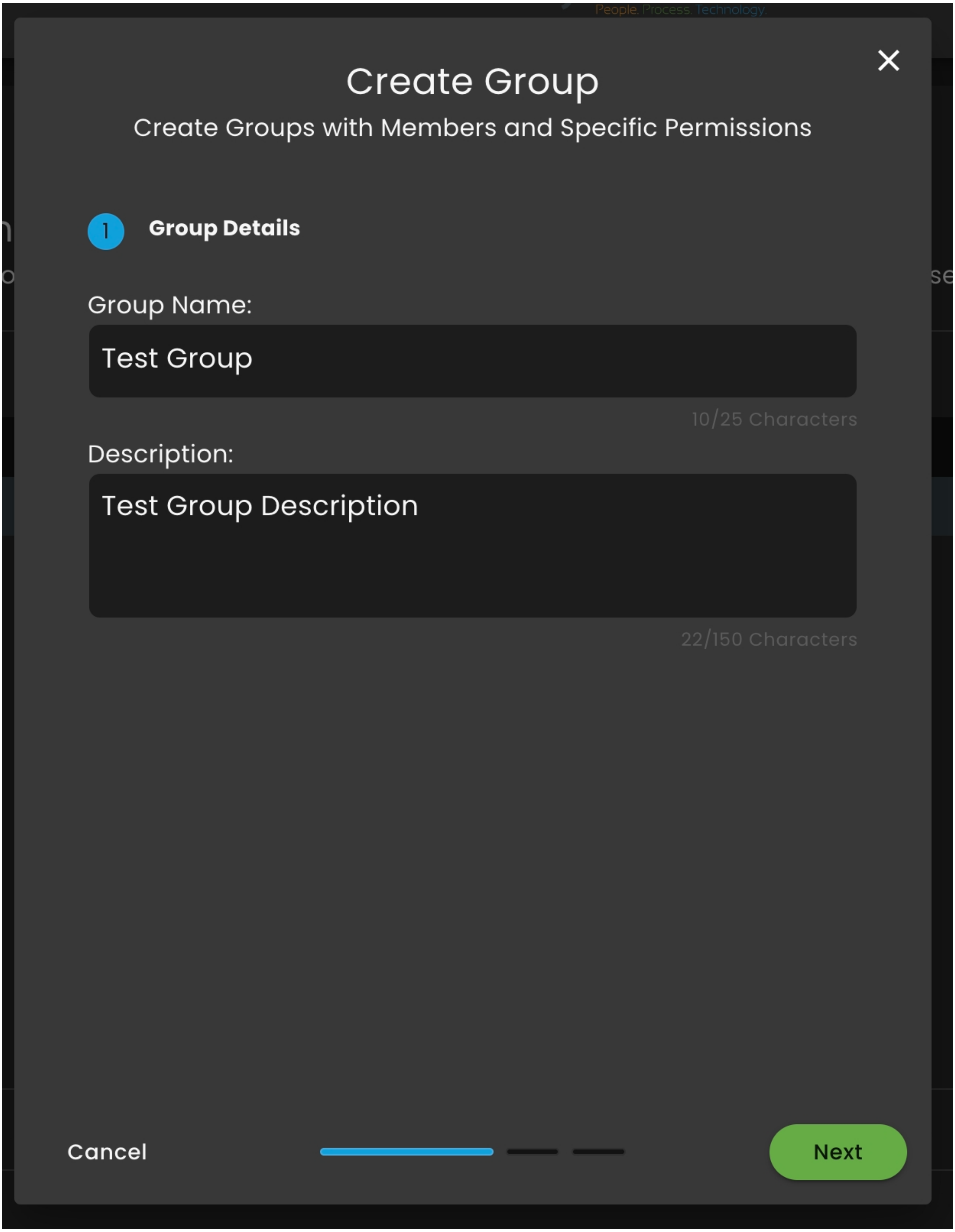
Access Control

Manage and enforce permissions who has access to the functions and data of the CIMS based on user roles

Group Name	Description	Date Created	Members Count	Action
Admin Group			75	View Details Delete
cytech_group			76	View Details Delete

1 row selected

1–2 of 2



Create Group

Create Groups with Members and Specific Permissions

1 **Group Details**

Group Name:

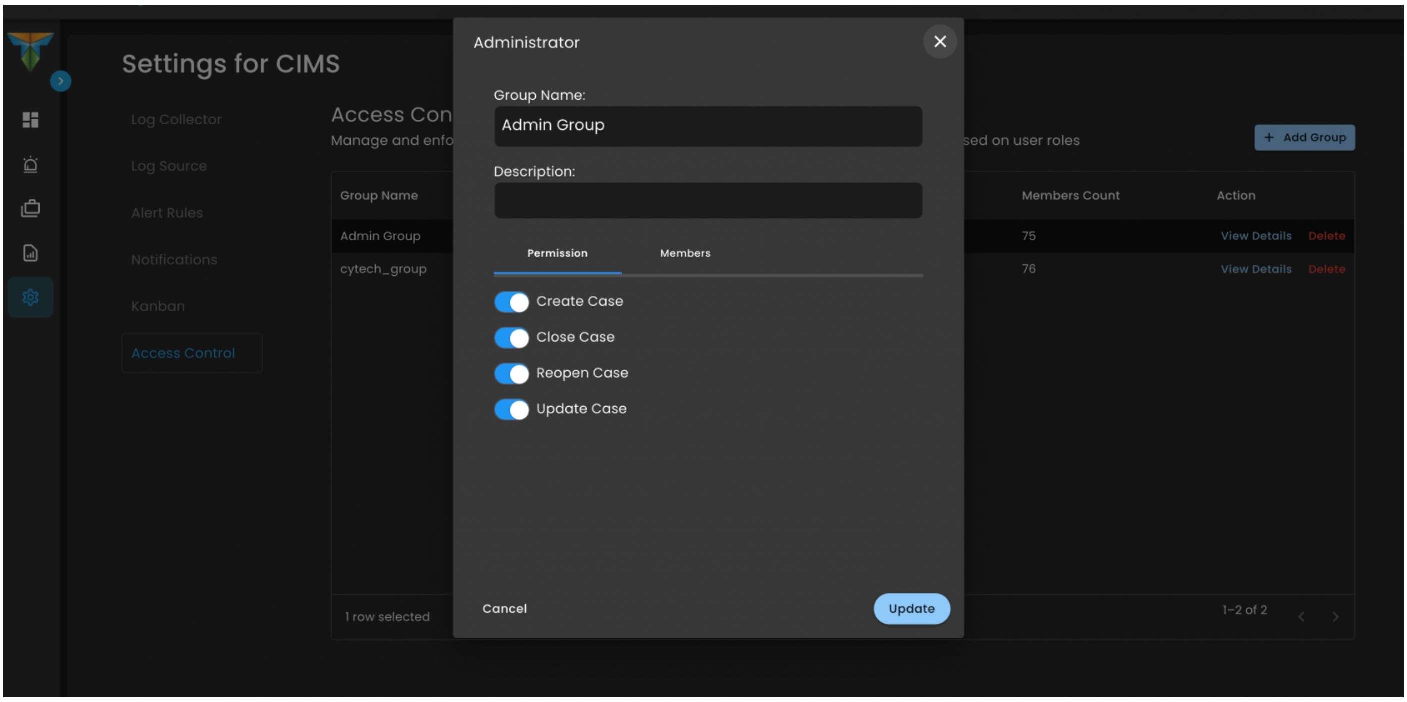
Test Group

10/25 Characters

Description:

Test Group Description

22/150 Characters



Group Name	Members Count	Action
Admin Group	75	View Details Delete
cytech_group	76	View Details Delete

Administrator

Group Name: Admin Group

Description:

Permission | Members

- Create Case
- Close Case
- Reopen Case
- Update Case

Revision #1
Created 25 September 2024 13:52:09 by Aldion Pueblos
Updated 25 September 2024 14:09:53 by Aldion Pueblos