

Daily Update: September 11

Here are the main updates of the CISO Workplace:

CIM Updates:

Improvement of the display of timeline elements to show more than 10 entries

The screenshot displays the 'Timeline Details' view for an alert titled 'Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]'. The interface is dark-themed and includes a navigation bar with 'Go back' and 'Case: 10113'. Below the title, there are tabs for 'Case Playbook', 'Alerts', 'Reports', and 'Incident Response'. The main content area is divided into two panels. The left panel, titled 'Related Alerts (2)', shows two alerts with a 'high' severity level and timestamps of 03:02 PM and 03:43 PM. The right panel, titled 'Timeline Details', shows a 'MITRE ATT&CK -> Credential Access -> Brute Force' timeline. A search bar is present above a table of events. The table has columns for 'Agent Name', 'User Name', 'Host Name', 'Source Ip', 'Destinati...', 'Event Categ...', 'Event Outca...', and '@Timestamp'. The table contains five rows of data, all with 'failure' as the event outcome and a timestamp of '2024-09-11...'. A 'Table Timeline' toggle is visible above the table. At the bottom of the table, a pagination control shows '1-5 of 14' with left and right navigation arrows, which is highlighted with a red box. To the right of the table, there is a 'No Timeline Selected' message with a folder icon and instructions: 'To view details, please select a timeline from the alert > related alerts > timeline.' The interface also includes a 'Json File (Raw)' button and a 'Timeline Details' header with various icons.

Go back > Case: 10113

TEP 3 Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]

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.

Case Playbook Alerts Reports Incident Response

Related Alerts (2)

- Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]
high
03:02 PM
- Attempts to Brute Force a Microsoft 365 User Account [cytech_developmentoperations]
high
01:49 PM

Timeline

Table Timeline

« < > » Jump to Change layout Change density

4 @ 18:37:48 11 Sep, 2024 @ 18:37:48

11 Sep, 2024 @ 18:37:48

cytech-logcollector 11 Sep, 2024 @ 18:37:48

UserLoginFailed

User Name:
Host Name:
Source IP:
Destination IP:
Event Category:
Event Outcome: failure

cytech-logcollector

UserLoginFailed

User Name:
Host Name:
Source IP:
Destination IP:
Event Category:
Event Outcome: fail

Investigation Guide

Bug fixes:

1. Client Onboard bug fixes
2. Removed unnecessary API calls

Revision #1

Created 11 September 2024 10:31:30 by Aldion Pueblos

Updated 11 September 2024 10:48:15 by Aldion Pueblos