

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

Go back

Case: 10113

STEP 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

03:43 PM

MITRE ATT&CK -> Credential Access -> Brute Force

Timeline

Search

Q

Table Timeline

Agent Name	User Name	Host Name	Source Ip	Destinati...	Event Categ...	Event Outco...	@Timestamp
✓	-----	-----	-----	-----	-----	failure	2024-09-11 ...
✓	-----	-----	-----	-----	-----	failure	2024-09-11 ...
✓	-----	-----	-----	-----	-----	failure	2024-09-11 ...
✓	-----	-----	-----	-----	-----	failure	2024-09-11 ...
✓	-----	-----	-----	-----	-----	failure	2024-09-11 ...

1-5 of 14

Investigation Guide

Timeline Details

Table

Json File (Raw)

No Timeline Selected

To view details, please select a timeline from the alert > related alerts > timeline.

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

p, 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