

Daily Update: November 13

Here are the main updates of the CISO Workplace:

CIM Updates:

Show Alert Details

The screenshot displays the configuration page for an alert rule titled "CyTech : Medium - O365 - Disable Mailbox". The interface is dark-themed and includes a close button (X) in the top right corner and an "Edit Alert Rule" button.

Description: It signifies the disabling or deactivation of a mailbox associated with a user or entity.

Metadata:

- Created by:** [Redacted]
- Updated by:** [Redacted]
- Severity:** Medium (indicated by a yellow dot)
- Risk Score:** 47 (indicated by a black dot)
- Last Run:** less than a minute ago
- Tags:** [Redacted]

Configuration Summary:

- Runs Every:** 5m (indicated by a clock icon)
- Additional Look-Back Time:** now-605100s (indicated by a clock icon with an exclamation mark)

Definition:

- Data View ID:** [Redacted]
- Data View Index Pattern:** [Redacted]
- Custom Query:**

```
data_stream.namespace : [Redacted] and event.module : "o365" and event.action : "disable-Mailbox"
```
- Rule Type:** query
- Timeline Template:** [Redacted]

Update Alert Rules

CISO Workplace 12:04 PM (UTC) | 8:04 PM (GMT +8) CyTech MSSP

← Back

Edit Alert Rule

Configure your alert rule to fit your monitoring needs.

About Definition

⚠ Edit at Your Own Risk
Make sure to review carefully, as editing may change the behavior of your alert, which is essential for internal operations.
[Need assistance? Reach out to our support team for help!](#)

Alert Details

Define the name and description for this alert rule.

Rule Name ⓘ
CyTech : Medium - 0365 - Disable Mailbox

Description ⓘ
It signifies the disabling or deactivation of a mailbox associated with a user or entity.

Alert Rule Severity

Assign a severity level to help prioritize responses.

Default Severity ⓘ
Medium

Save Changes? Restore Default Save Undo

Revision #1

Created 13 November 2024 12:01:28 by Aldion Pueblos

Updated 13 November 2024 12:07:57 by Aldion Pueblos