

Daily Update: September 5

Here are the main updates of the CISO Workplace:

Vulnerability Assessment and Management Updates:

Visual Improvements

Dashboard >> Scan >> Results Analysis

Asset Details

Asset Name: CyTech CyberNews Website Scan
URL: cybernews.cytechint.io
Hosting Provider: ec2-52-201-140-152.compute-1.amazonaws.com
Owner: aldion@cytechint.com
Asset Type: WEBSITE

Vulnerability Scan Details

Scan Date: July 12th 2024, 3:41:38 pm
Scan Duration: 21 second(s)
Total Vulnerabilities Detected: 65

Legend

0.0	None
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

Common Vulnerabilities & Exposures from Target Asset

CVE	Severity Score	Severity	URL
CVE-2023-38408	9.8	Critical	https://vulners.com/cve/CVE-2023-38408
B8190CDB-3EB9-5631-9828-8064A1575B23	9.8	Critical	https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064
8FC9C5AB-3968-5F3C-825E-E8DB6379A623	9.8	Critical	https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB6379A623
CVE-2020-15778	7.8	High	https://vulners.com/cve/CVE-2020-15778
SSV-92579	7.5	High	https://vulners.com/seebug/SSV-92579
PACKETSTORM:173661	7.5	High	https://vulners.com/packetstorm/PACKETSTORM:173661
F0979183-AE88-53B4-86CF-3AF0523F3807	7.5	High	https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0
1337DAY-ID-26576	7.5	High	https://vulners.com/zdt/1337DAY-ID-26576
CVE-2021-41617	7.0	High	https://vulners.com/cve/CVE-2021-41617
EDB-ID:46516	6.8	Medium	https://vulners.com/exploitdb/EDB-ID:46516
EDB-ID:46193	6.8	Medium	https://vulners.com/exploitdb/EDB-ID:46193
CVE-2019-6110	6.8	Medium	https://vulners.com/cve/CVE-2019-6110
CVE-2019-6109	6.8	Medium	https://vulners.com/cve/CVE-2019-6109
C94132FD-IFA5-5342-B6EE-0DAF45EEFF3	6.8	Medium	https://vulners.com/githubexploit/C94132FD-IFA5-5342-B6EE-0DAF
10213DBE-F683-58BB-B6D3-353173626207	6.8	Medium	https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-35317
CVE-2023-51385	6.5	Medium	https://vulners.com/cve/CVE-2023-51385
CVE-2023-48795	5.9	Medium	https://vulners.com/cve/CVE-2023-48795
CVE-2020-14145	5.9	Medium	https://vulners.com/cve/CVE-2020-14145

Running Scans

Showing all currently running scans along with percentage to completion and number of severities.

Search this Board

Show Completed

Scans

- Scan Success 100% cybernews.cytechint.io
Severities: 0 0 0 0 0 0
Scan Type: WEBSITE
Date Created: 2024-08-30 03:02:58
- Scan Success 100% cybernews.cytechint.io
Severities: 0 0 0 0 0 0
Scan Type: WEBSITE
Date Created: 2024-08-30 03:01:57
- Scan Failed Fail https://cybernews.cytechint.io/
Severities: 0 6 0 0 0 0
Scan Type: WEBSITE
Date Created: 2024-08-30 03:01:39
- Scan Success 100% selina.com
Severities: 0 0 0 0 0 0
Scan Type: WEBSITE
Date Created: 2024-08-30 02:48:47
- Scan Success 100% www.selina.com
Severities: 0 0 0 0 0 0
Scan Type: WEBSITE
Date Created: 2024-08-30 02:47:13
- Scan Failed Fail workplace.cytechint.com
Severities: 0 0 0 0 0 0
Scan Type: WEBSITE
Date Created: 2024-07-24 08:51:17
- Scan Success 100% www.selina.com
Severities: 0 0 0 0 0 0
Scan Type: WEBSITE
- Scan Success 100% cybernews.cytechint.io
Severities: 3 18 28 1 5
Scan Type: WEBSITE
- Scan Success 100% www.cytechint.com
Severities: 0 0 0 0 0 0
Scan Type: WEBSITE

RM and Compliance Modules Updates

Bug Fix on Task Gantt Chart

Requirements

All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In us...

Task Activity

Gantt Chart

Comments

Files

Task Activity	Start Date	End Date	21 Jul	22 Jul	23 Jul	24 Jul	25 Jul	26 Jul	27 Jul	28 Jul	29 Jul	30 Jul	31 Jul	01 Aug	02 Aug	03 Aug
Analysis for minimum requirements	2024-07-22	2024-11-22	[Gantt bar]													
Analysis for minimum requirements	2024-07-22	2024-11-22	[Gantt bar]													
Asset Analysis	2024-09-04	2024-09-04	[Gantt bar]													

No Results Found
It looks like there's nothing to display at the moment. Try adding a Timeline to get started.

[Add Timeline](#)

Task Completed: 0

Tasks Updated: 0

Total Tasks: 1

Search: Name/Target Search... Gantt Chart View Pending Tasks

Task names	Start Date	End Date	31 May	01 Jun	02 Jun	03 Jun	04 Jun	05 Jun	06 Jun	07 Jun	08 Jun	09 Jun	10 Jun	11 Jun	12 Jun	13
12.6.3.1	2024-05-31	2024-06-01	12.6.3.1													
12.8.1	2024-05-31	2024-06-01	12.8.1													
12.8.2	2024-05-31	2024-06-01	12.8.2													
12.8.3	2024-05-31	2024-06-01	12.8.3													
12.8.4	2024-05-31	2024-06-01	12.8.4													
12.8.5	2024-05-31	2024-06-01	12.8.5													
12.10.3	2024-05-31	2024-06-01	12.10.3													
1.1.1	2024-06-10	2024-09-28														
Analysis for minimum	2024-07-22	2024-11-23														
Analysis for minimum	2024-07-22	2024-11-23														
Asset Analysis	2024-09-04	2024-09-04														
1.2.1	2024-06-01	2024-07-26														

14-14 of 139

CIM Updates

Improvement on the display of JSON Formatted Alert Information

Go back > Case: 9013

CyTech : Medium - O365 - Access Request Approved

An event indicating that a user's request for access to a resource has been approved, allowing them to gain access.

Case Playbook Alerts Reports Incident Response

Related Alerts (2)

- CyTech : Medium - O365 - Access Request Approved (1:14 PM)
- CyTech : Medium - O365 - Access Request Created (10:01 PM)

Alert Details

Details Table **Json File (Raw)**

Find ...

```

{
  "_index": "[REDACTED]",
  "_id": "[REDACTED]",
  "_score": 1,
  "kibana.alert.severity": "medium",
  "kibana.alert.workflow_status_updated_at": "2024-09-04T09:38:51.142Z",
  "kibana.alert.rule.updated_by": "[REDACTED]",
  "signal.ancestors.depth": 0,
  "event.category": "web",
  "host.risk.calculated_score_norm": 43.418954,
  "user_agent.original.text": "Win32_Outlook_Webview 18.0.17928.20114",
  "kibana.alert.reason.text": "web event with source [REDACTED] created medium alert CyTech : Medium - O365 - Access Request Approved.",
  "client.address": "[REDACTED]",
  "kibana.alert.ancestors.depth": 0,
  "signal.rule.enabled": "true",
  "signal.rule.max_signals": 100,
  "source.geo.region_name": "Ireland",
  "kibana.alert.risk_score": 47,
  "signal.rule.updated_at": "2024-03-12T08:03:57.211Z",
  "source.ip": "[REDACTED]",
  "agent.name": "[REDACTED]"
}

```

Timeline

Alert Summary

The Summary of your Alert.

Summary Investigation Guide Table View **Raw File** Timeline

Find ...

```

{
  "_index": "[REDACTED]",
  "_id": "[REDACTED]",
  "_score": 1,
  "kibana.alert.severity": "medium",
  "kibana.alert.workflow_status_updated_at": "2024-09-02T17:28:27.987Z",
  "kibana.alert.rule.updated_by": "elastic",
  "signal.ancestors.depth": 0,
  "event.category": "web",
  "host.risk.calculated_score_norm": 56.29565,
  "user_agent.original.text": "AsyncMediaTransformation/1.282.2.0",
  "kibana.alert.reason.text": "web event with file [REDACTED] on sharepoint created medium alert CyTech : Medium - O365 - Shari ng Set.",
  "client.address": "[REDACTED]",
  "kibana.alert.ancestors.depth": 0,
  "signal.rule.enabled": "true",
  "signal.rule.max_signals": 100,
  "source.geo.region_name": "[REDACTED]",
  "kibana.alert.risk_score": 47,
  "signal.rule.updated_at": "2024-03-12T08:03:57.213Z",
}

```

Revision #1

Created 5 September 2024 11:13:45 by Aldion Pueblos

Updated 5 September 2024 11:38:29 by Aldion Pueblos