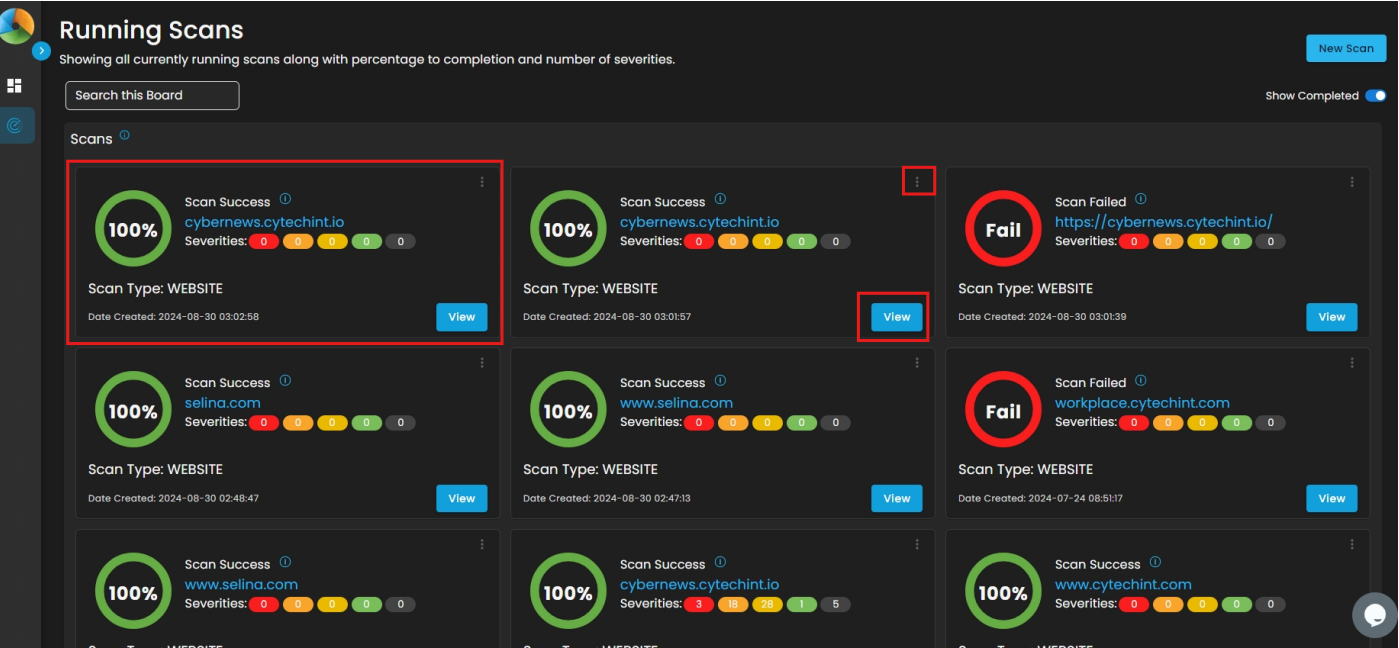


Daily Update: September 5

Here are the main updates of the CISO Workplace:

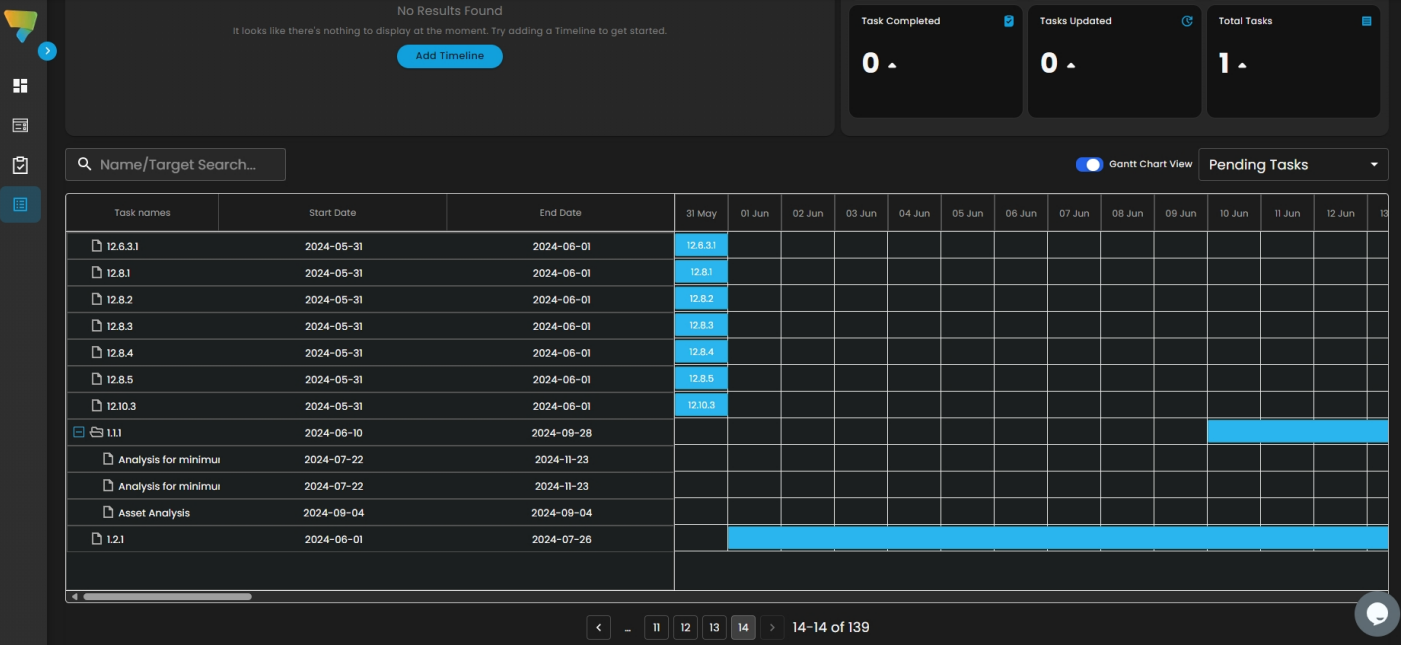
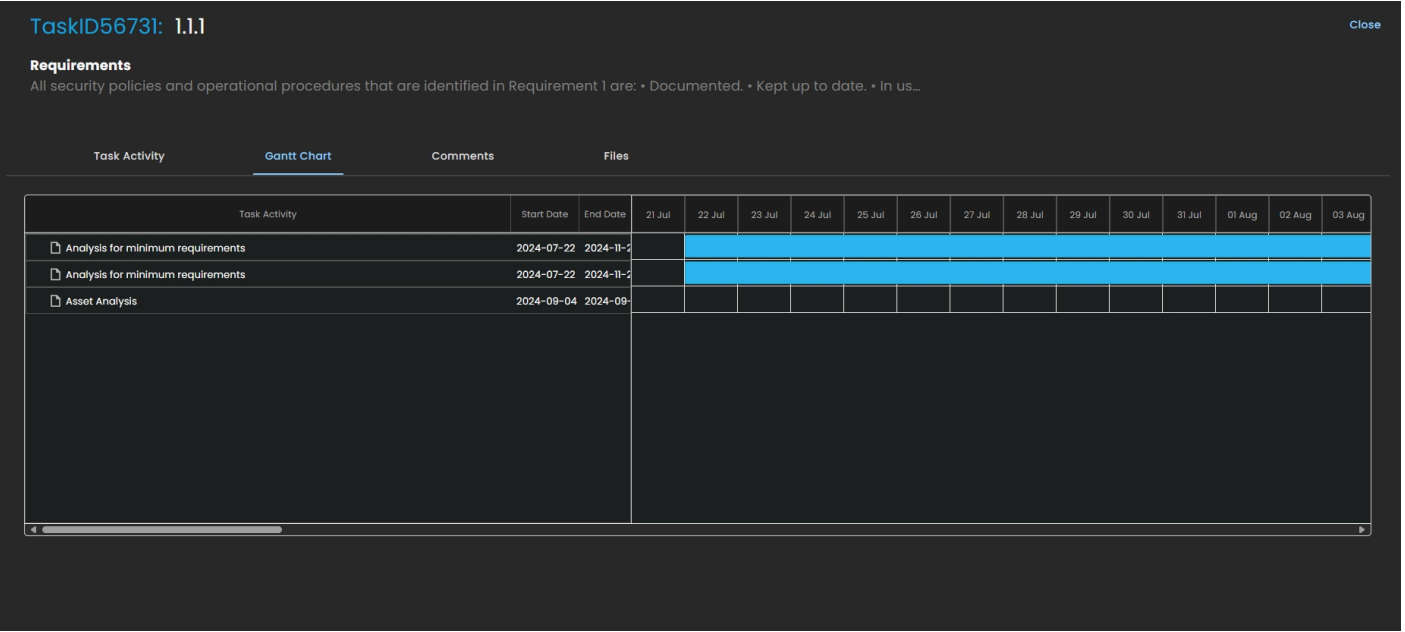
Vulnerability Assessment and Management Updates:

Visual Improvements



RM and Compliance Modules Updates

Bug Fix on Task Gantt Chart



CIM Updates

Improvement on the display of JSON Formatted Alert Information

[Go back](#) > Case: 9013

ITP

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

medium

10:14 PM

CyTech : Medium - O365 - Access Request Created

medium

10:01 PM

Alert Details

Details

Table

Json File (Raw)

Find ...

{

"_index":

"_id":

"_score":

"kibana.alert.severity": "medium",

"kibana.alert.workflow_status_updated_at": "2024-09-04T09:38:51.142Z",

"kibana.alert.rule.updated_by":

"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 > created medium alert CyTech : Medium - O365 - Access Request Approved.",

"client.address":

"kibana.alert.ancestors.depth": 0,

"signal.rule.enabled": "true",

"signal.rule.max_signals": 100,

"source.geo.region_name": "teinstar",

"kibana.alert.risk_score": 47,

"signal.rule.updated_at": "2024-03-12T08:03:57.211Z",

"source.ip":

"agent.name":

}

Timeline

Alert Summary

The Summary of your Alert.

Summary

Investigation Guide

Table View

Raw File

Timeline

Find ...

{

"_index":

"_id":

"_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 sharepoint created medium alert CyTech : Medium - O365 - Shari

ng Set.",

"client.address":

"kibana.alert.ancestors.depth": 0,

"signal.rule.enabled": "true",

"signal.rule.max_signals": 100,

"source.geo.region_name":

"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