

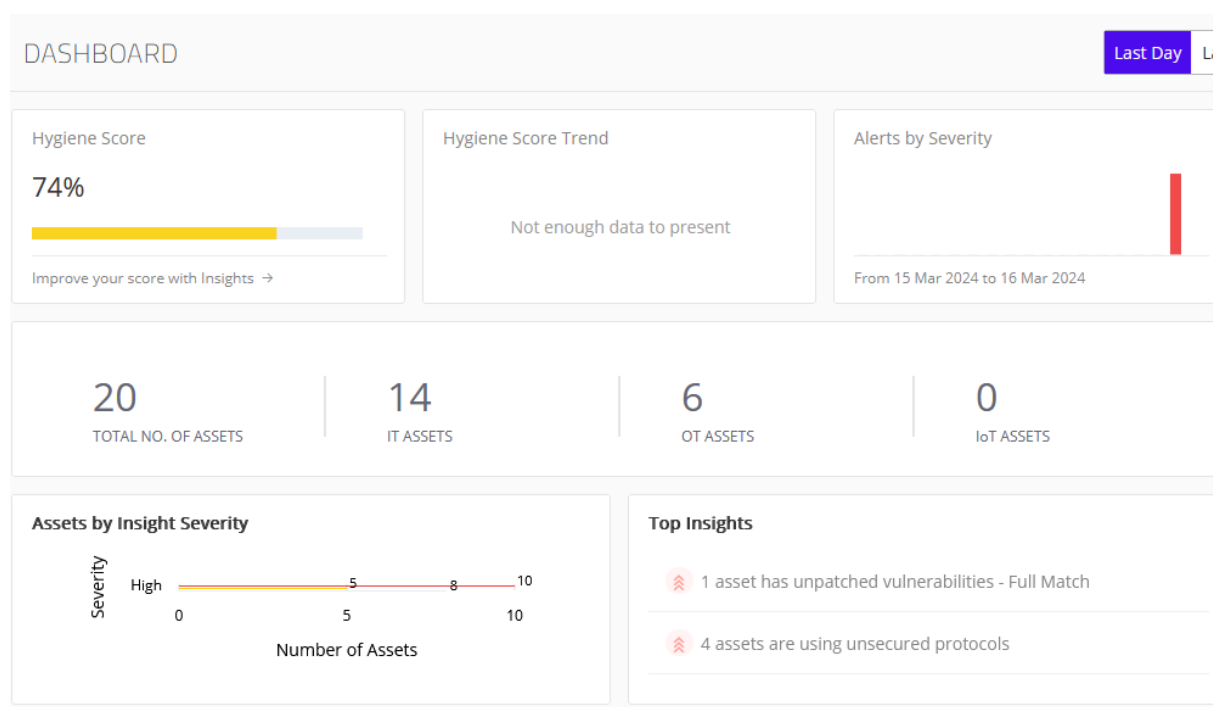
# Aplicatia Claroty-IoT

## REDUCEREA COMPLEXITĂȚII CYBERSECURITĂȚII INDUSTRIALE

Platforma Claroty oferă cea mai largă gamă de controale de securitate cibernetică industrială din industrie într-o singură soluție care se implementează fără probleme și se integrează perfect cu infrastructura existentă.

Platforma de Cyber Security destinata infrastructurilor industriale.

Pagina de start reprezinta starea generala a sistemului:



<https://claroty.com/blog/>

Securitatea cibernetică industrială eficientă începe cu a ști ce trebuie securizat. Platforma Claroty vă oferă aceste cunoștințe prin dezvăluirea și contextualizarea 100% din conținutul rețelei dvs., inclusiv conținutul său invizibil. Rezultatul este un inventar centralizat, ușor de gestionat și mereu actualizat al tuturor activelor, proceselor și căilor de conectivitate OT, IoT și IIoT din rețeaua dvs., precum și o perspectivă definitivă a modului în care arată normalul.

Vizibilitate

Acoperirea de neegalat a protocolului OT și tehnologia de scanare activă, pasivă și AppDB permit platformei Claroty să ofere vizibilitate deplină asupra tuturor celor trei variabile, care sunt integrante pentru evaluarea și reducerea eficiență a riscurilor în mediile OT. Acestea includ 1) Vizibilitatea activelor; 2) Vizibilitatea sesiunii de rețea; și 3) Vizibilitatea procesului operațional. Claroty este singurul furnizor care oferă acest calibru de vizibilitate OT.

## Detectarea amenințărilor

Platforma Claroty utilizează cinci motoare de detectare pentru a profila automat toate activele, comunicațiile și procesele din mediile OT, pentru a stabili o linie de bază comportamentală care caracterizează traficul legitim și pentru a elimina falsele pozitive și pentru a oferi o acoperire cuprinzătoare și continuă de monitorizare a securității și integrității OT - totul fără a necesita expertiza OT. Aceste motoare includ: Detectare anomalii, Comportamente de securitate, Amenințări cunoscute, Comportamente operaționale și Reguli personalizate.

## Scenariu Profesor:

Data Sources – Play PCAPS → pentru a “injectat” trafic in aplicatie

CLAROTY

CyberX / Data Sources / Play PCAPS

TRAININGAdmin

← Back to Main Menu

System Health Dashboard

Activity Log

Management

Data Sources

Active Detection

Interface Configuration

Project Files

Netflow

IoT Matchers

Play PCAPS

Alerts

Log Configuration

Integrations

User Management

Play PCAPS

+ Choose File

Upload

Cancel

RESULTS (15)

NAME	SIZE	UPLOAD DATE	NETWORK	DETECT KNOWN THREATS	ACTIONS	LAST RUN
ab_L71_download.pcapng	873.14 KB	14 Mar 2024, 11:43:54	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	14 Mar 2024, 13:23:16
ab_L71_firmware_update.pcapng	26.28 MB	14 Mar 2024, 11:43:56	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	14 Mar 2024, 13:23:43
ab_L71_online_edit.pcapng	2.48 MB	14 Mar 2024, 11:43:54	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	14 Mar 2024, 13:23:51
ab_L71_prog_mode.pcapng	6.07 MB	14 Mar 2024, 11:43:54	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	14 Mar 2024, 13:25:57
ab_L71_run_mode.pcapng	3.99 MB	14 Mar 2024, 11:43:54	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	14 Mar 2024, 13:25:01
ab_L71_test_mode.pcapng	2.31 MB	14 Mar 2024, 11:43:54	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	14 Mar 2024, 13:25:10
ab_L71_upload.pcapng	5.37 MB	14 Mar 2024, 11:43:55	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	14 Mar 2024, 13:25:15
Chomsky-ThreeepWood-VNC-NoEncryption.pcap	872.47 KB	16 Mar 2024, 10:06:18	Select network	Yes	<div>Play RT</div> <div>Play</div> <div>Delete</div>	16 Mar 2024, 10:06:40

← Back To Main Menu

System Health Dashboard

Activity Log

Management

Data Sources

Interface Configuration

App DB

Netflow

IoT Matchers

Play PCAPS

Alerts

Log Configuration

Integrations

User Management



## Se identifica Asset-urile critice

The screenshot shows the CLAROTY Assets page. The left sidebar contains navigation links: Dashboard, Visibility (selected), Overview, Assets (selected), Zones, Settings, Risk & Vulnerabilities, Threat Detection, Investigation, and Reports. The main area displays the ASSETS page with a filter bar at the top. The filter bar includes a search bar, a filter button, and a dropdown menu for Asset Criticality. The dropdown menu is open, showing options: High (selected), Medium, and Low. Below the filter bar, there is a table of assets with columns: NAME, IP T1, MAC T1, CLASS T1, TYPE T1, VENDOR T1, CRITICALITY T1, RISK LEVEL T1, FIRST SEEN T1, and LAST SEEN T1. The table contains 6 rows of data. The first row is highlighted.

NAME	IP T1	MAC T1	CLASS T1	TYPE T1	VENDOR T1	CRITICALITY T1	RISK LEVEL T1	FIRST SEEN T1	LAST SEEN T1
Chemical_plant	10.1.30.1	00:1D:9C:C0:04:9D	OT	PLC	Rockwell Automation	High	High	14 Mar 2024, 13:24	28 Mar 2024, 10:24
10.10.6.81	10.10.6.81	40:00:00:5D:3F:22	OT	PLC	Triconex	High	High	16 Mar 2024, 10:10	16 Mar 2024, 10:10
10.1.34.1	10.1.34.1	00:80:F4:12:8B:10	OT	PLC	Schneider Electric	High	High	16 Mar 2024, 10:09	16 Mar 2024, 10:09
HVAC-System	10.1.31.6	28:63:36:88:F7:AE	OT	PLC	Siemens	High	High	16 Mar 2024, 12:42	16 Mar 2024, 12:42
10.1.30.1:Card 2 \ Addr 255			OT	PLC	Rockwell Automation	High	Medium	14 Mar 2024, 13:24	14 Mar 2024, 13:24
10.1.31.1	10.1.31.1	28:63:36:26:F0:74	OT	PLC	Siemens	High	Medium	16 Mar 2024, 12:42	16 Mar 2024, 12:42

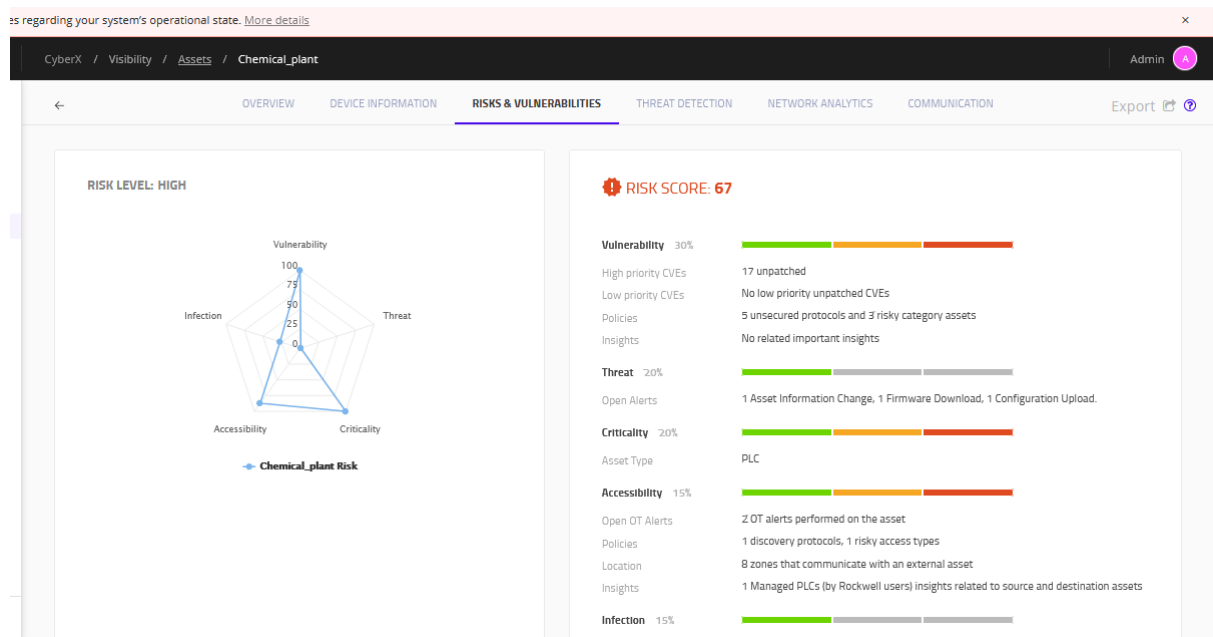
Se alege un asset critic exemplu → Chemical\_plant → si se analizeaza

[Chemical\\_plant](#)

La Risk & Vulnerability → se analizeaza detalii despre scorul primit:

The screenshot shows the CLAROTY Chemical\_plant overview page. The left sidebar contains navigation links: Dashboard, Visibility (selected), Overview, Assets (selected), Zones, Settings, Risk & Vulnerabilities, Threat Detection, Investigation, and Reports. The main area displays the Chemical\_plant overview page. The page has a header with the asset name and a sub-header with the device name. Below the header, there is a table of device information. The table has columns: IP, MAC, Virtual Zone, Risk Level, Type, and Vendor. The first row of data is highlighted.

IP	MAC	Virtual Zone	Risk Level	Type	Vendor
10.1.30.1	00:1D:9C:C0:04:9D	PLC: Rockwell	High	PLC	Rockwell Automation



Se analizeaza sectiunea Zones

CLAROTY CyberX / Visibility / Zones Admin

ZONES

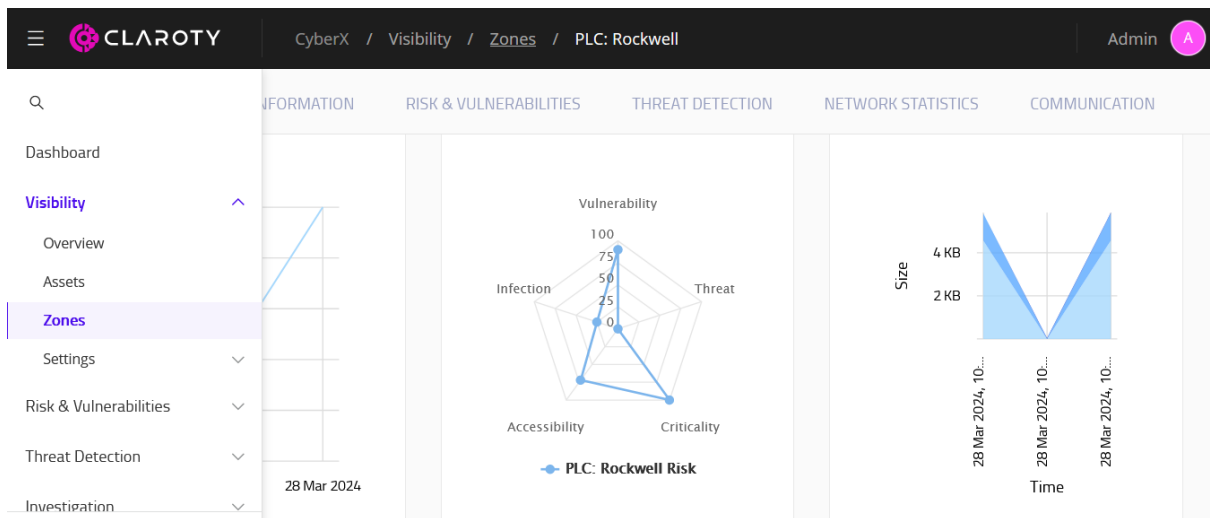
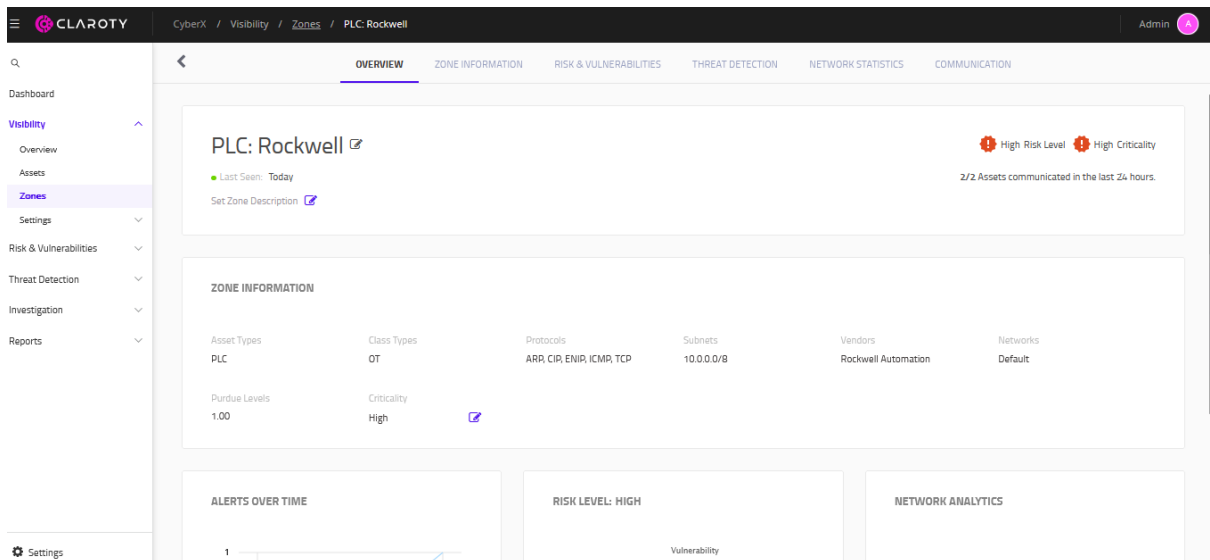
Filter By: Risk Level Criticality

Risk Level: Risk Level Criticality: Switch to Query View

RESULTS (17)

NAME	ASSETS	RISK LEVEL	CRITICALITY	ACTIONS
<input type="checkbox"/> PLC: Modbus,pcwin	1	High	High	Edit
<input type="checkbox"/> PLC: Rockwell	2	High	High	Edit
<input type="checkbox"/> PLC: Tristation	1	High	High	Edit
<input type="checkbox"/> Engineering Station: Modbus,pcwin	1	Medium	Medium	Edit
<input type="checkbox"/> Engineering Station: Rockwell	1	Medium	Medium	Edit
<input type="checkbox"/> PLC: S7	2	Medium	High	Edit
<input type="checkbox"/> HMI: Rockwell	1	Low	Medium	Edit

Din sectiunea Zones, se alege o zona critica care se analizeaza



Se realizeaza o investigatie → OT Audit

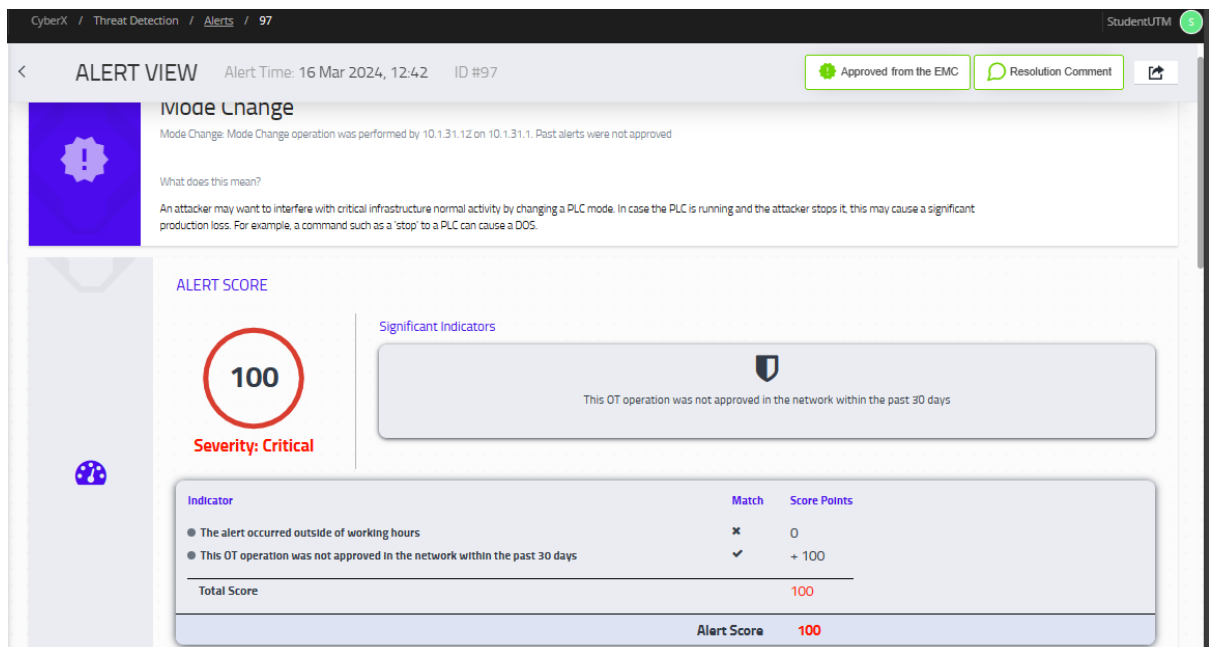
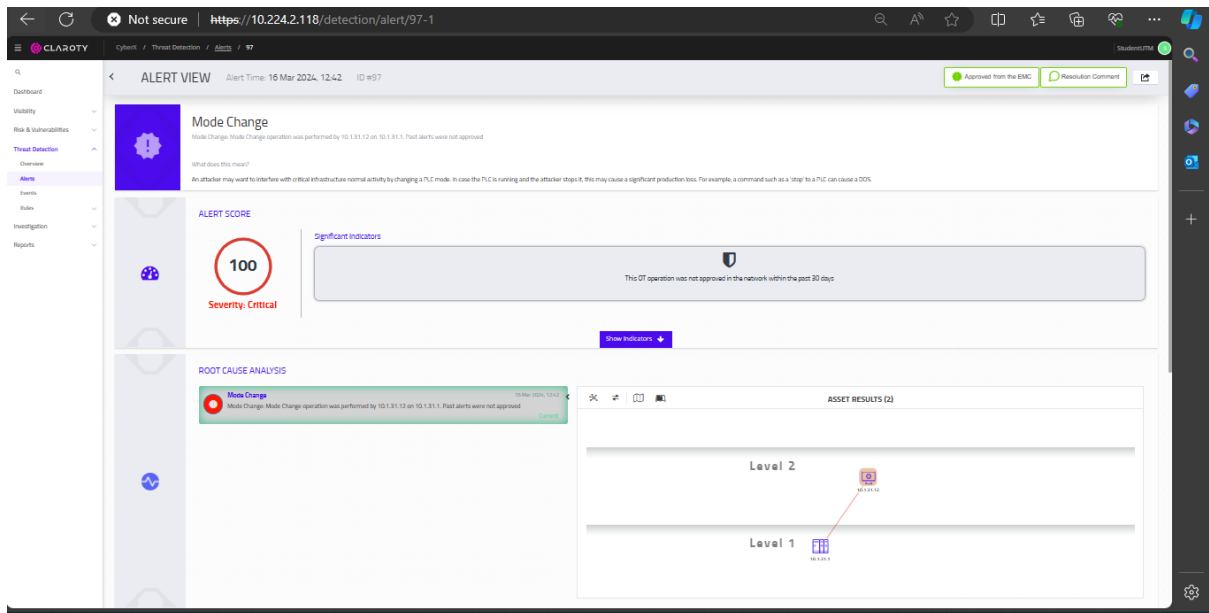
The screenshot shows the Claroty OT Audit interface. The left sidebar contains a navigation menu with options: Dashboard, Visibility, Risk & Vulnerabilities, Threat Detection, Investigation (selected), DNS, Process Values, Network Sessions, Protocols Summary, Baseline Summary, Baselines, OT Audit (highlighted), and Reports. The main content area displays 'RESULTS (16)' with a table of audit findings. The table has columns for 'DESCRIPTION' and 'DATE DETECTED'. The findings listed are:

DESCRIPTION	DATE DETECTED
Mode Change: Mode Change operation was performed by 10.1.30.10 on 10.1.30.1. Past alerts were not approved	28 Mar 2024, 10:28
Configuration Download: Configuration Download critical change operation was performed by 10.1.30.10 on 10.1.30.1	28 Mar 2024, 10:26
Firmware Download: Controller firmware download performed to 10.1.30.1 by 10.1.30.10. Firmware Download operation was performed by 10.1.30.10 on 10.1.30.1	28 Mar 2024, 10:26
Mode Change: Mode Change operation was performed by 10.1.31.12 on 10.1.31.1. Past alerts were not approved	16 Mar 2024, 12:42
	16 Mar 2024

The screenshot shows the Claroty OT Audit interface with a detailed view of results. The left sidebar is the same as the previous screenshot. The main content area displays 'OT AUDIT' with a 'Filter By' section and a 'Type' dropdown set to 'Select One or More'. The 'RESULTS (16)' table is expanded to show more details, including 'ID', 'TI', and 'TYPE' columns. The findings listed are:

ID	TI	TYPE	DESCRIPTION	DATE DETECTED
121		Configuration Upload	Mode Change: Mode Change operation was performed by 10.1.30.10 on 10.1.30.1. Past alerts were not approved	28 Mar 2024, 10:28
117		Configuration Download	Configuration Download: Configuration Download critical change operation was performed by 10.1.30.10 on 10.1.30.1	28 Mar 2024, 10:26
119		Firmware Download	Firmware Download: Controller firmware download performed to 10.1.30.1 by 10.1.30.10. Firmware Download operation was performed by 10.1.30.10 on 10.1.30.1	28 Mar 2024, 10:26
97		Mode Change	Mode Change: Mode Change operation was performed by 10.1.31.12 on 10.1.31.1. Past alerts were not approved	16 Mar 2024, 12:42
110		Configuration Upload	Configuration Upload: Configuration Upload operation was performed by 10.1.31.15 on 10.1.31.6. Past alerts were not approved	16 Mar 2024, 12:42
96		Firmware Download	Firmware Download: Firmware Download operation was performed by 10.1.31.15 on 10.1.31.6. Past alerts were not approved	16 Mar 2024, 12:42
80		Monitor Debug	Monitor / Debug operation mode: Monitor / Debug operation mode operation was performed by 10.4.0.6 on 10.4.0.14. Past alerts were not approved	16 Mar 2024, 10:11





Se obtine apoi un raport → EXPORT, care se analizeaza



## CTD Alert Report

Produced by CTD on Thursday, Mar 28, 2024

### ModeChange

Mode Change: Mode Change operation was performed by 10.1.31.12 on 10.1.31.1. Past alerts were not approved

Alert Score: 100

Status: Resolved

#### Alert Details

##### 10.1.31.12

IP	MAC	Network
10.1.31.12	00:50:56:8D:DF:88	Default
Vendor	Asset Type	Host Name
VMware	Engineering Station	-
Name	Firmware version	Risk Level
10.1.31.12	-	Low
Site	Parsed Asset	Virtual Zone
CyberX	No	Engineering Station: 57

##### 10.1.31.1

IP	MAC	Network
10.1.31.1	28:63:36:26:F0:74	Default
Vendor	Asset Type	Host Name
Siemens	PLC	-
Name	Firmware version	Risk Level
10.1.31.1	-	Medium
Site	Parsed Asset	Virtual Zone
CyberX	No	PLC: 57

CyberX / Visibility / Assets / Chemical\_plant Admin

← OVERVIEW DEVICE INFORMATION RISKS & VULNERABILITIES THREAT DETECTION NETWORK ANALYTICS **COMMUNICATION** Export

POLICIES

Filter By: Reset Filters

Source Zone

Destination Zone

Protocols

Category

Access Type

Cloud Reputation

Switch to Query View

Advanced Filters

RESULTS (12)

ID	ACTION	SOURCE ZONE	DESTINATION ZONE	PROTOCOL	PORT	CATEGORY	ACCESS	EXACT MATCH	DESCRIPTION	HIT COUNT
88	Allow	Networking: Other (1)	PLC: Rockwell (2)	ICMP		Network	None	No		7
86	Allow	PLC: Rockwell (2)	Endpoint: Other (27)	TCP	44818	Other	None	No		1



CTD Asset Report

Produced by CTD on Thursday, Mar 28, 2024

Asset Details

Chemical_plant	Class	Asset Type	Purdue Level	Name
	OT	PLC	1	Chemical_plant
	IP	MAC	Network	VLAN
	10.1.30.1	00:1D:9C:C0:04:9D	Default	N/A
	Protocols	Site	Vendor	Model
	ARP, CIP, ENIP, ICMP, TCP	CyberX	Rockwell Automation	1756-ENBT/A
	Firmware version	Serial		
	V6.006	00987DBF		

Additional Details	Criticality	Risk Level	Virtual Zone	Parsed Asset
	High	High	PLC: Rockwell	No
	Custom Information	First Seen	Last Seen	
	Mode (Card 0): Remote Run Mode	14/03/2024 11:24:33 UTC	28/03/2024 08:24:42 UTC	

Nested Devices

## CTD Alert Report

Produced by CTD on Wednesday, May 04, 2022

CLAROTY

### ConfigurationUpload

**Configuration Upload:** Configuration Upload operation was performed for the first time by 10.1.31.6 on 10.1.31.15

Alert Score: 100

**Status: Resolved**

#### Alert Details

##### HVAC-System

IP	MAC	Network
10.1.31.6	28:63:36:88:F7:AE	Default
Vendor	Asset Type	Host Name
Siemens	PLC	-

##### 10.1.31.15

IP	MAC	Network
10.1.31.15	00:50:56:8D:27:66	Default
Vendor	Asset Type	Host Name
VMware	PLC	-