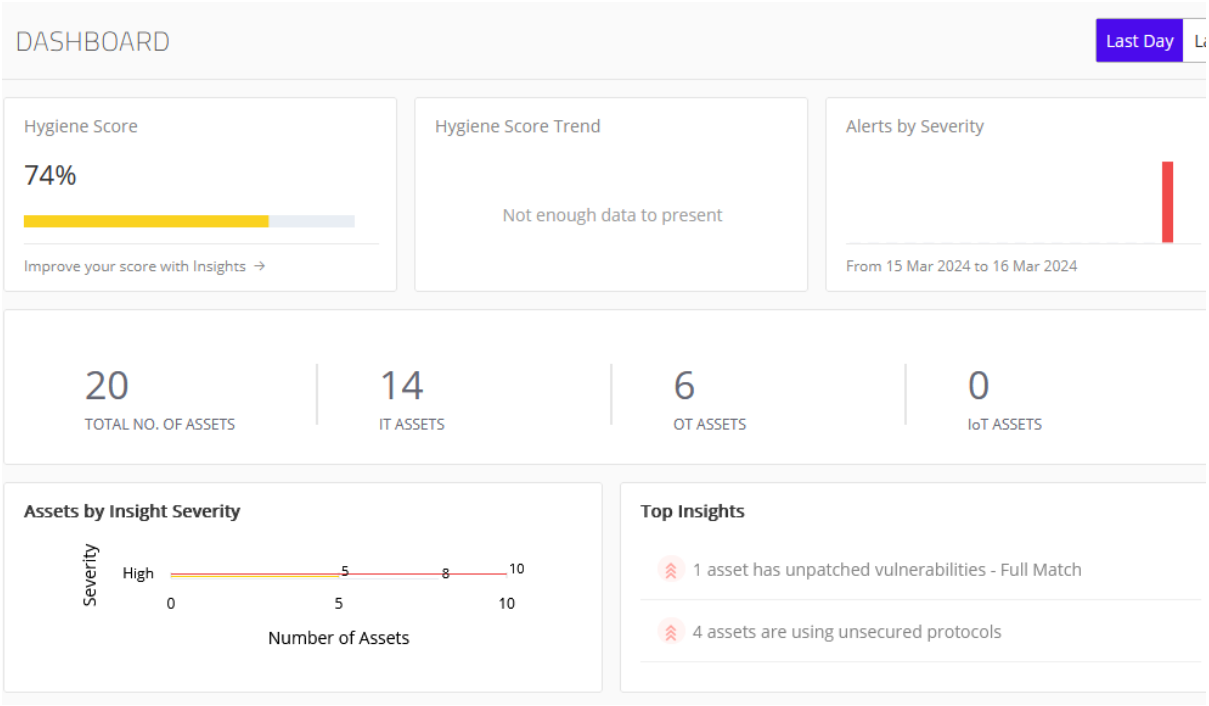
Aplicatia Claroty-IoT

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

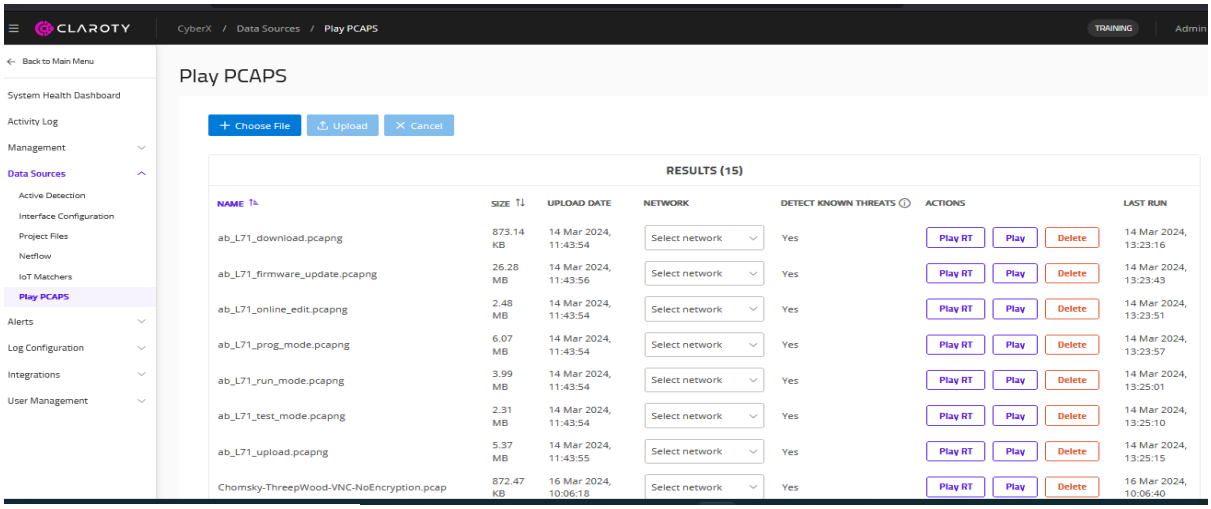
Acoperirea de neegalat a protocolului OT și tehnologia de scanare activă, pasivă și AppDB permit platformei Claroty să ofere vizibilitate deplină asupra tuturor celor trei variabile, care sunt integrante pentru evaluarea și reducerea eficientă a riscurilor în mediile OT. Acestea includ 1) Vizibilitatea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

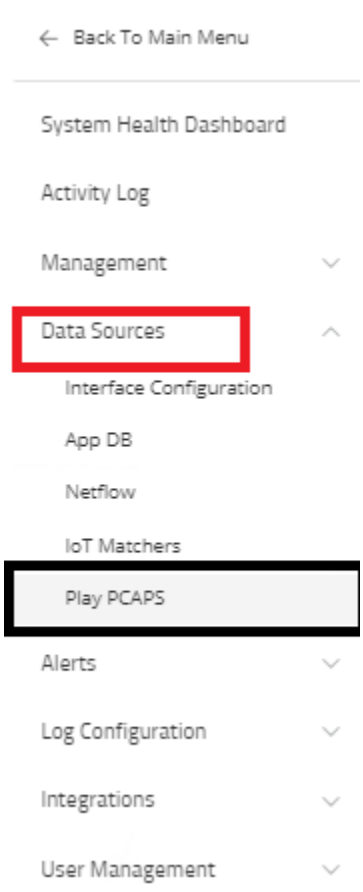
Detectarea amenințărilor

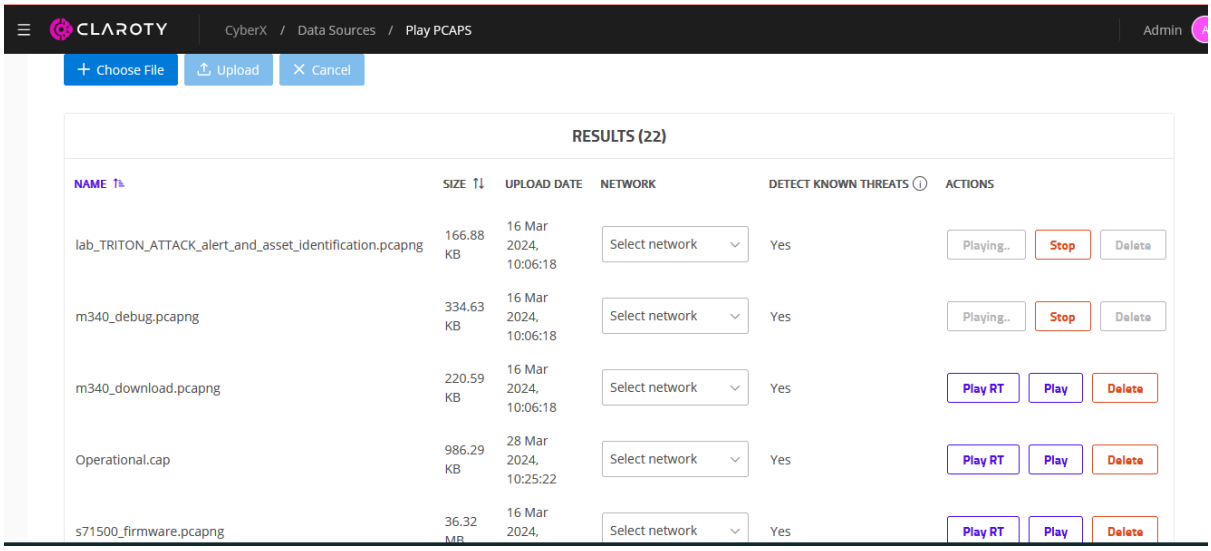
Platforma Claroty utilizează cinci motoare de detectare pentru a profila automat toate activele, comunicațiile și procesele din mediile OT, pentru a stabili o linie de bază comportamentală care caracterizează traficul legitim și pentru a elimina falsele pozitive și pentru a oferi o acoperire cuprinzătoare 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

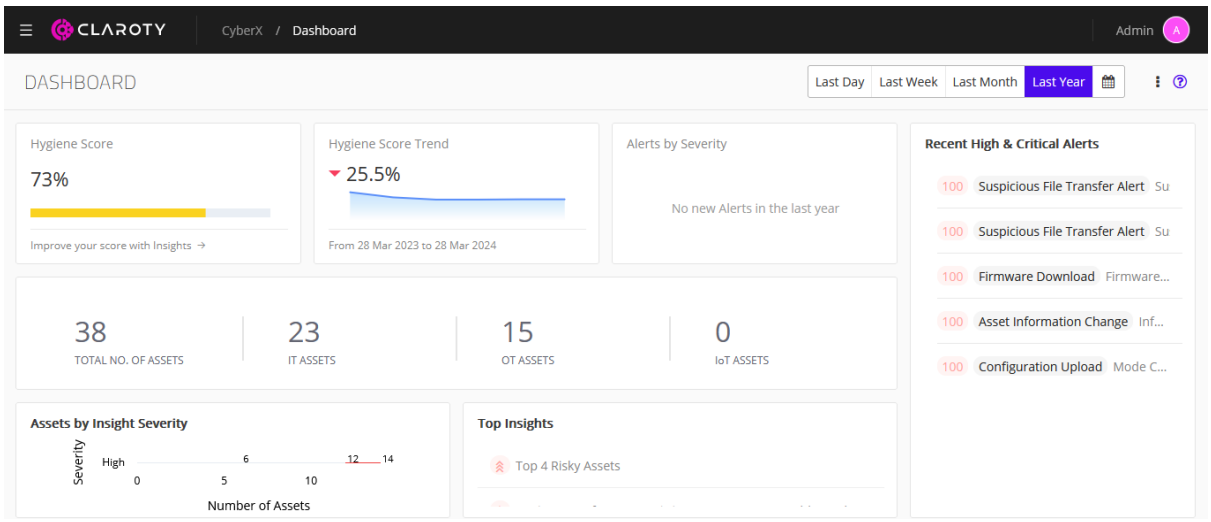

CLAROTY
CyberX / Data Sources / Play PCAPS
TRAINING
Admin
Back to Main Menu
System Health Dashboard
Activity Log
Management
Data Sources
Active Detection
Interface Configuration
Project Files
Netflow
IoT Matchers
Play PCAPS
Alerts
Log Configuration
Integrations
User Management
Play PCAPS
Choose File
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 Play RT Play Delete 14 Mar 2024, 13:23:16
ab_L71_firmware_update.pcapng 26.28 MB 14 Mar 2024, 11:43:56 Select network Yes Play RT Play Delete 14 Mar 2024, 13:23:43
ab_L71_online_edit.pcapng 2.48 MB 14 Mar 2024, 11:43:54 Select network Yes Play RT Play Delete 14 Mar 2024, 13:23:51
ab_L71_prog_mode.pcapng 6.07 MB 14 Mar 2024, 11:43:54 Select network Yes Play RT Play Delete 14 Mar 2024, 13:23:57
ab_L71_run_mode.pcapng 3.99 MB 14 Mar 2024, 11:43:54 Select network Yes Play RT Play Delete 14 Mar 2024, 13:25:01
ab_L71_test_mode.pcapng 2.31 MB 14 Mar 2024, 11:43:54 Select network Yes Play RT Play Delete 14 Mar 2024, 13:25:10
ab_L71_upload.pcapng 5.37 MB 14 Mar 2024, 11:43:55 Select network Yes Play RT Play Delete 14 Mar 2024, 13:25:15
Chomsky-ThreepWood-VNC-NoEncryption.pcap 872.47 KB 16 Mar 2024, 10:06:18 Select network Yes Play RT Play Delete 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

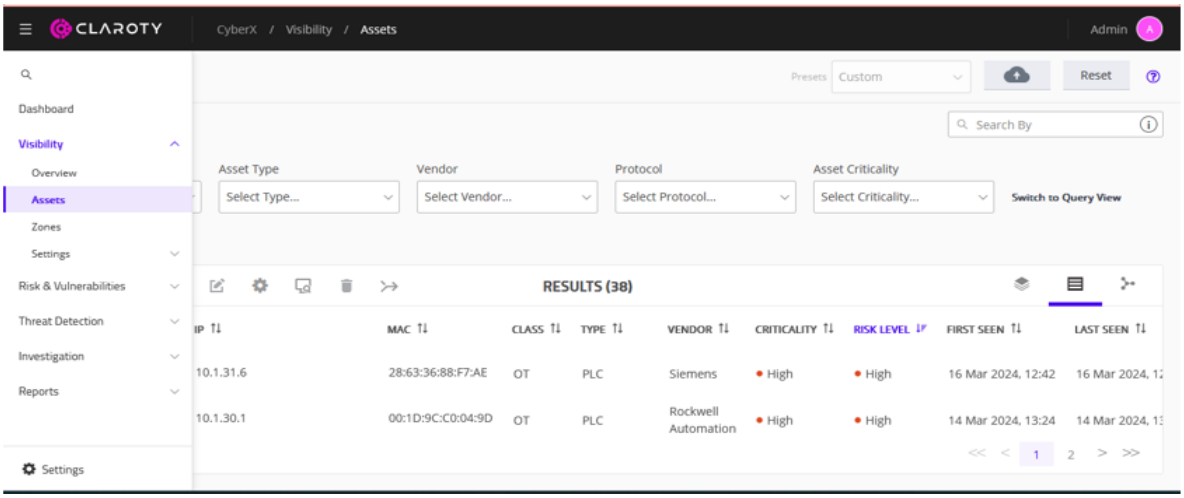


Scenariu STUDENT

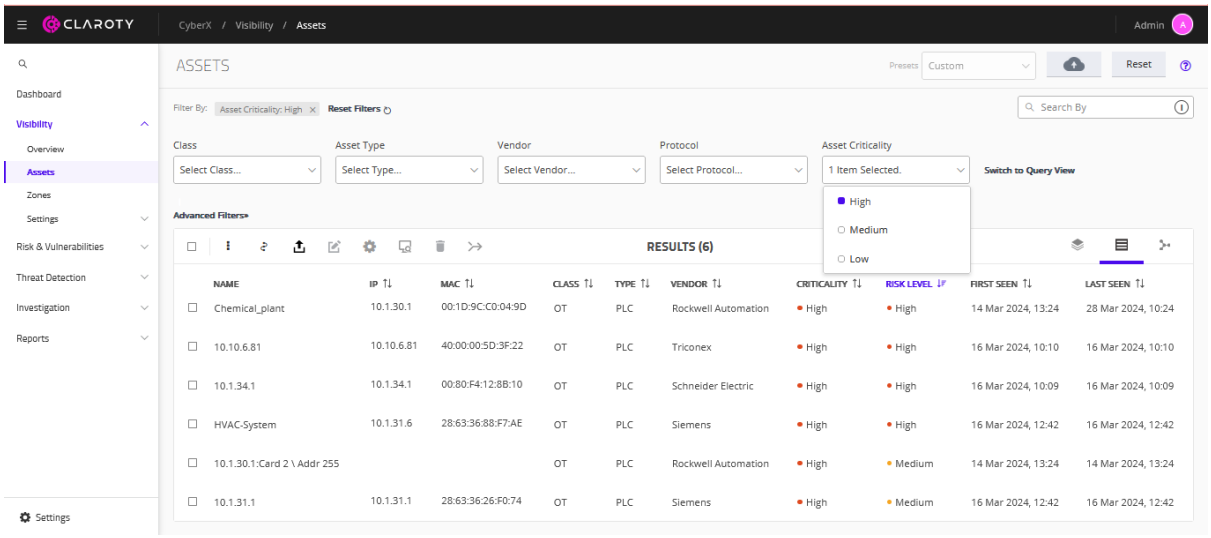
Analiza interfata principala → Dashboard



Visibility – Asset→ pentru analiza traffic



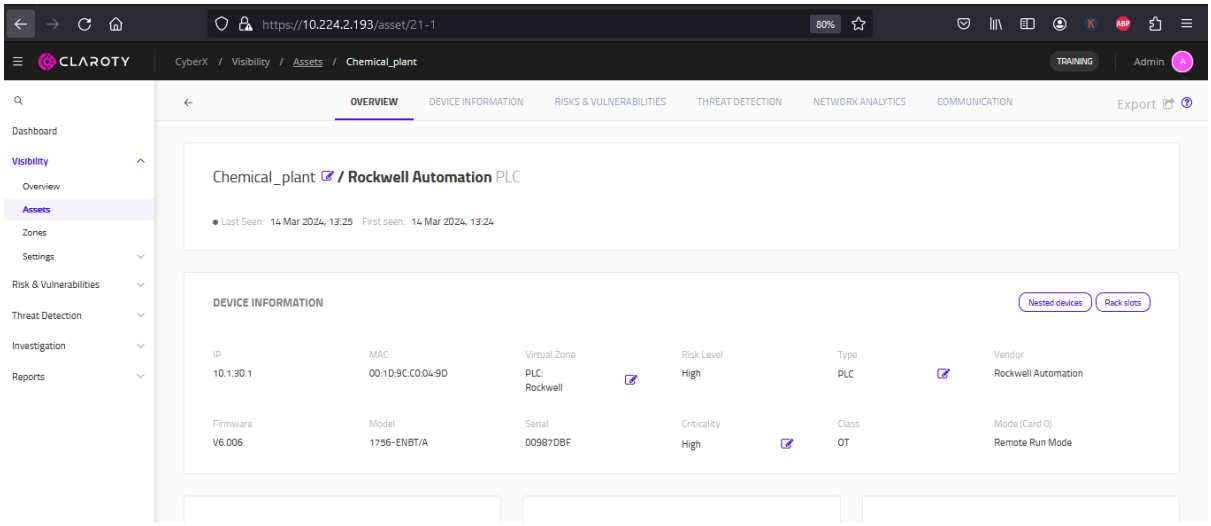
Se identifica Asset-urile critice

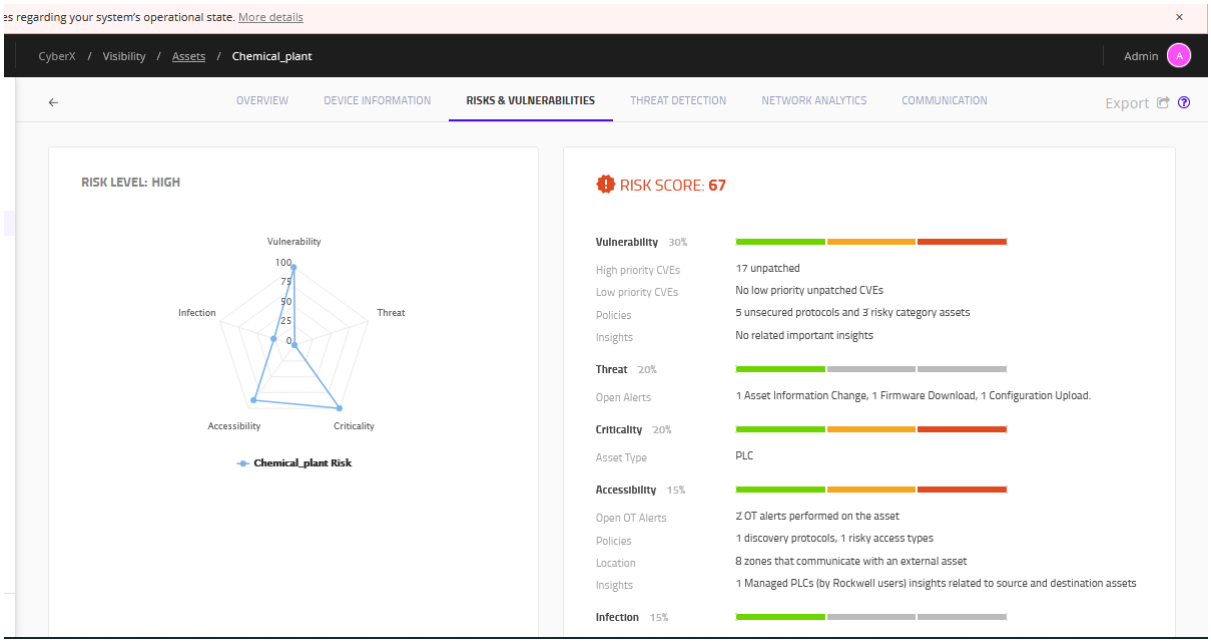


Se alege un asset critic exemplu→ Chemical_plant → si se analizeaza

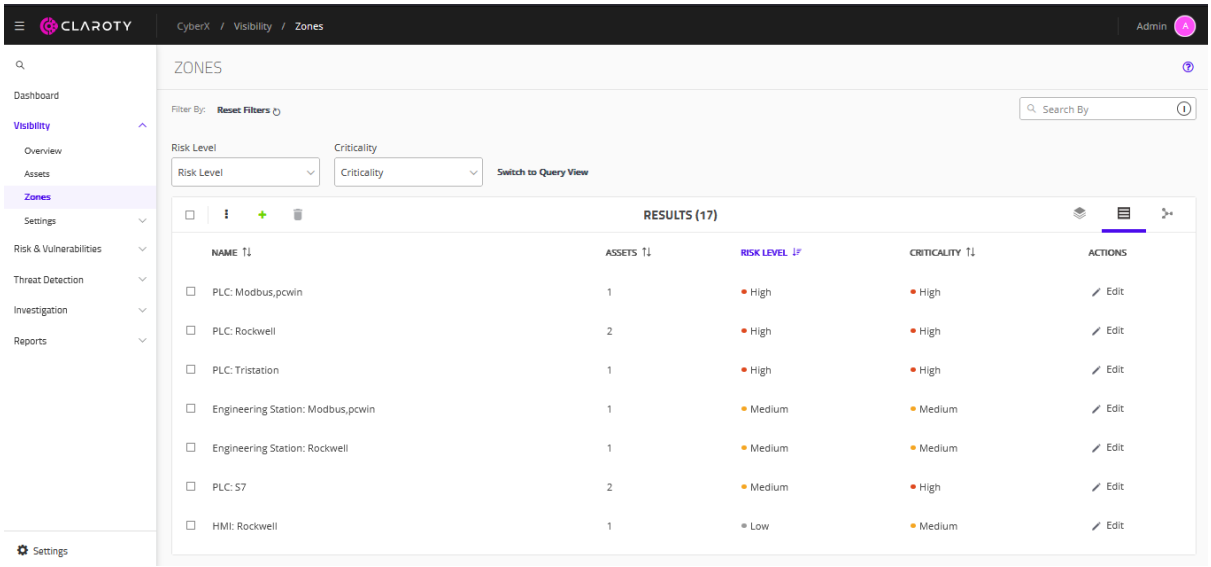
Chemical_plant

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

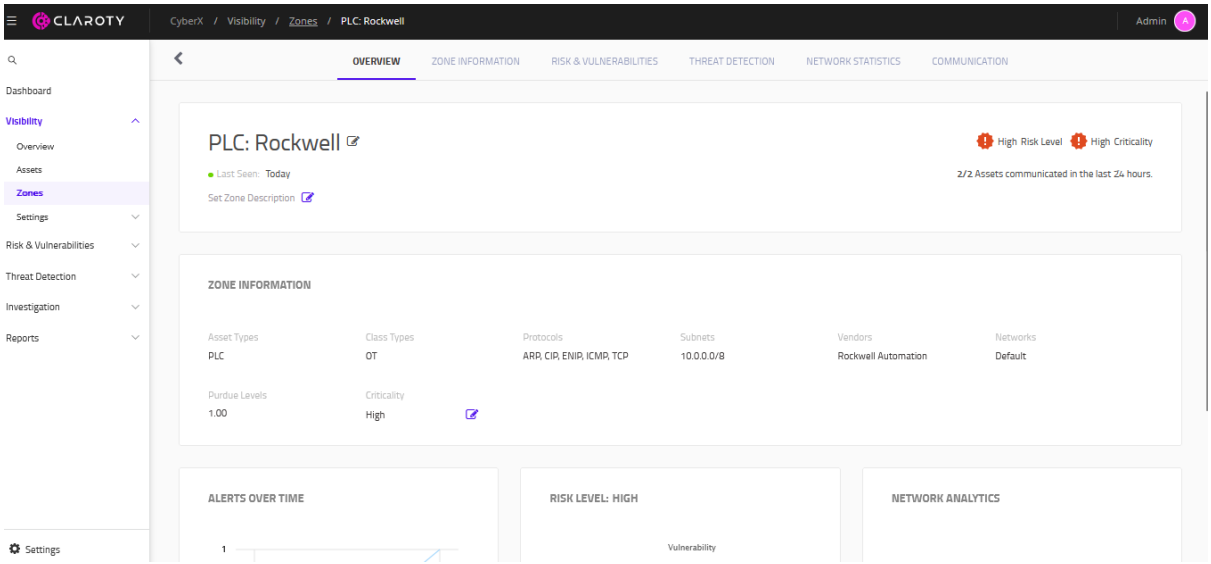


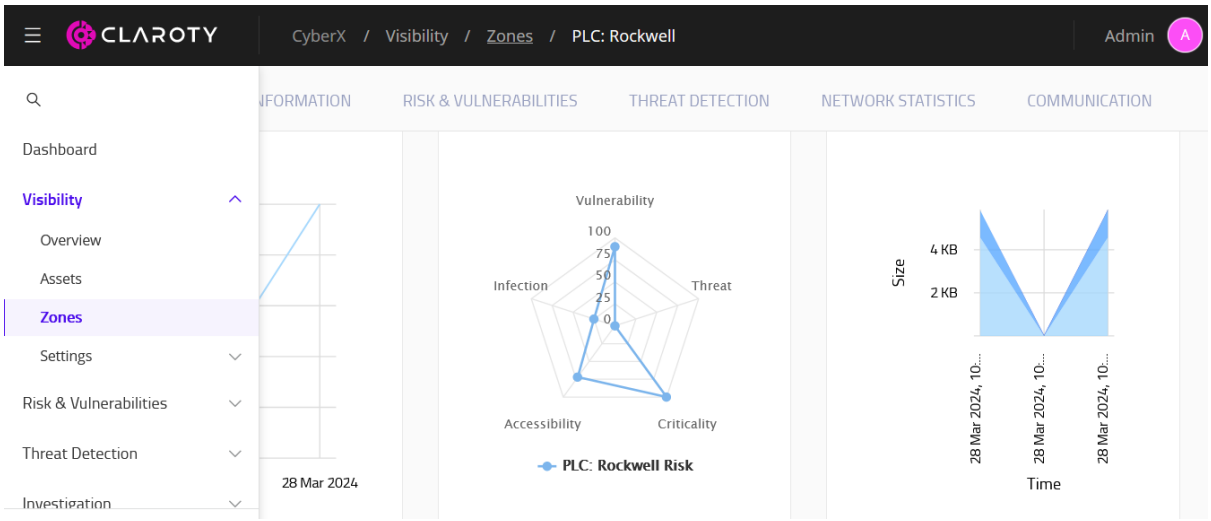


Se analizeaza sectiunea Zones

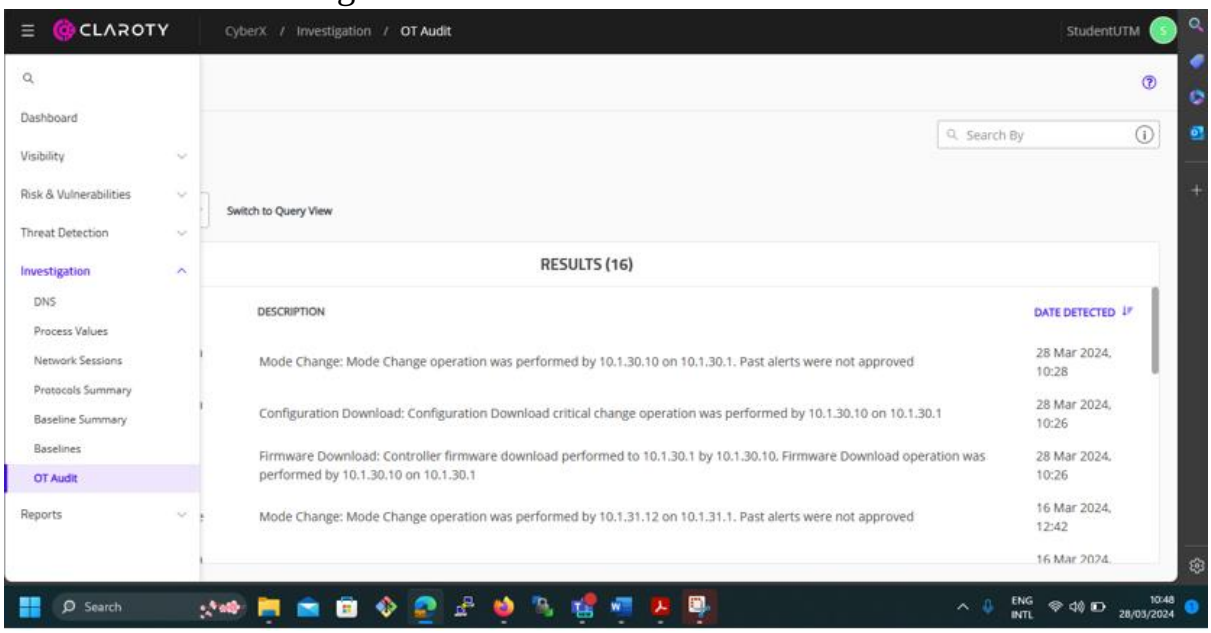


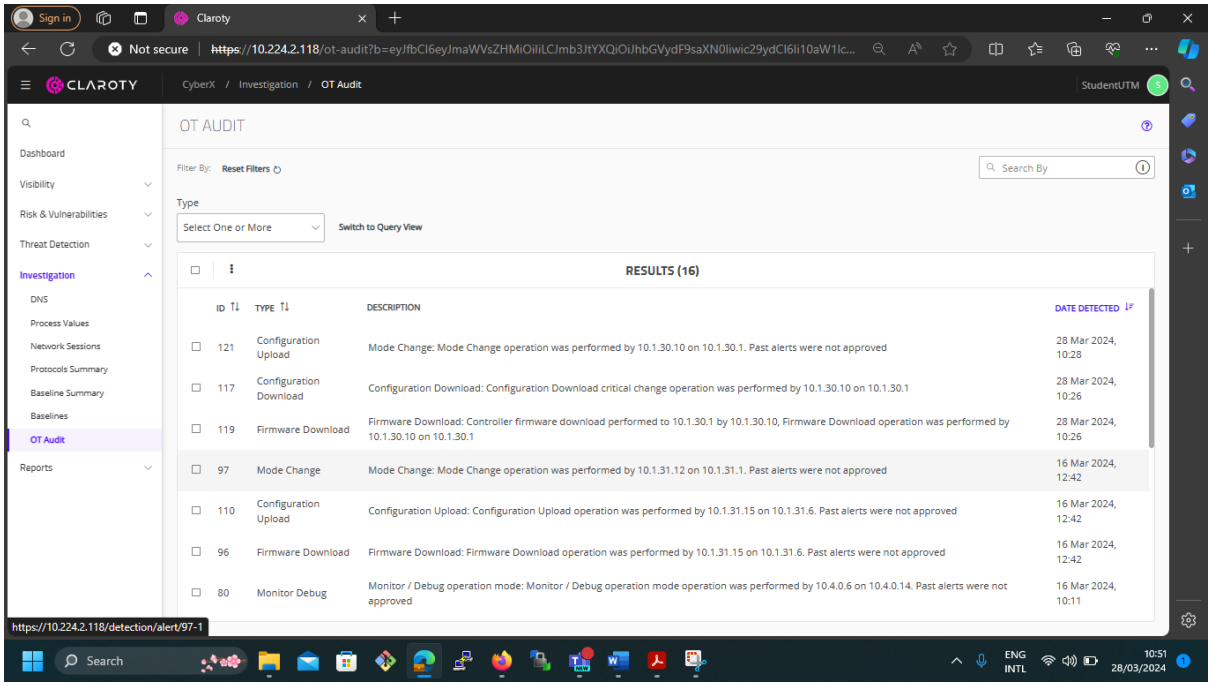
Din sectiunea Zones, se alege o zona critica care se analizeaza

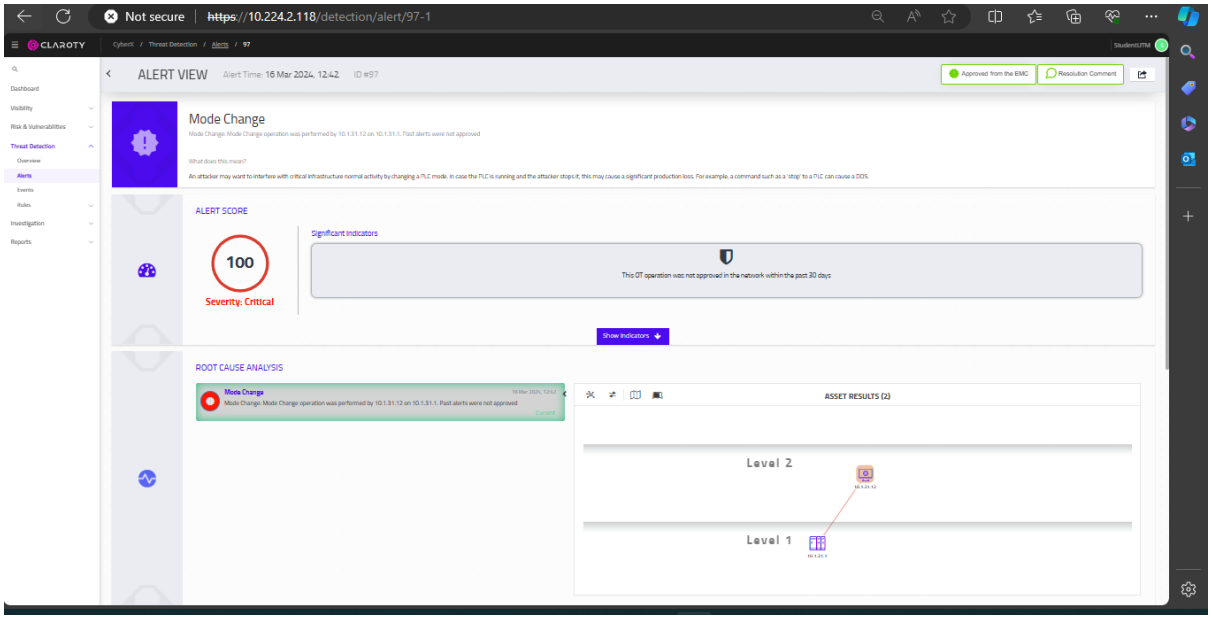

CLAROTY
CyberX / Visibility / Zones / PLC: Rockwell
Admin
Dashboard
Visibility
Overview
Assets
Zones
Settings
Risk & Vulnerabilities
Threat Detection
Investigation
Reports
OVERVIEW
ZONE INFORMATION
RISK & VULNERABILITIES
THREAT DETECTION
NETWORK STATISTICS
COMMUNICATION
PLC: Rockwell
Last Seen: Today
Set Zone Description
High Risk Level
High Criticality
2/2 Assets communicated in the last 24 hours.
ZONE INFORMATION
Asset Types
PLC
Class Types
OT
Protocols
ARP, CIP, ENIP, ICMP, TCP
Subnets
10.0.0.0/8
Vendors
Rockwell Automation
Networks
Default
Purdue Levels
1.00
Criticality
High
ALERTS OVER TIME
RISK LEVEL: HIGH
NETWORK ANALYTICS
Settings

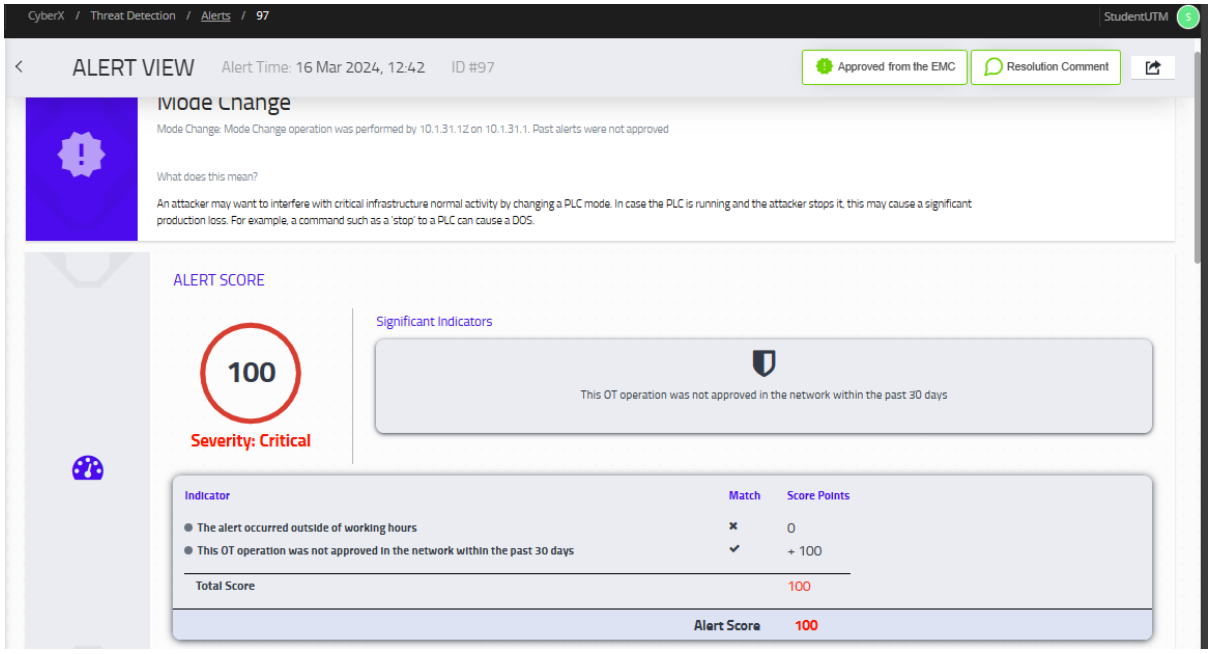

CLAROTY
CyberX / Visibility / Zones / PLC: Rockwell
Admin
Dashboard
Visibility
Overview
Assets
Zones
Settings
Risk & Vulnerabilities
Threat Detection
Investigation
NFORMATION
RISK & VULNERABILITIES
THREAT DETECTION
NETWORK STATISTICS
COMMUNICATION
28 Mar 2024
Vulnerability
100
75
50
25
0
Infection
Threat
Accessibility
Criticality
PLC: Rockwell Risk
Size
4 KB
2 KB
28 Mar 2024, 10:...
28 Mar 2024, 10:...
28 Mar 2024, 10:...
Time

Se realizeaza o investigatie → OT Audit









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

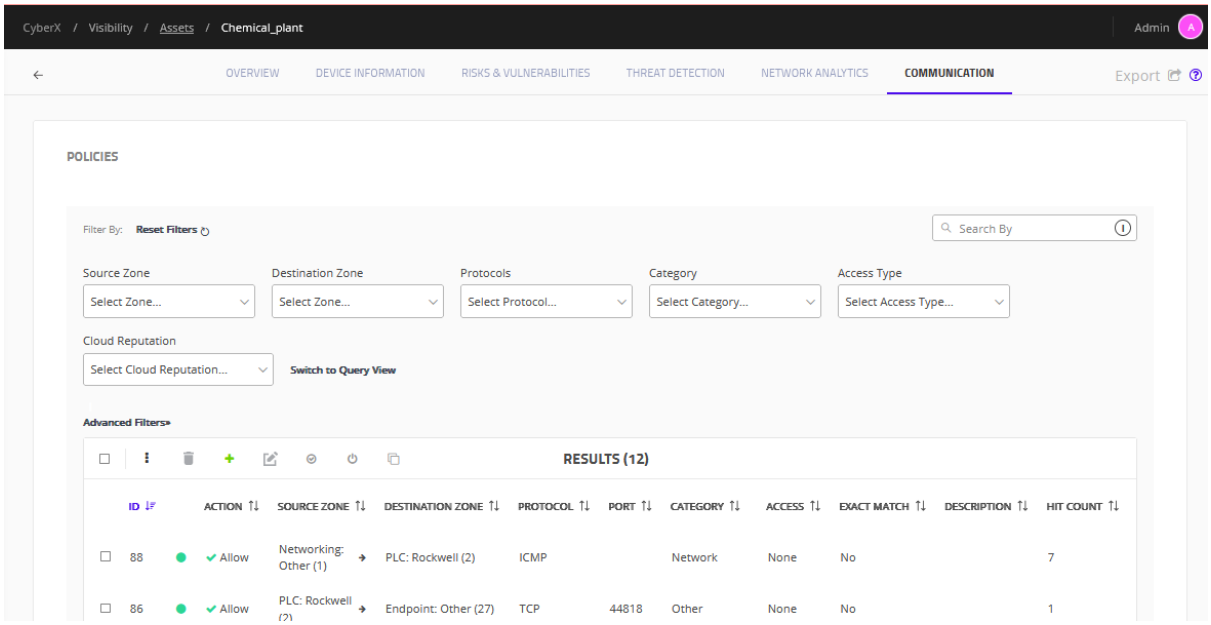
Alert Details

10.1.31.12

IP	MAC	Network
10.1.31.12	00:50:56:8D:DF:B8	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: S7

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: S7



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


1 / 2
100%
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
-