Enabling Cyber Resilience

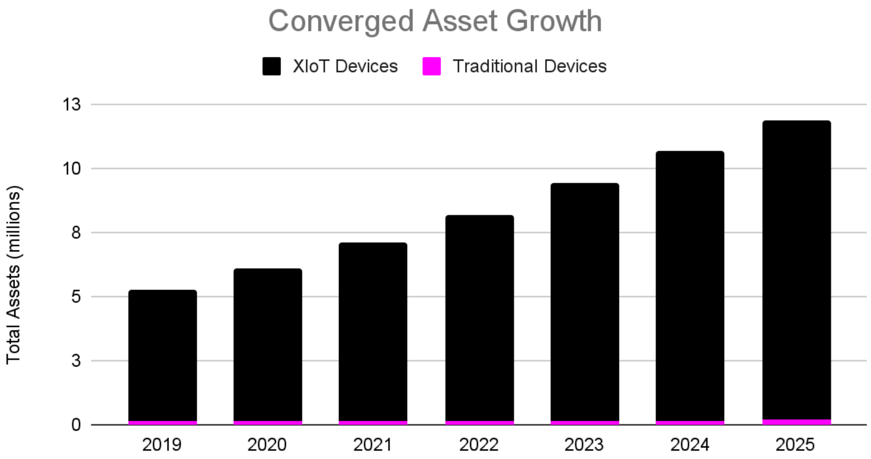
Introducing Claroty CTD

Julian Fleper

24.10.2023

The Growth of the XIoT

The rapid proliferation of cyber-physical systems that cannot easily be secured



Sources:
Gartner, Forecast: PCs, Worldwide, 2019-2025, 1Q21 Update
Gartner, Forecast: Servers, All Countries, 2019-2025, 1Q21 Update
Gartner, Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2019-2029

Top Challenges

Rapid device expansion increases exposure

Diversity of devices leads to decreased visibility

Increased frequency and severity of attacks

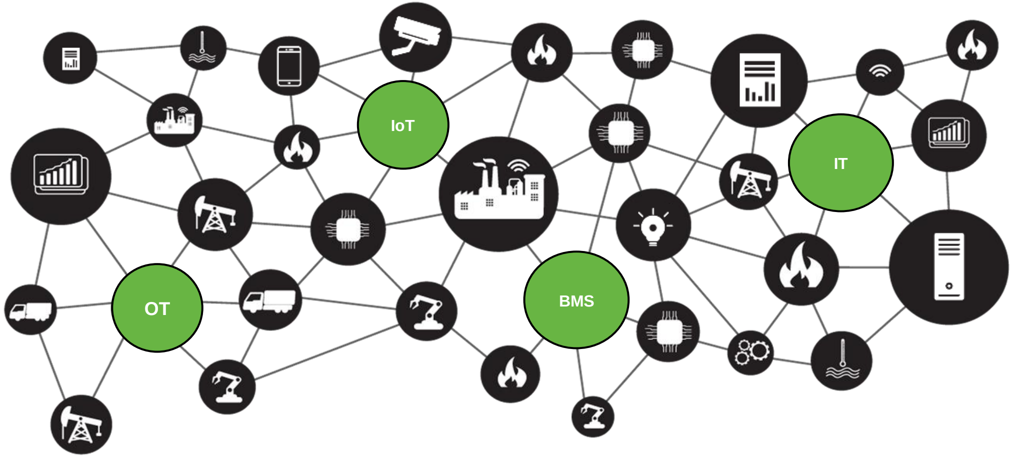
Increased skills gap between IT and OT staff

The Modern Industrial Network

The interconnectivity that drives productivity

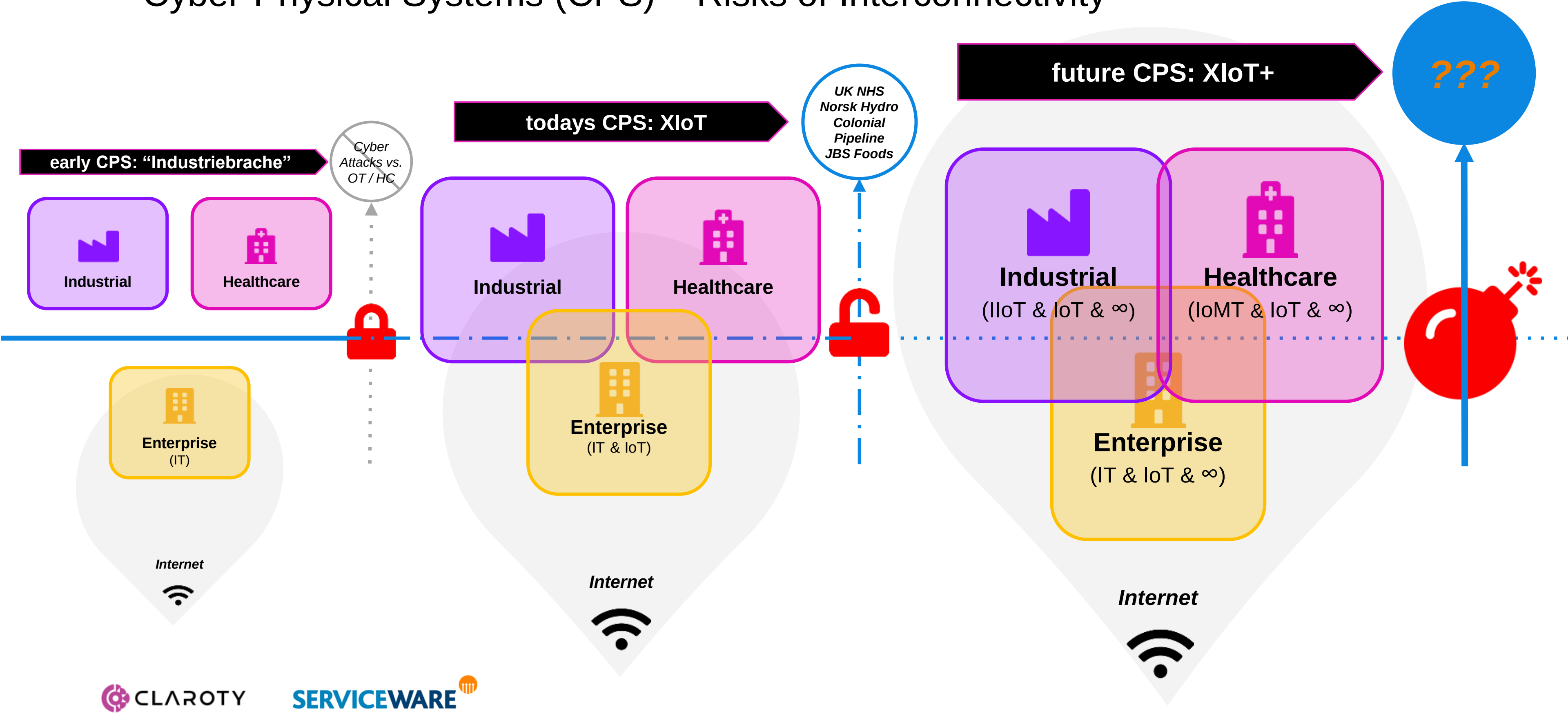
The Extended Internet of Things (XIoT)

The ever-growing web of connected devices that span and support cyber-physical systems and range from both legacy and greenfield OT assets, to IT and IoT devices, to building management system equipment.



Past, Present and Future

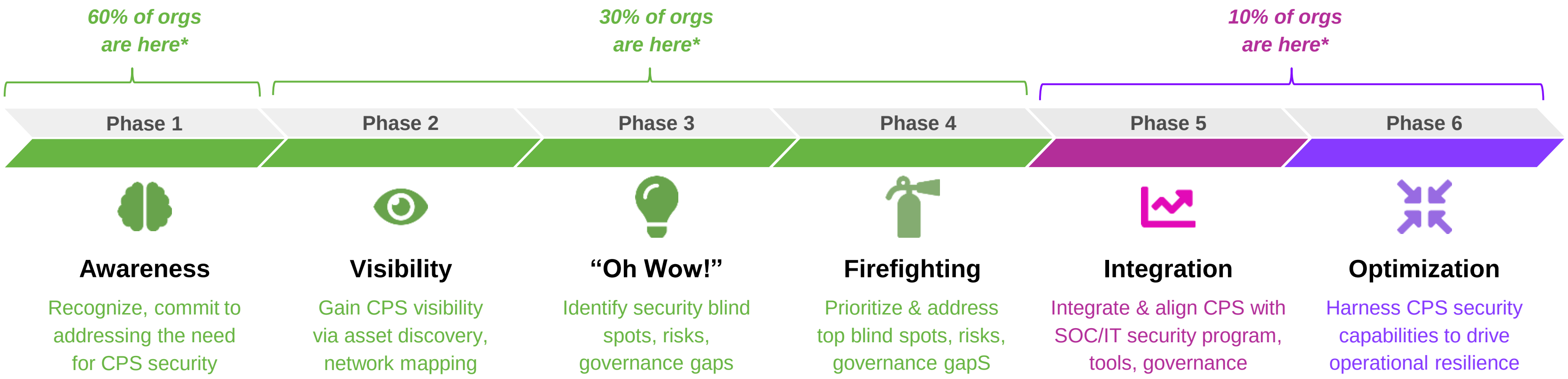
- Cyber-Physical Systems (CPS) – Risks of Interconnectivity



CLAROTY SERVICEWARE

The Journey To Achieving Business Outcomes

The CPS Security Journey: As Told by Gartner[1]



*60% of orgs are here**

*30% of orgs are here**

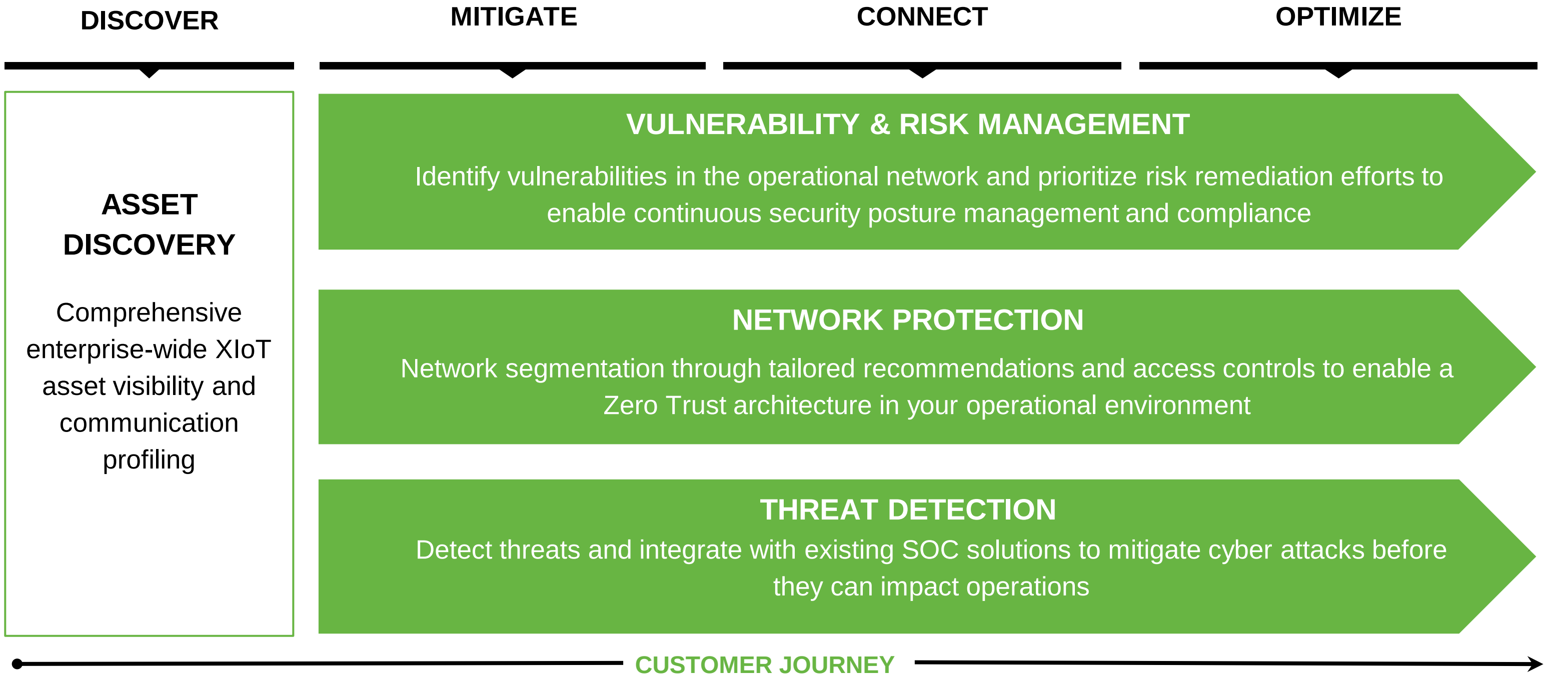
*10% of orgs are here**

Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6
Awareness	**Visibility**	**“Oh Wow!”**	**Firefighting**	**Integration**	**Optimization**
Recognize, commit to addressing the need for CPS security	Gain CPS visibility via asset discovery, network mapping	Identify security blind spots, risks, governance gaps	Prioritize & address top blind spots, risks, governance gapS	Integrate & align CPS with SOC/IT security program, tools, governance	Harness CPS security capabilities to drive operational resilience

[1] Source: Market Guide for Operational Technology Security, Gartner, 2021

The Journey to Achieving Cyber Resilience

Our approach tailored to your priorities



DISCOVER

MITIGATE

CONNECT

OPTIMIZE

ASSET DISCOVERY

Comprehensive enterprise-wide XIoT asset visibility and communication profiling

VULNERABILITY & RISK MANAGEMENT

Identify vulnerabilities in the operational network and prioritize risk remediation efforts to enable continuous security posture management and compliance

NETWORK PROTECTION

Network segmentation through tailored recommendations and access controls to enable a Zero Trust architecture in your operational environment

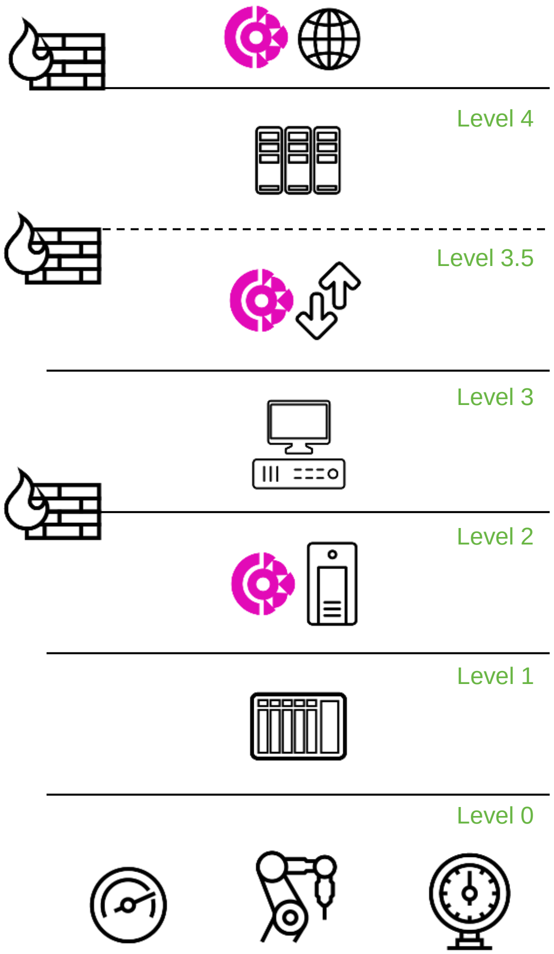
THREAT DETECTION

Detect threats and integrate with existing SOC solutions to mitigate cyber attacks before they can impact operations

CUSTOMER JOURNEY

Introducing Claroty Continuous Threat Detection (CTD)

XIoT Cyber Resilience Solution for your Industrial Cybersecurity Journey



CLAROTY SERVICEWARE

Risk & Vulnerability Management

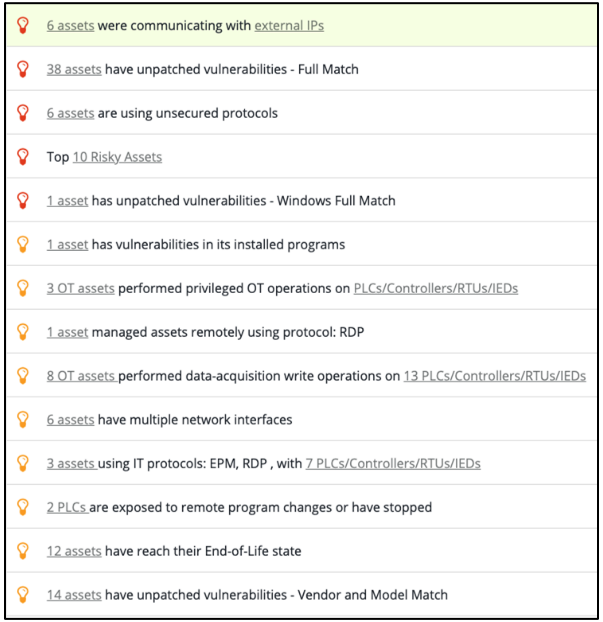
Identify and Understand Your Risk Ecosystem

Team82 powered vulnerability research **reveals risk** across the industrial environment

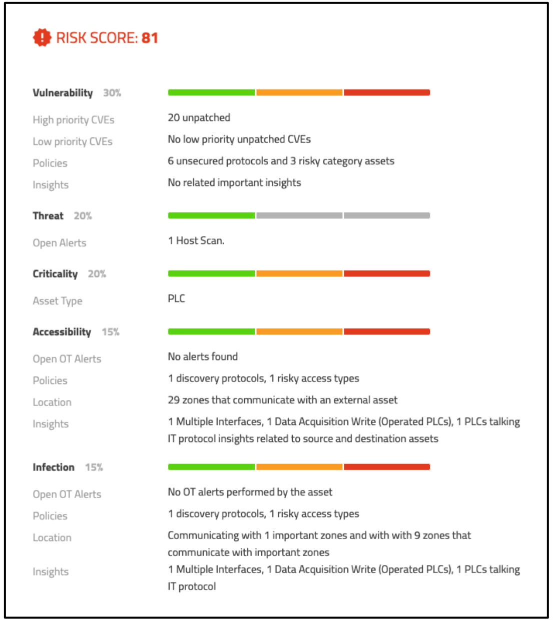
Full-match vulnerabilities and risk insights provide an **accurate assessment of risk**

Multi-factor risk score **prioritizes remediation** of assets most likely to be exploited

Holistic view of network posture with tiered risk scoring across asset, segment, and site



- 6 assets were communicating with external IPs
- 38 assets have unpatched vulnerabilities - Full Match
- 6 assets are using unsecured protocols
- Top 10 Risky Assets
- 1 asset has unpatched vulnerabilities - Windows Full Match
- 1 asset has vulnerabilities in its installed programs
- 3 OT assets performed privileged OT operations on PLCs/Controllers/RTUs/IEDs
- 1 asset managed assets remotely using protocol: RDP
- 8 OT assets performed data-acquisition write operations on 13 PLCs/Controllers/RTUs/IEDs
- 6 assets have multiple network interfaces
- 3 assets using IT protocols: EPM, RDP , with 7 PLCs/Controllers/RTUs/IEDs
- 2 PLCs are exposed to remote program changes or have stopped
- 12 assets have reach their End-of-Life state
- 14 assets have unpatched vulnerabilities - Vendor and Model Match



RISK SCORE: **81**

Vulnerability 30%	🟩🟧🟥
High priority CVEs	20 unpatched
Low priority CVEs	No low priority unpatched CVEs
Policies	6 unsecured protocols and 3 risky category assets
Insights	No related important insights
Threat 20%	🟩⬜⬜
Open Alerts	1 Host Scan.
Criticality 20%	🟩🟧🟥
Asset Type	PLC
Accessibility 15%	🟩🟧🟥
Open OT Alerts	No alerts found
Policies	1 discovery protocols, 1 risky access types
Location	29 zones that communicate with an external asset
Insights	1 Multiple Interfaces, 1 Data Acquisition Write (Operated PLCs), 1 PLCs talking IT protocol insights related to source and destination assets
Infection 15%	🟩🟧🟥
Open OT Alerts	No OT alerts performed by the asset
Policies	1 discovery protocols, 1 risky access types
Location	Communicating with 1 important zones and with with 9 zones that communicate with important zones
Insights	1 Multiple Interfaces, 1 Data Acquisition Write (Operated PLCs), 1 PLCs talking IT protocol

Threat Detection

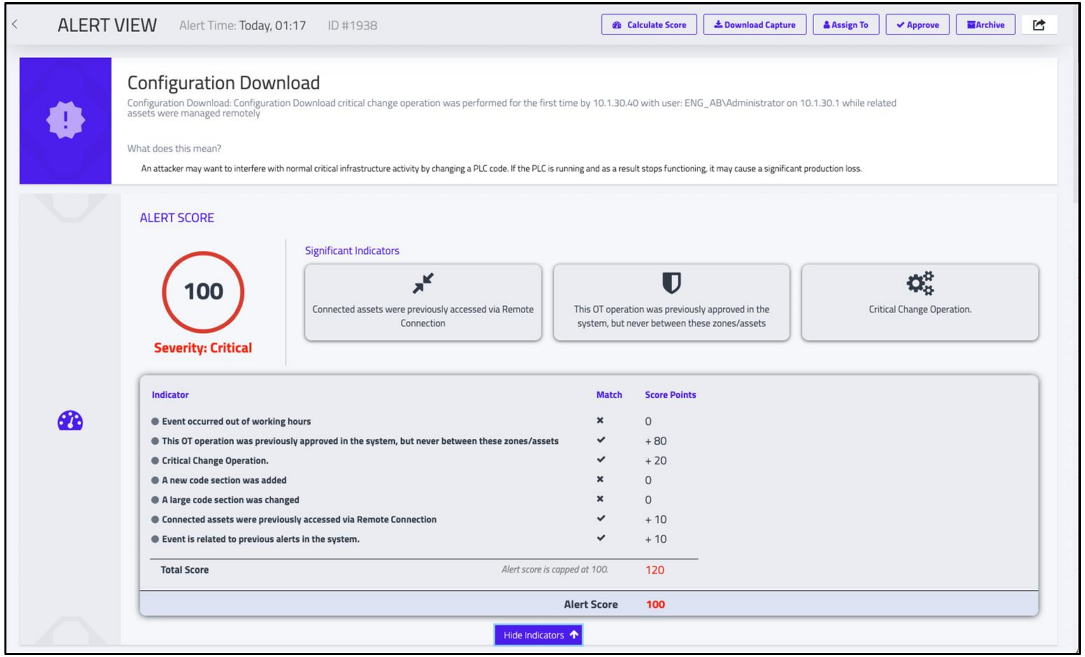
Detect Both Known and Zero Day Threats

Swiftly detect known threats **before they can impact operations**

Detect unknown threats resulting from potentially malicious network policy violations

Ensure process integrity by alerting on operational behaviors like config changes

Connect existing SOC capabilities to the industrial environment



Configuration Download

Configuration Download: Configuration Download critical change operation was performed for the first time by 10.1.30.40 with user: ENG_AB\Administrator on 10.1.30.1 while related assets were managed remotely

What does this mean?

An attacker may want to interfere with normal critical infrastructure activity by changing a PLC code. If the PLC is running and as a result stops functioning, it may cause a significant production loss.

100

Severity: Critical

Connected assets were previously accessed via Remote Connection

This OT operation was previously approved in the system, but never between these zones/assets

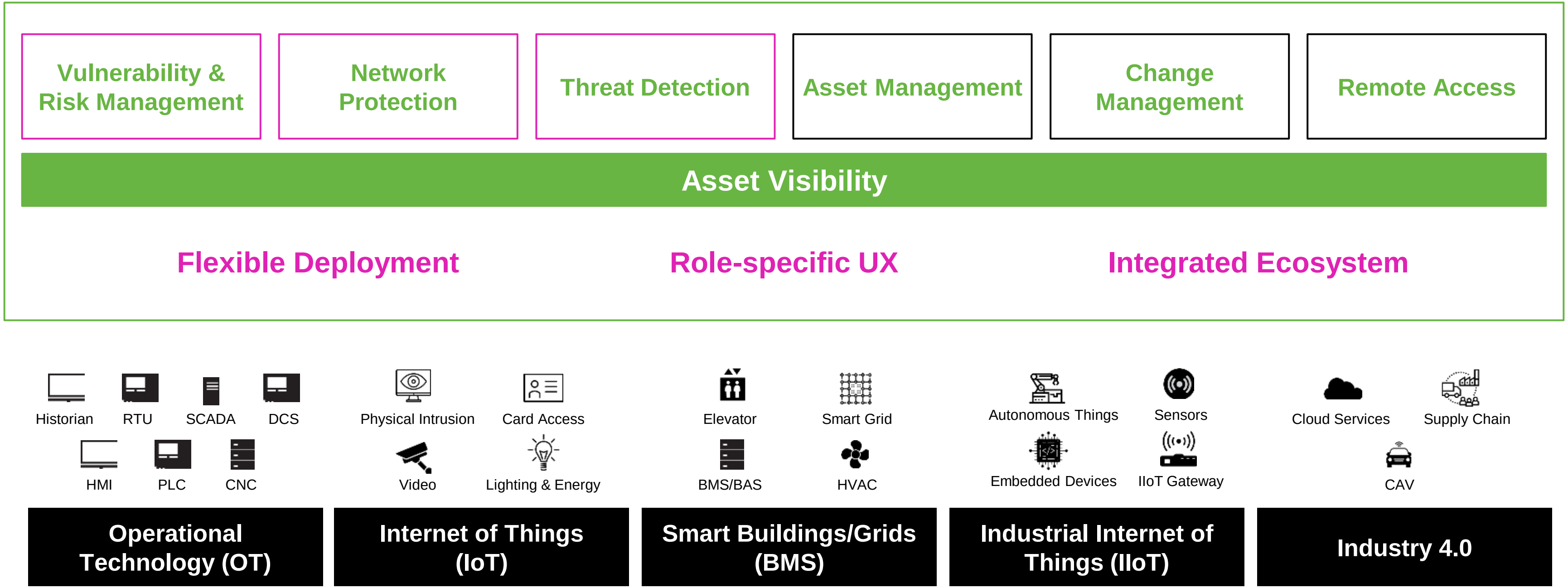
Critical Change Operation.

Indicator	Match	Score Points
Event occurred out of working hours	✗	0
This OT operation was previously approved in the system, but never between these zones/assets	✓	+ 80
Critical Change Operation.	✓	+ 20
A new code section was added	✗	0
A large code section was changed	✗	0
Connected assets were previously accessed via Remote Connection	✓	+ 10
Event is related to previous alerts in the system.	✓	+ 10
Total Score	*Alert score is capped at 100.*	120
	Alert Score	100

CLAROTY SERVICEWARE

Claroty CTD

The comprehensive industrial cybersecurity solution for your cyber resilience journey



Vulnerability & Risk Management

Network Protection

Threat Detection

Asset Management

Change Management

Remote Access

Asset Visibility

Flexible Deployment

Role-specific UX

Integrated Ecosystem

Historian, RTU, SCADA, DCS, HMI, PLC, CNC

Operational Technology (OT)

Physical Intrusion, Card Access, Video, Lighting & Energy

Internet of Things (IoT)

Elevator, Smart Grid, BMS/BAS, HVAC

Smart Buildings/Grids (BMS)

Autonomous Things, Sensors, Embedded Devices, IIoT Gateway

Industrial Internet of Things (IIoT)

Cloud Services, Supply Chain, CAV

Industry 4.0

CLAROTY INDUSTRIAL

Thank You

CLAROTY SERVICEWARE