CLAROTY

Cyber Security For Data Centers' Operational Technology (OT) Networks

Data Center's OT Networks - A Cyber Security Blind Spot In Your Enterprise

Data centers reliable operation is enabled by OT Networks that govern HVAC, electricity and fire alarm systems. These critical networks are typically excluded from the cyber security solutions and policies that safeguard an enterprise's IT networks and endpoints, thereby forming a blind spot in an enterprise's cyber security posture.

"Our trading operations are for all intents dependent on industrial control systems,"

- CISO of major US stock exchange

The Threat

Threat actors attempt to gain a foothold on OT networks components to compromise either:

- **Enterprise Data -** In this case, following an attack, the next step would be to search for unmonitored connectivity between the OT and IT networks and laterally move towards the targeted data.
- **Enterprise Operations -** In this case, following an attack, the next step would be to change the settings or disable the PLCs that govern vital systems such as electricity or HVAC. Once compromised, these systems can cause physical damage to the data center critically disrupting an enterprise's operations.

"FBI: Hackers Breached New Jersey Industrial HVAC System"
"Hackers Penetrate Google's Building Management System"

Claroty: See. Know. Secure.

Claroty is a cyber security platform, purpose-built for protecting OT networks from advanced threat actors. Claroty continuously monitors the network and alerts **critical and anomalous behavior,** enabling immediate response to malicious presence and activity.

Claroty passively connects to the OT network SPAN ports and employs a unique Deep Packet Inspection (DPI) technology that parses all the network traffic, providing the enterprise security personnel with **extreme visibility** into the OT network's internals. This extreme visibility applies to both the **serial** (LON, BACnet, Modbus, and others) and **Ethernet** portions of the data center OT networks, covering all the commonly used communication protocols.

Cyber-Security For Data Centers' Operational Technology (OT) Networks

Claroty Security Lifecycle

Proactive Protection

Claroty's monitoring covers the OT network from remote I\Os, fieldbus devices and PLC DLRs, to OT\IT and OT\Internet interfaces. Claroty's DPI technology delivers full network topology, unveiling hidden attack surfaces such as unattained IT\OT intersections and unmonitored third party access points. Claroty, enables OT network operators to maintain secure architecture and access policies to its network.

Incident Response

Cyber attacks on OT networks typically leverages legitimate operational commands rather than malware. A single PLC typically governs numerous OT processes. Claroty's real-time alerts enable the operator to immediately associate the alert with the affected process and apply the required resolving procedures.

Forensic Investigation

Following immediate remediation steps, Claroty provides full context of the attempted malicious activities enabling the security and control room staff to identify the attack's root causes and impacts, including a detailed timeline of the pre-alert events and reproduction of loaded code.

Benefits

- **Know** and track exactly how assets across your OT network are configured, communicating and changing
- **Discover** hidden and potentially problematic issues across all layers of your OT network
- Proactively fix problems to **reduce risk, maintain process integrity and enhance resiliency**
- **Rapidly detect and respond to malicious activities or other activity that could harm operational processes**

About Us

Claroty was conceived to secure the safety and reliability of OT networks that run the world's most critical infrastructures.

Claroty empowers the people who run and protect industrial systems to make the most of their OT networks.

By discovering the most granular elements, extracting the critical data, and formulating actionable insights, Claroty provides extreme visibility and brings unparalleled clarity to OT networks.