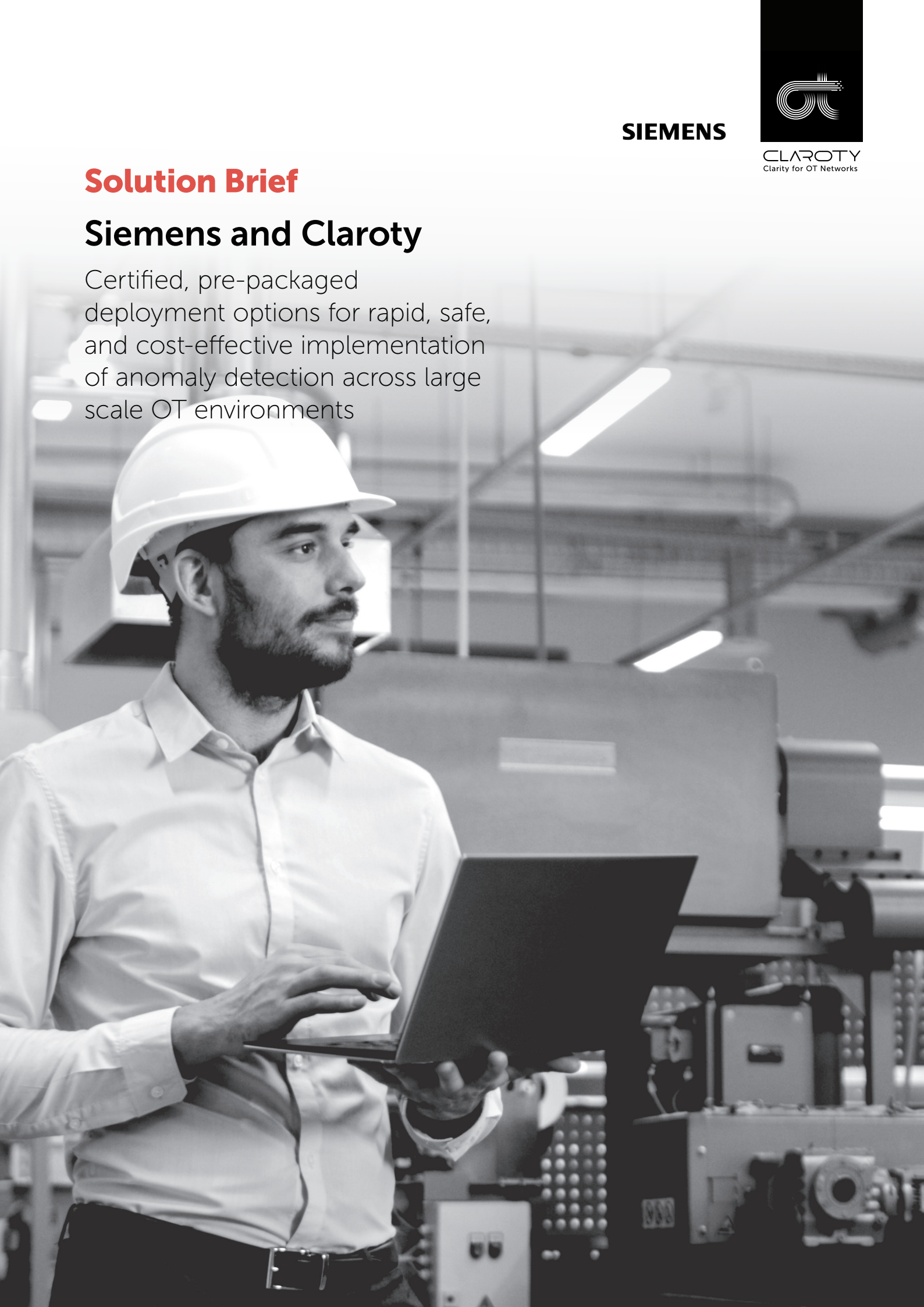
SIEMENS

CLAROTY
Clarity for OT Networks

Solution Brief

Siemens and Claroty

Certified, pre-packaged deployment options for rapid, safe, and cost-effective implementation of anomaly detection across large scale OT environments



Siemens and Claroty – Certified, rapid, cost-effective implementation across large scale OT environments

Solution Highlights

- **Extreme Visibility** of industrial control system networks allows critical infrastructure organizations to assess, monitor and mitigate potential threats more quickly.
- **Improved Threat Hunting** via real-time contextual alerting and immediate implications on process integrity and cyber resiliency.
- **Zero Impact on Industrial Control Networks** operating in a non-intrusive manner, does not require the installation of endpoint agents, and creates no downtime or disruption to industrial networks.

Business Drivers

While many enterprises have made great strides in protecting their IT business networks, industrial control system (ICS) networks remain at risk. Commissioned decades ago, without cybersecurity in mind and sometimes running outdated software, many of these networks and underlying assets are being increasingly targeted with sophisticated cyberattacks or are connected to IT networks and at risk of a "spill-over" effect from broader attacks. In fact, a number of documented attacks such as Industroyer CrashOverride, WannaCry, NotPetya BlackEnergy and STUXNET have created significant operational damage, disrupting production and putting environmental and personal safety at risk.

Until now, gaining comprehensive, real-time visibility into ICS networks, underlying protocols, and process-specific devices has been extremely challenging and has left industrial enterprises largely blind to potential security risks. Without contextual insight, industrial operators were unable to safely protect the control network from cyberattacks and avoid production disruptions.

Integrated End-To-End Security

Core industrial cybersecurity assets from Siemens such as the RuggedCom RX1500 swithc and router series and the Scalance SC600 security appliances protect network perimeters, connections between IT and OT systems, and enforce discrete zones within industrial networks. The integration of the Claroty Platform adds ICS intrusion detection and continuous OT network monitoring to the comprehensive Siemens security suite.

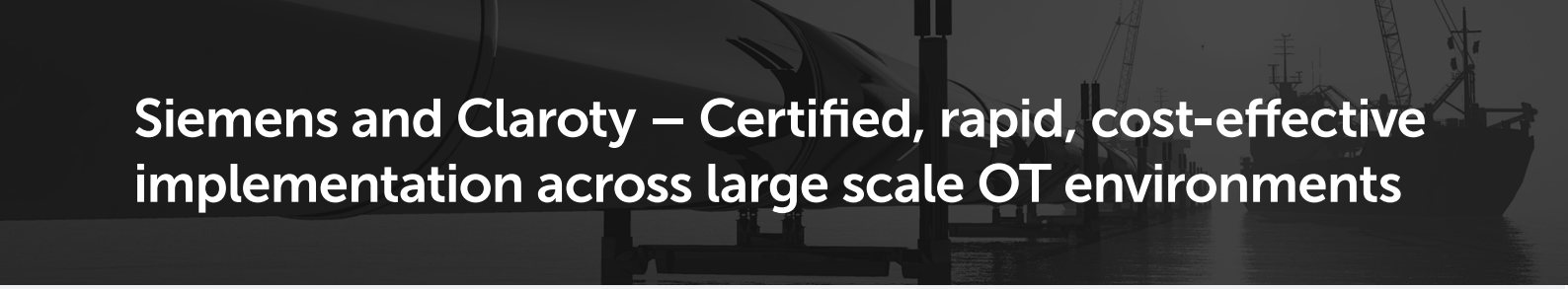
Claroty's Continuous Threat Detection (CTD) can be deployed in a number of methods including:

- Via a SPAN or mirror port on a standard Security Gateway/Rugged Security Appliance
- Pre-packaged into an existing offering – running atop existing network infrastructure

Regardless of the deployment option, the combined solution enables enterprises to quickly and safely implement real-time behavioral analysis in their industry control network, automatically identifying network assets and flagging anomalous activity that can affect the integrity of critical operational processes. With contextual alerts and recommended mitigation steps, organizations are provided with the detail they need to efficiently investigate suspicious behavior and improve overall cyber resiliency.

Architecture Components

Continuous Threat Detection (CTD), the anomaly detection component within the Claroty Platform, is designed to ensure safe, secure, and reliable operations in OT networks by extracting even the smallest details from large, complex environments – down to the serial and fieldbus networks. The system applies behavior-based anomaly detection and sophisticated pattern matching to identify early signs of malicious activity. CTD provides this extreme visibility, along with continuous threat and vulnerability monitoring, and ICS network segmentation in a single comprehensive solution.



Siemens and Claroty – Certified, rapid, cost-effective implementation across large scale OT environments

The components of the Claroty Platform integrated with the Siemens technology include:

- **Continuous Threat Detection (CTD) Server** a physical or virtual server that provides real-time cybersecurity and operational visibility of industrial control networks within distributed network environments and architectures.
- **Continuous Threat Detection (CTD) Sensor** a lightweight remote extension of the CTD server, used in sites with limited physical reach or across multiple remote isolated sites with limited out-of-band aggregation capabilities.
- **Enterprise Management Console (EMC)** a single pane of glass aggregating and consolidating data from various Claroty products. The centralized management interface displays a unified view of assets, activities and alerts making it highly suitable for Security Operations Centers (SOC).

Support for Multiple Integrations and Deployment Options

Integration of Claroty's industry-leading industrial cybersecurity platform with Siemens, one of the premier enablers of industrial automation and operator of nearly 300 factories worldwide, provides a self-contained solution set for industrial organizations undergoing digital transformations in which protecting operational networks is a pivotal element. The combination of Continuous Threat Detection and Siemens' industrial automation hardware both simplifies deployment within existing networking infrastructure and accelerates time to value.

In addition, the scalable architecture and management environment are designed for network monitoring across broadly distributed environments, so enterprises can ensure a consistent security posture across plants, isolated sites and even different geographies.

The table below provides a number of examples of how Claroty's advanced anomaly detection is tightly integrated into the Siemens network infrastructure along with the benefits of each integration:

Industrial PC (IPC) *Supported Model: 427E*	**SCALANCE Firewall** *Supported Models: SC600 Line*
The Siemens IPC line is built to support high-performance and space-saving applications particularly in the field of machine, systems and switchgear cabinet engineering. Claroty's advanced anomaly detection engine is provided as a pre-packaged offering – enabling existing and new customers to quickly and safely deploy its capabilities in their processes and operations. The integrated solution provides immediate, reliable, bandwidth optimized communication ideal for highly distributed networks. It can seamlessly operate in cases of logically or physically separated sites e.g. electric transmission grids, or oil and gas pipelines where space, power consumption and bandwidth are all precious commodities.	The Siemens SCALANCE line provides protection of devices and networks in discrete manufacturing and in the process industry. Claroty's advanced anomaly detection engine runs atop the existing SCALANCE hardware, all without the complications and inconveniences of procuring an external or additional industrial PC. The joint solution is ideal for discrete manufacturing plants; for example, in the automotive arena where real-time analysis of massive data streams is required both upstream and downstream. Fully integrated into the existing network infrastructure, Claroty's anomaly detection engine provides manufacturers with real-time visibility into critical assets – in a seamless fully passive manner and without requiring process downtimes.

Siemens and Claroty – Certified, rapid, cost-effective implementation across large scale OT environments

RuggedCom Switches

Supported Models: RX1500 Series

Leveraging the built-in switching and routing capabilities of the Siemens RUGGEDCOM line, it possible to run third party software applications such as Claroty's Continuous Threat Detection without the complications and inconveniences of procuring an external or additional industrial PC.

The joint solution is ideal for cases of logically or physically separated sites e.g. electric transmission grids and substations, or oil and gas pipelines where physical space, power consumption and bandwidth are all precious commodities.

Industrial IoT (IIoT)

Supported Model: IoT2040

The devices of the SIMATIC IOT family offer a robust, compact and flexible solution – focusing on IIoT environments.

Claroty's Continuous Threat Detection Sensor configuration can run atop the IoT2040 without the complications and inconveniences of procuring an external industrial PC.

Leveraging the product's lower output range and small physical footprint, it is an ideal solution for highly-distributed networks where space, power consumption and bandwidth are all precious commodities.

The figure below shows a deployment example of the Claroty Continuous Threat Detection Sensor running atop a Siemens Simatic IPC427 in a widely distributed environment as implemented at different levels of the system. In this specific example, a hierarchical architecture is shown with local monitoring and remote sites (substation) communicating with the Enterprise Management Console above them.

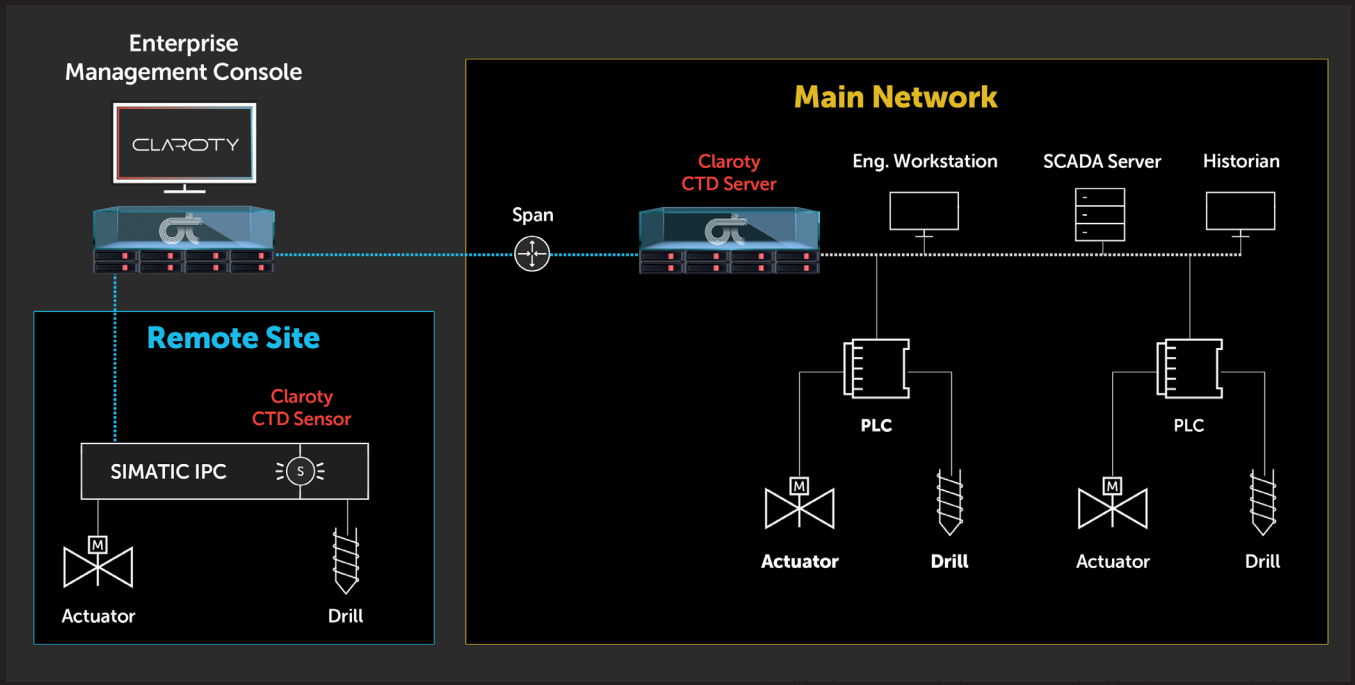


Figure 1 - Claroty Deployed on an IPC in a Highly Distributed Environment with local and Substation Examples

Siemens and Claroty – Certified, rapid, cost-effective implementation across large scale OT environments

Common Use Cases

Scenario 1: Highly-Distributed Networks

Electric power-generation systems and grids are characterized by large geographic spread and a substantial amount of infrastructure. This enormous scale creates challenges in managing and monitoring the industrial control network and its devices.

The Challenge

- The solution needs to be operational at a highly distributed environment with thousands of substations, each of which has many assets.
- Provide real-time visibility into assets, their status – all while handling large volumes and without negatively impacting performance.

The Solution

Claroty's advanced anomaly detection capability was designed to easily manage large-scale substation deployments in terms of setup, management, and maintenance. Leveraging a hierarchical architecture with local sensors deployed atop existing Siemens network infrastructure at various levels of the substation – all communication is aggregated and visible via a centralized Enterprise Management Console. This highly flexible model allows grouping substations together for easier system management and simplified visibility. SOC and security teams are empowered to rapidly respond to and remediate threats with alert aggregation from various Claroty products..

Scenario 2: Mitigating an attack on Remote Substation

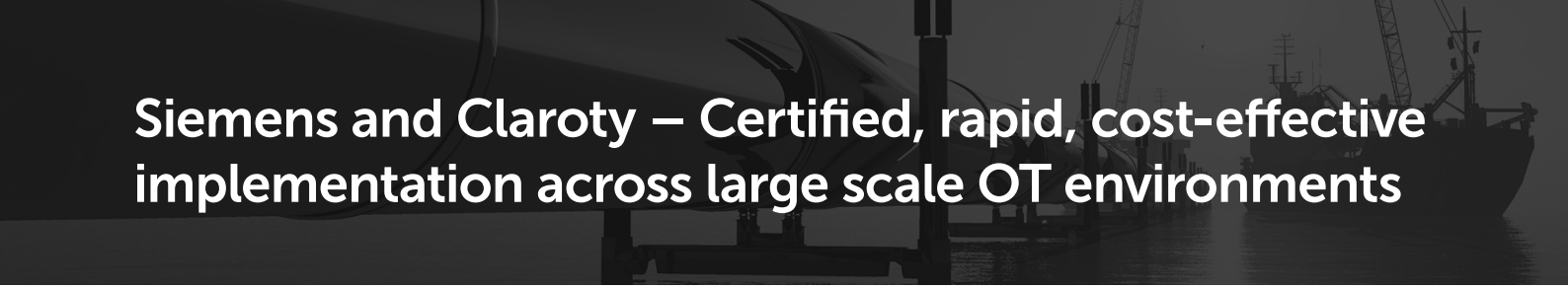
Electric substations are characterized by a large geographic spread and a substantial amount of infrastructure. This large scale creates challenges in managing and monitoring the physical or remote access to the substation's network.

The Challenge

A cyberattack on a regional substation provides an attacker with a foothold into additional substations with access (and potential control) over hundreds of RTUs – threatening to cause a wide-scale power outage.

The Solution

Claroty's advanced anomaly detection engine, deployed on existing Siemens network infrastructure at various levels of the substation's network, can quickly and easily detect and alert upon suspicious activity associated with a threat actor accessing the substation's network. Consequently, specific context-aware alerts are sent to the relevant SOC personnel to execute incident response plans utilizing network diagrams, asset inventories and process information available from the Claroty's anomaly detection system.



Siemens and Claroty – Certified, rapid, cost-effective implementation across large scale OT environments

The Claroty Platform

Claroty's fully integrated suite of cybersecurity products addresses the unique challenges of ICS systems so that engineers, operators, and cybersecurity professionals can protect even the most complex industrial networks.

The Claroty Platform enables enterprises to assess the security posture of their ICS network, protect critical systems, control access to network assets, continuously monitor and detect vulnerabilities and threats, and rapidly investigate and respond to cyber incidents.

About Siemens

Siemens was founded over 170 years ago by an entrepreneur who believed technology is a tool to advance the common good. Today Siemens is a global force in the areas of electrification, automation, digitalization and a leading supplier of systems for power generation and transmission, medical diagnosis, and infrastructure and industry solutions.

For Siemens, cyber security is a foundational component of digitalization and intelligent infrastructure. Through partnership with Claroty, Siemens utilizes cyber expertise and Claroty's ICS network anomaly detection to help customers increase visibility and reduce cyber risks to their industrial networks.

Contact Us

CLAROTY

Claroty was conceived to secure the safety and reliability of industrial control networks that run the world from cyber-attacks. The Claroty Platform is an integrated set of cyber security products that provides extreme visibility, unmatched cyber threat detection, secure remote access, and risk assessments for industrial control networks (ICS/OT).

www.claroty.com | contact@claroty.com |