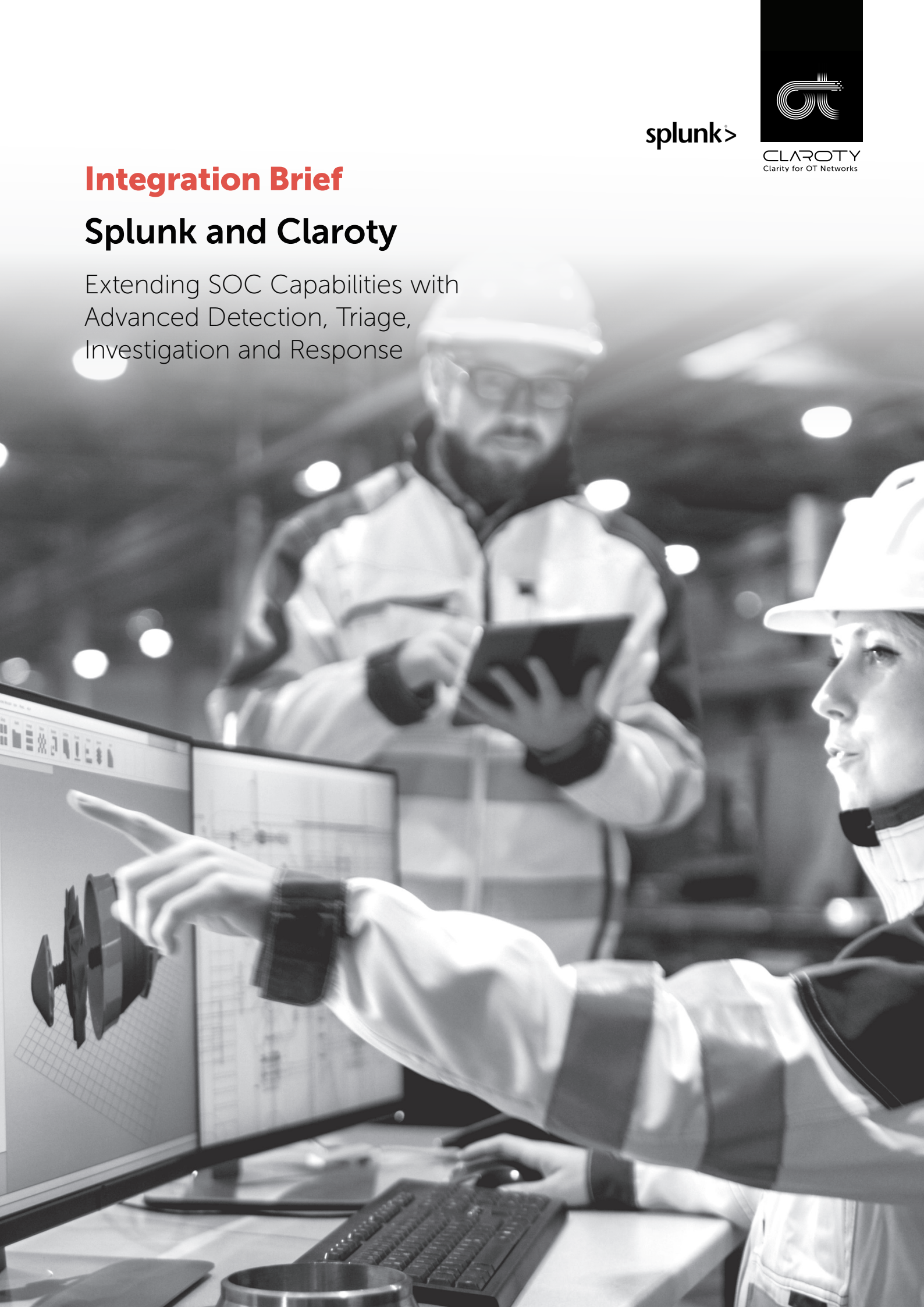
splunk>

CLAROTY
Clarity for OT Networks

Integration Brief

Splunk and Claroty

Extending SOC Capabilities with Advanced Detection, Triage, Investigation and Response



Splunk and Claroty – Extending SOC Capabilities with Advanced Detection, Triage, Investigation and Response

Solution Highlights

- **Delivers a Simple View of Complex Industrial Operations** – Seamlessly integrating data across disparate systems to assess monitor and mitigate potential threats across the entire infrastructure
- **Reduces Real-Time OT-Related Risks and Insights** – Proactively identify and fix configuration and other network hygiene issues that can leave your network vulnerable to attacks – minimizing unplanned downtime and the high costs associated with it
- **Shifts View of Operations from Reactive to Proactive** – Strengthen operational resiliency with real-time visibility across IT, OT and IoT resources

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 Commissioned decades ago, without cybersecurity in mind and sometimes running outdated software, many of these networks and underlying assets are being increasingly targeted with sophisticated cyberattacks or are connected to IT networks and at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 deep visibility into ICS networks, their underlying communications patterns and protocols, and detail on process-specific devices has been extremely challenging and has left industrial enterprises largely blind to potential security risks. Without this contextual insight, industrial operators have been challenged to proactively protect the control network from cyberattacks and avoid production disruptions.

Solution Overview

To address this lack of visibility into the security and resiliency of OT networks without burdening security teams with another monitoring tool, Claroty has partnered with Splunk to provide a broad security solution which spans both IT and OT environments.

Claroty's industry-leading OT industrial cybersecurity platform provides deep OT visibility and threat detection, and tight integration with Splunk's Security Information Event Management and Analytics (SIEM) platform enables SOC teams to efficiently monitor and respond to both IT and OT security alerts from a single pane of glass.

Unified Visibility Across
Claroty's unique network monitoring capabilities provide extreme visibility into the lowest levels of industrial networks, enabling security teams to identify OT threats more quickly. The insight Claroty delivers to SOC analysts into the assets and protocols deployed in their industrial environment, along with ICS-aware behavioral based-modeling to rapidly detect abnormal behavior. OT security alerts are delivered to Spunk, for a truly integrated IT/OT security monitoring, policy management and incident response solution.

Claroty Continuous Threat Detection (CTD) automatically discovers and monitors network assets, protocols, and communication patterns all the way down to the I/O level and builds an operational baseline of "known good" behavior. Consequently, any anomalous activity is immediately alerted upon enabling SOC and security teams to prioritize alerts as they emerge, evaluate and determine risk levels, and responds accordingly – all while allowing to effectively prevent the disruption of critical operations.

For example, when a high-risk activity is discovered, SOC teams can drill down to obtain a detailed view of the action/violation that triggered the alert. Leveraging Claroty's extreme visibility, SOC and security personnel are provided with contextual real-time information to accurately and effectively investigate early Indicators of Compromise (IoC) – materially reducing response times all the while enhancing cyber resiliency.

Splunk and Claroty – Extending SOC Capabilities with Advanced Detection, Triage, Investigation and Response

Common Use Cases

Continuous Monitoring of ICS and Industrial Network Assets – With a unified, real-time view into PLCs/RTs, embedded PCs, process control software and additional network assets, enterprises can proactively enhance reliability and overall process resiliency—all while minimizing unscheduled downtimes.

ICS Security and Safety – By continuously monitoring mission-critical assets and industrial systems, security teams are provided with comprehensive visibility into system performance including the detection of anomalous activity or violations from predefined set points that could put machines or people at risk.

Predictive Maintenance – Leveraging real-time insights into deployed assets identification, utilization and resource consumption, operations personnel can better prepare and predict unscheduled downtime of process-critical infrastructure. Employing advanced, behavior-based anomaly detection and sophisticated pattern matching algorithms, the system can detect and proactively alert when maintenance work is required – all while maximizing performance and production and minimizing unscheduled downtimes.

Summary

The increased digitization and connectivity of OT networks has delivered monumental advancements in industrial productivity. However, this connectivity has also increased the risk of ICS-targeted malware attacks and spill-over damage from broad-based cyberattacks.

Enterprise security teams, already over-burdened by protection of expansive IT environments, are increasingly taking responsibility for securing OT networks into which they have had little visibility. To meet this challenge, cybersecurity solutions must provide an efficient means of detecting and responding to cyberthreats no matter where in the infrastructure they are. Splunk and Claroty recognize these challenges and have moved aggressively to deliver a highly-effective, integrated cybersecurity solution. Leveraging Claroty's Continuous Threat Detection and Splunk's SIEM platform, security teams can now continuously monitor for threats, evaluate events as they emerge, determine consequent risk levels, and prioritize response as appropriate.

Splunk and Claroty – Extending SOC Capabilities with Advanced Detection, Triage, Investigation and Response

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.

Splunk

Splunk delivers real-time predictive analytics that enables organizations to proactively optimize operations and improve performance. By collecting, analyzing and visualizing real-time and historical machine data from a variety of source and formats—the Splunk SIEM creates a simple real-time view across complex data sets. Leveraging this information, security and SOC teams can accurately prioritize response and mitigation activities across the network to help organizations reduce the impact of security incidents.

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 |