Operational technology (OT) networks, including ICS and SCADA systems common in critical infrastructure and manufacturing organizations, have become increasingly connected to IT networks. While this has improved operational efficiency, it has also made OT a more prevalent attack vector and target for today’s threat actors.

Unlike attacks on IT that generally focus on data theft and monetary gain, a successful attack on OT can alter physical processes. Cyberattacks on OT could damage infrastructure, disrupt services, and endanger the health and safety of workers and the communities they serve.

As such, it has increasingly become the responsibility of IT security teams to inform OT engineers of their cyber risks and potential impacts. In order to do this, organizations need to have unified visibility of the hybrid network, its assets and vulnerabilities at all times.

Integration between Skybox and Claroty provides complete visibility across traditional IT, cloud and OT networks and contextual intelligence to understand risk.
Skybox and Claroty | Technology Brief

SKYBOX VALUE

• Provides hybrid network visibility in a seamless, comprehensive model
• Gives insight to reachability of networks and network zones
• Produces actionable intelligence, giving details of vulnerability attributes, exploitability and remediation options
• Prioritizes alerts to focus action on your most critical risks
• Centralizes security management and supports a variety of use cases from a single platform

CLAROTY VALUE

• Provides extreme visibility into ICS Networks
• Identifies security gaps — including known and emerging threats and vulnerabilities
• Automatically generates current state of OT process-level communications and presents an ideal network segmentation strategy
• Detects security posture changes
• Enables proactive threat hunting with actionable threat information
• Secures, monitors, and records remote connections to ICS assets

Skybox integrations with OT security platforms give organizations with ICS and SCADA systems a way to gain crucial visibility across the hybrid IT-OT environment to:

• Understand reachability between networks and network zones
• Contextualize risk and effectively plan remediation
• Proactively reduce risk to safeguard the organization without sacrificing uptime

Skybox provides the broadest set of out-of-the-box integrations with enterprise technology. These integrations allow Skybox to passively collect information from your networking and security solutions — including the Claroty Platform — normalize and merge data. By creating centralized data repositories, Skybox gives you the single source of truth to support a variety of security processes in IT and OT networks.

FIG 1: A diagram showing the collection method of Claroty Platform and relayed to Skybox Security. To see a full list of 130+ supported devices from which Skybox collects in the IT and OT space, visit our website.
Skybox builds collected data into a model of your hybrid environment, giving comprehensive and in-depth visibility to your traditional IT, cloud and OT networks.

Visibility, contextual intelligence and analytics-driven automation lets you see and understand where your biggest risks lie and streamlines processes to eliminate risks or quickly respond to attacks.

With the model, users can perform a variety of analyses and automated processes to understand and improve security posture in the hybrid IT-OT environment:

- Compare the aggregate access of your network to the access designed in your security policies, analyzing by Purdue level, device type, etc.
- Analyze access end to end to troubleshoot connectivity issues and protect critical assets
- Identify critical-risk exposed and exploitable vulnerabilities to effectively plan patches or mitigation
- Automate and orchestrate processes to maintain uptime and avoid costly or dangerous disruptions

The model-driven Skybox approach provides a straightforward way to understand the relationship of IT and OT networks and how it affects the risk of each. It is a valuable tool to improve collaboration and alignment between security teams and OT engineers, ensuring risks are controlled and uptime is optimized.
About Skybox Security

Skybox provides the industry’s broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 130 networking and security technologies, the Skybox® Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world’s largest organizations.

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060

About 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

Copyright © 2019 Skybox Security, Inc. All rights reserved. Skybox is a trademark of Skybox Security, Inc. All other registered or unregistered trademarks are the sole property of their respective owners. 05302019