SOLUTION BRIEF

EXPOSURE MANAGEMENT FOR CYBER-PHYSICAL SYSTEMS

Fortifying CPS in an Evolving Risk Landscape

In order to keep up with the continuous pace of digital transformation, manufacturing, healthcare, and other critical infrastructure organizations must evolve beyond traditional vulnerability management for their cyber-physical systems (CPS) and create a broader and more dynamic program for managing their overall exposure to risk.

Due to the unique nature of CPS environments, this requires a specialized approach that enables these organizations to create an Exposure Management program that takes into account asset complexities, unique governance, and the business critical operational outcomes of CPS environments. This approach encompasses a repeatable cycle of measures that optimize security beyond traditional means such as patching or playbooks.

Exposure Management

Gartner® defines Continuous Threat Exposure Management (CTEM) as "a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure and exploitability of an enterprise's digital and physical assets."

Per Gartner, "At any stage of maturity, a CTEM cycle must include five steps to be completed: scoping, discovery, prioritization, validation and mobilization. Organizations building a CTEM program use tools to inventory and categorize assets and vulnerabilities, simulate or test attack scenarios and other forms of posture assessment processes and technologies. It is important that a CTEM program has an effective and actionable path for infrastructure teams, system and project owners to take action on findings."[1]

[1] Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, 11 October 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

[2] Gartner, How to Manage Cybersecurity Threats, Not Episodes, Kasey Panetta, 12 August 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Driving Forces of Exposure Management

Managing CPS risk requires a more dynamic approach

Claroty Team82's analysis of more than 20 million CPS has revealed that 38% of the riskiest of them are overlooked by traditional vulnerability management approaches – revealing a major blind spot that can lead to exploitation by malicious actors.

Solely relying on a CVSS-based approach risks overlooking critical exposures and exploit viability.

Responsibility for securing CPS has shifted to IT

More than 95% of CISOs in manufacturing and critical infrastructure sectors are or will soon be responsible for securing not only their organization's IT environment, but also their CPS environment–directly affecting business outcomes.

Shifting to exposure management will help account for the full scope of risk across the organization.

Industry and regulatory pressures

From the PATCH ACT to version 5 of FedRAMP, recent regulatory developments have made it clear that transparency into software bills of materials (SBOMs) is key to understanding potential risks of embedded vulnerabilities within vendors' supply chains.

Current solutions lack the CPS expertise and vertical knowledge to validate the full attack path and aid compliance.

> 38% of the riskiest CPS are overlooked by traditional vulnerability management approaches

CPS Exposure Management with Claroty

Shifting to a dynamic exposure management program requires implementing more mature, strategy-driven preventative controls with detection and response capabilities. Claroty provides a series of capabilities tailor-made to support a CPS-specific exposure management process:

Scoping

Despite their potential impact on business outcomes, CPS are often overlooked by security programs. Claroty solutions are designed specifically for cyber-physical system and help to identify and prioritize business critical operations.

Discovery

CPS require specialized knowledge to effectively identify and assess exposures. Claroty uses multiple discovery techniques to profile CPS, map network communications, and correlate vulnerabilities and other exposures.

Prioritization

Claroty's unique risk framework, data feeds from CISA's KEV and the EPSS, and multiple exposure considerations highlight specific attack vectors, assesses exploitability and impact, and provides quantified remediation recommendations.

Validation

Confirming the exploitability of an exposure requires an intimate understanding of the CPS and environment involved. Claroty helps to validate exposures attributing VEX files to assets and leveraging our multiple OEM alliances with CPS vendors.

Mobilization

Operationalizing this cycle requires executing on the insights gathered throughout the process. Claroty integrates with a wide variety of enterprise solutions and provides detailed reports to help enable seamless exposure remediation workflows.

Having spent years empowering thousands of organizations to more effectively and efficiently strengthen their CPS cyber risk posture, Claroty offers a comprehensive portfolio of CPS security solutions that support the full extent of the exposure management journey for manufacturing and other critical infrastructure organizations. Visit claroty.com to learn more about how Claroty can support your CPS exposure management journey.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.

CLAROTY