MODULE OVERVIEW

VULNERABILITY & RISK MANAGEMENT

The Industrial Vulnerability & Risk Management Challenge

Connectivity within industrial cyber-physical systems (CPS) has dramatically reshaped their vulnerability and threat landscape, making traditional risk reduction workflows neither practical nor sufficient. Industrial networks require a more comprehensive and environment-aware solution for identifying, assessing, and contextualizing risk. Claroty xDome enables industrial and critical infrastructure organizations to mitigate risks & vulnerabilities before they compromise operational uptime, personnel safety, or service availability.

An effective vulnerability management & risk management program provides visibility into risks within connected assets, provides deep insights, and helps to streamline workflows for prioritization & remediation. Claroty xDome delivers a purpose-built solution for industrial environments, helping to reduce risk and safeguard against cyber threats. Highlights include:



xDome Platform VRM Module

How It Works

Claroty xDome offers multiple asset discovery methods in order to give fully enriched asset profiles and an accurate asset inventory of all your cyber-physical systems within OT, IoT, and IT. This caliber of visibility is made possible through a flexible deployment based on the unique needs of each environment. This level of asset detail enables xDome to assess overall risk based on technical asset attributes, external vulnerability intelligence, and proprietary in-house research. These discovery methods include:

- **Passive Monitoring:** Continuous monitoring of asset communications with deep-packet inspection (DPI) technology.
- **Safe Queries:** Targeted, non-disruptive discovery of assets in their native protocol.
- **Claroty Edge:** Speedy, host-based asset profiling through localized queries.
- **Project File Analysis:** Regular ingestion of offline configuration files for asset enrichment.
- **Ecosystem Enrichment:** Enrich ecosystem data through integrations with existing asset inventory and security solutions.

© 2023 Claroty Ltd. All rights reserved

Risk Identification

Understanding all the potential risks and vulnerabilities that impact assets across industrial environments can be challenging due to their unique attributes and applications. The xDome platform lays the foundation for comprehensive vulnerability & risk management with complete visibility into the assets and network blind spots most prone to risk. Highlights include:

- **Enriched Asset Profiles:** xDome correlates asset attributes with known vulnerabilities (CVEs) and other insights such as unsecure protocol usage, external connections, default password usage, and more creating the foundation for network risk assessment and prioritization.
- **Enterprise Risk Distribution*:** xDome identifies where assets with critical risk scores are distributed across your environment as well as what risk factors they are associated with in order to highlight the largest contributors to risk.
- **Vulnerability Management (VM) Integrations*:** Integrating with VM solutions enables industrial organizations to leverage existing solutions in order to provide further depth of visibility into their CPS while eliminating the risk of incorrectly scanning OT assets with the ability to create exclusion lists.

Risk Assessment

The ability to assess the risk of each asset and across sites is essential to building a strong foundation for vulnerability and risk management. Meaningful assessment of risk requires a deep understanding of both the assets and the environment in which they operate.

- **Proprietary Asset Risk Scores:** Claroty's risk framework provides risk scoring based on three core metrics: likelihood, compensating controls, and impact. A flexible and customizable risk score formula ensures that an organization's risk posture is reflective of their unique environment and risk reduction priorities.
- **Risk Simulator*:** The risk simulator illustrates the possible risk an asset poses to the network based on facts such as the likelihood an event will occur, its potential impact, and compensating controls in place to mitigate the event or its impact.
- **Vulnerable Assets Page*:** xDome creates a suggested order of priority groups for vulnerable assets aggregated by model, asset type, and manufacturer for easy prioritization of assets that require immediate attention.

Risk Prioritization

Once vulnerabilities and potentially impacted assets are identified, addressing remediation tactics ensure risk-based prioritization across the full lifecycle of a vulnerability.

- **KEV and EPSS Correlation:** Data enrichment from CISA's Known Exploited Vulnerabilities (KEV) catalog and the Exploit Prediction Scoring System (EPSS) provide additional context into a vulnerability's usage or exploitability.
- **Vulnerability Prioritization*:** In order to streamline remediation, xDome prioritizes vulnerabilities into groups based on their potential impact, exploitability characteristics, relevance, and available remediation information.
- **Risk Overview & Recommendations*:** Enables users to focus on the most impactful risk remediation efforts with visualized risk metrics across the network and tailored risk recommendations based on their quantitative impact on the overall network risk score.

* Included in advanced module

© 2023 Claroty Ltd. All rights reserved

Claroty xDome Vulnerability & Risk Management Module

Claroty xDome Essentials	Claroty xDome Advanced VRM Module
Comprehensive vulnerability & risk identification and assessment capabilities based on multiple sources of intelligence, proprietary risk profiling, customizable risk configurations, and endpoint management integrations.	End-to-end vulnerability & risk management including network-wide recommendation and prioritization features, risk simulation, manufacturer remediation information, and vulnerability scanning integrations. This module enables asset owners to take more impactful and efficient risk reduction measures at the site-level.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their 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, network protection, 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

© 2023 Claroty Ltd. All rights reserved