SOLUTION OVERVIEW

Crowdstrike Falcon Next-Gen SIEM and Claroty

Rapid Detection and Response Solutions for Converged OT/IT Defense

Continuous Detection and Rapid Response for Converged OT and IT

Digital transformation within industrial, critical infrastructure, building automation, and other complex environments delivers a wide array of benefits, including increased productivity and cost savings. As a result of this increasing connectivity between previously isolated operational technology (OT) environments and their information technology (IT) counterparts comes new opportunities for threat actors to access and abuse these environments. This connectivity has far outpaced industrial organizations' abilities to properly secure their networks–resulting in new attack pathways in critical Cyber Physical Systems (CPS).

The collaboration between **Claroty's xDome platform** and **CrowdStrike's Falcon Next-Gen SIEM** offers an integrated cybersecurity solution for industrial and operational technology (OT) environments. By combining Claroty's deep OT asset visibility and network monitoring with Falcon's advanced SIEM capabilities, this solution provides unparalleled threat detection across both IT and OT domains. The integration enables comprehensive, real-time visibility into interconnected systems, enhanced by AI-powered analytics and automated threat detection. This approach helps organizations identify and neutralize threats quickly, improving security posture and ensuring the continuity of critical infrastructure operations in today's increasingly digital industrial landscape.

Key Features & Benefits

- **Unified Asset Inventory & Enrichment:** Claroty xDome and CrowdStrike Falcon NextGen SIEM combine strengths to deliver comprehensive visibility into all managed and unmanaged IT/OT assets, empowering organizations to identify, prioritize, and mitigate risks across their entire attack surface from a single platform.
- **Continuous Anomaly & Threat Detection:** xDome's Advanced Threat Detection system continuously monitors OT networks and other Cyber Physical Systems (CPS) and integrates events, alerts, vulnerabilities, and other logs into CrowdStrike's Falcon NextGen SIEM for coordinated triage and faster SOC response times.
- **Rapid Incident Response and Automation:** Leverage dynamic visualizations to map threat pathways and accelerate response with an AI-powered content library featuring an expanded collection of prebuilt workflows and response actions.

©Copyright Claroty. All rights reserved

Key Uses Cases

Unified Asset Inventory & Enrichment (Visibility & Risk)

The combined capabilities of Claroty and CrowdStrike Falcon Next-Gen SIEM revolutionize Asset Inventory and Enrichment for IT/OT environments. By integrating endpoint and network sources, the solution automatically identifies and enriches industrial assets like human-machine interfaces (HMIs), historians, and engineering workstations (EWs) running CrowdStrike agents. Claroty enhances visibility by parsing configuration files fetched from CrowdStrike Falcon via its AppDB, eliminating the need for direct connections to the industrial network.

This enriched data populates directly within the Claroty Platform, providing users with a single source of truth for IT/OT assets and unprecedented visibility into isolated OT environments. This comprehensive asset understanding forms a robust foundation for superior threat detection and vulnerability management, ensuring proactive and effective protection across converged IT and OT networks.

Continuous Anomaly & Threat Detection (Detect & Respond)

The integration of Claroty and CrowdStrike Falcon Next-Gen SIEM provides a robust solution for IT/OT security by combining enriched asset visibility with advanced threat detection. The partnership merges proprietary and open-source YARA and Snort signatures, forming one of the industry's largest IT/OT threat signature databases. This allows for seamless and scalable threat detection across environments. By integrating endpoint and network data, the solution automatically identifies and enriches industrial assets, such as HMIs and engineering workstations with CrowdStrike agents. Claroty's platform further enhances visibility by parsing configuration files from CrowdStrike without requiring direct ICS network access, enabling organizations to strengthen their defense against threats across IT and OT environments.

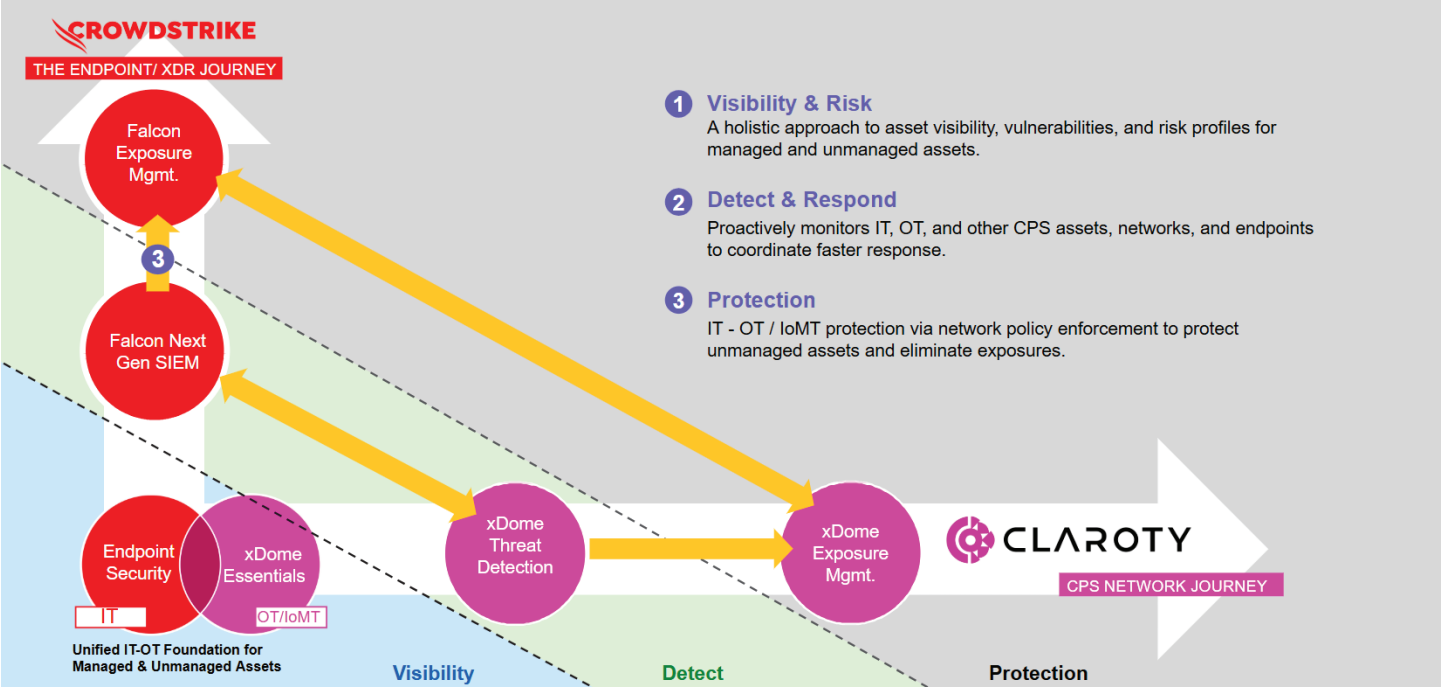
Rapid Incident Response and Automation (Protection)

The joint solution from Claroty and CrowdStrike significantly enhances incident response and automation by integrating advanced IT and OT security capabilities. Claroty's xDome provides in-depth monitoring and threat detection tailored to industrial and healthcare environments, using behavioral analytics to identify anomalies in XIoT assets and minimizing false positives. CrowdStrike Falcon Next-Gen SIEM complements this by offering AI-powered threat detection, automated triage, and rapid containment actions such as endpoint isolation and network policy enforcement. Together, these platforms deliver a unified view of IT and OT environments, streamline workflows, and enable faster, more coordinated responses to incidents, ensuring comprehensive protection against known and unknown cyber threats.

©Copyright Claroty. All rights reserved

The Crowdstrike - Claroty Joint Solution Journey

The CrowdStrike-Claroty joint portfolio encompasses a broad range of technical integrations and complementary solutions, all of which aim to empower our joint customers to secure converged OT and IT networks. Core offerings include, but are not limited to, the following:



About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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. To learn more, visit claroty.com.

©Copyright Claroty. All rights reserved