corelight | Axonius

Joint solution

Corelight for Axonius Asset Cloud

Accelerate vulnerability detection and prioritize investigations with integrated network, endpoint, and vulnerability data directly within the network sensor

Security teams face considerable challenges maintaining a strong security posture because legacy tools often fall short of supporting modern infrastructure and countering increasingly sophisticated threats. This visibility gap is compounded by a constant storm of alerts from countless devices scattered across the enterprise, especially unmanaged, unknown, or IoT assets that evade traditional endpoint management. All of this wears down the security operations center (SOC) team, leaving analysts grappling with too much data but far too few actionable insights.

Intelligence-driven alert prioritization

Corelight's Open NDR integration with Axonius Asset Cloud addresses modern visibility and detection challenges by combining Corelight's deep network telemetry with Axonius' comprehensive environmental asset intelligence. By enriching Corelight's comprehensive, Zeek®-based logs with timely Axonius endpoint and vulnerability data directly at the point of observation in the network sensor, security teams can streamline investigations, accelerate responses, and resolve incidents faster than ever.

By correlating network attack signals from Corelight with known vulnerable systems identified by Axonius, SOC leaders can dramatically transform their alert prioritization strategy. This intelligence-driven approach not only accelerates investigations but also reduces the time required for effective remediation (MTTR). It ensures that your limited SOC resources are applied precisely where they will have the greatest impact on improving the organization's overall security posture.

SOLUTION HIGHLIGHTS

Unified visibility: Gain rich, comprehensive network logs seamlessly enriched with contextual endpoint and vulnerability data

Risk-based prioritization: Simplify investigations and prioritize alerts according to actual, verified risks in your environment

Higher analyst productivity: Reduce alert fatigue by focusing your team's attention only on the vulnerabilities that matter

Compliance-ready evidence: Maintain immutable network evidence that goes back months or years to satisfy audit and regulatory compliance requirements

Streamline investigations with enriched network evidence

The native integration between Corelight and Axonius transforms how overburdened SOC teams manage the daily alert storm—a critical advantage when adversaries are increasingly leveraging artificial intelligence to accelerate their attacks.

Real-time network telemetry enriched with precise endpoint and vulnerability data, combined with Corelight's multi-layered detections (including unsupervised anomaly detection), empowers your team to stay one step ahead. When Corelight detects suspicious activity across the network, analysts no longer have to pivot between multiple solutions to gather key insights into the attack.

By immediately seeing if a target endpoint is actually susceptible to a specific attack when an alert is triggered, analysts can prioritize critical threats and significantly reduce false positives. This helps resource-constrained SOC teams simplify deployment and alert triage. Furthermore, Corelight's extensive visibility into all network activity helps pinpoint unmanaged and unknown systems across the environment, which can then be immediately inventoried and secured by Axonius.

With full contextual asset data and immutable network evidence integrated directly into your workflows, your analysts can simplify investigations, decrease response times, and drive a more secure posture across the entire enterprise.

corelight

To learn more about Corelight for Axonius, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497