Joint solution

Corelight for Tenable Vulnerability Management

Accelerate vulnerability detection and prioritize incident response

Security teams face considerable challenges maintaining a strong security posture because legacy tools often fall short in correlating ongoing network activity with current environmental risks. This is further compounded by the massive volume of alerts, many of which target systems that are not actually vulnerable, leading to unnecessary distractions and alert fatigue for analysts.

INTEGRATION HIGHLIGHTS

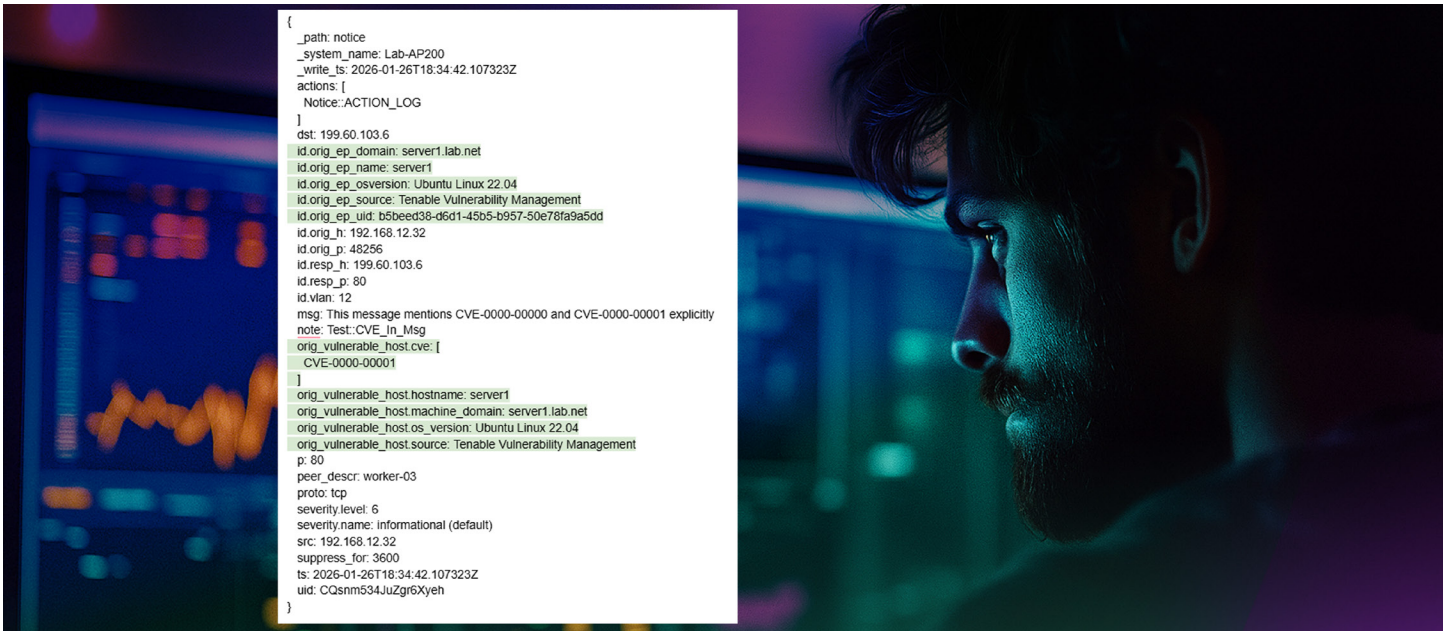
Unified visibility—rich network logs enriched with contextual endpoint and vulnerability data

Risk prioritization—faster investigations with risk-based alert prioritization

Hybrid coverage—seamless integration with Tenable Vulnerability Management and Tenable Security Center

Faster remediation—improve MTTD and MTTR by focusing analyst attention on verified, high-risk vulnerabilities

Integrated Corelight and Tenable Vulnerability Management data in a single view



Accelerate investigations and prioritize alerts based on risk by enriching Corelight logs with real-time Tenable endpoint and vulnerability data.

Corelight's Open NDR integration with Tenable Vulnerability Management (formerly Tenable.io) and Tenable Security Center (formerly Tenable.sc) addresses this by enriching network telemetry with real-time vulnerability data directly at the point of observation in the Corelight sensor. By providing deep network visibility that correlates detected network attacks with known vulnerable systems identified by Tenable Vulnerability Management, Corelight empowers Security Operations Center (SOC) teams to dramatically transform their prioritization strategy.

This timely correlation enables analysts to move beyond general vulnerability scoring and focus instantly on the highest-risk exploits currently targeted within the network. This intelligence-driven prioritization reduces the time required for effective remediation, ensuring that limited resources are applied where they will have the greatest impact on improving the organization's security posture.

Streamline investigations with enriched network evidence

The native integrations between Corelight and Tenable Vulnerability Management and Tenable Security Center transform how SOC teams handle security incidents. Corelight sensors poll Tenable APIs to ingest timely data on all discovered hosts and their specific CVEs (Common Vulnerabilities and Exposures) across the environment. This data is then used to enrich relevant Corelight logs, helping analysts focus on the hosts that pose the greatest risks.

When Corelight detects CVE-related suspicious activity across the network, it cross-references the targeted IP address against the Tenable data it ingests from its network sensors. If a match is found, Corelight enriches the relevant alert logs in real-time with the appropriate host and vulnerability data. By immediately seeing if a target is susceptible to a specific attack and exploit when an alert is triggered, analysts can prioritize critical threats and significantly reduce false positives.

In addition to enriching select logs with related CVE data, customers can use this Corelight integration to enrich all logs with essential host information, such as Hostname, Host Unique ID, and OS version, to simplify investigation workflows or cross-reference your asset inventory.

About Corelight

Corelight provides security teams with the network evidence they need to protect the world's most critical organizations. Founded by the creators of Zeek®, Corelight's Open NDR platform delivers superior visibility and analytics to accelerate investigations and expand threat hunting.

corelight

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

https://corelight.com/contact

info@corelight.com | 888-547-9497