ENLIGHTENMENT BRIEF:
Lumu and EDR

With more than 1,200 vendors in the cybersecurity industry, it is critical to understand how Lumu compares with and complements other technologies in the space to maximize the output of your cybersecurity strategy.

How does Lumu compare with an Endpoint Detection and Response (EDR) solution?

Lumu and EDRs are different technologies, designed with different purposes in mind.

For starters, Lumu is a technology that was built from the ground up with a single objective: **help to measure and understand your unique compromise level in real time**. This is done via Lumu's patent-pending Illumination Process which systematically collects, normalizes, and analyzes your company's **network metadata,** resulting in the identification of enterprise assets in contact with adversarial infrastructure. Simply put, Lumu identifies confirmed compromises.

On the other hand, Gartner defines EDRs as "solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems."

How can Lumu and EDRs work together?

If your company already has an EDR solution like Sentinel One, FireEye EDR, Crowdstrike, or the Like, Lumu Insights seamlessly integrates with your EDR via our API, while layering real-time compromise assessment. In order to assess compromises effectively, organizations must monitor not only the information assets that could have an endpoint software installed, but they need to go further and monitor legacy systems, IoT, and OT networks that most EDR solutions can't monitor.

According to Enterprise Strategy Group "even with the use of advanced machine learning and behavioral analytics, endpoint security solutions still are not able to prevent 100% of threats. This leaves a gap for security teams, who need a mechanism to detect and respond to threats that make it through preventative controls." Furthermore, in the last Threat Detection and Response Landscape Survey more than 75% of EDR administrators stated that this technology carries a high total cost of ownership. They claimed that the implementation project was more complex than anticipated and demanded advanced security analytics skills.

Lumu adds incredible value to EDR by providing visibility of the whole network whether or not you have an agent installed. Also, Lumu alerts only confirmed compromises and not only behavior-based alerts that have a good chance of being false positives. Lumu is capable of detecting residual compromise on EDR protected devices that maintain connection attempts with adversaries, hence eliminating the false sense of security.

If you do not have an EDR in place, Lumu provides full and enhanced visibility with the broad network metadata collected (DNS, Firewall and Proxy Logs, Network Flows, and Spambox) answering conclusively if your network is compromised.

In addition, Lumu includes Compromise Context and the automated MITRE ATT&CK® Matrix that enriches confirmed compromise with factual data related to each compromise's distribution, behavior, movement, and more. By accessing our Threat Triggers, you can enable policies that contain these compromises using your current cybersecurity infrastructure. Consequently, you can invest time to understand and eradicate each compromise, so you and your team can respond in a precise and timely manner.

Can Lumu replace the EDR?

EDR and Lumu are solutions used to address different challenges. Lumu can add incredible value to the security strategy of your organization, whether you have an EDR or not.

Organizations that have not invested in an EDR find the combination of Lumu and their current AV/Endpoint protection agent sufficient to identify threats, reduce the impact of cyber attacks, maximize their security team's efficiency, and drastically improve their compromise detection efforts. According to ESG, 43% of organizations prefer to use NTA solutions as a first line of defense rather than EDR solutions. By choosing Lumu as their first line of defense, businesses become empowered by the intelligence provided and use it to make informed decisions on future investments that allow for a stronger cybersecurity program.

Conclusion

EDRs serve a specific purpose and it is critical to understand that they are unable to provide conclusive evidence of compromise levels or serve as a compromise detection solution. Lumu's patent-pending data collection and analysis process is built to detect compromise in real time and allow organizations to respond to compromises quickly and precisely via Lumu API to orchestrate the defense without depending on the installation of endpoint software.

Learn more at: lumu.io/product/