LUMU

ENLIGHTENMENT BRIEF:
Lumu and IDPS

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 Intrusion Detection and Prevention System (IDPS) solution?

Lumu and IDPS are different technologies from different eras, designed with different purposes in mind.

For starters, Lumu is a technology that was built from the ground up with a single objective: **help measure and understand your unique compromise level and enable incident response capabilities 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 and feeds the information of your compromise level back into your cyberdefense architecture giving you the ability to take actions automatically.

On the other hand, Gartner defines IDPS as "stand-alone physical and/or virtual appliances that inspect network traffic, either on-premises or in virtualized/public cloud environments. They are often located in the network to inspect traffic that has passed through perimeter security devices, such as firewalls, secure web gateways, and secure email gateways."

Intrusion Detection System (IDS) is a legacy technology that was created in the early 1980s with the goal of protecting confidential assets from internal users. Over time this technology pivoted to Intrusion Prevention System (IPS) but retained many disadvantages and limitations, including:

- Focusing on north-south traffic, leaving blind spots in the movement of the attacker within the organization.
- Not being designed to detect evolving threats.
- Only detecting intrusions, but not the context around the compromise.
- Legacy technologies, and as such, there is plenty of information about how to bypass this technology.

How can Lumu and IDPS work together?

If your company already has an IDPS solution like FireEye NX, Alert Logic Threat Manager, McAfee NSP, Cisco, or the like, Lumu seamlessly integrates with your IDPS via our API and low-touch integration apps, while layering real-time compromise assessment. In order to assess compromises effectively, organizations must go beyond signatures, anomaly detection, and heuristics to confirmed indicators of compromise to minimize false positives. It is also important to monitor not only north-south traffic but also the east-west traffic that most IDPS solutions can't monitor.

Lumu adds incredible value to IDPS by providing visibility into the whole network, including lateral movements. According to Gartner "The plethora of breaches continues unabated, which highlights how organizations need to better address the protection of internal assets and improve their ability to detect and prevent the lateral movement of threats."

Also, Lumu alerts only confirmed compromises and not signature-based alerts that have a good chance of being false positives and that are difficult to keep up to date. Lumu is capable of detecting residual compromise on IDPS protected devices that maintain connection attempts with adversaries, hence eliminating the false sense of security.

If you do not have an IDPS 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 Insights includes Compromise Context 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.

How to boost your existing IDPS

Make your IDPS a key instrument in closing the feedback loop between threat detection and incident response. This can be achieved by measuring the outcome of your current cybersecurity stack (i.e. firewalls, switches, routers, and anti-virus, among others) and feeding the information of your organization's unique compromise level back into your cyberdefense architecture.

Since Lumu amplifies your existing cybersecurity tools' value, it provides an API-driven architecture that allows organizations to reduce the impact of cyber attacks, maximize their security team's efficiency, and drastically improve their compromise detection and response efforts. With Lumu, 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

IDPS technology has been present in the market for a long time. However, despite technology providers' attempts to modernize IDPS functioning, it is still unable to provide conclusive evidence of compromise levels, monitor east-west traffic, serve as a compromise detection solution, or confront most of today's cybersecurity challenges. Lumu's patent-pending data collection and analysis process is built to enable organizations to detect threats in real time and to respond to compromises in the most effective way. Lumu achieves this by taking into account much more than just signatures, anomaly detection, and heuristics.

Learn more at: lumu.io/product/