LUMU

# ENLIGHTENMENT BRIEF:
# Lumu & SIEMs

## How does Lumu compare to a SIEM?

Lumu and SIEMs 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 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 adversary infrastructure. Simply put, Lumu identifies confirmed compromises.

On the other hand, SIEMs are built to aggregate a wide range of **event data** and analyze it for security monitoring, long-term retention, compliance, forensic purposes as well as incident investigation, management, and reporting. Although SIEMs have evolved significantly in the last few years to include valuable features to expand its use cases, at its core, a SIEM remains a broad-focus security monitoring tool. As a result, a SIEM's native correlation rules are not designed to intentionally look for compromises.

## How can Lumu and SIEMs work together?

Lumu has the power of amplifying the benefits of a standalone SIEM technology. Lumu enables organizations to maximize their resources by allowing security teams to work more effectively and proactively identify the assets communicating with adversarial infrastructure. Once compromise is identified and contained, security teams may go back to their SIEMs to understand the root cause of each incident, perform forensic investigation and adjust the rules and configurations. With Lumu, companies can add a critical layer to their security strategy by obtaining conclusive compromise intelligence without interrupting the processes already in place.

## Can Lumu replace the SIEM?

SIEMs and Lumu are solutions used to address different challenges. Lumu can add incredible value to an enterprise's SIEM, by pointing out exactly where the compromises are, **reducing alert fatigue and making daily security operations more effective.**

Of note, Lumu is not dependent on a SIEM technology, as it is able to autonomously and systematically collect network metadata for real-time compromise detection. Organizations that have not invested in a SIEM find Lumu sufficient to reduce the impact of cyber attacks, maximize their security team's efficiency, and drastically improve their compromise detection 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

SIEMs may serve organizations in a variety of ways but 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 Illumination Process was designed to perform data collection and analysis, effectively detect compromise, and allow organizations to respond to compromises quickly and precisely via Lumu API to orchestrate the defense.