SentinelOne

SOLUTION BRIEF

Continuous Network Threat Detection and Attack Response

SentinelOne & Lumu Joint Solution Brief

Market Challenges

Responding to pervasive network threats can be complex due to the limitations of legacy cybersecurity tools and technologies. These solutions present high alert rates that often require manual processes and are limited in their ability to properly integrate with other tools. As threat actors are constantly evolving their tactics and techniques, cybersecurity solutions need to be able to respond automatically while continually keeping pace with the ever-evolving threat landscape.

Joint Solution

Lumu and SentinelOne have an automated approach to defend against pervasive threats impacting your organization. SentinelOne provides native behavioral AI detection and autonomous response against threats with broad coverage of device types and operating systems (OS). Lumu offers continuous real-time monitoring to detect malicious activity across networks with detailed context. Through the integrated workflow, organizations are better protected from malicious threats closing the attacker's window of opportunity.

> "
>
> The integration between SentinelOne and Lumu provides comprehensive network security and remediation against active threats. It allows organizations to obtain additional value from their existing tools.
>
> **RICARDO VILLADIEGO**
> CEO of Lumu

How it Works

- SentinelOne Singularity unifies and extends prevention, detection, and automated response capabilities across multiple security layers.
- Simultaneously, Lumu's Illumination Process analyzes collected metadata from various integrations within the Lumu platform for malicious association. When malicious activity is discovered, Lumu measures the compromise level, analyzes the IoC, and adds the hashes to the SentinelOne blocklist.

LUMU

JOINT SOLUTION HIGHLIGHTS

+ Continuously monitor your network for adversarial activity
+ Gain broad visibility into assets impacted by threats
+ Block malicious activity via joint incident response Access Review

INTEGRATION BENEFITS

- Gain relevant context into the most prevalent threats in your network
- Align your cybersecurity stack to quickly remediate threats before they impact your organization
- Easily automate incident response with SentinelOne and Lumu

- Together, the integration combines SentinelOne's industry-leading detection and autonomous response with Lumu's Illumination Process to protect enterprises from threats and malicious actors.

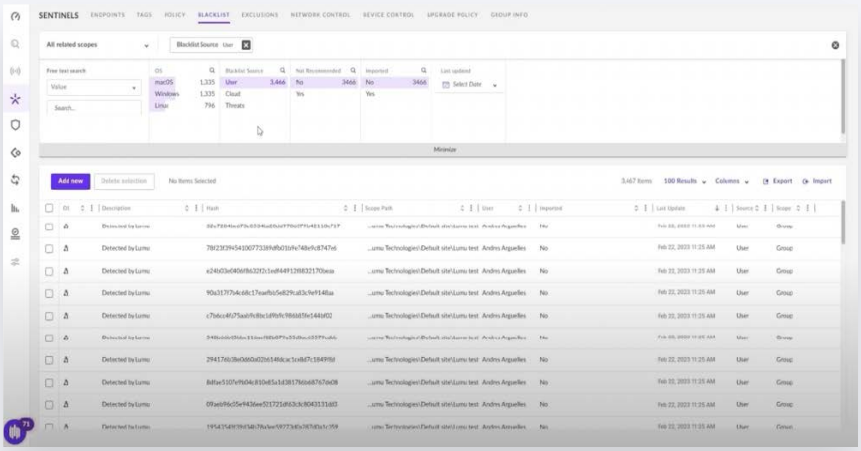

Figure 1 – Malicious file hashes, from Lumu's database, are added to SentinelOne's blocklist.

Solution Use Cases

01. **Workflow Automation:** Automatically measure your organization's compromise level with Lumu and automate workflows based on your needs with SentinelOne. This provides the ability to automate prevention, detection, and response for swift action against active threats.

02. **Secure Remote User Access:** Flexible integration options ensure that your entire user base is protected from targeted network attacks regardless of their work location.

Conclusion/Summary

Network visibility and incident response automation are critical components of a well-structured cybersecurity operation. SentinelOne and Lumu's combined capabilities provides organizations with the benefit of a seamless incident management workflow, saving time and improving the effectiveness of your cybersecurity strategy.

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity Platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

About Lumu

Lumu is a cybersecurity company focused on helping enterprise organizations discover threats and isolate confirmed instances of compromise. Lumu has built a powerful closed-loop, self-learning solution that helps security teams accelerate compromise detection, gain real-time visibility across their infrastructure, and close the breach detection gap from months to minutes.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733