Comprehensive network detection and response for an efficient cybersecurity operation.

SUMMARY

Lumu and Zscaler provide users the ability to seamlessly implement a cybersecurity practice across their organization. These solutions work together to provide powerful protection against malicious activity discovered across the entire network.

Lumu's capabilities provide continuous, real-time monitoring to detect malicious activity across the network. When an attack is discovered, it's reported to the customer with detailed context showing when it happened, who was impacted, and which IoC is associated with the incident.

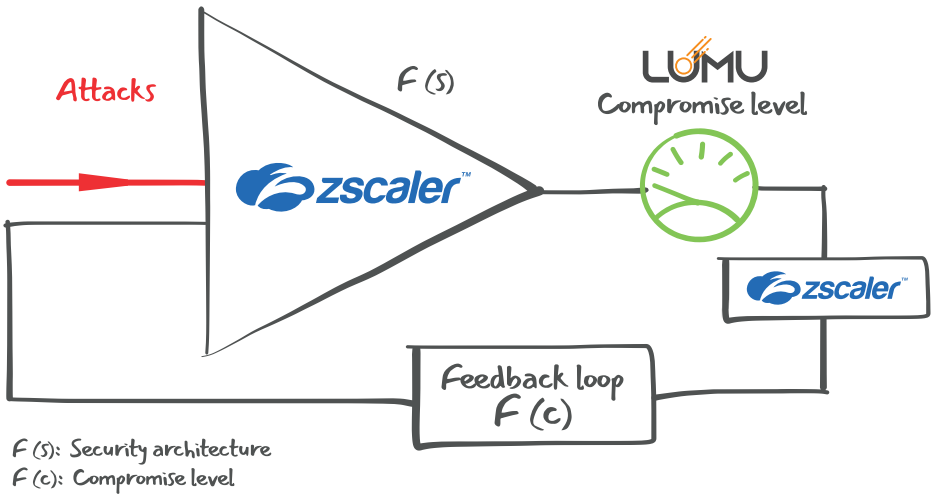
Lumu and Zscaler combine forces, providing powerful capabilities to actively detect and block threats, securing the entire user base before attacks can be fully carried out. This provides augmented network security and remediation against active threats.

BENEFITS

- Expanded network threat detection.
- Continuous, real-time monitoring of the entire network.
- Rich incident context with details surrounding the attack type and asset level visibility to identify the impact.
- Instant attack response, closing the attacker's window of opportunity.

HOW IT WORKS

Metadata is collected through various sources, including Zscaler, and fed into Lumu's Illumination Process where incident data is analyzed for malicious association. If an attack is discovered, Lumu measures the compromise level, does a complete analysis of the IoC, and feeds the incident details to Zscaler for automatic blocking of any connections with this IoC.



USE CASES

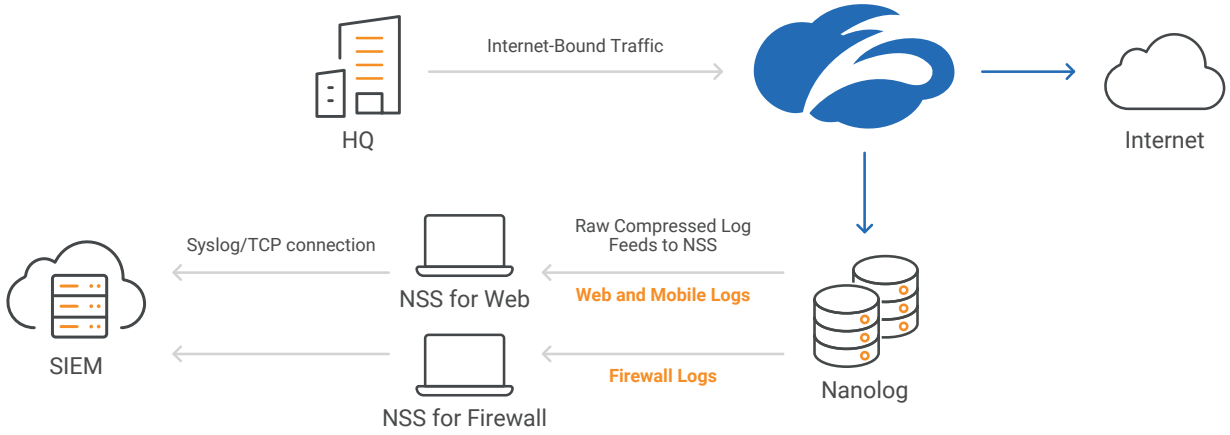
- **Orchestration and Automation:**

  Automate network detection and response for swift action against active threats to ensure malicious network activity is being stopped before it can be fully carried out.
- **Secure Remote User Access:**

  Secure remote users by offering visibility and protection to all Lumu and Zscaler users regardless of their work location.

DATA COLLECTION

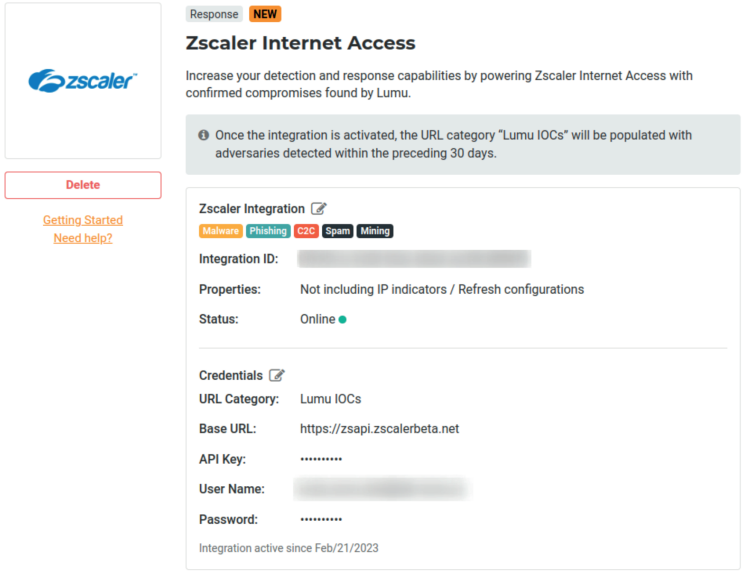
By collecting firewall data from Zscaler, organizations can add another metadata source to identify malicious network activity while leveraging existing sources.



Lumu Event data collection configuration from Zscaler

INCIDENT RESPONSE

Protect your user base from the most pervasive network-based attacks with this out-of-the-box integration. This enables you to continuously feed malicious IoCs discovered within the network by Lumu to Zscaler for automatic blocking of incidents like malware, phishing, C2C, email-based threats, crypto-mining, and more.



The integration is easy to implement and secures the entire user base from network based threats in just a few clicks.