Lumu Defender and Mira Encrypted Traffic Orchestrator Solution Brief

NETWORK DETECTION AND RESPONSE IN ENCRYPTED ENVIRONMENTS

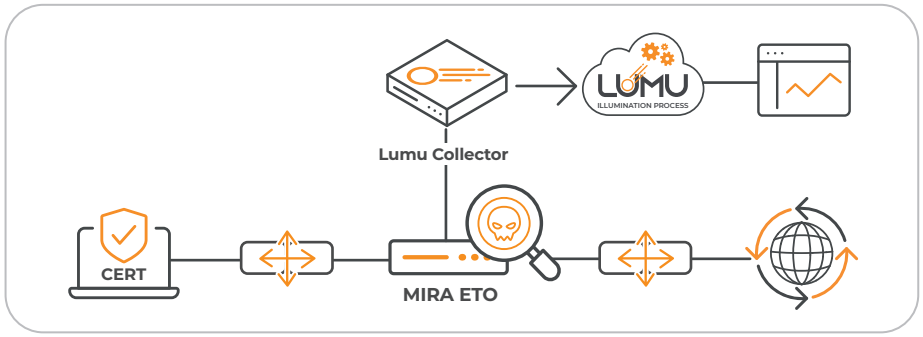
BUSINESS CHALLENGE

In many cases, analyzing metadata provides sufficient visibility, but in certain environments where deeper inspection is required, encryption can create gaps that must be addressed. Malicious actors exploit encrypted traffic to conceal malware, command-and-control (C2) communications, and data exfiltration. Organizations need a solution that restores network visibility while preserving privacy and compliance.

SOLUTION OVERVIEW

Lumu Defender is a high-fidelity Network Detection and Response (NDR) solution that empowers SecOps analysts to maximize the effectiveness of their existing cybersecurity tools. Mira's Encrypted Traffic Orchestrator (ETO) decrypts network traffic, providing Lumu with full visibility into encrypted flows to detect and respond to hidden threats.

HOW IT WORKS



- Mira ETO operates inline, detecting and decrypting SSL, TLS, and SSH traffic in real time. Organizations can fine-tune which flows are decrypted based on privacy or policy considerations.
- Mira generates clear, precise network traffic data, which is then fed to a Lumu collector. The collector forwards relevant data to the Illumination Process™ to detect confirmed compromises in real time.
- Mira ETO and Lumu Defender support various deployment models, including on-prem, virtual, and cloud-based environments, ensuring scalability and future-proof security operations.
- When Lumu identifies a compromise, it triggers an automated response to block or mitigate threats, seamlessly integrating with third-party security solutions to take immediate action.

About Lumu

Lumu enables proficient cybersecurity operations by analyzing network activity in real time to detect and automatically respond to compromises.

About Mira

Mira Security's mission is to provide visibility into network traffic as our customers transition to higher speeds and new architectures, and to eliminate the compromise between privacy and security along their journey. We build lasting relationships with our valued customers and partners and deliver innovative encryption software and products.

SOLUTION BENEFITS

- **Improved Threat Visibility:** Combining Lumu Defender's advanced detection capabilities with Mira ETO eliminates SSL/TLS blind spots, which might otherwise be hidden by encryption. The Mira ETO, while being a port-agnostic appliance that allows decrypting on more than just port 443, can handle decrypting SSL v3, TLS 1.0, 1.1, 1.2, and 1.3, as well as SSHv2.
- **Enhanced SecOps Efficiency:** Greater visibility and more precise threat detection empower security teams to operate more effectively, reducing alert fatigue and streamlining incident response.
- **Comprehensive Network Security:** Strengthens network defenses by addressing encrypted traffic challenges and enhancing NDR capabilities.
- **Regulatory Compliance Support:** Helps organizations meet deep packet inspection (DPI) and encrypted traffic analysis requirements while also protecting sensitive data via Mira's ETO rules and filtering options, which allow bypassing the decryption of specific categories of traffic.
- **Seamless Integration with Security Tools:** Lumu Defender integrates with SIEM, XDR, SOAR, and firewall solutions, enabling automated, responses within milliseconds.
- **Ease of Use:** Easy to install, configure, and integrate with other elements of the enterprise security monitoring and analysis infrastructure.

USE CASES

- Intercept early-stage encrypted C2 traffic to prevent ransomware attacks.
- Enhance threat hunting with decrypted network insights.
- Prevent data exfiltration by identifying encrypted insider threats.
- Support forensic investigations with decrypted traffic insights to trace attack paths.

8600 NW 36th St., Suite 150
Doral, FL 33166
sales@lumu.io
+1 (877) 909-5868