Continuous Compromise Assessment™

The Pervasive False Sense of Security

Despite billions of dollars being invested in cybersecurity, we continue to see an increase in the number of data breaches. The fact is, breaches still happen because the adversary is often already inside the organization doing unsupervised damage and making current testing practices insufficient. All cybersecurity investments are meant to avoid compromises, so why are we not measuring compromises to find out how the system is performing? Why are we not continuously improving cybersecurity systems with metrics?

The Power of Lumu:

- Extended Detection and Response
- Automated Threat Hunting
- Secure the Remote Workforce
- Combat Alert Fatigue

Key Facts:

- In 2020, the average time to detect and contain a breach was 280 days.
- Between 2015 and 2019, enterprises deployed $670 Billion on cybersecurity.
- The number of breaches grew from 781 in 2015 to 1108 in 2020.

The Answer is in Your Own Network Metadata

All attacks have a common denominator: the threat actor must use the network to compromise an organization. Therefore they leave behind a trail of evidence that Lumu follows by looking at a comprehensive array of metadata sources.

DNS Queries

When a device is compromised, it will resolve a domain that belongs to adversarial infrastructure, offering concrete compromise evidence.

Proxy and Firewall Logs

If the attack does not use DNS infrastructure, its only other option is to connect directly to an IP address.

Email

Threat intelligence across your email platform helps us analyze who is targeting your organization, how they are doing it, and how successful they are.

Network Flows

Collecting Netflows is completely optional but it's another source that can be utilized to gain information about an adversary's objectives.

How it Works

Lumu's Illumination Process is the core enabler of Continuous Compromise Assessment™ that correlates network metadata with known IoCs and AI, and results in actionable, confirmed compromise evidence.

Key Features

Confirmed Compromise Intelligence

Detailed, real-time compromise intelligence on how enterprise assets are communicating with adversary infrastructure.

Incident Grouping

Simplified compromise management by grouping related contacts into a single incident, for fewer alerts and reduced noise.

Cloud-based Delivery

Cloud-based model allows for accelerated deployment and immediate positive ROI.

Automated Response

Respond quickly and precisely. Integrate real-time information about confirmed compromise instances with your existing tools via API to orchestrate your defense.

Compromise Context

Robust context around confirmed compromise incidents that enables teams to enact the precise response in a timely manner.

Diverse Metadata Ingestion

Collect network metadata your way. Choose from a wide range of metadata collectors, including virtual machines, agents, or API collectors.

Playback™

Patent-pending capability that reviews up to 2 years of network metadata traffic and compares it to new known IOCs.

Custom and Out-of-the-box Integrations

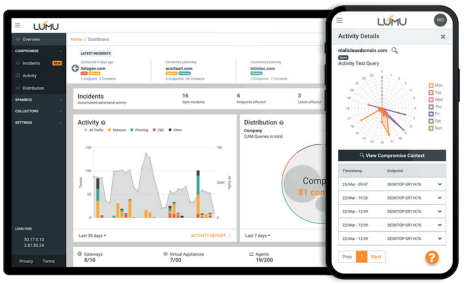
Take advantage of vendor-agnostic integrations, so you can use Lumu's threat intelligence where it's needed most.

> *"Medium-size to large enterprises looking for an easily consumed but highly capable NAV product should take a hard look at Lumu."*
> **- Forrester NAV Wave Q2 2023**

> *"While not dependent on the availability of a SIEM tool, Lumu adds a critical layer to a security strategy by providing conclusive compromise intelligence without interrupting existing processes."*
> **- Gigaom Radar Network Detection and Response, August 2023**

Your **FREE taste of Continuous Compromise Assessment™** is just a few clicks away!

Open your account at
https://portal.lumu.io/account/sign-up



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