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, it's only other option is to connect directly to an IP address.

Network Flows
Network flows provide insightful information into an adversary's objective and attempts to move laterally.

Spambox
Blocking spam is good, but analyzing it is better because you can discover who is targeting your organization, how they are doing it, and how successful they are.

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.

"Lumu's NTA (Network Traffic Analysis) is unique and comprehensive. CISOs looking for security analytics and operations help may want to seek out Lumu and evaluate how Lumu can help them with Continuous Compromise Assessment."
- ESG Showcase Report

"Lumu's distinctive approach rethinks the conventional security paradigm, one that has spent billions of dollars trying to keep attackers out of key enterprise networking assets. Instead, Lumu makes the assumption that cybercriminals are already lurking inside - as is all too often the case"
- EMA Vendor to Watch Report
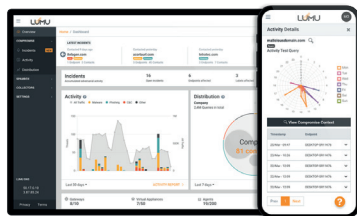
Your **FREE** taste of Continuous Compromise Assessment
is just a few clicks away!

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