Lumu Insights

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 due to an important, yet neglected truth: the adversary is often already inside, while current testing practices are insufficient. This results in the adversary going undetected for long periods of time and doing irreparable damage to the enterprise. If all cybersecurity investments are meant to avoid compromises, why are we not intentionally and continuously measuring them?

The Power of Continuous Compromise Assessment:

- Intentionally and continuously looks for compromises
- Operationalizes indicators of compromise
- Expands cybersecurity testing practices
- Tests cyberdefense strategy effectiveness

Key Facts:

- Data breaches have surged 88% from 2014 to 2019
- Cybersecurity spending is projected to have grown by 57% from 2014 to 2019
- In 2019, an attacker avoided detection for an average of 206 days

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.

Compromise Context

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

Compromise Radar

Powerful visualization tool that reveals attack patterns, conditions, and behavior.

Spambox Report

Unprecedented intelligence on who is targeting your organization, how they are doing it, and how successful they are.

Cloud-based Delivery

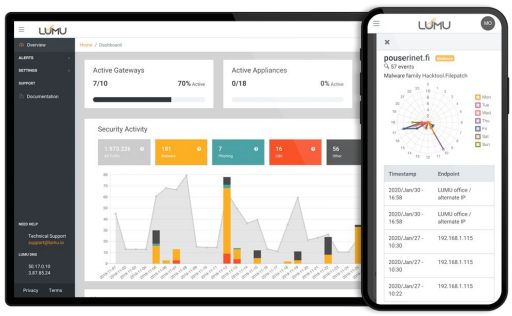
Cloud-based model allows for accelerated deployment and immediate positive ROI.

Playback™

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

> *"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

Lumu Technologies Inc. | 8333 N.W. 53rd Street Suite 450 Doral, FL 33166 | sales@lumu.io | +1 (877) 909-5868