How Continuous Compromise Assessment Is Changing SecOps Strategy

Lumu's Ricardo Villadiego on Gaining Visibility Across Identity, Cloud and Networks

Attackers now evade traditional defenses by using valid credentials and trusted tools, reducing alerts and masking activity, said Ricardo Villadiego, founder and CEO at Lumu Technologies. Security stacks remain valuable but lack visibility into active compromise. This gap limits detection when adversaries operate inside networks without triggering alarms.

Villadiego said organizations need a unified approach that identifies compromise across network, identity, cloud and endpoints. Lumu's model focuses on delivering a clear signal of compromise. This enables security teams to act with precision. Identifying compromise matters more than its origin, helping teams reduce noise and improve response.

"The way I like to put it is Lumu gives you the exact coordinates to all these signals that you have to where the adversary is, so that you can hunt them and take them down," Villadiego said.

Continuous compromise assessment shifts security strategy from prevention to rapid detection and action. This approach helps CISOs prioritize real threats and improve outcomes from existing tools. By acting as a decision layer, Lumu Technologies' solution enhances visibility without adding complexity, enabling faster and more confident responses, he said.

In this video interview with Information Security Media Group at RSAC Conference 2026, Villadiego also discussed:

- The evolution from malware-driven attacks to credential-based intrusions;
- Reducing alert fatigue through precise compromise identification;
- Enhancing existing security tools with a decision-focused layer.

Villadiego leads a cybersecurity company focused on helping organizations detect compromises faster. With 20 years of experience, he specializes in cyberthreat detection, fraud prevention and security strategy. He previously founded Easy Solutions and led the cybersecurity business unit at Cyxtera Technologies.

"The market is living in an age in which compromise has become more prevalent, and we have the commitment to help customers identify compromise whether it is coming from the network, from identities, cloud environments, or endpoints."

- Ricardo Villadiego, Founder and CEO, Lumu Technologies

A Post-Malware Threat Landscape

MICHAEL NOVINSON: Your 2026 Compromise Report suggests we are entering a post-malware era where attackers are logging in rather than breaking in. Is the traditional security stack essentially blind to this change?

RICARDO VILLADIEGO: When you look at the findings in the 2026 Compromise Report, what we identify is that adversaries are being very smart about evading the stack that is in place: evading EDRs, evading identities through compromised credentials, using the same cloud tools organizations use day-to-day to exfiltrate data. When that happens, the stack goes quiet. No alerts are generated. I would not say the stack is obsolete. I would say the stack is incomplete. It is lacking the layer that provides awareness that the adversary is within the network. That is where Lumu comes in to help.

A Single Source of Truth for Compromise

NOVINSON: Lumu is well known for providing ground truth in the network. Now that you are moving into more of a full stack covering network, identity and cloud, is the goal to create a single source of truth for compromise regardless of where it starts?

VILLADIEGO: My commitment to customers and to the market is to solve the problem. The market is living in an age in which compromise has become more prevalent, and we have the commitment to help customers identify compromise whether it is coming from the network, from identities, cloud environments, or endpoints. It is less relevant where the compromise is coming from and more relevant that you have the ability to identify signals of compromise in your environments. That is how Lumu is evolving from the network to include other signals: to provide the same approach that has built Lumu into a unique offering in the space and give customers an unequivocal signal of compromise that helps companies become decisive in operating cybersecurity.

Continuous Compromise Assessment

NOVINSON: How is continuous compromise assessment a game changer?

VILLADIEGO: It is changing mindset. Traditionally, companies have deployed defenses under the premise that you are going to keep the adversary out. But history has told us that the adversary always finds a way in. It is better to embrace the concept that you have the ability to identify when the adversary is within the network.

That becomes a game changer in the sense that when security teams have the clarity to filter through the noise, when the thousands of alerts they receive on a daily basis are associated with actual compromises, they become proactive

and decisive in taking the actions needed to keep the environment safe. It helps companies operate in a more proactive and effective way, and in a way that does not require them to constantly chase fixes to change the stack. Lumu helps them provide more value from the cybersecurity stack they already have.

Cutting Through Alert Noise

NOVINSON: How does Lumu Defender use its continuous compromise assessment model to filter that noise and tell a CISO exactly which identity or endpoint is compromised right now?

VILLADIEGO: One of the biggest problems CISOs and security teams face is the number of signals they have to chase and investigate. For a long time, they have been drawn into signals of maybes: this device may be exhibiting suspicious behavior, these cloud environments are behaving strangely, these endpoints need investigation. And with the increase of agentic traffic within networks, that is only going to generate even more signals for security teams to investigate.

The value Lumu adds to that equation is to tell security teams exactly which signal has to be investigated because that endpoint or identity is exhibiting behavior associated with past compromises Lumu has identified, or is making contact with known threat and adversarial infrastructure outside the organization. It makes security teams decisive in how they take action and secure their environment. Lumu gives you the exact coordinates through all those signals to where the adversary is, so that you can hunt them and take them down.

A Decisioning Layer, Not Another Dashboard

NOVINSON: Unified visibility is a popular message at RSAC this year. How do you convince a CISO who has already invested heavily in separate tools for endpoint and identity that adding Lumu's layer will not just create another dashboard to manage?

VILLADIEGO: They should be rightly skeptical. There are many companies that have offered the idea of unifying threat visibility into a single dashboard. Lumu does not provide another dashboard to investigate. Lumu is a decisioning layer. We are not here to replace your EDR, your firewalls, or your identity tools. Lumu is a complement to that stack, and a complement that helps the stack perform significantly better. You obtain additional return on investment from the tools you already have. Lumu is a decisioning layer that helps you cut through the noise, identify when a signal is worth acting on, and mitigate the potential catastrophic effect that can come from a missed alert.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of its 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Its annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY® (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP