Research Report

Enterprise Cyber-Crime

Misplaced trust in the current generation of network visibility technology creates opportunities for cyber criminals to exploit systems.

Lumeta, one of the nations top security firms hired LTM Research to interview over 100 corporate security officers and learned that organizations that had deployed the following technologies were facing risks and breaches they never expected.

Prescriptive technologies employed by respondents:

- Real-time assessment of threats from an outsider perspective
- Security validation procedures (with high confidence levels)
- IPAM based authentication of information and systems on the network
- Anomaly screening against baseline normal activity
- Monitor communication patterns against routing tables to identify anomalies

Despite "Industry Standard Protections," the same respondents reported that:

48%

69%

65%

1) In 48% of cases comprehensive security intelligence was not available across the network
2) 69% of security breaches were detected by suppliers, customers, or law enforcement
3) 65% of respondents could not track fast moving threats emanating from transitory assets

Currently, the mean time before a network security breach is even detected is **205** days!

We invite you to attend our research presentation where we will demonstrate why the perception of security is vastly different than the empirical reality.

Please contact us to set up a presentation today.

Paul Ludwig
Project Manager
Lead to Market Research
A Division of Unee Solutions
520-579-8458 (Direct)
pludwig@leadtomarket.com

Lumeta®
Network Situational Awareness