Lumeta ESI

SOLUTION BRIEF

As Banking Regulators Pursue Improved Resiliency & Cybersecurity Preparedness Real-time Network Visibility Takes Center Stage

Financial institutions affected by heightened Federal Reserve, FDIC, OCC & FFIEC cybersecurity standards deploy Lumeta ESI to hunt breaches and identify IT network infrastructure anomalies in real time

Banking and financial institution cybersecurity risks continue to escalate for a number of reasons including greater interconnectedness and increased sophistication of cyber threats. Instabilities to the financial system caused by these heightened risks is making **cybersecurity** a top priority for the Federal Reserve Bank, Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC). And that means U.S. national banks, federal savings associations, and federal branches and agencies should **be prepared for heightened focus by OCC and other regulators in this critical area**. Already regulators have proposed that the largest banking organizations with greater than $50B in assets must establish and implement plans that would allow them to continue core business functions during a cyberattack.

For the broader classification of financial institutions, the Federal Financial Institutions Examination Council (FFIEC) has issued a Cybersecurity Assessment Tool (Assessment) that institutions may use to evaluate their risks and cybersecurity preparedness. OCC examiners will incorporate the Assessment into examinations of **national banks, federal savings associations, and federal branches and agencies (collectively, banks) of all sizes – including community banks –** to determine a bank's ability to detect, prevent and respond to cyber threats. Among other things, the Assessment evaluates a bank's network devices (e.g., servers, routers, and firewalls; including physical and virtual), the use of cloud computing services, personal devices allowed to connect to the corporate network, and third-party access to internal systems. It looks to see that the enterprise network is segmented into multiple trust/security zones, all ports are monitored, threat intelligence is in use to discover cyber threats, and that continuous, automated monitoring is in place.

While it may be stating the obvious, it is impossible to protect a network or even evaluate its cybersecurity state if the full extent of the network infrastructure is not well understood, in real time. Financial institutions are turning to Lumeta ESI – Lumeta's platform for **real-time** network visibility, delivering breach detection, network infrastructure analytics and network segmentation analytics –to evaluate and hunt for core **network infrastructure security concerns**.

Breach Detection

Hunting for anomalous behavior like unauthorized (zombie) communications flows to known bad actor sites

Network Segmentation

Hunting for leak-paths to the Internet or in between fire-walled enclaves

Network Infrastructure

Hunting for dynamic changes to the network edge and changes caused by virtual, cloud, mobile assets on your network

Lumeta ESI monitors the network infrastructure in real time. It provides an authoritative index of all network connections and devices (including unknown networks, the 'edge' of a managed network, and physical, virtual, cloud, mobile assets), identifies devices joining and leaving the network, and uncovers possible segmentation leak paths.

Developed in conjunction with OCC-regulated clients, Lumeta ESI inserts itself into the network control plane and uses active and passive indexing techniques to evaluate network state in real time. Real time is required in today's cloud, virtual, mobile and software defined world. Traditional static or scan-based "network management", "performance management", "modeling" or "discovery", tools that require "credentialed" access to evaluate network infrastructure will always miss the unknown, dynamic or rogue infrastructure that malicious actors will embed on the network to cause chaos or pursue fraudulent activities.

Product Category	Breach Can it hunt & locate active zombie sessions to C&C botnets?	Infrastructure Can it find the real time state of a dynamic network edge altered by virtual, cloud?	Segmentation Can it find active leak-paths to the internet or between internal networks?
Lumeta ESI	Yes	Yes	Yes
Host VA scanner	No	No	No
NMAP scanner	No	No	No
NAC	No	No	No
IPAM	No	No	No
Network Modelers	No	No	No

Furthermore, Lumeta ESI leverages an embedded Hadoop Distributed File System to enable ingestion of new indexing triggers like threat intelligence (Verisign or open source, etc.) and to provide network state metadata to existing vulnerability assessment (Qualys, Tripwire, Tenable, Rapid7, etc.), network modeling (RedSeal, etc.), endpoint detection and response – EDR (McAfee, CarbonBlack, Tanium, etc.) or enterprise security data lakes (Splunk, Hadoop). These ecosystem integrations allow accurate network state metadata to be used to enable precise real-time action by these elements of the cyber security stack and to orchestrate faster remediation of anomalies that may lead to a breach.