Lumeta IPsonar

DATA SHEET

Network Situational Awareness via Recursive Network Indexing

To properly manage and secure a network, IT managers need authoritative intelligence about their network infrastructure and cybersecurity posture. Lumeta® IPsonar® provides a point-in-time view of every IP connected device on a network, as well as inbound and outbound leak path identification.

Lumeta's network situational awareness platform is the authoritative source for network infrastructure and cybersecurity* analytics.

Lumeta IPsonar provides comprehensive visibility into the entire routed infrastructure of a network via recursive network indexing – performing an active probe and mapping every IP asset, host, node and connection on the network. The data is then analyzed to understand policy violations and security vulnerabilities.

How It Works

Through recursive network indexing, IPsonar identifies the network perimeter, network topology and devices that encompass a company's infrastructure. It utilizes the following methodologies:

- ✔ Network protocols (learning network information via SNMP, TCP, UDP, DNS, HTTP, HTTPS, ICMP)
- ✔ Port responses (determining the services running in the network)
- ✔ Network packets (understanding the connectivity of a network via sending lightweight, standard, properly formed packets throughout the network)
- ✔ Network path tracing (reaching for devices within the network via tracing data paths)

What is recursive network indexing? If, for example, IPsonar finds a new router, one that wasn't previously known to the established scan, it will then drill into that new network device to assess what it is attached to, pull route tables, etc.

IPsonar provides a point-in-time view of a network, often used in compliance audit situations. It is also often used to provide a network 'baseline' for M&A activities or in the case of a new IT executive taking over the security and management functions of a network.

Highlights

- ✔ Lumeta IPsonar provides a clear understanding of entire routed infrastructure and confirmation that all assets are under security management.
- ✔ Patented leak path identification reveals unauthorized connections between the enterprise and another network, between segregated subnets, as well as unwanted connectivity between the network and the Internet, determining whether connectivity is outbound, inbound, or both.
- ✔ Device profiling using credential-less identification of attached endpoints.
- ✔ Authoritative census of attached devices for vulnerability scanning.
- ✔ Inventory of all SSL certificates, including issuer, signing authority and expiration date.
- ✔ Identification of potentially vulnerable (open) TCP ports for more targeted vulnerability scanning and patch management.
- ✔ Lightweight indexing/scanning techniques avoiding detection by IDS/IPS systems.
- ✔ Powerful dashboards that can be configured to present the most relevant data more effectively, at a micro- or macro-level. For instance, dashboards can be created for IT audit and regulatory preparation or for executive management reporting.
- ✔ Lumeta Network Index allowing for best practices based scoring (risk metrics) of IPsonar results.
- ✔ Network map detailing the topology, including routers and switches that define the network perimeter.
- ✔ Scales to handle the largest global networks.

*Refer to the "Operationalizing Threat Intelligence using Lumeta IPsonar plus Cyber Threat Probe" Solution Brief for cybersecurity use cases.

IPsonar Intelligence

Recursive network indexing and the various IPsonar scans provide intelligence regarding network segmentation and network architecture: What network enclaves are able to reach others? What are the 'unknowns' in the network? What does the network really look like? What devices are attached to the network and how? Does this violate policy?

Network Segmentation Analytics – advanced intelligence needed to verify network segmentation and understand the network architecture relative to an organization's policy

Leak Path Identification:

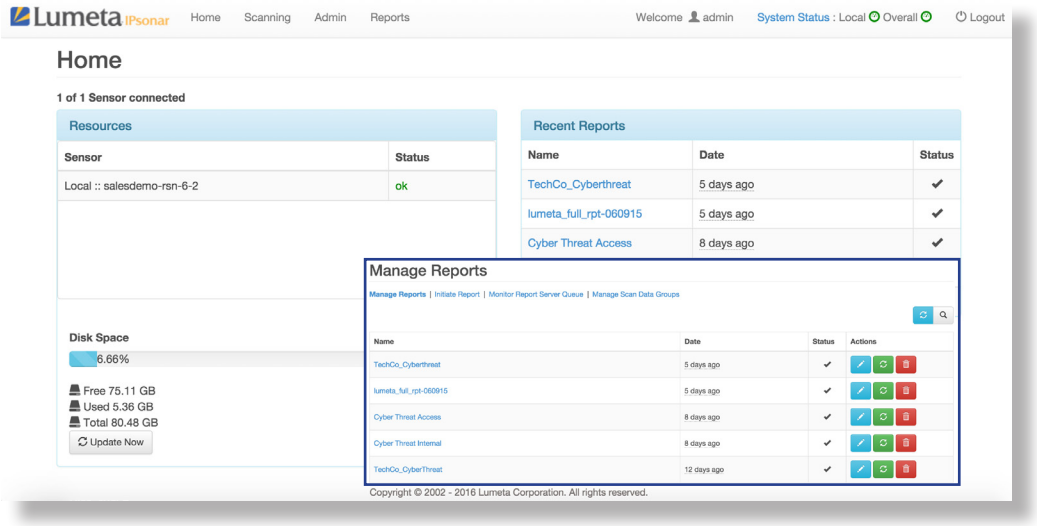
- Unauthorized Internet Connectivity
- Multi-homed Host Identification
- Split Tunneling Identification
- Unauthorized Bridging Device Identification
- Hybrid Physical/Virtual Segmentation

Unknown Network Identification:

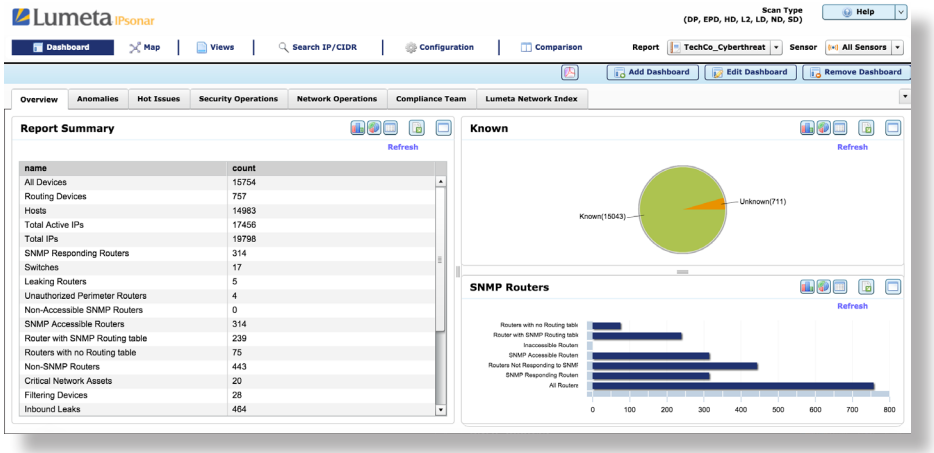
- Forwarding Device Census
- Rogue Network/Forwarder Identification

Network Architecture Analytics – a true view of what the network really looks like (what devices are attached to the network, and how)

- Authoritative Network Census
- Address Space Validation
- Network Edge Definition
- Unreachable Network Segment Identification
- Device Indexing/Profiling
- Enterprise-wide Certificate Identification
- Network Topology Mapping
- Port Mapping/Usage



Lumeta IPsonar Home page with Reports overlay



Lumeta IPsonar dashboard overview showing device counts by characteristic, known vs. unknown devices, and data on SNMP-responding routers

IPsonar Scan Types

Lumeta IPsonar actively scans the network to collect all data related to Network, Host, Service, Leak Path, Layer 2, and Perimeter. IPsonar also uses Device Profiling techniques to identify the type, vendor, model, operating system, and version of devices on the network. Users can accurately visualize what is on the network, drill down to analyze potential areas of risk, and identify appropriate corrective actions.

Network Discovery – Network Discovery gathers information about the network connectivity, leading to the identification of routing devices (including IPv6-enabled routers) and their interconnection, the network perimeter and topology, and, in general, the assets and stealth devices.

Host Discovery – Host Discovery identifies all IP addresses that respond, in one way or another, to network protocols. Host Discovery is a very important step as it leads to the creation of a Target List that is further targeted to understand device profile and details (Service Discovery and Leak Path Discovery).

Service Discovery – Service Discovery scans the ports of devices to identify vulnerable or infectious ports that may be open. One of the most common reasons that organizations fail a compliance audit is the inability to report on and secure open ports. IPsonar's Service Discovery scans and reports across all ports, addressing audit issues. This data can be further analyzed within the context of IPsonar's deep and broad network intelligence.

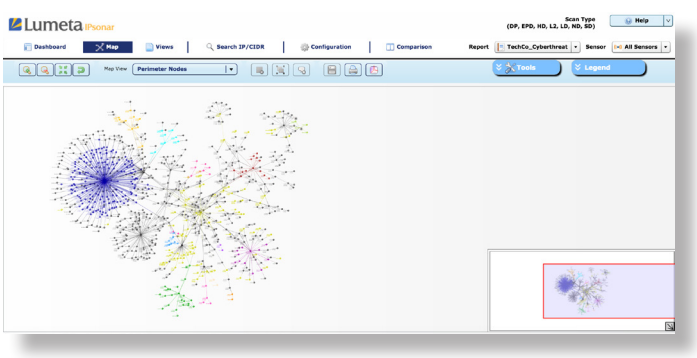
Leak Path Discovery – Leak Path Discovery verifies that no Layer 3 devices within the network are leaking to or from the Internet or other segmented portions of the network. This scan shows any device that has direct connectivity to the Internet or a device that has an inbound/outbound connection through the network perimeter.

Layer 2 Discovery – Layer 2 Discovery finds endpoints, SNMP-accessible switches, hubs, and bridges that are attached to SNMP-accessible routers.

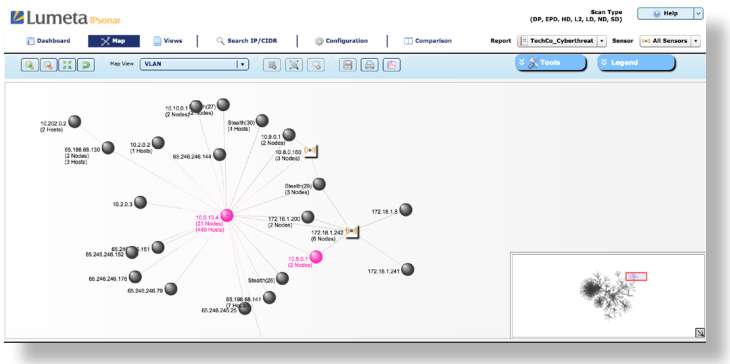
Device Profiling – Device Profiling helps determine the device type, hardware, model, vendor and operating system of all devices that have been indexed by IPsonar. Device Profiling is performed via various methodologies:

- Looking for device information via SNMP protocol
- Gathering HTTP/HTTPS responses
- Determining the type of device via the combination of running services
- Identifying windows devices via CIFS protocol and TCP pattern matching

Enhanced Perimeter Discovery – Enhanced Perimeter Discovery helps find Layer 2 attached devices that forward traffic (just like endpoints, routers or switches) so that they can be further investigated for forwarding traffic to unknown, unauthorized or untrusted networks.



Lumeta IPsonar maps in Perimeter Nodes view



Lumeta IPsonar maps in VLAN view

Alerting

IT administrators can receive email alerts on events that meet or exceed a severity tolerance threshold. Alerts are available in a twice-daily digest form or individually, as they are identified in near real time – empowering users to respond immediately to incidents and vulnerabilities.

Scalable to the World's Largest Networks with Multi-tier Enterprise Architecture

Lumeta IPsonar is available in a Cloud or Virtual Machine deployment.

IPsonar does not disrupt operations in order to completely scan a network - no matter how far-flung or numerous the resources are. IPsonar scales to handle large data sets as easily as it does small data sets. Thus, IPsonar is a true enterprise application, able to work efficiently in both large and small deployments.

IPsonar's three-tiered architecture is proven at the world's most complex networks and has been used to scan the entire Internet:

- ***Sensors:*** Accurate, complete network scanning is achieved through the use of network entry points called Sensors. These entry points are portable, providing flexibility to address even the most fast-changing networks. Sensors provide "scan and send results" functionality, sending results back to either a Scan Server or a Report Server.

- ***Scan Servers:*** These resources are positioned at appropriate points in the network to assure that business applications and even the lowest-speed network links are unaffected by IPsonar network traffic. Multiple scans can be run simultaneously. Scan Servers provide "scan and store" functionality.

- ***Report Servers:*** A full package, a Report Server provides the functionality to scan the network, analyze the scan data, and display the report based on the analysis. A single remote Report Server can support multiple Scan Servers.

Communication between IPsonar components is via HTTPS (SSL), so no changes to firewalls or network access control are required. The user interface supports signed digital certificates.

The number of systems required, and software-licensing costs depend on the size, complexity and segmentation of the network. A Lumeta consultant will work with you to determine the best architecture and product configuration for your environment.

Plugin Framework for Technology Partner Ecosystem

The intelligence gathered by IPsonar is a necessary foundation for comprehensive network situational awareness. It can be used in conjunction with an organization's existing security and network management tools, such as vulnerability management (VM), security incident and event management (SIEM), intrusion prevention systems (IPS) and network access control (NAC) – enhancing the value of an organization's investment in those products. Network, security and compliance products can only be fully effective when operating with 100% network visibility.

IPsonar contains a framework for embedding plugins with third-party products to facilitate integration. This allows customers to feed the IPsonar authoritative network intelligence directly into third-party integrated applications. Plugins are available on the Lumeta Support site for download.

Lumeta Corporation | 300 Atrium Drive, Suite 302 | Somerset, NJ 08873 USA | +1.732.357.3500 | www.lumeta.com

© 2016 Lumeta Corporation. All rights reserved. Lumeta, the Lumeta logo and IPsonar are registered trademarks of Lumeta Corporation in the United States and other countries. All other trademarks or service marks are the property of their respective owners.