Enterprise Situational Awareness

You can attain a real-time, dynamic view of your network infrastructure using Lumeta® ESI. Running in an always-on mode, ESI delivers next-generation network discovery, leak path detection, visualization and analytics to provide network situational awareness – including awareness of an organization’s presence in private, public, and hybrid clouds. ESI is for organizations in government, finance, high tech, energy, power grid, healthcare, insurance and manufacturing where network vulnerability assessment is critical.

It can be a daunting undertaking to keep track of network change. Change is constant. Traditional perimeter security methodologies are challenged by Cloud, BYOD and mobility programs, as well as a growing number of cyber-threats. Evolving network architectures such as Software-defined Networks (SDN) are rapidly increasing network complexity. M&A, consolidation and outsourcing programs are accelerating the speed of change within the enterprise.

The need for real-time, accurate network situational awareness is vital for any security risk management program. The ultimate goal is to:

- Identify and monitor 100% of network connections and devices
- Understand all aspects of the network environment – physical, mobile, virtualized, cloud (private, public and hybrid)
- Expose potential problems, such as unplanned Internet connections, unmanaged devices and unsecured ports
- Monitor in real-time for instant visibility – and quick response

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

Lumeta ESI delivers foundational intelligence to power real-time network situational awareness of the entire enterprise. It automatically discovers the entire enterprise and creates comprehensive, detailed network topology maps – in real-time. ESI yields accurate network and device intelligence, while issuing alerts and notifications as the enterprise changes and evolves. This foundational intelligence is a critical underpinning for network vulnerability management strategies to be truly effective.

### Highlights

- Aligns with Continuous Monitoring (US) and Protective Monitoring (UK) security programs.
- Combined active scanning and passive listening techniques provide the most comprehensive, accurate, best-of-breed results.
- Highly scalable to accurately discover the largest networks.
- Lightweight, causing little to no impact on network performance.
- Zones give flexibility to partition and organize discovery.
- Visualize complex network topology maps in real-time.
- Real-time notifications flag departures from the network steady state, facilitating immediate remediation of out-of-policy events and network vulnerabilities.
- Real-time leak path detection.
- ESI can be configured to test the security posture of IPv6-enabled devices to ensure they are properly configured and to detect possible vulnerabilities.
- Lumeta Network Index allowing for best practices based scoring (risk metrics) of ESI results.
- Integration with third-party products to maximize their results and value.
ESI Intelligence via Multisource Identification Techniques

Lumeta ESI uses a unique “always on” technique to produce comprehensive network visibility – a continuous recursive cycle of targeting, discovering, tracing, monitoring, profiling, and displaying of a network.

- Passive Discovery (listening) is agent-less, with no impact to the network. ESI largely relies on ARP traffic and the routing plane and uses route analytics / routing protocols and traffic monitoring (DHCP, etc.).

- Active Discovery (scanning) is a benign exploration that’s especially useful in identifying a network’s perimeter. ESI sends packets to a surmised target, and learns from the target’s response. Active discovery continuously incorporates data uncovered via passive discovery, yielding the broadest and most comprehensive results in the industry. This is largely achieved using TTL and multiple protocol ping.

- Targeted System Inquires (device profiling – or system access) is the close inspection of a known device or entity. It uses SNMP, and includes Port Discovery and DNS Lookups. Targeted discovery leverages the intelligence accumulated from ESI’s hybrid active/passive approach to discovery to provide rich data gathered from network equipment.

ESI uses advanced profiling techniques that detect newly connected devices and previously unmanaged assets. ESI automatically detects changes to the network topology, alerts of possible security policy violations and network vulnerabilities in real-time, and documents network changes for regulatory compliance. ESI identifies events or configurations linked to adversarial or anomalous conditions at the enterprise level. Recursive network indexing and the various multisource identification techniques used by ESI 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?

Real-time 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

Real-time 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
- Real-time Network Infrastructure Updates (Broadcast, OSPF, BGP, etc.)
- Address Space Validation
- Network Edge Definition
- Unreachable Network Segment Identification
- Device Indexing/Profiling
- Enterprise-wide Certificate Identification
- Network Topology Mapping
- Port Mapping/Usage

What Does ESI Identify?

Discover the Network – ESI maps the entire enterprise, discovers all networks and connections – including previously “unknown” portions of the network – and defines the network perimeter, partner connections, and cloud connectivity. It provides an integrated OSI Layer 2 / Layer 3 understanding of the network infrastructure.

Discover the Hosts – ESI takes a census of all active devices (including IPv6 enabled network devices) attached to the network and finds “stealthy” devices.

Profile Devices – ESI identifies the types of devices connected to the enterprise, highlighting those devices that fall outside of policy or are considered “rogue” in nature.

Discover Network Leak Paths – ESI reveals connectivity between networks (business units, partners, spin-offs, secure zones, etc.), or the corporate enterprise and the Internet. Through this intelligence IT professionals can determine whether the connectivity is authorized, or if proper security controls are in place.
Steady state – Upon initial deployment of ESI, a baseline of normal network behavior is established over a short period of time. This baseline describes the network’s steady state – that range of behavior indicating health and normalcy on the network. Once certain parameters have been defined as normal, ESI continuously monitors and flags any departure from one or more of them as anomalous.

Progress to auto-pilot – As new infrastructure elements are discovered, results are automatically tuned and refined. Discoveries trigger new threads of collection activity. The raw data backing map nodes is automatically updated. Maps refresh to display newly discovered entities. IT professionals are alerted to precisely those network events that merit attention. All in real time. All continuously.

Visual Analytics

Zone Segmentation – Create discovery zones, with individual rules and policies, to partition the continuous monitoring of security controls for compliance with regulatory and internal information security policies. This allows for discovery of enclaves, segregated networks, overlapping IP spaces, and more. Zones can be as simple or as complex as defined by an organization and can be comprised of logical networks and subnets, regardless of where they are physically deployed around the world (e.g., geographic zones, business unit / mission zones, corporate/guest/partner zones).

Enterprise Dashboard – Provides comprehensive visibility into the entire network infrastructure – including data about network connections and devices. When new devices connect to the network, IT professionals are notified via the dashboard, in real-time. The dashboard consolidates and communicates relevant security status in real-time, translating raw data into actionable information, (e.g., policy compliance and anomaly alerts). The dashboard can be zone-specific or can provide a consolidated view of all zones.

Dynamic Mapping – An interactive network topology map enabling global visibility across the enterprise – from high-level to specific devices. The map updates in real-time as the network changes.

Robust Reporting – Real-time reporting tools track network asset information and quickly identify changes in the network infrastructure. Next-generation reports include compliance reports and custom reports – all with drill-down capabilities.
IPv6 Support
IPv6 Discovery passively monitors ICMPv6/NDP traffic, the OSPF routing infrastructure and finds network paths and devices via active discovery techniques. ESI improves the quality of network provisioning, fault monitoring and service-level reporting/verification by using IPv6 Discovery to:

- Identify IPv6-enabled devices, both native and dual-stacked
- Find IPv6 routes and paths on the network
- Collect attributes of native IPv6 network equipment
- Deliver IPv6 discovery results in real-time
- Locate unwanted IPv6 devices and routes
- Identify unintentionally configured IPv6 devices
- Secure and manage policy-compliant IPv6 equipment

Scalable to the World’s Largest Networks with Two-tier Enterprise Architecture
Lumeta ESI is available in a Cloud, Virtual Machine or Appliance deployment.

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

ESI uses a distributed, two-tier model – proven at the world’s most complex networks. The system includes the ESI Command Center and ESI Scouts.

- **ESI Command Center**: A web-based management platform for administration, configuration, monitoring and reporting.
- **ESI Scout**: A distributed system for collection of network intelligence, reporting back to the ESI Command Center.

The size and configuration of the ESI deployment will depend on the network topology and use-case requirements. Deployments will vary in size from a single ESI Command Center to more complex installations. A Lumeta consultant will work with you to determine the best architecture and product configuration for your environment.

Extensibility of Foundational Intelligence
Without a means to obtain network situational awareness, security analysts largely rely on locally focused specialty products and manual data analysis from complex systems, like network management suites, to gain a level of insight into the network infrastructure. While a variety of monitoring products exist, continuous network monitoring without visibility into the state of the enterprise as a whole leaves inherent gaps in defenses.

ESI offers flexible integration options to provide seamless access of its foundational intelligence to third-party products, such as security incident and event management (SIEM), vulnerability management (VM), intrusion prevention systems (IPS) and network access control (NAC). ESI data can be exported to other network security products via an open API, to provide simplified integration options to ESI’s rich, salient data. This type of integration improves analytical capabilities, allowing organizations to fully understand their IT environment.

Lumeta ESI is “Layer Zero” of the network security architecture.