Lumeta ESI

SOLUTION BRIEF

Real-Time Network Behavior Analytics & Cybersecurity Breach Detection with Lumeta ESI

Network Situational Awareness coupled with external feeds (Threat Intelligence, NetFlow) identifies Threat Flows, Zombies and other Cyber Threats

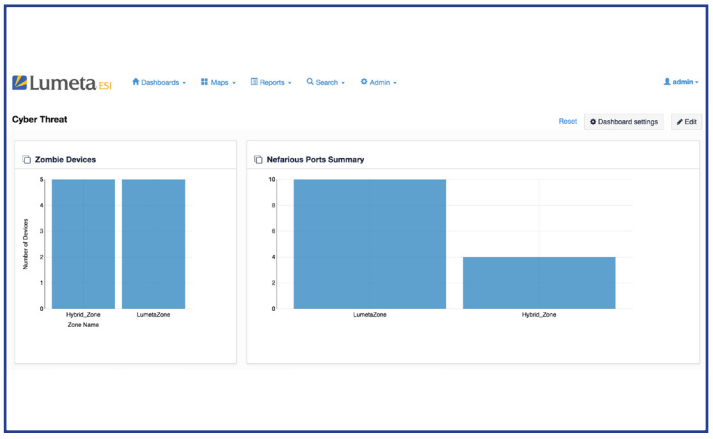
Breach Analytics **noun | \ˈbrēch- ˌa-nə-ˈli-tiks**

: On the assumption that attackers have already found a way into the network, monitor the network in real time for the telltale signs of nefarious activity. Prioritize findings for investigation and action.

Organizations are at constant risk of infiltration by adversaries on the Internet or the Dark Web, and need to quickly detect breaches to minimize their effect on the network and organization. Cybersecurity professionals are asking . . .

- Can known threat or malware IP address space on the Internet be reached from within the enterprise network?
- Are there live interactions with adversaries occurring on my network right now?
- Has any of the internal network infrastructure become a zombie participant in a botnet?
- Do any of our trusted network assets show up on blacklists? On Shadowserver or attacker lists?
- Is our organization harboring devices actively using known Trojan or malware ports right now?
- Are any of our trusted network assets behaving as TOR relays/bridges/devices?

Lumeta ESI provides authoritative answers to these questions, helping organizations quickly detect zombie infections and other threats from bad actors. Threat intelligence (from external sources and open source feeds) is made actionable by utilizing existing capabilities of the Lumeta ESI network situational awareness platform to correlate a comprehensive index of an enterprise's IP address space against known threats. In real-time, as new threat intelligence becomes available, ESI will report against the new threats and send out alerts. ESI includes a Cyber Threat Dashboard (and user-defined views) to highlight findings and ease remediation and incident response.



Lumeta ESI Cyber Threat Dashboard – Real-time indexing coupled with external feeds, such as threat intelligence and flow data

IT professionals can use the Real-Time Network Behavior Analytics & Cybersecurity Breach Detection included in Lumeta ESI for the following use cases:

✔ Threat Flows – Detect breaches via real-time and forensic analysis of conversations occurring between devices on your network and known malware command and control (C2) servers.

✔ Zombie/Bot Hunting – Determine whether or not any enterprise assets are malware infected infrastructure.

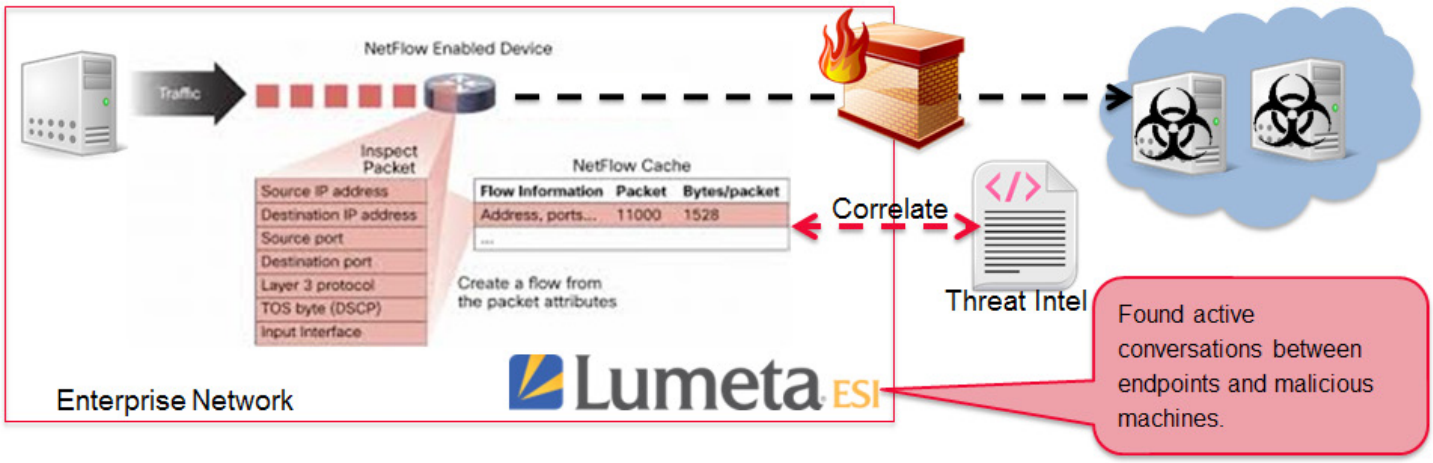
✔ Trojan or Malware Ports – Identify any active internal network use of known malware infection signature ports, Trojan ports or other vulnerable ports right now.

✔ TOR Relays/Bridges – Identify any enterprise assets acting as TOR relays/bridges potentially for nefarious purposes.

Threat Flows - NetFlow Correlation to Malware C2 Servers

✔ **Purpose**: Determine if cyber controls are preventing malware call back, C2 channels, and data exfiltration.

- Lumeta ESI with NetFlow ingestion allows **real-time and forensic** analysis of actual conversations occurring between devices on your network and known bad actor IP addresses supplied by an ingested threat feed. ESI validates communications are occurring from **specific devices** inside your network to these addresses now, or when those communications occurred historically.



✔ **How It Works**:

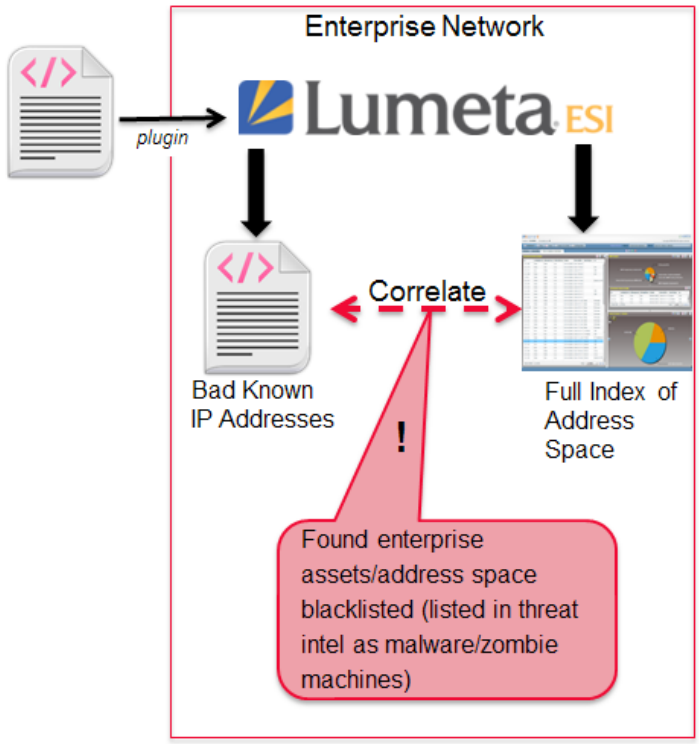
1. Parse open source and closed source intelligence feeds and repositories to enumerate known bad servers and networks, and associated attributes as available.

2. Ingest NetFlow traffic from the enterprise.

3. Execute real time correlation between network flows and threat intelligence identified.

Zombie/Bot Hunting

Purpose: Determine whether or not any trusted/enterprise assets are malware infected infrastructure participating in a C2 botnet; or part of blacklists, Dropnets, Shadowserver or attacker lists.



How It Works:

1. Parse open source and closed source intelligence feeds and repositories to enumerate known bad servers and networks (e.g., known to be participating in a zombie army), and associated attributes as available.

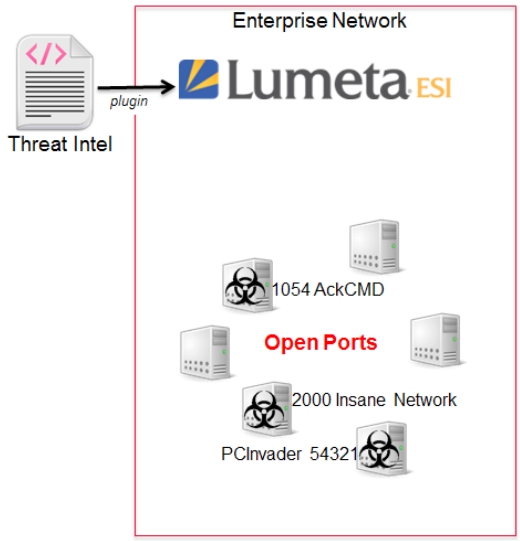
2. ESI's full index of the enterprise IP address space is correlated against known bad IP addresses from Step 1. ESI identifies devices on publicly routable addresses on your network (e.g., perhaps servers located in a DMZ or directly accessible via public IP addresses) that are also on the known bad IP address list.

3. Any IP addresses found on both lists are potentially compromised enterprise assets. ESI raises a flag regarding any machines that are blacklisted (listed in threat intelligence as malware/botnet machines).

Identification of Any Active Internal Use / Accessibility of Known Trojan or Malware Ports

Purpose: Determine if cyber controls are preventing malware call back, C2 channels, and data exfiltration.

- Malware Infection Signature Ports – Commonly used malware exploit ports which should be non-responsive but are actually responding
- Vulnerable Ports – Ports which should be non-responsive but are actually responding (e.g., prohibited ports which are often used for **lateral movement or exfiltration** like FTP, SSH, RDP, WMI, DISA Red Ports List)



How It Works:

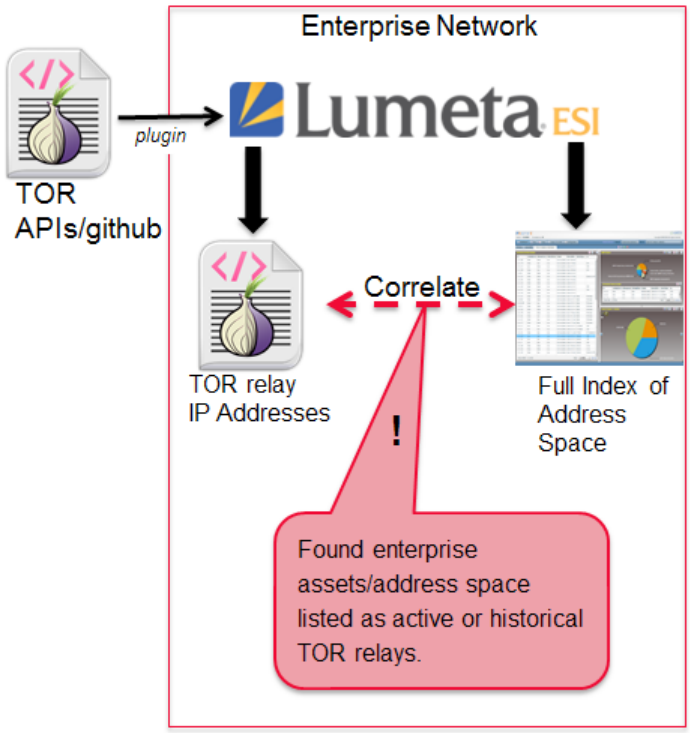
1. Parse open source and closed source intelligence feeds and repositories to enumerate known bad ports and services.

2. Perform ESI Port Discovery scans internally using the port list generated in Step 1.

3. Report on ports that respond as open, closed or inconclusive. Open bad ports indicate possible malware is running on the system. Closed ports may indicate that steganography-based port knocking exists.

Identification of Internal TOR Relays/Bridges

Purpose: Determine whether or not any trusted/enterprise assets are acting as current or past TOR relays/bridges, potentially for nefarious purposes (botnet/zombie, malware).



How It Works:

1. Parse/collect a list of current TOR relay/bridge nodes. Optionally, query the database of historical nodes.

2. ESI's full index of the enterprise IP address space is correlated against the IP address list from Step 1. ESI identifies devices on publicly routable addresses on your network that are also on the known TOR relay/bridge node list.

3. Any IP addresses found on both lists are enterprise assets that are listed as an active (or historical) TOR relay. ESI flags devices that are behaving as relays/bridges.