Adding Lumeta to Your Environment

Lumeta is a powerful solution that indexes a prodigious volume of data. Yet too much of a good thing—including information---can overwhelm. For this reason, Lumeta is designed to be configured incrementally.

- **Define scope**
- **Install & test components**
- **Configure discovery**
- **Tune settings**

Once the settings have been satisfactorily tuned and baselined for one zone of your network, that zone is explored using additional protocols, with additional discovery types, and with other options enabled, yielding a network that is increasingly known, analyzed, and understood by your organization. This approach brings Lumeta online in your environment deliberately, and uses it to generate result sets that are reasonably sized, digestible, and actionable.

Customer after customer has found that Lumeta tends to amplify the capabilities of other security systems running in their network. Ultimately, Lumeta helps customers to first achieve and then maintain the state of continuous network situational awareness.

Define scope

Lumeta Spectreis designed to be deployed incrementally, with a constrained discovery area gradually expanded in scope to encompass the whole of your network. This caps the volume of information generated to an amount that can be addressed reasonably by your troubleshooting teams. It also minimizes the amount of information you need to input to the system to get started.

Toward that end, the first deployment exercise is to identify critical core infrastructure. Consider selecting the backbone area (i.e., Area 0) of your OSPF network as the starting area for discovery.

Identify Critical Core Infrastructure
Your PSO technical consultant will ask you a series of questions to better understand your network. This preliminary information informs decisions to come regarding how and where you set up Lumeta components. It also helps in defining network zones and developing conceptual models that convey salient information to those in various roles visually.

A retailer, for example, stores its customers' credit card information in a protected enclave. That enclave would be an ideal candidate location from which to start. It's a best practice to limit your initial scope to one or two enclaves.

Identify What's Known: Zone & Collector List Types
The final preparatory step is to answer the question, "What do you already know about your network's critical core?" Your technical consultant will work with you to identify this information and embed it in Lumeta. This process entails associating IPs and CIDRs with particular network zones and within that zone, labeling them as Internal (aka "owned") or Known (aka "familiar").

Here's a preview of what to gather for entering data to Lumeta:

- **Internal**
  Internal is used in Lumeta to define the perimeter of your network--the edges where you might leave your internal network space to enter unmanaged outside space such as the Internet. Defining and refining the perimeter of your network helps you to better understand your ingress and egress points (i.e., usually firewall devices) to control and manage them. Internal subnets are those your organization has under management.
- **Known**
  The Known list is all of the "networks you know about." It's the address space (i.e., CIDR blocks and IP addresses) about which you are aware.
- **Eligible**
  The Eligible list signals to collectors, "It's okay to go here." It's the address space (i.e., CIDR blocks, IPs) Lumeta is permitted to investigate. If an IP is found during Host Discovery or on contact with a routing table and it is also on the Eligible list, then Lumeta interrogates that route or IP.

  To make Lumeta perform Path Discovery and Host Discovery on all Lumeta-discovered routes and devices, enter 0.0.0.0/0 on your Eligible list.

In preparation for discovery, you'll also need to associate collectors with areas to monitor and areas to avoid. Collectors go to their **Targets**, drop further interrogation after **Avoids**, and halt at **Stops**. The IP/CIDR list defines the coordinates within which discovery activities take place. At the collector level, scope coordinates are located in the Discovery Spaces tab. The Lumeta system appends discovered routes and IPs to its internally managed Target list. The Discovery Spaces Target List illustrated here, however, shows only those Targets input manually or imported by system users like you.

- **Target**
  The target list governs where collectors send packets during active and targeted discovery.
- **Avoid**
  The Avoid list itemizes those areas of a network that should *not* be probed during monitoring such as an affiliated company's subnet. Lumeta drops further interrogation of discovered devices and routes that are in the Avoid list.
- **Stop List**
  This list contains address points at which path discovery will halt. Probes beyond that address space cease. The Stop list serves as another way to prevent access to off-limit areas of a network.

Other information you'll need to provide includes:

- **OSPF Information**
  Your local domain's OSPF Area ID, typically Area 0, the backbone.

- **Network Information for the Command Center and Scouts**
  The following additional information, which you may choose to auto-configure via DHCP.
    - IP Address
    - Network Mask
    - Default Gateway
- **SNMP Information**
  A list of community strings and/or v3 credentials that Lumeta uses during Path Discovery and Device Profiling Discovery.

At the conclusion of this process, you'll have a clear definition of where you want to send discovery packets and where you don't. You'll know the network segments to which you'll connect your Lumeta, and you'll have enough information to set up a zone and configure Collectors. In brief, you'll have devised a vantage point from which to start observing a segment of your network.

Configure Discovery

Your preliminary discovery configuration will allow you to exercise Lumeta in a small target area of your network to see if it returns the results you expected.

To configure discovery, browse to any location in Lumeta, select Settings from the top navigation bar and use the following procedures to configure users, roles, a zone, and one or more collectors.

- See Users & Roles to configure Lumeta system users and roles.
- See Adding & Managing Zones to configure a zone.

Verify Lumeta Results

Spot-check a few known devices in your network to ensure that the system is producing the results you'd expect. Specifically, validate the Lumeta can correctly do the following:

- [ ] Discover your devices
- [ ] Profile your devices
- [ ] Access data via SNMP
- [ ] Discover specific ports

Verify Lumeta's view of these devices, profiles, and ports against what you know and expect to find about them, and assess the results.

Are you seeing results you didn't expect to see?
This would not be unusual. The expert services and support of your Solution Architect can be invaluable in interpreting preliminary discovery results and tweaking the configuration.

Possible causes of limited visibility include:

- Some kind of security blocking such as a firewall that won't let discovery probes through
- Insufficient or incorrect community strings or credentials that limit the amount of information returned about routing tables and SysNames
- Insufficient or incorrect target lists (CIDRs)
- Unchecked options in the Path Discovery pane. If Trace-to-Hosts is not selected, Lumeta will discovery hosts via broadcast and OSPF protocol, but would not try to find the path to those hosts.
- If Trace-to-Discovered-Routes is not selected or discovered routes are not on the Eligible list, and Lumeta gets routes/IPs from a routing device via SNMP, it does not pursue those addresses. This also can be controlled (i.e, limited, fine-tuned) by the Stop or Avoid lists in Discovery Spaces, and the Eligible list in the Zone configuration.

Can you see what you want to see and what you anticipated seeing? That's excellent!
Your successfully configured zone is now running and will continue to run. Lumeta will provide your enterprise with continual awareness (i.e., network situational awareness) about the core infrastructure segment you just successfully configured. That awareness is conveyed in the form of analyses, reports, notifications, and topology maps.

Tune settings

Continue to add zones that represent other enclaves and other uni-purposed aspects of your infrastructure such as Credit Card Zone, Classified Data Zone, Finance Zone, WiFi Zone, Guest Zone.

1. Adjust and tune your configurations as needed to achieve your visibility objectives.
2. Declare the network baselined.

The end result of this process is a finely tuned, baselined IT infrastructure that is monitored continuously. Your enterprise is positioned to ensure that . . .

- System changes do not negatively impact security
- Security plans remain effective after a change
- Security controls continue to perform as intended

Transactions and controls found to be weak, poorly designed, or poorly implemented can be corrected or replaced sooner rather than later, reducing risk and securing your enterprise network continuously.