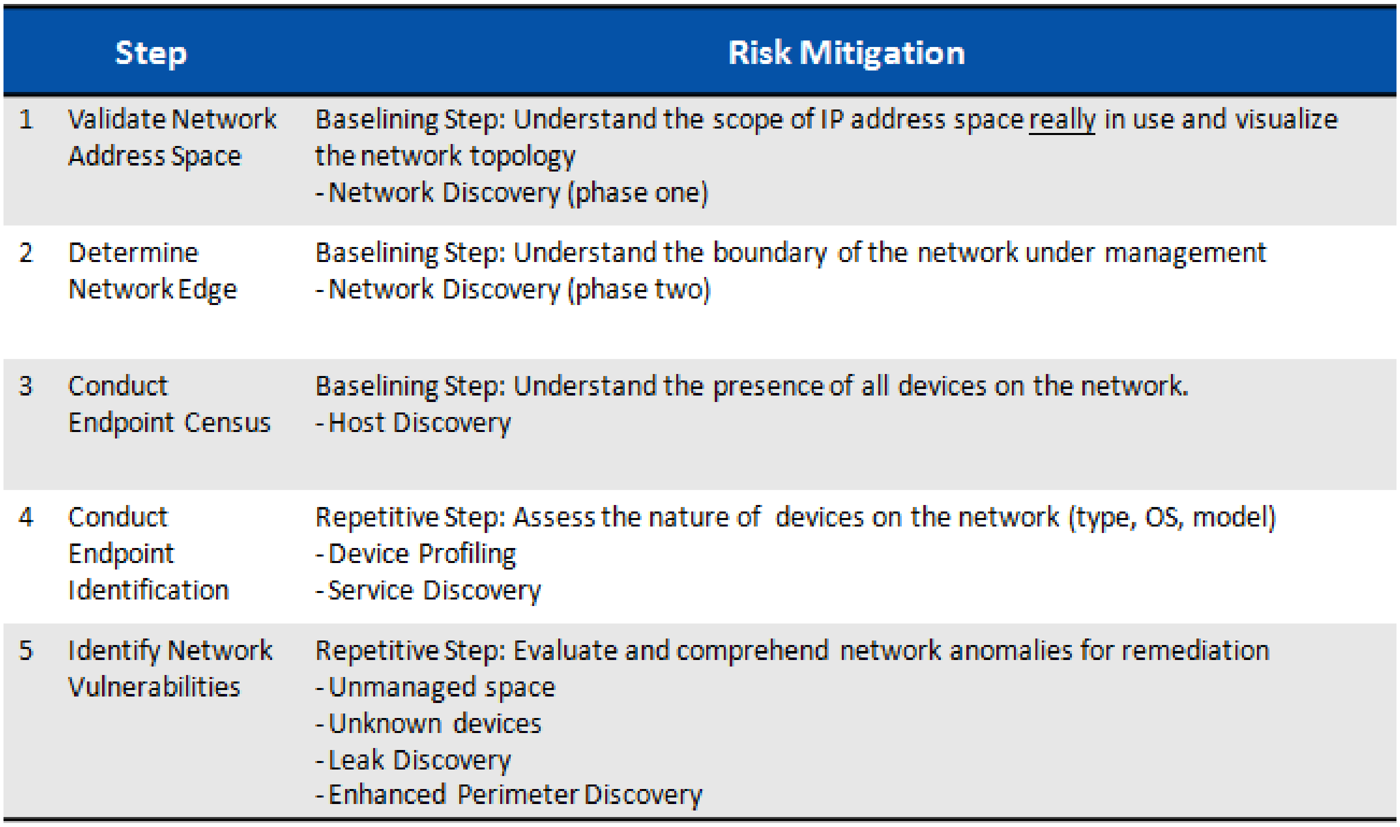
Quick Guide

5 Steps to Network Situational Awareness

A publication of Lumeta Corporation
www.lumeta.com



	Step	Risk Mitigation
1	Validate Network Address Space	Baselining Step: Understand the scope of IP address space really in use and visualize the network topology - Network Discovery (phase one)
2	Determine Network Edge	Baselining Step: Understand the boundary of the network under management - Network Discovery (phase two)
3	Conduct Endpoint Census	Baselining Step: Understand the presence of all devices on the network. - Host Discovery
4	Conduct Endpoint Identification	Repetitive Step: Assess the nature of devices on the network (type, OS, model) - Device Profiling - Service Discovery
5	Identify Network Vulnerabilities	Repetitive Step: Evaluate and comprehend network anomalies for remediation - Unmanaged space - Unknown devices - Leak Discovery - Enhanced Perimeter Discovery

Based on over a decade of experience with our clients – some of the largest global enterprise and government networks – Lumeta has developed a five step program to achieving Network Situational Awareness.

Network Situational Awareness means understanding the state of your network infrastructure. It starts with creating a “steady-state” level of network intelligence, to more closely manage change within the enterprise.

Step 1 – Validate the network IP address space. Instead of working from a set of known addresses that you think encompass the entire organization, verify that there are no “unknowns” in the network. Typically, due to the amount of changes and moves that occur on large networks, a network can have approximately 20% of unknown connections and devices.

Most organizations use an IP Address Management (IPAM) or a device Vulnerability Assessment (VA) product. Those products do what they do very well, but they would prove to be much more effective if they were working off of complete network address information.

Step 2 – Validate the edge of your infrastructure. What part is managed proactively vs. what is Internet or partner interconnectivity? What is the boundary of the network under management? Probe the network infrastructure to identify all firewalls, gateways, and forwarding devices – any way a packet can get out of the network.

Step 3 – What are the specific endpoints that are responding on that identified infrastructure? Create a holistic census of all devices on the network infrastructure – traditional (routers, gateways, firewalls, printers, VoIP phones, PCs, Mac, iPhone) and non-traditional IP-connected devices (medical equipment, security cameras, industrial control systems and so much more).

Steps 1-3 provide a baseline of your network.

Step 4 – Identify each device. What model is it? What operating system? What type of mobile device? Who is the manufacturer?

An additional step is to identify what services each device is attempting to access. Lumeta does this by probing various TCP ports. What ports are open, and what software leverages those open ports?

Step 5 – Identify vulnerabilities. Lumeta presents those anomalies with a sense of priority. What is the unmanaged address space? What are the unknown devices? Are there paths leading out of the network that you did not expect to see? Are there expired/invalid resources on web resources? This last step provides actionable items, prioritized for remediation.

These five steps are key to understanding a network in totality and achieving Network Situational Awareness.

© 2014 Lumeta Corporation