Enterprise Strategy Group | Getting to the bigger truth.™

ESG Lab Review

Lumeta Spectre: Cyber Situational Awareness

Date: September 2017 **Author:** Tony Palmer, Senior IT Validation Analyst

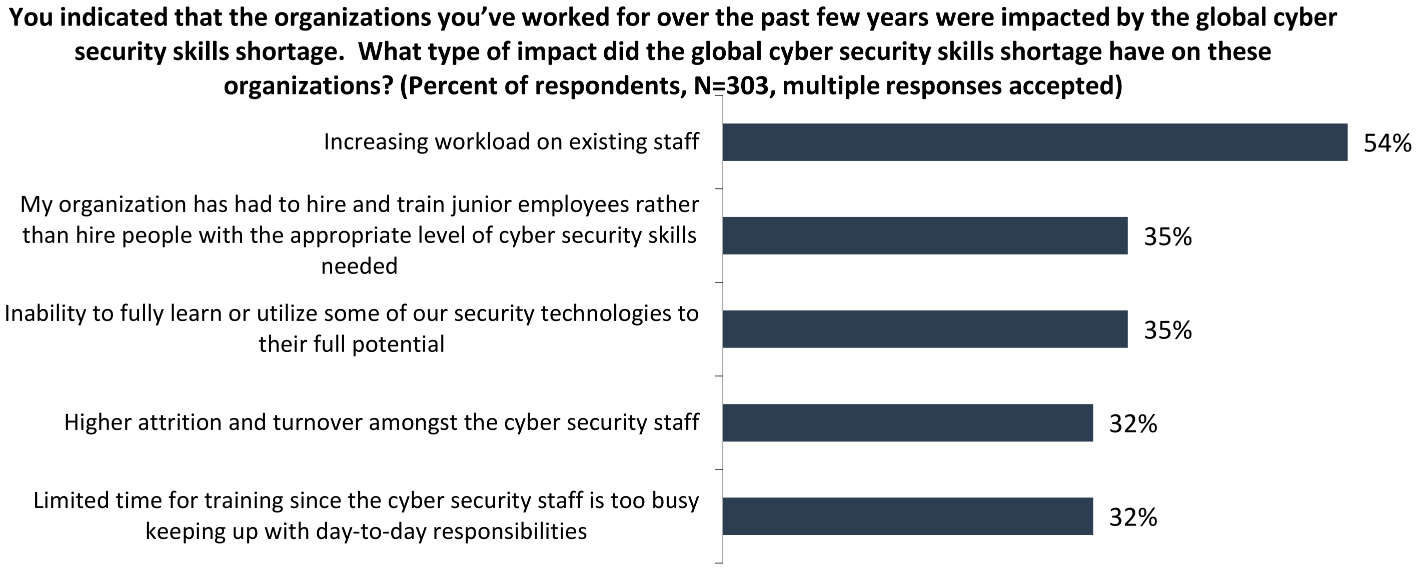
Abstract

ESG Lab performed hands-on testing of Lumeta Spectre, looking at how Lumeta's real-time, always-on monitoring and integration with best-of-breed cybersecurity tools can enable organizations to gain complete visibility into their network, enabling detection, prevention, and remediation of threats and vulnerabilities.

The Challenges

Network security can be an intimidating discipline for most organizations, and information security professionals would readily admit that they are engaged in a persistent cyber-war that puts their organizations under a constant barrage of attacks. The threat landscape is becoming increasingly dangerous, as malicious actors focus their energy on developing sophisticated, targeted attacks, often based upon zero-day malware that easily circumvents signature-based security controls. Facing persistent cyber-adversaries is a challenge, and network security has become more difficult because of an explosion in the number of users and devices, combined with a commensurate increase in traffic. Additional challenges are imposed by disparate security policies, controls, and technologies, and the increasing application of cloud-first, mobile-first, and digital transformation initiatives. The use of technology to radically improve the performance and reach of enterprises brings new types of applications with new security issues. Organizations are trying to cope with these changes while operating within the constraints posed by the global cybersecurity skills shortage. According to ESG research, 45% of organizations report that they have a problematic shortage of cybersecurity skills.[1] In a separate survey of cybersecurity professionals, 54% reported that the cybersecurity skills shortage increased their workload, 35% said the shortage led to an inability to fully learn or utilize security technologies to their full potential, and 32% reported higher attrition and turnover.[2]

Figure 1. Top Five Impacts of the Global Cybersecurity Skills Shortage



Source: Enterprise Strategy Group, 2017

[1] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

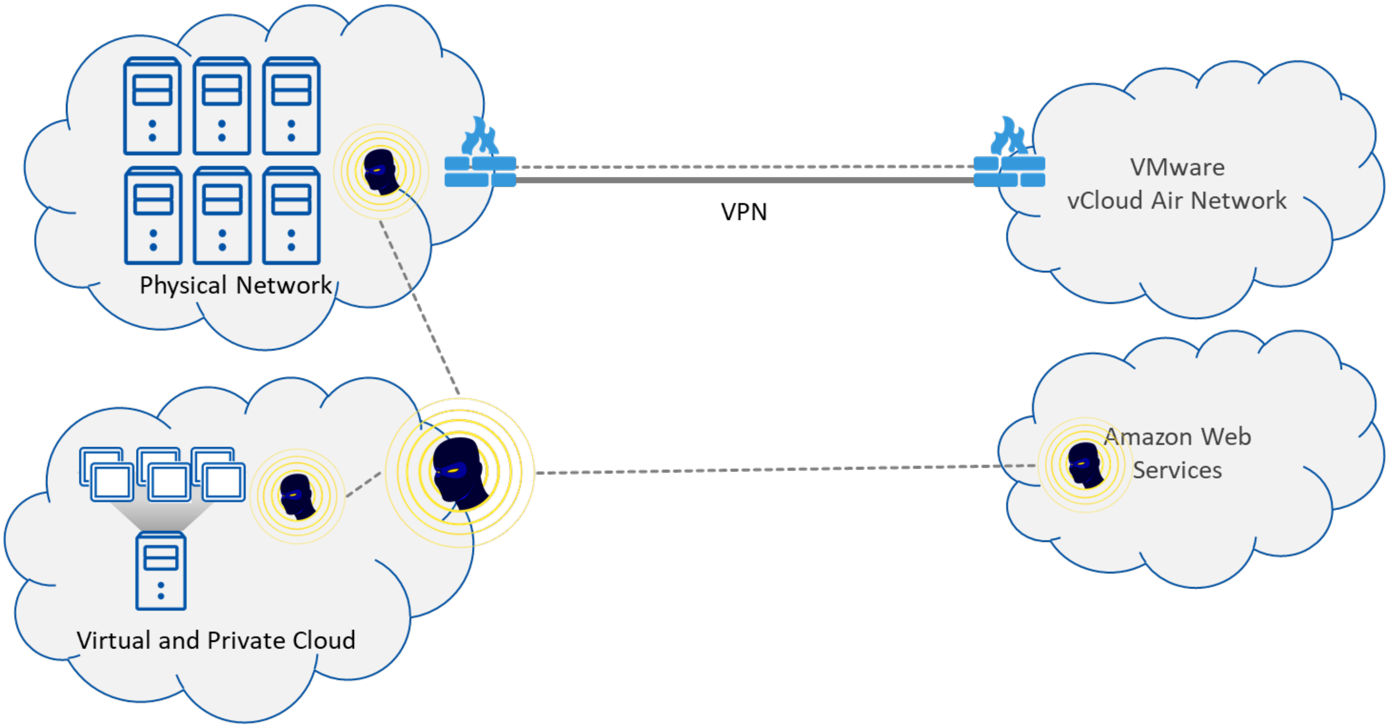
[2] Source: ESG/ISSA Research Report, *Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)*, December 2016.

Lumeta Spectre

Lumeta Spectre is designed to offer real-time, context-driven security intelligence to address these problems. By enhancing Lumeta's Recursive Network Indexing techniques with the context of network state change via analysis of network control plane protocols (OSPF, BGP, ARP, DHCP, DNS, ICMPv6, and others), Lumeta Spectre provides network situational awareness in real time as mobile, virtual, cloud assets, and even the physical/software-defined network changes. Lumeta Spectre hunts for anomalous behavior to provide context and to quickly prioritize issues for remediation. Lumeta Spectre includes the ability to ingest third-party threat intelligence feeds—an Accenture iDefense subscription is included—to correlate with network data to find potentially compromised enterprise assets that are malware-infected, i.e. participating in a C2 botnet, or identified in a blacklist, Dropnet, Shadowserver, or attacker list. Lumeta Spectre discovers internal use of known malicious ports, and hunts for unauthorized communication to known bad actor sites.

Lumeta Spectre hunts for dynamic changes to the network edge and changes caused by virtual, cloud, and mobile assets on your network. Recursive Network Indexing provides a real-time, authoritative view of network infrastructure. This enables organizations to gain a true view of all network devices, i.e. the total address space and everything in it. Lumeta Spectre can also identify leak paths, areas where there is unauthorized communication to the Internet or between firewalled segments.

Figure 2. Lumeta Spectre

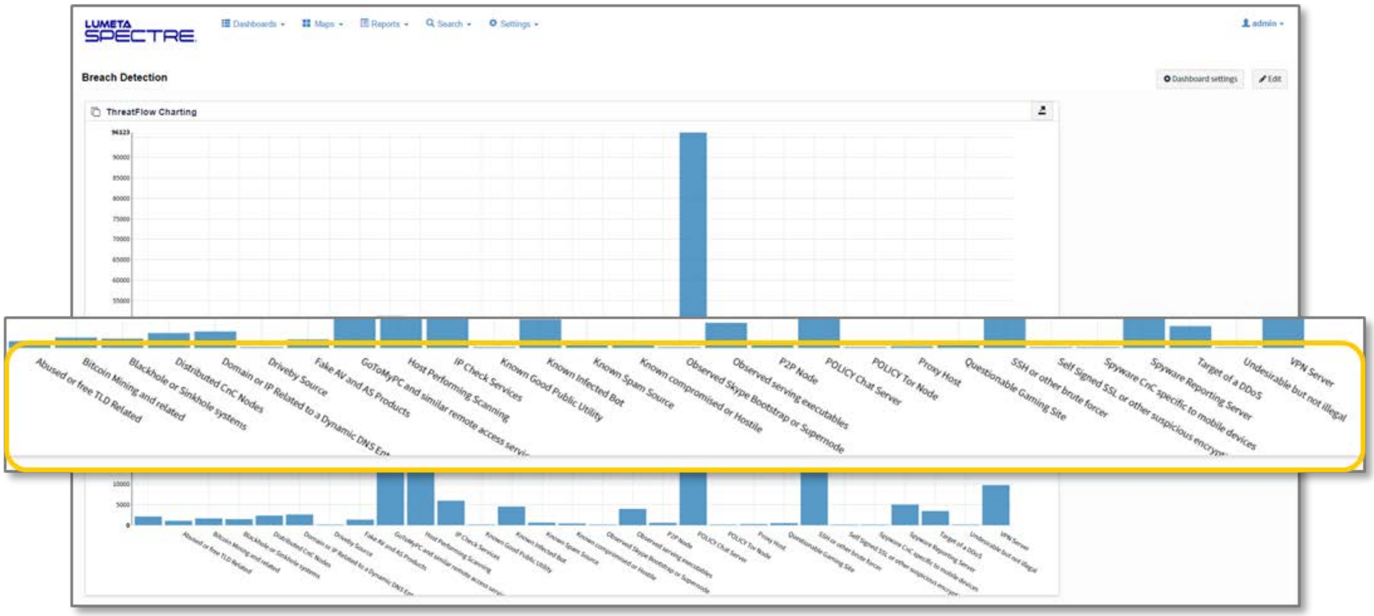


Source: Enterprise Strategy Group, 2017

ESG Lab Tested

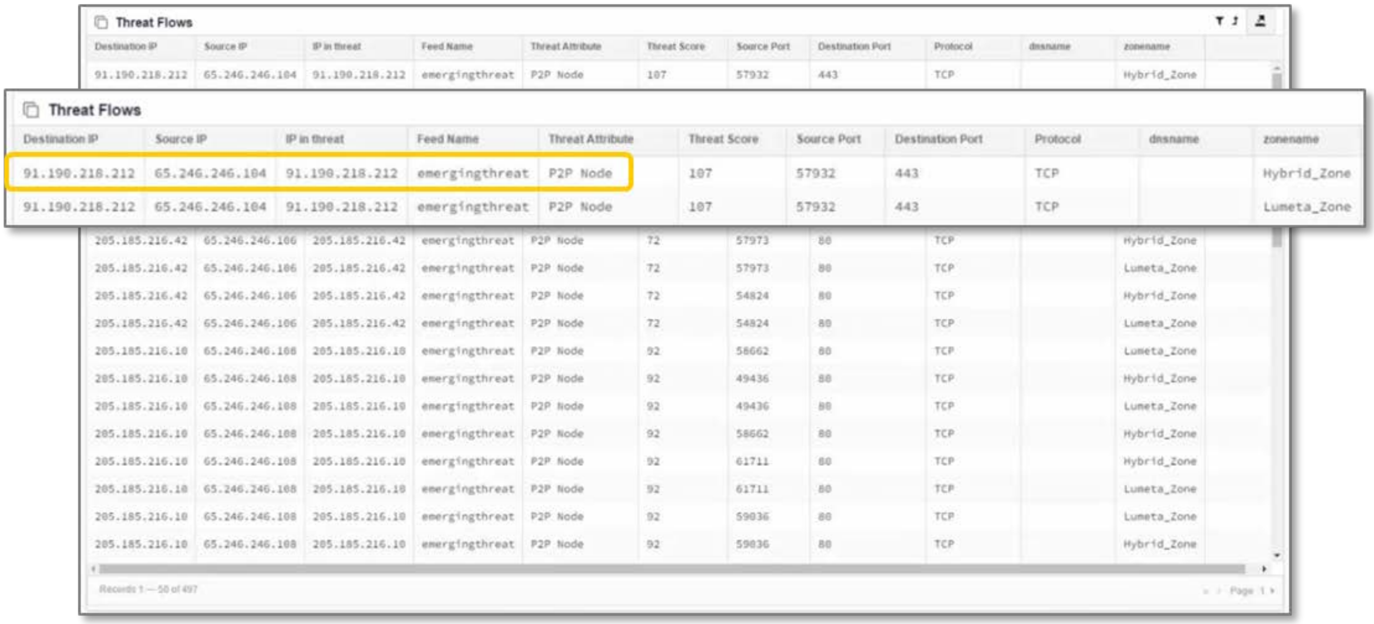
The Lumeta Spectre Command Center, shown in Figure 3, is where the user interface and HDFS data store are hosted. Configuration, analytics, and correlation are all done here. Lumeta Spectre uses the concept of Zones as configuration paradigms. Organizations can create their own zones based on the criteria that are most important to them and how they view their network—geographically, by department or business unit, by tenant, etc. Spectre Scouts are virtual machines spun up in various parts of the organization's network to facilitate visibility. The Command Center collects data from the Scouts. Users create zones to visualize the data. Lumeta provides a number of dashboards out of the box, including the ability to identify dark web elements like Tor relays and Tor exit nodes in the infrastructure.

Figure 3. The Lumeta Spectre User Interface—Breach Detection



Lumeta Spectre correlates what it knows about the network with threat intel and ingested netflows and uses the combined intelligence to identify threat flows. Figure 4 shows peer to peer (P2P) transactions. Lumeta Spectre shows the source IP, which is on the internal network, communicating with an emerging threat that has been identified. With this intel, security analysts can take remediating action, i.e. quarantine or shut down compromised nodes.

Figure 4. Threat Flows



Threat Flows

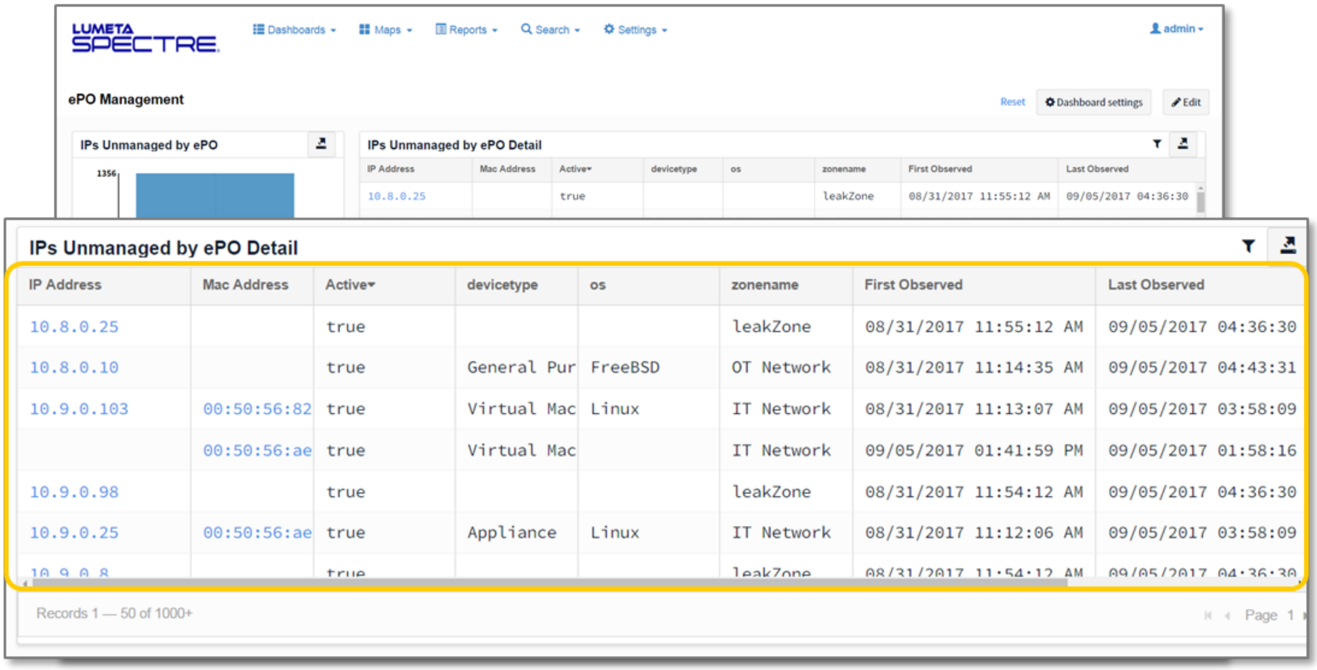
Destination IP	Source IP	IP in threat	Feed Name	Threat Attribute	Threat Score	Source Port	Destination Port	Protocol	dnsname	zonename
91.190.218.212	65.246.246.104	91.190.218.212	emergingthreat	P2P Node	107	57932	443	TCP		Hybrid_Zone
91.190.218.212	65.246.246.104	91.190.218.212	emergingthreat	P2P Node	107	57932	443	TCP		Lumeta_Zone
205.185.216.42	65.246.246.106	205.185.216.42	emergingthreat	P2P Node	72	57973	80	TCP		Hybrid_Zone
205.185.216.42	65.246.246.106	205.185.216.42	emergingthreat	P2P Node	72	57973	80	TCP		Lumeta_Zone
205.185.216.42	65.246.246.106	205.185.216.42	emergingthreat	P2P Node	72	54824	80	TCP		Hybrid_Zone
205.185.216.42	65.246.246.106	205.185.216.42	emergingthreat	P2P Node	72	54824	80	TCP		Lumeta_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	58662	80	TCP		Lumeta_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	49436	80	TCP		Hybrid_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	49436	80	TCP		Lumeta_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	58662	80	TCP		Hybrid_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	61711	80	TCP		Hybrid_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	61711	80	TCP		Lumeta_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	59036	80	TCP		Lumeta_Zone
205.185.216.10	65.246.246.108	205.185.216.10	emergingthreat	P2P Node	92	59036	80	TCP		Hybrid_Zone

Records 1 — 50 of 497

Page 1

Lumeta reports that in their experience there’s an average gap of 40% in knowledge regarding endpoints on an organization’s network. These endpoints are not managed or covered by endpoint or threat management solutions, so they are potentially exposed to threats. Lumeta works with best-of-breed providers to close this gap. In Figure 5, Lumeta is highlighting all unmanaged devices, where a McAfee ePO agent is not installed.

Figure 5. Endpoint Management



ePO Management

IPs Unmanaged by ePO Detail

IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed
10.8.0.25		true			leakZone	08/31/2017 11:55:12 AM	09/05/2017 04:36:30

IPs Unmanaged by ePO Detail

IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed
10.8.0.25		true			leakZone	08/31/2017 11:55:12 AM	09/05/2017 04:36:30
10.8.0.10		true	General Pur	FreeBSD	OT Network	08/31/2017 11:14:35 AM	09/05/2017 04:43:31
10.9.0.103	00:50:56:82	true	Virtual Mac	Linux	IT Network	08/31/2017 11:13:07 AM	09/05/2017 03:58:09
	00:50:56:ae	true	Virtual Mac		IT Network	09/05/2017 01:41:59 PM	09/05/2017 01:58:16
10.9.0.98		true			leakZone	08/31/2017 11:54:12 AM	09/05/2017 04:36:30
10.9.0.25	00:50:56:ae	true	Appliance	Linux	IT Network	08/31/2017 11:12:06 AM	09/05/2017 03:58:09
10.9.0.8		true			leakZone	08/31/2017 11:54:12 AM	09/05/2017 04:36:30

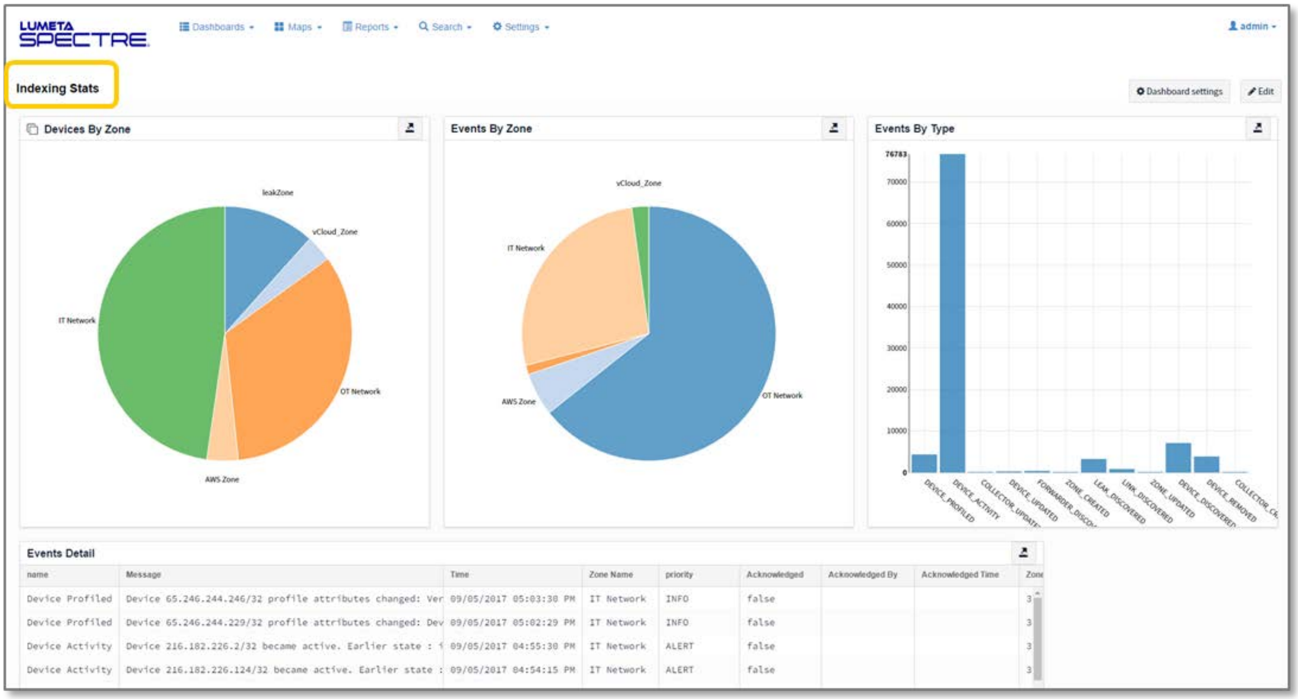
Records 1 — 50 of 1000+

Page 1

From here, users can drill down into device details to get pertinent information about the device, including addresses, interfaces, port status, when the device was discovered, and when it was updated.

Figure 6 shows the *Indexing Stats* view. *Indexing Stats* provides additional analytics, showing devices by zone. This gives users a feel for the size and scope of their zones, as well as events sorted by zone and type. ESG clicked on ***Hybrid Zone***.

Figure 6. Indexing Stats



Indexing Stats

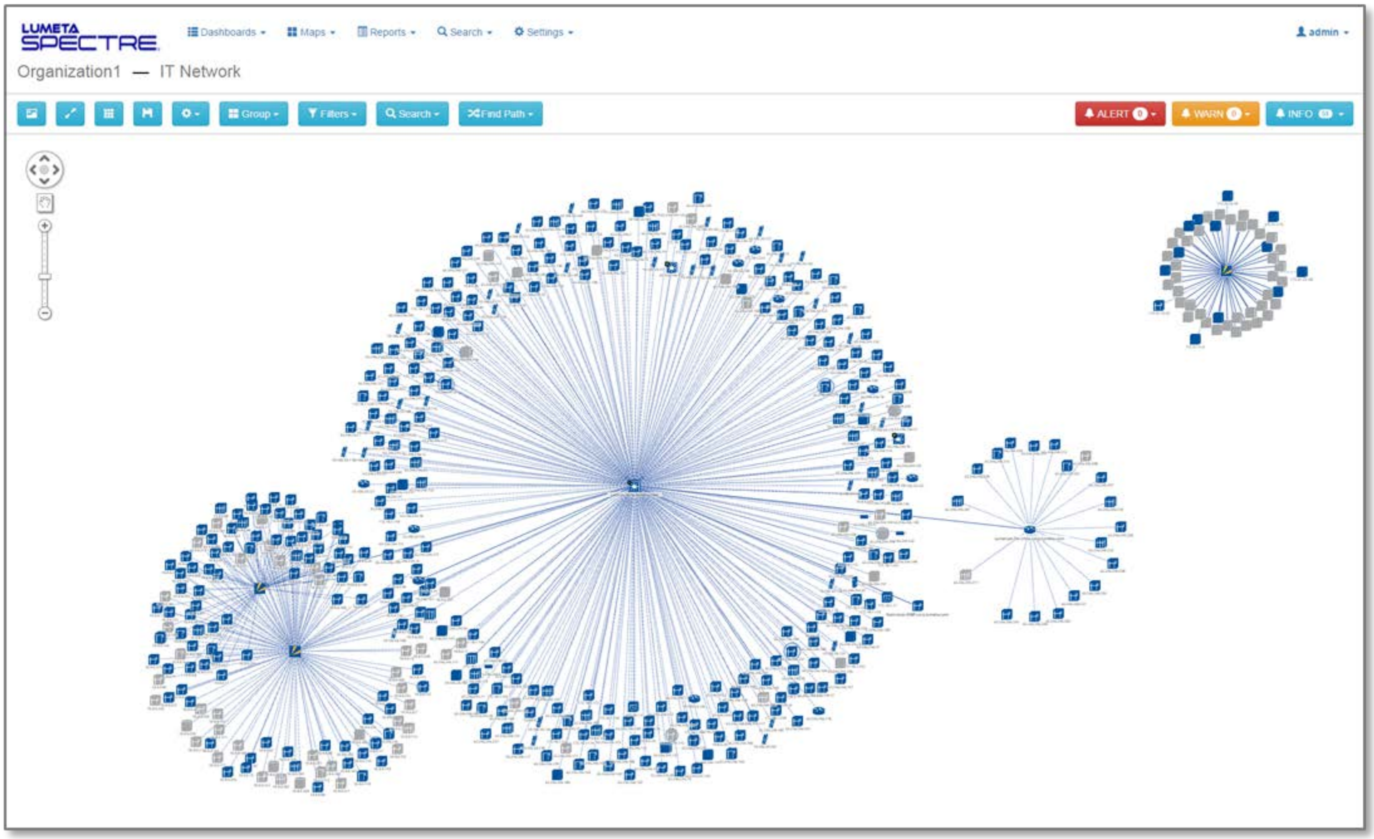
Events Detail

name	Message	Time	Zone Name	priority	Acknowledged	Acknowledged By	Acknowledged Time	Zone
Device Profiled	Device 65.246.244.246/32 profile attributes changed: Ver	09/05/2017 05:03:30 PM	IT Network	INFO	false			3
Device Profiled	Device 65.246.244.229/32 profile attributes changed: Dev	09/05/2017 05:02:29 PM	IT Network	INFO	false			3
Device Activity	Device 216.182.226.2/32 became active. Earlier state : i	09/05/2017 04:55:30 PM	IT Network	ALERT	false			3
Device Activity	Device 216.182.226.124/32 became active. Earlier state :	09/05/2017 04:54:15 PM	IT Network	ALERT	false			3

This took us to the map view, shown in Figure 7. This is a map of the entire network, which enables organizations to quickly confirm segmentation.

The island on the right, with no connections to the rest of the network, is segmented appropriately. Users can configure alerts to display on the dashboard and the map and can drill into alerts from either location.

Figure 7. The Lumeta Network Map



Lumeta Spectre also comes equipped with a visual query builder, which enables users to create complex queries by simply dragging and dropping items from a library of predefined elements.

Why This Matters

Cybersecurity professionals report numerous impacts of the global cybersecurity skills shortage, including increased workloads and an inability to fully learn or utilize security technologies.[3] Organizations should look to improve their network visibility and enforcement capabilities to minimize their attack surface and reduce potential avenues of attack.

With a couple of clicks, ESG Lab visualized an entire live network and all devices on it. The Breach Detection dashboard showed all devices on the network, identifying zombie devices and dark web (Tor) nodes.

Spectre also identified threat flows—peer to peer transactions between inside devices and IP addresses identified as P2P nodes. Devices with IP addresses not managed by the organization's endpoint and threat management solutions were also identified and reported on in detail, enabling identification and remediation. ESG Lab used the visual query builder that enables users to create and execute complex analytic queries by dragging and dropping elements, with no SQL required.

Lumeta's layered approach combines data collection and telemetry, threat intelligence from open source and subscription feeds, and integrations with best-of-breed cybersecurity products to deliver context-driven network situational awareness in real time.

[3] Source: ESG/ISSA Research Report, *Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)*, December 2016.

The Bigger Truth

Today's dynamic IT infrastructure, featuring the cloud, digital business transformation, and an increasingly mobile workforce, is evolving at a pace that's exceeding the capabilities of legacy security approaches. Traditional network security has proven to be insufficient, lacking the visibility, control, and intelligence necessary to keep up with changing needs. Infrastructures are left exposed to a dangerous threat landscape where persistent cyber-attackers have proven adept at bypassing aging security mechanisms, presenting an increased risk to the business.

To shrink an organization's attack surface and reduce potential avenues of compromise, security teams should look to improve their network visibility and enforcement capabilities. After all, it's impossible to protect users and their devices when you don't know who they are, what they've connected to, and what they're allowed to do.

With the ever-present cybersecurity skills shortage, enterprises need to supplement security staff, leveraging emerging technologies to offload human analytics. Enterprises can use thorough and up-to-date network inventories to take actions aimed at reducing the attack surface by applying the principle of least privilege, and developing granular access policies that ensure access is granted to the minimum resources necessary. Security teams need to be able to update policies to reflect changes in behavior that have been detected through continuous monitoring, regardless of user or device type.

ESG Lab looked at a live network environment using Lumeta Spectre, gaining visibility over the entire network and all devices on it quickly and with just a couple of clicks. The Breach Detection dashboard showed compromised devices on the network, identifying zombie devices and dark web (Tor) nodes. Lumeta Spectre also identified threat flows and devices at IP addresses not managed by the organization's endpoint and threat management solutions. Lumeta Spectre can drill down into the details for these devices for identification and remediation. The custom query builder enabled us to build complex analytic queries with a visual drag-and-drop interface, without requiring SQL expertise.

Given the need for network visibility, tight access controls, continuous monitoring, and real-time security policy flexibility, ESG Lab believes that Lumeta's integrated security solutions, including integrated network discovery, monitoring, and analytics, can provide authoritative cyber situational awareness in real time to address evolving network security requirements.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.