Going beyond the IoT/ICS Security Hype To Achieve True Visibility and Security

Lumeta Research Team Guide

LUMETA
DETECT WITH A HIGHER SENSE

www.lumeta.com

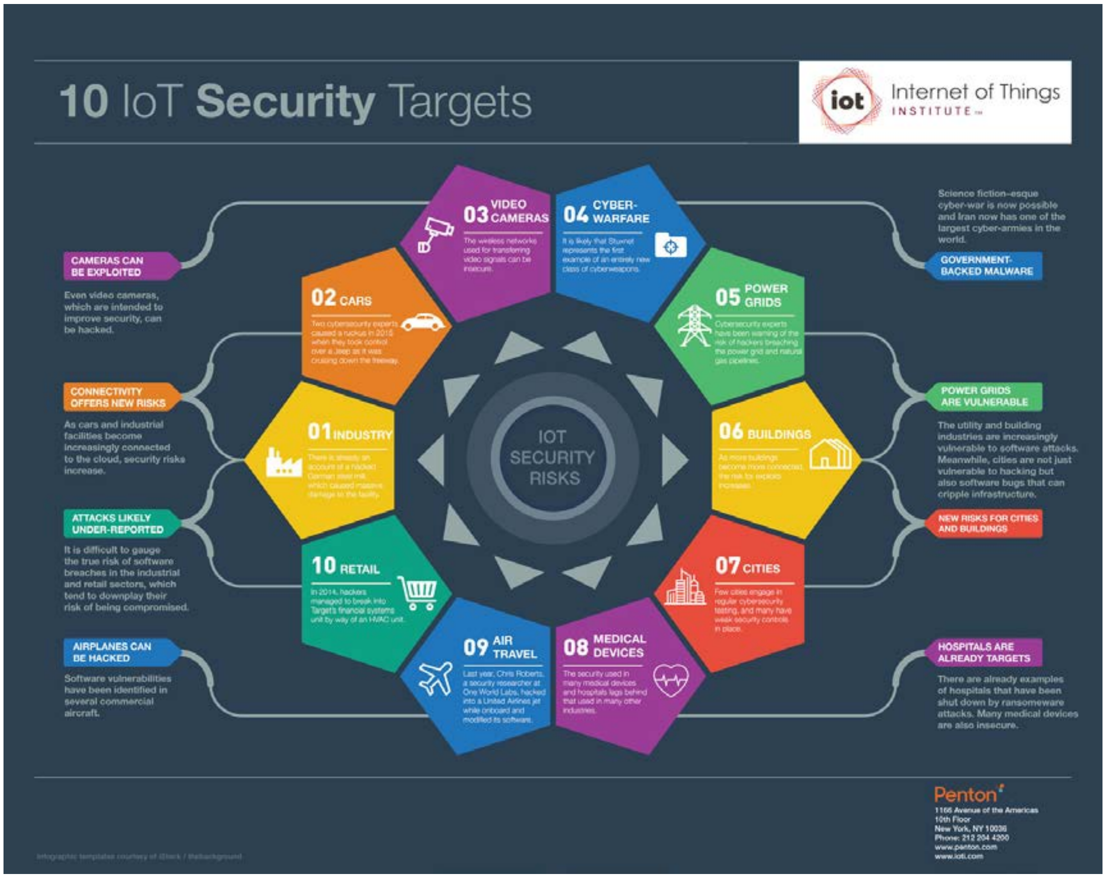
Contents

Introduction

The Internet of Things (IoT) is disrupting traditional networks. It's enabling greater centralized control and management over more and more services and greatly expanding business opportunities across all sectors. Like mobile devices and BYOD, we are seeing a shift from proprietary OS and communications to more standardized, even if customized, versions of commercially available OS and traditional IP networking.

We are seeing IoT being rapidly adopted within Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) supported organizations such as utilities, public works, and manufacturing. In addition, we are seeing IoT being utilized more in government, healthcare, retail and banking. Governments have large requirements around critical systems that include supply chain and military technology, as two examples. In healthcare, retail, and banking medical devices and POS systems are being upgraded to newer IP-enabled systems. In the manufacturing sectors, the factory floor is going through major transformations and upgrades. Across the board, IoT technologies are enabling better features, upgradability and centralized management through off-the-shelf OS support and IP- based networking.

However, by moving towards more standardized technologies, new security risks have been introduced as the attack surface has also expanded. The protected walls based on "closed" technologies are being torn down exposing organizations to common, yet advanced attacks.



There is already an account of a hacked German steel mill which caused massive damage to the facility.

Two cybersecurity experts caused a ruckus in 2015 when they took control over a Jeep as it was cruising down the freeway.

The wireless networks used for transferring video signals can be insecure.

It is likely that Stuxnet represents the first example of an entirely new class of cyberweapons.

Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.

As more buildings become more connected, the risk for exploits increases.

Few cities engage in regular cybersecurity testing, and many have weak security controls in place.

The security used in many medical devices and hospitals lags behind that used in many other industries.

Last year, Chris Roberts, a security researcher at One World Labs, hacked into a United Airlines jet while onboard and modified its software.

In 2014, hackers managed to break into Target's financial systems unit by way of an HVAC unit.

Even video cameras, which are intended to improve security, can be hacked.

As cars and industrial facilities become increasingly connected to the cloud, security risks increase.

It is difficult to gauge the true risk of software breaches in the industrial and retail sectors, which tend to downplay their risk of being compromised.

Software vulnerabilities have been identified in several commercial aircraft.

Science fiction–esque cyber-war is now possible and Iran now has one of the largest cyber-armies in the world.

The utility and building industries are increasingly vulnerable to software attacks. Meanwhile, cities are not just vulnerable to hacking but also software bugs that can cripple infrastructure.

There are already examples of hospitals that have been shut down by ransomeware attacks. Many medical devices are also insecure.

1166 Avenue of the Americas
10th Floor
New York, NY 10036
Phone: 212 204 4200
www.penton.com
www.ioti.com

Infographic templates courtesy of iStock / thebackground

Figure 1: The Wheel of Targets Subject to an Attack

Why IoT Security is a Major Concern

ICS attacks within IoT are becoming a regular occurrence with the expectation that both nation state and other sponsored activity will only continue to grow to disrupt foreign public and private interests. Confidence appears low for vendors to prevent the success rate given how the attacks maybe implemented. Different sectors have already seen compromises and breaches this years. Here are some examples of where attackers are concentrating efforts:

Manufacturing – Various forms of malware and ransomware have been employed to halt productions systems and take them offline for extended periods. This is done to either simply increases losses through loss of production or hold organizations hostage till payment is made to release control of these systems. This has happened at automotive and pharmaceutical companies as two major examples, but has been an issue in other sectors as well.

Power Grids, Water Utilities, and Nuclear Power Plants – The compromise of these facilities have been widespread, often by nation state attackers. Thus far most of the activity has been probing to see the level of control that can be achieved and see how quickly detection has occurred. The actual hijacking, while less frequent, thus far has been primarily for monetary gain via ransomware.

Retail and Banking: Most of the IoT compromises have occurred at Point-of-Sale or ATM compromises. These breaches have been primarily for stealing confidential personal and financial data of consumers and businesses versus ransomware.

Healthcare – What has grown, is thee continued discovery and evolution of medical device hijacking, sometimes called MEDJACK and MEDJACK.2, and the increase of ransomware across a variety of these targets.

The bottom-line, is that attackers are targeting these non-traditional compute systems and the number of breaches is going up all the time and therefore organizations need to be ready to embrace IoT but in a secure and structured way.

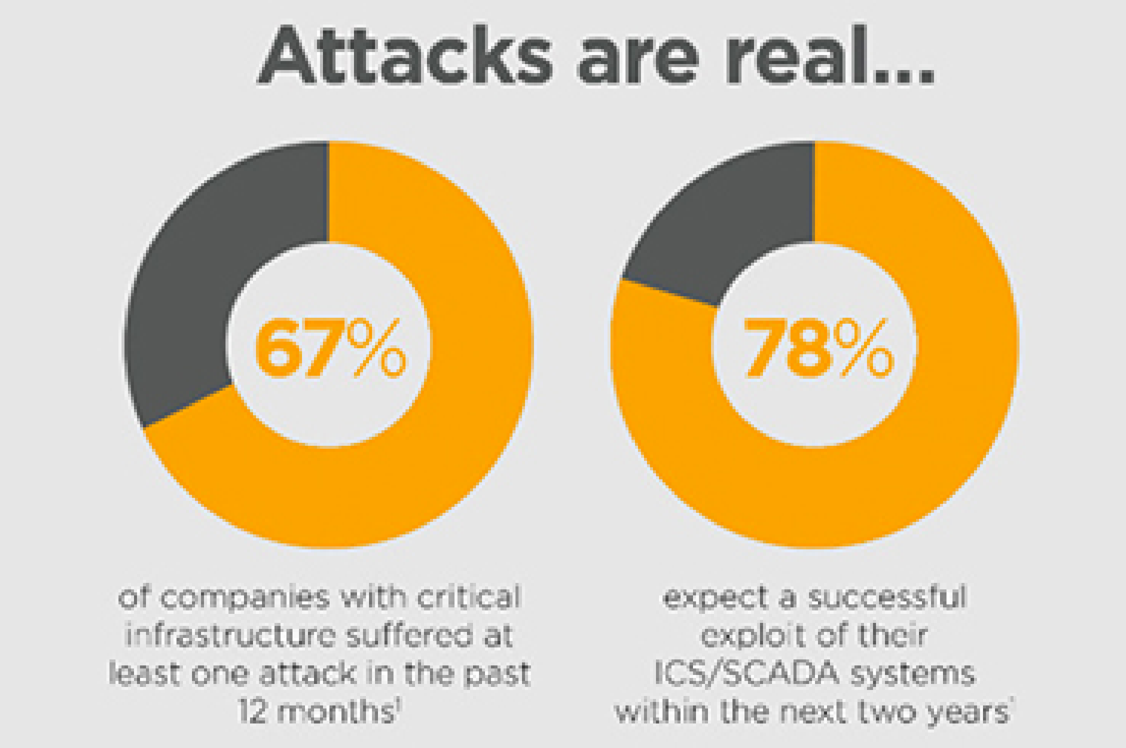


Figure 2. Attacks increased from 2016-17 and show no signs of slowing down.

IoT Policies

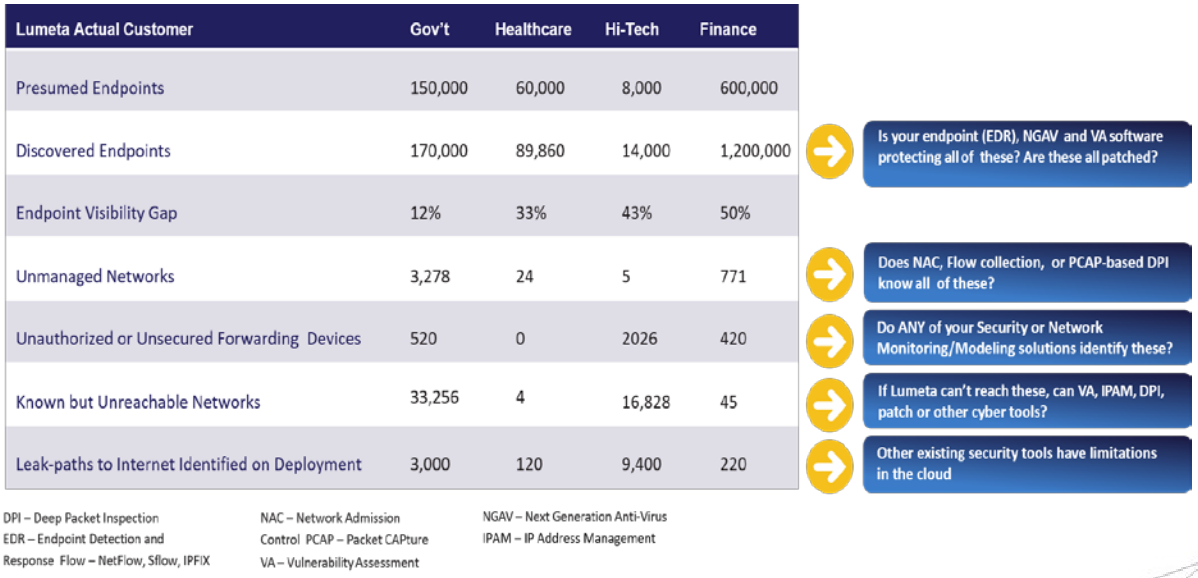
Any IP based device can expose an organization to a data breach. Most staff aren't IT or security specialists, and do not understand how IP-based devices can be compromised.. Employee error or "insider threat" is a major security problem that the majority of organizations face. This issue is made worse by poor or underdeveloped security policies that do not account for the IoT. In fact, most organizations cannot identify the number of IoT devices on their network(s).

To mitigate these concerns, some organizations limit the number of IoT-connected devices allowed on their networks, enabling only enterprise-specific vendors with robust security programs. However, this is a flawed strategy.

In addition, businesses cannot limit the IoT to only vendors that provide security patches and endpoint security solutions given the diversity of emerging technologies, across all business sectors. Plus, many businesses both large and small rely to some extent on their staffs' own devices for communications and responding to situations quickly.

Technology Challenges in Securing IoT Environments

Current solutions, readily available in the market today or commonly used by many organizations are fundamentally flawed at providing the full visibility needed to secure IoT environments effectively. On average, Lumeta's research has determined that over 40% of today's dynamic networks, endpoints, cloud infrastructure are unknown, unmanaged, rogue or participating in shadow IT, leading to significant infrastructure blind spots by both enterprise and government departments alike. This indicates a real lack of real-time awareness to prevent attackers compromising systems.



Lumeta Actual Customer	Gov't	Healthcare	Hi-Tech	Finance
Presumed Endpoints	150,000	60,000	8,000	600,000
Discovered Endpoints	170,000	89,860	14,000	1,200,000
Endpoint Visibility Gap	12%	33%	43%	50%
Unmanaged Networks	3,278	24	5	771
Unauthorized or Unsecured Forwarding Devices	520	0	2026	420
Known but Unreachable Networks	33,256	4	16,828	45
Leak-paths to Internet Identified on Deployment	3,000	120	9,400	220

Is your endpoint (EDR), NGAV and VA software protecting all of these? Are these all patched?

Does NAC, Flow collection, or PCAP-based DPI know all of these?

Do ANY of your Security or Network Monitoring/Modeling solutions identify these?

If Lumeta can't reach these, can VA, IPAM, DPI, patch or other cyber tools?

Other existing security tools have limitations in the cloud

DPI – Deep Packet Inspection
EDR – Endpoint Detection and
Response Flow – NetFlow, Sflow, IPFIX

NAC – Network Admission
Control PCAP – Packet CAPture
VA – Vulnerability Assessment

NGAV – Next Generation Anti-Virus
IPAM – IP Address Management

Table 1. Examples of Blind Spots Enabling Significant Gaps in Visibility

Following are existing security technologies that fall short when it comes to protecting the IoT:

a) NMAP – Limitations associated with NMAP solutions include open source; slow performance, especially on larger networks; experimental IPv6 support; and network congestion (no rate throttling). In addition, NMAP technology has been known to knock over scanned endpoints with malformed packets, and is typically used outside of normal business hours, making real-time network visibility unachievable.

b) IPAM – Network visibility isn't its primary use case for this management tool. The main features are IP address management, allocation and tracking. These solutions have very limited capability to authoritatively and recursively index a network making this solution very limited for IoT.

c) Vulnerability Scanning – Like IPAM, network visibility is not vulnerability scanning's primary use case, rather it's most often used to identify critical vulnerabilities on endpoints via credentialed access. These types of solutions frequently miss devices on networks. Very limited capability to authoritatively and recursively index a network results. Similar to NMAP, because the credentialed access is so heavy, these scans are often conducted outside heavy network usage hours which makes full network visibility in real time.

d) Network and Security Simulation/Modelers – These solutions gain credentialed access to the command line of known routers, packet forwarders, etc. to extract configuration information, and then mathematically simulate what the network topology looks like. They are ideal for "what-if" modelling exercises, however, modelling is only as good as the full extent of L3 forwarding devices, which are often unknown or incorrect. Relying on a network and security simulation method does not allow users to study the impact of transitory virtualized networking devices or rogue network infrastructure it doesn't have credentialed access and therefore, proves ineffective.

e) Network Management – As in the network simulation case, these tools are only capable of analyzing what they have access which is limited. Rogue, unmanaged or simply undocumented network elements installed on a network are invisible to network management tools, resulting in unknown vulnerabilities across the entire networks.

Smart devices offer benefits like automation and data collection, but can be hard to single out on a network, especially devices with low computing power that have to re-join a network frequently. Many of these devices are missed by Network Access (or Admission) Control technologies, which are looking for devices formally requesting access to the network and are typically not used in the network core and more at the edge.

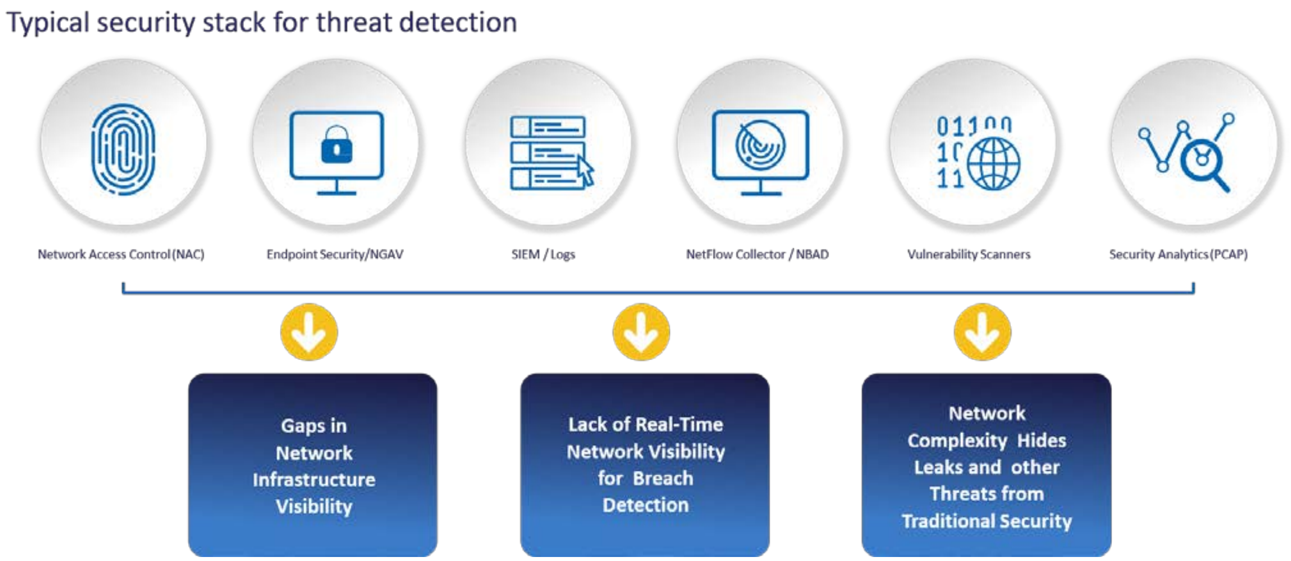

Typical security stack for threat detection
Network Access Control (NAC)
Endpoint Security/NGAV
SIEM / Logs
NetFlow Collector / NBAD
Vulnerability Scanners
Security Analytics (PCAP)
Gaps in Network Infrastructure Visibility
Lack of Real-Time Network Visibility for Breach Detection
Network Complexity Hides Leaks and other Threats from Traditional Security

Figure 3. Gaps in IoT Visibility and Awareness of Real-Time Changes Lead to Compromised Systems

While the solutions noted above provide some level of network visibility and insight, especially endpoints, none provide a true picture of real-time activities across the network, between IT and OT, and in cloud environments. Additionally, none of these technologies are able to identify potential leaks or unauthorized communication paths. Therefore, as networks become increasingly more complex, and attackers identify weaknesses in these solutions, the introduced blind spots must be eliminated to prevent compromises and costly breaches.

Where Segmentation Strategies fit into the IoT Equation, especially when Securing IT vs OT

The following rule applies to most situations: If it's too much to handle at once, break it up into smaller pieces. The same goes for securing IoT devices. Once the right visibility tools are in place, large networks can and should be broken down in order allow authorized communications to traverse only authorized areas of the network, whilst disallowing unauthorized activity

Anything touching the network should be segmented by type, purpose, access rights, and/or solution type. More than just knowing that a device is on the network, IT Teams need to have tight control over where they are, what they're doing and who they're communicating with at all times.   Devices should never be trusted unless authorized and segmentation rules should be implemented and updated ASAP.

When it comes to protecting Operational Technology (OT) systems from Information Technology (IT) systems in ICS environments, the OT environment was traditionally "closed" due to communications, and OS that were proprietary and incompatible with traditional mechanisms used in IT environments. As that changes and walls come down to enable better communications and control, it exposes OT environments to greater security risk. As a result, there is greater need for better segmentation across networks. It has also increased the need for improved monitoring, especially for real-time or instantaneous changes when it comes to communication channels and potential leak paths being created, potentially violating these segmentation policies.

What if an IoT Breach has Occurred?

It only takes one IP entry point to enable criminals to compromise a system and breach a network. A patient attacker uses time and easily available resources to their advantage to eventually find that one weak point to exploit as IT security teams struggle to root out all points of exposure.

Often it is too late to prevent a breach, but if it has been discovered despite data exfiltration having already begun, it is critical for security teams to employ what they've learned to prevent further loss, and determine when, where and how to contain the damage and lock down the point of ingress/egress.

Teams managing IoT networks will have to deal with tens or hundreds of thousands of endpoints/devices, where there are often 1,000 plus or more network infrastructure changes every month. This provides a ripe opportunity for the potential misconfigurations and can also expose potential vulnerabilities to attack by threat actors. The more network and endpoint context available with a holistic view on the entire infrastructure means security teams are better armed to work with network and desktop teams to remediate the current situation.

The Role of Threat Intelligence

As organizations operationalize threat intelligence, those feeds are ingested for action by commercial security prevention infrastructure (i.e. firewall/proxy, IPS, DLP or SIEM). However, whilst this level of automation is better than traditional manual or the forensic-only application of threat intelligence, critical shortcomings remain within this process.

For example, how does IT security validate that enforcement is working across the whole enterprise and hasn't been inadvertently turned off or misconfigured by the teams responsible for the operation of various infrastructure equipment?

As within minutes, just one newly installed, modified, or upgraded piece of IoT equipment lacking access to or improperly configured to use the threat feed will expose the whole the organization.
Attackers spend days and even weeks looking for exploitable systems and devices to begin doing their damage!

What are the Key Stages to Securing IoT

Securing IoT all starts with visibility. All IT Security Teams acknowledge that you cannot secure what is unknown, so 100% real-time network visibility of devices/ports/cloud/VMs and BYOD is step one.

Enterprise SoC Visibility of IT/OT Networks

- Identify endpoints that are frequently missed by vulnerability assessment tools for flagging CVEs exploited by attackers
- Monitor for new or changing IoT Infrastructure participating in the network

Real-Time Segmentation Analytics and Validation

- Watch for changes in the network flow paths
- Determine leak paths to the internet from OT Environments
- Identify Network Segmentation violations
- Catch erroneous firewall rule changes

Real-Time Breach Detection

- Detect remote server call back attempts by correlating NetFlow and Threat Intel Data
- Detect Tor connections initiated by malware for the purposes of tracking infection and facilitating file downloads
- Identify data path creation and leak attempts to know malware sites

Why Lumeta Spectre is Central to Your IoT Security Stack

Enterprise IoT infrastructure is virtualized, leveraging private, public or hybrid “clouds” consisting of internal and external compute resources of all kinds of IP devices. And, increasingly, enterprise network users are doing business on mobile platforms – smartphones, tablets and notebooks.

Traditional security and vulnerability assessment (VA) products already miss at least 20% of what was physically hardwired to the network because they don’t search for the unknown, this figure is much higher going as high as 40% across IoT networks.

Additionally, since VA scans stop, take too long to complete or consume too much network resource, they are often performed outside of normal business hours. This means IT security teams fail to gain cyber visibility into those mobile, virtual and cloud assets that simply aren’t present at the time the VA scan is looking. Lumeta® Spectre, offers real-time, context-driven security intelligence to address these IoT problems.

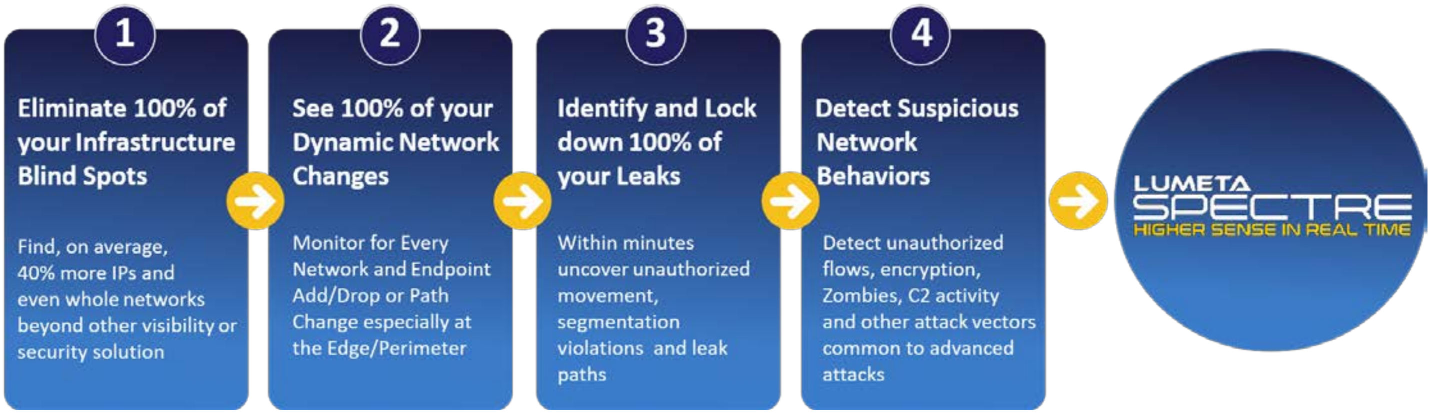

1
Eliminate 100% of your Infrastructure Blind Spots
Find, on average, 40% more IPs and even whole networks beyond other visibility or security solution
2
See 100% of your Dynamic Network Changes
Monitor for Every Network and Endpoint Add/Drop or Path Change especially at the Edge/Perimeter
3
Identify and Lock down 100% of your Leaks
Within minutes uncover unauthorized movement, segmentation violations and leak paths
4
Detect Suspicious Network Behaviors
Detect unauthorized flows, encryption, Zombies, C2 activity and other attack vectors common to advanced attacks
LUMETA
SPECTRE
HIGHER SENSE IN REAL TIME

Figure 4. Lumeta Spectre is the only solution that offers 100% real-time infrastructure visibility, real-time change monitoring and threat detection for preventing successful breaches

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 authoritative cyber situational awareness, in real-time, as mobile, virtual, cloud assets and even the physical/software defined network itself changes.

Lumeta Spectre hunts for anomalies using a combination of passive indexing (listening) and active indexing techniques – in context – to provide real-time updates as a network is changing. It identifies devices as they come onto the network (as well as other devices connected beyond the newly discovered ones).

The Key Unique Features of Lumeta Spectre Solving Your Real-Time IoT cyber visibility problem

Network Infrastructure Analytics

- Installs as a "non-routing" (OSPF, BGP) router to monitor for real-time changes to the network address space/routing table in use
- Discovers changes to the network's edge in real-time
- Authoritatively identifies new physical or virtual compute assets coming onto the network within minutes and provides dynamic visualization of changes
- Targets clientless/agentless profiling of new assets within minutes, while they remain present

Breach Detection Analytics

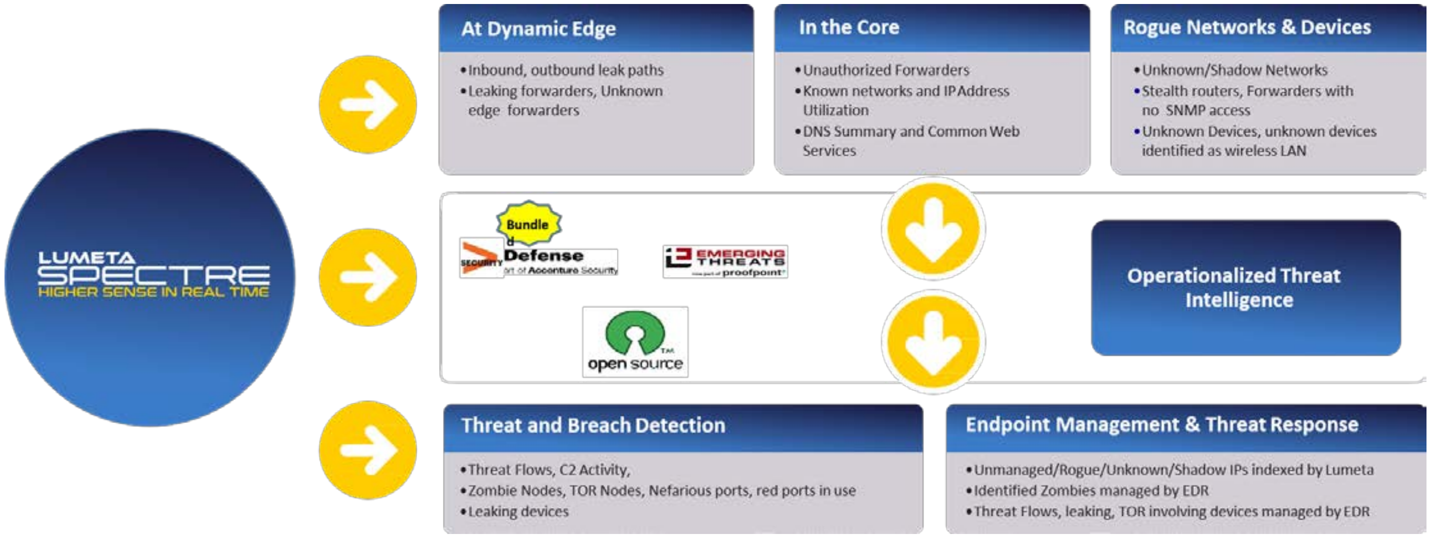
The Lumeta Spectre Cyber Threat Probe consumes open source and commercial threat intelligence data streams and correlates with Lumeta Spectre indexed metadata to:

- Discover newly compromised zombie computers that are operating on your network
- Discover within minutes whether known command and control (C2) infrastructure on the Internet is accessible from anywhere inside your network edge
- Discover within minutes whether known Dark Web (TOR) exit nodes are accessible from anywhere inside your network edge

- Provide real-time identification of nefarious TCP/UDP port usage by known malware exploits
- Provide real time identification of changes to TCP/UDP port usage which may be an indicator of compromise – i.e. RDP, FTP usage violations
- Adds the context of NetFlow and other data streams within the embedded Hadoop Distributed File System (HDFS) to provide deeper security intelligence, analysis and insights leading to faster remediation

Network Segmentation Analytics

- Discover newly active networks in real-time
- Discover networks that have become non-responsive, unreachable within minutes
- Find routed (L3) “leak paths” from critical internal networks to the Internet or in between network enclaves in real-time
- Issue network segmentation alarms and alerts into SIEM, GRC, device policy management tools for immediate remediation



LUMETA SPECTRE
HIGHER SENSE IN REAL TIME
At Dynamic Edge
•Inbound, outbound leak paths
•Leaking forwarders, Unknown edge forwarders
In the Core
•Unauthorized Forwarders
•Known networks and IP Address Utilization
•DNS Summary and Common Web Services
Rogue Networks & Devices
•Unknown/Shadow Networks
•Stealth routers, Forwarders with no SNMP access
•Unknown Devices, unknown devices identified as wireless LAN
Bundled Defense
SECURITY
Part of Accenture Security
EMERGING THREATS
now part of proofpoint
open source
Operationalized Threat Intelligence
Threat and Breach Detection
•Threat Flows, C2 Activity,
•Zombie Nodes, TOR Nodes, Nefarious ports, red ports in use
•Leaking devices
Endpoint Management & Threat Response
•Unmanaged/Rogue/Unknown/Shadow IPs indexed by Lumeta
•Identified Zombies managed by EDR
•Threat Flows, leaking, TOR involving devices managed by EDR

Figure 5. Only Lumeta Spectre Answers the Questions Where Other Solutions Fail to Protect IoT Environments

Conclusion

So, with all the current technology limitations, growth in malicious attacks how can you detect Breaches across ICS and IT networks?

Find and Eliminate ALL Blind Spots and See Changes in Real-Time
See, Discover and Monitor today's dynamic network and cloud infrastructure with real-time understanding of any changes

100% Real-Time Leak Path Detection
Identify ALL leak paths that you have today and in real-time not only to identify existing leak paths, but also new leak paths created in real-time. Adding threat intelligence, as described below, provides security context on leak paths being unauthorized, specific attack activity, misconfigurations or actual authorized change.

Apply Security Intelligence and Capabilities Everywhere
Full network context combined with best of breed security intelligence to identify threats across the darkest reaches of the network, the dynamic edge and into the cloud

Use, Validate, and Optimize Segmentation to be Proactive
Rather than just detect threats, more effectively control where authorized users can go, while limiting malicious users from accessing sensitive resources.

Lumeta Spectre for IoT and ICS is the only solution to deliver 100% real-time IP infrastructure visibility, real-time network change monitoring and threat detection for preventing successful breaches in these critical environments.

Lumeta Spectre provides unmatched *real-time* cyber situational awareness enabling network and security teams to not only identify even the darkest corners of your IP enabled, including dynamic network elements, endpoints, virtual machines and even cloud-based infrastructure paired with threat intelligence critical infrastructure but also monitor for changes or unusual behaviors without agents to detect and prevent threats that target these common gaps in visibility.

Lumeta Spectre can help ICS organizations both protect and optimize the segmentation of IT and OT networks. In addition, Lumeta can help IT and OT teams validate segmentation policies and monitor for unexpected paths, lateral movement or any sort of changes, all in real-time.

To learn more contact Lumeta today to get more information or organize your IoT POC.

www.lumeta.com

LUMETA
DETECT WITH A HIGHER SENSE