LUMETA
DETECT WITH A HIGHER SENSE

Solutions Brief

Real-time network cyber visibility required to prepare for implementation of European Network and Information Security Directive (NIS)

The European Commission has adopted the recent Directive on Security of Network and Information Systems ('NIS Directive'), which represents the first EU-wide legislation on cybersecurity.

The NIS Directive aims to achieve a high common level of security of network and information systems within the European Union via improved cybersecurity capabilities at national levels (with Member States required to be equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority) and increased cooperation among all the Member States in order to facilitate sharing information about risks and swift, effective operational cooperation on specific cybersecurity incidents.

Also under the new Directive, with an objective to achieve a culture of security across sectors which are vital for the EU economy and society, operators of essential services and digital service providers (DSPs) now have risk management and incident reporting obligations. Businesses in these sectors will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

The NIS Directive establishes minimum requirements for cybersecurity and has a significant impact on many organisations. The Directive will cover such operators and providers in the following sectors:

- Energy: electricity, oil and gas
- Transport: air, rail, water and road
- Banking: credit institutions
- Financial market infrastructures: trading venues, central counterparties
- Health: healthcare providers, including Primary Care Trusts and Hospitals
- Water: drinking water supply and distribution
- Digital infrastructure and DSPs: internet exchange points, domain name system service providers, top level domain name registries, search engines, cloud computing services and online marketplaces

LUMETA
DETECT WITH A HIGHER SENSE

Under the NIS Directive, identified operators of essential services and DSPs will have to take appropriate security measures and to notify serious incidents to the relevant national authority, such as:

- Preventing risks: Take technical and organisational measures to manage the risks posed to the security of networks and information systems that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: Provide information needed to assess the security of networks and information systems, including security policies, and provide evidence of effective implementation of security policies, such as the results of security audits.
- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services. Real-time leak path detection.

The security measures taken by DSPs should also consider some specific factors:

- security of systems and facilities incident handling
- business continuity management
- monitoring, auditing and testing
- compliance with international standards

What types of incidents will be notifiable by organisations? The Directive defines the following parameters which should be taken into consideration regarding significant incidents requiring notification to the relevant national authority:

- Number of users affected
- Duration of incident
- Geographic spread
- The extent of the disruption of the service (DSPs) The impact on economic and societal activities (DSPs)

Today’s Business Drivers Enable a Greater Attack Surface

Network Complexity with Mobile and IoT

Movement to Cloud With Less Visibility

Risk from

Infrastructure

On Average, over **40%** of Dynamic Networks, Endpoints, Cloud Infrastructure are Unknown, Unmanaged, Rogue and/or Shadow IT Leading to ***Significant Infrastructure Blind Spots*** and Lacking Real-Time Awareness

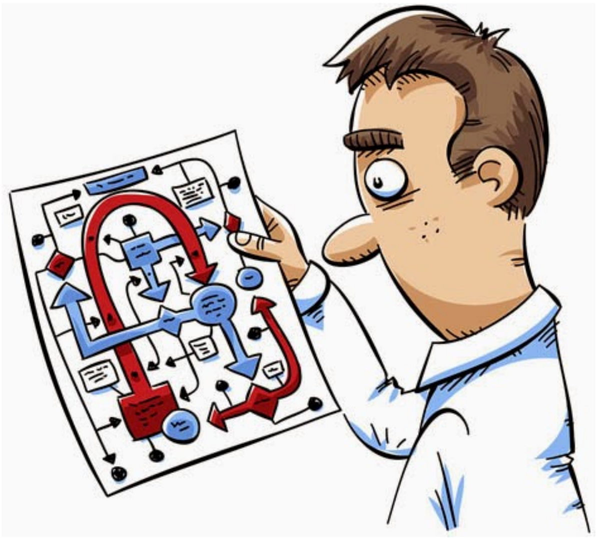
Diversification of products
Synergy
Security
Increase in quality staff
Reduces competition
Increasing Business Intelligence

Whilst it may be stating the obvious, it is impossible to protect a network or even evaluate its cybersecurity state if the full extent of the network infrastructure and endpoints is not well understood, or indeed unknown in real time.

Also, with the adoption of IoT IT security teams will be further challenged by this directive and the security, monitoring and management of this devices.

No consensus on how to implement security in IoT

- Reliance on IT Frameworks for IP Enabled OT Networks
- Endpoint focus is challenging due to variety and complexity of legacy systems
- Consensus is priority focus should be on network-based monitoring



Key technologies such as Packet Captures, Logs, Netflow, NAC, scan-only & “Continuous Monitoring” solutions are incapable of fully eliminating all the blind spots attackers exploit. This is because most of these solutions miss around 20-30% of the dynamic endpoints or devices on a network at any given time.

Lumeta Spectre monitors the network infrastructure in real time. It provides an authoritative index of all network connections and devices (including unknown networks, the ‘edge’ of a managed network, and physical, virtual, cloud, mobile assets), identifying devices joining and leaving the network, and uncovering possible segmentation leak paths.

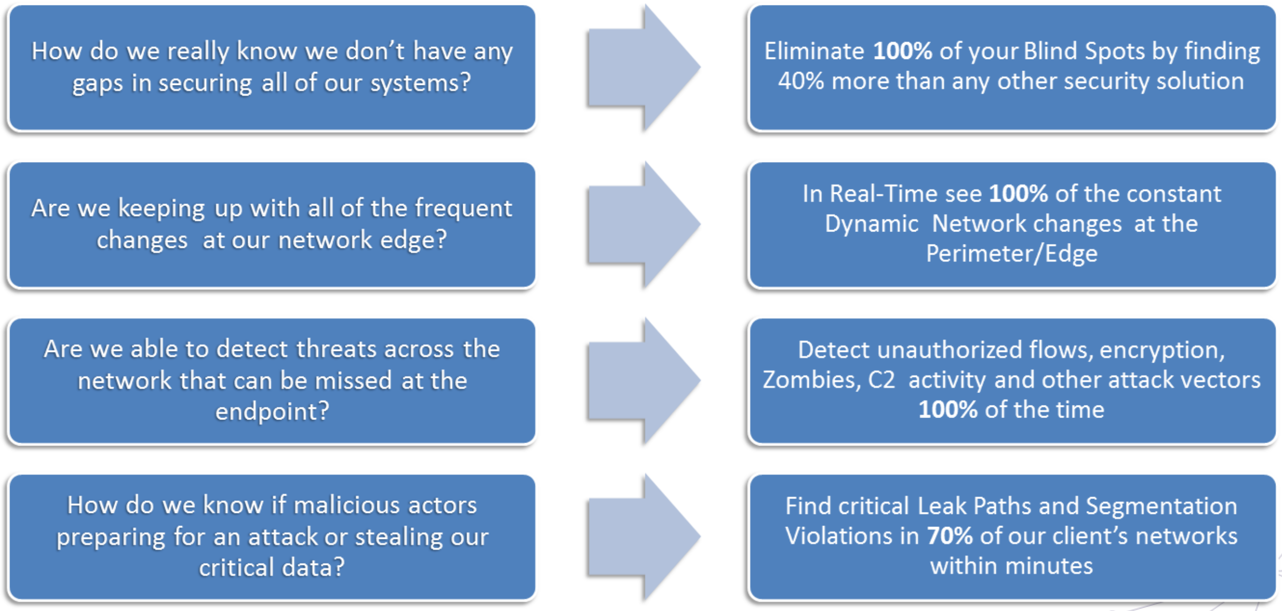
Lumeta Spectre inserts itself into the network control plane and uses active and passive indexing techniques to evaluate network state in real time. Real time is required in today’s cloud, virtual, mobile and software defined world. If it's not in real time you can miss it, which may lead to severe difficulties in locating a leak path after a breach. Traditional static or scan-based “network management”, “performance management”, “modeling” or “discovery”, tools that require “credentialed” access to evaluate network infrastructure will always miss the unknown, dynamic or rogue infrastructure that malicious actors will embed on the network to cause chaos or pursue fraudulent activities.

IT teams need further examination into the following areas:

- Identify and monitor 100% of the networks connections and devices at anytime
- Understand all aspects of the network environment – physical, mobile, virtualized, cloud (private, public and hybrid) along with usual netflow behaviour
- Expose potential problems, such as cyber threats, unplanned Internet connections, unmanaged devices and unsecured ports in real time so these maybe shut down and monitored in real-time for instant visibility – and quick response
- Know which virtual devices are present in the virtual/cloudinfrastructure,
- What is the status of shadowserver and are there any concerns?
- Are or could users be putting up and/or configuring virtual machines instead requesting IT support? Could IT identify rapidly if this was occurring - near real time - or could they sit on the enterprise network unnoticed?
- How could you identify split tunneling which would allow leakage between virtual environments, perhaps even between two virtual environments that are completelyunrelated?
- Is there any anomalous cybersecurity behaviour on the virtual enterprise, large netflows?

What Can Lumeta Spectre Do For You?

The ONE solution to Close the Gaps in Your Security Stack



How do we really know we don't have any gaps in securing all of our systems?

Eliminate **100%** of your Blind Spots by finding 40% more than any other security solution

Are we keeping up with all of the frequent changes at our network edge?

In Real-Time see **100%** of the constant Dynamic Network changes at the Perimeter/Edge

Are we able to detect threats across the network that can be missed at the endpoint?

Detect unauthorized flows, encryption, Zombies, C2 activity and other attack vectors **100%** of the time

How do we know if malicious actors preparing for an attack or stealing our critical data?

Find critical Leak Paths and Segmentation Violations in **70%** of our client's networks within minutes

Contact Lumeta today for a demo of Lumeta Spectre