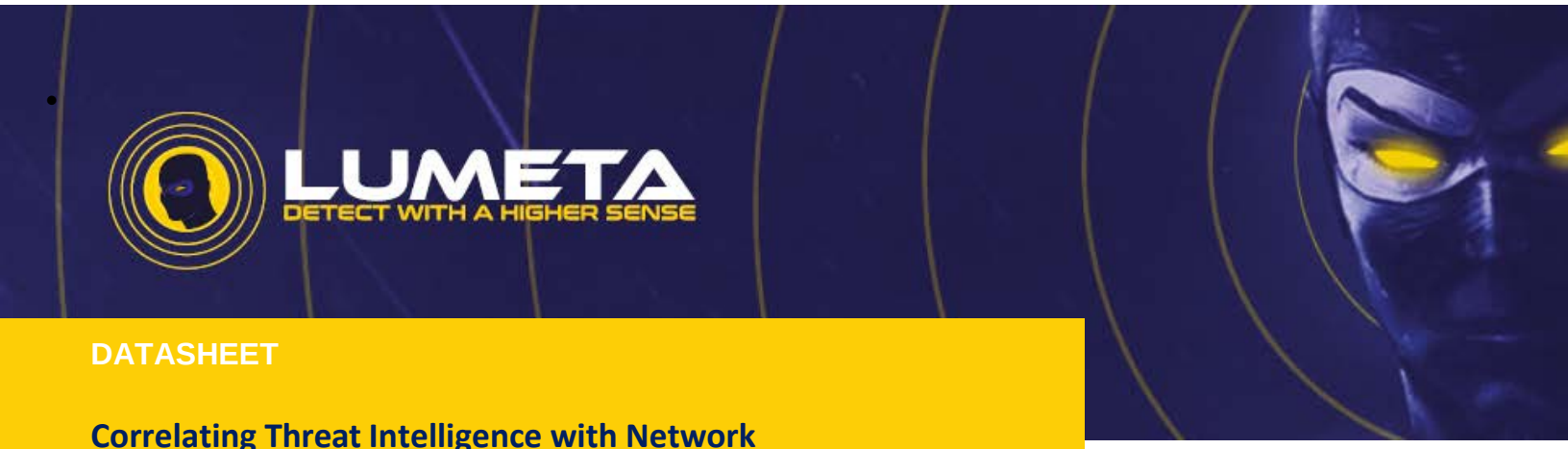


DATASHEET

Correlating Threat Intelligence with Network Situational Awareness for Real-time Cybersecurity Breach Analytics Accenture iDefense and Lumeta Spectre Integration

Using Accenture, Inc.'s iDefense Threat Indicators feed and Lumeta Spectre together gives information security and risk management professionals relevant, timely, contextual and actionable security intelligence, enabling them to make smarter decisions to defend against new and evolving cyber threats.

The Challenges
Businesses and governments are faced with a growing and evolving cyber threat landscape made up of criminals, hacktivists and cyberspies. Attacks are complex and multi-vectored and can be difficult to detect and mitigate. At the same time, organizations' critical infrastructure is spread among a shifting IT environment (cloud, mobile, virtual, on-premises).

The challenge remains **how does one maintain security when presented With** the growing attack surface and a diverse IT environment?

Benefits of the Accenture iDefense – Lumeta SPECTRE Integrated Solution Crafting effective defenses depends greatly on actionable intelligence and complete network visibility.

Accenture iDefense leverages an extensive intelligence-gathering network, proven methodology and highly skilled professionals to deliver comprehensive, actionable threat indicator data (actors, malware, targets, etc.) about existing or emerging cyber threats.

HIGHLIGHTS

- The Accenture iDefense Security Intelligence Services Threat Indicators feed offers organizations 24x7 access to timely and actionable cyber intelligence related to malicious code and global threats.
- Lumeta SPECTRE provides real-time authoritative indexing of all IP address space for complete network visibility across physical, virtual, mobile and cloud infrastructure.
- The Accenture-Lumeta integration enables customers to strengthen their security posture by using sophisticated cybersecurity insights to proactively detect, analyze, prioritize and mitigate cyber threats.
- Answer questions such as: Are there live interactions with adversaries occurring on my network right now? Has any of the enterprise network infrastructure become a zombie participant in a botnet?
- Help protect high-value assets, customer information, revenue and brand against nefarious activity by securing the network presence.

Lumeta Spectre network situational awareness provides an authoritative index of all devices (and networks with devices), whether physical, mobile, virtual or cloud. And, in real time, Lumeta immediately detects new devices connecting to the network. Together, the Accenture iDefense Threat Indicators feed and Lumeta Spectre help empower security teams to make timely and intelligent decisions critical to protecting their business. The combination of real-time network visibility and threat intelligence enables organizations to proactively identify cyber espionage, criminal activity or hacktivism. The threat intelligence aids in keeping organizations current with the evolution of cyber threat methods, while the network visibility maintains awareness of the dynamic network environment.

By identifying threats before they can establish a strong foothold within an organization, companies can reduce the likelihood and severity of these high-impact incidents and help protect their intellectual property, financial assets, reputation and customers' personally identifiable information (PII).

How Does It Work?

Via API access, the Acccenture iDefense Security Intelligence Services Threat Indicators feed is automatically integrated into the Lumeta Spectre network situational awareness platform. This provides users with complete network visibility, threat intelligence and the context needed to analyze and take action.

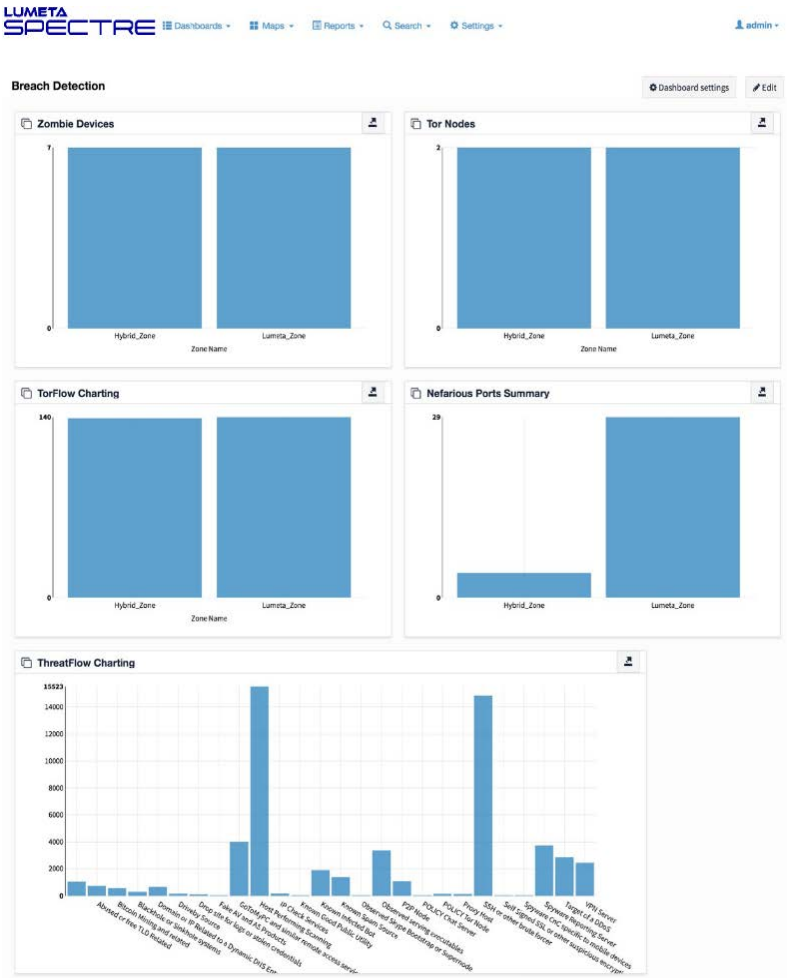
- Lumeta Spectre parses the Accenture iDefense Threat Indicators feed to enumerate known bad servers, networks and associated attributes.
- That intelligence is then correlated – automatically and in real time – against Spectre's authoritative index of network IP address space.
- Suspect devices are reported and mapped by Lumeta Spectre. This information is available in the Lumeta Spectre Dashboard for Accenture iDefense, as well as reports and maps, facilitating identification and remediation of vulnerable and compromised assets.
- The findings help enable IT security teams to analyze threats, prioritize and take action.

Use Cases

Identify Live Interaction with Adversaries (Threat Flows)

Detect breaches via real-time and forensic analysis of conversations occurring between devices on the network and known malware command and control (C2) servers.

- Lumeta SPECTRE ingests NetFlow traffic from the enterprise network as well as the Accenture iDefense Threat Indicators feed, and executes real-time correlation between them.
- This allows for **real-time and forensic analysis** of actual conversations occurring between devices on the network (internal origination points) and known bad actor IP addresses supplied by Accenture's iDefense Threat Indicators feed. Lumeta Spectre validates when communications are occurring from **specific devices** inside the network to these addresses now, or when those communications occurred historically.



iDEFENSE® SECURITY INTELLIGENCE

Now part of

Accenture

Security

Lumeta Spectre Breach Detection Dashboard – Real-time indexing coupled with Accenture iDefense Threat Indicators feed

Hunt Zombies/Bots

Determine whether or not any trusted/enterprise assets are malware-infected infrastructure (participating in C2 botnet).

- Lumeta Spectre correlates its full index of the enterprise IP address space against known bad IP addresses to find devices that are blacklisted (listed in the Accenture iDefense Threat Indicators feed as zombie/bot machines). It raises a flag regarding any potentially compromised machines

Lumeta Corporation | 300 Atrium Drive, Suite 302 | Somerset, NJ 08873 USA | +1.732.357.3500 | www.lumeta.com

LUMETA
DETECT WITH A HIGHER SENSE