Lumeta
Network Situational Awareness

DATA SHEET

Complete Vulnerability Management Across the Entire Enterprise

Lumeta IPsonar and Qualys Integration

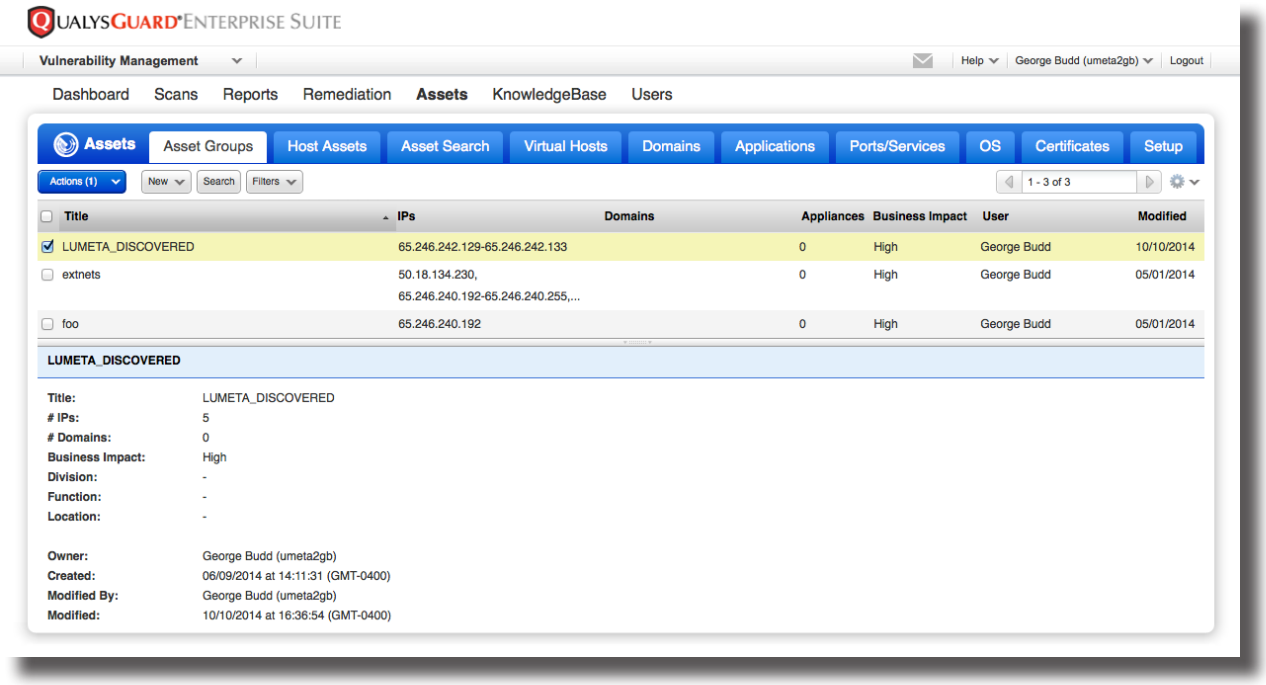
Device and network vulnerabilities throughout the enterprise can be targeted for exploitation, which may result in unauthorized entry into a network, exposure of confidential information, violation of privacy provisions, or paralysis of business operations. Not knowing about a vulnerability that actually exists in your network places your network at serious risk.

Most successful attacks are preventable with a properly implemented and effective vulnerability management program. A successful vulnerability management program needs to encompass the entire network – all connections and devices within the network – to provide a comprehensive assessment of the enterprise.

IPsonar provides best-in-class network situational awareness enabling customers to close the gap on network visibility and gain comprehensive network intelligence on every connection, device and leak path across the enterprise. Customers that deploy IPsonar in conjunction with Qualys VM are able to reduce operational risk and gain control of IP-enabled systems. The combination of IPsonar and Qualys provides automated discovery, identification, and protection of network assets that had previously represented security vulnerabilities across a more comprehensive view of the enterprise network.

Integration of the Lumeta IPsonar network situational awareness solution with Qualys Vulnerability Management (VM) brings together comprehensive network visibility and vulnerability scanning, enabling a more complete picture of security posture within an organization's enterprise and, therefore, an improved ability to quickly remediate identified risk.

Lumeta IPsonar excels at discovering an organization's connected network space (including hidden and unknown networks and devices), providing a clear definition of the network. Qualys VM excels at detecting vulnerabilities on any device connected to the network. When these two solutions join forces, gaps in vulnerability management coverage are eliminated, allowing an organization to get a true assessment of its security posture.



The connector compares IPs discovered by IPsonar against known/subscribed IPs in Qualys, and then creates an asset group of previously unknown IPs in Qualys.

The Capabilities and Benefits of the Lumeta-Qualys Integration

The integration combines the reach of IPsonar's network discovery with the depth of Qualys' vulnerability scanning of devices to deliver comprehensive vulnerability management. In simple terms, IPsonar maps all the residences in a town allowing Qualys VM to go door to door asking questions.

Step 1: Track Inventory and Categorize Network Assets

You can't measure risk if you don't know what you have on your network. In order to fix vulnerabilities, you must first understand what assets you have in your network. Discovering an accurate inventory of your assets helps you determine the areas that are most susceptible to attacks.

IPsonar gives users the capability to perform a full discovery of your networked assets on a global scale, enhancing Qualys VM's vulnerability scanning function. Identifying your inventory and categorizing assets establishes an evaluation baseline.

Step 2: Scan Systems to Find Vulnerabilities

Check hosts (any combination of IP numbers, ranges of IPs, and asset groups) to find any vulnerabilities that may exist on your network.

What should you scan? Hosts and devices that may introduce risk to the enterprise, including Web Servers, SMTP/POP Servers, FTP Servers, Firewalls, Databases, eCommerce, LDAP Servers, Load Balancing Servers, Switches and Hubs, Desktops, Mobile Devices, Virtual Machines, Cloud Instances. You also need to scan hosts and devices on business partners, in particular those with connections back to your network. Some business regulations require scans for business partners to ensure the confidentiality, integrity, and availability of personally identifiable information – whether for customers, employees, or partners.

Step 3: Remediate Vulnerabilities

Eliminate network weaknesses that leave your business exposed and at risk. A post-scan report reveals actual vulnerabilities and states what you need to fix in order of priority.

Step 4: Repeat

New devices appear frequently on a network in this day of virtualization and cloud computing. You need to incorporate steps 1-3 as new devices are attached to the network.

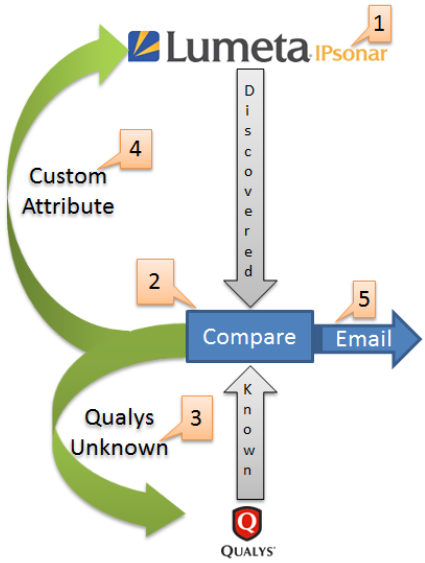
Also, new vulnerabilities appear every day due to flaws in software, faulty configuration of applications and IT gear, and (dare we say it?) good old human error. Whatever their source, vulnerabilities don't go away by themselves. Their detection, removal, and control require comprehensive vulnerability management.

How Does It Work?

The Lumeta-Qualys connector gets installed, configured and runs on IPsonar, and then connects to a Qualys instance. The connector allows users to compare IPs discovered by IPsonar against those known by Qualys VM, creating an asset group in Qualys VM for future scanning.

The integration between Lumeta IPsonar and Qualys VM works as follows:

1. User launches an IPsonar network discovery
2. The connector compares IPs discovered by IPsonar against known/subscribed IPs in Qualys VM
3. The connector creates an asset group and adds previously unknown IPs in Qualys VM
4. The connector tags each IPs within IPsonar indicating whether or not it is known/subscribed by Qualys VM
5. The connector sends an email alerting users of discovered devices, including those which have been added to Qualys VM asset group



Workflow of the integration between Lumeta IPsonar and Qualys Vulnerability Management

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