PRODUCT OVERVIEW

LogRhythm and Qualys®: Integrated Enterprise Security

LogRhythm

LogRhythm and Qualys have developed an integrated solution for comprehensive enterprise security intelligence and threat management. LogRhythm's advanced correlation and pattern recognition automatically incorporates vulnerability data imported directly from Qualys, delivering real-time cyber threat protection based on up-to-date situational awareness and comprehensive security analytics.

The integration provides:

- Real-time situational awareness via a QualysGuard VM feed that identifies and catalogs assets and discovers vulnerabilities at the scale of customers' organizations
- Alarm capabilities that notify users when imported vulnerabilities match preset thresholds
- Normalized QualysGuard vulnerability data that can be used in LogRhythm's SIEM correlation engine to help users prioritize events

LogRhythm for Enterprise Security Intelligence

- ☑ Real-time event contextualization for enterprise security intelligence
- ☑ Adaptive defense for protecting vulnerable assets
- ☑ Focused and automated vulnerability scanning for targeted devices
- ☑ Tight integration for consolidated threat management

By leveraging QualysGuard's open platform and APIs to feed accurate and timely vulnerability data into LogRhythm's Security Intelligence Platform, customers enjoy industry leading enterprise security intelligence and threat management capabilities. The combination delivers the ability to monitor and secure the entire range of systems and applications throughout the IT environment and to respond to security threats based on accurate, relevant and up-to-date information.

LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning Security Intelligence Platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence. LogRhythm delivers:

- Next Generation SIEM and Log Management
- Independent Host Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the art Machine Analytics
  - Advanced Correlation and Pattern Recognition
  - Multi-dimensional User / Host / Network Behavior Anomaly Detection
- Rapid, Intelligent Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's Smart**Response**™
- Integrated Case Management

Qualys

Qualys, Inc., is a pioneer and leading provider of cloud security and compliance solutions with over 5,800 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The QualysGuard Cloud Platform and integrated suite of solutions helps organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including BT, Dell SecureWorks, Fujitsu, IBM, NTT, Symantec, Verizon, and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

LogRhythm and Qualys are tightly integrated, combining the value of best-of-breed vulnerability management with the threat management capabilities of LogRhythm. The combined offering empowers customers to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.

Protecting Vulnerable Assets

Challenge Many organizations don't have the ability to tie current vulnerability data to potential threats and ongoing attacks. This results in a lack of visibility into which threats are immediately relevant and which can be ignored, hindering the organization's ability to respond quickly and appropriately.

Solution LogRhythm can incorporate the results of Qualys vulnerability scans into automated advanced correlation rules. This delivers highly focused alerts that identify when an attack designed to exploit known vulnerabilities is impacting a vulnerable device.

Additional Benefit Smart**Response**™ Plug-ins are designed to actively defend against attacks by initiating actions that neutralize specific cyber threats. These include adding attacking IPs to firewall ACLs, disabling accounts that may have been compromised and terminating suspicious processes and services.

Adaptive Defense

Challenge When a security incident takes place, organizations need assurances that the steps they have taken to secure their network have been successful. Performing a vulnerability scan on the entire network in response to any potential incident is inefficient, however knowing which devices to scan is difficult.

Solution When a security incident or attack has taken place, LogRhythm identifies which devices have been targeted and/or successfully impacted, and includes all relevant context in the alarm. Using this context, an out-of-the-box Smart**Response**™ plug-in can automatically initiate an ad-hoc vulnerability scan on only the impacted devices.

Additional Benefit Smart**Response**™ can dynamically adapt LogRhythm alarms to stay up-to-date without manual intervention by automatically adding vulnerable devices to a list. Alarms designed to detect vulnerability exploits use those lists to identify legitimate targets for increased accuracy.