LogRhythm and Rapid7 have developed an integrated solution for comprehensive enterprise security intelligence and threat management. LogRhythm automatically incorporates vulnerability data imported directly from Nexpose via API, as well as penetration testing results from Metasploit, delivering real-time cyber threat protection based on up-to-date situational awareness and comprehensive security analytics.

The integration allows you to:
- Gain visibility into the security risk of your entire IT environment including networks, operating systems, web applications and databases and correlate it against specific user, network and host activity for true enterprise security intelligence.
- Integrate vulnerability management, penetration testing and multi-dimensional behavioral analysis for truly accurate vulnerability assessment and breach detection and prevention.
- Expose security threats including vulnerabilities, misconfigurations, and exposures associated with malware, and correlate them against potentially malicious application, host, network, and user behavior.
- Prioritize threats, get specific remediation guidance for each issue and initiate automated responses.

By correlating Rapid7’s comprehensive vulnerability data and focused penetration testing results with the multidimensional behavioral analytics capabilities of LogRhythm’s Security Intelligence Platform customers enjoy comprehensive enterprise security intelligence and threat management capabilities through the integration of three industry leading technologies. The combination delivers the ability to monitor and secure the entire range of systems and applications across your organization 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 SmartResponse™
- Integrated Case Management

Rapid7
Rapid7 is a leading provider of IT security risk management software. Its integrated vulnerability management and penetration testing products, Nexpose and Metasploit, and mobile risk management solution, Mobilisafe, enable defenders to gain contextual visibility and manage the risk associated with the IT infrastructure, users and threats relevant to their organization. Rapid7’s simple and innovative solutions are used by more than 2,000 enterprises and government agencies in more than 65 countries, while the Company’s free products are downloaded more than one million times per year and enhanced by more than 175,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a “Top Place to Work” by the Boston Globe. Its products are top rated by Gartner®, Forrester® and SC Magazine. The Company is backed by Bain Capital Ventures and Technology Crossover Ventures. For more information about Rapid7, please visit www.rapid7.com.
LogRhythm and Rapid7 are tightly integrated, combining the value of Rapid7’s best-of-breed vulnerability management and penetration testing software with the threat management capabilities of LogRhythm. The combined offering empowers customers to identify behavioral anomalies, internal and external threats, and prevent breaches 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, hindering the organization’s ability to respond quickly and appropriately.

**Solution** LogRhythm can incorporate the results of Nexpose vulnerability scans into automated advanced correlation rules. This delivers highly focused alerts that warn when attacks designed to exploit known vulnerabilities are impacting a vulnerable device.

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

**Breach Protection**

**Challenge** When a security incident takes place organizations need assurances that the steps they have taken to secure their network have been successful. Penetration testing can automate the process of identifying high risk exposures, but stops short of alerting when a vulnerability is actually being exploited.

**Solution** Once a Metasploit penetration test has been performed, a LogRhythm SmartResponse™ plug-in can automatically create high priority lists of vulnerable users, hosts or devices based on specific findings such as weak passwords, exposed data or poorly managed vulnerabilities. Associated alarms, investigations and reports are automatically updated to deliver highly targeted details based on accurate risk data.

**Additional Benefit** LogRhythm can initiate additional protections, such as disabling accounts with weak passwords, alerting on attempts to access exposed critical data, and removing access to vulnerable hosts.