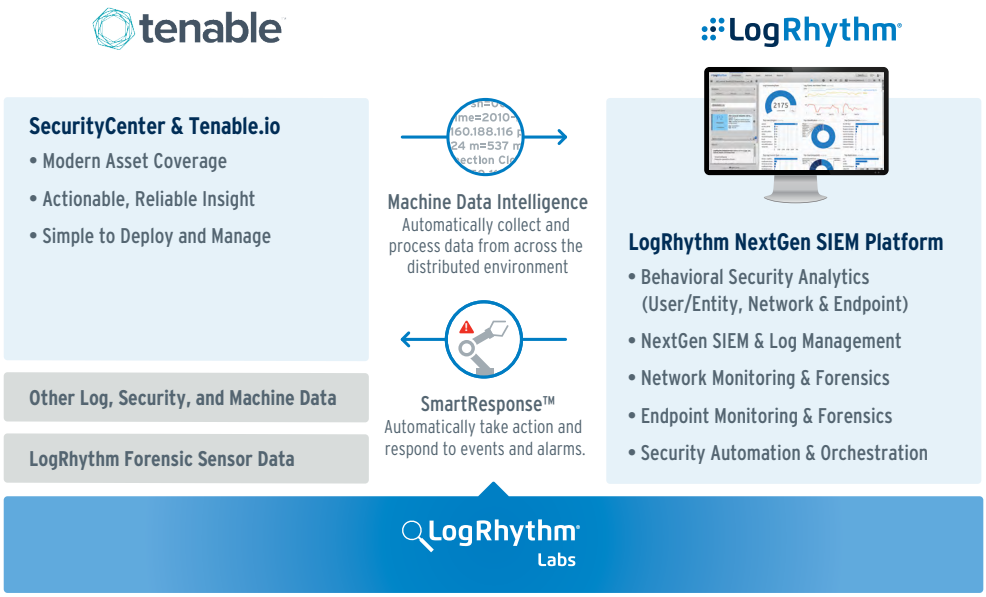
LogRhythm and Tenable: Integrated Enterprise Security

LogRhythm and Tenable have developed an integrated solution for comprehensive enterprise security and threat management. LogRhythm automatically incorporates vulnerability data imported directly from SecurityCenter and Tenable.io via API, delivering real-time cyber threat protection based on up-to-date situational awareness and comprehensive security analytics.

The integration allows users to:

- Gain visibility into the security risk within your entire IT/OT environment to include cloud, mobile devices, containers, and web applications by identifying assets within defined ranges as well as the applications running on those assets
- Expose security threats including vulnerabilities, misconfigurations, and exposures
- Establish timelines and thresholds for remediation and exceptions
- Leverage detailed analysis from factors such as the removal of vulnerable libraries, registry keys, and whether a remediation has taken place
- Utilize Tenable risk scoring based on impact, ease of exploit, and age to create automated responses

By correlating Tenable's comprehensive vulnerability data with the multidimensional behavioral analytics capabilities of LogRhythm's NextGen SIEM, customers enjoy comprehensive enterprise security and threat management capabilities. 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.



About LogRhythm

- Empowers organizations to rapidly detect, respond to, and neutralize damaging cyber threats with NextGen SIEM
- Unifies user and entity behavior analytics (UEBA), network traffic and behavior analytics (NTBA), and security orchestration, automation, and response (SOAR)
- Serves as the foundation for the AI-enabled SOC via LogRhythm's Threat Lifecycle Management (TLM) workflow
- Measurably secures cloud, physical, and virtual infrastructures for both IT and OT environments
- Recognized as a Leader on the Gartner SIEM Magic Quadrant

About Tenable

Tenable™, Inc. is the Cyber Exposure company. Over 24,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver Tenable.io, the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 20 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

LogRhythm and Tenable are tightly integrated, combining information from the world's first Cyber Exposure platform with the threat management capabilities of LogRhythm's NextGen SIEM. The combined offering empowers customers to identify behavioral anomalies and internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.

LogRhythm for Integrated Enterprise Security Intelligence

- Dynamic defense for detecting and stopping unauthorized network threats
- Multi-dimensional behavioral analytics to deliver real-time security intelligence
- Deep visibility into all aspects of user, network, and endpoint behavior activity throughout the IT environment
- Tight integration for consolidated threat management

Use Case: 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 Tenable 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 neutralize specific cyber threats. Leveraging the Tenable.io API, security analysts can launch a vulnerability scan against a specified IP address or hostname, display those results, and allow for searches of vulnerability CVEs within those results.

Use Case: Adaptive Defense

Challenge:
When a security incident takes place, organizations need assurances that the steps they take to secure their network are successful. Performing a vulnerability scan on the entire network in response to any potential incident is inefficient and 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 if applicable, successfully impacted) and includes all relevant context in the alarm. Using this context, a SmartResponse™ plug-in can automatically initiate an ad-hoc vulnerability scan on only the impacted devices.

Additional Benefit:
SmartResponse™ 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.