LogRhythm and Cylance for Integrated Threat Discovery and Remediation

LogRhythm and Cylance have partnered to deliver enterprise-wide threat prevention, analysis, and response. The LogRhythm NextGen SIEM platform continuously collects, normalizes, and analyzes rich, dynamic endpoint telemetry captured by CylancePROTECT. Cylance data is then combined with the petabytes of other machine data LogRhythm collects and analyzes from across the distributed environment. This analysis provides a holistic view of malicious activity and enables proactive detection of threats originating from or targeting an endpoint before they can result in a high-impact incident or data breach.

The integration between LogRhythm and Cylance allows mutual customers to:

• Detect and prioritize intrusions faster by correlating detailed endpoint activity with other environmental data to recognize early indicators of potential compromise
• Adopt a prevention-first methodology, using machine learning that harnesses algorithmic science and artificial intelligence to determine whether objects are good or bad in real time
• Visualize high-priority events in a Cylance-focused dashboard within LogRhythm’s centralized console
• Automate investigatory and response processes, including deployment of real-time countermeasures on an endpoint to prevent further impact and expedite incident response
• Streamline processes that were once largely manual, such as attack analysis and adaptive threat defense
Use Case: End-to-End Threat Management

Challenge:
Your security team is faced with numerous alarms and alerts. Filtering and prioritizing events consumes a security team's already-constrained resources. Your organization needs the ability to correlate data from disparate security products and effectively distinguish the real threats from false alarms.

Solution:
LogRhythm collects and processes endpoint data from Cylance and analyzes it centrally alongside diverse machine data. Correlating log data from multiple sources generates prioritized alerts to identify suspicious activity within the environment.

Additional Benefit:
SmartResponse™ plug-ins enable active defense by initiating actions to neutralize specific cyberthreats. By reducing the time to perform common mitigation steps, SmartResponse helps prevent high-risk incidents from escalating.

Use Case: Prevent the Spread of Advanced Malware

Challenge:
Once an attacker controls an endpoint, they are likely to attempt to compromise additional systems. Left undetected, malware can quickly propagate across the network. It is imperative that security professionals quickly detect compromised endpoints and take immediate protective action to reduce the risk of a high-impact incident or data breach.

Solution:
CylancePROTECT's architecture consists of a small agent that integrates with the LogRhythm Platform. The endpoint detects and prevents malware through tested mathematical models on the host, independent of a cloud or signatures. Cylance provides this telemetry to the LogRhythm Platform, which centrally analyzes it with other event, log, and flow data to detect anomalies and indicators of compromised endpoints. This real-time visibility ensures that security teams are quickly alerted to the first signs of malware within the corporate network.

Additional Benefit:
When suspicious activity is detected, LogRhythm SmartResponse plugins can be executed to rapidly neutralize a potential threat. Actions include “Display Host Status,” which takes host info such as host name or IP and returns scan data and other data about that host, and “Quarantine Global File,” which takes file name/hash as an input and quarantines the file globally.