Ernst & Young estimates by 2021 the global cost of cybersecurity breaches will reach $6 trillion in their Cybersecurity Regained 2017-2018 Report.1 With increasing risk and mounting pressure, security teams face an uphill battle. Unfortunately, many organizations spend a significant amount of time chasing benign threats due to resource limitations and a lack of threat prioritization. At the same time, the increasing number of compliance mandates created in response to the exponential growth of cyber incidents introduces additional challenges for security operations.

How do you defend your enterprise against this onslaught of threats, attacks, and growing compliance mandates with limited resources and expertise? To be successful, you must find flexible and efficient threat detection technologies best suited to your organization’s size, industry, and operational maturity, tailored to gain visibility and context around high-risk areas while limiting exposure to your most valuable assets.

Focus Your Efforts with Targeted and Prioritized Threat Detection

LogRhythm DetectX delivers prebuilt security analytics content and visualizations designed to accurately detect malicious activity while supporting adherence to compliance regulations. Stop wasting time investigating false positives, and shift to a more targeted approach that prioritizes on activity that poses the greatest liability to your organization. Achieve rapid and accurate threat detection through diverse analytical techniques and use case-oriented alarms that produce a comprehensive view of malicious actions across your environment. The breadth of analytics content in LogRhythm DetectX recognizes security-relevant activity, generating prioritized, risk-based alarms for immediate identification of critical threats.

LogRhythm DetectX applies curated threat detection content that identifies patterns of compromise and threat progression to qualify threats faster. Content such as the MITRE ATT&CK module provides threat models and alarms aligned to the adversary tactics and techniques mapped within the framework. DetectX’s comprehensive set of threat detection content enables you to realize immediate value and reduce time spent on false positives, while also providing integration of relevant, actionable threat intelligence for proactive mitigation. LogRhythm’s Threat Intelligence Service (TIS) immediately operationalizes commercial and open-source threat intel to support further corroboration of malicious activity, leading to faster qualification and mitigation.

Benefits

- Maximize your time and resources with more effective threat detection and qualification
- Automatically prioritize security relevant activity to address your most critical threats first
- Achieve immediate value and long-term success through prebuilt, continuously updated threat detection modules
- Avoid costly violations and save time with built-in compliance automation capabilities
- Proactively defend your enterprise by applying relevant, actionable threat intelligence

Features

- Prebuilt analytics modules contain models and alarms that recognize known patterns and characteristics of malicious actors
- Threat Intelligence Service operationalizes both commercial and open-source threat feed information into the NextGen SIEM for threat qualification
- Threat prioritization helps score and prioritize alarms based on enterprise risk
- Consolidated Compliance Support helps teams demonstrate continuous compliance, detecting control-specific violations as they occur

---

1 EY Cybersecurity Regained 2017-2018 Report, page 3
**Simplify Compliance Through Automated Policy Management**

With the continual growth of compliance mandates, organizations are facing multiple challenges around interpreting compliance requirements and implementing the necessary measures to avoid legal consequences. LogRhythm DetectX simplifies adherence to regulatory requirements and provides tools that create awareness and strengthens your overall security posture. Our prebuilt compliance modules automatically detect violations as they occur to remove the burden of manually reviewing audit logs. LogRhythm Labs develops and updates a comprehensive library of compliance modules including PCI, GDPR, HIPAA, and NIST among many others. Compliance content, including rules, investigations, and reports are mapped to the individual controls for each regulation. Our Consolidated Compliance Framework further streamlines your compliance program by providing a core, shared module mapped to multiple regulations, encompassing the most common cybersecurity controls. This reduces the effort spent on setup and correlating multiple, identical alarms across frameworks.

---

**Advance your Security Operations Maturity with the XDR Stack**

By applying a combination of analytical techniques and threat intel, you are solidifying a critical part of your security infrastructure that will act as your most powerful ally against threat actors.

With LogRhythm's modular NextGen SIEM Platform design, your organization can add capabilities and increase its security sophistication as the need arises.

LogRhythm's XDR Stack centralizes all the necessary components to establish a security foundation capable of identifying malicious patterns, uncovering unknown threats, and ensuring rapid threat response and compliance adherence.

---

See DetectX and the XDR Stack in action. Request a demo today.
logrhythm.com/demo