SERVICE OVERVIEW

Incident Investigation & Response Services

LogRhythm®

Augment Your Security Team with Incident Response Experts

LogRhythm's Security Intelligence Platform detects compromises in your environment and gives your team the tools to investigate and contain the threat. But hiring, developing and retaining talented security professionals – particularly those with expertise in forensic investigations and malware analysis – is challenging. These personnel have specialized, rare, and valuable expertise.

With the growing frequency and severity of cyber-threats, it is more important than ever to be prepared to respond quickly. But meeting this challenge isn't getting easier. That is why intrusions that result in a data breach typically persist for over 200 days before being detected.

> *"The average cost of a data breach involving personally identifiable information (PII) was $3.8 million, $154 per record."*
>
> **–Ponemon Institute, 2015**

Incident Investigation and Response (IIR) Services provide critical staff augmentation for LogRhythm customers when they need it most. It connects you with incident response experts who can help you rapidly contain advanced threats impacting your organization.

Incident Response Experts Who Know Your Platform

LogRhythm's incident response experts have decades of experience leading investigations for the world's largest defense contractors, credit card processors, health care and media companies, telecom providers, and other organizations. They also have a deep knowledge of the LogRhythm platform and work alongside other subject matter experts in LogRhythm Labs. This enables them to quickly recognize and shut down emerging threats and then buttress your environment against future attacks with custom AI Engine rules and SmartResponse™ plug-ins.

Incident Investigation & Response Services

LogRhythm IIR Services experts limit an attack's impact on your environment. They work to determine the cause of a compromise, identify targets, define the scope of the impact, mitigate the risk, and protect your environment from similar future attacks. Our team provides these services using your LogRhythm platform, on a retainer or emergency basis, and delivers them remotely for maximum efficiency.

Forensic Analysis

- Investigate the incident using your LogRhythm deployment
- Piece together the whole story of the security event
- Pinpoint the attack sequence
- Identify whether sensitive data was accessed and/or exfiltrated
- Recommend steps to neutralize the threat

Malware Analysis

- Assess and analyze suspected malware using techniques such as static analysis, sandboxing, and reverse engineering
- Provide a report on indicators found throughout your environment

Tactical Containment

- Provide recommendations for incident containment and remediation
- Incorporate threat intel from your incident back into your platform
- Refine LogRhythm security analytics to identify similar attacks
- Implement SmartResponse™ countermeasures to automate response to future attacks

We focus on services that allow us to provide customers unique value. If you require full-scope incident response services or long-term remediation, we can connect you with a trusted services partner.

IIR Services Use Cases

Unknown Malware: A security tool raises an alarm in LogRhythm about a potentially malicious file on a host. Internet searches are not able to adequately identify the file, its functionality, or its business implications. You contact LogRhythm IIR Services to analyze the file, determine if it's malicious, and help you fortify your network.

Advanced Persistent Threat: An alarm appears in LogRhythm identifying a sophisticated network reconnaissance tool on a host. Neither IT nor the user installed the tool. Further investigation suggests that an unauthorized party has been accessing the host for the past six months. You contact LogRhythm's IIR Services to determine the impact of the breach, including what information has been accessed.

Widespread Security Incident: Your security team is working around the clock dealing with a security incident affecting multiple hosts. The added workload has stretched the team so far that day-to-day tasks are falling behind. You contact LogRhythm IIR Services to augment your team to address the incident. LogRhythm experts handle the forensic investigation and then develop signatures for ongoing detection.

Threat Containment: An alarm fires, alerting you of unexpected changes made to the Windows Registry. LogRhythm forensic experts investigate and find that malicious software has been added to the Windows Registry. After remediating the threat, the LogRhythm team implements security analytics and SmartResponse™ plug-ins to instantly detect and neutralize future attacks.

Why LogRhythm IIR Services?

Accelerate response and neutralization of advanced threats by working with IR professionals who can harness the full power of the LogRhythm platform

Maximize ROI by augmenting your team with battle-tested IR experts instead of adding expensive headcount

Prevent similar attacks by fortifying your environment with custom countermeasures