Reliance acsn

Specialists in IT Security Management

Job Description

Role: **LogRhythm Onboarding Specialist**

Role:	LogRhythm onboarding Specialist
Reporting to:	Ben Woodcock – Lead Security Onboarding Specialist
Number of direct reports:	1
Job type:	Permanent role
Location:	Working from home with occasional travel to the Gloucester office

Responsibilities:

- Ensure clients are onboarded onto the SIEM platform with relevant log sources to detect and investigate security intrusions.
- Measure the quality of security telemetry, identify when the logging levels are not sufficient, and provide guidance to clients.
- Troubleshoot availability issues.
- Establish onboarding standards for log sources and ensure clients meet these standards.
- Proven technical understanding of logs from different operating systems and security tooling.
- Ensure the SIEM platform and components are maintained and kept up to date.

KPIs:

KPIs will be reviewed on a monthly basis.

- Onboarding of Key log sources from client environments in a timely manner.
- Identify and resolve SIEM issues within SLA.

Personality profile:

- Take ownership of your responsibilities and ensure they are completed to a high standard.
- Positive and professional attitude
- Be curious and want to learn more.
- Capable of working alone or collaborating within a team.

Skills and experience:

Must Have:

- The fundamental understanding of LogRhythm components, both managing and configuring.
- Understand log sources and how they are used during investigations.
- Experience in deploying and ongoing management of the LogRhythm platform.
- Knowledge of security network devices (e.g. Firewalls, AV, switches, EDR tools.)

Desirable experience:

- Previous experience in one of the following: system administration, networking, cyber security.
- Worked in a previous role onboarding log sources using the LogRhythm SIEM.
- Experience in writing Regular Expressions (RegEx).
- Experience in deploying and ongoing management of the LogRhythm platform.
- Knowledge of complex network architectures.
- Experience in using and managing unix/linux environments.
- Experience in PowerShell or similar scripting language.
- Certifications desirable: LogRhythm Deployment Engineer (LRDE) or LogRhythm Platform Administrator (LRPA)