Reliance acsn

Specialists in IT Security Management

Job Description

Role: **MDR Security Analyst**

Role:	MDR Security Analyst
Reporting to:	Sean Loftus - MDR Team Lead
Number of direct reports:	1
Job type:	Permanent role
Location:	Working from home with occasional travel to the Gloucester office

What you will do:

- Work with a team of exceptional SOC analysts to monitor client environments 24/7/365 on a 12 hour, four on four off shift pattern.
- Provide security monitoring to our clients by detecting security intrusions and writing detailed incident reports and recommendations.
- Monitor and respond to client incidents and requests in line with SLAs.
- Create weekly and monthly management reports.

KPIs:

KPIs will be reviewed on a monthly basis.

- Notify and respond to client incidents and requests within SLA.
- Complete weekly and monthly reports on time.
- Carry out threat detection rule tuning when necessary.
- Ensure all alarms are actioned and completed for your shift.
- Gather regular threat intelligence data.

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:

- Minimum of one year working within an internal SOC, MSSP, or similar.
- Experience using SIEM tools to investigate alerts.
- Understand how attacks are carried out and be able to talk about detection for these attacks from the perspective of multiple log sources.
- Know the difference between IOCs and TTPs.
- Experience investigating phishing emails, malware, brute force, etc.
- Understand log sources and how they are used during investigations.
- Knowledge in one or more areas – system administration, networking, forensics, cyber security, compliance, and incident response.