SOC MDR Manager

The SOC MDR Manager will be responsible for coordinating, scheduling, and project coordination for security related projects and services. The desired candidate will have very strong verbal skills, so they can convey the information properly to clients. They will act as an escalation point for SOC Analyst I/II team from an operational standpoint.

Principle Accountabilities:

- Create, and manage shift schedules
- Ensuring that there is always someone on shift / call-offs/ shift changes / trades etc.
- Ensuring on-call rotation is up to date, and working effectively
- Serve as overall Point of contact for the MDR
- Act as incident commander during high severity incidents, as necessary
- Report MDR metrics
- Responsible for managerial responsibilities such as staffing, performance assessment, career path planning, training, and coaching/mentoring for all MDR team members
- Identify MDR capability enhancements ideas for continuous improvement of services
- Act as a liaison for other entities inside of organization, and challenge other departments as well as receive challenges from other departments on improving our services
- Escalating / involving resources outside of the MDR into current projects, or escalations, or other areas of assistance from outside of the team.
- Constantly improving our current policies, procedures, and standards
- Improving our current setup for tickets, projects, and metrics
- Weekly review of alerts
- Weekly review of reports with appropriate organization members
- Weekly spot check of all solutions to ensure that they are all up/functioning
- Ensuring they are complying with, and adhering to all Information Security Policies as well as privacy policies. They must also ensure they are protecting and keeping secure all client information considered or believed to be private or sensitive.
- Ensuring all security and operational controls are followed and enforced to ensure client data remains secure, available, and private, where applicable.

Experience/Skills:

- SOC / NOC / Blue team experience with 4+ years in a client-facing support role.
- Experience as a System Admin, or Network Administrator
- Knowledge of configuring and implementing technical security solutions (Firewalls, IDS/IPS, Antivirus, SIEM, etc.)
- Strong desire to constantly learn
- Customer –oriented focus with a strong interest to satisfy our customers
- Solid understanding of networking and security
- Knowledge of Windows Operating systems applications
- Knowledge of Linux Operating Systems and applications
- Knowledge of Penetration Testing Operating Systems and applications

Additional Information

- Functioning personal vehicle for transportation and a valid PA driver's license required.
- Preferred Education: Technical or Associate degree in relevant field or 1 year's equivalent experience preferred.
- Some travel and heavy lifting may be required.