SOC Analyst II

The SOC Analyst will be responsible for analyzing, identifying and mitigating customer security alerts, events, or incidents. The desired candidate must document all situations accurately and completely. The desired candidate must possess strong verbal skills to convey information accurately to clients.

Principle Accountabilities:

- First responder to Incidents, and main Point of Contact
- First to backfill open shifts
- Respond to Alerts, events, and incidents per our specified procedures and processes
- Log and record all alerts with ticketing system
- Identify weaknesses in customer infrastructures and suggest improvements
- Technical and analytical skills to handle security events, incidents and threats
- Resolve or escalate events and incidents
- Provide timely and reliable service to customers
- Stay up to date on latest vulnerabilities exploits and any other relevant threat information
- Operation, implementation, and maintenance of security solutions
- Document solutions, processes, or procedures in written, verbal, phone, or in person.
- Requirement for 24/7 on-call work
- Ability to work in a very fast-paced environment
- Assist in creation and maintenance of documentation for SOC procedure and processes
- 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.
- Taking on escalated issues
- Taking on implementation tasks

Experience/Skills:

- SOC / NOC / Blue team / Red team / Purple team experience
- Programming / Shell scripting experience (PERL, Python, Java, Shell, PowerShell, etc.)
- Experience as a System Administrator, 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

- Understanding varying Security standards PTES, Defense in Depth, etc.

Additional Information

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

Classification Information

- Level/Department: Technical Level II
- Reports to: SOC Manager
- Date Reviewed: 04/16/2019