Security Operations Engineer I

The Security Operations Engineer 1 will be responsible for the implementation of all security solutions. The desired candidate will be a subject matter expert in all technical solutions which the security operations center (SOC) offers. The desired candidate will oversee all aspects of implementations and projects from initiation to completion of the project. The desired candidate will allocate time to finding new solutions for those issues which may arise in the security department. The desired candidate must document all situations accurately and completely. The desired candidate must possess strong verbal skills to convey information accurately to clients, and for the training of SOC members.

Principle Accountabilities:

- Technical lead on endpoint security
  - SME in all areas surrounding technology
  - Provide and build implementation strategy and framework - both internally and externally
  - Provide analysts support while executing onboarding/implementation
  - Assist and provide support for all tier 3 and above issues
  - Continuous communication with vendor regarding road map and feature requests
  - Review software/code versions and upgrades in lab environment
  - Continuous review of technology
  - Lead all POC's in this specific area
  - Provide demonstrations to future customers
  - Responsible for all advanced consulting projects
  - Provide knowledge transfer to both SOC analysts and customers
- Technical lead or backup on macro/micro segmentation
  - SME in all areas surrounding technology
  - Provide and build implementation strategy and framework - both internally and externally
  - Provide analysts support while executing onboarding/implementation
  - Assist and provide support for all tier 2 and above issues
  - Continuous communication with vendor regarding road map and feature requests
  - Review software/code versions and upgrades in lab environment
  - Continuous review of technology
  - Lead all POC's in this specific area
  - Provide demonstrations to future customers
  - Responsible for all advanced consulting projects
  - Provide knowledge transfer to both soc analysts and customers
  - Designate a SOC 2 analyst as a back-up lead for macro/micro seg
  -
- Technical lead or backup on SIEM
  - SME in all areas surrounding technology
  - Provide and build implementation strategy and framework - both internally and externally
  - Provide analysts support while executing onboarding/implementation
  - Assist and provide support for all tier 3 and above issues
  - Continuous communication with vendor regarding road map and feature requests
  - Review software/code versions and upgrades in lab environment
  - Continuous review of technology

- Lead all POC's in this specific area
- Provide demonstrations to future customers
- Responsible for all advanced consulting projects
- Provide knowledge transfer to both SOC analysts and customers
- Designate a SOC 2 Analyst as a back-up lead for SIEM

- S.O.A.R. Management
  - Assist in onboarding new and current customers
  - Assist in API integration
  - Assist in building playbooks
  - Assist in reviewing implementation strategy and framework
  - Tier 1,2, and 3 support for all known issues/tickets generated
  - Knowledge transfer to SOC analysts
- Network Security Management
  - Review and assess customer perimeter security
  - Provide health-checks and ruleset reviews
  - Co-manage devices where need be
  - Create security policy when a request is generated
  - Provide knowledge transfer and guidance to customers
- IR responsibilities
  - Assist in technology issues tier 3 and above
  - Assist in deployment strategy and framework
  - Assist when needed and if time allots as 2nd point of contact

Other Accountabilities:

- 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 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.

Experience/Skills:

- SOC / NOC / Blue team experience / Red Team experience
- Programming / Shell scripting experience (PERL, Python, Java, Shell, PowerShell, etc.)
- 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
- 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: Minimum of 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 I
- Reports to: SOC Manager
- Date Reviewed: 06/21/2021