SOC Analyst Level I Responsibilities & Qualifications

We are currently seeking an SOC Analyst to join our team. The chosen candidate for this position must have a love of diverse technologies and IT-related infrastructure. (This is a learning job and we offer many avenues for furthering your craft and sharpening your skillset).

Desired Technical Skills:

- Handle first level response for security events: IDS / IPS alarms, malware (alerting, not triage), account misuse, network security events, etc.
- Able to effectively weed out false positives and make decisions on triage steps.
- Assist in creating new processes and automations for Level 1 events.
- Analyze risk alarms and events for customers.
- Able to work in a fast-paced environment with service level agreements in place across clientele.
- Understand and able to use a SIEM for event investigation.
- Keep up on the latest security news and events, and effectively communicate them to team members.
- Linux skills are a plus, but not required.

Necessary Soft Skills:

- Ability to read and understand written English.
- Ability to clearly communicate on the phone and through e-mail/ticket updates.
- Ability to manage multiple tasks simultaneously and prioritize tasks appropriately.
- Good customer service skills. Note: this job requires you to speak to clients throughout the day, please remember when applying

Education / Experience:

- Associates Degree in Cyber Security or Comparable Preferred, but not required.
- Must be a U.S. Citizen.

Technologies

- UTM Firewalls
- EDR / XDR Platforms
- SIEM
- SOAR Platform

Schedule

- M-F 8AM – 5PM EST
- On-Call Rotation (1-2 Weeks per Month)

Location

- Miamisburg, OH Office (Remote Work for On-Call only)

SOC Analyst Level I Responsibilities & Qualifications