**SOC Analyst (Entry-Level)**

This is an entry-level position in cyber security, targeted toward individuals just coming out of college or very early in their careers. Educational or personal experience with network/systems administration and/or information security related work is necessary, but it is assumed that experience will be limited. This position is designed to create opportunity for growth and career advancement.

**Responsibilities:**

SOC Analysts are responsible for monitoring and maintaining systems used in our internal security program. This includes the following of procedures:

- to triage and investigate security alerts, and escalate issues as necessary.
- SOC Analysts have opportunities for mentorship from more senior members of the team, and involvement with maturing procedures, evaluating new security technologies, incident response, penetration testing, and the freedom to try out new ideas and technologies to improve the SOC. Experience with the following technologies should be referenced by applicants with details about software/hardware versions were relevant:

**OS Skills:**

- Linux – intermediate skill preferred.
- OSX - intermediate skill preferred.
- Windows – Any skill level.

**Scripting Skills:**

- Experience with any of the following is a plus:
  - Bash, batch, perl, python, powershell, c#, awk

**Technologies Used:**

- Firewalls (e.g. PaloAlto Networks, Checkpoint, Cisco ASA, Juniper SSG, PFSense, etc..)
- Routers (e.g. Cisco, Juniper, etc..)
- Log Management and SIEM (e.g. Splunk, IBM QRadar, HP ArcSite, etc..)
- Network Analysis Tools (e.g. NetWitness, Wireshark, etc..)
- System Analysis and Forensic Tools (e.g. FTK, EnCase, etc..)
- Endpoint Security (e.g. Bit9, Carbon Black, Symantec, McAfee, Forefront, etc..)
- Windows Management (e.g. WSUS, SCCM, SCOM, Active Directory, Group Policy Objects, etc..)
- Vulnerability Management (e.g. NeXpose, Tenable Nessus, etc..)
- Penetration Testing Tools (e.g. Metasploit, Backtrack, Kali, etc..)
- Operating Systems (e.g. Windows Server 2008/2012, CentOS Linux, OSX, etc..)
- Enterprise Microsoft Solutions (e.g. Exchange, Sharepoint, Lync, etc..)
- Regulatory Regimes (e.g. ISO27K, SSAE16, HIPPA, PCI, FISMA, etc..)
- Video Surveillance and Physical Access Control Systems

**Requirements:**

- The ideal candidate will have Linux OS and scripting skills. OSX and Windows skills are a plus (in that order).
- BS/BA degree in Computer Science, Information Systems, or related discipline or equivalent experience.
- Prior internship, classwork, or previous work experience in information security and/or related areas, along with a strong appetite to apply such experience in a practical setting
- 0 – 3 years of professional experience. Recent college grads are encouraged to apply. Preference will be given to those with previous work/internship experience in IS/IT/Information Security, and strong record of academic achievement.
- Future aspirations for CISSP, SSCP, or similar security certification
- A love of puzzles and figuring out the unknown
Interested candidates should apply here.