Tier 1 Security Analyst Job Description

Position Summary:
The Tier 1 Security Analyst will possess experience with networking, endpoint protection, and threat intelligence, as well as the functioning of specific applications or underlying IT infrastructure. Acts as a first responder to account/system attacks and compromises to determine threat vectors and provide initial remediation; uses SIEM to monitor/analyze incidents, and works with stakeholders to resolve incidents; escalates incidents when necessary using policies and procedures; and will be closely involved in developing, tuning, and implementing threat detection analytics.

Responsibilities:
- Act as network incident first responder for a staffed SOC, reviewing and verifying system alerts
- Assist with the development of incident response plans, workflows, and SOPs
- Maintain security sensors and tools
- Monitor security sensors and review logs to identify intrusions
- Escalate security incidents using established policies and procedures
- Uses tools and techniques to perform initial extraction, de-obfuscation, or other manipulation of malware related data
- Perform initial analysis of security events, network traffic, and logs to engineer new detection methods, or create efficiencies when available
- Work directly with cyber threat intelligence analysts to convert intelligence into useful detection
- Collaborate with incident response team to rapidly build detection rules as needed
- Identify incident root causes and take proactive mitigation steps
- Perform lessons learned activities
- Review vulnerabilities and track resolution
- Review and process threat intel reports
- Implement detection use cases
- Implement IDS signatures
- Assist with incident response efforts
- Provide critical information for customer report briefs
- Participate in customer security assessments
- Participate in table top exercises

Job Requirements:
- Understanding of root causes of malware infections and proactive mitigation
- Understanding of lateral movement and footholds

- Understanding of data exfiltration techniques
- Demonstrated ability in critical thinking, problem solving, and analytics
- Enjoy analyzing patterns looking for outliers
- Enjoy creating ways to find needles in haystacks
- Have real world experience analyzing complex attacks and understand TTPs of threat actors
- Define relationships between seemingly unrelated events through deductive reasoning
- Experience in network/host based intrusion analysis, malware analysis, forensics, and cyber threat intel
- Knowledge of advanced threat actors and complex attacks
- Possess excellent writing skills and the ability to communicate to teammates as well as technical and executive level staff
- Quick study with new tools
- Basic knowledge of Splunk
- Knowledge of network routing and switching fundamentals

Required/Desired Skills:

- Technical understanding of operating systems, network architecture, design, and Active Directory (AD)
- Knowledge of encryption, key management, and cryptology
- Experience performing threat modeling, risk analysis, root cause analysis, risk identification, and risk mitigation
- Experience with planning and implementing secure networking practices such as: application segmentation, network segmentation, NAC and other access control testing/validation, updating access control SOPs
- Understanding of configurations and experience with an enterprise SIEM solution including signature tuning, development of correlation rules, reports, and alarms

Required Education and Experience:

- Degree in Computer Science, Cyber Security, or equivalent

  OR

- Technical certifications such as: GIAC, CCNA, CCNP, PCNSE, CEH, etc.

  OR

- 1-2 years of relevant experience working in a SOC environment