L1 Analyst (SOC)

The security operations centre is a team dedicated for providing first response to security incidents, and is focused on the operational aspect of web-application security: analysing the threat, suggesting immediate methods of remediation and mitigation and actively working to block attacks is real-time.

The scope of activity ranges throughout the layer 7domain. Encompassing DoS & DDoS attacks, Brute-Force attacks, Scraping and filtering of unwanted traffic, and also extending into initial analysis and mitigation of application attack vectors, such as XSS, SQLi and Remote code execution.

The SOC will work closely with the first tier support team, acting as a focal point for security related events and incidents. We are hiring professionals for project deployment and their duties and responsibilities will be as follows :

Responsibilities:

- Monitor security technologies for alerts
- Conduct hunts (specialized searches) for evidence of compromise
- Tracking suspicious network, application and user behaviour
- Investigating breaches, gathering evidence, and analysing data
- Manage, tune and optimize security controls such as NGFW, IDS/IPS, SIEM, network anomaly detection, endpoint security, vulnerability management, data loss prevention (DLP)
- Performing risk assessments
- Write up findings and provide recommendations.

Skills Required:

- Bachelor’s Degree in a related field or equivalent demonstrated experience and knowledge
- Minimum 1 year in hands-on IT role that can include either system or network administration
- Deep understanding of network and application layer protocols
- Some experience with SIEM. NGFW and endpoint security technologies.
- Excellent communication skills
- 1+ years of experience with any SIEM (preferably LogRhythm)
- 1+years of experience managing NGFW like Fortinet, Palo Alto Networks etc
- 1+years of experience with endpoint security, like Symantec, McAfee etc
- Hand-on experience in Unix/Linux and Windows administration
- Understanding of incident response procedures and practices
- Formal incident response training or certificate, such as SANS
- Must be able to word weekends, evenings, and on-call
- Excellent knowledge and experience with a wide variety of IT technologies and security solutions. Day-to-day operation and interactions
- Troubleshooting skills and experience
- Able to create excellent relationship with your customer and internally across internal teams- Systems Engineering, Marketing, Professional Service etc.
- Exemplary communication and interpersonal skills
- A willingness to be challenged and a strong desire to learn

- Fluent in English
- Security certifications, CISSP, CISM, Security+, CEH, etc are a added advantage. Support the SOC Manager in the preparation of SOC management and statistical reports.
- Strong foundation in Internet protocols (TCP/IP) and security concepts.
- Strong ability to understand and analyse log and network packet data.

Additional Information

- Office Hours: Monday - Friday, 9am - 6pm
- Smart Casual Fridays
- Salary is negotiable depending on experience
- Welfare
- Social Security
- Health insurance
- Incentive
- Bonus
- Holidays