cybArmor

https://cybarmor.com/careers/cyber-security-engineer-2/

SOC Analyst

Hiring organization
cybArmor

Employment Type
Temporary

Job Location
Remote work possible

Date posted
March 20, 2024

Description

We pride ourselves on being mission-focused on helping to grow a brand built on accuracy and integrity. We care deeply about our products and our customers. We're more than just a company: We help millions of consumers make more-informed decisions every day. We know that our teammates are our most valuable asset, and we value a balanced life while tackling challenging projects in a fast-paced environment. One last thing: Our four-day week continues in Summer 2024!

The Cyber Security Engineer role will have significant responsibility in securing cybArmor\'s networks, systems, and applications. This position will work closely with data center, cloud, and security teams as well as third-party organizations to ensure that security, privacy, and compliance solutions are adequately designed and integrated into our IT operations. This position will monitor and research current trends in the industry to optimize and align our IT operations security processes to model industry best practices.

This role has an expectation of 3 days in the London, Ontario office per week, subject to change based on future business needs.

Responsibilities

- Develop a deep working knowledge of cybArmor's network architecture, customized system functions and dependencies, and how security infrastructure, controls, and processes protect critical data and assets.
- Design, build, and assist with solutions and core security projects related to network architecture.
- Perform threat hunting, event analysis, and investigations tailored to our threat environment.
- Operate and maintain vulnerability scanning tools to identify and remediate security weaknesses.
- Serve as a subject matter expert and provide expertise on topics related to network security.
- Monitor the general security landscape and research current trends in the industry to optimize and align Information Security processes to industry best practices.
- Conduct detailed assessments of network security systems and access rules to ensure they are appropriate, secure, and defensible based on least privilege.
- Enhance network security posture to better protect against attacks and detect new threat vectors.
- Participate in supporting a diverse, distributed, and agile environment.
- Self-organize and prioritize activities independently.
- Create and maintain documentation and perform status reporting.
- Build working relationships with business and operational units across the organization.

Qualifications

- Bachelor of Science degree in Computer Science, Information Assurance, or a related field with a minimum of 3-5 years hands on experience in a security engineering role.

- Preference for CISSP, GIAC, CCNA Security, Security +, CCNP Security, PCNSE certifications.
- Understanding of OSI stack – L2, L3, TCP, UDP, common ports.
- Experience with network protocols (TCP/IP, host, and network-based access controls, routing and switching), DNS/DNSSEC.
- Solid understanding of transport layer security (TLS)
- Working knowledge of security tools/languages including NMAP, Nessus, Kali Linux, Python, etc.
- In-depth experience with Incident Response, digital forensics, and knowledge of Windows functionality. Ability to perform forensic analysis with common security analysis tools.
- Experience with cloud technologies including SaaS, PaaS, IaaS, FaaS.
- Knowledge of Cisco FW, Cisco ISE, Palo Alto, AWS network security, and ELK Stack
- Understanding of Group Policy and Local Security Policy
- Familiarity with Backup and Disaster Recovery best practices
- Windows Server permissions (Global Groups, Universal Groups, Domain Local Groups)
- Base level understanding of Virtualization
- Knowledge of security operations concepts such as perimeter defense, data loss protection, insider threat, kill-chain analysis, risk assessment, common security frameworks, Multi-Factor Authentication solutions (Okta, Auth0) and VPN architecture.
- Experience with conducting firewall reviews, including firewall rule audits and risk assessments.
- System hardening experience utilizing CIS benchmarks and CIS-CAT tools.
- Working knowledge with automation and monitoring platforms (Chef, New Relic, Zabbix, etc.)
- Experience with VMware and Windows/Linux based systems

Job Benefits

- Competitive compensation, benefits and generous time-off policies
- 4-Day summer work weeks and a winter holiday break
- 401(k) / DCPP matching
- Annual bonus program
- Casual, dog-friendly, and innovative office spaces