Client Name

Cybersecurity/SOC Analyst

Detail-oriented professional with hands-on experience optimizing end-to-end cybersecurity operations through security risk assessment and incident response, as well as improving security posture and advancing IT asset protection by deploying cutting-edge security technologies within fast-paced environments.

Skilled in executing business continuity management/disaster recovery plans and distinguishing/interrupting vulnerabilities for eliminating aftermaths of cyber-attack incidents and maintaining equipment optimal functionality. Excel at administering multiple cybersecurity platforms and coordinating complex transformational projects/programs, while adhering to SOC requirements and quality standards/regulations. Instrumental in leading and mentoring technical teams in alignment with organizational SOPs and emerging IT industry trends to automate business processes and improve overall performance/productivity. Adept at collating, analyzing, and preserving digital evidence, monitoring network traffic for security events, and conducting triage analysis to identify security incidents. Proficient in designing/delivering SIEM solutions and devising threat intelligence procedures to ensure data protection and maintain high-level confidentiality.

AREAS OF EXPERTISE

Cybersecurity Environment Implementation | Incident Response Planning & Recovery | Cyber Security Management | Network Access | Performance Optimization | Cybersecurity Event Detection | Cost Planning & Control | Project/Program Management | Vulnerability Analysis | Network & Security Fundamentals | Firewall Configuration | Threat Detection & Intelligence

CAREER EXPERIENCE

Defendege, Chicago, IL — 2021 – Current

Security Operation Center Analyst Intern

Analyze and monitor logs/alerts from varied technologies, including IDS/IPS. Firewall, proxies, and anti-virus to mitigate potential threats. Discern patterns of complex threat actor behavior for articulating aftermaths of existing and emerging cyber threats. Identify and navigate online forums, specialized websites, social media, and traditional sources through effective utilization of online research tools. Attain functional deliverables by maintaining and reviewing insightful reports of security-related incidents. Oversee a broad range of cybersecurity cases with enterprise SIEM systems, such as ArcSight, Splunk, and Sourcefire. Ensure alignment of clients with security policies and procedures inclusive of NIST 800-53 and NIST 800-53A. Investigate and deliver uncategorized sites to Symantec for categorization and vulnerability scan detection. Install and configure links for VPN tools used by the agency comprising Cisco AnyConnect, Pulse Secure, and Network Connect.

- Prioritized and resolved over 500 tickets since joining by leveraging cybersecurity and IT expertise.
- Increased team efficiency by devising and organizing area processes.
- Enhanced threat detection capabilities by establishing and monitoring new investigation processes.

US NAVY, Norfolk, VA — 2017 – 2020

Engineman Second Class

Strategically positioned as lead engineer for a 50-member maintenance team and assigned with managing engineering/auxiliary equipment, as well as ensuring the completion of three Patrol Boats 95% mission. Steered multiple complex projects to execution in a highly motivated environment by enhancing work coordination with peers throughout the lifecycle ranging from planning, design, and delivery. Coached, motivated, and guided 12 junior subordinates towards enrolment into college and United Service Military Apprenticeship Program. Ascertained repairing needs by conducting testing procedures on marine engines and equipment. Led the major and specialized mechanical overhaul/repair work on gasoline marine engines, equipment, and systems by extensively using technical manuals and schematic charts.

- Pivoted the completion of 4,586 man-hours, covered 140 maintenance checks, and enabled three $17M Patrol Boats to remain mission capable during a 12-week training cycle.
- Saved $500M for the Navy by preventing major causality on boat jet systems with attention to detail.
- Increased maintenance check readiness from 31% to 96% through effective scheduling of weekly security watch-bill for 50 sailors.
- Won a Good Conduct and three Battle E medals for outperforming in supervisory duties.
- Accomplished MK VI Patrol Boat first refueling at sea in partnership with a diverse group of coworkers.
- Facilitated the planning, development, and execution of MK VI Patrol Boat's first well deck embarkation.

US NAVY, Sasebo 2015 – 2017
Engineman Third Class

Initiated a broad spectrum of preventive and corrective maintenance actions for equipment, computer systems, and pumps on the Patrol Boat. Trained 158 personnel on combat ship casualty procedures, increasing junior sailor's CPR knowledge, fire, and flooding prevention proficiency skills. Identified issues and optimal resolutions through the execution of 1K inspections and diagnostic procedures.

- Played a significant part in the Navy Ship USS Ashland program completion to 95%.
- Awarded with the Navy and Marine Corps Achievement Medal for implementing robust action plans for combat electrical fires that generated savings by over half a million dollars.
- Minimized downtime for the ship's crew by interpreting and swiftly repairing mechanical malfunctions independently and in partnership with crews.

VOLUNTEER EXPERIENCE

- Boosted patrons' morale by dedicating 500 hours to USO in Sasebo, Japan from 2015 to 2017.
- Cultivated positive relationships with Australian natives by devoting eight community hours towards landscaping and resurfacing of six acres for the Bunbury, Australia Wildlife Park and Zoo in 2015.
- Collaborated with Saipan locals, dedicated 8 hours toward beatification project for the Juan M. Guerrero Elementary School in Saipan in 2015.
- Established strong community ties between Thai and South Korea through a three-hour engagement in various sports activities with both countries in 2016.

EDUCATIONAL BACKGROUND

Bachelor of Science in Computer Network & Cyber Security | University of Maryland Global Campus, Adelphi, MD

CERTIFICATIONS

- Cisco Certified Network Associate Routing and Switching (CCNA). 2021
- Certified Ethical Hacker. 2020
- CompTIA Security +CE. 2020
- CompTIA Linux +Ce. 2020
- CompTIA Cyan +CE. 2020