Alan Schneider

Cyber Security Analyst with 21 years of experience designing, implementing, and troubleshooting network. infrastructure and security. Experience with Risk Management Framework in support of DOD Information Assurance.

WORK EXPERIENCE

United States Navy, Virginia Beach, Virginia

Cybersecurity Network Analyst 11/1998 – 09/2008

- Responsible of maintaining troubleshooting logs for client networks
- Utilized 10+ monitoring tools to identify and fix irregular CPU, disk, and memory utilization levels.
- Monitored daily operations of IT networks, ensuring maximum uptime and performance for all applications.
- Identified and resolved trouble tickets encompassing active directory account issues, CISCO routing and switching, firewall configuration and testing.
- Responsible for scanning and remediation for network vulnerabilities and installation of Security Technical Implementation Guides (STIGS) when required.
- Responsible for the planning and implementation of a thirty-six-week training pipeline encompassing nineteen advanced USSOCOM communications suites and network certification programs in support of NAVSOF.

United States Navy, Virginia Beach, Virginia

Information Systems Security Manager 09/2008 – 06/2019

- Subject matter expert responsible for Host based security and Network security systems Information Assurance program for over seven thousand military personnel encompassing six Navy commands.
- Ensures the implementation of the Risk Management Framework (RMF), through the required government policy, makes recommendations on process tailoring, participate in and document process activities.
- IT project lead directing the infrastructure design, acquisition, and phased delivery of a fully compliant network for a 2.5-million-dollar UAS Operator Training facility.
- Developed community wide Department of the Navy compliance procedures for personal electronic device utilization aboard military aircraft.
- DOD Public Key infrastructure program manager.
- Responsible for security systems analyzing potential threats using security tools such as SIEM, firewalls, vulnerability scanners, IDS/IPS, and anti-virus.
- Performed event log analysis and network traffic monitoring/analysis to differentiate between potential intrusion attempts and false alarms.
- Escalated cybersecurity events per standard operations procedures (SOPs).
- Managed information assurance training and implemented phishing campaigns to educate employees and reduce risk.
- Evaluated potential cybersecurity security risk and took appropriate corrective and recovery action utilizing various tasking mechanisms such as Remedy, eMASS, XACTA, ACAS, etc.
- Provided oversight and guidance of thirty cybersecurity personnel implementing applicable patching oversight and validation of all security related updates including Cyber Tasking Order compliance.

CONTACT

- Virginia Beach, Virginia
- 757-373-9575
- alschn3134@gmail.com

SKILLS

Hard Skills:

- Network Administration
- Penetration Testing
- Ethical Hacking
- Incident Response
- Cyber Defense
- Threat Assessment

Techniques:

- Network Access Control
- Threat & Vulnerability Management
- Systems Backups and Network Security
- Vulnerability Scanning and Remediation

Tools and Software:

- Microsoft Products
- C++
- Linux
- Python
- Nessus Scanner

Languages:

- English (Native)

EDUCATION

BS, Cybersecurity *Old Dominion University* **Anticipated December 2023**

AS, Applied Science *(Cyber)* *Tidewater Community College* **December 2022**

CERTIFICATIONS

- ISC² CISSP **Anticipated February 2023**