INFORMATION SECURITY ANALYST INFORMATION SECURITY ANALYST INFORMATION SECURITY ANALYST - CONSTELLIS Camden, NC Authorized to work in the US for any employer

Work Experience INFORMATION SECURITY ANALYST CONSTELLIS - Moyock, NC May 2018 to Present 40+ HOURS/WEEK 58,000/YR SECURITY ANALYSIS & OPERATIONS: Manage and analyze monitored data on a day-to-day basis for various security related events and activities via several information security systems and tools. Detect any unauthorized attempts to access the system. Review security logs, investigate issues, and report to IT management. Actively research emerging threats identified in data sources to help detect and correct those emerging threats from internal user activities.   LEADERSHIP: Support Cyber Security Awareness Initiatives based on defined requirements and defined engagement parameters. Coordinate and provide expert operational support to enterprise-wide cyber defense technicians. Provide technical expertise of current and evolving best practices in cybersecurity and the broader IT industry. Support the development of contingency plans to ensure availability and accessibility of network resources. Collaborate with the technical services team and cross-functional departments to remediate security risks.   INCIDENT RESPONSE: Provide first level security incident response for incidents alerted by monitoring systems. Maintain user security by developing access controls, monitoring and evaluation of security standards. Manage security patches on server devices and workstations. Conduct internal network penetration test to look for confirmation weaknesses, unsecure network files shares, and data leakage. Monitor the organization s computing environment (servers, firewalls, intrusion detection/prevention systems, anti-virus and malware) logs, and network traffic for activities including but not limited to policy violations, abnormal behaviors, intrusions, best practice recommendations, etc. Schedule regular cybersecurity reports (i.e., event logs, firewalls, cyber incidents). Remediate items found during vulnerability scanning both internal and external. Execute information security project and initiatives. Maintain a complete inventory of assets in the configuration management database.   RISK MANAGEMENT: Develop methods to monitor and measure risk, compliance, and assurance efforts. Implement and integrate risk management procedures. Participate in information security audits and oversee penetration testing of all networks

and systems to identify system and application vulnerabilities. Identify new vulnerabilities and threats. Create and maintain a cybersecurity risk assessment.   IT SECURITY: Serve as a cyber security protection analyst on penetrations and testing. Identify, investigate, analyze, and remedy information security events to ensure enterprise integrity against technical and physical risks. Conduct quality management reviews to evaluate the effectiveness of security controls. Report on the controls effectiveness for mitigating exposure to identify risks. Investigate cybersecurity violations to determine their effect on the integrity of information IT systems and infrastructures, such as unauthorized access, malware, or misuse. Troubleshoot and configure computer issues, anti-virus software, device encryption, and Internet browser issues.   IT OPERATIONS: Direct and coordinate the installation and configuration of server operating systems. Develop, test, certify, and implement disaster recovery and contingency plans. Provide support, implement, and manage desktop software patching and installation, including packet creation, using organization approved processes and tools. Review proposed new systems, networks, and software designs for potential security risks; recommend mitigation or countermeasures and resolve integration issues related to the implementation of new systems within the existing infrastructure.   DOCUMENTATION AND COMPLIANCE: Track and document cyber defense incidents from initial detection through final resolution. Write policies, guidelines, and standards that assure compliance with company policies and facilitate integration, implementation, assessment and authorization of IT security systems. Draft long-range plans for IT security systems and processes that anticipate, identify, evaluate, mitigate, and minimize risks associated with IT systems threats and vulnerabilities.   CUSTOMER SUPPORT / HELP DESK OPERATIONS: Manage the intake of incidents and reports from internal customers through internal ticketing system in a timely accurate manner in order to resolve a multitude of information security related situations. Assess, identify and escalate issues as appropriate. Accomplishments: =Current Special Projects: O365 Multifactor Authentication Company-wide Deployment. Served as the primary decision-maker on planning and executing O365 MFA to end-users. Trained HD personnel on setup of MFA for end-users. Created multiple SOPs to instruct end-users on independently setting up MFA. Created Technical SOPs for troubleshooting issues

with MFA. =Upcoming Projects: Participate as a team member on the implementation of a company wide Cybersecurity Awareness Training via Wombat Security Education Platform. IT SUPPORT SPECIALIST ACADEMI/CONSTELLIS - Moyock, NC June 2014 to May 2018 40+ HOURS/WEEK 52,000/YR   IT SUPPORT & DEVELOPMENT: Designed, configured, and tested computer hardware, networking software and operating system software. Reviewed and/or conducted audits of information technology (IT) programs and projects. Collaborated with network specialists, application developers, system administrators, and security specialists to prevent recurring problems. Assisted in the development, configuration, installation, and maintenance of network systems to include the LAN/WAN. Coached junior IT specialist in resolving highly complex IT problems and systems issues. Implemented security programs designed to anticipate and minimize system vulnerabilities. Coordinated with all Information Systems departments and teams to gather data, resolve issues or develop action plans. Performed root cause analysis.   SECURITY ASSESSMENT: Identified security risks, threats and vulnerabilities of networks, systems, applications and related components. Performed assessments in an enterprise environment including vulnerability exploitation and identifications consisting of webs application, mobile applications, databases, networked systems, and operating systems and attached devices. Performed cyber defense incident triage and made recommendations that enabled expeditious remediation. Assisted in the development of long-range plans for IT security systems that anticipate, identify, evaluate, mitigate, and minimize risks associated with IT systems vulnerabilities. SECURITY INCIDENT ANALYSIS: Managed security initiatives that facilitated the implementation of appropriate systems security policies. Assisted in the review and evaluation of cybersecurity policies, recommended changes, developed testing procedures and methodologies for cybersecurity policies, and prepared reports that evaluated cybersecurity awareness and compliance. Analyzed, advised and developed solutions to solve issues and problems associated with agency-wide IT programs and initiatives. Evaluated statistical data and market trends, and interpreted findings to determine meaning and develop recommendations. Recommended needs for equipment and software and oversaw acquisition process. Reviewed security incident response policies and

identified the need for changes based on new security technologies or threats.   POLICY COMPLIANCE: Implemented security requirements, integrated security programs and defined the scope and level of detail for security plans and policies.   IT & NETWORK OPERATIONS: Installed, administered, and supported server and workstation-based applications. Modified configurations, utilities, software default settings, etc. for workstations, servers and network equipment. Performed maintenance and troubleshooting of active directory and group policy. Diagnosed hardware/software problems and replaced defective components. Provided support, problem resolution and recovery of operating malfunctions involving hardware and software. Performed broad range of technical Local Area Network (LAN)/Wide Area Network (WAN) functions, to include Secret Internet Protocol Router Network and Non-Secret Internet Protocol Router Network. Installed computer terminals, printers, routers, bridges, repeaters, transceivers, network cards, cabling, networking software, E-mail, application packages, and internetworking functions. Managed WEB development, maintenance and Internet Protocol addressing support.   CLIENT SERVICES & COMMUNICATIONS: Gathered feedback on customer satisfaction and internal service performance to foster continual improvement. Communicated security issues and controlled gaps through security governance process. Drafted and reviewed information security policies, standards and procedures. PROBLEM RESOLUTION: Applied new developments to previously unsolvable problems; made decisions and recommendations that significantly influenced important IT policies or programs. Managed and monitored server and storage resources including performance, capacity, availability, serviceability, and recoverability. Isolated and defined unprecedented conditions; resolving critical problems; developed tests and implemented new technologies. Managed the movement and installation of IT equipment to assure coordination of IT support and customer service. Evaluated usage patterns and incorporate customer feedback into recommendations to the Lead or Supervisory IT Specialist for improving the functionality or performance of a given system. COMPUTER SOFTWARE APPLICATIONS: Proficient with Microsoft Office products (Word, Excel PowerPoint). Familiar with using SharePoint (ability to create/modify lists, document libraries, views, etc.)   ADMINISTRATIVE OPERATIONS: Coordinated project schedules, including participation in

meetings; documentation and distribution of minutes and action items; and tracing action items for their successful completion. Planned and executed special project assignments to include task definition, scheduling, resource allocation, progress monitoring and reporting. RECEPTIONIST ACADEMI - Moyock, NC June 2013 to June 2014 40+ HOURS/WEEK 29,500\YR   FRONT DESK OPERATIONS: Handled differing situations, problems, and deviations in the work according to the supervisor's general instructions, priorities, duties, policies, and program goals. Screened telephone calls, visitors, and incoming correspondence; responded to requests for information; determined which requests should be handled by the supervisor, appropriate staff member or other offices. Professionally interacted with customers, colleagues and members at all levels; fostered positive business relationships.   ADMINISTRATIVE SUPPORT: Provided classified and unclassified administrative support to include telephone, e-mail, video teleconference, correspondence, calendar management, visitor reception/escort and meeting planning, and execution support. Edited and proofread memos, emails, presentations and reports. Screened calls, managed calendars and coordinated meetings and events. Worked independently on projects requiring research and preparation of briefing charts and other presentation materials. Completed email follow up, meeting scheduling, preparing budgeting summaries, project schedules, and analysis of information for function.   COMMUNICATION & TEAMWORK: Maintained a close and highly responsive relationship to the day-to-day activities of the supervisor and staff. Demonstrated excellent oral and written communication skills. Learned job-related material primarily through oral instruction and observation or through on-the-job training. Possessed excellent typing abilities and the skill to prepare documents accurately with minimal errors.   STAFF SUPPORT: Performed various clerical and secretarial duties requiring knowledge of office routine and an understanding of the organization, programs, and procedures related to the work of the office, as well as knowledge of certain office software programs. Arranged conferences and meetings and assembled established background materials as directed. Scheduled tentative appointments. Attended meetings and recorded and reported on the proceedings as required. Collected information from the files or staff for routine inquiries on office program(s) or periodic reports and referred non-routine requests to

supervisor or staff. Supported tasks requiring the collecting, compiling, evaluating and publishing of information and statistical data included in documents, records, forms, reports, plans, policies and regulations.   SOFTWARE/HARDWARE USE: Proficient use of office software, such as Microsoft Word, Excel, Power Point, databases and e-mail and the operation of office automation equipment, including copy machines, facsimile machines, networked computers, laser printers, shredders, scanners, and other electronic equipment is necessary in the performance of this task.

ORGANIZATIONAL SKILLS: Possessed excellent organizational and file management skills and the ability to plan and execute administrative work with little or no supervision. Maintained sensitive files and documents and maintained a high level of confidentiality. Worked efficiently in a fast-paced environment and always maintained a calm and consistent demeanor. Demonstrated organizational and interpersonal skills. Meteorologist United States Navy September 2006 to September 2012 40+ HOURS/WEEK 48,000\YR   WEATHER ANALYSIS: Performed in-depth satellite imagery and weather model analysis to create and brief accurate weather forecasts. Chronicled inclement weather trends to analyze and establish regional weather patterns affecting operations. Assisted in guiding ships, aircraft and troops with recommendations based on weather forecasts and ocean conditions. Relayed forecast updates and weather warnings to military and civilian authorities. Prepared ocean, sea and waterway charts and maps for anything from basic navigation to search-and-rescue efforts. Maintained the military s primary master clock, which provided the most precise time interval in the world and drives the Global Positioning System (GPS).

METEOROLOGICAL TECHNICAL AND USER SUPPORT: Gathered and accurately interpreted meteorological information on multiple linear and digital platforms. Created detailed Oceanographic products for use when conducting submarine warfare operations. Maintained existing computer software and hardware. Managed an archive of meteorological data using computer storage systems. Ensured standardized meteorological support for the Navy and other government and international agencies. Utilized professional knowledge of meteorology, supported project teams in the development of new products and/or technical capabilities to support user requirements.

DOCUMENTATION & REPORTING: Generated storm-following short fused forecast reports

depicting information for significant weather events including severe weather and tropical systems. Maintained records and prepared reports and correspondence related to the work. Documented user satisfaction surveys and correspondence regarding quality and effectiveness of organization space weather products and services.   AIR QUALITY: Analyzed and evaluated climatological factors to develop short and long-range forecasts of air pollution. Examined meteorological and air pollution data and prepared pollution forecasts. Calculated air quality effects at different emission levels; used inventories of emission sources, meteorological and topographical data, and population. Maintained records of pollution levels and advised officials as to when to declare air pollution alerts.   EQUIPMENT OVERSIGHT: Operated, calibrated and maintained specialized scientific equipment in climatological observation stations. Assisted with meteorological and climatological problems.   Accomplishments: =Highly rated Junior Forecaster with a 98% accuracy rate. =Served proudly onboard the USS George Bush, USS Enterprise, USS Essex, USS Iwo Jima. Education MASTER'S OF CYBERSECURITY in UMUC NIST May 2017 Skills RECEPTIONIST (1 year), CISCO (Less than 1 year), CITRIX (Less than 1 year), CUSTOMER SERVICE (Less than 1 year), LINUX (Less than 1 year), Cyber Security, Nist, Information Security, Siem, Network Security Certifications/Licenses CompTIA Security+ December 2015 to December 2021 Additional Information TECHNICAL SKILLS Windows Linux Palo Alto Citrix Cisco Rapid 7 Dark Trace Wireshark Snort Bro VEEAM Replication Solarwinds Nmap Office   SKILLS   Familiarity with Information Technology infrastructure and integrations.   Ability to maintain a high level of confidentiality.   Attention to detail   Teamwork   Critical and Analytical Thinking   Customer Service   Incident Responder   Vulnerability Researcher   Threat Hunter

Name: Joe Green

Email: stephanie25@example.net

Phone: 001-237-203-1247x81783