Senior Cyber Security Engineer (Tier 3 SOC) Senior Cyber Security Engineer (Tier 3 SOC) Senior Cyber Security Engineer (Tier 3 SOC) Manassas, VA Please do not attempt to contact me if you are a staffing company. Authorized to work in the US for any employer Work Experience Senior Cyber Security Engineer (Tier 3 SOC) ECS Federal LLC - Fairfax, VA December 2018 to Present Performed configuration, tuning and operating of several Cybersecurity tools from vendor McAfee such as ePO, Endpoint Security (ENS), Application Control (AC), Change Control (CC), Whole Disk Encryption (WDE), McAfee TIE/DXL. and McAfee Cloud Workload Security Administered and configured operation of AWS and Microsoft Azure environments. Evaluates new methodologies to deliver cybersecurity capabilities. Deployed, configured and administer the McAfee Advanced Threat Defense product. Performed and supported investigations and contribute to large- and small-scale cyber breaches. Conducted product configuration, testing, evaluation and deployment of the McAfee Endpoint Security (McAfee ENS) and McAfee SolidCore module. Managed STIG compliance activities for various host products. Performed ENS Threat Prevention System l administration on multiple servers and endpoints. Performed ENS Firewall administration. Performed ENS Web Control administration. Deployed, configured and administer the McAfee ePolicy Orchestrator product for multiple clients. Participated in patching and deployment of administrative tools. Implemented policy configurations for all security apps. Performed Threat Event Analysis and mitigations on the network. Identified and deployed required security patches throughout the client's environment to multiple security or mission essential products. Performed Rogue Detection Systems analysis and mitigation on the network. McAfee SME Engineer (SOC) Meridian - Quantico, VA June 2018 to December 2018 Built, configured, tested and deployed the McAfee Enterprise Policy Orchestrator (McAfee ePO) environment for the site's laboratory. Conducted product configuration, testing, evaluation and deployment of the McAfee Endpoint Security (McAfee ENS) and McAfee SolidCore module. Built, configured, tested and deployed the McAfee Enterprise Security Manager (McAfee ESM) environment for the site's laboratory. Performed administration on the SIEM environment. Created and collaborated in providing a detailed Standard Operating Procedures (SOP) documents pertaining to the modules and environments I have been assigned to work on (McAfee ENS, McAfee SolidCore, and McAfee ESM) Managed STIG compliance activities for various host products. Performed Host Intrusion Prevention System (HIPS) Firewall administration on multiple servers and assets. Evaluated and modified host products including Virus Scan. Participated in patching and deployment of administrative tools. Implemented policy configurations for all security apps. Performed Threat Event Analysis and mitigations on the network. Remediated servers to bring into DoD security compliance Identified and deployed required security patches Performed Rogue Detection Systems analysis and mitigation on the network. Security Systems Engineer (SOC) Insight Global - Quantico, VA June 2017 to June 2018 Managed STIG compliance activities for various host products. Performed Host Intrusion Prevention System (HIPS) Firewall administration on multiple servers and assets. Evaluated and modified host products including Virus Scan. Participated in patching and deployment of administrative tools. Implemented policy configurations for all security apps. Administered regional servers and documented CRQs. Upgraded ePO versions and formulated change management procedures. Prepared, updated and maintained POAMs and other security compliance documentation Created and submitted change orders for critical systems Performed Threat Event Analysis and mitigations on the network. Remediated servers to bring into DoD security compliance Composed server security mitigation documents Identified and deployed required security patches Performed and managed Data Loss Prevention(DLP) administrative duties on both the UNCLASS and SIPR networks. Performed Rogue Detection Systems analysis and mitigation on the network. Provided detailed status updates on existing cyber security incidents daily to include follow up with client/customer to ensure satisfactory resolution Cyber Security Engineer (SOC) Netcentrics - Washington, DC March 2017 to June 2017 Conducted inspection of information systems and cyber security management. Participated in root cause analysis and risk identifications on the network. Evaluated security models and tested physical security controls. Recognize potential successful and unsuccessful intrusion attempts and compromises and report incidents for follow up investigations. Ability to independently understand, troubleshoot, and resolve security alarms. Monitor and analyze Intrusion Detection Systems (IDS) to identify security issues for remediation. Performed CND and information analysis functions utilizing HBSS and ACAS. Evaluated and modified host products including Virus Scan, HIPS, ACCM, SIR and DAT. Participated in patching and deployment of administrative tools. Implemented policy configurations for all security apps. Upgraded ePO versions and formulated change management procedures. Performed Threat Event Analysis and mitigations on the network. Managed security compliance on the UNCLASS and SIPR network by blocking non-compliant assets. Performed and managed Data Loss Prevention(DLP) administrative duties on both the UNCLASS and SIPR networks. Managed multiple Remote Intrusion Detection Systems(RIDS) assets deployed on the network. Performed Rogue Detection Systems analysis and mitigation on the network. Cyber Security Analyst Cyber Security Research and Solutions - Arlington, VA January 2017 to March 2017 Provided high level analysis on security data to identify significant activity. Developed coordinated, implemented and maintained standards and procedures to protect the security and integrity of information systems and data. Observed and analyzed traffic to learn valuable lessons from known malicious actors and to determine countermeasures against such threats. Provided detailed status updates on existing cyber security incidents daily to include follow up with client/customer to ensure satisfactory resolution. Conveyed verbal briefings to management on pending cyber incidents as well as coordinate with Army Cyber Command as necessary to convey incident information. Monitoring security patch levels of the servers, workstations and network environments, and anti-virus systems. Make recommendations to senior military officials on results of analysis and work closely with other Information Technology groups to refine and enhance security controls. HBSS Engineer (SOC) SMS Data Products Group, Inc - North Charleston, SC July 2016 to January 2017 Managed STIG compliance activities for various host products. Evaluated and modified host products including Virus Scan, HIPS, ACCM, SIR and DAT. Participated in patching and deployment of administrative tools. Implemented policy configurations for all security apps. Upgraded ePO versions and formulated change management procedures. Performed Threat Event Analysis and mitigations on the network. Managed security compliance on the UNCLASS and SIPR network by blocking non-compliant assets. Performed and managed Data Loss Prevention(DLP) administrative duties on both the UNCLASS and SIPR networks. Managed multiple Remote Intrusion Detection Systems(RIDS) assets deployed on the network. Performed Rogue Detection Systems analysis and mitigation on the network. Coordinated and perform HBSS training for new hires and other personnel on other projects. Performed troubleshooting with the purpose of helping the user bring up the asset compliant on the network. System Administrator KSH Solutions - North Charleston, SC June 2015 to June 2016 Performed troubleshooting, cyber security and asset re-imaging on all assets that belong on the RDT&E network. Also provided troubleshooting solutions for networking and Citrix issues to customers in person or by phone. Performed HBSS and Active Directory administration on the RDT&E network. While working under this contract, I have attended training, which gave me the opportunity to further my knowledge configuring, maintaining and troubleshooting Cisco routers, switches(QoS, OSPF, BGP, VLAN, SPANNING Tree, Fiber and Ethernet), incident response and firewall security policies Laborer/ IT Support Rug Masters - Charleston, SC January 2014 to June 2015 Performed cleaning, maintenance and repairs on a variety of Persian rugs. Executed computer troubleshooting, virus removal and analyze/resolve any network connectivity to ensure smooth operations on Cisco routers (layer 2/3 switch configuration, security (ACL), maintenance, and troubleshooting. Responsible for VM Server implementation for virtual clients. (VDI) Interact with customers that do not use English as a first language and assist clients on their every need. Infantry Team Leader United States Marine Corps - Camp Lejeune, NC July 2007 to July 2012 Oversaw the welfare, training and deployment of an infantry fire team; supervised and managed six Marines for infantry combat operations on a team level in order to accomplish combat missions. Responsible for deployment, training, troubleshooting and maintenance of Electronic Warfare equipment (THOR, WOLFHOUND) in combat operations. Carried out encryption and troubleshooting on military radio equipment. Education B.S. in Cloud Computing and Virtualization ECPI University - North Charleston, SC November 2016 B.S. in Network and Cyber Security ECPI University - North Charleston, SC August 2016 A.S in Network Security ECPI University - North Charleston, SC August 2015 Skills McAfee ePolicy Orchestrator Engineering (3 years), McAfee

Network Security Manager (NSM) administration (1 year), McAfee Enterprise Security Manager (ESM) Engineer (1 year), Host Intrution Prevention Systems (3 years), Rogue Detection Sensors (3 years), Virus Scan Enterprise (3 years), Data Loss Prevention (3 years), HIPS Firewalls (3 years), Microsoft 2008 Server Administration (3 years), Microsoft 2012 Server Administration (3 years), Cisco Routers (2 years), Cisco Switch (2 years) Links https://www.linkedin.com/in/armando-valentine-653a5211b/ Military Service Branch: United States Marine Corps Rank: Lance Corporal Certifications/Licenses CompTIA Advanced Security Practitioner (CASP) Certified Ethical Hacker (CEH) CompTIA Secure Cloud Professional (CSCP) CompTIA Cloud Admin Professional (CCAP) CompTIA Security+ce CompTIA Network+ce CompTIA Cloud+ce DISA HBSS Admin ePO5.3 DISA HBSS 301 Advanced ePO5.1 DISA HBSS 501 Analyst ePO5.1 DISA ACAS Version 5.3 McAfee Certified Product Specialist: ePolicy Orchestrator (ePO) McAfee Certified Product Specialist: Advanced Threat Defense (ATD) McAfee Certified Product Specialist: Endpoint Security (ENS) A valid IT Specialist certification Additional Information Training: McAfee Enterprise Security Manager (ESM) Engineer 1 McAfee Enterprise Security Manager (ESM) Engineer 2 McAfee ENS Endpoint Security 10.5.3 Training McAfee Network Security Platform 9.2 1806 Training MCCOG NSM Signature Development Training MCCOG NSM Network Sensor Support Training

Name: Robin Howe

Email: uross@example.org

Phone: +1-469-879-2323x736