Lead Information Security Engineer Lead Information Security Engineer Lead Information Security Engineer Union, KY Experienced Computer Systems Analyst with diverse industry experience in the Department of Defense. Professional expertise includes Risk Assessment and Analysis, Cyber Security, Network Exploitation, Vulnerability Management, and Network Counter-measures Development. Work Experience Lead Information Security Engineer Fifth Third Bank - Cincinnati, OH July 2018 to Present Functioned as one of the lead engineers for Fifth Third Bank's Information Security Team. Supported several applications with diverse operating systems, and supported projects for acquiring new technologies. Administered several critical Windows and Linux systems by performing regular maintenance and vulnerability patching Lead three projects that included a hardware refresh for Security Analytics, and on boarding two technologies known as Falcon Sandbox (Cloud) and Attivo Worked closely with vendors such as Symantec and IBM to identify troubleshoot configuration and architectural errors in the environment Authored several engineering procedures documents to assist in cross training for junior engineers and to assist with Business Continuity efforts Constructed a Disaster Recovery Environment for IBM Site Protector and authored the procedures for fail-over. Senior Principal - Cyber Security Subject Matter Expert ManTech International Corporation - Quantico, VA November 2017 to July 2018 Functioned as a cyber security system analyst and engineer for U.S. Marine Corp in the continental United States. Maintained cyber security systems by performing regular vulnerability scans with ACAS, and then patched and upgraded these systems to maintain Department of Defense (DOD) compliancy. Served as the Splunk system administrator. Maintained the back end servers as well as the application. Developed and deployed a Splunk deployment server configuration for the network to automate configuration and version updates across the network. Monitored and analyzed network traffic for internal and external threats as a member of an incident response team using Websense, Splunk, and Host Intrusion Prevention Systems (HIPS). Authored detailed reports on incidents and events that were discovered, and provided guidance and supervision for mitigation efforts to address them. Prepared technical architecture proposals for enhancements and integration of existing third party software systems. Designed, documented and executed maintenance procedures, including system upgrades, patch management and system backups. Facilitated the change management process for two divisions within the organization by documenting requirements, implementation plans, and risk assessments for new technologies. Assessed current and new systems for vulnerabilities by conducting SCAP and ACAS scans. Associate - Senior Computer Network Defense Analyst Booz Allen Hamilton - Arlington, VA April 2017 to November 2017 Functioned as a cyber security administrator for the networks used in the Pentagon. Performed daily maintenance, troubleshooting, and operational checks to ensure optimal performance. Created and deployed host intrusion prevention system (HIPS) signatures that detected current and emerging threats against the network. Detected and responded to identified network incidents. Prepared trending analysis and statistical reports on network activity using multiple proprietary and industry accredited network monitoring devices. Utilized comprehensive knowledge of network protocols, computer operating systems, vulnerabilities, and intrusion methods to initiate Computer Network Defense activities. Proposed plans to senior management for implementing new technologies and processes that would improve organizational capability for intrusion detection and prevention. Counter Measure Developer and Computer Network Defense Analyst/Incident Handler Administrator United States Navy - Virginia Beach, VA June 2011 to June 2017 for a defense sensor grid for U.S. Navy networks in the continental United States. Performed daily maintenance, troubleshooting, and operational checks to ensure optimal performance. Worked in a team environment and developed/conducted Computer Network Exploitation (CNE) operations to determine the effect of various Open Source Software (OSS) and server functions on traffic patterns and network performance in a WAN and wireless environment. Created comprehensive exploitation strategies that identified technical and operational vulnerabilities.Analyzed multiple networks and identified/assessed vulnerabilities in order to conduct CNE operations. Utilized various Enterprise-specific and commercially available tools to conduct CNE target development. Ensured validity of all SNORT rules prior to deployment and developed/deployed SNORT signatures used to detect emerging threats against U.S. Navy networks. Created and deployed HBSS signatures that detected current and emerging threats against the networks. Coordinated response and remediation of HBSS alerts with designated Points of Contact (POCs) across the enterprise. Detected and responded to identified network incidents. Prepared trending analysis and statistical reports on network activity using multiple proprietary and industry accredited network monitoring devices. Utilized comprehensive knowledge of network protocols, computer operating systems, vulnerabilities, and intrusion methods to initiate Computer Network Defense activities in response to 100,000 network events. Identified adversary's Tactics, Techniques, and Procedures (TTPs) and advised senior management on technical mitigation strategies for preventing, controlling, and isolating incidents. Coordinated with the local site Information Assurance Managers (IAM) on incident discovery, isolation, and remediation. Developed comprehensive expertise in Netflow and PCAP analysis and skills in various network and hosted devices for use in forensic network investigations and compromises that include Windows IIS, ISA, and Firewalls. Education Bachelor of Science in Computer and Information Science ECPI University - Virginia Beach, VA 2017 Associate of Science in Computer and Information Science ECPI University - Virginia Beach, VA 2016 Skills INTRUSION (7 years), SNORT (6 years), SPLUNK (Less than 1 year), IDS (Less than 1 year), IPS (Less than 1 year) Military Service Branch: United States Navy Rank: E5 Certifications/Licenses CISSP June 2018 to Present CCNA August 2015 to August 2018 Additional Information Strong analytical skills Certified Information Systems Security Proficiency in TCP/IP protocols Professional (CISSP)(2018) Information security CISCO Certified Network Associate (CCNA) Network penetration testing (2015-2018) UNIX/LINUX EC-Council Certified Ethical Hacker Excellent problem solving skills (CEH)(2015-2018) Windows (7,8, and 10) CompTIA Security +(2014-2017) Windows servers (2008 and 2012) Joint Cyber Analysis Course (JCAC) Python TS/SCI Clearance (CI/FS) Technical Writing Risk Assessment Risk Management Technical Skills Skills Experience Total Years Last Used Wireshark (Reading PCAP/ Hex Journeyman 6 Years Current Headers) Network Administration Journeyman 3 Years Current Penetration Testing Apprentice 2 Years 2017 Python Apprentice 2 Years 2017 McAfee Host Intrusion Prevention Journeyman 3 Years Current System Splunk Journeyman 3 Years Current Snort Journeyman 3 Years 2017 McAfee, BRO, Sentinel, and Squil Journeyman 5 Years Current (IDS/IPS) ACAS Apprentice 1 Year Current

SCAP/ STIGS Apprentice 1 Year Current

Name: William Perez

Email: patrickrachel@example.net

Phone: +1-618-595-5981