DISA JSP V&V Analyst/Blue Team Security Auditor DISA JSP V&V Analyst/Blue Team Security Auditor DISA JSP V&V Analyst/Blue Team Security Auditor | Certified Splunk Architect Alexandria, VA Highly motivated cyber security professional with an active Secret clearance, in-depth technical knowledge, and experience with tools and methodologies for conducting Blue Team and IV&V activities for systems supporting DISA and the DoD. Authorized to work in the US for any employer Work Experience DISA JSP V&V Analyst/Blue Team Security Auditor Booz Allen Hamilton, Arlington - Arlington, VA June 2018 to Present Perform assessments of multiple Pentagon and tenant networks using various vulnerability and compliance testing tools such as Tenable Nessus/ACAS, SCAP Compliance Checker, STIG Viewer, Nipper Studio, and Rapid7 Nexpose Created PowerShell script and Excel macros to automate the analysis and scoring of assessment data, including IAVM and STIG findings, saving an estimated 500 man hours/year for the team, while increasing efficiency and thoroughness of our assessments Utilized Splunk to mimic and expand upon the automation of my PowerShell script to perform analysis of both IAVM and STIG data as they are pulled into Splunk, removing all manual assessment analysis requirements for my team Refined data ingested into Splunk via regex to allow for more granularity to fit reporting and automation requirements Created Splunk Dashboards that present assessment information at a high level for leadership, with the ability to drilldown for more granularity pertinent to system administrators Utilize Nmap to perform enumeration of devices within IP ranges to validate mission scope Manually assess Linux, Windows, network devices, and databases for DISA STIG compliance to eliminate false positives / negatives and resolve checks left undetermined by automated tools Performed Independent Verification and Validation (IV&V) vulnerability assessments in support of system reaccreditation activities Create numerous Best Practice and DISA STIG Compliance reports for Cisco and Juniper network devices using Nipper Studio Document findings in concise reports for the customer; reviewing vulnerabilities scored with CVSS and recommended remediation methodologies Track and share mission progress and key information between team members through Microsoft SharePoint, Remedy, and in-house mission trackers Created and improved upon Blue Team/V&V SOPs and reporting template in order to

train team members in tool usage and provide better transparency to the customer See Present Job Superlative Technologies - Arlington, VA May 2017 to June 2018 See Present Job CACI NSS - Alexandria, VA February 2016 to May 2017 See Present Job L-3 Communications - Alexandria, VA March 2015 to February 2016 See Present Job CGI Federal - Alexandria, VA May 2014 to March 2015 IT Support Specialist Tait Towers - Lititz, PA May 2009 to August 2012 Assisted system administrator with Windows administration, working within active directory and group policy to manage users and groups Configured and maintained Cisco wireless access points through web interface and CLI Created Windows images consisting of required programs and security controls Installed and configured new user workstations using various preconfigured images Performed troubleshooting and maintenance for defective computers and devices Provided assistance to non-IT personnel by utilizing a help desk ticketing system Education B.Sc. in Information Technology Pennsylvania College of Technology - Williamsport, PA August 2009 to May 2013 Certifications/Licenses Splunk Enterprise Certified Architect August 2019 to August 2022 CEH Security+

Name: Craig Foster

Email: timothypena@example.net

Phone: 001-686-734-1330x89867