

Cyber Security Engineer Cyber Security Engineer Cyber Security Engineer - PENN STATE MILTON S. HERSHEY MEDICAL CENTER Mechanicsburg, PA Eight years of experience in Information Technology, with five years of specialization within Cyber Security. Skilled in Incident Response, Network Forensics, Malware Analysis, Vulnerability Management, and Cyber Security Systems Integration. Strong, professional communication Actively seeking leadership skills opportunities

Effective communication to all Able to meet and exceed knowledge levels expectations and deadlines Innate problem solving skills Solid team player with a penchant Passion for education for accomplishing goals as a unit Authorized to work in the US for any employer Work Experience Cyber Security Engineer PENN STATE MILTON S. HERSHEY MEDICAL CENTER September 2014 to Present Responsible for configuring, maintaining, and troubleshooting a wide variety of Cyber Security infrastructure for a diverse 14,000+ user environment (Hospital and College) Working hand in hand with other teams to secure our environment, while making changes to the end-user environment and business seamless Participating in a wide range of enterprise -wide, cross-team projects Systems include (\* indicates primary responsibility):

Symantec Anti-Virus \* Identity Finder DLP \* Dell Data Protection \* Resilient Incident Management \* WinMagic SecureDoc \* Cisco Web Security Appliance FireEye CM, AX, EX, NX, PX, HX \* Palo Alto Firewall Exterro eDiscovery \* Symantec DLP Splunk Rapid7 Nexpose/UserInsight Cisco StealthWatch \* Incident Response Performing in-depth incident response and forensic analysis of security incidents Responding and triaging alerts generated by various internal sensors (FireEye, Splunk ES, Palo Alto, Symantec, etc) and 3rd parties Shaping the Incident Response capabilities at Penn State Hershey by establishing our incident response framework and playbooks Proactive hunting on internal network utilizing a wide -array of tools and techniques to find anomalies, and abusive/malicious behavior Utilizing Incident Response tools such as: Redline, Google Rapid Response (GRR), FireEye tools suite, Splunk Enterprise Security, and others Conducting network forensics and analysis on packet capture and netflow data Performing malware analysis using a variety of both manual and automated tools 1726 English Dr. Mechanicsburg, PA 17055 jgale@alumni.harrisburgu.edu IT Security Analyst CAPITAL

BLUECROSS September 2008 to September 2014 Project lead on a variety of projects including CyberArk Password Vault and Sophos products Architecting user internet filter rules and policies on Sophos Web Appliance platform and Websense Monitoring and responding to security alerts based on log monitoring and alerting Conducting network and host based analysis and forensics Conducting internal penetration tests on the network, individual systems, and web applications, to insure strength and integrity of defenses Responsible for giving company-wide security awareness training and presentations bi-annually Helping to build a sustainable vulnerability management program Administering and implementing a wide variety of IT security applications Systems include (\* indicates primary responsibility): Sophos Anti-Virus \* CyberArk Password Vault \* Sophos Web Security \* Lumension Endpoint Protection Sophos Safeguard Encryption \* Arcsight SIEM Websense Web Filtering PGP RSA SecureID (Two-factor Axway MailGate authentication) \* Desktop Computing Specialist (Level 3) Troubleshooting various network, software, and hardware problems Building/Configuring desktop, laptop, and thin client computers Administering Group Policies and Active Directory for Windows Transitioning software/hardware/users from Windows XP to Windows 7 Installing/Configuring/Implementing/Supporting video conferencing equipment Education Bachelors of Computer Information Sciences in Computer Information Sciences Harrisburg University Computer Information Sciences Cumberland Perry Area Vocational Technical School Certifications/Licenses CompTIA Security+ November 2012 to November 2015 GIAC Certified Incident Handler (GCIH) August 2017 to August 2021 GIAC Certified Intrusion Analyst January 2017 to January 2021

Name: Frank Garcia

Email: steve03@example.com

Phone: 241.426.6977