IT Security Engineer IT Security Engineer IT Security Engineer - Radford University Salem, VA Dynamic, Motivated and Energetic Information Security Engineer professional with several years of progressive experience in installation, configuration of systems and applications identifying and troubleshooting system as well as network issues, possess a proven track record of providing specialist technical and user support in the IT industry. Extensive experience in researching, Installation & Configuration, System Administration, Technical Support, Business & IT Planning, Customer Service & Presentation and Strategic Planning. Good team player with the ability to organize and present complex solutions clea540 765 8253 ray.swingle@gmail.com 2232 Irish Cir. Salem, VA 24153 TIMOTHY "RAY" SWINGLE, JR rly and accurately. Seeking Information Security Engineer position in this prestigious organization, where i can utilize my IT skills and offer opportunities for personal and professional growth. Work Experience IT Security Engineer Radford University - Radford, VA 2012 to Present Responsible for conducting regular security scans and vulnerability scans to test computer hardware, software, and networked devices of all types. Develop summary reports from scans and provide to system owners. Conduct follow-ups to ensure that identified issues have been fully remediated. Conduct penetration tests of new and installed systems, working with system owners and custodians to remediate issues that are discovered during these tests. Document test results and ensure that these are archived and available for audit if necessary. Regularly perform penetration tests against University assets both on and off-site in an effort to confirm all border and internal protections are effective and no data is unintentionally exposed. Installed, configured, and maintained campus Data Loss Prevention software (Spirion's IdentityFinder). Designed, developed, and engineered campus security monitoring solution utilizing Gigamon network taps and collector, open source Intrusion Detection Software (Bro, Snort, and Suricata). Implemented a dedicated, multi-server Splunk environment to run the Enterprise Security Add-on as rudimentary SIEM solution. Event triggers in Splunk were then analyzed via dedicated Security logging server for all IDS and Bro events, correlated with custom scripts. Played an integral role designing, developing, and implementing a border firewall solution. Conducted all vendor research and tested all potential solutions provided by the vendors and

delivered reports to management with recommendations. Designed, developed and implemented and Intrusion Detection system utilizing open source tools for alerting and log management as well as network taps and vendor-supplied collectors. Carefully monitored reports from logging and intrusion detection systems for security related events. Coordinated resolution of identified issues with university stakeholders also collaborated with the Information Security Officer (ISO) to build and maintain new security tools as necessary for responding to potential threats. Implement and maintain the appropriate balance of protective, detective and corrective controls for agency IT systems commensurate with data sensitivity, risk and systems criticality. Configured tenable.io deployment to utilize SSO and role-based access to the system to aid in vulnerability mitigation tasks Provided assistance for the ISO with Incident Response, which may include network forensics, host forensics, incident documentation, coordination with systems personnel, cooperation with Law Enforcement and communication to outside legal counsel. Ensure the integrity of evidence, and follow proper procedures so that investigations are brought to satisfactory conclusions and according to Radford policy. Assisted the central help desk with the resolution of security incidents also responsible for troubleshooting technical and complex problems and resolve issues to completion. Performed migration of vulnerability scanning solutions to tenable.io from Rapid7.. This included migrating all previous scans and policies as well as configuring the instance to allow systems administrators access to their assets in the system. Work with system owners and administrators to remediate found issues. Perform vulnerability scans against all new servers at each phase of the deployment cycle to ensure no known vulnerabilities. Works with other members of IT and some end users to evaluate and provide secure configuration recommendations when needed. Works with the ISO to manage and maintain University annual security awareness training. Work with the ISO to maintain and edit University policy and standards to move towards NIST 800-53 compliance. Work with Internal Audit to gather data needed for audits and investigations. Configured and maintained internal Intrusion Detection systems and ensure all logs report to centralized log server. Diligently worked with the ISO to detect and swiftly respond to any incident that may occur using proper incident response techniques and protocols. Performed

diagnostics and troubleshooting of system issues, documented help desk tickets/resolutions, and maintained equipment inventory lists. IT Security Analyst Jefferson Lab - Newport News, VA 2009 to 2012 Provided adequate computer help desk support and technical training on hardware/software to end users. Documented help desk tickets/resolutions, and provided overall assistance in daily administration. Efficiently performed set-up, break-down, and transport of agency equipment on an as-needed basis. Adequately monitored active Snort IDS alerts and escalated issues to senior staff as needed per Lab policy and procedure. Monitored daily logs looking for indicators of compromise and other artifacts that may point to an incident. Diligently worked with other team members to respond to incidents and escalate as needed. Oversaw to Lab's vulnerability management program, monitoring a constant Nessus scanning process and removing false-positives from search results. Effectively oversaw vulnerability remediation process of issues found by Nessus scanner to reduce the number of false-positive vulnerability results, automated the Metasploit framework to run all known safe exploits against machines identified as vulnerable. Used Nessus scanner daily to detect and prioritize vulnerabilities in Lab assets. Used Nexpose scanner daily to detect and prioritize vulnerabilities in Lab assets. Successfully performed internal phishing exercises and trained end users as needed based on exercise results. Education MS in Cyber Security Operations ECPI University 2018 BS in MIS ECPI University - Richmond, VA 2006 Skills firewall (7 years), Ids (10+ years), Information security (7 years), Security (10+ years), Splunk (7 years), It Security, Siem, Cissp, Network Security, PCI, Cyber Security, Nessus, Palo Alto Certifications/Licenses GIAC GPEN, #10186 CSA CCSK, #090039038991 CISSP #724593 Additional Information Core Competencies Information Security System Administration Scripting and Automation Strategic Planning Installation & Configuration Security Systems Engineering and Design Cyber Intelligence Troubleshooting Firewall/IPS Configuration and Management Incident Resonse Vulnerability Management Log Analysis Tools Technical Skills Windows XP-10, OSX/Mac OS, Ruby, Splunk Linux, Perl, VMware, Firewalls, Bro, Suricata Bash, Python, ELK Stack, IDS/IPS Vulnerability Management and Penetration Testing: Nessus, Nexpose, Metasploit Professional Skills Excellent analytical, diagnostic and problem-solving skills.

Self-motivated, proactive, and has the ability to thrive in a fast-paced, mission-critical operations environment. Strong understanding of Information Security. Excellent team player with strong organizational skills. Strong ability to work under pressure, prioritize schedules and manage workloads. Strong work ethic and irreproachable integrity. Planning, installation, configuration and optimization of IT infrastructure to achieve high availability and performance. Strong analytical, troubleshooting and customer service skills. Ability to communicate efficiently with excellent management and organizational skills

Name: Tina Dunn

Email: matthew95@example.com

Phone: 943-446-8555x145