Cyber Security Analyst Cyber Security Analyst Cyber Security and Information Technology Professional Washington, DC Work Experience Cyber Security Analyst AMTRAK - Washington, DC 2018 to Present Responsible for handling the intelligence and email operations for the SOC while maintaining proficiency of adversary tactics, techniques, and procedures (TTPs) through analysis of email headers, malware analysis, and open source intelligence. Monitors, analyzes security alerts information from all approved security devices, collection techniques and designated system logs. Coordinates and synchronizes cyber security operations and investigations involving the Office of Inspector General. Provides security support and evaluation for the security tool development team in order to integrate information assurance/ security throughout the System Life Cycle Development of major and minor application releases. Conducts advanced level forensic analysis to determine the legitimacy of files, domains, and emails using tools such as Microsoft O365 Suite as well as online resources such as Virus Total, Hybrid Analysis, Scout Vision, and CrowdStrike EDR. Led the development of security awareness and compliance training programs and provides communication training as needed. Built malware analysis lab infrastructure using Windows and Linux operating systems and open software tools. Developed Standards of Operations documentation for overall security tools and implemented procedural playbooks for the team. Identified opportunities for organizational improvements to senior management on pending cyber incidents as well as coordinate with US-CERT and CVE resources as necessary. Interfaces with senior management and business users to strategize and document Infosec requirements, baseline cyber security operations, system infrastructure data and other technologies. Implements incident response procedures that utilized available resources to increase oversight capabilities within the Infosec domain. Develops intelligence reports through analysis of alerts and briefings from various sources and documents indicators of compromise (IOCs)/ indicators of attack (IOAs). Processes alert and tipper data from external sources of threat intelligence to create rules for detection of emerging adversaries and zero-days. Deploys software upgrades within the Amtrak enterprise and ensures efficiency and effectiveness by continuously monitoring. Cyber Security Analyst II-Shift Lead DIGITAL CONSULTING LLC 2017 to 2018 Aided JSP Pentagon in the testing of JRSS

security stack through traffic monitoring and generating device status reports. Provided technical analysis and briefings to senior leadership on emerging vulnerabilities and network defense actions for JSP Pentagon customers. Managed the daily shift operations and oversaw task ordersof the team to ensure the JSP CIRT mission standards were met.Mentored new associates on process and procedure, manage group mailbox, and open tickets for new incidents. Operated various network tools (ArcSight, TippingPoint, Fidelis, etc.) to monitor network for malicious activity. Hands-on experience with Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP). Researched adversarial tactics, techniques, and procedures (TTPs) while utilizing the knowledge gained from research to data mine NetFlow and packet capture repositories in order to identify current threats. Maintained and implemented Attack Sensing & Warning (AS&W) policies of JSP tenants and customers throughout the National Capital Region. Developed security newsletters, and awareness emails for the entire Infosec team. Collaborated with multiple teams to provide information and support for JSP Pentagon infrastructure incidents. Performed infrastructure tuning to intrusion detection and health monitoring event management platforms to ensure optimum analysis. Monitored JSP sensor grid with concentration in Intrusion Detection Systems (IDS). Analyzed rogue connectivity utilizing Wireless IDS (WIDS). Implemented configurations for web content filtering, enterprise proxies and firewalls. Utilized Niksun and WireShark for full packet capture analysis. Reviewed and resolved open remedy tickets assigned to the ADP team. Facilitated the JSP ADP Program IAW applicable CNDSP Evaluation Scoring Metrics, DOD and CJCSM regulations along with CND SOPs and government directives. Developed, coordinated, and implemented DoD standards and procedures to protect the security and integrity of information systems and data. Applied vendor and customized signatures to IDS and IPS devices and implemented by identifying new and pre-existing malicious network traffic. Sr. Information Security Analyst Rollout Systems, LLC - Paxtuxent River, MD, US 2016 to 2017 Developed and institutionalized, strategic process to ensure accurate assessment of security baseline remains current to DOD compliancy standards. Formulated resolutions for highly visible system vulnerabilities identified during certification inspections. Guided

senior leadership as the SME in ensuring DISA security baseline fulfilled the Risk Management Framework criteria. Validated information system boundaries in support of the C&A process; created system architecture diagrams; worked with information system managers to verify operating environment, system interconnections, and system level boundary protections. Managed DoD client s security assessments within compliance with DoD IA C&A Process (DIACAP). Executed network analysis/scans to identify vulnerabilities using tools such as (ACAS, Vulnerator, SCAP, Nessus etc.) Conducted technical reviews of DISA STIGS, DIACAP Packages and IAVA s. Responsible for ensuring unit compliance with STIG regulations. Conducted internal audits for preparation for over 300 security systems using SCAP Compliance Checker. Trained system owners on remediation procedures and necessary steps needed to meet unit compliance. Developed and implemented mitigation strategies for vulnerability scans. Updated systems with latest rule sets. Prepared RMF / DIACAP C&A Security Plans. Responsible for preparing Validation Reports, System Security Plans, Contingency Plans, Privacy Impact Assessments and POA&Ms. IT Specialist FREEDOM STAFFING LLC, PATUXENT - RIVER, MD, US 2015 to 2016 Coordinated installation, configuration and administration of hardware and software for 1000+ NMCI NAVAIR field base-ops end-users. Responsible for identifying operating system failures and resolving tickets per specific SLA requirements. Re-imaged over 200 Dell and HP laptops/desktops while spearheading newer OS upgrades on noncompliant devices through Microsoft SCCM. Administered and managed NMCI end-user account information, activations and e-mail configurations. Liaised with senior military leadership and cross-functional departments to plan and coordinate major system updates and enhancement initiatives. Coordinated with customers to resolve issues, implement patches and create / unlock / decommission user and administrative accounts. Researched and resolved issues utilizing SM9 ticketing system. Provided up to ten on-site NMCI field-technician maintenance visits on a daily basis, troubleshooting various technical problems and performing operating system administration with Windows-based computer systems. Cyber Security Engineer ICF INTERNATIONAL - Atlanta, GA 2015 to 2015 Analyzed and evaluated system information and event activity. Generated weekly system reports and updates to the

government customer (DCMA). Collaborated with the teams for configuration and implementation of the FireEye log integration. Researched & developed tool set recommendations for Log Rhythm SIEM. Created the Log Rhythm SIEM SOPs for DCMA CNDSP users. Coordinated plans and executed deliverables for DCMA s log aggregation management project. Jr. Systems Operations Administrator EXELIS - Norfolk, VA 2012 to 2014 Managed Active Directory forests and tree organizational units, user accounts, passwords, mailboxes, and file level permissions. Extensively administered and monitored the CNIC network for any possible operational crises. Resolved over 1500 User related trouble tickets and generated monthly reports to senior leadership. Analyzed escalations from end-users throughout the CNIC enterprise. Monitored and analyzed IAVA/CVE s of known vulnerabilities; coordinated remediation with system owners. Supported the Information Assurance team with asset deployments and maintenance. Engaged with stakeholders on future projects for CNIC data center enhancements. Managed CNIC system network architecture, installation, project implementation and risk remediations on for various government clients. Conducted weekly vulnerability assessments and collaborated with clients to provide recommendations regarding critical infrastructure and network security operations enhancements. Education Bachelors ECPI University - Virginia Beach, VA 2011 Skills SECURITY, WEB SECURITY, WEBSENSE, NESSUS, NMAP Links https://www.linkedin.com/in/cedrik-matthews Additional Information Comprehensive cross-functional expertise in: Vulnerability Management Network & Mobile Security Risk Management Intrusion Detection Malware Analysis Incident Management Reverse Engineering Threat & Intelligence Analysis Interoperability & Portability Infrastructure & Virtualization IT Governance & Enterprise Risk Management Datacenter Security SIEM Tools Project Management Data Security & Information Lifecycle Management Cloud Forensics & E-Discovery Change Control & Configuration Identity & Access Management Encryption & Key Management Technical Proficiencies: Tipping Point, Fidelis, FireEye, Sourcefire, Stealthwatch (Lancope, InQuest, Websense, Bro, NikSun, ArcSight SIEM, AirTight, Nessus, Acunetix Web Security Scanner, Nmap/Zenmap, Snort, What's Up Gold Network Monitoring, SolarWinds Network Monitoring, Horizon Open NMS, Wireshark, SCCM, VMware

VSphere 5.5, Log Rhythm SIEM, Core Impact, Retina, Citrix, Symantec Netbackup Administration, File Server Management, Cisco Routers/ Switches, WSUS, 3PAR, IAV Compliance, Remedy, RDC, IBM Tivoli, NetSkope, CrowdStrike EDR, Alert Logic, Akamai WAF, Scout Prime, Scout Vision

Name: Paula Martinez

Email: brandipowell@example.net

Phone: 001-809-372-5718x504