Tier II (SOC) Cyber Security Incident Responder Tier II (SOC) Cyber Security Incident Responder Cyber Security specialist | Veteran | Cleared | CISSP | CEH | CHFI | ECIH | SEC+ | NET+ | ITIL Greenville, NC Reliable veteran and dedicated Cyber Security specialist seeking opportunity with a reputable company that appreciates strong instincts and sound communication skills. Looking to on-board with an organization that possesses room for growth and opportunity. Authorized to work in the US for any employer Work Experience Tier II (SOC) Cyber Security Incident Responder NLogic - Fort Lee, VA July 2019 to Present Coordinated the response activities for cyber security incidents across the DECA Enterprise. Reviewed, triage, analyzed, and re-mediated cyber security incidents. Handled validated cyber security incidents, in accordance with the cyber security incident response process. Performed functions such as log analysis, conducted in-depth technical analysis of network traffic and endpoint systems, enriched data using multiple sources, was responsible for rapid handling and mitigation of cyber security incidents. Mentored and advise others, and drove the operational and strategic growth of DECA. Acted as Incident Commander for high impact cyber breaches and advanced attacks in accordance with Cyber Kill Chain methodology and incident response process.Participated in analysis, containment, and eradication of cyber security events and incidents. Conducted malware analysis and identification of Indicators of Compromise (IOCs) to evaluate incident scope and associated impact. Utilized analytic experience to address cyber-attacks and mitigate indicators and correlations to identify attribution and potential threat and impact to Verizon. Enhanced workflow and processes driving incident response and mitigation efforts Executed the Incident Response Life cycle to drive threat remediation and identify strategic countermeasures improving future defenses. Leveraged network security tools and capabilities to support Cyber Threat Monitoring activities. Documented results of cyber threat analysis effectively and prepared comprehensive hand-offs. Leveraged forensics techniques, tools, and capabilities to support Cyber Incident Response activities. Performed analysis of logs from various security controls, including, but not limited to, firewall, proxy, host intrusion prevention systems, endpoint security, and application and system logs, to identify possible threats to network security. Provide leadership and guidance to advance the defensive capabilities of the Threat Management Center

(TMC) and its subsequent ability to defend the DECA Enterprise. Collaborate with Threat Monitoring event handlers and to improve prevention and detection methods. Assessed the security impact of security alerts, incidents, and traffic anomalies to be able to gather a broad view of the overall risk profile of the enterprise, tracked suspicious network, application, and user behavior, Investigated breaches, gathered evidence, and analyzing data, Conducted hunts for evidence of compromise, Wrote up findings and provided recommendations Executed analysis of email based threats to include understanding of email communications, platforms, headers, transactions, and identification of malicious tactics, techniques, and procedures and phishing attempts Utilized and adhered to defined workflow and processes driving the threat monitoring and escalation/hand off actions. Analyzed potential cyber threats from a variety of sensors taking appropriate response actions to include threat containment and/or escalation. Tier II (SOC) Cyber Security Analyst NLogic - Fort Lee, VA February 2019 to July 2019 CSSP SOC Watch Analyst for Defense Commissary Agency (De Ca). Worked in support of monitoring a 24x7x365 Security Operations Center (C2SOC). Primary responsibilities were to monitor, detect, analyze, investigate, report, and track security-related "events" such as signs of intrusion, compromise, misuse, and compliance. Utilize provided sensors, systems, tools to monitor networks and systems for signs of intrusion, compromise, misuse, and non-compliance. Proactively monitor and track down anomalies, non-compliant systems, and other observed events that were detrimental to the overall security posture of the IT infrastructure.

Supported detection of vulnerabilities and sophisticated and nuanced attacks, discerned and remove false positives, and analyzed the information generated by systems. Supported scanning of devices on the network for network and system vulnerabilities. Supported daily analysis of security logs to detect incidents. Supported generation of metrics and reporting on a regular basis. Performed additional tasks or duties as assigned. Performed analysis of log files from a variety of sources within the Network Enclave (NE) or enclave, to include individual host logs, network traffic logs / packet captures, firewall logs, and intrusion detection system logs at least daily. Characterized and analyze network traffic to identify anomalous activity and potential threats to network resources. Assisted in the construction of signatures which can be implemented on CND network tools in

response to new or observed threats within the NE or enclave. Monitored appropriate security bulletins and report any security issues that may impact the IDS to the De Ca Computer Network Defense Service Provider (DSP) Manager, DSP Incident Responders, De Ca CIRT Lead, other DSP related personnel and DeCA Information Assurance personnel. IDS logs, databases, and security incident response reports were prepared and maintained. Received and analyzed network alerts from various sources within the NE or enclave and determined possible causes of such alerts. Reviewed and responded to events identified in the Host-Based Security System (HBSS). Coordinated with enclave CND staff to validate network alerts. Notify CND managers, CND incident responders, and other CNDSP team members of suspected CND incidents and articulated the event's history, status, and potential impact for further action. An analysis of any suspicious internal and/or external action must be accomplished and reported to DeCA CNDSP management based on established guidelines. Performed event correlation using information gathered from a variety of sources within the NE or enclave to gain situational awareness and determine the effectiveness of an observed attack. IT Specialist: Help Desk/Desktop Support IT Contracting Company - North Carolina June 2016 to January 2019 Tier II Desktop support technician supporting over 600 endpoints for the Defense Logistics agency at DLA Cherry point. Responsible for Asset Management, troubleshooting, and Re-imaging of out of compliance systems. Supported through an IT service management system an average of 10 tickets/day in response to network connectivity, software management, credential management, hardware troubleshooting, peripheral installation, printer configuration, Host OS error management, and Virtual Desktop Infrastructure configuration and error troubleshooting. Logistics Planner United States Army - San Antonio, TX November 2014 to May 2016 Served as a Logistics Planner to the U.S. Army North Assistant chief of Staff for Logistics and Distribution, conceptualized the writing, reviewing, and implementing of all logistics plans pertaining to Homeland Defense, and emergency civil distribution center coordination with FEMA and department of defense assets. Operations Officer United States Army - Colorado Springs, CO February 2014 to November 2014 Planned and launched all major training events for an organization of over 800 personnel. Managed and reserved all resources and materials required

to execute scheduled training. Personally oversaw from inception to completion all projects involved in setting up unit mandated training events for all five companies and attachments to the Division Headquarters. Logistics Manager United States Army - Colorado Springs, CO June 2012 to February 2014 Mentored program administrators and unit leadership on all distribution, transportation, and supply chain management operations within the organization. Facilitated the requisition, storage, and distribution of multiple types of supply, material handling equipment, and mobile distribution assets and platforms. Monitored the organization's required level of consumable materials to ensure correct quantities and quality were procured for specific functional requirements. Company Commander United States Army - Colorado Springs, CO June 2011 to June 2012 Commanded a fuel transportation company comprised of 60 5,000 Gallon fuel tankers. Provided Fuel distribution support to four Brigade Combat Teams, three separate brigades, four separate Battalions on Ft. Carson and surrounding installations. Managed the training, health, welfare, and morale of 169 individuals and their families. Operations Officer United States Army - El Paso, TX May 2009 to June 2011 Served as the organization's operations manager directly overseeing for the planning, synchronization, and resourcing of training events. Infantry Platoon Leader United States Army - El Paso, TX May 2008 to May 2009 Managed and coached a section of 33 Soldiers of an Infantry platoon. Facilitated the maintenance, accountability, and readiness of four Combat Vehicles and platoon equipment Trained and mentored Soldiers to be adaptive to an increasingly dynamic environment. Distribution Platoon Leader United States Army - El Paso, TX March 2006 to May 2008 Team Leader of a distribution section that implemented and oversaw the total supply chain operation effort from procurement to delivery to the entire organization of over 1300 personnel. Coordinated procurement, inventoried and distributed fuel, ammunition and heavy transportation equipment to the entire unit. Education Bachelor of Business Administration in Finance Radford University - Radford, VA December 2005 Skills BMC Remedy IT Services Management, TCP/IP, DNS/DHCP, IDS/IPS, Wireshark, Security, SIEM, Splunk, Easy IP, Cisco Firepower, HBSS, ACAS, Symantec/Bluecoat Reporter, Netcool/Netscout, Cyber Security, Information Security, NIST, Network Security, Information Assurance, RMF, NMAP, It Security, Cybersecurity, Comptia, Cissp,

CHFI Military Service Branch: United States Army Rank: Captain March 2006 to May 2016 Certifications/Licenses CompTIA Security+ CompTIA Network+ EC Council Certified Ethical Hacker, CEH MTA Windows 10 Operating System Fundamentals DoD-Secret Security Clearance- Active CISSP ITIL v3 EC Council Computer Hacking Forensics Investigator, CHFI EC Council Certified Incident Handler, ECIH

Name: Patricia Villegas

Email: ckent@example.org

Phone: 8495373512