Kerry P. Stinson jr Aberdeen Proving Ground, MD

 kerry.p.stinson@gmail.com 240-439-9671

TS/SCI Clearance (Top Secret with access to Sensitive Compartmentalized Information) with Polygraph(Active)

**Network Engineering | Cloud Engineering |**

United States Army veteran and a dynamic security officer with over 9 years of experience in the Federal and Military sector. Experienced Network Engineer and development for 10 years in both the federal government civilian sector and military component. Completed Cloud Architect pathway training program; acquired academic expertise in designing, planning, managing, and securing cloud solutions to create a sustainable cloud environment. Capable of designing, setting up, configuring, and optimizing a cloud computing environment to facilitate accessibility and eliminate cloud design issues. Capable of replicating data in several regions and availability zones by setting up cloud control measures for fault tolerance and disaster recovery. Developed excellence in defining access control lists for data privacy and security of data in transit and data at rest. Well conversant in AWS services, including EC2, S3, VPC EBS, Lambda, RDS, DynamoDB, and other services. Gained understanding of methods and tools to maintain security and protect data. Demonstrated knowledge of cloud architecture and implementation features (OS, multi-tenancy, virtualization, orchestration, elastic scalability). Excellent in configuring routers, switches, VOIPS, Taclanes and working with cables, and connectors.

Areas of Expertise

Network connectivity| Linux | Cisco| Network engineering| Command Prompt/Line | Routers | Switches | VOIPS| Taclanes | Amazon Web Services | Cloud Platforms | Data Privacy and Security | Configuration Management | Cloud Network Security | Multi-Tenant Implications | Rack cabling | CISCO 4331/9300 | Server Installation | S3 | VPC EBS | Wireshark l Lambda | RDS | DynamoDB | Trojan Analysis Node | IT System Problems and Troubleshooting (Windows) | Configuring Routers, Switches, and Hubs | IOS upgrades| ROMMON upgrades | Solar Winds | Tera Term | PuTTY Software |

Network Engineering(10yrs)

Cybersecurity(5yrs)

Physical/Personnel Security (10yrs)

AWS(2yrs)

IT Courses

* **Cloud Architect Pathway Program (Intellectual Point, Sterling VA/ Learn key):**

AWS Certified Solutions Architect Associate course completion certificate

CompTIA Sec+ CE, Certificate (comp001022006470)(Active)

CCNA(Currently Pursuing)(Learnkey)

Education

* *BS, Criminal justice, Southern New Hampshire University, 3.7 GPA, Graduated jan22*
* *AS, Criminal justice, Southern New Hampshire University 3.7 GPA, Graduated jan22*
* *Governor Thomas Johnson High School, Frederick, Maryland, 2011. Graduated 2011*

Professional Experience

CACI

***Network Engineer***  **August- Present**

Functioned as a key team member to evaluate and make tactical and strategic recommendations for the systems architecture, communications, data security, messaging, applications, support, performance, and availability.

* Performed system engineering, administration, maintenance, and engineering in primarily Microsoft Windows Server Environments
* Installed Cisco 4300/9300 series, KVM’s, Dell R440 Servers, KG-175D Taclanes, Cisco VOIPS
* Utilized software programs such as Tera Term, Solar Winds
* TFTP Server and Laptop LAN configuration setup for military fielding installations
* Conducted rack cabling, network configuration, and drawing packages based on the customer’s needs
* Provided system engineering to integrate external system interfaces with the Data Center Infrastructure Management
(DCIM) solution
* Integrated software plugin connector with ServiceNow for enterprise asset management and workflows
* Collaborated with engineers or software developers to select appropriate design solutions and ensure the compatibility of system components
* Developed system engineering, software engineering, system integration, and distributed system architectures
* Provided system administration of development, test, and production environments in AWS cloud environment
* Documented design specifications, operating instructions, and other system related information
* Identified system data, hardware, or software components required to meet user needs
* Performed ongoing hardware and software maintenance operations to include installing or upgrading hardware or software
* Performed security analysis of developed or packaged software components
* Provided technical guidance or support for the development or troubleshooting of systems
* Verified stability, interoperability, portability, security, and scalability of system architecture

Vision Quest Solutions, Quantico Virginia

***Network/Physical Security Officer* May 2022- August 2022**

Provided security / logistical solutions utilizing a customized approach to meet the demands of organizations. Utilized and demonstrated in depth knowledge of the security industry, and real-world experience conducting security operations both in the US, and around the world.

* Conducted risk management and mitigation
* Workstation configuration
* Router configuration
* Physical security assessments and site surveys
* Corporate security solutions and executive protection
* Vital infrastructure assessments
* Operational experience in developing and leading curriculum and training missions

Defense Intelligence Agency, Washington D.C **Jan 2020 – May 2022**

***Cyber Security Officer***

*Performing cybersecurity and force protection activities as part of an organized security team with the accountability of engaging in various protective functions, including cyber network defense, hazardous materials response activities, antiterrorism assessments, threat management, system diagnostics, security countermeasures, and global specialized protective operations in support of DIA field operations.*

* Engaged in various protective functions involving hazardous materials response activities, and antiterrorism assessments.
* Assisted in designing and testing modems, switches, routers, power converters and flash drives.
* Familiarity with NoSQL databases (DynamoDB, MongoDB, etc.)
* Experience working in a fast-paced environment to deliver innovation and improvements to new and existing infrastructure automation and development tooling.
* Assisted with building and managing massively scaled services.
* Automated complex tasks and processes.
* Consistently tracked the health of services, identified and fixed problems on complex systems.
* Experience with configuration automation (configuration as code, zero config, etc.)
* SAP experience: Developing solutions that facilitated effective data processing and information flow across the organization.
* Monitored Host Intrusion Prevention Systems (HIPS), Anti-Virus (AV), Rogue Sensor Detection (RSD), and Data Loss Prevention (DLP) via HBSS alerts to detect and prevent network security violations and data spillage.
* Provide guidance and oversight of position Standard Operating Procedures (SOP) documentation and execution.
* Perform research to determine requirements to include the implementation of and efficient network infrastructure to support various testing efforts which conform to UCR requirements. Ensure all systems are up to date, fully operational, and current with all Risk Management Element (RME) mandated security guidelines and directives.
* Created custom Host Intrusion Detection/Prevention signatures, host firewall rules, and filter out false positive events as they are generated.
* Troubleshoot network connectivity issues to include ports, protocols, and services (PPS), PKI authentications key exchange issues, network hardware malfunction or software corruptions, and or firewall issues.
* Utilized ArcSight, Wireshark, Intrusion Detection System (IDS), and other toolsets to identify and investigate anomalies.
* Conducted vulnerability assessment and monitored industry resources for latest hardware and software vulnerability reports and threats; and developed mitigation strategies to target those vulnerabilities.
* Troubleshooting, testing, and debugging security applications such as Wireshark, Security Onion, HBSS, or ACAS on desktop and laptops.
* Investigate computer incident and provided report to the Forensic Team for follow-up.
* Perform maintenance on networks, computer systems, hardware, and software
* Employ applicable security countermeasures to manage threats and minimize cyber-attacks.
* Maintained knowledge of and communicated changes in security regulations, best practices, countermeasures, compliance, and threats.
* Extract and prepare information and reporting from internal and external cyber elements into daily situational awareness and operational update briefings to leadership.
* Monitored network traffic for security events and performed analysis to identify security incidents.
* Performed and participated in the incident handling process, e.g., incident discovery, analysis and verification, incident tracking, containment and recovery, incident response coordination, escalation, and notification.
* Coordinate and ensure DOD incident handling procedures adhere to DOD guidance, regulations, and directives.
* Developed, enforced, analyzed, and interpreted security policies and procedures.
* Monitored, evaluated, and analyzed information systems and other data feeds to detect potential insider threats and provide advice and guidance for threat mitigation.
* Formulated policies and guidance based on requirement assessment not addressed in existing security directives and operations; manage, coordinated, and track individual insider threat cases from identification to mitigation.
* Promoted awareness of security issues among management and the workforce.
* Ensured sound security principles are reflected in the organization’s vision and goals.

United States Army National Guard, Westminster, MD **Jan 2020 – OCT 2022**

***Security officer***

*Provided seamless support in concluding the installation and community’s security, law enforcement, force protection, fire prevention, fire protection, emergency operations, and other emergency services programs using initiative and judgment.*

* Commended for quick reaction and diligence to duty while responding to medical, fire, car accidents, and in-flight emergencies while leading supervision, management, welfare, morale, and training of 60 Soldiers and consistently improving the efficiency of the sections and law enforcement services provided.
* Provided logistical management and accounted for over $100,000 worth of government equipment without loss.

United States Army, Fort Lewis, WA **May 2019 – Jan 2020**

***Security Officer/Senior Squad Leader***

* Conducted reoccurring training and counseling sessions to ensure the team understood and achieved the collective goals and objectives of the platoon and the company.
* Efficiently maintained a close working relationship with counterparts to conduct reoccurring assessments of the installation’s physical security posture.
* Conducted security in allowance with installation and tenant support agreements with a special emphasis on protecting arms, ammunition, explosives, and (AAE) facilities.
* Evaluated subordinate personnel's work performance and provided advice, counseling, or instruction to employees on both work and administrative matters.
* Supervised battlefield drills, area security, prisoner of war operations, civilian operations, law, and order operations, and support to the Army community through security and crime prevention.

United States Army, Camp Casey, South Korea **May 2018 – May 2019**

**Security Officer/Team Leader**

*Led a team of 25 police officers performing law enforcement operations in Camp Casey Korea. Worked side by side with the foreign government/host’s police force to provide law enforcement, anti-terrorism, and physical security protection to the installation and its outlined camps and training areas. 1 year of professional software and programming experience.*

* Selected over 12 police officers to complete a prisoner escort mission from Korea to Joint Base Lewis-McCord, WA.
* Spent time as part of an engineering team for software development.
* Worked with CI/CD infrastructure platforms such as Kubernetes, Jenkins, Circle Cl, AWS code suite, azure DevOps, etc.
* Contributed to the architecture, design patterns, reliability, and scaling of new and current systems.
* Performed anti-terrorism risk assessments a survey in support of the Camp Casey physical security plan; collaborated with Korean police officers (KPs) and other local agencies to determine security-in-depth and to aid in identifying supplemental controls to protect critical installation infrastructure.
* Aided senior supervisor in maintaining the accountability and serviceability of $1.8 million worth of military equipment.

United States Army, Fort Drum, NY **May 2015 – May 2018**

**Security Officer**

*Provided support in protecting* *over 9,000 soldiers, family members, civilians, and contractors engaged in military operations and support on Fort Drum, NY.*

* Performed in part of the Special Reaction Team (SRT). Participated in and excelled in a comprehensive program of periodic exercises to test and improve the readiness of the installation’s Emergency Services to deal with terrorist attacks, mass casualty situations, Emergency Operations Center procedures, and depot evacuation capability.

Professional Development

* *Basic Leaders Course, 2017.*
* *Special Reaction Team Phase 1, 2017.*
* *Special Reaction Team Phase 2, 2017.*
* *Unix Security for System Administrators*
* *Military Police One Station Unit Training, 2015.*