Security Engineer Security Engineer Security Engineer - WestRock (S.com) Atlanta, GA I'm a Network, Security & CyberSecurity professional with good experience working on Security frameworks SOC1/2, Information Security and Governance, System Access, Network Infrastructure, Asset Management, Cyber Defense/Offense, Risk & Compliance Analyzing Incident response alerts and monitoring, Information assurance, System hardening, Vulnerability management, Antivirus, Active Directory, Project Coordination, Operating Systems, DLP, Log Analysis, Standard Operating Procedures (SOPs), Service Level Agreements (SLAs) Work Experience Security Engineer WestRock (S.com) - Norcross, GA March 2019 to Present Use ITIL Service Request, Incident, Risk, Problem, ServiceNow, and Change Management Develop and maintain documentation related to the installation, administration, and Vendor IT security teams. Troubleshoots security related issues: firewalls, IDS/IPS, VPN, Proxy, segmented network infrastructure, multiple security zones Review, approve and assign user access requests submitted via WestRock access request portals, Active Directory, ServiceNow Information Security frameworks: ISO 27000, HIPAA, SOC1/2, NIST Cyber Security Framework, FFIEC Cyber Security Framework IDS/IPS Incident response alerts and monitoring, Information assurance, System hardening, Escalation, Vulnerability management, Network Security Monitoring & Analysis, Antivirus, Active Directory, Group Policy, Windows Environment Ensure network infrastructure and security standards for data centers, POPs, remote sites, and Cloud infrastructure align to site patterns that are communicated and adopted globally Research security standards, security systems and authentication protocols Works with internal customers to interpret/clarify/implement change requests on security devices; primarily firewalls, IDS/IPS and WAF and Web Filtering systems Manage perimeter security systems such as Access Control and Intrusion Detection Systems Maintain knowledge of VPN technologies and security protocols such as IPsec, ISAKMP, SSL, PKI, RADIUS, TACACS, EAP, LDAP Implement Cisco FirePower, ISE, ASA, FireEye, Palo Alto, Nessus, AWS, McAfee Security solutions etc. Works with BGP, OSPF routing protocols, Cisco Switches & Router, F5 Big-IP ASM, F5 Virtual Edition (VE) and Load Balancers Signal Support Systems Specialist (25U) United States Army Reserve - Birmingham, AL May 2013 to

Present IT Team Lead supervise group of 10 or more, lead small & large technical teams and/or work independently Telcommunications, VoIP, Satellite Communication (SATCOM), COMSEC, Operational Intelgenece/Analystics, VTC Equipment, IT Inventory Manager & IT Helpdesk Supervisor Knowledge and solid understanding of networking technologies and topologies (i.e. Layer 1-4, TCP/IP, IPv4, RSTP, REP, IPSec, DHCP, DNS, SNMP, NTP, VLAN, NAT, WAN, Cisco IOS) and remote access connectivity requirements Mobility, Data Management/Government Issued Devises/End User Experience, VDI Administrator, IT service management (ITSM), IT Infrastructure Library (ITIL), IT Project Management, Network Infrastructure, Lifecycle Management, Agile/Waterfall methodology, IT Project Management via Six Sigma DMAIC or SDLC method, Agile/Waterfall methodology knowledge, SCRUM methodology & Coordinate project management activitie vis Microsoft Project,, resources, equipment and information Networking Experience - Provided high-level information assurance training and classified network configuration and Management of all core and Cisco switches/routers; Tier 2 administration via Active Directory Users and Computers (ADUC) Contribute and provide training, adoption and compliance for all service & technical processes, cross-functional technical projects via all phases of the project lifecycle, handling multiple medium to large projects simultaneously. Analyze, capture, and document, analysis other required documentation to ensure compliance Advanced knowledge and use of MS Office Suite including Word, Excel, Project 2016, PowerPoint, Visio, SharePoint. Work within Tactical Operations Center (TOC), Security Operations Centers (SOC), Network Operations Centers (NOC) CyberSecurity Analyst Department of Health and Human Service - Atlanta, GA January 2018 to December 2018 Work in CSIRC/SOC environment executing VMware virtualization, Cyber Kill-Chain process, Enterprise Data Management / BYOD / End User Experience, Windows Infrastructure, DoD Information Assurance/Cybersecurity. Tools: FireEye, Cisco Stealth Watch, Wireshark, RSA Security Analytics/Netwitness, Interdictor Respirator, SolarWinds, Remedy, Palo Alto, Sourcefire, McAfee ESM, Agiliance Risk Vision, Salesforce, Cisco WebEx and Splunk Provide incident response and ownership based on escalation and handoff procedures from junior or mid-senior team members; Actively participate in large scope high impact cyber breaches and

manage Incident Response workflow and activities to support response and remediation. Use SIEM procedures & investigative methods, perform root cause analysis for recurring cyber incidents using via Information Security frameworks: ISO 27000, PCI DSS 3.2, HIPAA, SOC1/2, NIST 800-53, NIST Cyber Security Framework, FFIEC Cyber Security Framework. IDS/IPS Incident response alerts and monitoring, Information assurance, System hardening, Escalation, Vulnerability management, Antivirus, Active Directory, Operating Systems, DLP, NAC, AWS, Log Analysis, IOCs, Network Traffic, Packet Analysis, and email analysis, event logs, Standard Operating Procedures (SOPs), develop and monitor SLAs. Malware responsibilities: viruses, Trojans, Zero-Day, Worms, Logic Bomb, Botnets, Root-kits, Ransom Ware, Adware, Backdoor, Spyware, etc. Provide Identity Access Management (IAM) and/or Privilege Access Mgmt. (PAM), Microsoft Active Directory, IT service management (ITSM), IT Infrastructure Library (ITIL), Six Sigma continuous improvement, Established reporting process and modified/created policies and procedure to support DHHS CSRIC & Risk Management Program. Strong understanding of HIPAA and privacy laws regarding release of information. Composed and deployed a unifying governance standard for all applicable elements of HIPAA, also delivered HIPAA training to new employees. Planned for information security risk assessments to meet DHHS requirements and audit recommendations Provide Tier Level 2/3 support in fast-paced, multitasking, cross-functional team in Government & Enterprise entities covering areas in Cyber Security, ITIL Change Management, Information Security and Governance, Risk, & Compliance. Splunk configuration, query, reports, dashboards & Assist Information Security Managers during all 3rd party audits. Network Engineer/ IT Asset & Lifecycle Manager DCMA/Department of Defense - Atlanta, GA June 2017 to December 2017 Large 24/7 government DoD, corporate, and enterprise environments; in Security Operations Centers (SOC), Network Operations Centers (NOC). On-site & Remote access troubleshooting of classified DoD systems. Tier Level-1/2 support, configuration management, and troubleshooting for over 200 + sites to identify and solve issues at Layers 1,2,3 (i.e., Physical, Data Link and Network) Knowledge and solid understanding of networking technologies and topologies (i.e. Layer 1-4, TCP/IP, IPv4 & IPv6, RSTP, REP, IPSec, DHCP, DNS, SNMP, NTP, VLAN, NAT, WAN, Cisco IOS) and remote access

connectivity requirements Assisted Firewall team in analyzing anything that causes detriment to the user, computer, or network Provide technical support through allocating systems resources, managing accounts, administering passwords, documentation, security, recoverability and access including deploying security and operating system patches. Maintain hardware and software inventories including developing and updating departmental distributed software license management policy Coordination with business vendors and technical DoD partners, Process Owners, Service Catalog Managers, Service Owners and Service Managers to identify services and related elements (i.e. applications, infrastructure, knowledge, requests, groups etc.) in support of ITSM, IAM processes and IT Infrastructure Library (ITIL) Gather, develop, coordinate, and maintain requirements for projects and/or systems from initial phase to final implementation, assuring requirements meets standards & Create and maintain process documentation Responsibilities: Inventory Management, IT Project Coordination, Infrastructure Mapping/Design, Incident Response Assistance, Operational Readiness for New Installation & Circuit Upgrades, Log Analysis, Network Traffic Packet Analysis, Change Management Planning and Cisco Configuration & Implementation, Assist with Intrusion Detection/Intrusion Prevention (IDS/IPS) Solutions & Network Security Monitoring, System hardening, Vulnerability assessment and VDI Design and Implementation VMware, VPN, VLANs, ITIL Port Configuration, Powershell, Active Directory and Windows/Cisco, PuTTy, SSH and Secure CRT, Change Gear Ticketing System, Solarwinds Monitoring, Experience with Oracle reports, MS Project and PL/SQL skills. Experience developing, entry-level Network Security Architecture & Integrated Systems, Identity and Access Management. DoD Network infrastructure hardware (Cisco routers & switches, optimizers, media converters, Wi-Fi controllers, VoIP, VTC components) Information Innovators Inc January 2016 to June 2017 Education Computer Information Systems Georgia State University - Atlanta, GA 2020 Skills Active directory, Hipaa, Pci, Solarwinds, Vmware, Dlp, Ids, Ips, Malware, Microsoft project, Data analysis, Sdlc, Sap, Process management, Quantitative, Mitigation, Risk management, Problem solving, Strategic sourcing, Inventory Additional Information Skills: IDS/IPS monitoring, Self-Directed and Goal Driven, Project Management, Asset/Inventory Management Excellent Management Skills,

Business Analytics, Microsoft Suite/Office 365, Microsoft Project, DMAIC/SDLC/Agile/Waterfall, HIPAA/PII/PHI/PCI, Strategic Sourcing Process, Strong Quantitative Aptitude Solarwinds Monitoring, System Hardening, Microsoft Active Directory, Problem Solving Skills, Excellent Leadership Skills, Excellent Troubleshooting, Risk Management, Malware, Mitigation & Escalations Process Management, Planning & Scheduling, SAP experience, Contract Management, Data Analysis/DLP, VMware, Solarwinds Monitoring, System Hardening, Microsoft Active Directory

Name: Kristy Mclaughlin

Email: ljones@example.org

Phone: 421.549.1450