Security Engineer Security Engineer Security Engineer - Ingenicomm Manassas, VA Ten+ years of security engineering. Thorough knowledge of systems analysis, hardware and software troubleshooting, customer focused technical training and technical process management. 10+ years of experience in Microsoft network/server hardware/software engineering and support, 2+ years of Linux server/workstation support, as well as client-server network management/administration/engineering, customer support/training, technical research/writing, and software analysis. 2+ years of firewall administration on both Checkpoint and Cisco platforms. Authorized to work in the US for any employer Work Experience Security Engineer Ingenicomm December 2017 to Present December 2017-Present Ingenicomm specializes as an engineering company, primarily servicing the civilian aerospace market (NASA, NOAA). Products include configurable ground systems, programmable telemetry processors, signal conversion devices and CCSDS calculators. Security Engineer Information Technology Security engineer and liaison responsible for the implementation of the IT security architecture on the NOAA Jason-3 (NJGS) tech refresh ground system. Duties included the installation of the system's hardware firewalls, hardware Intrusion Prevention System (IPS/IDS), software firewall and software Host Intrusion Prevention (HIPS) as well as multi-factor user authentication. Built, configured and implemented Windows Server 2016 Standard Domain controllers with full Active Directory redundancy. Implemented Active Directory integrated DNS. Responsible for user and group security/administration. Maintain Group Policy -- responsible for building, testing and rolling out GPO's that meet Center for Internet Security (CIS) benchmarks. Configured and integrated the following hardware solutions: McAfee Network Security Platform IPS solution, Cisco ASA firewalls, CheckPoint firewalls and RSA Secur-ID two-factor authentication. Implemented Tripwire Enterprise security configuration compliance software. Integrated solution with disparate systems in a 100+ node environment. Windows/Red Hat hosts files, registry monitored for change. Cisco routers/switches monitored for change. Implemented Tripwire Log Console for Windows/Syslog/application log file collection. Installed, configured and rolled out Symantec Altiris for the purpose of hardware/software monitoring and auditing. Worked with Symmetricom time servers and integrated all hosts and network appliances with this solution. Information Assurance Analyst Lead for conducting scheduled scans of all Windows, Red Hat hosts and network appliances. Ran scans, compiled results and disseminated to management for review. Mitigated vulnerabilities by patching software (utilizing WSUS and RHSS) and creating specialized GPO's to modify registry settings on hosts throughout the Domain. Also worked to update/upgrade IT security application software for compliance as well as patching/upgrading Cisco/CheckPoint IOS software. Responsible for maintaining Tripwire Log Console - setting up audit loggers, creating audit logger reports, setting up event databases, integrating all hosts/network devices in Domain for reporting purposes. Responsible for IPS event analysis and monitoring. Work with McAfee Network Security Platform threat monitors to analyze events, determining threat severity. Monitor McAfee ePO, utilizing reports for anti-virus and HIPS related activity. Setup RSA SecurID appliances. Integrated RSA with Active directory. Disseminated tokens to end-users. Responsible for running reports related to any potential security incidents. Information Assurance Risk Analyst (Senior) Kratos Secure Information November 2017 to December 2017 November 2017-December 2017 Kratos functions as a 3PAO, one of several companies responsible for providing information assurance/risk management for the FedRAMP (Federal Risk and Authorization Program) cloud computing program. Information Assurance Risk Analyst (Senior) Responsible for conducting FedRAMP security assessments. ? Assessment of customer cloud computing systems based on NIST 800-53 security controls. * Information, evidence gathering * Onsite interviews * Report writing Security Analyst (Senior) Freddie Mac November 2015 to November 2017 November 2015 - November 2017 Freddie Mac, a government sponsored public enterprise, has as its mission, to aid in the expansion of the home mortgage secondary market. My function is to serve as a senior level analyst on the security information and operations (SIOC) monitoring team. Security Analyst (Senior) Responsible for oversight on daily platform processes that ensure Sarbanes-Oxley Act control compliance. Review junior level analyst's daily control documentation, providing evidence oversight and assist in correcting reporting errors. Create, edit and update security related documentation. Primary author of security monitoring team's (SIOC) standard operating procedure (SOP). Primary author of SIOC security and information event management (SIEM) SOP, as well as ticketing system, documentation. Review document repository (SharePoint) and act as the primary for authoring new SIOC documentation (SOP's or runbooks), editing documentation, and working with junior level analysts to help assist in the creation of new documentation. Security monitoring: ? Splunk application management: * Primary tasked to assign Splunk notable events to junior level analysts. Duties include event assignment, follow up and checks against established service level agreements to ensure notable events are being assigned, analyzed, escalated or closed. All in agreed time frames. ? Splunk analyst: * Utilize Splunk application to detect gaps in security posture, including mis-configured devices, applications, hosts, network devices, servers, appliances, system processes and protocols. * Utilize application to detect potential security incidents. Escalate incidents to incident response (IR) team, providing detailed, written analysis and recommended next steps. ? Splunk engineering: * Tasked to evolve into the team application subject matter expert (SME), effectively developing future use cases, writing moderately complex search statements, expanding knowledge of regex statements. Duties will expand as needed. Security Engineer Navstar Incorporated/US Department of the Treasury/FinCEN - Tysons Corner, VA October 2014 to October 2015 Tysons Corner, VA October 2014 - October 2015 Navstar is a federal defense and civilian sector information technology solutions provider, acting as the prime contractor for IT infrastructure and IT security support at FinCEN. I worked on the IS (information security) team as a security engineer and certification and accreditation analyst. Security Engineer IS security engineer responsible for the implementation and maintenance of the security tools utilized at FinCEN. Duties include engineering the network access control (NAC) hardware solution (ForeScout CounterAct NAC), and conducting security scans of multiple host networks (web, operating system, application, database) in support of annual and delta security assessments (required by FISMA). Engineer the ForeScout NAC platform. Duties include creating and editing NAC policy rules to accept or prevent hosts from accessing the network based on device properties, researching/testing NAC plugins for expanded functionality, applying software patches to maintain the platform, and troubleshooting any issues that may arise. Work includes proficiency at the command line (SSH), utilizing ForeScout utilities as well as Red Hat Linux commands. Engineer the Tenable Nessus scanning platform (Nessus Security Center, Nessus Scanner, Nessus Log Correlation Engine). Work includes scoping the FinCEN network to setup discovery scans, coordinating with infrastructure technical personnel to ensure scans run correctly, setting up scan policies as well as implementing Nessus audit files. Engineer the DbProtect database scanning platform. Ensure the application has up to date configurations for FinCEN target databases. Test connectivity, credentials and coordinate with database administrators to ensure the entire environment is being covered. Engineer the WebInspect web application scanning platform. Ensure the scan database is up to date and coordinate with application engineers to schedule scans. Utilize Penetration Testing software (CoreImpact) to conduct network scans. Additionally, setup software to perform a system wide phishing test. Assist the FinCEN Information Systems Security Officer (ISSO) in planning and executing assessments mandated by federal law (FISMA). Coordinate with external representatives for scanning engagements, including working with the infrastructure team to ensure proper network access is gained for scanning purposes. Editing security documentation (ex. FinCEN policies, system security plans, rules of engagement, technical assessment reports). Assist technical representatives with the resolution of POAMS (plan of action and milestone) that arise from system assessments. Perform daily log file review and analysis, with the objective of providing deterrence of a potential security breach. Review includes syslog/Windows event review with Tenable Log Correlation Engine as well as web traffic analysis utilizing Blue Coat Reporter. IT security analyst Camber Corporation/Avaya Government Solutions - Suitland, MD September 2011 to October 2014 Suitland, MD September 2011-October 2014 Camber Corporation is a federal defense and civilian sector information technology solutions provider. I worked as an IT security analyst/sysadmin/information assurance engineer on a high-profile project for the National Oceanic and Atmospheric Administration (NOAA). Security Engineer Information Technology Security engineer and liaison responsible for the implementation of the IT security architecture on the NOAA Jason-3 (NJGS) ground system. Duties included the installation of the system's hardware firewalls, hardware Intrusion Prevention System (IPS/IDS), software firewall and software Host Intrusion

Prevention (HIPS) as well as multi-factor user authentication. Built, configured and implemented Windows Server 2008 R2 Standard Domain controllers with full Active Directory redundancy. Implemented Active Directory integrated DNS. Responsible for user and group security/administration. Maintain Group Policy -- responsible for building, testing and rolling out GPO's that meet Center for Internet Security (CIS) benchmarks. Configured and integrated the following hardware solutions: McAfee Network Security Platform IPS solution, Cisco ASA firewalls, CheckPoint UTM-1 firewalls andR SA Secur-ID two-factor authentication. Configured and installed McAfee ePolicy Orchestrator Server. Built firewall rule-set and policies for all Windows hosts. Built HIPS policy for all Windows/Red Hat hosts. Built anti-virus policy for all hosts. Pushed or installed ePO security software to all servers/workstations in Domain. Maintain security posture with frequent updates of anti-virus signature files and HIPS signature files. Implemented Tripwire Enterprise security configuration compliance software. Integrated solution with disparate systems in a 100+ node environment. Windows/Red Hat hosts files, registry monitored for change. Cisco routers/switches monitored for change. Implemented Tripwire Log Console for Windows/Syslog/application log file collection. Installed, configured and rolled out Symantec Altiris for the purpose of hardware/software monitoring and auditing. Worked with Symmetricom time servers and integrated all hosts and network appliances with this solution. Information Assurance Analyst I functioned as the primary in the preparation for the Security Test and Evaluation (ST&E). I worked with the government IT security liaison, to create IT security controls testing documentation and to test against the controls. It was my responsibility to generate documentation that conformed with FIPS 199 categorization of a high impact system as it relates to IT security confidentiality, integrity and availability. FIPS 200 controls were then mapped to the documentation for testing. Implemented security controls drawn from NIST 800-53 standards and guidelines in compliance with FISMA. My duties include acting as the primary for the annual Assessment and Authorization (A&A). Responsibilities for the A&A included reviewing documentation and providing artifacts proving the ground system meet IT security controls drawn up during the ST&E. Additionally, Nessus scans are done on all ground system components with the objective of resolving all documented vulnerabilities classified as critical, high, medium and low. I lead a team of 4 engineers, coordinating the task of resolving these vulnerabilities.   Lead for conducting scheduled scans of all Windows, Red Hat hosts and network appliances. Ran scans, compiled results and disseminated to management for review. Mitigated vulnerabilities by patching software (utilizing WSUS and RHSS) and creating specialized GPO's to modify registry settings on hosts throughout the Domain. Also worked to update/upgrade IT security application software for compliance as well as patching/upgrading Cisco/Checkpoint IOS software.   Created reports for Tripwire Enterprise specific to CIS policy compliance benchmarks. Responsible for additional reports for NIST 800-53 compliance. Acted on results, (for example creating scripts to modify host settings for compliance).

Responsible for maintaining Tripwire Log Console - setting up audit loggers, creating audit logger reports, setting up event databases, integrating all hosts/network devices in Domain for reporting purposes.   Responsible for IPS event analysis and monitoring. Work with McAfee Network Security Platform threat monitors to analyze events, determining threat severity.   Monitor McAfee ePO, utilizing reports for anti-virus and HIPS related activity.   Setup RSA SecurID appliances. Integrated RSA with Active directory. Disseminated tokens to end-users. Responsible for running reports related to any potential security incidents.   Documentation duties included creating tailored System/Software User's Manuals (SUM) and System/Software Description Documents (SDD) for IT security components. I was also tasked to create PowerPoint training slides for instructing the federal IT security resources on how to work with the IT security components of the ground system.

Note: My career history in information technology extends back to 1994. For the sake of relevance and for brevity, that information has been omitted. It will be provided upon request. Education Bachelor of Arts The Catholic University of America - Washington, DC Skills Altiris (4 years), authentication. (4 years), Checkpoint (4 years), Cisco (4 years), Cisco asa (4 years), databases (5 years), firewall (4 years), firewalls (4 years), Intrusion (4 years), Ips (4 years), log file (5 years), Nessus (4 years), Network security (4 years), Red hat (5 years), Rsa (4 years), Security (7 years), solutions (5 years), Symantec (4 years), Tripwire (4 years), Wise (4 years) Additional Information Operating Systems: Microsoft Windows 10, Microsoft Windows 2016 Server, Red Hat Enterprise

Linux Server   Software: IT Security Policy/Controls Compliance: Tripwire Enterprise IT Security Vulnerability Scanning/Assessment: Nessus Firewall: Cisco ASA 5505/5520 Series, CheckPoint SecurPlatform, McAfee Host Intrusion Prevention (HIPS) Intrusion Prevention System (IPS): McAfee Network Security Platform (NSP/NSM) Inventory Control (Hardware/Software): Symantec Management Platform/Symantec Altiris Multi-Factor Authentication: RSA SecurID Anti-virus solutions: McAfee Virus Scan Enterprise, McAfee Virus Scan Enterprise for Linux, McAfee ePolicy Orchestrator Log File Management/Analysis: Tripwire Log Console Software Patching Solutions: Microsoft Windows Server Update Services (WSUS), Red Hat Satellite Server (RHSS) Time Servers: Symmetricom Databases: MS SQL Server, MySQL Virtualization Software: VMWare, Sun Virtual Box (open source virtualization software) Scanning Software: Tenable Nessus Security Center, Nessus scanner, Tenable Log Correlation Engine, HP WebInspect, CoreImpact Professional, DbProtect Network Access Control (NAC): ForeScout CounterACT NAC Web Monitoring: Blue Coat Reporter SIEM: Splunk   HARDWARE: Dell servers/workstations, Hewlett Packard servers/workstation, Cisco routers/switches, Cisco ASA 5500 series firewalls, CheckPoint firewalls, McAfee Network Security Platform IPS, Symmetricom time servers, Wyse thin client

Name: Erica Johnson

Email: jsilva@example.net

Phone: 435-438-6542