**Anjali k**|732-338-8659 |

**Summary:**

* Cyber Security Engineer with good experience in Implementation, Administration, Operation, and Troubleshooting of enterprise data networks
* Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical information security solutions, and sound knowledge in SOX and PCI compliance requirements, and understanding of NIST and ISO standards
* Experience as a Splunk Engineer configuring, implementing and supporting Splunk Server Infrastructure across Windows, UNIX and Linux environments
* Configure, maintain and design network security solutions including firewalls (CheckPoint, Cisco ASA, and Fortinet), IDS/IPS (Cisco, CheckPoint and SourceFire), VPN, ACLs, Web Proxy, etc.
* Hands-on experience on the Operations and management of Aruba based wireless network providing multiple SSID platforms for DoD users
* Hands-on experience on Web Application Firewalls and attack mitigation techniques
* Work closely with clients Information Assurance analysts to oversee the preparation of a comprehensive and executive and Accreditation (C&A) package for approval of an Authorization to Operate (ATO); generate, review and update the System Security Plan (SSP) against NIST and NIST requirements
* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001
* Facilitate implementations of information security policies, account security policies and standards for logical and physical security
* Perform Risk Assessment, Gap analysis & create Risk Mitigation plan
* Good experience to provide remediation consultation to organizations and system owners, ensuring vulnerabilities are remediated IAW DISA/NIST and Cyber Threat Intelligence research
* Modernize assessment tools by researching emerging technologies and outlining their procurement to increase productivity and effectiveness
* Having a good understanding and Knowledge for implementation for ISO 27001, NIST 800-series, DIACAP, and FISMA guidance/governance
* Strong knowledge of Imperva web application firewall for monitoring for in-depth analysis of attacks and SIEM tools such as Splunk, HP ArcSight for analysis and log monitoring.
* Led an effort to create a new process in filtering and manage IPS events by automating the process and streamlining Security Operation Center (SOC) triage efforts.
* Managed HBSS McAfee ePO, configured HIPS 8.0 policies, verified and created server tasks, monitored events, created and enforced DLP policy, managed Rogue System Detection.
* Support deployment of all HBSS point products and updates to include Mcafee agent, HIPS, VSE, DLP. Perform HBSS policy tuning, HIPS, IPS tuning, and all related tasks.
* Experienced with Proxy and Malware-mitigation (BlueCoat, Radware/ApplXcel/Alteon, FireEye), threat detection and data leakage protection (Network DLP/Vontu/Symantec, BlueCoat Security Analytics.
* Dedicated, multifaceted, and detail-oriented professional with progressive experience in Cybersecurity operations; complemented with wide-ranging knowledge of McAfee ePolicy Orchestrator (ePO) and networking technologies such as firewalls, switches, and routers.
* Analyzed the Policy rules, monitored logs and documented the Network/Traffic flow diagram of the Palo Alto Firewalls placed in the Data Center with MS Visio.

**Work Experience:**

**Cyber Security Engineer/Vulnerability Management**

**New York, New York, United States Dec 23– Till date**

**Morgan Stanley**

**Responsibilities:**

* Establish and maintain an IT Compliance program for Financial Security Infrastructure team that minimize risks to IT objectives through effective, efficient, scalable, and cost-effective design and operation of controls, including Sarbanes Oxley (SOX), ITGC (IT General Control) using COBIT framework, and other domestic and international compliance requirements.
* Involved in DLP data encryption, monitoring/reporting and remediation of internal and external threats/vulnerabilities.
* Experience as a Splunk Engineer conguring, implementing and supporting Splunk Server Infrastructure across Windows, UNIX and Linux environments
* Implemented the vulnerability management concept as an enterprise solution to mitigating vulnerabilities effectively
* Supervised a Vulnerability Management Team
* Created and modified scripts/ batch files in order to push patches or perform installation on multiple computers
* Trusted Agent for Smart Card and CA Token Deployment
* Assisted with implementation of software patches and remediated for all classified and unclassified computers, switches/routers, printers, video teleconference units (desktop and suite)
* Develop Best Practices to maximize the use of Splunk Enterprise Security with Carbon Black, Qualys, Varonis, CyberArk, Symantec, and Zscaler.
* Resolved electronic spillages (classified to unclassified)
* Investigated and resolved information assurance incidents.
* Splunk Administration and analytics development on Information Security, Infrastructure and network, data security, Splunk Enterprise Security app, Triage events, Incident Analysis.
* Provided Azure Security and Compliance reviews and solutions for government systems to facilitate the secure and compliant use of Azure for government agencies and third-party providers building on behalf of government.
* Ensured Azure Government system was compliant to meet a FedRAMP Provisional Authority to Operate (P-ATO) and DoD Provisional Authorization (PA).
* Understand the threat landscape as related to vendors and perform vendor risk assessments
* Works with Encase, FTK, Cellebrite, Gargoyle, IEF, tools, plus dozens of utilities for ripping, extracting, repairing, copying, de-duplicating, automating and more
* Played an Integral role in migrating company's security firewall environment from FortiOS 4.0 firewall platform to Fortigate FG 100D.
* Collaborate with Internal audit, External Audit, SOX PMO in a regular cadence, discuss changes to the control environment and prepare effective, efficient compliance and substantive test plans and SOX Calendar.
* Work closely with the Risk and finance teams to associate a monetary value to security risks within the User Behavior Analytics (UBA) tool.
* Worked on projects moving to cloud services such as Azure, Office 365 and Amazon Web Services (AWS).
* Worked Directly with Splunk Inc sales team in determining Log size and licensing cost for the client's Infrastructure
* Expertise in development of Information Security Programs based on frameworks such as NIST, NIST, NIST, ISO 27002, COBIT 5.0, FFIEC, GLBA, SOX, PCI & PII with IT Risk drivers KPI's and KRI's to ensure Financial regulatory compliance and data security.
* Conduct internal and external security audits based on standard cybersecurity frameworks from ISO 27002, COBIT, NIST, OWASP and Cloud Security Alliance
* Troubleshoot Splunk servers, agent problems, and issues
* Worked extensively in Configuring, Monitoring Elk,Extrahop.
* Built proof of concept (POC) for Localization to use AWS for some transcoding workloads. AWS services used were EC2, S3, Lambda, Elastic Transcoder. Second phase would be to add Captions and Digital Rights Management (DRM).
* Assessment guidance/standards used; NIST SP, NIST, NIST, ISO27002, ISO27005, to ensure regulatory compliance and proper assessment of risk.
* Develop documentation for new/existing policies and procedures in accordance with Risk Management Framework (RMF), NIST SP requirements.
* Used GZIP with AWS Cloud front to forward compressed files to destination node /instances.
* Dynamic monitoring and analysis of Intrusion Detection Systems (IDS) to identify security issues for remediation. Analyze, recognize, correlate, and report any potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information from AccelOps SIEM, Snort logs and Checkpoint FW logs.
* Consulted with business and technology partners to create and provide security recommendations and best practices.
* Expertise in development of Information Security Programs based on frameworks such as NIST, NIST, NIST, ISO 27002, COBIT 5.0, FFIEC, GLBA, SOX, PCI & PII with IT Risk drivers KPI's and KRI's to ensure Financial regulatory compliance and data security.

**John Wiley & Sons International Rights**

**Cyber Security Analyst Mar 19 – sep 2023**

**Pittsburgh, PA Responsibilities:**

* Perform cybersecurity assessments of the Marine Corps Enterprise Networks (MCEN) General Support Systems, Sites, and Major Applications for Assessment & Authorization (A&A).
* Perform the United States Marine Corps (USMC) Risk Management Framework (RMF) and Department of Defense (DOD) Information Assurance and Accreditation Process by the DOD Instruction 8510.01, National Institute of Standards and Technology (NIST) Special Publication (SP), and SP Rev 4
* Use Splunk Search Processing Language (SPL) and Regular expressions
* Document and complete the RMF packages using the Marine Corps and Accreditation Support Tool (eMASS) throughout the A&A lifecycle.
* Develop Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) Test Plans to assess the technical and non-technical security features in the accreditation boundary.
* Perform security scans using ACAS tool and analyze a variety of network devices, applications, and operating systems for STIG compliance.
* Review routers, firewall policies, Intrusion Prevention Systems (IPS) and Intrusion Detection systems to ensure appropriate network traffic and unauthorized protocols are filtered, and encryption and authentication algorithms are FIPS 140-2 compliant.
* Measuring performance metrics of CPU, Memory Disk space utilization before and after the installation of Crowdstrike sensors using Splunk
* Review Cybersecurity authorization artifacts such as COOP, Contingency Plans, System Security Plans (SSP), Configuration Management Plans, Information Assurance Vulnerability Management Plans, account management, Physical security, MOU/SLA’s, network diagrams for compliancy with RMF IA controls, DOD, and USMC Headquarters Marine Corps (HQMC) policies, procedures, orders, and directives.
* Document security assessment results and perform risk assessments using CVSS based calculations.
* Prepare Security Assessment Reports (SAR) based on the Plans of Action & Milestone (POA&M) findings, category levels, mitigations and determine the risk level of systems to provide to the USMC Authorizing Official (AO) for an authorization decision.
* Assisted in implementing the defense levels, security categorizations, and overlays required for systems and the RMF control selection per the Committee on National Security Systems (CNSSI) 1253 standards.
* Use Splunk Security Manager to identify threats and assigned category
* Proactively implemented updates, maintained, managed, monitored, and supported enterprise network and systems security operations infrastructure throughout the shared services environment.
* Perform daily DLP Incident monitoring, analysis and reporting, solution checks, client interaction, and day-to-day DLP operations.
* Managing SIEM - Net forensics
* Create and run routine reports and data analytics in Excel and Tableau. Audit and validate data/reports
* Responsible for delivering an end to end continuous integration - continuous delivery system for the products in an agile development approach using Chef/Ansible and Jenkins and Shell Scripts.
* Developed customSIEMdeliverables in Splunk to meet customer needs in a variety of domains like security, nancial services, IT Ops, human resources, physical security, etc.
* Wrote Ansible playbooks to setup Continuous Delivery pipeline and this primarily consists of a Jenkins and Sonar server, the infrastructure to run these packages and various supporting software components such as Maven.
* Managed the large security, risk and compliance initiatives of SOX-404 IT, PCI DSS and HIPAA/HITECH, Privacy Act, and FTC including security policies, procedures and controls.
* Experience with Windows, Linux, vulnerability assessment tools, firewalls, IDS/IPS, HIPS/HIDS, Nessus, NMAP, SIEM, Splunk, Rapid7 Nexpose and InsightVM, WAF, routers, switches, VMware, Endpoint Security, Cloud Security, Symantec Endpoint Protection.

**Cyber Security Engineer Pittsburgh, PA Sep 18 – Jan 2019**

**Alcoa**

**Responsibilities:**

* Responsible for the installation and maintenance of new network connection for the customers.
* Configured all the required devices and equipment for remote vendors at various sites and plants.
* In-depth expertise in the implementation of analysis, optimization, troubleshooting and documentation of LAN/WAN networking systems.
* Maintained and managed assigned systems, Splunk related issues and administrators
* Manage enterprise security systems, identifying key security risks, reporting risks to management with recommendations for corrective action utilizing NIST frameworks.
* Worked on log parsing, Splunk searches, including external table lookups.
* Involved inDigital Guardian DLPdata encryption, monitoring/reporting and remediation of internal and external threats/vulnerabilities SME (Subject matter expert) on SIEM and writing detection rules on the platform Scripting or programming experience in Python and PowerShell.
* Supported nationwide LAN infrastructure consisting of Cisco 4510 and catalyst 6513.
* Worked with cisco routers 2600, 2900, 3600, 3800, 7200 and 7600 and switches 2900, 3560, 3750, 4500, 4900, 6500
* Perform ISO 27001, PCI and SOX Audits and drive them to the closure of findings.
* Developed Cyber Security Standards on NIST Frameworks and insured their proper implementation to reduce the risk of vulnerability to IT assets.
* Implementing various policies as per client compliance to restrict web access, troubleshooting proxy related access issues and generate Internet access reports using Websense web proxy
* Creating compliance rules, extracting Security risks and auditing the policies in firewall using Tufin firewall monitoring tool
* Reviewed encryption logs and DLP logs to regulate use base technological risk violations
* Upgrade, managing and troubleshooting various issues with Cisco IPS
* Rules implementation, log analysis, logical troubleshooting and managing various Checkpoint products-Power-1, UTM-1, Smart-1 appliances and Cisco ASA appliances
* Part of Disaster Recovery Datacentre’s Security Configuration and Management team

**Honeywell India Mar 2012 – Dec 2015**

**Cyber / Network Security Engineer**

**Responsibilities:**

* Knowledge and experience in IT risk or compliance disciplines including risk assessment.
* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001.
* Websense, Symantec Endpoint Protection and Active Directory (User Account Management specific) events monitoring and analysis.
* Infrastructure security design and implementation expertise (Firewall, IDS/IPS, SIEM, Proxy services, Antivirus, Vulnerability Management, Key management, Web application firewall and PKI).
* Developed customSIEMdeliverables in Splunk to meet customer needs in a variety of domains: IT security, nancial, IT Ops, human resources, physical security, etc.
* Management of Cloud security, Vulnerability assessment, and security audits.
* Review and updated System Security Plan (NIST SP ), Risk Assessment (NIST SP ), and Security Assessment Report (NIST SP A).
* Reducing Proofpoint Digital Risk to defend impersonation of the brand to harm current market.
* Managing SIEM - Net forensics, its prevention controls, Penetration testing
* Perform personnel interviews during assessments and review proper analysis of testing results.
* Review documentation as applicable to controls for compliant/non-compliant status.
* Ability to provide an independent assessment per control and ensure security controls are implemented correctly; operating as intended; and are producing the desired outcome.
* Designed and documented Compliance logging & auditing strategy, provide analysis and trending of security log data from security devices, provide threat and vulnerability analysis as well as security advisory services.
* Designing and maintaining production-quality Splunk dashboards.
* Co-ordinating pen testing and application security testing audits with PenTest Tools like Metasploit, NMAP, Wireshark and Kali on Linux/Unix operating system.
* Monitoring and remediating daily security alerts generated by end users with the tools like Intel/McAfee SIEM, ForcePoints Websense, and Intel/McAfee EPO 5.X and also responsible for effectiveness of tools and scans, as well as assessing and tracking risk of exposure.
* Respond to security incidents and follow through to resolution, reporting, and lessons learned phases.
* Cisco ASA/Palo alto firewall troubleshooting and configuring policy based on change request, allowing/denying communication between different segment of the network based on requested ports.
* Conduct vulnerability scans to support to our risk/threat/vulnerability management program including resolving risks and the documentation of any residual risks.
* Maintain serviceability of assessment tools with latest software and firmware resulting in zero equipment failure during assessments
* Identifying flaws and weaknesses in information systems that may be exploited to impact the confidentiality, integrity and availability of a system.
* Prioritize vulnerabilities/assets that should be patched during maintenance cycles.
* Analyze vulnerability assessment results, identify remediation strategies and provide timely reports to management for review.
* Configured AWS Identity Access Management (IAM) Group and users for improved login authentication.
* Solution partner product compatibility validation with Cisco UCS servers. Functional and Feature testing of various datacenter and IT solutions and extracting test results for the quarterly marketing press release for Cisco partners.
* Investigate, document, and report on information security issues and emerging trends, Implemented Strategy for Security Compliance and Auditing (HIPAA, SOX). Coordinate with Symantec technical support to resolve product issue escalations to assist in faster resolution and reduce unplanned downtime.
* Used Splunk to analyze Bluecoat, Palo Alto, Juniper firewall, Windows Infrastructure logs. Configured UTM policies in juniper SRX 3600.