Sayed Shah

Sr. Cybersecurity Engineer

Email: sayedaliusa@gmail.com

Phone: +1 401-310-3677

**Professional Summary:**

* Over 8 years of experience in Application Security, DevSecOps, Cloud Security, Threat Modeling, SSO, Application Security Controls and Validation, Risk Assessments, IT Risk Assessments, cryptography, security assurance, Security Architecture & Design, Mobile Application Security,, Regulatory Compliance and Secure Software Development Life Cycle (secureSDLC) and Continuous Integration (CI) and Continuous Delivery (CD) of security scanning, Security Information and Event Management (ArcSight SIEM, Splunk), Penetration Testing and Secure Coding. Cyber security (FISMA) for US Government DoD (DIACAP), Civilian (NIST)
* Responsible for logical and physical database design, implementation, transforming logical data models into physical databases and defining strategies for database implementation, high performance, replication and failover.
* Hands-on experience on Citrix Provisioning Services, XenApp, App-V, Met frame PS, XenDesktop and VMware ESX/ESXi.
* Experience with Project documentation tools & implementing and maintaining network monitoring systems and experience with developing network design documentation and presentations using Visio.
* Supported the development of technical standards and guidance related to access control, governance / risk management, privacy / data protection, configuration management, continuous monitoring and vulnerability management.
* Experience in managing complex routed networks providing technical support, troubleshooting and configuration.
* Configure, maintain and design network security solutions including firewalls (CheckPoint and Cisco ASA), IDS/IPS (CheckPoint and Source Fire), VPN, ACLs, Web Proxy, etc. Cyber Security Forensic (malware analysis/ identifying intelligence-related activity)
* Hands on experience on NGFW Firewall management and UTM solutions (IPS/IDS, DLP, Gateway Antivirus, Antispam, Content Filtering, Application Control). Project management for large cyber security projects utilizing advance methodology (e.g. Six Sigma).
* Developing strategies to enhance overall cyber security program. Maintaining and improving security posture for IT governance.
* Expertise in writing Splunk searches, Splunk Infrastructure and Development expert well-versed with Splunk architecture and design
* Experience converting Palo Alto VPN rules over to the CISCO ASA solution. Migration with both Checkpoint and CISCO ASA VPN experience
* Administrating Carbon Black to do host based monitoring. Created script in Python for calling REST APIs.
* Involved in representation of the system in hierarchy form by defining the components, subcomponents using Python and developed set of library functions over the system based on the user needs. Experience with AWS Cloud Security and architectural technology.
* Apply Malware analysis, including viruses, worms, trojans, botnets, and rootkits using both static and dynamic analysis.
* Skilled finding Cyber Security vulnerabilities and risks in computer networks and resolving vulnerabilities by updating systems accordingly.
* Ensure security compliance with the NIST Risk Management Framework.
* Follow Incident Response Plans to mitigate system breaches, document findings, and perform post-incident analysis to update the Incident Response Plan. Perform Access Control Identity Management, Penetration Testing, Vulnerability
* Experienced with Identity and Access Management using ForgeRock.
* Experience in implementing Enterprise level Identity and Access Management
* Experience in installing and configuring ForgeRock AM stack ( Open AM, OpenID)
* Perform log analysis, intrusion detection/prevention, and incident management as SOC Analyst by reviewing alerts from various SIEM tools.
* Produce reports about Cyber Security events and Vulnerabilities found in vulnerability assessment scans using tools such as Nessus, OpenVAS, Retina CS. Skilled with tools such as Splunk, Nessus, WireShark, IDA Pro and  ArcSight
* Investigate and analyze Cyber Security events found in vulnerability scans and suggest countermeasures to mitigate threats.
* Conduct penetration tests/audits on systems and networks for vulnerabilities by performing Foot printing and Scanning using tools such as Whois Lookup, Path Analyzer Pro, Nmap, Hping3, OpUtils, and Google hacking.
* Skilled collecting network traffic and performing analysis from network devices such as Firewall, IDS/ IPS, Antivirus, Switches, and Router traffic through Log and Event-based on TCP/IP.
* 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 Hands-on designing Active Directories using power shell scripts.
* Configure, maintain and design network security solutions including firewalls (CheckPoint, Cisco ASA and Fortinet), IDS/IPS (Cisco, CheckPoint and Source Fire), VPN, ACLs, Web Proxy, etc. Advanced Persistent Threat (APT)/ Cyber CI (Counterintelligence)
* Hands on experience on Operations and management of Aruba based wireless network providing multiple SSID platform for DoD users
* Work closely with clients Information Assurance analysts to oversee the preparation of a comprehensive and executive and Accreditation (C&A) packages for approval of an Authorization to Operate (ATO); generate, review and update System Security Plan (SSP) against NIST and NIST requirements. Hands-on with Penetration Testing, DAST, SAST and manual ethical hacking.

**Technical Skills**

**Hardware:** Confidential V5K, V10K, i500

**Routers:** Cisco routers Switches: Cisco Switches

**Security Appliances:** PIX, ASA 5500. IPS 4200 & IDS, Access Points: Cisco, Meraki

**IPS/IDS:**McAfee IPS, HP Tipping Point, Cisco IDS, SecureWorks IDS/IPS

**SIEM:**RSA Envision, Arcsight, Splunk security manager, IBM Qradar

**Cloud Security:**AWS, Azure, OpenStack, Docker, Ansible, Chef, Ansible, CI/CD, Terraform

**MSS:**Vulnerability Assessment, Content Filter, Antispam, IDS/IPS Management

**Security Tools:**Splunk ES, McAfee Vulnerability management solutions, Burpsuite, OpenVAS, Nessus, Qualys, SolarWinds, Forescout

**Middleware:** TIBCO EMS, IBM WebSphere MQ, JMS

**Databases:** Oracle, MS SQL Server, Sybase.

**Web Services:** Restful/SOAP, SOA, UDDI, WSDL.

**Work Experience**

**Role: Sr. Cyber Security Engineer**

**Client: Motorola Solutions, Chicago, Illinois. Feb 2022 - Present**

**Responsibilities:**

* Utilized Syslog-NG on Red Hat Linux to pull firewalls, Windows, and DHCP logs.
* Monitored and escalated potential reconnaissance and privilege escalation events on client servers in AWS cloud by analyzing audit logs in ArcSight ESM and Logger. Utilized Windows Event Viewer on Windows Server 2008 to pull security events.
* Utilized HP Tipping Point IPS to monitor potential intrusion events. Utilized WhatsUpGold to monitor critical devices’ health and uptime.
* Utilized McAfee ePO to run reports and checks on end hosts. Utilized McAfee NSM to pull historical data and export PCAPs in Wireshark.
* Utilized Wireshark to analyze DNS and HTTP traffic traces. Imported data sources into Splunk and wrote custom RegEx to parse key fields. Ran searches in Splunk and exported logs as CSV. Mentored junior analysts on not only information security but also on networking concepts, design, and terms. Mentored junior analysts on potential security events’ investigation using ArcSight ESM.
* Reviewed junior analysts’ work and advised them before escalating security events to clients. Briefed management on security events pertaining to clients’ environment during daily morning calls.
* Created weekly activity reports for management regarding security events handled by the SOC. Created SOPs for monitoring the SIEM health and performing packet level analysis. Utilized Remedy ticketing system to update and track incidents, tasks, and work orders
* In - depth knowledge of Mobile Application Security, Application Security Controls and Validation, IT Risk Assessments, Regulatory Compliance and Secure Software Development Life Cycle (secureSDLC) and Continuous Integration (CI) and Continuous Delivery (CD) of security scanning. Hands on experience on Web Application Firewalls and attack mitigation techniques
* Cyber Security Engineer with good experience in Implementation, Administration, Operation and Troubleshooting of enterprise data networks Knowledgeable of penetration testing, vulnerability assessment, threat hunting, and security program development.
* Skilled at designing and implementing cyber security solutions for global petroleum, government and financial organizations that consistently reduce security costs while elevating the security status of the environment.
* Accomplished history with working with various private business and IT organizations to facilitate security architecture in order to further enhance the security stance of the company. Cyber security for critical infrastructure Nuclear, Oil, & Gas (SCADA/NERC CIP)
* Adept at security policies, developing solutions, assessing environments, and interpreting standards that constantly pass the security and regulatory audits. Working knowledge of Cloud Access Security Broker (CASB).
* Successful in initiating six separate security programs which passed all third-party audits and all established laws and regulations.
* Comprehensive background in developing and implementing strategic technology and security road maps aligned with the needs of the business to deliver exceptional security and privacy solutions.
* Ensured Azure Government system was compliant to meet a Fed RAMP 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 Maintained GIT repositories, branches and tags and Experience in Administering GITHUB repository.
* 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).
* Interacted with Cloud Service Provider (CSP) to conduct Incident Response (IR) and Contingency Plan (CP) exercises for Disaster Recovery Plan (DRP) and procedures. Served as the primary SME for RSA SecurID and all multi-factor authentication products including Azure MFA.
* 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 Worked extensively in Configuring, Monitoring Elk, and Extrahop.
* Developed custom SIEM deliverables in Splunk/McAfee/QRadar/ArcSight to meet customer needs in a variety of domains: IT security, financial, IT ops, human resources, physical security, etc. Worked as a PCI-DSS consultant to perform a 3rd party audit.
* Design, development, implementation, tuning and testing of standard and nonstandard content for Mcafee SIEM (Nitro).

**Role: Cyber security Analyst**

**Client: Citizens Financial Group, Providence, Rhode Island. Oct 2019 - Jan 2022**

**Responsibilities:**

* Worked on Cloud Security Products to ensure security of customer from cyber attacks.
* Knowledge of various DDoS attack types (UDP/ICMP Flood, SYN Flood, HTTP Get Flood, TCP Connection Attack, TCP Flag-based Attacks).
* Coordinated internal and external information security compliance activities with respect to AT101 (SOC 2&3), SOX, PCI DSS, HIPAA, Cloud Security Alliance CCM, ISO 27001/27002, ITAR, FedRAMP, and FISMA.
* Identification of phishing attempts, malware detonation, and knowledge of the DHS SOC email analysis toolset and Security Analyst.
* Ensured authorized IA tools were used to perform vulnerability testing and analysis of networks and systems to ensure DoD compliance.
* Using FISMA template to categorize the strength of a network, Reviewing and updating systems security documentation and artifacts such as SSP, ISRA, MOU, SSR, CAP and POA&Ms.
* Analyzed network traffic with ArcSight tools on network traffic, firewall (Source Fire defense center) and AV (McAfee) logs.
* Preparing daily checklist and weekly Infra call report. Deployments of Security patch management through WSUS server. Manage Symantec Antivirus. Create / Delete / Modify User and Group in File Server.
* Good knowledge on GRE tunnel, IP sec tunnel, troubleshooting of different issue of tunnels.
* Experience with Firewall migrations from PIX firewall to Cisco ASA and Juniper SRX firewall appliances.
* Experienced with RSA DLP, as well as Symantec DLP versions 12.5, 14.0, 14.5, and 14.6.
* Provided remote Technical support on implementation of technology using various Juniper Network & Security products and applications and resolve product related issues through research and troubleshooting.
* Involved in configuring and troubleshooting Juniper Firewalls including UTM features like anti-virus, deep inspection (IDP), URL filtering and screening. Responsible for Cisco ASA and Palo Alto configuration and administration of networks.
* Troubleshoot traffic passing managed firewalls via logs and packet captures
* In-depth knowledge of penetration testing for web and mobile (iOS and Android) applications.
* Working knowledge on cloud security engineering and administrating for SaaS, PaaS, and IaaS (including AWS and Azure)
* Aggregate, correlate, and analyze log data from network devices, security devices and other key assets using QRadar. Analysis of various use cases in the Qradar console like Malware, AD related issues. Advanced cyber intrusion analysis/detection/forensic (rootkit, malware, etc.) Worked with global security teams performing application and IT infrastructure security assessments.
* Applied current information assurance technologies to architecture, design, development, evaluation, and integration of systems and networks infrastructure Experience with Security Information and Event Management Tools like Splunk and IBM QRadar
* Worked with Legal and Compliance teams and perform electronic discovery and computer forensics to support investigations
* Maintained up-to-date procedures and documentation to support IT security processes.
* Experience and knowledge of threats, analysis, and remediation efforts in reference to Intrusion Prevention and penetrations
* Experience as a Splunk Engineer configuring, implementing and supporting Splunk Server Infrastructure across Windows, UNIX and Linux environments providing support to Microsoft Active Directory, Microsoft SCCM servers and SQL servers.
* Monitored Security Management Console for Security Operation Centre (SOC) for ensuring confidentiality, Integrity and Availability of Information systems. Symantec DLP and RSA DLP architecture and implementation for enterprise level companies.
* Experience with Risk assessment using Industry standards like NIST Rev5, HIPPA, PCI/DSS and develop Security policy as per these standards. projects that installed, deployed and/or maintained multiple security solutions for security tools such as Nexpose Rapid 7, Comodo, Qualys, threat stop Provide IT Governance, Risk, and Compliance (GRC) service to fulfil client requirements.
* 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.

**Role: IT Security Analyst**

**Client: CyberArk Software, Inc, Newton, Massachusetts. July 2017 - Sept 2019**

**Responsibilities:**

* Knowledge of various DDoS attack types (UDP/ICMP Flood, SYN Flood, HTTP Get Flood, TCP Connection Attack, TCP Flag-based Attacks)
* Created a new team to monitor three aspects of RSA DLP: Data in Motion (Network), Data at Rest (Datacenter), and Data at Endpoint.
* Creation, development, and/or restructuring of DLP programs from conception to fully perational state. Worked on DDOS mitigation and have good idea on different kind flood attacks. Good knowledge on GRE tunnel, IP sec tunnel, troubleshooting of different issue of tunnels. Experience with Firewall migrations from PIX firewall to Cisco ASA and Juniper SRX firewall appliances.
* Provided remote Technical support on implementation of technology using various Juniper Network & Security products and applications and resolve product related issues through research and troubleshooting.
* Involved in configuring and troubleshooting Juniper Firewalls including UTM features like anti-virus, deep inspection (IDP), URL filtering and screening. Responsible for Cisco ASA and Palo Alto configuration and administration of networks.
* 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. Assist penetration testing and investigation.
* Consulted with business and technology partners to create and provide security recommendations and best practices.
* Assisted CSO with completion of established goals, objectives, and streamlining of internal office procedures.
* Deployed the following Azure services to enable IT Security and IT Operations to move applications into the Azure cloud environment by allowing for monitoring and alerting: Azure Operations Management Suite (OMS), Service Map, Network Watcher, and Wire Data
* Conducted onsite penetration tests from an insider threat perspective. Performed host, network, and web application penetration tests.
* Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk, Solutionary, LogRhythm, SCCM, Altiris, LanDesk, BigFix, and McAfee/Symantec.
* Configuring Virtual Chassis for Juniper switches EX-4200, Firewalls SRX-210 Troubleshoot traffic passing managed firewalls via logs and packet captures Involved as Platform Engineer for Sourcefire including all 4.10 and NG and NGFW
* Integrated web application delivery controller(ADC). Involved in a team responsible for Network security management by implementing and managing NGFW systems. Virtual Private Networks on Cisco ASAs with AnyConnect, Cisco ISE for authentication, as well as site to site VPN Implemented new Cisco ASA's, installed the framework for Cisco ACI and implemented new F5 LTM's and GTM's.
* Creating, implementing and testing Citrix NetScaler ADC (Application Delivery Controller) responder.
* Managed multiple complex security implementations such as evaluating and adopting security Baseline standards and a Rapid7 Nexpose to Service Now integration to automate the reporting of vulnerabilities.
* Worked on Converting the Partner IPSEC VPN from one Data Center to Another Data Center
* 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. Experienced with tools like Metasploit/Qualys/Network forensics technologies
* 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.
* Monitor, analyze and 0respond to network incidents and events. Participate in disaster recovery implementation and testing under NIST framework, HIPPA, & HITECH standards. Used Microsoft Azure Security center to monitor the cloud environment.
* Developed approaches for industry-specific threat analyses, application-specific penetration tests and the generation of vulnerability reports. Assesses a residual risk rating for the vendor based upon their control environment
* Work with the network team to architecture Azure and AWS VPN, AWS Direct Connect, and Azure Express Route connections
* Providing proper remedy to fix vulnerability in the client network after analysing security incident queries alerted by ArcSight Performing Vulnerability Assessments and taking the required counter actions and measurements to ensure the security of the IT infrastructure / systems. Experience implementing/architecting cloud-based Active Directory solutions for Azure and AWS

**Role: Jr. Analyst**

**Client: A10 Networks, San Jose, California. Aug 2015 - June 2017**

**Responsibilities:**

* Analysis and documentation of network & information security requirements and define security policy for enterprise client and business critical servers. Implementation of Symantec Mail Security for SMTP and Symantec Endpoint Protection.
* Perform daily duties supporting and trouble-shooting digital rights management on a Windows and Linux Platform, while defining and implementing patching Build and operate a security & awareness program relating to vendor risk management program
* Performing system auditing using audit reduction tools; following up on audit findings; maintaining authorization documents; and supporting the local Information Systems Security Manager (ISSM) as needed to maintain system authorization.
* Respond to inbound security monitoring alerts, emails, and inquiries that arose from various monitoring tools that included Symantec DLP.
* Performed application security and penetration testing using IBM Appscan.
* Perform vendor risk assessments as assigned. Work with vendors and business owners to gather documentation and develop vendor remediation plans. Worked on AWS designing and followed Info security compliance related guidelines.
* Addressed critical areas of potential information security risks and opportunities with gap analysis for Data protection, Cloud Security and Data Classification and handling of tools (Trend Micro and IBM Qradar).
* Review and updated System Security Plan (NIST SP ), Risk Assessment (NIST SP ), and Security Assessment Report (NIST SP A).
* Reducing Proof point Digital Risk to defend impersonation of the brand to harm current market.
* 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.
* Co-ordinating pen testing and application security testing audits with PenTest Tools like Metasploit, NMAP, Wireshark and Kali on Linux/Unix operating system.
* Modified internal infrastructure by adding switches to support server farms and added servers to existing DMZ environments to support new and existing application platforms. Configured switches with port security and 802.1 xs for enhancing customer's security.
* Validate existing infrastructure and recommend new network designs. Created scripts to monitor CPU/Memory on various low end routers in the network. Configuring and troubleshooting multi-customer network environment.
* Involved in network monitoring, alarm notification and acknowledgement.
* Implementing new/changing existing data networks for various projects as per the requirement.
* Installed and maintained local printer as well as network printers
* Configuration, installation and support of equipment in a MS Environment to terms of client proposals.
* Installation, configuration and administration of Asterisk based VOIP Telephony
* Troubleshoot and resolve computer/network issues by providing both on-site and remote support.
* Maintaining software applications, operating systems Win2K, Win XP, Win2007, and Linux.
* Responding to inquiries from staff, administrators, service providers, site personnel and outside vendors and etc. to provide technical assistance and support. Supervising administration of systems and servers to ensure availability of services to authorized users.
* User administration, setup, maintaining system and verifying peripherals are working properly.
* Quickly arrange repair in occasion of hardware failure and Monitor system performance
* Experience using DAST tools to detect potential vulnerabilities such as HP Webinspect, SolarWinds, Zap, Burp, Tenable, Splunk, Alertlogic, Symantec Endpoint Protection, Zscaler, McAfee security, Portswigger, Fiddler, Wireshark, Nmap, JIRA, Sonatype, Coverity. Experience in Palo Alto Networks and Firewall. Experience in maintaining local and remote networks.
* Lead the design, implementation, and migration of enterprise infrastructure and application services to software defined networks. Experience in Palo alto networks and firewall. Configure and manage AWS/Azure cloud infrastructure.
* Develops and leads procedure for testing disaster recovery plan. Provides help-desk-style assistance.
* Administered MS Windows Server, Red Hat Linux Server, and Network/Security Administration.
* Using tools including but not limited to Kali Linux, Burp Suite professional, Metasploit, IDA pro etc.
* Malware Analysis - full spectrum analysis of malicious code both dynamically and statically using tools such as Wireshark, RegShot, Process Monitoring tools, and debugging tools such as IDA pro and Olly debugger etc.
* Developed predictions about cyber attackers and their activities based on previous malicious attempts
* Working in SOC to keep an active defense against various cyber-attacks while working with red team.
* Static Code analysis using Valgrind, Flaw finder and manually checking the code flow
* Working with red team in SOC to apply security awareness to Cyber Kill Chain management as well as using moving target defense approach.