**Mustafa Shaik Sr. Cyber Security Analyst**

**mustafashaik.now@gmail.com**

980-494-9234

**SUMMARY:**

Overall 9+ years of experience as Cyber Security Engineer and Vulnerability Management Engineer.

* Experience with Risk Assessment on systems, applications, and Active Directory.
* Experience with Windows/Linux OS, Database Policy Compliance, and configuration with CIS.
* Experience with IT - Governance (GRC) risk tool Digital Manager 360 (Modulo) and reporting tool Nexpose.
* I have good experience in Vulnerability Scanner Nexpose and Insight VM dashboard.
* I seek to utilize these skills in improving the security posture of information systems and networks by detecting threats and vulnerabilities in target systems, and applications by conducting systems, network testing.
* Responsible for managing all aspects of the Vulnerability Risk Management Program including vulnerability identification, analysis, remediation coordination and reporting.
* Experience with VM identification, analysis, metrics, as well as processes enabling proper governance, risk and compliance (GRC).
* Progressive experience in Enterprise Vulnerability Management, Risk Assessment, penetration testing, generating reports, SQL Injection XSS and major hacking protection techniques.
* Experience in testing using various tools like Burp Suite, DirBuster, NMap, OpenVAS, Nexpose, Nessus, HP Fortify, HP Web Inspect, Confidential AppScan enterprise, Kali Linux, Metasploit and Jira. knowledge on OWASP Top 10 based Vulnerability assessment of web applications.
* Coordinate with dev team to report vulnerabilities by explaining the exploitation and the impact of the issue Reporting the identified issues in the industry standard framework.
* Experience with Security Risk Management with TCP-based networking.
* Domain knowledge in Retail, Banking and Financial Services, Health Care.
* Knowledge in detecting vulnerabilities over authentication, authorization, input validation, session management.
* Involved in Security Development Life Cycle (SDLC) to ensure security controls are in place.
* Having good experience SAST and DAST applications using different tools HP Fortify and Confidential AppScan. Capable of identifying flaws like Security Misconfiguration, Insecure direct object reference, Sensitive data Exposure, Functional level access control and Invalidated redirects.
* Ability to develop and maintain metrics and reports on vulnerability findings and remediation compliance.
* Knowledge on STIG Validation in support of DISA, CIS and proactive vulnerability detection.
* Having good Knowledge on Jira, Root Kit, IP Spoofing, Virtual Box, SELinux, Software Hardening concepts and SIEM.
* Good Knowledge of HTTP, HTTPS, Web application firewalls, checking logs, SSL, and TLS.
* Good knowledge of SQL and programming skills in Java. Experience with Windows and Linux environments.
* Vulnerability Assessment includes analysis of bugs in various applications by using manual and Automation tools. Knowledge of network security such as Firewalls, TCP/IP, IDS/IPS, Routing Active Directory and IOS devices.
* Good team player and ability to learn concepts effectively and efficiently.
* Ability to work in large and small teams as well as independently.

**TECHNICAL SKILLS:**

* SIEM : Splunk, IBM Qradar, Google Chronicle
* IDS/IPS : Snort, Cisco Meraki
* EDR / EPP : Sentinel One, Carbon Black Defense, Sophos
* Cloud Security : AWS Guard Duty & Inspector, MS Defender
* Threat intelligence : Burp Suite, OpenVAS, Qualys guard & Kali Linux tools
* NGFW/ WAF / Firewall : Palo Alto, Imperva, Checkpoint, PaloAlto
* WAF : A10, Mod security, Wapples
* Network Analysis : Wireshark, Bro/Zeek
* VA/PT tools : Burp Suite, OpenVAS, Qualys guard & Kali Linux tools.
* Log Management : Syslog, Splunk Cloud & IDM, ELK/EFK Stack
* Monitoring tools : Zabbix, Ops Ramp
* Programming Language: Python, C#, PowerShell
* Scripting Languages : PHP, HTML, CSS,

**Education:**

Bachelors in computers, 2012

**WORK EXPERIENCE:**

**Bank of America, Raleigh, NC Jan 2019 to Present**

**Sr. Cyber Security Engineer/Analyst**

**Responsibilities:**

* + Experience with tools such as Rapid7 Nexpose and InsightVM vulnerability scanner.
  + Generate the reports daily and execute the daily tasks. Managing and adapting the scan schedule.
  + Managing permissions and access to the product. Performing authenticated and unauthenticated vulnerability scanning.
  + Troubleshooting and debugging scans.
  + Assisting teams with vulnerability resolution, including aiding researching vulnerabilities solutions, and addressing false positives to reduce system workloads, performing confirmation scans when appropriate, meeting regularly with remediation team, and building reports to provide teams with necessary data. Assisting teams with tracking remediation approaches within InsightVM or Excel.
  + Review and advise on existing reports and suggest reports that would solve current business use cases as well as factor the relevant metrics to track Vulnerability Management program.
  + Experience with vulnerability management metrics as per Organization standards.
  + Experience with Firewall Rule Requests (Ports, Protocols and Services)
  + Handled Baseline Configurations, vulnerability exceptions and Compliance exceptions. Update, create and adjust custom policies, standards, and procedures. Manages Policy Compliance scans to configure the settings.
  + Design, Configure and adjust Vulnerability and Compliance scanning operation.
  + Assist with routine compliance and audit functions to ensure regulatory scanning requirements are satisfied.
  + Perform vulnerability, configuration, and compliance scan with Nexpose to detect deficiencies and validate compliance of information systems configuration with organization's policies and standards such as Center for Internet Security (CIS) Benchmarks.
  + Work closely with Threat Intelligence and Incident Response teams to proactively and reactively identify IOCs and additional content needed for hunting and response.
  + Create and maintain SLAs and metrics for Cyber Threat Hunting and content development.
  + Experience in a Threat Hunting or Security Analysis role.
  + Analyze vulnerabilities to determine remediation measures and rule out false positive using resources such as National Vulnerability Database (NVD), US-CERT and CIS
  + Develop Vulnerability Assessment Report (VAR) to document findings and recommend remediation measures Risk management framework knowledge /Risk assessments security awareness.
  + Brief System Administrators on the vulnerability report and the recommended remediation
  + Assist in the planning of remediation strategies. Work with client to provide advice Remediation, Scanning and projects.
  + Worked on setting up Data Dog on end to end setup.
  + Also implemented data dog SAAS product end to end.
  + Created data dog dashboards, tagging and deployed data dog agents on various landscape technologies.
  + Coordinate with team members to provide guidance related to requirements.
  + Experience with SAI Digital Manager 360 (Modulo) to do the risk assessment of systems and applications. Assist in the implementation of Risk Management Framework (RMF), through the required government policy and participate fully in documentation process.
  + Performed security analyses to validate established risk on systems and applications.
  + Develop Authorize to Operate (ATO) document to amend the deficiency is system operation as required.
  + Document Assessment result and Authorized technical activities and coordinate system security plan (SSP)
  + Periodically conduct a complete review of each system audits and monitor for corrective action.
  + Strong knowledge of threats and vulnerabilities associated with cloud and on-premises network security.
  + Experience using DAST tools to detect potential vulnerabilities such as Qualys, ZAP, Burp, Tenable, Wireshark, Nmap, JIRA. Experience in Palo Alto Networks, Panorama and Firewall. Experience in maintaining local and remote networks.
  + Developed threat & vulnerability management policies, procedures & manage SIEM systems.
  + Coordinating and conducting event collection, log management, event management, compliance automation, and identity monitoring activities using the QRadar SIEM
  + Research, analyze and understand log sources utilized for the purpose of security monitoring, particularly security and networking devices (such as firewalls, routers, anti-virus products, proxies, and operating systems)
  + Creates and develops correlation and detection rules, utilizing Regex, within QRadar SIEM to support alerting capabilities within the Threat Management Center
  + Creation of technically detailed reports on the status of the SIEM to include metrics on items such as number of loggings sources, log collection rate, and server performance.
  + Examined alerts from QRadar security monitoring tools, monitored, investigated, and reported incidents of suspicious activity. Analyzed security breaches to determine the root cause of problems.
  + Identified potential risks, such as virus and malware attacks, and hacking, conducted initial research based on analytic experienced.
  + Assisted with implementation of counter measures, as well as mitigating controls. Provided and developed the forensic capability to enhance response to the investigation.
  + Assist with designing and documenting work processes within the SOC and act as a point of escalation for other Engineers (Associate SIEM Engineer & SIEM Engineer) and provide guidance and mentoring.

**FHL Bank, San Francisco, CA July 2016 – Dec 2018**

**Sr. Cyber Security Engineer**

**Responsibilities:**

* Experienced with DLP, Bluecoat web sense, Proofpoint, Trend Micro, and IBM QRadar Enterprise SIEM security tools to monitor network environment.
* Worked on tools like Information security and Group Policy, Symantec Data Loss Prevention, Symantec End- Point Protection Manager, Symantec Endpoint Encryption, Windows Server Update service, Bluecoat Proxy, Syslog, GFI.
* Conduct network and system **vulnerability assessments** using **Rapid 7 Nexpose** and documentation of corrective/remediation actions.
* Experience using Rapid 7 Insight VM
* Experienced primary Voltage secure data encryption engineer heading up the International Project encryption servers worldwide.
* Oversee Vulnerability assessment/penetration testing of scoped systems and applications to identify system vulnerabilities.
* Application support for tripwire, research and understand all aspects of tripwire and troubleshooting as well as find other ways to automate practices. would help other teams in cyber security as well for any projects dealing with Nessus tools vulnerability management, risk, and compliance in NERC standards.
* Lead a team of cloud security engineers in various areas of expertise to execute complex solutions to meet delivery timelines.
* Recognize, adopt, utilize, and teach best practices in cloud security engineering.
* Internal Network Vulnerability Assessments to enhance the Information Security culture of an organization through identifying, analyzing, and reporting the gaps which may be used to threaten the CIA of information.
* Converting existing AWS infrastructure to server less deployed via Terraform or AWS Cloud formation.
* Frameworks used ISO 27001 ISMS, PCI DSS, SSAE16, OWASP, SANS, Forcepoint.
* Monitored and researched Cyber Threats with a direct & indirect impact to the organization internally.
* Experience on Nessus VA and Burp Suite PT with Implement RSA SecurID
* Multi model Consulting on different frameworks & standards like ITIL, COBIT, SDI, CMMI & ISO 2000, ISO 9001.
* Security Consultant specializing in Data Loss Prevention and large infrastructure encryption.
* Security Engineer for Proof Point Email Gateway Security.
* Develop reference architectures and proof of concept implementations of cloud security environments.
* Responsible for architecting, implementing, and supporting cloud-based infrastructure and its solutions.
* Manage all repeated threats to all systems and perform vulnerability tests.
* Responsible for the design, development, and implementation of new and innovative solutions to protect lucid sensitive data and strengthen data protection capabilities.
* Used Splunk Deployment Server to manage Splunk instances and analyzed security-based events, risks & reporting.
* Experienced with Handling Cloud environments (AWS and Azure).
* Simplified knowledge sharing by creating and maintaining detailed and comprehensive documentation and necessary diagrams.
* Managing the enterprise infrastructure of the System Security team, such as configuration of File Integrity Monitoring systems, Data Loss Prevention (DLP) toolsets, enterprise Antivirus solutions, and endpoint encryption.
* Assisted internal users of Splunk in designing & maintaining production-quality dashboard, assisted team to understand the use case of business and provided technical services to projects, user requests & data queries.
* Performed HITRUST CSF self-risk assessment and scoring of organizations Policies, Procedures, Implementation, and in-scope systems in preparation for HITRUST CSF readiness validated assessment.
* Coordinated with multiple departments to collect HITRUST CSF request of Policies, Procedures, Implementation screen shots, generated reports, and inventories for on-site HITRUST CSF assessors.
* Reviewed HITRUST CSF final validated assessment report and continually executed implementation of corrective action plans (CAPs) to address HITRUST CSF GAPs identified.
* Monitor the audit findings are followed up by the system owners for closure of any non-conformances. Following up with secondary audits to ensure the work is completed.
* Explain to all levels of the organization the purpose of an Information Security Management System (ISMS) and explain the processes involved in establishing, implementing, operating, and monitoring, reviewing, and improving ISMS as defined in ISO27001.
* Responsible for technical evaluation, testing and upgrading of quality systems used for organizations ISMS initiatives.

**HSBC Financial, Hyderabad, India April 2012 – June 2015**

**Cyber Security Analyst**

**Responsibilities:**

* Experience with many of the following technologies/roles: Privileged Account Management, Two-Factor Authentication, Web filtering, Web Application Firewalls, Virtualized computing environments, Encryption-at-rest and encryption-in-transit, Vulnerability Management.
* Installation and configuration of networks and network devices such as web application firewalls, network firewalls, switches, checkpoint firewall, blue coat proxy and routers.
* Network Security configuration, audit, and management of Windows servers. Installation, configuration, audit, and management of security tools.
* Security configuration, audit, and management of applications and databases. Leading security incident investigations, including basic forensic analysis and reporting. Deploying, automating, maintaining and managing AWS cloud-based production system, to ensure the availability, performance, scalability and security of production systems.
* Maintenance and monitoring of network and host intrusion detection and prevention technologies. Implementing security controls. Experience with using a broad range of AWS technologies (e.g. EC2, RDS, ELB, EBD, S3, VPC, Glacier, IAM, CloudWatch, KMS) to develop and maintain an Amazon AWS based cloud solution, with an emphasis on best practice cloud security.
* Implemented physical and procedural safeguards for information resources within the facility. Communicate effectively with senior management, peers, staff, and customers both inside and outside the corporation.
* Administered access to information resources and makes provisions for timely detection, reporting, and analysis of actual and attempted unauthorized access to information resources.
* Proposed and assisted with the acquisition of security hardware/software. Develops and maintains access control rules. Experience with VOIP systems.
* Maintains user lists, passwords, encryption keys, and other authentication and security-related information and databases.
* 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 procedures for testing disaster recovery plans. Provides help-desk-style assistance.
* Administered MS Windows Server, Red Hat Linux Server, and Network/Security Administration.