Mahesh Reddy

###### Senior Cyber Security Engineer

###### [mahesh.reddy3318@gmail.com](mailto:mahesh.reddy3318@gmail.com) Phone: **817-382-9752**

**Professional Summary:**

* As an IT Security Professional with over 8 years of specialized experience in areas like Cyber Security, Risk Management, SIEM, and Penetration Testing, my forte lies in Web Application and Thick Client Security Assessments, along with generating insightful reports using various tools.
* Proficient in developing IAM strategies that align with organizational security policies and norms.
* Skilled in deploying and configuring Palo Alto Firewalls, notably PA3200, PA5220, and cloud-based firewalls.
* In-depth knowledge of security paradigms, including access management, perimeter security controls, URL filtering, DNS security, and malware protection.
* Demonstrated ability to collaborate with business partners and internal teams to ensure secure network integrations in line with organizational guidelines. Skilled in automating security tasks and log data analysis using scripting languages like Python and Bash.
* Extensively involved in Network Security assessments utilizing Qualys Guard.
* Well-versed in the setup and administration of Sailpoint IdentityIQ, with an emphasis on application onboarding, troubleshooting, and lifecycle management.
* A key contributor to the optimization of security processes, aiding in the design and rollout of effective security solutions.
* Assisted in the formation and implementation of security controls for FedRAMP policies for I.T. systems and major applications in AWS, Azure, and Sales Force (PaaS, SaaS. IaaS).
* Capable of conducting compliance assessments, with a solid understanding of frameworks like PCI-DSS, HIPAA, and GDPR.
* Familiar with container security best practices, including the utilization of Docker and Kubernetes.
* Strong background in Firewall configurations, IDS policy setups, and Linux system administration.
* Implemented and monitored security controls for I.T. systems and major applications in the cloud environment for Azure, AWS, and Sales Force (IaaS, SaaS, PaaS) using FedRAMP guidelines.
* Knowledgeable in cloud security architecture and adept at implementing security best practices in cloud-based systems.
* Skilled in dissecting network traffic using tools such as Wireshark and Snort to pinpoint and counteract security risks.
* Demonstrated proficiency in executing access reviews and certifications, ensuring that users possess only the necessary permissions, thereby enhancing the organization's security posture.
* Proficient in IT Security tools such as **F5 ASM, ShapeSecurity, WAF, and deep packet inspection techniques.**
* Strong knowledge of **application layer security, HTTP, Python, TCP/IP, SSL, DNS, and cybersecurity best practices.**
* Comprehensive understanding of TCP/IP Stack and UNIX-based operating systems.
* Experienced in leveraging multi-factor authentication (MFA) solutions to fortify access controls, adding an extra layer of security against unauthorized access to sensitive systems and data.
* Hands-on experience with Selenium Grid for parallel testing, thereby speeding up test execution
* Comprehensive experience in integrating IAM tools with a diverse range of business applications, platforms, and databases.
* Effective in incident response with established protocols, and capable of scrutinizing log data for potential security incidents.
* Experience in GCP Dataproc, GCS, Cloud functions, BigQuery, Azure Data Factory DataBricks.
* Expertise in the Software Development Lifecycle (SDLC) and well-acquainted with methodologies like CWE, OWASP Top 10, and WASC Threat Classification 2.0.
* Proficient in identifying mobile device and application vulnerabilities through various frameworks.
* Skilled in web technologies like **HTTP, HTML, and CSS, and knowledgeable about regulatory standards such as PCI DSS, SOX, and HIPAA.**
* Versatile in identifying application vulnerabilities like **XSS, SQL Injection, CSRF,** along with weaknesses in cryptography and authentication mechanisms.
* Served as the main point of contact for security matters concerning infrastructure, applications, and databases.
* Adept at implementing and managing role-based access control (RBAC) across various systems, contributing to both compliance and streamlined access management within the organization.
* Equipped with expertise in CyberArk Privileged Access Management, focusing on safe creation, platform and account onboarding, and system-wide compliance.
* Excellent in team collaboration and a fast learner of fundamental concepts.
* Conducted client presentations to highlight the security offerings of the firm and proficient in scripting languages like Python and PowerShell.
* Familiar with identity and access management solutions such as Active Directory, LDAP, and SSO technologies.
* Well-versed in log searching tools like Splunk, regular expressions, and natural language query formulation, coupled with system vulnerability identification.
* Experienced in Secure SDLC practices and manual & tool-based Source Code Analysis on web applications.
* Knowledgeable in different security testing approaches including black-box, white-box, and gray-box testing, coupled with threat modeling and risk assessment expertise.
* Skilled in automating user provisioning and de-provisioning workflows, reducing manual errors and enhancing operational efficiency.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| * L0phcrack, SMB, IBM AppScan, Nessus, IBM Rational AppScan, Burp Suite Pro. | * Wireshark, Ettercap, Cain& Abel, Maltego |
| * Nmap/Nmap Scripting Engine (NSE), Netcat, Nessus, OpenVAS | * Metasploit Framework Languages & Databases HTML |
| * HP Fortify, HP Fortify, LDAP | * Hydra |
| * Google Hacking | * Manual SQL Injection, Manual Cross Site Scripting(XSS), Cross site request forgery(CSRF), SQLmap. |
| * Nikto | * Python, JavaScript, SQL, SQLmap |
| * Rainbow Crack | * Arc Sight Penetration Testing Wireshark, Paros, Pyrit. |
| * Burp Suite | * Vega, NMAP |
| * Aircrack-NG Suite and Kismet. | * QualysGuard Application Security Websense, OpenVAS |
| * Acunetix | * DNS, PHP, HPWeb Inspect, John the Ripper |
| * OllyDbg, WinDBbg. | * Metasploit, Social Engineering Toolkit (SET). |

**SECURITY SKILLS/TOOLS:**

* **Network Enumeration:** Maltego, Google Hacking, DNS, SMB, LDAP, AWS
* **IAM Tools:** Okta, Microsoft Azure Active Directory, OneLogin, Ping Identity, SailPoint Identity Now, ForgeRock, CyberArk Privileged Access Management.
* **Port/Vulnerability Scanning:** Nmap/Nmap Scripting Engine (NSE), Netcat, Nessus, OpenVAS
* **Sniffing/Man-in-the-Middle:** Wireshark, Ettercap, Cain & Abel
* **Web Application Vulnerability Scanning:** Nessus, OpenVAS, Vega, HP Fortify, Selenium, Acunetix, HP Web inspect, IBM AppScan, Burp Suite Pro.
* **Server/Client-Side Exploitation:** Metasploit, Social Engineering Toolkit (SET).
* **Web Application:** Manual SQL Injection, Manual Cross Site Scripting (XSS), Cross site request forgery (CSRF), SQLmap.
* **Networks Cisco/Juniper/Palo Alto, AWS Services:** EC2, Lambda, CloudWatch, CloudFormation.
* **Debuggers:** OllyDbg, WinDBbg.
* **Wireless:** Aircrack-NG Suite and Kismet.
* **Vulnerability Testing:** Tenable Nessus, NMAP, OpenVAS, QualysGuard
* **Penetration Testing:** Wireshark, Metasploit Framework
* **Languages & Databases:** HTML, JavaScript, C, C++ PHP, SQL, Python

**PROFESSIONAL SUMMARY**

**Commonwealth Care Alliance, NJ Mar 2022 – Present**

**Cyber Security Engineer**

* Assessed the security configurations of partner firewalls, identifying and addressing potential vulnerabilities and risks.
* Maintained and modified hardware and software components, content and documentation. Azure O365 Advance Threat Protection.
* Played a pivotal role in the deployment and configuration of Palo Alto Firewalls, ensuring secure connections between partner networks and the core infrastructure.
* Designed and implemented dedicated firewalls for enhanced internet connectivity and service hosting.
* Reduced dependencies on internal network resources and improved the resiliency of critical SQL server and web applications by leading a project to plan, develop, and implement the move to Azure, including transfer of development systems, operations, and data.
* Extensive experience in Cloud and On-Prem (Hybrid) environment. AWS & Azure Cloud security experience.
* Worked with the Director of VDOT to planed, designed and implement new technologies.
* Managed VDOT network to facilitate PCI compliance efforts for better product delivery to customers.
* Addressed and resolved Palo Alto firewall-related incidents, ensuring minimal disruption to network operations.
* Employ McAfee ePO to manage client endpoints, taking care of agent management, VirusScan Enterprise (VSE), and task assignments.
* Prioritize vulnerabilities in applications based on established frameworks like OWASP Top 10 and SANS 25, categorizing them as critical, high, medium, or low.
* Integrate customer input into the agile development cycle, working hand-in-hand with internal development teams.
* Design LAN and WAN network for the future to scale as VDOT continues to grow
* Participate in VDOT wide initiatives such DUO security two factor implementation.
* Leverage the OWASP Top Ten, WASC, and CWE frameworks to enhance security testing approaches.
* Extensive experience in Managing Qradar Use - cases, administering Qradar, Defender ATP, O365 ATP, Azure AD and other security application which includes Microsoft, Cisco, Palo-Alto, ITSM Tools, Symantec and various other products.
* Utilize an assortment of tools for security management and monitoring, including SIEM, IDS/IPS, McAfee endpoint encryption, DLP, and malware analysis platforms.
* Respond promptly to security incidents affecting systems or networks, with a focus on technologies from Cisco, Juniper, Palo Alto, and AWS services like EC2 and Lambda.
* Conduct in-depth evaluations of hardware and software against NIST 800-53 controls, identifying areas for security enhancement.
* Implement NIST 800-53 controls into software projects from the ground up, coordinating with development teams.
* Project manager for VDOT network upgrade which included a Request for Proposal, vendor selection, equipment selection.and Bill of Materials (BOM) creation.
* Administered and managed IAM solutions using SailPoint IdentityNow and Microsoft Azure AD, including user provisioning, de-provisioning, and role-based access control.
* Work collaboratively with various departments to examine security vulnerabilities and develop remediation plans in line with NIST 800-53 guidelines.
* Utilize network surveillance tools to monitor network stability and employ protocol analyzers to troubleshoot service disruptions.
* Produce and share comprehensive security vulnerability reports with both internal and external parties.
* Extensive experience on deploying compute and storage Azure cloud.
* Leverage Kali Linux and tools like DirBuster and Nessus for vulnerability assessments.
* Utilize Dynamic Application Security Testing (DAST) tools, such as IBM AppScan and Burp Suite Pro, to discover vulnerabilities beyond the application code.
* Stay abreast of the latest trends and advisories in cybersecurity, regularly communicating updates to increase organization-wide awareness.
* Worked closely with IT compliance teams to ensure IAM processes meet PCI-DSS, HIPAA, and GDPR requirements.
* Integrate cybersecurity best practices into the design, development, testing, and deployment phases of software projects.
* Assist leadership in shaping the organization's future cybersecurity strategy and initiatives.
* Schedule and execute regular threat assessments to proactively identify and address security vulnerabilities.
* Utilize the ComDroid tool to identify communication vulnerabilities in mobile applications.
* Involve yourself in the architecture, documentation, and enhancement of security monitoring systems, including the configuration of dashboards and metrics views.Assist developers in remediating issues with security assessments.

**Northern Trust Corporation, IL Jan 2020 – Feb 2022**

**Cyber Security Engineer**

* Evaluate system vulnerabilities by carrying out assessments with IBM AppScan, subsequently formulating security measures and remediation strategies.
* Collaborate with business units to review solution architectures from a security standpoint, aiming to preemptively tackle security issues at the project's onset.
* Employ the CWE/CVSS framework for scoring vulnerabilities and classifying them by their level of criticality.
* Engage in the development and enhancement of security monitoring systems, focusing on dashboard configuration, alert responses, and threat analytics.
* Incorporate established security frameworks like OWASP Top Ten, WASC, and CWEs into security testing routines.
* Integrated CyberArk Privileged Access Management for secure handling and rotation of sensitive credentials.
* Configured private and public facing Azure load balancers etc.
* Analyze source code in Python and .Net to pinpoint security flaws and recommend remedial actions to developers.
* Initiate kickoff meetings with application teams to gain insights into security requirements, app functionality, and architectural elements.
* Lead efforts to set cloud security standards, collaborating with app development teams to enforce robust cloud solutions.
* Led the secure integration of business partner remote sites and data centers, ensuring adherence to established security guidelines and policies.
* Collaborated with business partner network/security teams to drive network integrations using next-gen security controls.
* Reviewed and assessed the security posture of partners through a detailed examination of firewall security policies, identifying high-risk flows and providing remediation advice.Offer prompt responses to security incidents affecting systems and networks.
* Assist development teams in addressing security issues in line with OWASP guidelines.
* Implemented Single Sign-On (SSO) and Multi-Factor Authentication (MFA) solutions using Okta and Ping Identity.
* Extensive experience implementing software throughout the SDLC process, deep hands-on experience of networking, migration and implementation in Azure
* Develop a comprehensive threat assessment plan to proactively identify and address security vulnerabilities.
* Excellent experience with Red hat Linux Server, macOS Server, and Microsoft Windows Server, MS Active Directory, GPO and AWS/Azure Cloud environments with the capability and passion to quickly learn new tools.
* Conduct web application scans, threat modeling, and secure code reviews to identify security risks in applications.
* Collaborate with app development teams to help them understand identified vulnerabilities and suggest remedial actions.
* Manually review Java/.Net application vulnerabilities reported by AppScan to eliminate false positives and categorize issues based on their severity.
* Stay updated on current security trends and advisories, regularly disseminating this information to enhance company-wide security awareness.
* Utilize Dynamic Application Security Testing (DAST) tools like IBM AppScan and Burp Suite Pro for in-depth penetration testing.
* Established dedicated firewalls for internet connectivity and hosting services, ensuring robust security.
* Managed and resolved incidents related to Palo Alto firewalls, providing support during cutover phases.
* Administered AzureAD for providing O365 and Defender ATP permissions.
* Migrating virtual environments VMWare to Azure cloud using ASR
* Upgraded PAN OS on Palo Alto Firewalls and Panoramas, ensuring systems are up-to-date with the latest security patches.
* Northern Trust Corporation, IL (Jan 2020 – Feb 2022) - Cyber Security Engineer:
* Led initiatives to securely integrate partner networks, focusing on compliance with established security standards and guidelines.
* Worked in close collaboration with partner network/security teams, leveraging advanced security controls for seamless integrations.
* Report conclusive findings, including successful exploits and recommendations for security improvements.
* Coordinate with security and engineering teams to address security vulnerabilities as outlined in the Plan of Actions and Milestones (POA&M).
* Provide end-user training focused on security awareness and compliance with NIST 800-53 controls.
* Assist leadership in shaping the future direction of the organization's Information Security Management System.
* Employ Static Application Security Testing (SAST) tools like HP Fortify and SonarQube to evaluate software vulnerabilities prior to deployment.
* Use the ComDroid tool to identify communication vulnerabilities in mobile applications.

**Aflac Insurance, GA Nov 2018 – Dec 2019**

**Cyber Security Engineer**

* Evaluated client application vulnerabilities through proactive assessment techniques, significantly reducing audit issues.
* Administered vulnerability assessment tools like Nexpose and Nessus for efficient security evaluations.
* Engaged with design teams in the early stages of the Software Development Life Cycle (SDLC) to convey security requirements, thereby minimizing post-penetration testing rework.
* Employed Dynamic Application Security Testing (DAST) tools like IBM AppScan and Burp Suite Pro to probe live applications for vulnerabilities, including those in third-party interfaces.
* Performed security analyses to pinpoint vulnerabilities in key derivation functions, subsequently preparing comprehensive assessment reports with mitigation strategies.
* Spearheaded the implementation of an identity governance framework using ForgeRock, ensuring efficient access reviews and certifications.
* Undertook threat modeling exercises to identify prospective security risks in software applications.
* Experienced with Azure E5 security tools products (Defender ATP, Azure Sentinel, Azure ATP, Office 365 security, security center, Defender for Identity, Defender for endpoint.
* Addressed security gaps uncovered during certification tests or advocated for risk acceptance to senior leadership.
* Diagnosed and recommended fixes for cryptography and exception management issues in web applications.
* Managed and resolved issues in LAN/WAN infrastructure, including installation, configuration, and troubleshooting.
* Established a risk register based on the NIST framework and quantitative risk assessment methods.
* Collaborated with teams to audit applications before production launch.
* Used an array of penetration testing tools, including Burp Suite, DirBuster, HP Fortify, NMap, and QualysGuard, for daily security checks.
* Conducted an in-depth analysis of vulnerability scan results at both the OS and application levels, contributing to the vulnerability management process.
* Assessed the organization's security landscape, leveraging threat modeling, OWASP, and CWE methodologies to suggest protective measures.
* Conducted periodic audits on IAM systems to identify and rectify any compliance gaps.
* Employed network surveillance and protocol analyzers to troubleshoot issues causing network service interruptions.
* Automated web data extraction tasks using Selenium WebDriver for web scraping.
* Conducted compatibility tests across multiple browsers and platforms using Selenium WebDriver.
* Utilized Static Application Security Testing (SAST) tools such as HP Fortify and SonarQube for pre-deployment code analysis.
* Partnered with Vulnerability Management teams and application developers to secure the transition of applications into production settings.
* Offered remediation guidance to developers on security issues, helped plan code and application reviews, and ensured OWASP compliance.
* Validated fixed vulnerabilities to confirm their resolution.
* Checked the implementation of foundational security mechanisms like job rotation, least privilege, and defense in depth.

**Lean Data Technologies PVT LTD, India Jun 2016 - Mar 2018**

**Cyber Security Engineer**

* Evaluated and updated current IT security measures and controls, incorporating advanced technologies such as machine learning-based threat detection.
* Delivered periodic reports and presentations on the organization's information security posture to senior management and stakeholders.
* Spearheaded vulnerability scanning activities using industry-standard tools like Nessus, enhancing the company’s overall security posture.
* Authored and obtained Authorization and Accreditation (A&A) packages, securing Authority To Operate (ATO) for multiple high-stakes projects.
* Conducted in-depth internal security audits, utilizing frameworks like MITRE ATT&CK, to assess the effectiveness of security controls and to identify areas for strategic improvement.
* Established and led a specialized security incident response team, significantly improving the company's resilience against cyber threats. (New Point)
* Implemented an organization-wide secure code review process, reducing software vulnerabilities by 30%.
* Conducted comprehensive quarterly risk assessments, adapting the organization's cybersecurity strategy based on emerging threats and vulnerabilities.
* Formulated and executed a secure cloud migration strategy, ensuring zero downtime and data loss.
* Created a real-time security metrics dashboard, enabling continuous monitoring and KPI tracking for informed decision-making.

**Infotel India PVT LTD, India Apr 2015 - May 2016**

**Cyber Security Engineer**

* Formulated and revised security policies and Standard Operating Procedures (SOPs), laying the groundwork for the company's security architecture.
* Established templates for conducting mandatory security assessments, streamlining the system authorization process.
* Conducted foundational security assessments of various systems, adhering to NIST 800-53A guidelines.
* Collaborated with Information Systems Security Officers (ISSO) to evaluate security vulnerability scans and coordinated with IT teams for remediation.
* Managed patching and remediation activities for identified security vulnerabilities, using Plans of Actions and Milestones (POA&M) as a guide.
* Developed continuous monitoring mechanisms to enforce existing security policies and procedures.
* Led training sessions on cybersecurity awareness for end-users, promoting a culture of security within the organization.
* Designed and implemented a data governance framework to ensure compliance with data storage and handling requirements.
* Led a small team of junior security analysts to monitor real-time security events, helping to identify and prioritize potential threats.