



 A senior web and mobile application security professional with 8+ years of experience in financial, insurance, and hospitality industries, specializing in information technology assurance, web application security, secure coding, mobile application security, application security controls and validation, risk assessment, regulatory compliance, and Secure Software Development Life Cycle (Secure SDLC).

 Hands-on Qualys to perform Infrastructure Security, Cloud Security, Asset Management, Compliance, Application Security and Sensor Management.

 Having experience in SQL Injection protection, Script Injection, XSS Protection, and major hacking protection techniques

 Having experience in Secure SDLC and Source Code Analysis (Manual & Tools) on WEB-based Applications.  Hands-on with DAST, SAST, and manual ethical hacking.

 Expertise in working on Penetration Testing and Vulnerability Scanners.

 Working knowledge of the Payment Card Industry (PCI), Sarbanes-Oxley Section 404 (SOX), Federal Financial Institutions Examination Council's (FFIEC) regulations, including OWASP

 Vulnerability Assessment includes analysis of bugs in various applications spread across N-tier on various domains by using both manual and Automation tools.

 Worked with global security teams performing IT infrastructure and application security assessments.

 Excellent knowledge and industry experience in Vulnerability Assessment and Penetration Testing on WEB based Applications, Infrastructure penetration testing and mobile-based applications.

 Hands-on experience in developing threat models, security controls, threat analysis, creation of risk control matrices, and risk mitigation strategies.

 Penetration testing of web and mobile (iOS and Android) apps.



A Global Product Security Engineer to manage Vulnerability scanning of the products that are distributed around the globe using different vulnerability scanning tools. Also, assists in different security measures for products like

Incident Response, Penetration Testing, Risk assessment, and Disaster recovery for all global products.

Implemented web application vulnerability scanning for the products to identify, report, and remediate security vulnerabilities from applications deployed in DEV and PRE-PROD.

Performing Infrastructure Vulnerability Scanning for the product assets using vulnerability scanning tools to identify critical vulnerability and collaborate with product teams to mitigate them.

Conducting monthly scans of Infrastructure vulnerabilities, Web Application vulnerabilities, and Cloud configuration assessments.

Perform different security activities like privilege access management (PAM), penetration testing, incident response, logging and monitoring, business continuity plan, disaster recovery plan, and risk assessment regularly.

Conducted monthly developer workshops to educate and train developers on

Secure-SDLC, scan source code using IBM App-Scan Source, triage, and resolve security vulnerabilities. Conducted comprehensive vulnerability assessments using tools such as Qualys,

Rapid7, etc. Skilled in analyzing and addressing vulnerabilities (CVEs) based on NIST and CVSS scoring systems.

Performed thorough cybersecurity risk assessments for medical devices, identifying potential threats and implementing risk mitigation strategies.

Skilled in creating SBoMs and analyzing vulnerabilities for embedded systems.

Developed and implemented security protocols for IoT devices, enhancing threat detection and response times by 30% ensuring robust protection against emerging cyber threats.

Conducted security assessment to ensure compliance with the firm's security standards (i.e., OWASP Top 10). Specifically, manual testing was performed to identify cross-site scripting (XXS) and SQL injection-related attacks during the code review.

Led the implementation and integration of Software Composition Analysis (SCA) tools, such as Nexus IQ, into the CI/CD pipeline, resulting in a 30% reduction in open-source vulnerabilities across the application portfolio.

I have designed and implemented advanced authorization solutions using PlainID's

Policy-Based Access Control (PBAC) framework to enhance the security and compliance of enterprise applications. I developed and managed dynamic authorization policies to streamline user access management and reduce the risk of unauthorized access.

Proficient in TLS, PKI, BIOS secure boot, bootloader validation, and code signing processes. Skilled in implementing encryption algorithms and hashing for secure communication in embedded systems.

Successfully implemented and managed Intrusion Detection Systems (IDS) and

Intrusion Prevention Systems (IPS) to monitor network traffic for suspicious activities and potential threats, ensuring real- time protection and compliance with security policies.

I spearheaded the creation and enforcement of strong cloud security policies and procedures to meet industry standards like ISO 27001, NIST, and GDPR. This involved setting up Identity and Access Management (IAM) policies, overseeing encryption key management, and establishing monitoring and logging systems.

Implemented and monitored policies and procedures to ensure compliance with

HIPAA regulations, protecting patient confidentiality and safeguarding sensitive health information. Participated in the implementation of AWS Cloud security for applications deployed in the Cloud. Developed and implemented security policies and procedures following NIST SP

800-53 guidelines to ensure robust information system security controls and compliance with federal standards. Successfully deployed and configured the Nexpose security scanner using

PowerShell scripting to automate installation processes, configure settings, and schedule scans across multiple servers, thereby enhancing the efficiency and consistency of security assessments.

Regular audits and risk assessments were conducted to identify and mitigate potential HIPAA violations. Spearheaded HIPAA compliance initiatives, including developing and implementing privacy policies.

Conducted risk assessments and vulnerability analyses using the NIST SP 800-30,

37 framework to enhance organizational risk management strategies and mitigate potential security threats.

I implemented and carried out plans to respond to incidents and recover from disasters in cloud environments. I worked with different teams to quickly detect, analyze, and resolve security incidents, reducing downtime and data loss. I also used cloud-based tools and services for automatic backup and recovery processes.

Proficient in integrating and managing enterprise-wide cybersecurity tools, including CyberArk, Qualys (vulnerability scanning), Az MFA for enhanced threat detection and response.

Extensive experience in developing and implementing security policies aligned with industry standards to ensure network security across local, wide, and virtual private networks (LAN/WAN/VPN).

Administered and optimized IAM solutions such as Okta, Microsoft Azure AD, and

AWS IAM to enhance security posture. Conducted regular audits, user access reviews, and compliance checks to ensure adherence to organizational security policies and regulatory requirements.

Developed and enforced comprehensive security policies and procedures, ensuring compliance with industry standards and regulatory requirements to protect sensitive data and critical infrastructure across various business units.

Conducted comprehensive vulnerability assessments using Nexpose, identified and mitigated security risks across enterprise systems, leading to a 30% reduction in critical vulnerabilities.

Reviewed Android and iOS mobile code for mobile apps and recommended code fixes.

Worked with the Incident Response team (events from DLP) in reviewing events generated by DLP and guided in identifying the root cause of the event and a solution to resolve it.

Participated in the Proof of Concept (POC) to implement Checkmarx (a code analysis tool for web apps) and Arxan (application protection software for Mobile apps).

Regularly reviewed and optimized existing security policies, aligning them with evolving cybersecurity threats and best practices, leading to improved organizational security posture and reduced risk of breaches.

Conducted comprehensive security risk assessments using the STRIDE methodology, leading to implementing effective countermeasures and improving the overall security posture of applications.

Integrated cloud-based security tools such as ZScaler and Google Chronicle to monitor and enhance cloud security compliance across various platforms.

Worked with DevOps teams to automate security scanning into the build process. Developed Secure-SDLC guidelines for Web and Mobile apps.

Developed and maintained processes for ongoing monitoring, detection, and remediation of vulnerabilities in open-source components, ensuring compliance with industry standards such as OWASP to minimize the risk of supply chain attacks. Managed and optimized the Mimecast email security gateway by implementing protocols to safeguard against phishing, malware, and data leakage threats.

Generated executive summary reports showing the security assessment results, recommendations, and risk mitigation plans and presented them to the respective business sponsors and senior management.

Performed security assessments for the client-facing apps. The associated IT infrastructure such as database management systems, middleware systems, and web services (SOA) were also included in the security assessments. Experience in using Burp Suite, Acunetix Automatic Scanner, NMAP, Havij, and

DirBuster for web application penetration tests and conducted functional testing of RSA 2-factor Authentication. Implemented Secure Software Development Life Cycle (S-SDLC) processes; developed secure coding practices for web, and mobile applications, including database and middleware systems.

Reviewed Architecture Design Documents (ADD) and Solution Overview Documents

(SODs) to identify security anomalies in the system architecture and design and provided recommendations to address data security and privacy concerns.

Reviewed security vulnerability reports for applications and databases and analyzed and worked extensively with the development teams for the implementation of mitigating controls.

Conducted pen testing for the Web Services (SOA) used by various travel agency partners to connect to Wyndham for booking and reservations.

Designed and implemented comprehensive Identity and Access Management (IAM) solutions to enhance security and compliance across multiple platforms and applications. Successfully integrated multi-factor authentication (MFA) and single sign-on (SSO) to streamline user access and reduce unauthorized access incidents by 30%.

Implemented IBM App-Scan standard, source editions, HP Web-Inspect, and

Qualys-Guard web application scanners. In addition, the security tools Metasploit and Burp-Suite were utilized for manual penetration testing.

Monitored and analyzed security alerts using ASOC tools, and responded to potential threats with incident triage, investigation, and mitigation strategies to ensure minimal disruption to operations.

Conducted regular security assessments to identify vulnerabilities within applications. Collaborated with development teams to prioritize and deploy patches, enhancing overall security posture.

Successfully deployed, configured, and maintained IDS/IPS solutions to enhance network security, resulting in a 30% reduction in unauthorized access incidents.

Conducted manual source code reviews of the client-facing Wyndham brand web and mobile applications, including iOS and Android mobile Apps. The key areas of confidential and sensitive data stored on the mobile devices were reviewed and recommendations were made to secure customers PII and PCI data.

Black box pen testing on internet and intranet-facing applications.

Monitored network traffic, analyzed IDS/IPS alerts, and promptly identified and mitigated potential security threats to enhance organizational security..

Providing fixes & filtering false findings for the vulnerabilities reported in the scan reports.

Supporting in the preparation of plans to review software components through source code review or application security review.

Skilled in managing Microsoft security features for cloud environments, utilizing FireEye/Trellix for malware detection and Cisco ISE for network access control to protect infrastructure against unauthorized access and potential threats.

I have successfully secured multi-cloud environments (AWS, Azure, Google Cloud) by implementing best practices. This includes continuous security assessments, vulnerability scanning, and automated threat detection and response. I have utilized tools like AWS Security Hub, Azure Security Center, and Google Cloud

Security Command Center to enhance the security posture.

Implemented and managed security patch updates for COT applications, ensuring that known vulnerabilities were addressed in a timely manner to mitigate security risks.

Expertise in using Security Information and Event Management (SIEM) tools like

Splunk and IBM QRadar for monitoring, detecting, and responding to security incidents. I am adept at analyzing security alerts, correlating events from multiple sources, and implementing real-time threat detection to improve organizational security.

I created and managed PowerShell scripts to automate repetitive administrative tasks, increase system efficiency, and improve operational workflows. I successfully deployed scripts for user account management, system monitoring, and data extraction tasks, delivering significant time-savings and reducing errors.

Performed Static and Dynamic Analysis and Security Testing (SAST and DAST) for various applications as per the firm security standards (i.e., OWASP, SANS 25).

Designed, developed, and enforced robust Identity and Access Management (IAM) policies and procedures to ensure secure access to critical systems and sensitive data. Implemented role-based access control (RBAC) to streamline user permissions and minimize security risks.

Developed security policies and baselines for mobile and web applications.

Performed compliance audits to ensure security policies and baselines have been adequately implemented. Developed and implemented automated vulnerability scanning and patch management protocols for devices, including servers, workstations, network devices, and IoT.

This resulted in a 30% reduction in security vulnerabilities and compliance with industry standards. Conducted workshops and user awareness training on security policies, procedures, and baselines.

Evaluate and manage security risks associated with SaaS vendors, including reviewing security certifications, conducting risk assessments, and ensuring compliance with data protection regulations.

Participated in the implementation of SafeNet product for encrypting customer credit card information using Public Key Infrastructure (PKI).

Analyzed correlation rules developed for the Security Incident and Event

Management (SIEM) system. Reviewed the solution implemented for “log forwarding” from various network devices to ArcSight central logging for alerting and security monitoring.

Successfully enhanced the security posture of enterprise cloud environments by configuring and managing Azure Security Center.

Performed PCI pre-assessment audit for the entire network as well as the related applications in preparation for the annual external PCI compliance audit.

Documented security findings, and recommendations and presented them to the business users, executive committee, and Compliance departments.

Conducted security assessments for various applications supporting Corporate &

Investment Banking, Loan, Treasury, Equities, and FI businesses. The web application infrastructure such as IBM WebSphere, Apache Tomcat, and IIS web/application servers were reviewed for compliance with the firmʼs security baselines.

Performed penetration testing for external-facing web applications. Security areas covering DMZ architecture, threat modeling, secure coding practices (i.e.,

OWASP standards), and vulnerability analysis were assessed.

Developed audit programs for IT infrastructure supporting the Corporate and

Investment Banking department to facilitate end-to- end compliance with Global as well as Federal Financial Institutions Examination Council (FFIEC) guidelines and controls.

Managed security assessments for several types of Operating Systems (O/S) used by the firm. The audits of RedHat Linux, Oracle Solaris, Windows (including Active

Directory), and IBM AIX were conducted. Several control enhancements, specifically, on the patch management process, were recommended.

Performed database management system audits across all business lines and entities in the North American hub. Database servers such as Oracle, SQL Server, and Sybase were reviewed for compliance with global and local security baselines.

Ensured strict adherence to HIPAA regulations by maintaining confidentiality of patient records, implementing secure data handling protocols, and conducting regular audits to safeguard sensitive health information.

Reviewed a newly implemented Security Incident and Event Management (SIEM) system. Reviewed technical specifications for SIEM, and logging and proposed recommendations to improve the overall deployment of the solution.

Designed and developed a suite of applications used by the internal audit department, including B-Planner, OATS, and Time tracking systems.

Developed server-side business components using Java/J2EE, Spring Framework, Servlets, JSPs, Web Services, and Enterprise Java Beans (EJBs)

Developed graphical charts using Sitraka, and JClass to show the departmentʼs performance statistics. Analyzed performance issues in the application, and related system configuration and developed solutions for improvement.

Developed stored procedures, views, and triggers using Oracle PL/SQL.

Involved in WebLogic and Tomcat application server installation and configuration in production, development, and QA environments.

Security vulnerability assessment, Penetration testing, Security infrastructure architecture, Architecture reviews, Analytical and Critical Thinking, C++, Java, C#, .net., Python, HTML, CSS, JavaScript, XML Platforms: Windows XP, 10, UNIX/LINUX. Web Server: Apache, IIS 6.0/7.0, Windows 2003/2008/2012 Servers Database: MySQL, SQL, Oracle Networking Concepts: OSI Model, TCP/IP, UDP, IPV4, IPv6, LAN, WAN, Subnetting



MySQL, SQL, Oracle

Azure, AWS, GCP

Burp Suit, Jfrog X-ray, F5, Checkmarx, Metasploit, Sonar Cloud, Sonar Qube, ZScaler, Rapid7, SIEM, Splunk, Git, Jenkins, Postman, PlainID, Kali Linux, CyberArk, SQLmap, HP Fortify, Nexpose, Nexus IQ Metasploit, OpenVAS, IDS/IPS, OWASP ZAP proxy, DLP SoapUI, Qualys, GDPR, FireEye, ServiceNow, NIST, HIPPA, SOC2, PCI DSS, Ciscofire power CrowdStrike.



AWS Security Specialty

https://[www.linkedin.com/in/sai-kumar-r-6503b4247/](http://www.linkedin.com/in/sai-kumar-r-6503b4247/)