Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

Summary:

Having 8+ years of experience in **Financial, Telecom and Healthcare industries**, specialized in **Web Application Security, Security Architecture & Design,Cloud Access Security Broker, Penetration Testing, Secure Coding, Mobile Application Security, Application Security Controls and Validation, Risk Assessments, Security Audits,** Regulatory Compliance and Secure Software Development Life Cycle (secureSDLC) and Continuous Integration (CI) and Continuous Delivery (CD) of security scanning.

- IT Security Strategy in meeting the Company's IT Security efforts for dynamic Business Goals. Additionally, proficient in security policy write up, procedures and control review to attain optimal maturity level.
- Expertise with security practices related to network switches, routers, load balancers, servers, storage systems
- Expertise in **Security assessment** on the applications, web sites, and web applications to determine the security posture.
- Experience in performing manual exploitation using different tools like **NMAP**andKali Linux.
- Expertise in **Penetration Testing** and established a formal vulnerability managementprocess.
- Experience in monitoring and recommended solutions for correcting issues related to security technologies such as to monitor viruses, malware, and intrusions.
- Hands-on experience in developing threat models, security controls, threat analysis, creation of risk control matrices and risk mitigation strategies.
- Experience in conducting **IT Security Risk Assessments** in accordance to **NIST and FFIEC** framework.
- Experience in collaborating with various product management and development teams to ensure alignment between security and development practices.
- IT Professional Security /Risk Analytic and Architectural skills, IT Governance and Security Operations expertise overseeing the alignment of enterprise

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

- Hands-on with Penetration Testing, Source Code Review, **DAST, IAST, SAST** and manual ethical hacking.
- Hands-on in securing APIs, Microservices using Apigee, and **AWS API** Gateway.
- Thorough knowledge on **COBIT, OWASP, FFIEC, NIST, HIPAA** regulations and frameworks.
- Experience in Security Audit proactive mindset for Risk Mitigation and proven ability to using Information Technological Solutions and Tools to Optimized differentInformation Security Frameworks and approaches through Practical Application to evolving Business needs.
- Experienced in Security Assessment tools: **Nessus, Burp Suite, NMap, Netcat, andWireShark** etc.
- Experience and also have strong working knowledge on various information security standards and compliances such **HIPPA, HITRUST, PCI-DSS, FISMA, GLBA, SOC2, NIST** and other GRC's. Additionally, passionate in Enterprise Data Classification,**Identity and Access Control management (IAM)** deployment solutions, IT Risk Management, Governance, Security Compliance Methodologies.

Experience

Client: MasterCard, O Fallon, MO **Jan' 2019 - Present**

Title: Lead/Sr. Security Engineer

- Experience using a wide variety of security scanning (**SAST, DAST, IAST**) tools to **include Kali-Linux, Metasploit, Checkmarx, MicrofocusWebInspect, Microfocus Fortify, Burp Suite Pro, Wireshark, L0phtcrack, Snort, Nmap,Nmap-NSE, Cain and Abel, Nitko, Dirbuster, HCLAppScan, OWASP ZAProxy,Zed Proxy, Microsoft, Rapid7, Cisco, Imperva, Nessus, Open Vas, W3AF,**BeEF, Etthercap, Maltego, Wifi-Security, SIFT, SOAP UI,FOCA, Havij, Yersinia, Recon-ng, **Aircracking** suite.
- Penetration testing based on **OWASP Top 10 and SANS25.** Analyze the results of penetrations **tests, design reviews, source code reviews** and other security tests.

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

- Expertise on full scale **Ethical Hacking/Penetration testing** practice. Participated in Pen Testing andEthical hacking activities on identified tasks.
- Involved in implementing and validating the security principles of minimum attack surfacearea, least privilege, secure defaults, avoiding security by obscurity, keep security simple, Fixing security issues correctly. Strong knowledge in Manual and Automated Security testing for Web Applications.
- Developed Application Security program **(DAST and SAST)** at the enterprise level to identify, report and remediate security vulnerabilities.
- Hands-on with Secure Coding, **Penetration Testing, DAST, SAST** and manual ethical hacking.
- Implement and maintain the **Vulnerability Scanners.** Experience in Qualys Vulnerability Management.
- Working Experience of **OWASP Top 10 and SANS Top 25** software guidelines, Federal Financial Institutions Examination Council's (FFIEC) regulations, including **Payment Card Industry(PCI-DSS), HIPAA and Sarbanes-Oxley Section404 (SOX).**
- Experience with **Identity and Access Management (IAM)** and development of user roles and policies foruser access management.
- Enforcement of policies and procedures for users, admins, and management Reverse engineering of malware using tools like malwr, process hacker and so on **Incident response** tabletop exercise by documenting and alerting necessary personnel.
- Experience in **Threat Modeling** during Requirement gathering and Design phases.
- Good Experience in exploiting the recognized vulnerabilities and Performed **security Risk analysis** and gap analysis.
- Particiapted in the implementation of **API Security projects** including OAuth2.0 and SAML.
- Gathered the requirements, Developed **API** use cases, scenarios and worked on Application boarding, **API i**ntegration and troubleshooting.
- Guides Cyber Delivery teams in adoption of **NISTand COBIT IT Risk Framework** Capabilities.
- Experience working with a variety of security-related platforms andservices, including: **SIEM** systems, Threat Intelligence platforms,Security Orchestration, **Automation and Response (SOAR)**

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

solutions,Encryption technologies, File Integrity Monitoring (FIM), and othernetwork and system monitoring tools.

- Analyzed the results of **penetrations tests, design reviews, source code reviews** and other security tests.
- Participated in the implementation of **AWS Cloud security** for applications being deployed in the Cloud. Developed WACLS for AWS Web Application Firewalls (**WAF**) and configured the rules and conditions to detect security vulnerabilities in the Cloud Front.
- Configured **AWS Simple Storage Service (S3)** to securely store the organization's critical file systems. Implemented Access Control Lists (ACLs) and Bucket Policies for controlling access to the data.
- Implemented Security Group Policies for **Elastic Compute Cloud (EC2)** instances within AWS. Developed AWS Service Roles to protect Identity Provider access.
- Developed security policies for **controlling APIs**(**Apigee**) and their access to the backend web services (**RESTful, SOAP**).
- Briefs the customer and other contractors on recommended solutions and designs.
- Worked on HSMs using **Gemalto ProtectDB** and Good understanding of Object-Oriented Programming and Design **(OOP/OOD).**
- Conducted security assessment of **Cryptography applications** including the apps that use **Hardware Security Model (HSM).**
- Performed **Continuous Integration (CI) and Continuous Delivery(CD**) of **SAST** scans using IBM AppScan Source for Automation.
- Familiar with **DevOps** technologies/applications like **Puppet, CHEF, Jenkins, Docker,ANT** and **Maven.**
- Analyze network topologies and traffic and capacity requirements and provide recommendations and guidance through the secure lens of Tenable.

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

- Participated in the implementation of data tokenization in various environments to ensure compliance to regulations. Expertise in **Qualys Policy Compliance.**
- Participated in the implementation of **Virtual Private Cloud** (VPC). Implemented multiple layers of security, including security groups, network access control lists, to control access to Amazon EC2 instances in each subnet.
- Experience with Qualys AssetView, Cloud Agents, Indicators of Compromise and Experience with Qualys asset tags and asset groups for reporting.
- Experience in the administration configuration, scanning, reporting, authentication, user administration, and performance tuning using Qualys enterprise suite of tools.
- Worked on security protocols such as **TCP/IP, SNMP, SMTP, NTP, DNS, LDAP and NFS** on implementation, maintenance and monitoring.
- Experience with Security Risk Management with **TCP-based networking.**
- Experience with **TCP/IP, Firewalls, LAN/WAN.** Experience in implementing Security.
- Incident and Event Management System (SIEM) using HP ArcSight, **Splunk ES, Exabeam** UBA, UEBA.
- Excellent problem-solving and leadership abilities. Experience in Web UIDevelopment implementing web development tools like **HTML 4.0/5, XHTML,DHTML, CSS/CSS3, JavaScript, jQuery, AJAX, JSON and XML.**

Client: LabCorp,Princeton, NJ **Jun' 2017 – Dec'2018**

Sr. Security Engineer

- Penetration testing based on **OWASP Top 10 and SANS25.** Analyze the results ofpenetrations tests, design reviews, source code reviews and other security tests.
- Decide on what to remediate and what to risk accept based on securityrequirements. Highly analytical computer security analyst with success both defending and attacking large-scale enterprise networks.

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

- Developed **Security API** and deployed to development teams which helps them write lower riskapplications in a secure manner.
- Experience in **Threat Modeling** (**STRIDE**) during Requirement gathering and Design phases.
- Implemented Multifactor Authentication (**MFA**) for **AWS** root accounts, including password rotation policies. Set up Access Keys and Secret Assess Keys for newly created users.
- Enabled threat detection for databases in the **Azure** portal. The security alerts generated in the Azure Security Center have been reviewed and remediated.
- Configured **AWS Simple Storage Service** (S3) to securely store the organization's critical file systems. Implemented Access Control Lists (ACLs) and **Bucket Policies** for controlling access to the data. .
- Implemented security around **Dockers** to ensure Containers and the data present in them are secured as part of secureSDLC. The Container security tool such as **AquaCloud Native Security** has been utilized.
- Developed security controls for implementing Azure storage security. The RBAC with Azure AD has been implemented for securing the storage account. The data transmission between applications and Azure has been secured by client-side encryption, HTTPS, SMB3.0.
- Develop **security requirements** for applications and infrastructure deployed in the Cloud. Ensured that **Cloud security** best practices have been followed.
- Analyzed **security incidents** originated from various network/application monitoring devices (e.g., **Symantec DLP**) and coordinated with Engineering teams for tracking and problem escalation, including remediation.
- Experience using a wide variety of security tools to include Kali-Linux, Metasploit, MicrofocusWebInspect, Fortify, BurSuite Pro, Wireshark, L0phtcrack, Snort, Nmap, Nmap-NSE, Cain and Abel, Nitko, Dirbuster, IBM App Scan, Microsoft, Rapid7, Cisco, Imperva, OWASP ZAProxy, Nessus, Open Vas, W3AF, BeEF, Etthercap, Maltego, Wifi-Security, SIFT, SOAP UI, FOCA, Havij, Yersinia, Recon-ng, Aircracking suite

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

- Involved in implementing and validating the security principles of minimum attacksurface area, least privilege, secure defaults, avoiding security by obscurity, keep security simple, Fixing security issues correctly. Strong knowledge in Manual and Automated Security testing for Web Applications.
- Working knowledge of OWASP Top 10 and SANS Top 25 software guidelines, Federal Financial Institutions Examination Council's (FFIEC) regulations, including **Payment Card Industry** (PCI-DSS), HIPAA and Sarbanes-Oxley Section404 (SOX).
- Analyzed the results of **DAST, SAST, IAST**, penetrations tests, design reviews, source code reviews and other security tests.
- Decide on what to **remediate** and what to risk accept based on security requirements. SOX Compliance Audit experience on controls like User access management, ChangeManagement, Incident Management.
- Good Experience in **exploiting** the recognized vulnerabilities.
- Experience with Security Risk Management with TCP-based networking.
- Experience with TCP/IP, Firewalls, LAN/WAN. Experience in implementing Security
- Incident and Event Management System (**SIEM**) using HP ArcSight, **Splunk Enterprise Security**.
- Quick Learner, Committed team player with interpersonal skills and enjoy challenging environment with scope to improve self and contribute to the cause of the organization.
- Excellent problem-solving and leadership abilities. Experience in Web UI Development implementing web development tools like HTML 4.0/5, XHTML, DHTML, CSS/CSS3, JavaScript, jQuery, AJAX, JSON and XML.
- Knowledgeable about Document Object Model (DOM) and DOM Functions along with experience in Object Oriented Programming Concepts, Object Oriented JavaScript and Implementation.

Edward Jones, St Louis, MO **Jul' 2015 – May '2017**

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

Security Analyst

- Vulnerability assessments using HP Web Inspect,Acunetixscanners perform map and gap analysis on all systems, software, and network appliances Access vulnerability dataprepare reports and load scan data into database.
- Discuss false positives and prepare a plan of action and milestones for mitigation Prepare incidentreports for reported and unreported attacks APT hunting for Ransomware.
- Performed Root Cause Analysis for the incidents reported at Security Operations Center. Performed Security event monitoring of heterogeneous networks such as Firewalls, IDS/IPS, Cisco ASA, DLP devices using Splunk.
- Reviewed Azure network security architecture and implemented security controls. Specifically, Azure virtual networks, including on-premise connectivity, traffic filtering, secure communication, point-to-site VPN etc.,
- Implemented Network Security Groups (NSG) to control network traffic to various Azure network resources. Created NSG rules (inbound and outbound) and prioritized the rules based on the requirements. Associated NSGs to VMs, NICs, and subnets based on the deployment model.
- Validated database security for SQL servers deployed in Azure Cloud environment. Implemented Integrated Windows authentication supported by Azure Active Directory.
- Wrote scripts on servers using PowerShell on Windows Server 2008 in order to update servers with the latest patches and changes systems configurations at large.
- Assisted in design and implementation of McAfee DLP solution companywide for the information systems. Collaborated with the team leaders to complete the implementation.
- Provided assistance to management with administration and configuration of critical enterprise security systems and software like McAfee ePO, McAfee DLP, Complete Endpoint Protection, Proofpoint.

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

- Used Remedy Information Technology Service Management (ITSM) tool for managing the incidents based on the priorities and solved issues which are in the security domain.
- reports to monitor the health of the applications and also reported High, Medium and low vulnerabilities in this system.
- Analyze attack patterns Build workflows to automatically analyze the samples
- Determine what functionality attackers may have introduced and scan for malicious artifacts based on sandbox results Investigate endpoint attacks and replay attacks onsystems.
- Analyze JavaScript, PDFs, Office documents, and packet captures for signs of malicious activity SIEM implementation and analysis by writing rules and reference sets.
- SIEM to determine attack vectors and source of incidentTroubleshoot network application inbound/outbound connectivity utilizing Cisco WSA proxies and Wireshark.
- Actively involved on Bridges in solving High/Severe incidents reported in the application or in the environment.
- Ironport URL filtering for known bad URL content IronportMail.
- Analysis and blocking for known bad emails Analysis of pcap files using FireEye and Wireshark System audit and analysis using DOD checklist for PA series Threat and virus scanning using Malwarebytes from centralized console.

Cloud Data Solutions **Oct '2012 — Jun' 2015**

Java/J2EE Developer

- Worked in Agile SCRUM SDLC process to implement the sprint tasks which are 4 weeks.
- Developed web layer using Spring MVC along with UI technologies like HTML5, CSS3.
- Implemented controller, service, DAO and utility classes using Core Java concepts like OOPS, Exception Handling, String manipulation, and Collection framework.
- Implemented Hibernate framework as ORM for DAO layer to access the Oracle database.

Teja

Sr. Security Engineer

Email: tejat4255@gmail.com

Tel: 314-833-7946

-

- Implemented Entity classes for ORM mappings and HQL queries for data retrieval.
- Used Spring ORM to integrate spring framework with Hibernate.
- Developed JAX-WS SOAP web services using XML, WSDL, XSD through Apache CXF Implementation
- Developed REST web services with JSON message transformation using Spring REST.
- Developed Junit test cases for unit testing and Mockito for mocking.
- Wrote SQL queries to verify the data related issues.
- Worked with Q team to resolve the defects and UAT defects with the business users.
- Configure and deployed application on WebLogic application server.
- Developed and debugged the application using Eclipse IDE.
- Tested the application in different environments like DEV, QA and UAT.
- Maven for the application builds and Jenkins for the continuous integration.
- Used JIRA for the Agile project management and issue tracking.
- Participated in daily scrum meetings, sprint planning sessions.

Certifications

CompTIA Security+

AWS Certified Security Specialty

Certified Ethical Hacker (CEH)

Certified Information Systems Security Professional (CISSP) (in progress)

CompTIA Security +

Education

Bachelor's in Information Technologyfrom India.