**Sr. Cyber Security Engineer**

**Aditya Tirumala**

**adityabittu3@gmail.com**

**LinkedIn: http://www.linkedin.com/in/aditya-yadagiri-216966311**

**PROFESSIONAL SUMMARY:**

Over 9+ years of experienced in Cybersecurity Professional with expertise in various domains, including Application Security, Vulnerability Management, Penetration Testing, Cloud Security, and Security Operations Center (SOC) operations. Proficient in utilizing industry-standard security tools and frameworks to identify, assess, and mitigate security risks and vulnerabilities. Proven ability to collaborate with cross-functional teams, communicate effectively, and drive security initiatives within organizations.

* Performed vulnerability assessments, penetration testing, and secure code reviews for web applications, APIs, and network infrastructure.
* Design, Configuration of Network using GNS3 and Packet tracer.
* Analyzing and Troubleshooting Network issues using Wire Shark
* Performed vulnerability assessments, penetration testing, and secure code reviews for web applications, APIs, and network infrastructure.
* Experienced in manual and automated testing of websites and applications against OWASP Top 10, SANS 25, and other industry-standard security vulnerabilities.
* Utilized SAST tools (Fortify, Checkmarx), DAST tools (Burp Suite, IBM AppScan), SCA tools (Black Duck), and other security scanning tools for code analysis and vulnerability identification.
* Created comprehensive vulnerability assessment reports, including identified exposures, severity ratings, and mitigation recommendations.
* Designed and implemented IAM configurations to secure access to sensitive data and applications across the organization.
* Gained extensive experience with SIEM tools (Splunk, IBM QRadar) for log analysis, security incident monitoring, investigation, and mitigation.
* Expertise in embedded C++ programming and Real Time Operating Systems (RTOS).
* Managed and administered Entra ID, ensuring seamless user authentication and authorization across multiple applications.
* Designed and implemented robust API security measures using Cloudflare to protect web applications from malicious traffic and DDoS attacks.
* Implemented Perl Scripting for network Analysis.
* Experienced in automated deployment (terraform, AWS Cloud Formation), and serverless architecture AWS lambda and other AWS services.
* Implemented SSO solutions, enabling users to access multiple applications securely with a set of credentials.
* Expertise in writing the playbooks using the YAML scripting which manages the configurations also have experience in setting up master minion architecture in Kubernetes to maintain the containers with the help of using YAML files, also deployed Docker containers through Kubernetes to manage the Microservices using its nodes, ConfigMaps, selector, Services, Pods.
* Analyzed security event data from network devices (IDS, IPS, firewalls) and performed static malware analysis on isolated virtual servers.
* Architected end-to-end security solutions for various organizations, ensuring the integration of best practices in network security, data protection, and threat management.
* Monitored and analyzed security events in a 24x7 Security Operations Center (SOC) environment for intrusions and malicious activities.
* Investigated and responded to security incidents, phishing attempts, and cyber threats impacting the organization.
* Configured SSO authentication protocols, such as SAML and OAuth2, to ensure secure, access management.
* Collaborated with stakeholders to install, update, and troubleshoot automated systems adhering to cybersecurity standards and practices.
* Planned and executed remediation activities for identified vulnerabilities, mitigating risks in web applications and architectural weaknesses.
* Involved in Configuration of Access lists (ACL) on checkpoint firewalls for the proper network routing in B2B network connectivity.
* Implemented Entra ID to streamline identity management, providing a unified and secure platform for user access.
* Configured and optimized Cloud flare’s API Shield to enforce strict security policies, including mutual TLS authentication and schema validation.
* Assisted in assessing compliance with cybersecurity frameworks (PCI-DSS, ISO 27001, NIST) and industry best practices.
* Implemented and supported cloud-based security solutions, architectures, and proof of concepts for AWS and Azure environments.
* Trained development teams on secure coding practices, security requirements, threat modeling, and security testing to improve the SDLC.
* Demonstrated proficiency in various technologies, including Active Directory, PKI, VMware, application servers (WebSphere, Tomcat), and databases (Oracle, SQL Server).
* Conducted risk assessments, prepared risk registries, and developed risk mitigation strategies.

**Certifications:**

**Certified Information Systems Security Professional (CISSP).**

**Technical Skills:**

|  |  |
| --- | --- |
| **Skill Set** | **Details** |
| Application Security | OWASP Top 10, ASVS, MSTG, Secure Code Reviews, SAST (Checkmarx, IBM AppScan, Fortify), DAST (Burp Suite, OWASP ZAP, Contrast), Threat Modeling, Secure SDLC |
| Penetration Testing | Web Application Pentesting, Network Pentesting, Cloud Pentesting (AWS, Azure, GCP), Mobile App Pentesting, Burp Suite, Nmap, Nessus, Metasploit, Kali Linux |
| Vulnerability Management | Vulnerability Assessments, Patch Management, Vulnerability Scanning (Nessus, Qualys, Nexpose), Remediation Tracking (Archer, BitSight, ScoreCard) |
| Cloud Security & Automation | AWS Security (JAM), Azure Security, GCP Security, Cloud Configuration Audits, Cloud Architecture Reviews, DevSecOps (CI/CD with Git, Jenkins, Ansible, Docker, Kubernetes), Ansble, Puppet |
| Identity & Access Management | IAM, RBAC, PAM, Privilege Management, Identity IQ (SailPoint, Crowdstrike, CyberArk) |
| Security Monitoring | SIEM (Splunk, QRadar, LogRhythm), IDS/IPS, Firewalls, Endpoint Security (McAfee, Symantec), Network Monitoring, Log Analysis, Threat Intelligence |
| Compliance & Standards | SOC 2, PCI-DSS, HIPAA, GDPR, ISO 27001, (800-30, 800-53, 800-61, 800-63), FIPS |
| Security Engineering | Security Architecture, Secure Design, Threat Modeling, Risk Assessment, Security Controls Implementation |
| Incident Response | Incident Handling, Forensic Investigations, Malware Analysis, Incident Response Lifecycle |
| Programming Scripting & Databases | Python, PowerShell, Bash Scripting, Embedded, Java, C, C++, MySQL, MongoDB, PLSQL, Oracle  |
| Networking & Protocols | TCP/IP, DNS, DHCP, HTTP, HTTPS, SSH, TLS, VPN (IPsec, SSL, PPTP, L2TP), Firewalls, IDS/IPS, Packet Analysis (Wireshark, tcpdump) |
| Collaboration & Training | Technical Presentations, Security Awareness Training, Product Demonstrations, Customer Engagements, Sales Enablement |
| Security implementations | SSL certs, TLS, data encryption 512 and 256 standards , Kerbos authentication and PAM access management |
| Operating systems  | Widows 2019, 2022 Linux rhel 7, 8 and 9, IBM AIX, UNIX sun Solaris |

**PROFESSIONAL EXPERIENCE:**

**Client: Amdocs, Plano TX Sep 2022 to Present**

**Sr. Cyber Security Engineer**

**Responsibilities:**

* Collaborated with stakeholders to install, update, and troubleshoot automated systems adhering to cybersecurity standards and practices.
* Planned and executed remediation activities for vulnerabilities identified through application scanning tools like Qualys, mitigating risks in web applications and architectural weaknesses.
* Communicated effectively with business units regarding web application vulnerabilities and managed access control mechanisms.
* Designed and implemented secure cloud architectures for platforms such as AWS, Azure, and Google Cloud, ensuring robust protection of data and applications.
* Design, development, and unit, system and integration testing of embedded application software’s with C++ on a multithreaded QNX environment.
* Implemented OAuth2 protocols to enable secure authorization and access to APIs and third-party services.
* Investigated and documented network security incidents, reported to management, monitored security data, and analyzed threats.
* Acted as a Subject Matter Expert (SME) in cybersecurity, offering expert guidance on threat detection, incident response, and risk management to internal and external stakeholders.
* Managed security tools for PCI DSS compliance, collaborating with the security team to standardize policies.
* Conducted daily vulnerability assessments, prioritized risks, and established remediation timelines.
* Assisted in assessing compliance with cybersecurity frameworks and remained updated on industry trends and emerging technologies.
* Installed and configured SPLUNK for centralized logging in distributed environments.
* Coordinated with global teams, including security architecture, penetration testing, application development, and risk officers.
* Integrated Cloudflare’s performance optimization features, such as caching and content delivery network (CDN) capabilities, to improve API response times and reduce latency.
* Involved in standardizing Splunk Phantom SOAR POV deployment, configuration and maintenance across UNIX and Windows platforms.
* Integrated Entra ID with cloud services like Azure and Microsoft 365, enabling centralized identity management.
* Security assessments and audits across multiple platforms and systems, identifying vulnerabilities and recommending actionable solutions to mitigate risks.
* Managed user identities, roles, and permissions within the IAM system, ensuring proper access control.
* Configured applications that run multi-container Docker applications by utilizing the Docker-Compose tool which uses a file configured in YAML format. Used Kubernetes to manage containerized applications using its nodes, Config-Maps, selector, Services and deployed application containers as Pods.
* Utilized Jira and Confluence for tracking and monitoring vulnerabilities and performance indicators.
* Provided comprehensive reporting, analysis, and follow-up on vulnerability assessments.
* Conducted internal network vulnerability assessments to enhance the organization's security culture.
* Analyzed vulnerabilities using scanning tools, removing false positives for accurate reporting.
* Monitored and researched cyber threats impacting the organization.
* Collaborated in the automation of AWS infrastructure via Terraform and Jenkins - software and services configuration via chef cookbooks.
* Developed and enforced security policies and procedures tailored to specific organizational needs, ensuring compliance with industry standards and regulatory requirements.
* Developed and implemented SSO policies, ensuring compliance with organizational security requirements.
* Utilizes NIST 800-53A and NIST 800- 53 rev-4 to review implemented controls and enter information into the Requirements Traceability Matrix (RTM) and findings into the Security Assessment Report (SAR).
* Managed and enhanced cloud security operations on Azure and GCP, integrating robust firewall strategies and ensuring alignment with NIST cybersecurity frameworks and CJIS compliance requirements.
* Developed and implemented security policies and control measures for Cisco's cloud environments, continuously assessing and optimizing policies to uphold NIST and CJIS standards Azure and GCP platforms.
* Managed security devices, generated configuration requirements, reviewed efficiency, and implemented change management processes.
* Performed log reviews, initiated appropriate actions, and participated in incident response processes.
* Received and prioritized alert notifications, responding promptly to mitigate potential threats.
* Maintained approved policy exceptions and conducted periodic reviews.
* Participated in audits and assessments, providing support and ensuring adherence to security standards.
* Demonstrated flexibility by performing ad-hoc security requests and additional duties as assigned.

**Client: Cisco, Sanjose, CA Jun 2021 to Aug 2022**

**Role: Information Security Analyst**

**Responsibilities:**

* Performed vulnerability assessments, network penetration testing, and web application penetration testing for Java and .NET applications.
* Conducted static and dynamic code analysis, threat modeling, design reviews, and penetration testing to identify vulnerabilities in internal and external web applications.
* Experienced in manual and automated testing of websites against OWASP Top 10 and SANS 25 vulnerabilities.
* Thorough understanding of OWASP Top 10 vulnerabilities, their attack vectors, and defense mechanisms (e.g., XSS, SQLi, CORS).
* Used assembly language and C, writing the embedded software for 8031/8051 board.
* Utilized SAST tools (Fortify), DAST tools (Burp Suite, IBM AppScan), and SCA tools (Black Duck) for code scanning, generating reports, and collaborating with developers for remediation.
* Conducted vulnerability assessments and penetration testing using Nessus, Qualys, IBM AppScan, Burp Suite, and publicly available tools.
* Implemented Multi-Factor Authentication (MFA) policies in Entra ID, enhancing security for all user accounts.
* Familiar with PCI-DSS compliance requirements.
* Hands-on experience with Cloudflare for API security, enhancing protection against DDoS attacks and unauthorized access.
* Created vulnerability assessment reports detailing identified exposures, severity ratings, and mitigation suggestions.
* Executed vulnerability scans and delivered reports using approved tools like Burp Suite, Qualys Guard, and HP Web Inspect.
* Deployed Azure IaaS virtual machines (VMs) and AWS Cloud services (PaaS role instances) into secure VNets and subnets.
* Provide review of security controls employing NIST 800-53 recommended security controls.
* Gained experience with SIEM tools (Splunk) for log analysis and security incident monitoring, investigation, and mitigation.
* Analyzed security event data from network devices (IDS, SIEM) and performed static malware analysis on isolated virtual servers.
* Developed and documented best practices for using OAuth2 in application development, ensuring secure implementation.
* The cloud platforms proficient in, such as AWS, Azure, Google Cloud Platform (GCP).
* Recognized and analyzed potential, successful, and unsuccessful intrusion attempts and compromises.
* Enforced organizational security policies through vulnerability scanning and monitoring.
* Researched new and evolving threats and vulnerabilities that could impact the monitored environment.
* Identified suspicious or malicious activities and codes.
* Orchestrated the transition of security operations to integrate with GCP, leveraging Azure for comprehensive security enhancements and ensuring adherence to NIST and CJIS regulatory requirements through strategic firewall deployment.
* Worked in a 24x7 Security Operations Center, monitoring and analyzing security events for intrusions and malicious activities.
* Managed conditional access policies in Entra ID, ensuring secure access based on user location, device, and other factors.
* Investigated malicious phishing emails, domains, and IPs using open-source tools and recommended appropriate blocking measures.
* Configured IAM policies to enforce least privilege access, The risk of unauthorized access to critical systems.
* Demonstrated clear understanding of computer networks, protocols, and technologies (IP, domains, firewalls, routers, HTTP, HTTPS, DNS, LDAP, SNMP, FTP, SNTP).
* Proficient in technology areas like Active Directory, NPS, DHCP, DNS, and VMware.
* Experienced in implementing Public Key Infrastructure (PKI) with Active Directory.
* Gained knowledge in cyber threat hunting, incident response, and code review.
* Performed bug hunting and identified vulnerabilities (XSS, session hijacking) in internal web applications.
* Experienced with various application servers like IBM WebSphere and Apache Tomcat.
* Knowledge in writing SQL queries, triggers, views with databases like Oracle, SQL Server, and MS Access.

**Client: Best Buy, Minneapolis, MN Nov 2019 to May 2021**

**Position: Application Security Engineer**

**Responsibilities:**

* Perform security code reviews and provide remediation guidance in Java web applications and microservices.
* Good knowledge of web technologies like HTML, CSS, and JavaScript to ensure protection from XSS by reviewing the code.
* worked on the DOM XSS by analyzing the JavaScript.
* For the network, we use Nmap and Metasploit scripts. For the Web, we use Metasploit scripts and work manually as well.
* Alternatively, we do a nexus scan and an infrastructure scan for both network and web services.
* Experience in API testing tools like Postman or SoapUI
* In-depth knowledge on the OWASP top 10 API vulnerabilities and mitigations.
* performed development staff for test planning, create weekly reports, develop test cases, ensure code functionality, and identify defects to implement a strategy to enhance testing.
* performed static application security testing assessments for web applications, microservices, and mobile applications using Checkmarx.
* Performed application security programs (DAST and SAST) at the enterprise level to identify, report, and remediate security vulnerabilities from applications deployed in DEV, PRE-PROD, and
* PROD environments.
* Managed OAuth2 token lifecycles, ensuring proper issuance, validation, and expiration of access tokens.
* Worked closely with developers to integrate Cloudflare security features into API development workflows.
* Integration of the IBM Appscan tool with Jenkins in the agile development process for dynamic analysis and security testing.
* Implemented multi-factor authentication (MFA) within the IAM system to strengthen security for user access.
* Responsible for ensuring IT systems have all security controls in place and functioning properly in accordance with NIST 800-53rev4 publication.
* Used Terraform to provision the instances on AWS Cloud.
* Designed Terraform templates to create custom sized VPC, subnets, NAT to ensure successful deployment of Web applications and database templates on AWS.
* I worked extensively with software development teams to review the source code, triage the security vulnerabilities generated by Checkmarx, and eliminate false positives.
* Developing threat modeling framework (STRIDE, DREAD) for critical applications to identify Potential threats during the design phase of applications.
* Developing mitigation strategies to address identified threats and enhance the security posture of the system.
* Analyzing the system's design and architecture to understand potential vulnerabilities and attack surfaces.
* Detect problems early in the software development life cycle (SDLC)—even before coding begins
* Improving the application security posture of the company's online business by performing periodic assessments on mission-critical applications.
* Log defects in Jira and assign them to the application team for fixes. Work with application teams to help them remediate security vulnerabilities.
* Perform risk analysis to identify points of vulnerability and recommend disaster recovery strategies and business continuity planning.
* Implemented a robust continuous monitoring program utilizing a NIST SP 800-137 compliant Information System Continuous Monitoring (ISCM).
* Identifying and evaluating new marketing opportunities to increase website traffic and online production.
* Proficient in understanding application-level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws, etc
* Analyze data packets, review signatures, and analyze and interpret PCAP using Wireshark
* Monitor the Security of Critical System (e.g., e-mail servers, database servers, Web Servers, Application Servers, etc.).
* Perform vulnerability analysis utilizing Ethical Hacking tools, techniques and procedures.
* Initiate Incident Response procedures to mitigate and, or eliminate, known threats to the client's business operations.
* Identifying the critical, High, Medium, and low vulnerabilities in the applications based on OWASP Top 10 and SANS 25 and prioritizing them based on their criticality.

**AmeriHealth, Philadelphia, PA Nov 2018 to Oct 2019**

**Application Security / Cloud Security Engineer**

**Responsibilities:**

* Monitored networks using DLP, Websense, Trend Micro, and IBM QRadar SIEM tools.
* Worked with security tools like Symantec DLP, Endpoint Protection, Encryption, Bluecoat Proxy, and syslogs.
* Led international encryption server projects as a Voltage secure data encryption engineer.
* Conducted vulnerability assessments and penetration testing to identify system vulnerabilities.
* Supported Tripwire application, assisted with Nessus, vulnerability management, and compliance.
* Led a cloud security engineering team, executed complex solutions, and delivered projects.
* Adopted and taught best cloud security engineering practices.
* Spearheaded cloud migration strategies, focusing on the transition to Azure and AWS platforms, ensuring seamless integration and robust security.
* Developed and maintained documentation for IAM configurations and procedures, ensuring clarity and consistency across the organization.
* Conduct Information System Audit (Security Control Assessment) and Security Authorization (SA) using NIST Risk Management Framework SP 800-37 guide.
* Performed internal network vulnerability assessments to enhance security culture.
* Utilized frameworks like ISO 27001, PCI DSS, OWASP, SANS, and Forcepoint.
* Monitored and researched cyber threats impacting the organization.
* Specialized in data loss prevention and large infrastructure encryption.
* Developed cloud security environment architectures and proof of concepts.
* Architected, implemented, and supported cloud-based infrastructure and solutions.
* Managed repeated threats and conducted vulnerability tests across systems.
* Designed and implemented solutions to protect sensitive data and strengthen data protection.
* Supported IT teams with risk remediation, including VBlock infrastructure vulnerability remediation.
* Integrated Splunk with ServiceNow, Active Directory, and LDAP.
* Managed Splunk instances, analyzed security events, risks, and reporting using Splunk Deployment Server.
* Created comprehensive documentation and diagrams for knowledge sharing.
* Assisted with Splunk dashboards, use cases, technical services, and data queries.
* Worked with NERC CIP, Tripwire, Tenable, and IP360 Enterprise 8.6.
* Developed and implemented NIST-based cyber security standards to reduce IT asset vulnerabilities.
* Tracked and ensured compliance with information assurance initiatives, vulnerability assessments, and security policies.
* Managed various industry-standard security tools like SIEM, IPS, CASB, firewalls, and endpoint managers.
* Supported Symantec Endpoint Protection 12.1 installation, configuration, and management.
* Automated centralized vulnerability detection with scripts for tools like ArcSight and Splunk.
* Performed problem identification, resolution, monitoring, and capacity planning for cloud infrastructure.
* Conducted network vulnerability scans quarterly or after significant changes.
* Analyzed vulnerabilities using Nessus and Qualys Guard, removing false positives before reporting.
* Utilized SIEM, IDS/IPS, DLP, PIA, Forcepoint, forensics, sniffers, and malware analysis tools.

**Target, Minneapolis, MN Aug 2016 to Nov 2018**

**Product Security Engineer**

**Responsibilities:**

* Performed manual penetration testing of applications and APIs to identify OWASP Top 10 and SANS 25 vulnerabilities.
* Trained development teams on secure coding practices.
* Trained teams on security requirements, threat modeling, and security testing to improve SDLC and achieve secure SDLC.
* Conducted black box penetration testing on internet and intranet-facing applications.
* Identified OWASP Top 10 issues like SQLi, CSRF, and XSS.
* Performed static code analysis using HP Fortify to identify vulnerabilities in applications.
* Utilized tools like Burp Suite, Dirbuster, HP Fortify, and Nmap for assessments.
* Conducted security code reviews for Java, .NET, and PHP using HP Fortify and IBM AppScan, and helped teams remediate issues.
* Designed and implemented secure cloud architectures for platforms such as AWS, Azure, and Google Cloud, ensuring robust protection of data and applications.
* Prepared risk registries for various projects.
* Provided details on identified issues and remediation plans to stakeholders.
* Conducted grey box testing of applications.
* Participated in client interviews to determine the Security posture of the System and to assist in the completion of the Security Assessment Plan using NIST SP 800-53A test required to maintain Company Authorization to Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization
* Verified existing controls for least privilege, separation of duties, and job rotation.
* Provided insights on separating client data and securing PII during a major company merger.
* Identified application vulnerabilities using proxies like Burp Suite to validate server-side validations.
* Identified issues related to session management, input validations, output encoding, logging, exceptions, cookie attributes, encryption, and privilege escalations.
* Executed and crafted payloads to attack systems and execute XSS and other attacks.
* Used SQL map to dump database data locally.

**Client: Zensar Technologies, Pune, India Apr 2015 to Feb 2016**

**Position: Cyber Security Analyst**

**Responsibilities:**

* Performed vulnerability assessments of Java and .NET web-based applications using Burp Suite and HP Web Inspect.
* Conducted web application vulnerability assessments, threat modeling, and secure code reviews.
* Performed network vulnerability assessments using tools to evaluate attack vectors, identify vulnerabilities, and develop remediation plans and security procedures.
* Conducted automated web application security testing using Checkmarx, HP WebInspect, Fortify, and Burp.
* Configured and used tools like SSO, Fortify, Checkmarx, and App Scan for web and mobile application testing and issue remediation.
* Captured and analyzed network traffic at all OSI layers, monitored security of critical systems (email, database, web, and application servers).
* Worked with operational security tools and practices like IDS, firewalls, and third-party security products.
* Proactively monitored blogs and blocked malicious IPs/URLs at the organization level.
* Responsible for security outbreak incident reports and post-incident response reports.
* Performed effective security event monitoring and log analysis from various security controls like Websense, IDS/IPS, and firewalls.
* Managed compliance of network devices and configurations according to standard build procedures.
* Demonstrated knowledge of system and network security, log analysis, and intrusion detection technologies.
* Provided 24/7 computer network security auditing and fraud, waste, and abuse detection for government agency customers.
* Maintained technical knowledge and troubleshooting skills for supported application and network security products and services.
* Tracked incidents until closure, coordinated with teams for resolution and reporting.
* Monitored bandwidth utilization of links and used monitoring tools for network systems.
* Experienced in maintaining IP addressing and subnetting, wireless router configuration, email verification for phishing, and solving end-user security issues.
* Stayed up to date with information security news, techniques, and trends.

**Client: HashedIn, Bangalore, India Oct 2014 to Mar 2015**

**Position: Security Engineer**

**Responsibilities:**

* Black box pen testing on internet and intranet-facing applications
* OWASP Top 10 Issues identifications like SQLi, CSRF, and XSS
* Preparation of risk registry for the various projects in the client
* Training the development team on secure coding practices
* Providing details of the issues identified and the remediation plan to the stakeholders
* Gray Box testing of the applications.
* Identified hidden files using dirbuster.
* Worked on DOM-based XSS manually.
* Worked on Directory Traversal attacks manually
* Implemented Agile methodology to follow the workflow process.