Srikanth

 Secsrikanth@gmail.com                        5103580649

**CAREER OBJECTIVE**



To obtain a role of a Senior Security Engineer and to apply solid information technology background and 10 years' experience in vulnerability management, threat hunting & intelligence, risk assessment, incident response, security analytics, application security, scripting and networking design coupled with good communication skills.Total 8 Years of diverse experience in Information Technology with 3 years of Quality Assurance and 5 years of experience in Security Domain.

**EXPERIENCE**



**Security Engineer**

**HSN-Pennsylvania Oct 2021 - Present**

**Security Engineer**

**Experience:**

* Extensive experience in architecting and securing GitHub and GitLab repositories, implementing access controls, and ensuring code integrity throughout the CI/CD pipelines.
* Proficient in designing and implementing robust automation pipelines for security testing, vulnerability scanning, and code analysis in GitHub, GitLab, and AWS environments.
* Demonstrated expertise in configuring and managing security tools and services on AWS, including AWS Identity and Access Management (IAM), AWS Config, AWS CloudTrail, and AWS Security Hub.
* Developed and maintained automated security and compliance checks for AWS infrastructure, ensuring adherence to industry standards and regulatory requirements.
* Implemented Infrastructure as Code (IaC) principles using tools like Terraform or CloudFormation to automate the deployment and configuration of secure AWS environments.
* Led security incident response activities, leveraging automation to rapidly detect, contain, and mitigate security breaches in GitHub, GitLab, and AWS platforms.
* Conducted security assessments and audits of CI/CD pipelines and infrastructure, identifying and remediating security vulnerabilities and weaknesses.
* Collaborated with development and operations teams to integrate security into the software development lifecycle (SDLC) through automated security testing and code reviews.
* Implemented Continuous Integration (CI) and Continuous Deployment (CD) practices, automating the secure and efficient delivery of software applications.
* Led security training sessions for development teams, promoting security awareness and best practices for secure coding and infrastructure management in GitHub, GitLab, and AWS.
* Maintained up-to-date knowledge of security trends, best practices, and emerging technologies to proactively enhance security measures and infrastructure.
* Participated in security risk assessments and provided recommendations to enhance the overall security posture of the organization's GitHub, GitLab, and AWS environments.
* Implemented encryption and data protection mechanisms for sensitive data stored in GitHub, GitLab repositories, and AWS infrastructure.
* Worked closely with stakeholders to define security requirements, design secure architectures, and ensure compliance with security policies and standards in GitHub, GitLab, and AWS deployments.
* Actively contributed to the development and improvement of security-related documentation, standard operating procedures, and incident response plans.
* Orchestrated development teams within an agile development process to fix security issues identified in largescale user-facing web applications.
* Lead and mentored developers in utilize secure development techniques and libraries.
* Collaborated with a team of architects and developers, operational leads and functional owners to plan and implement security technical features.
* Coordinated with application development teams to assess the security posture of applications.
* Provided security recommendations as a subject matter expert for development teams during all phases of development.
* Performed static/dynamic code testing, manual code inspection, threat modeling, design reviews and penetration testing of internal web applications and external partner applications to identify vulnerabilities and security defects.
* Designed, implement, and maintain Mimecast's email security infrastructure to protect against threats.
* Configured and optimize Mimecast's security policies, including email filtering rules and threat detection settings.
* Monitored the performance and effectiveness of Mimecast's security solutions, making adjustments as needed.
* Worked with cross-functional teams to integrate Mimecast with other security tools and systems.
* Developed new automation and tooling to improve our detection and prevention capabilities and evaluated application security tools for internal consumption.
* Implemented and automated full CI/CD pipelines (SAST and DAST) so that each commit a developer makes will go through standard process of software lifecycle and gets tested well enough before it can make it to the production.
* Performed the risk analysis and write-ups for the critical & high vulnerabilities related to Network and web applications.
* Investigated potential or actual security violations or incidents in effort to identify issues and areas that require new security measures or policy change.
* Vulnerability management; Scanning and Assessments to identify risks with tools including Tenable Cloud and Security Center, Axonius, CrowdStrike and Splunk.
* Responsible for identifying and classifying cyber security vulnerabilities and work on mitigation plans with system owners, ensure plans are documented understood and track the results of the plan execution.
* Provided support, investigated, documented, and performed investigations of incidents that occur in client-facing and corporate environments.
* Maintain and update information security policies and standards and enhance internal security processes, programs and procedures.
* Lead the organization follow secure development practices such as OWASP Top 10, NIST, SANS 25, SOC2, ISO 27001 and ISO 27002.
* Extensive expertise in SAML, OAuth, and Kerberos authentication protocols, implementing and managing secure single sign-on (SSO) solutions for enterprise applications.
* Proficient in secure software development lifecycle (SSDLC) methodology, ensuring that security is integrated into every phase of the software development process.
* Skilled in utilizing Burp Suite and other industry-leading tools for vulnerability assessment, penetration testing, and identifying security weaknesses in applications and systems.
* Strong understanding of GDPR (General Data Protection Regulation) compliance requirements, including data protection principles, privacy by design, and consent management.
* Familiarity with NIST 800-53 security controls framework, implementing and maintaining security controls to protect systems and data from various threats and vulnerabilities.
* Experienced in interpreting vendor SOC 2 (Service Organization Control 2) information, assessing the security posture of third-party vendors and ensuring compliance with relevant security standards.
* Proven track record in driving SOC 2 compliance initiatives, collaborating with cross-functional teams to establish and maintain robust security controls, policies, and procedures.
* Knowledgeable in conducting risk assessments, threat modeling, and security audits to identify potential security gaps and develop mitigation strategies.
* Strong problem-solving and incident response skills, effectively mitigating security incidents and leading investigations to determine root causes and implement appropriate remediation measures.
* Excellent communication and interpersonal skills, adept at conveying complex security concepts to both technical and non-technical stakeholders and fostering a culture of security awareness within the organization.
* Developed threat models, security controls, threat analysis, creation of risk control matrices and risk mitigation strategies.
* Designed, build and deploy automation to scale infrastructure vulnerability discovery efforts.
* Secured the operations of organization by responding to security alerts, RCA of the problem, and security incident management support.
* Managing all aspects of an organization's information security system, including researching, testing, training and implementing programs designed to safeguard sensitive information from any possible breaches.
* Research new threats, attacks and vulnerabilities that may affect the organization computing environment to learn how to identify and react to them.
* Act as key contributor in the Cybersecurity Incident Response Team's growth and evolution, actively improving our cyber incident response capability.
* Monitoring, operating, and supporting network security devices and applications (firewalls, intrusion detection/intrusion prevention, authentication, content filtering, enterprise security management, VPN, etc.) to include any modifications to the firewall rule-set, intrusions prevention signatures, monitoring of security logs, anti-virus/spyware, Internet proxy, operating system hardening (Microsoft and Linux), Active-Directory security, and incident response.
* In-depth technical, operational and all application layers experience in AWS, Azure and GCP.
* Performing Level 1, Level 2 and Level 3 computer security incident response activities including coordinating with Teams, Business Leaders and Stake holders.
* Analyzing and triaging anomalies to ensure appropriate identification of risk to the organization.
* Coordinating incident response efforts including working with I.T., Business Leaders, and Third Parties to mitigate the impact of the risk.
* Postmortem analysis of incidents reports and methodology and results of investigation.
* CrowdStrike Falcon – Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Cyber Threat Intelligence and Threat Hunting.
* Daily monitoring, threat assessment, mitigation, and reporting activities to safeguard assets.
* Conducting active real-time security monitoring.
* Security event detection, triage, and threat analysis for complex and/or escalated security events.
* LogScale (Humio)– SEIM, Log Management and Monitoring
  + Assist in the creation of an end-to-end technology strategy for SIEM to address current and future security concerns, emerging threats, regulatory compliance and alignment with technology and the business.
  + Integrated multiple data feeds from local network devices and forwarded into Humio via Falcon Log Scale Collector and seamless integrations via API for analysis.
  + Perform assessment and security evaluation for systems, network and perimeter controls, log and event correlation, and system and network component baselining.
  + Triage of escalated security events that require in depth review and analysis, including ability to troubleshoot an event, research the potential cause, and recommend a course of action
* Proofpoint – Email Protection and Defense
  + Administering security policy on various email exchange.
  + Identifying and remediating phishing/impersonation attacks before, during, and after they happen.
  + Analysis & Validation of DMARC logs to recommend resolution for failing email.
* Proofpoint DLP- Data Loss Prevention
* Spearheaded the implementation and management of Proofpoint DLP solutions, safeguarding sensitive data and mitigating data breach risks.
* Led data discovery and classification initiatives, identifying and categorizing critical information assets across the organization.
* Developed and enforced comprehensive data loss prevention policies and procedures to ensure compliance with industry regulations and standards.
* Configured and monitored DLP rules, policies, and alerts, proactively identifying and responding to potential security incidents.
* Collaborated closely with cross-functional teams to integrate Proofpoint DLP into the existing security infrastructure, enhancing overall data protection measures.
* Conducted regular risk assessments and vulnerability scans, effectively identifying and addressing potential data leakage risks.
* Developed and delivered training programs to educate employees on data protection best practices and promote a strong security culture within the organization.
* Proofpoint ITM- Insider Threat Management
* Oversaw the implementation and maintenance of Proofpoint ITM solutions, ensuring the integrity and availability of critical information assets.
* Developed and enforced robust information security policies and standards, aligning with industry best practices and regulatory requirements.
* Conducted comprehensive risk assessments and audits to identify vulnerabilities, implementing effective security controls to mitigate risks.
* Managed security incidents and conducted forensic investigations to determine root causes, implementing timely remediation measures.
* Collaborated closely with IT teams to implement secure configurations, access controls, and encryption mechanisms to protect information assets.
* Conducted security awareness training sessions, fostering a culture of information security and compliance throughout the organization.
* Proofpoint CASB – Cloud Access Security Broker
* Led the deployment and management of Proofpoint CASB solutions, ensuring secure access and protecting cloud-based applications and services.
* Implemented access control policies, data encryption, and user authentication mechanisms, mitigating unauthorized access and data breaches.
* Monitored user activity, performed threat analysis, and implemented proactive measures to detect and prevent security incidents.
* Conducted assessments of cloud service providers, evaluating their security posture and compliance with industry standards.
* Integrated Proofpoint CASB solutions with existing security infrastructure, including SIEM systems, enhancing overall security monitoring and response capabilities.
* Provided strategic recommendations and guidance to stakeholders on cloud security best practices and risk mitigation strategies.
* Zscaler – Zero Trust Exchange |ZPA|ZIA|ZCC|ZDX
  + Technical subject matter expert in implementing, understanding, articulating and evangelizing the Zscaler approach to transforming the way users access private applications and the Internet.
  + Participating in all phases of the product development cycle, from requirements, design, through implementation and test.
  + Managing and enhancing Zscaler Internet Access (ZIA) , Zscaler Private Access (ZPA) & Zscaler digital experience (ZDX) Admin portals.
  + Implemented and administering Firewall policies, Web filtering policies, SSL Decryption policies, Access Policies.
  + Configuration and Troubleshooting user, application and IT security connectivity issues.
  + Maintaining detailed records of customer interaction and problem resolution in a ticketing system.
  + Troubleshooting complex connectivity issues involving multiple firewalls, IPS and load balancer and VPN devices.
  + Delivering 24\*7 support to enterprise users with multiple time zone in a large enterprise environment.
  + Assisting other team members in troubleshooting and project efforts.
  + Develop standard operating procedure and network topology documentation.
  + Provide on-call and afterhours support as required.
* Axonius - cybersecurity asset management platform
  + Identified and implemented methods to scale and automate product maintenance, management of core platform, and analytics.
  + Technical subject matter expert in the Axonius platform and its integrations, and continuously maintaining the operations.
* Splunk – SEIM and Operational Intelligence
  + Maintaining Splunk log ingestion and dashboards for team use cases; update dashboards based on new requirements.
  + Developed security-focused content for Splunk, including creation of complex threat detection logic and operational dashboards.
* SAST and DAST –
  + Expertise in Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) methodologies.
  + Proficient in using Checkmarx and GitLab to perform comprehensive security assessments of software applications.
  + Extensive experience in configuring and utilizing Checkmarx and GitLab to identify and mitigate security vulnerabilities in code.
  + Skilled in analyzing application source code using Checkmarx's SAST capabilities to identify potential security weaknesses, such as SQL injection, cross-site scripting (XSS), and insecure API usage.
  + Demonstrated ability to interpret Checkmarx scan results and provide actionable recommendations for code remediation and secure coding practices.
  + Proficient in executing DAST scans through GitLab to simulate real-world attack scenarios and identify vulnerabilities related to authentication, authorization, and input validation.
  + Strong understanding of application security best practices, secure coding guidelines, and industry-standard security frameworks (e.g., OWASP Top Ten).
  + Experience in integrating Checkmarx and GitLab into the software development lifecycle (SDLC) to ensure continuous security testing and vulnerability management.
  + Skilled in collaborating with development teams to prioritize and remediate security issues identified by SAST and DAST scans.
  + Proven track record of successfully enhancing application security posture by leveraging SAST and DAST capabilities in Checkmarx and GitLab.
  + Excellent problem-solving and analytical skills, with the ability to identify and address security gaps proactively.
  + Strong communication skills, including the ability to effectively communicate complex security concepts and recommendations to technical and non-technical stakeholders.

**Security Engineer**

**Matson, Inc. Oakland, California,Jul 2020 - Sep 2021**

**Responsibilities:**

* Experience in Implementation, installation and maintenance of CyberArk 10.3 Privileged Account Security (PAS) suite and established connections to Windows, Data bases and Linux servers.
* Experience in CyberArk PAS suite which includes Enterprise Password Vault, Password Vault Web Access, Central Policy Manager, Privileged Session Manager, Proxy and PACLI.
* Managed CyberArk Security that offers wide range of services and support including implementation, consulting, training, maintenance, online support and vault.
* Enabled services and applications with ADFS and SAML SSO.
* Design, Implement and troubleshoot Layer 7 application API Gateways for Company wide application services.
* Gathering technical requirements and worked as primary point of contact for American Home Shield CyberArk's Operations and Maintenance Tasks.
* General Managing of Cyber-Ark Security that offers any enterprise a wide range of services and support options to making digital vault solution a success; these services include implementation, consulting, training, maintenance, online support and vault scripting, SIEM, and Digital Certification supporting.
* Provided solutions to remediations for security issues and vulnerabilities identified during assessments.
* Conducted research on and maintain proficiency in computer network exploitation, tools, techniques, countermeasures, and trends in computer network vulnerabilities, network security, and encryption.
* Prepared audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions for standards such as PCI, ISO 27001.
* Developed a continuous monitoring approach to regularly measure and report the status of the following control areas: patching, hardening, audit and log config, authentication mechanisms.
* Responsible for identifying and classifying cyber security vulnerabilities and work on mitigation plans with system owners, ensure plans are documented understood and track the results of the plan execution.
* Hands on experience in information security hardening guidelines such as CIS or DoD guidelines and industry standard scoring models such as CVSS, CCSS.
* Planning, Conducting and reporting Vulnerability and risk assessment of applications.
* Risk associated with vulnerability explained to the project team for better understanding and guiding project team towards its closure and remediation.
* Provided guidance to all engineering teams regarding secure web application development best practices.
* Familiar with OWASP Application Security Verification Standard (ASVS) and how it applies securely to application development teams.
* Integrated and automated scripts web application security-related tools such as Checkmarx, Nessus security center and cloud Tenable.
* Collect application vulnerability metrics and introduce automated security checks into application build continuous integration and continuous development (CICD)process.
* Documented secure coding guidelines and run training programs to assist internal development personnel and teams.
* Maintain and update information security policies and standards and enhance internal security processes, programs and procedures.
* Work closely with the development teams within an agile development process to fix security issues identified in largescale user-facing web applications.
* Proficient in creating and customizing SAST and DAST scan configurations in Checkmarx and GitLab to align with specific project requirements and security standards.
* Skilled in setting up continuous integration and continuous deployment (CI/CD) pipelines in GitLab to automate SAST and DAST scans as part of the development workflow.
* Experience in leveraging Checkmarx and GitLab APIs to automate scan initiation, retrieve scan results, and integrate security findings into other tools or systems.
* Familiarity with advanced SAST features in Checkmarx, such as taint analysis, data flow analysis, and control flow analysis, to uncover complex security vulnerabilities.
* Proficient in conducting secure code reviews and providing guidance to development teams based on Checkmarx scan findings and industry best practices.
* Experienced in triaging and prioritizing security findings from SAST and DAST scans to address the most critical vulnerabilities first.
* Knowledgeable about integrating Checkmarx and GitLab with issue tracking systems, such as Jira or Bugzilla, to ensure efficient vulnerability tracking and remediation.
* Proven ability to perform manual security testing in conjunction with SAST and DAST scans to uncover vulnerabilities that automated tools might miss.
* Skilled in creating comprehensive reports and executive summaries based on Checkmarx and GitLab scan results to communicate security posture and progress to management.
* Stay up-to-date with the latest trends, techniques, and tools in application security, particularly in the context of SAST, DAST, Checkmarx, and GitLab

**Information Security Analyst**

**Green Dot Corporation/ Pasadena,CA May 2019 - Jun 2020**

* Created cyber security policies for organizations to follow and remediate vulnerabilities, to avoid threats, to keep their users, systems, data safe and to comply with different security standards like NIST 800-53, IST 800-171, FFIEC and HIPAA.
* Implementation of Multi-Factor Authentication mechanisms, Replay Resistant mechanisms, SIEM tools, IDS/IPS, Firewalls and other methods in organizations to help them comply with NIST, FFIEC and various other standards.
* Conducted system security assessments based on NIST standards using CSET 8.0.
* Generated security documentation including security assessment reports, system security plans, contingency plans and disaster recovery plans.
* Provided security support and evaluation to development teams to integrate information assurance/security throughout the System Life Cycle Development of major and minor applications.

**QA Analyst**

**BCBS of North Carolina, RDU,Jan 2018 - Apr 2019**

**Responsibilities:**

* Performed Smoke, Integration and Regression test based on analysis and understanding of the requirements and end user needs.
* Involved in development of Test Plan, Test Cases based on user requirement specifications.
* Coordinated with application engineers and prepared test cases and ensured all software applications are compatible with tests
* Participating in the design review, requirement analysis and Agile meetings
* Coordinating Acceptance testing processes documented and address all the issues during the testing
* Involved in implementation of Test Automation Framework build like Data Driven, BDD Framework using Selenium WebDriver, TestNG, Cucumber.
* Designed automated testing Scripts using Javain Selenium WebDriver in Eclipse IDE for functional testing.
* Developed Test Scripts and running test scripts on different browsers using Selenium Web driver, TestNG.
* Logged and managed defects using IBM Rational Quality Manager.
* Developed and execute SQL queries to verify the proper insertion, updates into database.
* Used SOAP UI tool to test SOA based architecture application to test SOAP services and REST API.
* Worked on distributed test automation execution on different environment as part of Continuous Integration Process using Selenium Web driver and Jenkins for nighty batch run of scripts.
* Integrated the test suites to Jenkins to execute them automatically after every successful deployment.
* Prepared user documentation with screenshots for UAT (User Acceptance testing).

**Quality Analyst**

**Integra Technologies, India June2014 - Dec 2015**

* Developed Test Cases and Procedures based on User requirement specifications and System requirement specifications.
* Involved in Performing Functional testing, Regression testing, System testing, Integration testing, Security testing, Configuration testing, GUI testing and User Acceptance testing.
* Setup and Configured the testing environment with Eclipse, TestNG, Selenium WebDriver and Selenium Java Driver.
* Identified test cases to automate. Automate those test cases using Selenium WebDriver, TestNG and Java(Eclipse IDE)
* Written and executed Selenium tests for automation testing of the web application using Selenium IDE and WebDriver.
* Created user defined functions in Java and implemented the functionality with Selenium.
* Implemented assertions, error collector functionalities for better validation using TestNG.
* Involved in the Continuous Integration of the automation framework with Jenkins.
* Created Test plan, High level scenarios, test case construction and test estimates, resource estimates and weekly status reports.
* Responsible for implementation of Hybrid Test Automation Framework build using Selenium WebDriver,TestNG and Maven technologies under Java platform.
* Developed automated tests for continuous regression testing and reducing manual testing using Selenium,TestNG and Maven.
* Designed and developed Page Objects using Page Object Design Pattern and Selenium WebDriver.
* Integrated Automation scripts (Selenium WebDriver API) in Continuous Integration tools (Jenkins) for nightly batch runs of the Script.
* Used Selenium WebDriver for writing test scripts for regression test coverage.
* Used Xpath and DOM to work with dynamic and static objects in Selenium.
* Executed the Test Cases to verify actual results to expected results.
* Designed and developed test structure for web services to validate API calls using SOAP UI.
* Used SOAP UI tool, to create a Web Service Test from SOAP request and validate the response against the database.

**EDUCATION**

**Wilmington University, *New Castle, DE, USA***

* Master of Science in Information Assurance (Dec 2017)

**Krishna University, *Vijayawada,Andhra pradesh,India,***

* Bachelor of Science in Electronics and Communications Engineering (Jul 2014)

**ADDITIONAL SKILLS**



* Email Protection
* Secure SDLC Development
* Vulnerability Management
* Threat Modeling, Threat Intelligence, Threat Hunting and Risk Assessment
* Incident Handling and Response
* PCI DSS, NIST, OWASP Top10, SOX, ISO 27001 and ISO 27002 frameworks.
* Automation expertise with scripting languages (e.g. PowerShell/Python
* Quick Learner
* Endpoint Security
* Administration & Management
* Automation Framework:Selenium WebDriver, Selenium IDE, Cucumber-Gherkins, Specflow,Calabash, TestNG, Maven.
* Testing Tools:QTP/UFT, JMeter, Postman, Load Runner, Rational Test Manager, Jenkins.
* Version Controls:CVS, TFS and Visual Source Safe , GIThub.