Security Engineer Security Engineer Security Engineer - Walgreens Boot Alliance Vernon Hills, IL Performance-driven Information Security professional with six years of combined experience in IT/ Infrastructure management and Cyber security space. Strong knowledge and exposure to various IT security frameworks, governance, vulnerability management, Operational security best practices, tools and methodologies   As security QA in Walgreens Boot Alliance, Involved in various security capability implementations, where sensitive ePHI Data is not meant to be exposed following HIPPA compliance making applications & infrastructure are non vulnerable   As Security Analyst at AT&T, Ethical Hacking is my primary area of responsibility securing the IF, PCI,SPI corporate applications and preventing fraud.   Experience in detecting - SQL injection, XML injection, techniques to obtain command prompts on the servers, PDF exploits, HTTP response splitting attacks, CSRF, web services vulnerabilities, Anonymity (TOR) traffic identification - DOS pattern identification using Artificial Intelligence algorithms etc.   Sound knowledge and industry experience in Vulnerability Assessment and Penetration Testing on WEB based Applications, mobile based application and Infrastructure penetration testing.   Extensive knowledge in Emergency Response planning, operations, training, and management.   Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools.   Developed secure coding standards that are based on industry-accepted best practices, such as OWASP Guide, SANS CWE Top 25, or CERT Secure Coding, to address common coding vulnerabilities.   Respond and assist in information and cyber security assessment requests. Communicate and coordinate with business area stakeholders. Interface and participate with business and technical teams on cyber security architecture discussions.   Proven experience in manual/automated security testing, secure code review of web and mobile applications.   Provide detailed mobile apps security test reports highlighting possible vulnerabilities and security fixes.   Experience as an Information Security Analyst, involved in OWASP Top 10 based Vulnerability Assessment of various internets facing point of sale web applications and Web services.   Extensive experience in Penetration testing - Expertise in detecting various vulnerabilities (including OWASP top 10) comprised over authentication, authorization, input validation, session management, server configuration, cryptography, information leakage areas.   Experience on vulnerability assessment and penetration testing using various tools like Burp Suite, DirBuster, OWASP ZAP Proxy, NMap, Nessus, Kali Linux, Metasploit, HP Web inspect and IBM Appscan.   Hands on experience with IBM QRadar Security Intelligence Platform. I can collect, analyze, and archive security event logs and identify security threats and implement solutions.   Experienced with Symantec DLP Policies (DLP templates) compliance and regulation standards such as SOX, PCI, and HIPAA   Strong Knowledge of Security features like AAA (authentication, authorization, Auditing), Encryption, Decryption, Digital Signatures, Secure Socket Layer (SSL) Profiles, Single Sign-On, html forms and OAuth , Multi factor authentication etc.   Experience in working with C,C++,C#,.Net, Java, JavaScript, UNIX , J2EE, XML and Objective C Software teams and try to solve the errors in order to reduce Flaws.   An enthusiastic team player who embodies a strong work ethic and a leader who utilizes complex problem solving skills for incident analysis.   As a Security Consultant involved in enhancing the security stature of the project by initiatives like Threat Modeling, Security awareness sessions, Dormant & Never Logged IDs clean-up.   Good knowledge on Threat Analysis and Threat modeling of the application using STRIDE and DREAD models.   Excellent communication, analytical, troubleshooting, customer service and problem solving skills; excels in mission-critical environments requiring advanced decision-making.   Developed testing practices, training plan and trained new members in penetration test duties.   Developed remediation plans for various vulnerabilities and assisted development teams across the organization in remediating them. Work Experience Security Engineer Walgreens Boot Alliance - Deerfield, IL August 2018 to Present Working on a new project "RxRenewal" which includes various applications where the flow involves from patient entry to a pharmacy store with erx prescription till the labelling & billing is done. The flow includes the Erx prescription, Manual Refill, Supply chain Management, Drug inventories, Stock adjustments, Adjudication(with external partners), Labeling etc. The whole program is getting redeveloped writing the code from the scratch, building infrastructure, various Microservice modules, Kubernetis, Multiple deployments in Microsoft Azure. My role as a Security QA, involve in implementation of

Various security capabilities: Login Authentication - Via Enterprise IDP Keycloak Implementation - Assigning pharmacy Roles APIM Implementation Microservice Authorizations HP Voltage - Encryption & Decryption Single SignOn between multiple clients BFF Service Vulnerabilty Tests: Application Source code scans - Veracode Infrastructure scans - Twistlock Kafka Authentications Kerberos Authentications Azure Keyvault VDI Implementations Performed POC's for Encryption and Decryption of sensitive fields at each microservice level and verify any sensitive data leakage happening at any point. Automating the SAST tool Veracode with Jira and make sure the developers run scans on their own and can fix the vulnerabilities upfront. As following the Agile Methodology, Supporting all the lower test environments like DEV, QE, SIT, UAT, E2E & Perf with the implementation of the security capabilities and supporting the qe testers with the backend flows. Worked on Keycloak tool assigning Roles and permissions to the pharmacy roles providing Single sign on linking Identity access management (Ping Federate) with RxMs and IC+. Troubleshooting the Authentication and authorization issues if any discrepancies occurs regarding the access of applications, verifying the access tokens and Jwt tokens. Retesting the SQL injection vulnerabilities and XSS vulnerabilities when once ASVM teams have worked on them to analyze the false positives Supporting for VDI implementations in offshore in Italy, Naples etc for the usage of the applications based on profiles and also the sensitive and non sensitive environments. Keep tracking the vulnerabilities as per the severity and making sure they are getting fixed with in the Timelines as per the ASVM standards. Involved in the Design phase discussions of Key rotations and batch utility for encryption, performing the POC, notifying the changes happened in the performance of the end to end flow of the application. Working on the Global login and logout strategies for the users which needs to be implemented across all over the 10k stores in US with having different roles. Implementing Authentication and Authorization from the Client app to the Cloud infrastructure mapping through LDaps and various scenarios Include Product owners in test cases review meeting to make sure the requirements are understood correctly and valid test cases are written to validate the functionalities Execute the automated test scripts and generate the test report with the percentage of passed, failed and skipped test cases along with the screenshots of failed test cases Email the test reports to all stake holders to keep them updated with the latest status of the development Implementation of Field Level Encryption between End to End App flows, Microservices to Microservices and Microservices to external engines. Use Authentication APIs to access the Microservices which is in AZZURE environment include SQL queries to validate the data integrity in data bases Working on the applications like Stock managements and Adjudication process, involves the external partners which have to be encrypted until our end and gets automatically gets decrypted when passing the data to the external agents Working for erx application which involves the prescriber prescription getting stored in our Rx Database through the third party using Sure scriots. Manually verifying the Raw source code in Kafka through an Optimus tool for writing queries. Creation of test users for all the IC+ stores and providing to the required users and automated the script for the users to make them on their own. Researching the existing technologies for finding any possible threats and sharing my view with the management for the risk potential and also the options for remediations. Regular assistance for the Developers for fixing the Veracode & Pentesting vulnerabilities and providing possible guidelines for understanding the concepts of OWASP top 10. Alerting all the lower environemnts about the new deployments of code base added security capabilities to the new and existing applications coordinating with Devops for deploying in Kubernetes. Security Analyst AT&T Labs - Middletown, NJ December 2016 to August 2018 Responsibilities Working as Security Analyst at AT&T involved in performing Dynamic and Static Application Security Testing (SAST & DAST). Static code Scans on java and .net applications using HP Fortify tool and Analyzing vulnerabilities to identify false positives, providing remediation's to the App teams. Performing Dynamic scans using HP Web inspect for finding the security vulnerabilities (Configured Web Inspect Scans for vulnerabilities and manual Pen-Tests). Performing Manual Penetration tests(Light) for the applications which are Internet Facing, PCI and SPI using Burp Proxy Automated Fortify tool with Jenkins plugin on Linux machines to perform Static scans by the App Team Developers as many times they need to make sure they are fixing the code while they are developing and make sure the app gets vulnerable free. Conducting Light Manual Pen tests includes Injection Attacks, Broken Authentication and Session

Management, finding security Misconfigurations and to check any Sensitive Data Exposure. Performing Manual Pen test for gaining Unauthorized access to the systems to steal Confidential data like Client Information, Business logics, and the Server Versions Documented findings, observations, provide remediation recommendations and draft a comprehensive written Pen test report for end clients. Working with CSO Teams and App teams for the vulnerabilities which we can't fix and recorded as Known Vulnerabilities and filing TSS Exceptions. Remediated security vulnerabilities which are reported by fortify like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Broken Authentication and Session Management, SQL Injection, Session Timeout and Header Manipulation. Have worked with a team of individuals dedicated for conducting research, attack detection and build mitigation techniques for threats posed in network and application layers. Perform peer reviews of Security Assessment Reports and Involved in requirement gathering and outlining. Compiler warnings are triaged and fixed prior to code check-in for each development phase. Database Auditing encompasses Oracle, MS SQL, MySQL and LDAP. Web server configurations include IIS and Apache. Developed customized-built tools for auditing using perl, C and shell scripting. Utilized Identity Access Management ("IAM") software for audit reports, user requests for adding/removing access. Involved in testing the applications for the Functionality and Database Testing with manual testing and performed black box testing such as Functional, Integration, UAT and Regression. Reviews latest patch releases to identify the risks of delaying patch application and to identify possible alternative mitigations. Assist developers in remediating issues with Security Assessments with respect to OWASP standards and as per fortify recommendation. Perform security reviews of application designs, source code and deployments as required, covering all types of applications (web application, web services, mobile applications) and Performing Vulnerability assessments using Qualysguard and Nessus scanner. Report deliverables and security signoff on time to the Project teams before going into the Deployment. Providing the vulnerability metrics to the application team of each on the severity of Critical, High, Medium, Low, where the security test of application is based on Categorization of SEV1, SEV2, SEV3, SEV4 and SEV5. Communicated technical application security concepts to application teams once the fortify scan reports are generated. Regularly performed research to identify potential vulnerabilities in and threats to existing technologies, and provided timely, clear, technically accurate notification to management of the risk potential and options for remediation. Cyber security & Infrastructure engineer Kohls - Milwaukee, WI June 2015 to November 2016 Performed application and infrastructure penetration tests, as well as physical security review and social engineering tests for our global clients. Review and define requirements for information security solutions and performed vulnerability scans with Qualys vulnerability scanner. Used IBM AppScan to test websites for vulnerabilities and reviewed source code and developed security filters within AppScan for critical applications. Administered software applications by identification of security malfunctions using Sqlmap, Burpsuite and other tools. Scanned web and mobile applications prior to deployment using AppScan to identify security vulnerabilities and generated reports and fixed recommendations. Produced associated cloud risk assessment framework utilizing industry best practices and open sources tools from the Cloud Security Alliance, Microsoft and others. Framework allows control category comparisons, gap analyses and asset value based compensating controls. Perform peer reviews of Security Assessment Reports and Involved in requirement gathering and outlining. Used Burp Suite, Dir-buster, Acunetix Automatic Scanner, AppScan Nessus, NMAP, SqlMap, and Nessus for web application penetration testing & infrastructure testing. Worked closely with software developers and DevOps to debug software and system problems. Researches and stays abreast of tools, techniques, countermeasures, and trends in computer network vulnerabilities Assessments. Conduct network vulnerability assessments using tools to evaluate attack vectors, identify system vulnerabilities and develop remediation plans and security procedures Vulnerability scanning for offenses and incorporate Network behavior Anomaly Detection with QRadar & Generating reports from QRadar that list magnitude of offenses and track them to mitigate vulnerabilities. Use QRadar to map out entire network to collect configuration data across several devices as well as see what devices are connected to the network at any given time. Configure QRadar to set rules manually or dynamically as well as trigger scans to detect further vulnerabilities. Produce vulnerability management reports based on current patch levels, vulnerability severity, PCI compliance standards, and malware risk levels Qualys. Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws etc. DLP Profile deployment report for detecting servers and Update DLP policies - Incident Analysis Perform security reviews of application designs, source code and deployments as required, covering all types of applications (web application, web services, mobile applications, thick client applications, SaaS). Work on improvements for provided security services, including the continuous enhancement of existing methodology material and supporting assets. Skilled using Burp Suite, NMAP, WebInspect, Kali Linux, CheckMarx, DirBuster , IBM appscan, for web application penetration tests. Responsible for performing static code analysis of application source code and ensure all the controls are covered in the checklist. Having review meetings on daily basis, Weekly & Monthly basis for software development i.e. relying on agile scrum development model. Generated and presented reports on Security Vulnerabilities to both internal and external customers. Security assessment of online applications to identify the vulnerabilities in different categories like Input and data Validation, Authentication, Authorization, Auditing & logging and providing fixes & filtering false findings for the vulnerabilities reported in the scan reports. Scan Networks, Servers, and other resources to validate compliance and security issues using numerous tools and conducted onsite penetration tests from an insider threat perspective Worked with Data Analysis team which is responsible for proactive monitoring of the STB's running on the RDK 2.X stack and find out the root cause of the defects identified with possible fix. To address and integrate Security in SDLC by following techniques like Threat Modeling, Risk Management, Logging, Penetration Testing, etc. Regularly performed research to identify potential vulnerabilities in and threats to existing technologies, and provided timely, clear, technically accurate notification to management of the risk potential and options for remediation. Network Security Engineer Genpact - Hyderabad, Telangana April 2012 to November 2013 Troubleshooting the L2 Network Issues and making sure the network traffic is stable 24/7 coordination with various teams all over the Client Locations. Explanation of the security requirements to the design team in initial stages of SDLC to minimize the efforts to rework on issues identified during Network Scans. Utilized Identity Access Management ("IAM") software for audit reports, user requests for adding/removing access. Created Functional Requirements and Use Cases for Identity management and Access Control projects in the Financial Services industry. Worked on troubleshooting for LDAP and SiteMinder issues with Support Teams for newer initiatives at organization level Perform peer reviews of Security Assessment Reports and Involved in requirement gathering and outlining. Works with engineers and application developers' groups to implement solutions for the company's LDAP services. Experienced with facilitating RSA authentication manager and RSA secureID token-based authentication systems. Performed quarterly and Ad-hoc (risk assessment) internal, external and web site scans using Rapid 7 toolset; Nexpose, AppSpider. Using various add on in Mozilla to assess the application like Wappalyzer, Flagfox, Live HTTP Header, cookie manager, Tamper data. Involved in a major merger activity of the company and provided insights in separation of different client data and securing PII Troubleshooting the network with the Packet capturing in Wireshark and resolving the issue using the filtering of the packet capture using TCP/IP filtering. Conducted an analytical analysis of client business processes and identified areas of risk to develop and implement comprehensive preventative strategies. Good knowledge on the Failing over of the Firewalls in the Active/ Standby Mode while configuring the Versions of Firewall's. SQLMap to dump the database data to the local folder Developed ontological and heuristic behavior frameworks for incident investigation and response. Many of my findings were implemented into a leading security platform. Updating of the checklist on weekly basis to ensure all the test cases are up to date as per the attacks happening in the market Creation of secure virtualized lab for exploit creation, malware distribution analysis and security product testing. System Administrator Wipro - Hyderabad, Telangana June 2010 to April 2012 Analyze, log, track and complex software and hardware matters of significance pertaining to networking connectivity issues, printer, server, and application to meet business needs. Provide network support for new application and device deployment; identify new connectivity requirements and develop solution. Build site to site VPN for remote locations and partner connections using Cisco Next Generation Firewalls. Actively involved in new store openings, closings, renovations, relocations, and technology lifecycle initiatives. Helped design and document troubleshooting techniques for Kerberos with the QA department. Planned, managed, and implemented a Wi-Fi deployment project to upgrade more than 1000 Cisco wireless access points; certified wireless coverage using Air Magnet wireless tool. Led the implementation of RSA SecurID for two factor authentication, as well as the deployment and support of Windows 2007 computers. Respond to network connectivity and regional data center outages; coordinate efforts with Service Desk, ISP provider; local tech and/or store personnel to restore network services. Configure\Deploy\Maintain Symantec DLP. Worked with Symantec DLP upgrades and patches. Handled the tasks of designing and planning LAN network expansion of the organization. Responsible for upgrading and configuring Microsoft Window servers. Monitor QRadar, a SIEM product, to identify any security violations. Handled the tasks of monitoring database and ensures security of stored data monitored the access of stored information in company databases. Managed computer/user accounts in Active Directory. Installed network routers, firewall and cabling. Responsible for preparing, loading, documenting and testing desktop and network developed applications for deployment, staff training, and inventory Managed computer/user accounts in Active Directory. Supported users in multiple branches with computer, network and desktop application software; image new PCs for new employees or reimage current; install printers to user profiles; map network drives; assist in user login and connectivity issues. Education Bachelors in Computer Science Engineering in Computer Science Engineering JNTU Skills Encryption, Pki, Rsa, Ssl, Database

Name: Kelly Frederick

Email: joel46@example.org

Phone: (754)732-1872