IT Security Specialist IT Security Specialist IT Security Specialist - Client - Northwestern Mutual Milwaukee, WI 5+ years of Information Security, design and development experience in information security architecture, Security Engineering Assessment, Vendor Information Protection, security assurance, threat modeling, Identity Access Management, risk remediation activities. Experience in conducting IT Security Assessments in accordance with NIST Special Publication 800-53 (Rev.4), FFIEC, 23 NYCRR 500 (NYDFS), NIST Cybersecurity Framework, HIPPA, PCI- DSS, ISO-72002 framework. Experience in creating Minimum Security Baselines and Enterprise Standards for the Identity Access Management as well as Mobile Device Management. Experience in Vendor Information Protection Plans, and evaluate third party services according to the enterprise standards, worked with the law department on Service Level and Master Level Agreement's Experience In creating Incident Response Plans, Business Continuity Plans /Disaster Recovery. Created an Enterprise standard for the Apple MAC Hardening for OS X 10.11, 10.12, 10.13 and mapped them with NIST.SP 800-179 & CIS Benchmarks. Expertise in Application Security and identifying and fixing OWASP Top 10 and SANS 25 security vulnerabilities. Strong foundation and In-depth technical knowledge of Identity Access Management, security engineering, computer and network security, authentication and security protocols. Hands-on with Penetration Testing, DAST, SAST and manual ethical hacking. Worked with global security teams performing application and IT infrastructure security assessments. Hands-on experience in developing threat models, security controls, threat analysis, the creation of risk control matrices and risk mitigation strategies. Working knowledge of Imperva and AWS Cloud Security in implementing Web Application Firewalls (WAF). Working knowledge of OWASP Top 10 and SANS Top 25 software guidelines, Federal Financial Institutions Examination Council's (FFIEC) regulations, NIST-CSF including Payment Card Industry (PCI-DSS), HIPAA and Sarbanes-Oxley Section404 (SOX). Experience in implementing Security Incident and Event Management System (SIEM) using HP ArcSight, Splunk. Work Experience IT Security Specialist Client - Northwestern Mutual - Milwaukee, WI January 2018 to Present Designed Security Engineering Assessment process based on NIST Special Publication 800-53 R4, NYDFS, HIPPA, PCI DSS and established the cross-team alignment process to make the process faster. Participated in the implementation of Privileged Access Management Tool CyberArk and vaulted all privileged access accounts into CyberArk which provided an extra layer of security to protect from the Insider Risk. Created an Enterprise standard for the Apple MAC Hardening for OS X 10.11, 10.12, 10.13 and mapped them with NIST.SP 800-179, CIS Benchmarks and created a checklist for the administrator. Performed Security Engineering assessment on Microsoft O365 environment including SharePoint Hybrid, Outlook, Yammer, Delve, OneDrive OneNote and worked with product owners given solutions to mitigate the findings. Tested Cloud Access Security Broker (CASB) Palo Alto Aperture for SaaS Solutions primary for Microsoft O365. Experience with Identity and Access Management (IAM) and development of user roles and policies for user access management. Worked extensively with G4S Company AMAG - Symmetry unified security platform which offers physical access & badge control, video management and visitor management. Implemented Hawkeye Harmony Mobile Building Evacuation application around all the Northwestern Mutual facilities from New York to Milwaukee WI. Planned and design infrastructure for automating VPC flow logs through kinesis into Splunk managed on AWS. Setup & Performed Security Engineering assessment according to the NIST 800-53 on CheckMarx SAST tool and successfully configured into GitLab & Jenkins CICD pipeline. Automated Splunk infrastructure for Logging and Monitoring team by through Kibana, Ansible, Kubernetes, Jenkins, and GitLab. Worked with more than 30 application teams to create a use case for logging & monitoring tools to capture security-related logs. Worked on automated ingestion of VPC flow logs, DNS query logs, S3 bucket logs from multiple AWS accounts through kinesis firehose into Splunk for monitoring and logging. Performed security design and architecture reviews for web and mobile applications which comes in day to day tasks. Worked on security engineering assessments of various technologies and mitigating the risks around it. Worked with application team to setup Confluent Kafka Enterprise as well as Confluent Cloud Kafka cloud, and given remediation security solutions on AWS platform. Reported security findings, recommendations and presented to the business users, executive committee, and Compliance departments. Created an enterprise standard to compliance with the NY-DFS cybersecurity regulations 23 NYCRR 500. Security

Engineer Compass Group - Charlotte, NC January 2016 to December 2017 Developed security requirements for both infrastructure and applications (web and mobile) and worked with Infrastructure engineering, application development, DBAs, SysAdmin teams and made sure the requirements are incorporated into the systems during the design and architecture phase of the delivery lifecycle. Develop security requirements for applications and infrastructure deployed in the Cloud. Ensured that Cloud security best practices have been followed. 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. Developed AWS Security Groups to control traffic to various instances in the Cloud. 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. 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., Azure disk encryption has been implemented for encrypting OS and data disks. Validated database security for SQL servers deployed in Azure Cloud environment. Implemented Integrated Windows authentication supported by Azure Active Directory. Performed security assessments to ensure compliance with the firm's security standards NIST 800-53. Worked with Pen testing team to identify XML External Entity (XXE), Cross-Site Scripting, ClickJacking, Session Management/Hijacking, and SQL Injection related attacks within the code. Implemented Cloud Access Security Broker (CASB) for enterprise application infrastructure. Installed, configured and administered IBM AppScan Enterprise, including scan agent configuration, scan scheduling, troubleshooting of failed scans, user administration. Implemented authentication solutions for various types of applications using OAuth2.0, SAML, and OpenID. Good understanding of web application attacks including SQL, XSS, Clickjacking, CSRF, and other common security issues beyond the OWASP Top 10. Implemented security controls for AWS Virtual Private Clouds (VPCs), EC2 instances, RDS and Route53. Designed security architecture for web and mobile apps. Reviewed Solution overview

Documents (SODs) to identify security anomalies in the system architecture and design, and provided recommendations to address data security and privacy concerns. Developed a threat modeling framework (STRIDE, DREAD) for critical applications to identify potential threats during the design phase of applications. Worked extensively with software development teams to review the source code, triage the security vulnerabilities generated by IBM AppScan, BurpSuite, Imperva WAF HP WebInspect, HP Fortify and eliminated false positives. Participated in the development of IT security risk assessments for enterprise applications. The NIST, FFIEC frameworks have been utilized for IT risk assessments. This included leading the data discovery meetings, identification of existing controls and validated them against the expected controls. The control gaps or non-compliance to security policies were presented to the stakeholders for remediation. Working knowledge of Splunk in developing search queries including, knowledge objects such as Event Types, Tags, Database Queries, etc., Rolled out Beyond Trust Privileged Access Management (PAM) solutions for controlling privileged accounts and users. Implemented authentication for applications using web application vulnerability scanning tools (IBM AppScan, IBM AppScan Source, HP Fortify, HP WebInspect, BurpSuite Pro, ZAP, Kali Linux, etc.) Strong knowledge of web application security, web-related protocols (HTTP, HTTP/2, SSL, WebSockets, etc.) Generated executive audit summary reports showing the security assessments results, recommendations and risk mitigation plans and presented them to the respective business sponsors and senior management. Worked with DevOps teams to automate security scanning into the build process. Participated in the implementation of Imperva SecureSphere, Database Activity Monitoring (DAM) and AWS Cloud security for applications being deployed in the Cloud. Developed security best practices for the applications and infrastructure deployed in AWS. Cyber Security Analyst Mantle Future Systems - IN April 2013 to July 2015 Reviewed security vulnerability reports for applications and databases, analyzed and worked extensively with the development teams for the implementation of mitigating controls. Reported security findings, recommendations and presented to the business users, executive committee, and Compliance departments. Participated in the implementation of SafeNet/Gemalto product for encrypting customer credit card information using Public Key Infrastructure (PKI), creating and handing the certificates. Learn how to use the IBM AppScan standard, source editions, HP WebInspect and QualysGuard web application scanners. Also, the security tools Metasploit and BurpSuite were utilized for manual penetration testing. Participated in the integrated security audits of Global Equities Derivatives & Commodities (GECD) and Fixed Income (FI) business lines. Mainly responsible for the review of input/output processing, data security. Reviewed Architecture Design Documents (ADD) and Solution Overview Documents (SODs) to identify security anomalies in the system architecture and design, and provided recommendations to address data security and privacy concerns. Worked with Internet Engineering team in the design and configuration of BlueCoat Internet proxy. Implemented WebFilter database for URL content Filtering. Worked with team to develop security policies and baselines for mobile and web applications. Performed compliance audits to ensure security policies and baselines have been adequately implemented. Performed PCI pre-assessment audit for the entire network as well as the related applications in preparation for the annual external PCI compliance audit. Reviewed a newly implemented Security Incident and Event Management (SIEM) system. Reviewed technical specifications for SIEM, logging and proposed recommendations to improve the overall deployment of the solution. Performed penetration testing for external facing web applications. Security areas covering DMZ architecture, threat modeling, secure coding practices (i.e., OWASP standards) and vulnerability analysis were assessed. Conducted security assessments for various applications supporting Corporate & Investment Banking, Loan, Treasury, Equities and FI businesses. The web application infrastructure such as IBM WebSphere, Apache Tomcat, and IIS web/application servers was reviewed for compliance with the firm's security baselines. Education Bachelor's Skills IIS (2 years), SECURITY (5 years), TOMCAT (2 years), WEBSPHERE (2 years), SPLUNK (2 years) Additional Information TECHNICAL SKILLS Information Security Tools CyberArk, Paros, Nmap, BMC BladeLogic, Nessus, Rapid7 Nexpose, Tripwire, Symantec Vontu, BeyondTrust PAM, DBProtect, e-DMZ Password Auto Repository (PAR), Varonis, AppDetect, AppRador, JHijack, Metasploit Pro, ZED attack proxy, SQLMAP, Wireshark, WebScarab, Amazon Web Services (AWS) Cloud security.

DAST and SAST tools Checkmarx, Veracode, Fortify SCA, IBM AppScan Enterprise (ASE), Standard & Source editions, HP WebInspect, QualysGuard, BurpSuite Pro Operating Systems Oracle Solaris UNIX, RedHat LINUX 4/5, Windows Server2013/2016. Java & J2EE Technology Spring Framework, EJBs, Struts2, Servlets, JavaServerPages (JSPs), JMS, Java Mail API, JNDI, LDAP, JDBC, JTS, RMI, AWT, Swing, Socket Programming, IONA Orbix CORBA. SIEM Kibana, HP Arc Sight ESM, Logger, SmartConnectors, Express, Splunk Networking Symantec DLP, Checkpoint, Palo Alto, Check Point, Cisco, IDS/IPS, Anti-virus, Cisco IronPort, BMC BladeLogic, Remedy. Application Servers Weblogic Server, iPlanet, Netscape Application Server and Microsoft IIS. Languages Java, Python, C/C++, C#.NET, Perl, UML. Scripting Languages AngularJS, XML, XSLT, XPath, XQuery, HTML/JavaScript/JQuery, AJAX. Middleware TIBCO EMS, IBM WebSphere MQ, JMS, Apache Kafka Databases Oracle, MS SQL Server, Sybase. Web Services RESTFul/SOAP, SOA, UDDI, WSDL. Web Servers Apache Tomcat, Netscape Enterprise Server3.5, Jboss and JRun.

Name: Jeffery Richmond

Email: iphillips@example.net

Phone: +1-207-251-8072