Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Comerica Bank Houston, TX Experienced security consultant with seven years of vast IT Experience in cyber security, network security and firewall security with a focus on designing and developing security solutions. Knowledge of Vulnerability Management, Threat Analysis, Risk Management, Compliance and IT Governance. Accomplished researcher who turns challenges into building blocks to learn new technology, master advanced skills and streamline processes. ~~~~~~ ITS SECURITY CERTIFICATIONS CompTIA Advanced Security Practitioner - (CASP) CompTIA Security+ Certified Ethical Hacker (CEH) AWS Solution Architect-Associate Qualys Certified Specialist - Vulnerability Management, Web Application Scanning & Policy Compliance. Udemy Certification: Completed Practical Penetration Testing Certification with Khali and Metasploit. Work Experience Cyber Security Analyst Comerica Bank - Auburn Hills, MI March 2017 to Present Expertise in improving the Risk and Control functions against Governance, Risk Management and Compliance (GRC). Expertise in Gathering and analyzing metrics, key risk indicators and maintain scorecards defined within the area of information security to ensure our information security program is performing effectively and efficiently. Familiar with general security risk management principals and best practices. Ran vulnerability scans and edited all server IPs on Nexpose Administered cryptography, certificate management and implemented dual keys to address segregation of duties issue between DBAs and security admins. Administered cryptography, certificate management and maintained key rotation. Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF, Authentication bypass, Weak Cryptography, Authentication flaws etc. Supported the information security audit and third-party assessment initiatives during planning, execution, and remediation phases, as well as coordinating and tracking remediation activities. Using Google's proprietary tools to perform Static and Dynamic analysis of the application (SAST and DAST) Experience in Qualys as Cyber Security Analyst to secure Organization Network and vulnerability management. Performing Vulnerability Management by scanning, mapping and identifying possible security holes using Qualys Guard and Nessus scanner. Performed password recovery and SSH configuration on Cisco Routers. Set up ACL / zone security to block SSH attacks from a foreign country. Conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs, Gathers and organizes technical information about an organization's mission and goals in remediation process. Develop remediation plans to resolve the vulnerabilities uncovered by Nexpose Rapid 7 penetration testing reports. Participated and assisted with information security activities highlighting schedule, risk assessments, evaluations, analysis. Escalated and documented findings & exceptions requests in timely fashion to appropriate IT and business stakeholders to facilitate resolution. Ensuring Qualysguard vulnerability scan results are loaded in RSA Archer and groups them by affected Product (e.g., Adobe Reader, Java, MS) document findings and communicate effective remediation action plans with the remediation plan. Knowledge and experience in standard security and regulatory frameworks including ISO, NIST 800-71, HIPAA, SOX and PCI DSS. Good knowledge of network and security technologies such as Firewalls, Network layer protocols, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching. Experienced in working on Patch Management, Vulnerability Scanners and Penetration Testing. Familiar with threats and vulnerabilities, latest trends and risks and be able to understand the technical remediation action steps or plans and communicate them effectively to teams within the organization. Worked as an Information Security Test Consultant, involved in recommending security solutions of new applications incorporating secured SDLC, OWASP Top 10 based Vulnerability Assessment of various internet facing point of sale web applications. Managed policy exceptions with Business Unit requestors and coordinate the annual exception review process. Worked directly with various teams to document exceptions, identify compensating controls, and remediation action plans accordingly. Provided process improvement suggestions for more effective management and review of exceptions. Supported and helped mature the security risk management program. Familiar with general Governance, Risk and Compliance (GRC) programs with specific knowledge of vendor risk and policy management. General knowledge in the areas of IT management, acquisition and maintenance of systems, system operations and Information security control activity.

Analysis of Offenses created based on vulnerability management tools such as: Rapid7 Penetration testing based on OWASP Top 10. Conducted hands-on DAST and SAST with adherence to OWASP and SANS standards Monitored and researched Cyber Threats with a direct & indirect impact to the organization internally. Developing and maintaining current knowledge of technology, security standards, guidelines, policies, and procedures based on best practices and compliance requirements. Performing technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, applications, etc.) Ensured completion of risk assessment, security compliance and preventing the unauthorized use, release, modification or destruction of data. Working with the security engineers to schedule testing of systems (scans, system test and evaluation) and examines active monitoring to ensure controls are in place and are effective. Working on different tools for static(checkmarx) and dynamic(Netsparker) security code analysis(SAST and DAST). Performing security reviews, network-based vulnerability scans and penetration tests to determine security gaps and apply continuous improvements to secure applications. Collaborating with the department IT managers outside of the Information Services Department to ensure information security and privacy risks are identified, documented and addressed in a timely manner. Enforcing information security standards, guidelines, policies, and procedures to other IT project teams. Maintaining and enhancing vulnerability management program, to include network vulnerability scanning, exception requests, reporting, and remediation efforts. Conducting application security assessments, verifying plans for threats, including static analysis, dynamic analysis, and manual testing of web and mobile applications and establish test procedures for remediation. Web Application & Network Scanning with HP Webinspect, IBM Appscan, VERACODE (SAST/DAST), Qualys, Nessus 5.x/6x, PVS, LCE Security Center, Port Scanning with NMAP Making recommendations regarding the selection of security controls to mitigate risk (e.g., protection of information, systems, and processes) Documentation of findings & remediations plans through risk rating whenever required in GRC Archer. OWASP Top 10 Issues identifications like SQLi, CSRF, XSS, Path

Manipulation. Assisting with development and maintenance of technical documentation and standard operating procedures. Conducting Application Security testing & code reviews verifying the scripts written for various functions and instances. Additional responsibilities as identified. Information Security Analyst DST Systems - Kansas City, MO January 2016 to March 2017 Involved in Security Development Life Cycle (SDLC) to ensure security controls are in place. Involved in CWE's Top 25 based Vulnerability assessment of web applications. Strong knowledge on Vulnerability Management using Qualysguard. Experience on Network scanning and reviewing penetration testing results using various web application security tools like Metasploit, Nmap. Working closely with Appscan, Symantec and Rapid7 for any malware activity on environment. Running the Vulnerability scans using Rapid7 and send the reports to Management. Perform global deployment of Rapid 7 Nexpose vulnerability scanner Created Dashboards, Reports and Documentation in Nexpose. Monitored Security Management Console for Security SOC to ensure Confidentiality, Integrity and Availability of Information systems. Validate Input validations, session managements, client protocol controls, cryptography, Logging, Information leakage. Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like QRadar. Managed Cyber Security threats through prevention, detection, response, escalation and reporting in effort to protect Enterprise IT Assets through Computer Security Incident Response Team (CSIRT). Responsible for CSIRT included SIEM, Context Filtering, Web Security, Incident Tracking, IPS/IDS and Malware Analysis. Conducted secure code reviews using automated tools and manual techniques. Proficient in understanding application level vulnerabilities like SQL Injection, Authentication bypass, Weak Cryptography, Authentication flaws. Provided necessary designs and implemented security solutions for egress/ingress points using the IPS/IDS sensors across the networks to provide better incident handling and event monitoring. Developed Cyber Security Standards on NIST Frameworks and insured their implementation to reduce the risk of vulnerability to IT assets. Developed various functions including identifying, protecting, detecting, responding and recovering for performing concurrent and continuous operation of dynamic security risk. Provided suggestions and inputs to Global Security Council as a part of project consulting towards Information Security and Cyber Intelligence. Opened, Assigned and closed the tickets assigned in SOC Security Management Console towards Qualys for various Remediation Process and Patch Management Process. Web Application & Network Scanning with HP Webinspect, IBM Appscan, VERACODE (SAST/DAST), Qualys, Nessus 5.x/6x, PVS, LCE Security Center, Port Scanning with NMAP Vulnerability Management: Configured Qualys Guard Tool for Vulnerability Analysis of Devices and Applications. Monitored them constantly through the dashboard by running the reports all the time. Created Asset Groups, scheduled Scans/Reports for smooth remediation process and assigned the correct sensors to those scanners placed in the network. Dockers containers for WAF/DDOS testing on internal applications (OWASP top 10 and DDOS) Identified flaws (Security Misconfiguration, Insecure direct object reference, Sensitive data exposure, Functional level access control, and Invalidated redirects) both in automated and manual testing environment. Coordinated with dev team to report vulnerabilities by explaining the exploitation and the impact of the issues over application. Managed all the scans including discovery maps, authentication scans to ensure proper scheduling, reporting and smooth functioning of IP's. Managed Qualys Cloud Agents. Assisted in installing them over the devices, servers or also for remote users. Scanned the entire devices using the cloud agents for employees working from home and provided the solutions to fix the vulnerabilities.

Managed a Vulnerability Remediation Team (VRT) for reporting all the scan reports and guided them to fix the vulnerabilities and patches using the QID's, Bugtraq ID's and CVE ID's from knowledge base from vendors. Worked on Qualys Web Application Scanning for monitoring the Web Applications, filtering and crawl scoping to detect the vulnerabilities in the web applications and fix them. Performed SAST (Static Application Security Testing, code reviews) on web applications using HP Fortify Managed to secure the devices across entire network by using the ThreatProtect Module from Qualys. Measured the level of Severity of devices to fix the issues arising from them by providing solutions. Generated and presented reports on Security Vulnerabilities to both internal and external customers. Report the identified issues to development teams, train them over common vulnerabilities, prescribe remediation and follow up on the fixes. Excellent code reviewing and programming skills on java, JavaScript, XML environments. Had proven adeptness to assigned work with good analytical, interpersonal and problem-solving skills. Information Security Analyst Schenck Process - Jacksonville, FL January 2014 to December 2015 Developed, implemented and monitored a strategic, comprehensive enterprise information security and IT risk management program to ensure the Confidentiality, Integrity and Availability (CIA) of information owned, controlled or processed by the organization. Managed Security Operation Centre Services, Information Security Transitions, Security Controls Gap Analysis, Service Assurance Programs, help team for Internal and External IT Audits, Security Consultation, Information Risk Assessment for various processes. Assisted Senior Information Security Officer in the conduct of Information Security Assurance roles and ensuring system safety. Implemented IT security process using Risk Management Framework NIST 800-37, Certification & Accreditation, and Assessment & Authorization document from categorization of information system to monitoring security control. Developed System Security Plan SSP to provide an overview of systems requirements. Checked events logs for irregularities, identified regularities are then reported as incidents. Responsible for monitoring compliance with information security policies by coaching others within the organization on acceptable uses of information technology and how to protect organization systems. Performed risk and security assessments of applications, databases, and servers and supports networking technologies, such as routers, switches, access points, in order to determine if these assets have any vulnerabilities to potential internal or external threats using Qualys. Performed cyber security risk and regulatory compliance assessments. Ensured that Security Authorization Package such as SSP, POA&M and SAR Security Assessment Reports are maintained, reviewed and updated in accordance with the guideline. Conducted time to time risk assessment and reviewed controls for any deficiencies, and the deficiencies where reported to the ISSO for complete mitigation actions. Involved in drafting Contingency Plan recommendations for system owners. Implemented IT security process using Risk Management Framework NIST 800-37, Certification & Accreditation, and Assessment & Authorization document from categorization of information system to monitoring security control. Provided technical and operational leadership for cyber- security incident response. Designed a performance and security monitoring system, risk assessment report, incident response, vulnerability assessment and risk mitigation. Responsible for web application vulnerabilities (OWASP TOP 10) to review application source code to find its security vulnerabilities and recommend remediation. Responsible for the day-to-day security operations of a system. Excellent Project Management skills and adaptable to work in any work environment Bangalore Trainee Network Engineer Schenck Process India Private Ltd May 2012 to December 2013 Planned IT network infrastructure with clients to ensure that the systems are tailored and comply with their requirements and needs. Replaced branch hardware with new routers and switches. Deployed, configured and supported Windows based software packages and operating systems. Used Active Directory to administrate and troubleshoot network objects and resource issues, also to troubleshoot DNS, Group Policy and DHCP issues with machines running Windows Server 2008, 2008 R2. Dealt with monitoring tools like network packet capture tools such as Wire-shark, OPNET, Cisco Tracer, etc. Maintained security systems and administers security policies to control access to systems. Maintained the company's firewall and utilizes applicable encryption methods. Worked on various Firewall platforms for Checkpoint R77.30, R77.20 and Palo Alto, PAN OS. Worked on Checkpoint blades including IPS, Threat prevention, Identity awareness, Application & URL filtering. Configured and created rules (Access, deny and Block) to control traffic for new gateways. Firewall Policy enforcement per customer Policy including global policy and objects. Created information security documentation related to work area and completes requests in accordance with company requirements. Identified opportunities and executed plans to improve workflow and understands and quantifies business impacts of those improvements for communication to management. Spraying Systems Co Bangalore IT Technology Intern May 2011 to August 2011 Planned IT network infrastructure with clients to ensure that the systems are tailored and comply with their requirements and needs. Replaced branch hardware with new routers and switches. Deployed, configured and supported Windows based software packages and operating systems. Implemented multi router graphing tool to monitor the company WAN links and Internet T1's.

Involved performing a diagnosis first then contacting the clients, IT team, presenting them with my findings and working with them to resolve the issue. Implemented numerous Site to Site T1's utilizing hardware from Cisco & Netopia. Implemented and managed Norton's corporate anti-virus solution. Education masters Skills Nexpose (3 years), Nist (5 years), Nmap (3 years), Qualys (5 years), Security (7 years) Additional Information TECHNICAL SKILLS Networking Technologies: LAN/WAN Architecture, TCP/IP, VLAN, Routing Protocols Security Firewalls ASA's, Checkpoint and Palo Alto Firewalls Qualys Continuous Monitoring Vulnerability Management, Web Application Scanning, ThreatProtect, Policy Compliance, Cloud Agents and Asset Management Event Management RSA GRC Archer, Blue Coat Proxy, Norse, Splunk, NTT Security, LogRhythm, HP Arcsight Pen Test Tools Metasploit, NMAP, Wireshark and Khali Frameworks NIST SP 800-171, ISO 27001, HIPPA, HITRUST, PCI DSS Security Intelligence WhiteHat Web Security, iDefence, NTT Security, LogRhythm. SIEM Splunk, Solarwinds, ArcSight, Nitro, IBM QRadar, Forcepoint, Rapid7 Nexpose Other Tools Bitbucket, Jira, MS Office Suite, AWS Console Web Technologies HTML, CSS, JavaScript, XML

Name: Christian Sanchez

Email: katherine45@example.net

Phone: +1-348-281-6527x5178