Sr. Cyber Security analyst Sr. Cyber Security analyst Sr. Cyber Security analyst - Tevora Business Solutions Irvine, CA I am an experienced Information security professional with detailed knowledge of enterprise security tools, technologies and best practices. I love working with people to create, deploy and sell solutions protecting enterprise networks, systems and information assets for organizations. Authorized to work in the US for any employer Work Experience Sr. Cyber Security analyst Tevora Business Solutions March 2018 to Present Responsibilities: Executed daily vulnerability assessments, threat assessment, mitigation and reporting activities to safeguard information assets and ensure protection has been put in place on the systems. In depth experience with internal, external, network, & application vulnerability assessments utilizing QualysGuard and FireEye with strong knowledge on Vulnerability Management using QualysGuard and Nexpose Verified that the Windows Virus Definitions on the SEPM are within 24hours from those reported by Symantec. Designed and implemented QualysGuard vulnerability management program. Upgraded and Optimized Splunk setup with new discharges. Worked on Setup Splunk Forwarders for new application levels brought into environment. Extensive experience in deploying, configuring and administering Splunk clusters. Helped application teams in on-boarding Splunk and creating dashboards, alerts, reports etc. Developed custom app configurations (deployment-apps) within Splunk in order to parse, index multiple types of log format across all application environments. Analyzed the existing data of Risk and compliance of the company and comparing it to the ISO 27001/2 standards for completing the gap analysis Responded to client requests and conducted third-party and internal risk assessments, gap analysis, evidence collections, and tracked remediation action plans. Experienced with various RSA Archer 5.x and 6.x EGRC solutions, development, deployment and implementation including upgrade, distributed and 3rd party system interfaces and data feed requirements. Established an on-going risk assessment program and conducted gap analysis based upon NIST 800-30 to comply with statutory law (i.e. HIPAA/HITECH) and information security requirements (i.e., PCI DSS). 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). Worked with

Splunk professional services to make the best practices that can be followed by everyone to maintain the performance of Splunk Enterprise Security. Handling database issues and connections with SQL and NoSQL databases like MongoDB, Cassandra, Redis, CouchDB, DynamoDB by installing and configuring various packages in python. Experience on vulnerability assessment and penetration testing using various DAST & SAST tools like BurpSuite, DirBuster, NMap, Nessus, IBM App Scan, Kali Linux etc Used McAfee ePolicy Orchestrator to monitor and identify potential intrusions and attacks for the Security Operations Center (SOC). Managed security incidents resulting from Splunk and third-party alerts, including investigation and remediation. Conduct network Vulnerability Assessments using tools to evaluate attack vectors, Identify System Vulnerabilities and develop remediation plans and Security Procedures. Internal, External, White box, Black box, Grey box penetration testing. Sound knowledge in Metasploit Framework and Social Engineering. Cyber Security analyst Nike - Hillsboro, OR May 2017 to February 2018 Responsibilities: Conducted onsite penetration tests from an insider threat perspective. Good understanding of administering and implementing SIEM, DLP, Web sense, Advance malware detection program, vulnerability assessment, and prevention, Experience with the Splunk Phantom SOAR Proof of Value (POV) project and participate in testing the out of the box use cases. Support the implementation of RSA Archer 6.2 Regulatory and Corporate Compliance, Incident, Task and Risk Management Solutions/Use Cases and maintenance of technology for the Compliance Management. Responsible for Splunk SIEM monitoring and configuration aligned to internal PCI and SOX controls Strong knowledge and experience in creating web based presentation for the client using HTML5, JSP, Servlets, Ajax, JQuery, EXT.JS, JSTL and JavaScript.

Making API calls using PYTHON scripts to retrieve data from cloud and writing on the disk and then On-boarding it into Splunk using file monitoring inputs Extensive Experience with McAfee DLP architecture and implementation for enterprise level. Identified confidential and sensitive data (PII, PCI) using IDU data classification framework and generated reports for management review and recertification. Assisted on creating the Indexers, Indexes, Source types, and search-heads. Pushing logs into Prod and non-prod Splunk as per the requirements. Helped in automating the

DDP report in Splunk to see the machines that are out of compliance. Guided all the SME's in using Splunk to create dashboards, reports, Alerts etc. Helped in identifying the Domains that are not allowed to access and been accessed by users and been blocked in proxy and Palo-Alto. Helped the SOC team and Cyber security team to see what are the Vulnerabilities that are hitting the environment and see what are machines that have vulnerabilities. Extracting the fields using Rex, Regex, IFX, which are not extracted by Splunk and Experienced in developing Web Services with Python programming language. Immense use of commands like Makemv, mvexpand etc., to extract the values from logs. Worked on Splunk ES to build the correlation searches, alerts, reports and dashboards to get specific monitoring. Configuring LDAP and Single Sign-On for User Authentication in the organization. Proficiency in Splunk 5.x / 6.x Development, System integration under cross platform consisting of Red Hat Linux and Windows operating system. Oversee Vulnerability assessment /penetration testing of scoped systems and applications to identify system vulnerabilities. Excellent knowledge of FISMA, HIPAA and NIST Compliance usage, rules and regulations Used Splunk Security Manager to identify threats and assigned category Implemented automation script using python to run the web crawler. Engineered Splunk to build, configure and maintain heterogeneous environments and in-depth knowledge of log analysis generated by various systems including security products Architecture various components within Splunk (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, Parsing, Indexing, searching concepts, Hot, Warm, Cold, Frozen bucketing, License model. Upgraded and Optimized Splunk setup with new discharges. Worked on Setup Splunk Forwarders for new application levels brought into environment. Extensive experience in deploying, configuring and administering Splunk clusters. Helped application teams in on-boarding Splunk and creating dashboards, alerts, reports etc. Developed custom app configurations (deployment-apps) within Splunk in order to parse, index multiple types of log format across all application environments. Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework. Performed risk assessments to ensure corporate compliance. Symantec DLP and RSA DLP architecture and implementation for enterprise level companies. Developed detailed remediation reports and

recommendations for compliance and security improvements across industries based on changing threats. Assisted Splunk Enterprise Admins by creating requested dashboards and reports required for NERC compliance. Performed application security and penetration testing using IBM Appscan. Use Splunk Enterprise Security to configure correlation search, key indicators and risk scoring framework. Managing Security tools DLP, SIEM, Vulnerability scanner and Penetrations test. Perform automated and manual security assessments to identify configuration and patch related vulnerabilities using commercial and open source tools. Configuration, troubleshooting, and management of Websense Data Security (DLP). Monitoring McAfee dashboard for updated DAT versions in all the client. IT Security Analyst Webframe Systems - IN May 2013 to July 2016 Responsibilities: Served as the primary responder for managed security incidents pertaining to client firewalls and all network infrastructure component. Worked with the Splunk professional to remediate the Search Head load issue by distributing the load equally between the search Heads. Helped the Operations team completing Splunk Hygiene Project to make sure there are no issues Experienced on Setup Splunk Forwarders for new application tiers introduced into environment and existing applications. Worked closely with Application Teams to create new Splunk dashboards for Operation teams. Troubleshoot and resolve the Splunk - performance, log monitoring issues; role mapping, dashboard creation etc. Created Splunk app for Enterprise Security to identify and address emerging security threats through the use of continuous monitoring, alerting and analytics. Created Regular Expressions for Field Extractions and Field Transformations in Splunk. Anonymize the PII (Personally Identifiable Information) data in Splunk. Masked sensitive information such SSN numbers, Addresses when showing results in Splunk. Configured Splunk for all the mission critical applications and using Splunk effectively for Application troubleshooting and monitoring post go lives Administration of Splunk (SIEM), ARCOS (Privilege Identity Management), DLP (Symantec), Imperva WAF tools. Worked with Symantec DLP version 14.6 and 15.0. and assessed and built a data protection program through data classification skills and a clear understanding of privacy standards and regulation. Making API calls using PYTHON scripts to retrieve data from cloud and writing on the disk and then On-boarding it into Splunk using file

monitoring inputs Collaborated with fellow analyst and leadership to develop and streamline operational guidelines and perform analytical support of security incident calls across the enterprise

Helped to research open-source intelligence feeds for current and emerging threat information Education Master's Skills Nist, Cissp, Siem, Information Security, Cyber Security Additional Information CORE COMPETENCIES Extensive experience in Information Security and threat analysis. Facilitating implementations of information security policies, account security policies and standards for logical and physical security. Operated with Splunk professional services to make the best practices that can be followed by everyone to maintain the performance of Splunk Enterprise Security 7.0.4. Designed and secured environment and release automation for a high traffic custom travel service on cloud using AWS, Python, CI/CD, and security tools. Develop SIEM / User Behavior Analytics (UEBA) use cases, rulesets, and content definitions based on numerous intelligence and detection products in Securonix SNYPR 6.2. Experienced in Preparing, arranging and testing Splunk search strings and operational strings. Splunk, Sentinel One, SIEM, Akamai, e Drive Encryption, McAfee, Imperva DAM, WIPS, Proxy, Crowd Strike, Data Pipe, DDos Analysis, Bot Detection NCDC, EVTK Tool, Bit9, Zscaler, Scansafe, Fire Eye, DNS logs, Shield Ticketing System, Service Now, Cireson, BlueCoat, Symantec DLP, Cisco IronPort, Nexpose, Coalfire. Thorough understanding of OWASP Top 10 Vulnerabilities, CWE/SANS Top 25 and CIS Critical Security Controls and evaluating web application firewall (WAF) configurations Using Qualys for automated scans and vulnerability management, prepared & presented reports to Client & Management, raised Incident for vulnerability mitigation. Performing Risk Assessment, Gap analysis & create Risk Mitigation plan and perform Internal & External Audits. Experience with convert Checkpoint VPN rules over to the Cisco ASA solution. Migration with both Checkpoint and Cisco ASA VPN experience. Deliver niche technology projects such as DLP and forensics to catch and prevent fraud, manage overall operational aspect of DLP. Experience with Installation and Maintenance of Splunk Universal Forwarders, Solving Forwarder Issues, Deployment Server Classes and Apps through Deployment Server. Solid understanding of OWASP top Vulnerabilities and other software security best practices Knowledge of Information Security tools like: Splunk,

Cisco Ironport, Bit9, CrowdStrike, Nexpose, Sophos, RSA Security Analytics, Encase, Barracuda WAF, BeyondTrust, Metasploit Splunk, Sentinel One, SIEM, Akamai, e Drive Encryption, McAfee, Imperva DAM, WIPS, Proxy, Crowd Strike, Data Pipe, DDos Analysis, Bot Detection NCDC, EVTK Tool, Bit9, Zscaler, Scansafe, Fire Eye, DNS logs, Shield Ticketing System, Service Now, Cireson, BlueCoat, Symantec DLP, Cisco IronPort, Nexpose, Coalfire. Building, Deployment, Configuration, Management of SPLUNK Cloud instances in a distributed environment which spread across different application environments belonging to multiple lines of business. Monitored and investigated SOC incidents and alerts with Splunk SIEM. Experience with industry recognized SIEM (Security Information and Event Management) solutions such as NITRO, Splunk, Forcepoint and many other tools. Experience object-oriented programming (OOP) concepts using Python, C++, C# and PHP. Proficiency in Splunk 5.x / 6.x Development, System integration under cross platform consisting of Red Hat Linux and Windows operating system. Experienced in WAMP (Windows, Apache, MYSQL, Python/PHP) and LAMP (Linux, Apache, MySQL, Python/PHP) Architecture. Oversee Vulnerability assessment /penetration testing of scoped systems and applications to identify system vulnerabilities. Excellent knowledge of FISMA, HIPAA and NIST Compliance usage, rules and regulations Used Splunk Security Manager to identify threats and assigned category. Engineered Splunk to build, configure and maintain heterogeneous environments and in-depth knowledge of log analysis generated by various systems including security products Architecture various components within Splunk (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, Parsing, Indexing, searching concepts, Hot, Warm, Cold, Frozen bucketing, License model. Oversee Vulnerability assessment /penetration testing of scoped systems and applications to identify system vulnerabilities. Identifying the critical, High, Medium, Low vulnerabilities in the applications based on OWASP Top 10 and prioritizing them based on the criticality. Performed Symantec DLP environments management and support configuration as well as data security environments used in testing and configuring client sites prior to installation. Expert in installing SPLUNK logging application for distributed environment. Experience in Automated and Manual Penetration Testing, Contractor Assessments, Source Code

Review, Controls Assessment. Software Development of Custom Compliance Modules, Attacks, and Exploitation for Nessus and Metasploit. Experience with industry recognized SIEM (Security Information and Event Management) solutions such as SNORT, Splunk, Log Rhythm and many other tools. Antivirus McAfee Virus Scan Enterprise, Symantec, Endpoint Protection Suite Conducts vulnerability scans and penetration tests to meet PCI requirements. Experience in supporting, operation and troubleshooting the problems. Written map scanner and multithreaded python program to brute-force an ftp server using password file. Technical Skills Tools: Kali Linux, Tableau, Lotus Notes, ERP - SAP, Visio, Qlikview, Oracle, Identity and access management Security Web Applications: TCP/IP OWASP, Nessus, Grabber, Zed Attack, Skipfish Hydra, Firewall, IDS, IPS Languages and Database: SQL, C++, Visual Basic, Java script, JSON, Python, Bro, ASP.NET MVC, Powershell, PowerBI, STIX Networking & Frameworks: DNS, DHCP, SSO , SAML, NAT, PCI-DSS Continuous Monitoring: Vulnerability Management, Web Application Scanning, ThreatProtect, Cloud Agents, Asset Management, Sourcefire, Nexpose, Forcepoint, Rapid7 Event Management: RSA Archer, Blue Coat Proxy, Splunk, NetWitness, LogRhythm, HP Arcsight PenTest Tools: Metasploit, NMAP, Wireshark and Kali Security Software: Nessus, Ethereal, NMap, Metasploit, Snort, RSA Authentication Frameworks: NIST SP 800-171, ISO 27001/31000, HIPPA, HITRUST CSF, PCI DSS

Name: Timothy Carter

Email: paige89@example.net

Phone: 429.857.1920