Security Analyst / Engineer Security Analyst / Engineer Security Analyst / Engineer - MGIC Chicago, IL Several years of experience in the Information Security field as an IT Security Analyst/ Engineer and Network Engineer. Proficient with SIEM tools like QRadar, LogRhythm and Loglogic. Also, Qualys and Nessus for Vulnerability Management. Expert level skills with Qualys Cloud Platform with modules Vulnerability Management, Policy Compliance, AssetView and PCI-DSS. Extensive hands on experience with Symantec Security tools like Symantec DeepSight Threat Management, Symantec DLP, Symantec SOC and Symantec MSS. Proficient knowledge on OWASP Top 10 Vulnerabilities. Knowledge of scripting like Python, Bash. Proficient with TCP/IP and relative OSI models. Technical support for improvement, upgradation & expansion of the security and network architecture. Capable enough to work independently with minimal supervision. Proven capabilities in learning and working with emerging new technologies. Work Experience Security Analyst / Engineer Confindental - Milwaukee, WI July 2017 to Present Responsibilities: Lead managed and revived Vulnerability Management program using Qualys, Trustwave and HP Fortify. Prioritized vulnerabilities by generating pivot tables weekly per team based on exploitability and exposure. Monitored Qualys Policy Compliance module for policy violations and followed up with tech teams for remediation. Helped deploying, tuning and tweaking Logrhythm. And log collection for it. Threat hunting using Logrhythm, LogLogic, Proofpoint Protection Server, NTT MSS, Paulo Alto Panorama and Enterprise McAfee Anti-Virus. Submitted monthly remediation reports to upper management. Fixed Qualys Authentication across the company for Qualys Authenticated scans. Investigated false positive Qualys, Trustwave and Fortify tickets. Setup baseline Security standards and reviews using CIS/ NIST Benchmarks for MS SQL Servers, Oracle Servers, Windows 7 2008 2102 2016 Servers, VMware ESXi servers. Configured security software (OSSEC, Loglogic, NTT MSS and Qualys) for newly built servers. Currently integrating Qualys with ServiceNow TVM module. Upgraded/ Patched/ Fixed security software like Password Manager Pro, RSA authentication manager and Loglogic. IT Security Analyst/ Engineer Confindental - Rosemont, IL March 2016 to April 2017 Responsibilities: Investigated email threats, fraudulent emails and advised further actions for Bank's internal employees. Successfully carried out email

security awareness program across the bank using Phishme. Used SourceFire/ FirePower management console to monitor, validate and remediate attacks/ incidents. Provided possible remediation for every incident. Monitored and Investigated Symantec Security Operations Center Incidents to provide incident response. Used Cisco NGIPS, Cisco Firepower, Symantec MSS, Symantec Deepsight Intelligence for validating Security Operations Center (SOC) incidents. Monitored, managed, tuned and tweaked LogRhythm SIEM for internal Security Alarms/ Events. Extensively used Qualys Guard for Vulnerability Assessment / Management, performed regular scans and deployed/ managed Endpoint agents as required. Managed tracking and remediation of vulnerabilities by leveraging agreed-upon action plans and timelines with vendors and support teams. Deployed Qualys Endpoint Cloud agents on Mobile devices, Tablets and Laptops which enabled File Integrity monitoring, Indicators of Compromise (IoC), Policy Monitoring and Vulnerability Management. Tuned and tweaked Cisco Email Security Appliance (Cisco ESA) for email filtering and security. Researched in-progress attacks by analyzing Symantec MSS Incident logs. Used Microsoft Endpoint Protection to schedule malware scans across the bank. Tuned and tweaked Symantec DLP to avoid false positives. Monitored Symantec DLP incidents and analyzed DLP reports. Performed deep investigations on Ransomware Attacks, Web Server Attacks, Reconnaissance Incidents, Suspicious Activity Incidents, Anomalous Activity incidents and Aggressive SSH incidents to ensure they were blocked at the IPS/ Firewall. Conducted phishing email awareness campaigns using PhishMe to educate employees on phishing email threats like Locky, CryptoLocker, WannaCrypt and PowerWare. Security Engineer Smart IMS Inc - Plainsboro, NJ February 2012 to August 2014 Responsibilities: Developed IT roadmaps for security. Collaborate with Network Engineering team and Design team to understand TE needs and thereon design Security Protocol for the client network Conduct expert level R&A for corporate wide security Developed lab scenarios to act as test beds for testing custom security solutions designed Worked with Nexpose and Critical Watch tool and actively involved in Quarterly and Annual PCI - DSS scans, Vulnerability Assessment and their remediation and making sure they are compliant. Used Nexpose for Vulnerability Management, Assessment. Worked with SIEM tools like QRadar

and RSA Envision to find security violation events and validate IDS findings to negate False Alarms. Used QRadar analyzing log, flow, vulnerability, user and asset data. Created custom rules in QRadar. Deployed VPN' s with other partner companies, IPsec, GRE Worked with Nexpose vulnerability management solution for Vulnerability Management, patch and configuration auditing. Designed and deployed internal and external security edges for the company: DMZ and Extranet based security. Consistently monitor unusual changes to the traffic patterns and hence identify a threat and troubleshoot its removal. Worked with Symantec DLP for data leakage prevention incidents. Document designs and configurations. Performed preventative maintenance along with installation of hot fixes and version upgrades. Monitored resource usage and make required adjustments. Education Master's in Computer Science Chicago State University - Chicago, IL Skills SECURITY (4 years), DLP (3 years), SIEM (3 years), SYMANTEC (3 years), VULNERABILITY ASSESSMENT (3 years) Additional Information Skills/Knowledge: Vulnerability Management, Vulnerability Assessment, IT Auditing and Reporting, Security Baseline reviews, Security Policy review/ Update, Incident Response, Threat Modeling, Email Security, Threat hunting, Cyber forensics Investigation and Response, Malware Methods & Reverse Engineering, OWASP Top 10 Application Security Risks, SDLC, Agile, Network Traffic Analysis, Wireless Penetration testing, Network Penetration testing, Web Penetration testing, PCI-DSS, Data Loss Prevention (DLP), SIEM, IDS, IPS. Tools/ Software Used: Qualys Guard, OSSEC, Metaflows, Nessus, Nexpose, Burp, QRadar, LogRhythm, LogLogic, Symantec DLP, Symantec SOC, Symantec MSS, Veronis, DatAdvantage, PhishMe, Snort, Wireshark, Nmap, Metasploit, Microsoft SCCM, Active Directory, Microsoft Endpoint Security, Enterprise McAfee Anti-Virus, Cisco Firepower, Sourcefire, SolarWinds, JIRA.

Name: Alexis Hunter

Email: tatekevin@example.com

Phone: (582)447-2683