Security Engineer/ IT Security Tool Engineer/Manager(SECOPS) Security Engineer/IT Security Tool Engineer/Manager(SECOPS) Security Engineer/ IT Security Tool Engineer/Manager(SECOPS) - Current Project Responsabilities Nashville, TN 8 years of experience in IT Security operations in SIEM, Vulnerability Assessment& cloud services, Incident Response, and Forensics Member of Security incident response Team for Delta Dental corporation & JP Morgan Dallas & New York Super Admin for SIEM Facility(Qradar), vulnerability management (Rapid7-insight vm Nexpose), Threat Management (Fire Eye) And Email Security (Baracuda, Guava), solar winds (NPM, SAM) Experienced with Vulnerability Scanning tools like Nessus, Rapid7 and Qualys Implemented and Maintained SIEM infrastructure using Qradar and Splunk Member of Sec-Ops team for Incident Response plans and layouts Good understanding of disk dissection & memory issues as part of Incident Response Involved in enhancing the stature of the project by initiatives like Threat Modelling,awareness Security sessions, Dormant & Never Logged IDs clean-up Worked on SAST and DAST tools to check the potential of application and SAST for white box testing. Good knowledge in monitoring and management system that performs discovery, dependency mapping, monitoring, alerting, ticketing, run book automation, dash boarding and reporting for networks, compute, storage and applications Maintain proper auditing standards of SSAE 16, ISAE 16, SAS70, AT101 Good knowledge in compliance requirements and understanding of SERIES standards based on (NVD) National vulnerability databases. Good exposure to System/Network Analysis, Intrusion Detection, and Malware Analysis Involved in managing documentation to support IT security processes Provide root cause analysis and remediation techniques for management regarding security incidents and governance documents Good knowledge of threats analysis and remediation efforts about Intrusion prevention and penetrations Good knowledge in writing Firewalls rules and reviewing in seem, and Database Activity Monitoring (DAM) Ability to identify network and application vulnerabilities and create a remediation plan Good Understand of OWSAP Top 10 and SANS vulnerabilities Knowledge of networking concepts - LAN/WAN, TCP/IP, Routing & Switching and OSI Layers Strong troubleshooting, reasoning and problem-solving skills Authorized to work in the US for any employer Work Experience Security

Engineer/ IT Security Tool Engineer/Manager(SECOPS) Current Project Responsabilities - Franklin, OH October 2017 to Present October 2017-Till Date Security Engineer/ IT Security Tool Engineer/Manager(SECOPS) Manage information Security architecture, design, installation, operational planning, and risk remediation activities on various systems spanning more than 15000 devices spanning 48 locations. Design, implement and monitor Customer Program & Policy to assure compliance with federal regulations and industry standards. Managed operating metrics that enable the tracking of program progress and risk Monitored remediation plans with service providers on responses Produced a monthly reporting pack Worked with the Risk Analysis unit to define and create a repeatable process for managing authorized and unauthorized local network Administrator access Oversee operational support for Intrusion Detection, File Transfer, Mail Gateways, Web Content Filtering, and Entitlement Provisioning (includes support for Business Recovery) Design, implement and monitor Customer Information Security Program & Information Security Policy to assure compliance with federal regulations and industry standards. Instituted an Incident Response Program; planned 2018 table-top exercises Draft technical manuals, installation manuals, and procedures in order to enhance system security required for compliance. Performed installation, relocation, and maintenance on a wide variety of field equipment and infrastructure components including but not limited to routers, switches, firewalls, and telephone systems. Provided troubleshooting, repairs, testing, and modifications of Local Area Network (LAN)/Wide Area Network (WAN) electronic equipment and services. Provided level II and III help desk support as needed to staff of more than 4500 employees, and various 3rd parties. Consult and advise business units on various information technology projects. Identify risks and propose solutions to minimize adverse impact. Project Summary Security Engineer Delta Dental of New Jersey & Connecticut April 2016 to September 2017 Responsibilities: Analyze and review data from SIEM - Qradar for suspicious activity and trigger alerts to the concerned teams and applying rules and Building Blocks to SIEM Involved in leading Security incident response team(SIRT) Dedicated security monitoring and analysis of cyber security events (Triage) of tracking phishing URLs, and emails and deep dug investigations. Integration of different

devices/applications/databases/ operating systems with Qradar SIEM Monitor security alerts from IBM Qradar and report any issues to the concerned team. Monitor and analyze data feeds of events and logs from firewalls, routers, and other network devices or host systems for security violations and identify vulnerabilities. Conducted SAST and DAST with tools like HP Fortify, IBM Appscan, Webinspect, Nmap, Nessus. Analyzed the Exploited systems with vulnerabilities using Metasploit framework. Static and dynamic scanning of various application using HP Fortify and HP Webinspect, Identify false positives and reports it to soc Coordinate with subject matter experts to resolve any security incidents and correlate threat assessment data as needed. Support in the detection, understanding and resolving information security incidents affecting information systems & the business. Research and recommend corrective actions to ensure information dissemination regarding targeted or potentially targeted attacks. Responsible for IBM Qradar SIEM monitoring and configuration aligned to internal PCI and SOX controls Performed day-to-day administration of McAfee EPO 5.1 for maintenance of system policies, container maintenance, coordination of system maintenance and client upgrades for desktop environment Responsible for assisting various sites with troubleshooting and integrating all aspects of the ePO5.3 suite to include HIPS, Asset Baseline Monitor, AV, Rogue System detection, Policy Auditor. Configure and install McAfee IPS sensors, and Cisco ASA with Firepower Appliances. Troubleshot and resolved client communication problems, and firewall and McAfee IPS blocking problems Implemented and maintained McAfee Endpoint Encryption system to protect computers. Advanced threat detection, Antivirus, MacAfee IDS/IPS rule sets and signature creation, packet analysis. Perform vulnerability scanning and assist with compliance auditing to ensure customer networks conform to all relevant compliance standards, including PCI-DSS, HIPAA and Sarbanes-Oxley Manages PCI Compliance Program for organization protecting cardholder data and executing the PCI-DSS Program Life Cycle. Security Engineer JP Morgan Chase - Chase, NY August 2014 to March 2016 Analyze and review data from SIEM - QRadar for suspicious activity and trigger alerts to the concerned teams. Troubleshoot and researched security incidents based on QRadar Network Flow and Log Activity. Analysis of multiple log sources including firewalls, routers, switches, web servers and multiple

networking devices. Responsible for assisting with deployment of network infrastructure configurations across multiple product and technologies. Acted as the primary responder for managed security incidents pertaining to client firewalls and all network infrastructure components. Part of the Blue Team to identify the vulnerabilities and have a defense mechanism in place. Learned and helped IR team with Log collections, analysis, and forensic activities. Investigating logs and payloads for server crashes/core dumps, DDoS attacks, SQL/XSS, SPAM, etc. Installing and configuring Qualys in premises and on cloud environment. Responsible for performing vulnerability assessment on critical systems using Qualys. Configured and scheduled Qualys Scanner in QRadar to perform scan on regular intervals. Collaborate with team members in tuning SIEM applications to establish a baseline for network activity and rule out false positive events. Coordinate with SMEs to resolve any security incidents and correlate threat assessment data as needed. Support in the detection, understanding and resolving information security incidents affecting information systems & the business. Research and recommend corrective actions to ensure information dissemination regarding targeted or potentially targeted attacks. Investigate, document and recommend appropriate corrective action plans relating to IT security. Provide root cause analysis and remediation techniques for management regarding security incidents and governance documents Security Consultant EMC CORPORATION - Bengaluru, Karnataka December 2012 to July 2014 Responsibilities: Performed vulnerability assessments on web applications using IBM App Scan and Database systems using Guardium VA. Conducted dynamic and static analysis of web application using IBM Appscan. Performed security testing, analyze test results, document risk and recommends counter measures. Analyzed and reported management on current vulnerabilities and provide countermeasure recommendations Responsible for performing penetration testing all the way from planning, designing, executing and reporting. Used appropriate tools, techniques and conforming to agreed process standards and industry specific regulations. Created and maintained test ware (test cases, test scripts, test reports, test plans, etc.) to measure and improve the security of the application being scanned. Security Analyst EMC CORPORATION - Bengaluru, Karnataka February 2012 to November 2012 Responsibilities:

Monitor, Analyze and respond to security incidents in the infrastructure. Troubleshoot any security issues found in the infrastructure per the security standards and procedures. Expert in using Burp Suite for web application penetration tests. Actively used NMAP for port scanning and made sure only appropriate ports are in use. Actively researched on any security gaps that are beyond the ability of detection by any security scanner. Responsible for performing periodic Vulnerability assessment (VA) as per the security policy and standards. Involved in documenting all web applications and systems, audit data and ensuring compliance with legal and regulatory requirements. Engaged the development team to incorporate security in all phases of SDLC and to perform Threat Modeling, Risk Management, Logging, Penetration Testing, etc. Conducted application penetration testing of 20+ business applications and compliance audits. System Engineer Global Infrastructure Ltd January 2010 to December 2011 Responsibilities: Installation and Configuration of Linux systems like CENT OS, Red Hat and Windows Servers. Also involved in user account management. Actively involved in Monitoring the server's health status using different tools. Responsible for application support on Red Hat servers which included apache configurations Experience in Performance monitoring, usage and load the system. Created Perl and Shell scripts to automate administration tasks. RPM package installation & upgrade released by Red Hat in the repository Administration of client machines using SSH and FTP Supported for application upgrade and rollback, Start or Stop services in Linux Servers. Education Master of Science in Industrial Engineering and Information Architectures Sciences Lawrence Technological University Bachelor of Science in Mechanical Engineering Kamala Institute of Technology & Sciences - Hyderabad, Telangana Skills SECURITY (6 years), SIEM (3 years), LINUX (1 year), RED HAT (1 year), NETWORKING (1 year) Additional Information Skills: SIEM Tools: QRadar, Splunk Security/Vulnerability: Snort, Wireshark, Insight Vm Nexpose, Nessus, Qualys Appscan,Webinspect,Fortify Compliance: SOX (CoBIT, Coso) PCI, NIST SP 800-53,53A, HIPAA, HITRUST, MARS-E 2.0, FISMA Networking Protocols: TCP/IP, HTTP/HTTPS, SSH, SSL, DNS, SNMP Networking Monitoring: Routers, Switches, Load balancers, Cisco VPN, NAC/NAP Email Security Tools: Barracuda-spam firewall, Guava-E-mail Filtering Service MFA & SSO: Ping

Identity(Ping-one,Ping-Federate) Encryption: Twofish,blowfish,AES Threat Management: Fire eye, MacAfee _epos & Hips, Websense,Iprism (URL filtering service) Network Monitoring: ScienceLogic, Solar winds (NPM,SAM) Patch Management: Lumension-Prism Patch Certificate Monitoring: Digi-cert Operating Systems: Linux (kali Linux, red hat Linux), Windows Ticketing Systems: Service Now, Remedy, Heat, Clarify DAM: IBM Info Sphere Guardium DLP & EDR TOOLS: SYMENTEC, digital guardian

Name: Katherine Ward

Email: morsejames@example.com

Phone: 858.900.3123x2685