Princ Info Security Analyst Princ Info Security Analyst Princ Info Security Analyst - Veritas Technologies LLC Fairfax, VA Incident Handling and Vulnerability Management (SME), responsible for developing and maintaining the vulnerability management program Prioritizing vulnerabilities based on the attach vectors and coordinating with multiple teams to mitigate the risks. Utilizing Vulnerability Management tools (Qualys) to scan and detect vulnerabilities in a global infrastructure Responsible for implementing vulnerability management and web application security throughout the enterprise environment. Upkeep the security posture for 8000 endpoints, ~900 VDI, 1500 on prem servers and 10k cloud-based servers across multiple different operating system and web applications. Identifying and validating findings from vulnerabilities, risks, or improper configurations on the network that did not match approved enterprise guidelines. Integrating and automating the Threat Vulnerability Management process by using data sources from multiple platforms. Implementing the host hardening standards to improve security Threat posture and reducing overall risk to the organization using the knowledge of the organization and security standards (CIS, HIPAA. SOX, and POI) Document all processes, vulnerabilities, policies, and exceptions in formal documentation to be approved as accepted risks by the business while providing security guidance around each individual finding. Delivered infrastructure and web application vulnerability reports and findings to external customers and worked with multiple teams to address any concerns or remediation plans that needed to be utilized and deliver them to our customers. Developing SDLC practice and leading a web application security initiative within the organization. Maintain and configure enterprise vulnerability management tools (Qualys) in a global scale Configuring monitoring tools and deploy SEIM (AlienVault or OSSIM) in secured environment. Building VM's with the needed toolset to facilitate remote vulnerability scans and penetrating testing (Gray box and White box). Filtering and fine tuning SIEM platform per client environment to generate appropriate alarms for the SOC team to analyze and report. Deploy AlienVault logger to store logs for long term storage. Knowledge of network protocol analyzers such as Wireshark and Netflow Traffic Analyzer. Troubleshooting and resolving SEIM and network related issues escalated by SOC Familiar with Windows, Ubuntu, Red Hat Linux, and

Centos Investigate possible or actual security violations and incidents to identify issues and areas of weakness and make policy changes accordingly. Deploying and configuring HIDS agents (OSSEC & NxLog) on Windows servers such as Microsoft Windows IIS, SQL, Exchange using Ansible. Experience in deploying small to medium scale network monitoring tools such as Nagios and PRTG. Working in Data Center's managing servers, SAN and NAS devices like Cisco routers, switches and Dell servers. Expert knowledge of virtualizing applications such as VMware Workstation, ESXI, XenServer and Virtual Box. Deploying, configuring and managing network and service monitoring tools to monitor field appliances using SNMPv3, SSH and Nagios Agent. Utilize network scanning tools such as nmap and ethercap to do scans and find open ports. Experience in installation and configuration of various Unix/Linux platforms: DHCP, DNS, FTP, SSH and Syslog package management. Automating daily redundant task by using programming language such as python, shell, scriptFTP and IMacros Team player with excellent interpersonal skills, and understanding the demands of 24/7 system maintenance and criticality of prompt response. TECHINICAL SUMMARY SIEM /Monitoring Platform Qualys, AlienVault, Nagios, PRTG and Applications Virtualization VMware ESXI, VSphere, VCenter & XenServer Services SSH, SFTP, FTP, TFTP, OSPF, EIGRP Languages HTML, Python & Java Networking TCP/IP, UDP, LAN, WAN, DNS, DHCP, NAS, HTTP/S, LDAP Work Experience Princ Info Security Analyst Veritas Technologies LLC November 2017 to Present Configure and maintain Qualys vulnerability management platform in a global scale Develop strategies and processes to establish an efficient threat vulnerability management program Research, identify and mitigate newly released vulnerabilities based on enterprise impact Insure that the company assets follow a defined host hardening standard based on CIS benchmark Automate Threat vulnerability management reporting process based on various company needs and standards Help develop CMDB to maintain a proper asset count across the enterprise Security Engineer TruShield Security Inc - Sterling, VA August 2016 to September 2017 Configuring and deploying virtual SEIM appliance (AlienVault) in a distributed environment Troubleshooting escalated issues by the SOC and coming up with dynamic solution (automation) to existing day to day problems Deploying

agent based open source tools (OSSEC agent/server or NXLog) to monitor workstations and servers Deploying, configuring and managing agent/server based appliances to monitor network infrastructure using protocols and agents such as SNMPv3, SSH and Nagios Agent Working with the team of security engineers to identify and troubleshoot security problems Deploying ESXI platform with various VM's to deliver SEIM services to various government and commercial clients VoIP Engineer I BroadSoft to Netsepiens - Sterling, VA May 2015 to January 2016 Expert in configuration, management and deployment cloud based VoIP systems for small to medium size corporations Migration of hosted VoIP services across to a cloud based platforms (BroadSoft to Netsepiens) Troubleshooting VoIP and network related issues Setting up remote services to manage voice routers, switches, and phones by enabling encrypted remote tunneling protocols Securing VoIP services by implementing dynamic and static IP access list Train office administrators/operators to be proficient at managing their own internal VoIP services such as number reassignment, re-configuring phones for different users, deleting and adding new users to the platform Manage and resolve escalated incoming VoIP related tickets Work with a group of dedicated voice engineering team to deliver the best VoIP service possible IT Associate - Intern Sterling, VA February 2014 to April 2015 Manage incoming and outgoing tickets from customers Tier 1 help desk responsibility such as taking calls and replying to the customer in a timely manner Responsible for alerting the voice, network, and cloud engineers during emergency e911 ticket scenarios Education BA in Information Technology in Cyber Security George Mason University - Fairfax, VA 2015 to Present Associate of Science in Information Technology in Information Technology Northern Virginia Community College - Annandale, VA 2015 Skills Cyber Security, It Security, SEC, Information Security Additional Information Operating Systems Windows OS, Centos 4/5/6, Ubuntu 16.04/14.04, Kali, Debian 5/6/7/8

Name: Oscar Thomas

Email: sabrina01@example.net

Phone: (988)752-2566