Security Analyst Security Analyst Atlanta, GA Work Experience Security Analyst ControlScan - Alpharetta, GA October 2015 to Present Monitor clients network(s) for security events and alerts clients to potential (or active) threats, intrusions, and/or compromises Handle support tickets in line with ControlScan SLA Ability to identify anomalous network activity based on log and event data Interfacing with customers via phone and email Triaging and escalating support issues effectively Ability to troubleshoot issues that inhibit the transmission of log data such as; networking, software, or hardware issues Initiating in Incident Response processes to a potential compromise Respond to alerts and investigate anomalies for various Information Technology (IT) issues such as viruses, spyware, unauthorized access Evaluate and execute application whitelisting and URL filtering requests for IT security access Assist Information Security Engineers and Management in developing and refining policies and procedures for logging, monitoring, response, and escalations Collect data for IT security metrics and create reports Maintain up-to-date knowledge of the Information Security industry including new threats, mitigations, tools and trends; inform management accordingly Also performed duties of a SIEM Engineer, onboarding new custom customers, configure Alarm and Advanced Intelligent Engine Rules, create custom Message Processing Rules for logs using regex, maintain production environment of seven servers. Support all aspects of Security Information and Event Management (SIEM) initiative. Develop content for a complex and growing infrastructure. This includes use cases for Dashboards, Alerts, Reports, Rules, and Filters. Participate in the operation of Security Information and Event Management systems to include connectors, loggers/indexers, Windows and Linux servers, network devices and backups. Supporting the establishment, enhancement, and continual improvement of an integrated set of correlation rules, alerts, searches, reports, and responses. Coordinating and conducting event collection, log management, event management, compliance automation, and identity monitoring activities Tunes performance and event data quality to maximized system efficiency. Perform routine equipment checks and preventative maintenance. Performing systems hardening to PCI & HIPAA Standards Security analytics skills. Security Operations Center Sr. Analyst Dell Secureworks - Atlanta, GA June 2014 to October 2015 ? Provide firewall and IDS support for a large

global enterprise client ? Learn fundamentals for current firewall technology (Checkpoint, Juniper Netscreen, and Juniper SRX) as well as any new firewall/IDS technology introduced into the network ? Answer inbound calls and emails from technical clients (Network Administrators / Application Owners), authenticate callers, create or update tickets for all work, and address the client request or issue ? Meet service level agreements related to change processing and incident resolution ? Remotely access managed devices via in-band and out of band connections ? Work within a 7x24 shift-scheduled security operations environment ? Demonstrate excellent communication and client care skills by documenting all activities within our client delivery system and communicating with the client in a timely manner ? Support and Monitor Network Firewalls such as Nokia Checkpoint, Juniper, Cisco ASA 5500 firewalls, Proventia, SRX, and Tipping Point. ? Working knowledge and support of IPS(Intrusion Prevention Systems), NIDS (Network intrusion Detect Systems), and HIDS (Hardware Intrusion Detect Systems) and i-sensors ? Monitor Syslogs for Threat intrusion such as DOS, DDOS, malicious logic, sequel injections among other malwares. ? View and monitor EFD Event Flow Data for Anomalies Trending History of Security Devices ? Historical reports for third parties and Work with high visibility clients within a dedicated team ? Liaison between the Service Delivery teams, IT managers, Device Engineers and clients. ? Provide support for Customers in a 24/7 Security Support Center (SOC) ? Provide System upgrades and create and submit RMAs ? Monitor the HIT Health Information Technology Systems for a varied of clients/Platforms ? Interpret network diagrams IT Support Engineer GNAX - Atlanta, GA October 2013 to March 2014 ? Provide IT and customer support for user and backend support for a Vendor Neutral Archive (VNA) ? Setup and maintain the integrity and security of the Cloud environment in a VMware environment ? Conduct system analysis and development to keep systems current with changing technologies in a closed environment, Proxy, Cloud and Transfer Servers for Red Hat Linux, Cent OS Linux, Oracle Linux and Windows 2008 Server systems. ? Setup and administering of Operational tools virtual machines via VMware VCenter, like Puppet Labs ? Setup and administered and maintained a server running McAfee ePO orchestrator, including deployment and administering McAfee Agent, McAfee Endpoint Security products, such as McAfee VirusScan Enterprise, McAfee Realtime ePO,

McAfee Host Intrusion Prevention and Endpoint Firewall ? McAfee ePolicy Orchestrator (ePO) administrator experience ? McAfee Anti-Virus administration experience ? Experience with VMware vSphere 5.x products and services (vCenter, ESXi, SRM etc.) ? Solid understanding of virtual and physical network and security concepts and practices ? Proficient with Linux operating systems, i.e. Red Hat Linux server, Oracle Linux, CentOS Linux server and command line operations ? Working knowledge of data center management concepts and practices ? Maintaining Microsoft windows patch management and adhering to system security standards ? Monitoring and optimizing the performance of both physical and virtual servers ? Backup and recovery of OS and application information ? Working knowledge VMware infrastructure specifics of vSphere 5.x and View ? Experience consolidating policy sets, simplifying rules, and building documentation for handing down operations. ? Creating/maintaining virtual servers ? Disaster recovery for virtual environment ? Creating, managing, and deploying Active Directory Group Policy Objects (GPOs) and associated custom GPO templates for the virtual environment. ? Experience with Desktop VDI Environments such as VMware View ? Backup and Recovery strategies using Idera ? managing virtual hosts in a Data Center Environment ? Knowledge of web server services like Microsoft IIS and Apache ? Knowledge of storage technologies such as RAID, Snapshots, SAN and NAS Certifications/Licenses CCNA Routing and Switching June 2015 to June 2020 Security+ March 2013 to March 2017

Name: Kenneth Sosa

Email: garciajessica@example.net

Phone: 001-733-926-8871