IT SECURITY ENGINEER IT SECURITY ENGINEER IT SECURITY ENGINEER - AMERIPRISE FINANCIAL Minneapolis, MN Work Experience IT SECURITY ENGINEER AMERIPRISE FINANCIAL September 2017 to Present ArcSight, SumoLogic, Logstash, LogicHub, AWS, SiteScope, Analysis, Windows, Linux. Integrated various Firewalls (Application, Network), Load Balancers, Domain Controllers, Cloud Logs, SaaS logs, Productivity Applications into ArcSight for Security Monitoring. Configuring and testing of log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases and applications. Log Volume analysis for SIEM integration of the devices. Onboarding of the new VM's for the additional support of our environment. Integrating cloud-based log retention capabilities with ArcSight and creation of various dashboards. Management of ArcSight ADP platform resources (ArcMC 2.80, ESM 6.11, EB). Deployment of SIEM in Cloud, and Logstash pre-integration for SIEM. Experience in creating queries, reports, and setting up alerts in SumoLogic. Knowledge in admin activities of SumoLogic. Technical engineer with more than two PoC implementation. IT SECURITY ENGINEER CVSHEALTH January 2017 to August 2017 ArcSight, Symantec Critical System Protection, Windows, Linux. Installation of SCSP File integrity monitoring (FIM) agents on Windows and UNIX devices for PCI compliance. Creating various policies and asset groups in the SCSP console and adding of various devices and files to be monitored. Coordinating across various departments across the company for installation of the FIM agents to meet the audit requirements. Installation of Connectors and Integration and testing of multi-platform devices with ArcSight Express, Develop and test Flex Connectors for unsupported devices and Business applications Integration of FIM to ArcSight and analyse the logs to filter out False positives and add False negatives in to FIM rule set. SECURITY ANALYST ALERT ENTERPRISES December 2015 to December 2016 ArcSight, Splunk, Windows, Linux. Configuring log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases and apps. Categorize the messages generated by security and networking devices into the multi-dimensional ArcSight normalization schema. Installation of Connectors and Integration of multi-platform devices with

ArcSight ESM, Develop Flex Connectors for the ArcSight Unsupported devices / Custom Apps Develop content for ArcSight like correlation rules, dashboards, reports and filters, Active lists and Session list. Creating alerts and reports as per business requirements and Threat modelling with specific security control requirements. SECURITY ANALYST SMARTNET IT SOLUTIONS June 2012 to August 2013 ArcSight, Windows, Linux. Installation of Connectors and Integration of multi-platform devices with ArcSight ESM. Configuring log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases and apps. Integration of IDS/IPS to ArcSight and analyse the logs to filter out False positives and add False negatives in to IDS/IPS rule set. Categorize the messages generated by security and networking devices into the multi-dimensional ArcSight normalization schema. Creating alerts and reports as per business requirements and Threat modelling with specific security control requirements. Education Master of Science in Engineering Wright State University - Dayton, OH Bachelor of Technology in TG, IND Jawaharlal Nehru Technological University Hyderabad Skills AWS (1 year), SPLUNK (1 year), SYMANTEC (Less than 1 year), NESSUS (Less than 1 year), NMAP (Less than 1 year), Siem Additional Information SKILLS ArcSight SumoLogic LogStash AWS Burp Suite, Nessus, Nmap, Dir buster Splunk Symantec Critical System Protection (SCSP) Windows, RHEL 6.x/7.x

Name: Travis Morales

Email: davisleah@example.com

Phone: 968.394.7352