Sr. Information Security Analyst Sr. Information Security Analyst Sr. Information Security Analyst - Mast Global Palo Alto, CA Work Experience Sr. Information Security Analyst Mast Global January 2018 to Present Roles and Responsibilities: Driving end to end incident handling/incident response for LBrands and Mast Global. Developing new incident response process to newly added environment and bringing in changes to the existing one. Content creation in ELK. Developing new process in Threat Intelligence and Hunting. Driving Threat Intelligence and hunting activities. Providing threat intelligence and threat hunting metrics to higher management. Preparing metrics on incidents and threat hunting. Fine tuning signatures of incidents raised by MSS partners. IT Security Engineer Qlik October 2017 to January 2018 Roles and Responsibilities * Vulnerability assessment. * Asses MSS Providers for Qlik. * Asses disk/file encryption vendors for Qlik and drive the POC. * Handling phishing events and other security related incidents. * Monitoring IPS/IDS signatures for incidents and drive them towards mitigation. * Monitoring Cisco Umbrella for incidents and drive them towards mitigation. Information Security Analyst III Juniper Networks December 2014 to October 2017 Roles and responsibilities: * Protect Juniper Networks from emerging threats with standard incident handling procedures. * Look for new emerging threats to add its IOCs for monitoring * In depth analysis of headers of spam and phishing mails and driving phishing incidents towards containment, eradication and recovery. * Automation of ticket generation in Service Now ticketing tool with the integration of SIEM. * Assess new tools for POC from security point of view. * Creating metrics on incidents handled to higher management. * Coordinating with MSS Providers in fine tuning signatures. * Training new hires on SIEM management and incident analysis to support ongoing expansion of Juniper SOC. * Vulnerability management (scanning, follow up, remediation). Security Engineer Tata Consultancy Services December 2011 to November 2014 Roles and responsibilities: * Monitoring the security appliance dashboard and investigating the threats and providing deep analysis. * Reporting about the Web/Network related attacks and depicting/justifying the false positives and true positive attacks. * Submitting the IDS/IPS evidence report with the vendor and to do considerable changes in the attack signature. * Identifying the patch levels required for containing the vulnerability. * Various Log analysis depending on the need

and scope. * Analyzing the traffic and identifying the signature pattern related to the attack. * Dealing with the virus related issues/outbreaks and driving them through containment, eradication and recovery phases. * Handling phishing/spam related incidents and driving them towards mitigation. * Submitting the undetectable virus samples to the vendors and getting the right set of signature set to make the detection possible by pushing them to ePO * Written Knowledge base articles on handling specific kind of incidents. Education Bachelor of Engineering in Electronics & Communication RYM Engineering College (VTU University) 2007 to 2011 Certifications/Licenses CCNA CEH GCIH Additional Information KEY SKILLS * Incident handling/response * Threat Intelligence * Threat hunting

Name: Matthew Smith

Email: hsutton@example.net

Phone: +1-344-426-6975x62283