Sr. Security Engineer Sr. Security Engineer Sr. Security Engineer - CloudPassage Sunnyvale, CA Information security professional, having an experience of 3+ years in POC, incident management, malware analysis and troubleshooting of network and security related issues. Familiarity with AWS and Azure Strong hands-on experience in SIEM tools like Splunk, QRadar, ArcSight Strong background on Insider Threat, Cyber Analytics and Cloud Security, UEBA Exposure to ITIL process and ISO 27001 Security Framework as applied to ISMS. Strong analytical and problem solving skills as needed to perform the job of a SOC analyst. Tools used Snort, Nmap, Wireshark, BurpSuite, Metasploit. Good understanding of CISPA and CASB and SaaS Solutions with CSA Matrix. Threat & Vulnerability Management, Change Management and being a key member of a successful Security Operations Centre. Work Experience Sr. Security Engineer CloudPassage April 2018 to Present Experience in cloud security program for CloudPassage Cloud Secure. Hands on knowledge on CISPA. Performed security engineering for complex, multi-platform systems. datacenters, AWS and/or Azure cloud environments Experience in creating detection content and writing correlation rules and business specific use cases Analyze security breaches, perform root cause analysis and plan and implement corrective measures Experience in researching and assesses new threats and security alerts and recommends remedial action Security Engineer Securonix November 2016 to April 2018 Working on Implementation of new data sources, writing parsers and policy for Insider Threat Management. Monitor the Securonix ecosystem including infrastructure, application, database, and data feeds for performance and efficiency Troubleshoot and remediate issues with the Securonix ecosystem quickly to minimize impact on customer environment Work with DevSecOps team to automate tasks that require more effort on daily basis Build and maintain standard operating procedures (SOPs) documentation for each customer Align with co-managed services team where applicable to provide 24x7 support for customers Worked on SecuronixCloud platform using AWS. IT Security Analyst (SOC) NTT DATA August 2016 to November 2016 Creating Dashboards and Reports according to business needs using Advance XML and search queries in Splunk Writing Splunk SPL Queries and Correlation rules Configuring Indexers, Forwarders (Universal and Heavy) and Deployment servers Participated in

daily and weekly standup calls with client for SecOps briefing Responsible for the immediate escalation of Security issues ensuring adherence to SLAs and driving resolution/mitigation in 24/7 environment. Monitoring Splunk health status on daily basis. Build and fine tune custom correlation rules which were used to define the security incident alerts with various priorities. Good working experience in scripting languages(bash) Internship Interactive Intelligence September 2015 to November 2015 Housekeeping of IT assets to prepare them to integrate with SIEM tool Onboarding Data Source to QRadar SIEM Work with various departments like Networks, Systems, Application, Database and Security to solve communication issue between SIEM and data sources Sort events under various categories to meet the compliance requirements of ISO 27001:2013 Modify built-in dashboards and reports Security Analyst ConscienceSoft June 2013 to July 2014 Client - Mercedes Benz Tools - ArcSight, Endpoint Encryption, Data Loss Prevention Responding to and managing security incidents and breaches as appropriate Investigating incidents, remediation, tracking and follow-up for incident closure with concerned teams, stakeholders Assess network activity and system configuration for anomalous activity to determine system security status. Provide network security monitoring, reporting, and incident handling with SIEM Compose security alert notifications. Advise incident responders on the steps to take to investigate and resolve computer security incidents. Create and track investigations to resolution. Assisted in creating an internal knowledge base forum Education Masters of Science in Computer Science THE UNIVERSITY OF TEXAS AT ARLINGTON - Arlington, TX August 2016

Name: Gary Scott MD

Email: fuentesnorman@example.net

Phone: 001-457-325-9951x59663