Senior Cyber Reliability Engineer Senior Cyber Reliability Engineer Senior Cyber Reliability Engineer Westbury, NY (CEH | CHFI | ITIL | ISO 27001 LA) A professional with 8 years and 6 months of experience in Cyber Security and Information Security Systems Management. Able to receive UAE air force and intelligence clearance while working in Abu Dhabi. I have handled a lot of major security incidents and breaches with ease for multiple clients and help them identify, which controls have failed and what remediation needs to be taken to secure their critical data and network infrastructure. I have implemented ISO 27001, Security Operation Centers and managed multiple security products. I can be your trusted security advisor. Authorized to work in the US for any employer Work Experience Senior Cyber Reliability Engineer SKOUT CYBERSECURITY December 2018 to June 2019 Technical Account Manager for Midsize and Enterprise clients for Managed Security Service Provider. Introduction of SKOUT Services to New Client. Manage Tier-3 Technical Customer Escalations. Incident Response for existing Customers Develop and communicate Cyber Strategy/Customer Roadmap Participate in Professional Services Debrief with SME Develop Technical Customer Profiles Identify New Threats and Security pertinent to each customer Technical Advisory (Virtual CISO) for multiple clients. Quarterly Executive Reporting to Business and Technical parties Leading threat advisory meetings. Creating and presenting dark web monitoring reports. Sr. SOC Analyst /Squad Lead Detection & Response Team DarkMatter LLC June 2018 to October 2018 DarkMatter is an international digital defense and cybersecurity consultancy and implementation firm with head offices in the UAE, and research and development centers in Canada, Finland, and China. Squad Lead for Detection & Response Team for SOC operations. Escalation point for major security incidents. Part of Red team exercises & Threat hunting. Deep- dive investigation using SIEM (Splunk) fine-tune and reduce false positives. Forensic Analysis. Co-ordinate with all team members, define and document processes. Maintain compliance with NESA regulations. Security Engineer IT Network October 2016 to February 2018 Advanced Military Maintenance Repair & Overhaul Center (AMMROC) A semi-government organization which is specialized in military MRO services for GHQ of the UAE Armed Forces partnered with Lockheed Martin and Sikorsky Aerospace Services. Security

Operation lead handling critical incidents raised by the SOC team. Review of Policy, Procedures and Work Instructions Advanced Persistent Malware monitoring, investigation, and reporting Next Generation Firewall monitoring, investigation and reporting. Intrusion Prevention System signature review. Supporting ISMS audit requirements. Handling POC for new security products and implemented DLP, Data Classification, etc Manager Information Security Vulnerability Management April 2016 to September 2016 3i Infotech Ltd. Design and implementation of Security Operation Center (SOC). Creating road map, policies and procedures for clients and its subsidiaries. Preparation of job description for tier 1, tier 2 and tier 3 resources. Handling escalation of security incidents. Reporting to Director (CISO). Training new resources for Security Operation Center (SOC) incident handling. Prepared automated health check report from SIEM. Added external open source and paid data sources for gathering threat intelligence. Was responsible for incident escalation and problem management. As part of ISO27001, imparting training on Information Security Awareness to all employees and third parties. Technical adviser for all information security-related matters, part of the change management committee. Senior SOC Analyst Abu Dhabi Commercial Bank July 2015 to March 2016 SecureLink Monitoring and Administration of Security Operation Center. SIEM - Symantec MSS, IBM Qradar Monitoring and in-depth analysis to identify the root cause, providing recommendations to mitigate the risk. Rule creation and modification for alerting offenses, adding log sources, parsing logs using regex for unknown log sources. Verifying the raised incidents and follow-up till closure, handling escalations, mentoring analysts. Handling and tracking IBM and Symantec vendor cases till resolutions. Spam mail, Phishing, Fraudulent Mail Investigation, and reporting. VIP profile users of clients are monitored on Social Media, Fake profiles, accounts are tracked and taken down. Firewall rule change monitoring using Firemon alerts and IPS signature review. Forensic & Malware analysis using virtual sandboxing tools like the cuckoo, virus total. Identifying an Indicator of compromise (IOC) alerting higher management and CERT. Suggesting controls as per the industry best practices, CERT notification and vendor notifications. IT Security Consultant Union National Bank August 2014 to June 2015 Synechron Managing and monitoring of security devices under the

scope of SOC. Perform Vulnerability management with a focus on scanning, detection, and reporting. Liaison with the Team on various aspects of Information Security control assurance. Security log monitoring & incident reporting. Monitoring security incidents and events logs from various devices that are integrated with SIEM solution and managing administration of more than 20+ security solutions. Information Security Analyst Travelex November 2012 to August 2014 Working as part of the Incident Response Team and ISO27001 implementation for Travelex GDC. Spam mail, Phishing, Fraudulent Mail Investigation and reporting to Regional Information Security Managers. Worked as First Responder conducting preliminary interviews, documenting the electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence maintaining the chain of custody and reporting. Worked on X-Ways Forensic for Disk cloning and imaging, trained on Encase and FTK Imager. PCI compliance systems are investigated and monitored using Symantec Managed Security Services. Developing and Presenting Employee Information Security Awareness Programs for Travelex. Reviewing User Access Management (UAM). Setting up processes and procedures for new projects. Monitoring and carrying out mail analysis using Cisco Iron Port. Managing Tripwire, Cyber-Ark (PIM, PSM, PVWA), Websense and Tufin. Reporting to Senior Management for incident alerts and notifications if any, along with weekly and monthly reports on security incidents and trends. Intrusion Prevention System (IPS) Signature based review. Approving Change Request that comes in for Global Information Assurance Team. RSA Envision implementation done for Mumbai GDC. Tripwire FIM Enterprise upgrade is done from 7.7 to 8.3 latest version. Associate Engineer Security Management ICICI Bank December 2010 to November 2012 Wipro Ltd. - India Part of 24*7 On-site Incident monitoring using SSIM (Symantec Security Information Manager), Analysis, Notifications, and Escalations. SSIM (Symantec Security Information Manager) Appliance maintenance, troubleshooting, agent up keeping and adding devices for log collection. To monitor output and events from security devices including firewalls, IDS, and IPS and all SOX critical devices ensure the security events are identified and segregated based on the criticality. Monitoring sources, including Symantec Deep sight, Symantec platinum bulletins and other vendor

bulletins for new vulnerability and threat alerts. Reporting phishing incidents & maintaining tracker. Analysis and reporting of forensic information including customer IDs that have been detected as compromised as part of the Anti-phishing and Anti-Trojan services. Analysis, reporting and ensuring closures for pharming and brand abuse cases as part of the Anti-Pharming and Brand Abuse management services. Monitoring wireless IPS & Firewall assessment tool related to incident management. Good Understanding of Incident Management and RCA process. Education Master of Science - MS in Cyber Security Charisma University 2014 to 2016 Bachelor of Technology in BTech, Computer Science Engineering Karnataka State Open University 2011 to 2014 Diploma in Cyber Security Yashwantrao Chavan Maharashtra Open University 2009 to 2010 Diploma in Computer Engineering Pillai College of Engineering 2006 to 2009 Skills SECURITY, INFORMATION SECURITY, ITIL, PCI, SIEM, ISO27001, SOC, FORENSICS, VULNERABILITY ASSESSMENT, Cybersecurity, Cyber Security, It Security, Nist, Network Security Links http://linkedin.com/in/george-varghese-a377566b

Name: Benjamin Davis

Email: qtyler@example.net

Phone: 952.571.4016x4662