Director of Cybersecurity Operations (Consultant) Director of Cybersecurity Operations (Consultant) Director of Cybersecurity Operations (Consultant) Aldie, VA Work Experience Director of Cybersecurity Operations (Consultant) ECS September 2018 to August 2019 Manage security engagement teams. Trains and educates personnel on security related topics including network and endpoint analysis, forensics, and incident response ? Lead and manage the daily operations of all Cybersecurity Operations services under the contract. Managed multiple client environments ? Drive strategic technological innovation, demonstrating a breadth and depth of knowledge in all things related to the complex operations of the Cybersecurity Operations Center ? Provides recommendations to client leadership and technical management regarding policy compliance, incident response procedures, and security hardening ? Collaborate effectively with colleagues, stakeholders, and leaders across multiple organizations to achieve objectives ? Coordinate program-related activities and deliverables to ensure effective collaboration within the team and across stakeholder groups ? SIEM & Team metrics reporting to client and internal leadership ? Digital forensics and Incident response SME escalation point ? Product/Application POC vetting pre-purchase for internal and client use ? Use case and alarm creation for internal and client environments with focus on emerging threats potentially impacting clients or internal security Director of Regional Sales (Consultant) Film Source May 2018 to September 2018 Management of vendor and client relations ? Website, social media, specialist groups advertising ? Special events organization and promotions ? RFP completion and submissions ? Asist in management of daily operation such as inventory, client scheduling, and account management Senior Cyber Risk Defense Analyst AIG July 2017 to May 2018 Daily triage of escalated events to the SR queue ? Quality assurance checks of event analyst work ? Triage of events via Splunk & Cyber Reason for SR developed rulesets ? Identification of asset compromises for DFIR collection ? DFIR via Volatility with following incident reports for C-Level ? Official floor trainer and daily ad-hoc escalation point for on shift analyst, as well as on-call off shift escalations ? Development and maintenance of phish triage SOP for AIG SOC ? Development and customization of in house VM image for AIG event analyst to work within ? Malware analysis/ Reverse engineering basics of samples submitted via event analyst ? Correlated Search/ Rule creation for notable events triaged by floor analyst Senior III Cyber Security (Consultant) E&Y LLC November 2015 to June 2017 Security Monitoring (Virginia , California, Texas Clients) * Provided daily triage of notables & phish/ Log analysis * Built Analyst VM for Malware Analysis * Correlation search tuning to reduce false positives * Use Case creation * Threat Hunting Training sessions & documentation for new analyst * Malware analysis escalation point * SOP development * SOC infrastructure acquisition * SEIM & Sensor acquisition & deployment * VTI Retro Hunts ? Incident response (Chicago Client) * Custom SPLUNK reporting dashboard for endpoint health monitoring * Custom SPLUNK dashboard to locate high value assets with signatures firing * Custom SPLUNK dashboard for IP to Host name correlation * Custom SPLUNK dashboard for Anomalis email traffic/ IP range to domain mismatch * Developed documentation for each Dashboard purpose and use to hand off to client * Incident identification - Compromised host via APT or Generic Cybercrime * Containment of the asset or assets effected by the incident * Investigation of TTPs via Log & image collection for compromised assets * Eradication of threat/malware from the enterprise environment with network hardening * Coordinate and see the recovery phase of machine/server restoration till ticket close * IR report development & client presentation with proposed changes for future mitigation ? Audit (West Virginia Client) * Subject matter expert for a client SEIM audit * Identified resource inadequacy for endpoint count on the network * The chosen SEIM did not allow real time monitoring against APT * In house hardware to host SEIM was inadequate resulting in storage compliance issues * Primary focus of triage was on the "Infected" phase, no action was being taken to mitigate only response on detection * No Phish triage * Client was not concerned with identified visibility gaps due to housing no proprietary data. This demeanor was gently swayed with a presentation showing risk of market/supplier data theft. LEAD INFORMATION SECURITY ANALYST GE CORPORATE May 2015 to October 2015 Provide leadership to event analysts and serve as an escalation point for security incidents ? Develop and refine processes and procedures for day-to-day operations ? Identify compromised computers using SIEM, pcap, logs, live response, and related computer and network centric evidence sources ? Tune IDS detection signatures to reduce false positives ?

Identify errors in cyber intelligence and update records for identified APT actors ? Identify gaps in cyber intelligence on APT actors and assist with building detection for identified gaps and indicators ? Provide mentoring and training to event analysts ? Provide QA for alerts previously analyzed by event analysts ? Analyze malware carved from network pcap and obtained through phishing attempts ? Work various projects to improve the security of GE network and user environment ? Trained & On-boarded contracted night shift team of six ? Data/Metrics visualization for presenting to management INFORMATION SECURITY EVENT ANALYST GE CORPORATE June 2013 to April 2015 Participate and contribute to weekly training sessions ? Perform daily detect & response functions ? Daily open source malware and malware domain research for preventative measures ? Identify and contain malicious domains and IPs via proxy blocks ? FireEye malware analysis ? Collection of live response data on compromised host ? Corporate Spear Phishing triage ? Identify compromised computers using logs and related computer centric evidence sources ? Accurate and timely routing of verified compromises to the appropriate IT operations teams for further analysis and remediation ? Appropriate escalation of incidents as defined in the established operating procedures ? Continually research the current threat landscape and tactics as it applies to team focus ? Advise management on the effectiveness of established operating procedures and recommend modifications. ? Lead departmental presentation of the SOC for Board member visit in competition against other departments. Winning best in show and second best overall. UIS TECH SUPPORT / NOC TECHNICIAN SSVA - RHT January 2013 to June 2013 Lead Devon IT Thin Client acquisition project communicating directly with the VP to request necessary features and quotes ? Assist Doctors in registering with Universal Identity service ? Maintain ongoing knowledge base ? Configure OTP mobile devices ? Resolve tickets escalated from Tier I UIS Team to Tier II NOC ? Domain Administration ? User management with Active Directory ? Remote Support via Kaseya ? Switch, router, patch panel, and cable management ? Vipre Business antivirus administration ? Network printer and scanner configuration and management ? Configure and deploy client desktops and domain controllers ? Install and configure Cisco VPN client for users ? SSVA & Client Data back up and management ? Windows Update Management ? Server management with Windows Server 2003 & 2008 ? Exchange Management Console ? Thin client configuration and management ? Echo Management Console Administration IT ANALYST DOMINION CREDIT UNION January 2012 to December 2012 Install and maintain server room surveillance system ? Maintain cleanliness of rack cabling and re-cable servers to offer power redundancy on the UPC systems. ? Responsible for daily server backups and offsite storage of backup tapes ? Process DCU transactions to make them viewable to members via online banking services ? Perform checks on the server database to ensure account changes and actions have been properly made ? Troubleshoot DCU workstations ? Logical board repair of KVM server switches ? Headed the release of Docusign an online app for sending and signing EDocs. ? Administrator for Docusign ? Create a change management form to track server changes and updates in the event of a crash or failure ? Assist with maintaining DCU's SharePoint site ? Assist with VMware Image maintenance and updates PC/LAN TECHNICIAN WELLS FARGO - APEX July 2011 to September 2011 Configure new and used laptops and desktops ? Prepare the machines for deployment ? Configure Office laser printers ? Image & Encrypt new hard drives ? Set up user account information and Overlays COMPUTER REPAIR TECHNICIAN/ NETWORK SPECIALIST COMPUTER SURGEONS INC October 2007 to November 2010 Troubleshoot and repair client's computers ? Order and maintain stock/inventory for retail store ? Logical board repair ? LCD Inverter and Back Light repair ? Virus removal ? Data backup and recovery ? Custom computer builds ? Small home and office network setup ? Maintain Company network cabling Education M.S. in risk management and mitigation of APT Western Governor's University - Salt Lake City, UT December 2016 to Present B.S. in Network Security & Management in design and implementation ECPI University - Glen Allen, VA June 2011 Groups EVENT S ORGANIZER & PROMOTER - STAR WARS RIDES NPO May 2018 to Present (https://theresasjacobs.org)   The Foundation s purpose is to provide a fun and exciting Mobile Entertainment themed experience that creates beautiful memories that can last a lifetime for children and adults. Our mission is to create an experience for children and adults who are battling cancer, serious illnesses, have disabilities and challenges.

Name: Benjamin Reese

Email: camposlinda@example.com

Phone: 6136514567