Senior Cyber Forensics Specialist Senior Cyber Forensics Specialist Senior Cyber Forensics Specialist - HCSC / Blue Cross Blue Shield Hershey, PA Able to perform forensic investigations, cyber threat hunting and incident response by utilizing several years as a network engineer and security professional. Always looking to roll up my sleeves and dive in to threats and analysis and able to learn and adapt quickly. Authorized to work in the US for any employer Work Experience Senior Cyber Forensics Specialist HCSC / Blue Cross Blue Shield of Texas January 2018 to Present Perform network forensic analysis on acquired pcap and Bro/Zeek metadata. Deep dive on memory images to extract artifacts to aid in research/investigations. Perform incident response (IR) on proactive and reactive basis. Utilized Volatility, Rekall, FTK, EnCase, SIFT and multiple open source tools for disk and memory analysis. Analyze log files from multiple sources to aid various teams for investigations. Initiated and owned network visibility project from the ground up. Built the forensics lab environment (ESXi and FRED) Trained SOC and junior security members on various technologies and concepts. Information Security Engineer Portico Benefits April 2017 to January 2018 Built out NSM project for packet capture and flow retention. Administer and maintain Splunk Enterprise Security SIEM. Provide IR to security events as they occur. Maintain Varonis environment for DLP and data exfiltration monitoring. Enterprise IT Security Specialist / Senior Network Security Analyst Delta Dental of Minnesota November 2013 to April 2017 Perform Blue Team and hunt searches utilizing zero capital expenditure tools such as Bro, Snort, wireshark, tshark, tcpdump, squil and full packet captures. Implemented expansive internal linux Security Onion IDS system. "Forensicate" based on security leads provided by hunting and automated alerting. Administer LogRhythm deployment and the onboarding of networked devices. Perform incident response and forensics on security incidents, including root cause analysis and management briefing. Manage prioritization and remediation activities/projects and collaborate with impacted departments in remediation. Identify areas for architectural, engineering and operational improvements of existing infrastructure security solutions, and drive such improvements start to finish. Responsible for designing and maintaining Check Point perimeter firewall deployment. Train junior IT and new staff on IDS, firewall and network infrastructure. Network

Engineer Consultant Matrix Communications, Inc January 2012 to November 2013 Extensive experience providing customer service for enterprise businesses. Responsible for architecting and designing elaborate LANs, WANs, and WLANs. Manage relationships with hardware, software, and technology vendors. Stay up-to-date with latest vendor offerings and technical specifications. Responsible for the design and architecture of large enterprise networks utilizing the full Extreme product set. Responsible for pre/post-sales detailed network documentation. Maintain virtual environment for internal organization. Network Administrator Wayzata Properties, LLC 2004 to December 2011 One-man IT shop, end user support, project manager, and vendor coordinator. Designed and supported a Microsoft Windows network utilizing TCP/IP, Active Directory, DNS, and DHCP. Education Bachelor's Certifications/Licenses cissp gnfa gcia gcih gcfa Additional Information SUMMARY OF SKILLS Able to perform forensic investigations, cyber threat hunting and incident response by utilizing several years as a network engineer and security professional. Always looking to roll up my sleeves and dive in to threats and analysis and able to learn and adapt quickly.

Name: Roy Adams

Email: melissacarroll@example.com

Phone: 841-576-1814x279