SOC Analyst SOC Analyst Corona, CA Work Experience SOC Analyst Bechtel - Glendal October 2015 to November 2018 Review, analyze, and parse logs from different internal and external sources to identify, and investigate suspicious and anomalous activity Collect and analyze LR data, artifacts, memory and disk images from live ma- chines Create high fidelity alerts as well as tuning an alert to reduce noise/false positive Proactively hunt for potential attacks, based on indicators, artifacts, TTP, and tools Analyze malicious file using dynamic and static analysis Develop Yara/Snort signatures as well as creating IOC as part of our detection mechanism Identify repeatable task, and develop scripts to automate those tasks Assisted in developing and building out playbooks using security orchestration platform Participate in red team exercise to identify/correct visibility gap as well as testing our capabilities Involved in every step of the incident, from preparation to lesson learned IT Security and Risk Management Intern US Foods June 2015 to September 2015 Create and interpret monthly security reports of compliance with security base- lines, vulnerability patching, and antivirus deployment Identified vulnerabilities, recommend corrective measures and ensure the ade- quacy of existing information security controls Conducted an internal penetration testing to provide proof of concept attacks to demonstrate the vulnerabilities are real Prepared a security awareness article to be published to users on a topic of general user interest Developed and implemented group policy security settings Managed and Utilized SIEM, IDS/IPS, DLP, packet analyzer, vulnerability management and malware analysis tools Deskside Support Arizona State University - Phoenix, AZ October 2014 to May 2015 Assisting faculty, staff and students to evaluate and diagnose technical issues with their personal mobile devices and computers Troubleshooting and diagnosing problems, including identifying and removing malware Install of PC software and peripherals, and Support imaging, setup and deploy- ment of PCs and severs Check with user guides and technical manuals to research solutions Education Bachelor of Science in Applied Computing Arizona State University - Tempe, AZ May 2015 Skills Malware Analysis (3 years), Security (5 years), STIG (1 year), Vulnerability Assessment (3 years), Vulnerability Management (3 years), Linux (5 years), SIEM (3 years), Group Policy (3 years), Security Policy (3 years), Active Directory (3 years), IDP/IPS (3 years), Splunk (3

years), SEP (3 years), Wireshark (5 years), Volatility (3 years), Python (5 years), Incident Response (3 years) Certifications/Licenses GIAC Network Forensic Analyst (GNFA) November 2016 to November 2020 GIAC Certified Forensic Analyst (GCFA) January 2018 to January 2022 Additional Information Skills: Wireshark/Tshark, Volatility, Redline, Bulk Extractor, Python, EnCase, GRR, Yara, Snort, Metasploit, Scapy, ngrep, dnscat2, Bro, Security Onion, ELK, Cuckoo, Xplico, pfSense, Sleuthkit, log2timeline, IOC

Name: Daniel Rodriguez

Email: sayala@example.org

Phone: 959-324-7436x92175