SOC Analyst SOC Analyst SOC Analyst - Binary Defense Systems New Middletown, OH Work Experience SOC Analyst Binary Defense Systems - Hudson, OH October 2018 to Present 24/7 365 - Monitor 30+ clients at a time in various SIEMs (Alienvault, IBM QRadar, LogRhythm, Splunk, etc) including our own proprietary platform called Vision - Monitor client's network/infrastructure for malicious activity and alert them via ticketing system or phone call - Use SIEMs and Loggers to threat hunt to verify if activity is malicious or a false positive IT Security Specialist Medical Mutual of Ohio - Strongsville, OH November 2016 to August 2018 management, infrastructure/network security, and application security - Worked with developers to review secure design/implementation of new code or functionality for applications - Perform red team-like tests to help colleagues detect malicious activity and improve alerting in Splunk enterprise security - Building enterprise vulnerability management program from the ground up - Work as apart of an IT Security team but own multiple individual projects Retail IT Analyst Darice Inc - Strongsville, OH January 2016 to November 2016 environment allowing stores to operate smoothly and solve IT related issues in a timely manner - Provide hardware support and troubleshooting over the phone and also on site for all Information Systems related hardware in our retail environment - Contributing to various ongoing projects such as rolling out Cisco Meraki systems into our retail stores - Serve on the Security Council, a monthly meeting in the IT department where we make decisions on security policies and discuss projects such as ongoing PCI compliance - Work on a team of 5 but also have various solo projects Education BSAS in Computer Information Systems in Computer Information Systems Youngstown State University 2011 to Present Skills C+ (Less than 1 year), Linux (Less than 1 year), Mac (Less than 1 year), Mac OS (Less than 1 year), Metasploit (Less than 1 year), Nessus (Less than 1 year), nmap (Less than 1 year), Python (Less than 1 year), Security (2 years), Splunk (2 years), testing (Less than 1 year), testing tools (Less than 1 year)

Name: Barry Hall

Email: linda50@example.net

Phone: 001-542-528-7857x43775