

Security Operations Manager Security Operations Manager Security Operations Manager - GuidePoint Security LLC Orlando, FL Work Experience Security Operations Manager GuidePoint Security LLC - Saint Petersburg, FL May 2018 to Present Created and delivered weekly, monthly, quarterly and ad-hoc strategic reports and presentations to customer stakeholders. ? Developed tailored and security-driven use case content through SIEM knowledge objects based on threat actor tactics, techniques, and procedures expected or discovered in customer environments. ? Managed customer relationships and expectations with focus on value-driven decision-making. ? Managed team of 7 direct reports. ? Oversaw resource coordination and migration from legacy documentation platform as part of value-add enhancement to services. ? Participated in feedback and improvement cycle of service offerings to customers. vSOC Analyst GuidePoint Security LLC - Saint Petersburg, FL October 2017 to May 2018 Monitored small portfolio of high-value customer SIEM environments and third-party tools for suspicious and anomalous activity. ? Participated in remote incident response engagements with retrospective investigatory support and targeted monitoring efforts. ? Created and responded to customer security incidents in case management system, providing contextual analysis via event correlation, OSINT, and threat intelligence platforms. ? Provided feedback on use-case content to Engineering team to drive content improvements and maturity. IT Security Administrator HostDime.com, Inc - Orlando, FL December 2015 to October 2017 Carried out large-scale infrastructure audits for exploits, vulnerabilities, configuration issues. ? Authored 3x faster malware signature scanner for incident response operations. ? Authored automated tooling for log analysis, IP RBL lookups, CMS file integrity checking, server/network audits. ? Improved existing tooling for WAF Management, spam filtering, incident response. Abuse Security Analyst HostDime.com, Inc - Orlando, FL July 2013 to December 2015 Analyzed logs for threats to ensure systems are clear of malicious actors or compromises. ? Consulted for appropriate remediation steps after cybersecurity events and incidents. ? Analyzed network IPS, detailed firewall, and proxy logs for indicators of compromise. ? Conducted detailed audits for industry-standard requirements (PCI-DSS). Operations Intern CF Industries - Fort Green, FL May 2009 to July 2009 Relocated, repaired, and maintained Dragline excavators on schedule. ?

Rerouted, repaired, and maintained pipeline systems for strip-mining operations. ? Acquired MSHA safety certification for duration of internship. Education Bachelor of Science in Computer Engineering University of Central Florida August 2011 to December 2015

Name: Michael Neal

Email: johngarcia@example.com

Phone: (864)739-5190x622