Incident Response, Senior SOC Analyst, and Contract Lead Incident Response, Senior SOC Analyst, and Contract Lead Incident Response, Senior SOC Analyst, and Contract Lead - Perspecta Burke, VA Cleared and certified Incident Response/Senior Security Analyst with 7 years of experience in the Information Technology and 4 years in Cyber Security. Highly technical and motivated, with experience in intrusion analysis and incident response from start to resolution. Penetration testing hobbyist and enthusiast, looking for opportunities to leverage these skills and knowledge in a red or purple team capacity. Work Experience Incident Response, Senior SOC Analyst, and Contract Lead Perspecta - Herndon, VA November 2017 to Present Facilitating the handling and analysis of declared security incidents to a full resolution Monitoring, analyzing and triaging network & host-based traffic in ArcSight ESM, Splunk, and McAfee ePO Creating and tuning SIEM content in the form of rules, dashboards, queries and reports Developed and continuously improving a new Incident Response Standard Operating Procedure Leading daily morning conferences to review all relevant security events and provide updates Providing 24/7 on call support for incident response and assisting junior analysts Cyber Security Analyst Hewlett Packard Enterprise - Herndon, VA April 2015 to November 2017 Monitored and analyzed traffic in ArcSight ESM and Splunk Escalated security events to appropriate team members or clients to resolve possible intrusions Created tuning requests and suggested content improvements for better intrusion detection Generated, reviewed and sent weekly ArcSight reports to clients. Provided phone and email support for any security related incident found Performed adhoc analysis to find security events that escaped created content IT Support Specialist ALTA IT Services - Rockville, MD November 2013 to April 2015 Daily use of Oracle Cloud Services CRMS RightNow ticketing system Installed and configured of Windows 7 Enterprise x32/x64 and USAccess Software Troubleshoot routers, switches and network connectivity Provided desktop software support for Win7, Java, Adobe, ActiveClient, and Internet Explorer Resolved hardware & software issues across IT platforms for a national network of users Technical Customer Support Representative Kelly IT Resources - Washington, DC October 2013 to December 2013 Daily use of BMC Remedy Action Request Ticketing System Resolved inquiries to the end user's

satisfaction over phone, email and voicemail messages for the Cognosante Exchange Operation Support Center Monitored management systems for tickets assigned to software/hardware/network queues to provide a quick and effective response based on priority level and first-in-first-out basis Provided technical support and guidance to end users experiencing difficulties with applications Snelling Temporary Agency - Chantilly, VA November 2012 to April 2013 Hardware Installation and Peripheral Connectivity Performed workstation Inventory for the EPIC Project (Loudon Hospital) Configured workstations, printers and portable scanners according with network diagram Worked with a small team to roll out 1,000 New WYSE client workstations Installed peripherals on JACO workstations Performed QA & functionality standard of portable WYSE client workstations Education Associate of Science degree in Information Technology ITT Technical Institute - Chantilly, VA September 2013 Skills Esm, Incident response, Ips, Metasploit, Nessus, Siem, Snort, Splunk, Tcpdump, Wireshark, Cyber security, Security, Sql, Python, Scripting, Bash, Linux, Microsoft office, Medusa, Traffic analysis, Network Security, Nist, Information Security, It Security, Comptia Certifications/Licenses Secret Security Clearance A valid IT Specialist certification Additional Information SKILLS & TOOL PROFICIENCIES Skills Incident Response handling and procedure Cyber Security principles and details SIEM monitoring and network traffic analysis SIEM content creation and tuning Snort and YARA signature creation Bash and Python scripting Server OS hardening and assessment Script analysis of excessively large raw log files Host enumeration and vulnerability assessment Exploitation and post exploitation pivoting Privilege escalation and local host enumeration Create functional exploit from Proof of Concept Fuzz applications to develop Proof of Concept SQL injection and blind SQL injection Cross Site Scripting - Session Hijacking Exploit language conversions Obfuscation and IPS evasion Procedure development & process improvement Developing training materials for juniors Strong written and oral communication Ability to build productive relationships, resolve complex issues and win customer loyalty Interfacing with government clients Tool Proficiencies ArcSight ESM & Logger, Splunk, Sguil TippingPoint, Snort, Bro McAfee ePolicy Orchestrator Bash & Python Wireshark & tcpdump YARA VirusTotal Intelligence, RiskIQ PassiveTotal

Tanium Any.run Sandbox Sysinternals Suite Security Onion - Personal Research Tool Tenable Security Center Kali Linux - PWK Student Nessus, OpenVAS, Nikto, SQLmap Dirb & Dirbuster Enum4linux, nbtscan, snmpwalk Metasploit, nasm, venom, shikata_ga_nai BurpSuite, TamperData Netcat, Ncat Hydra, Medusa, Ncrack, Hashcat, John Powershell Microsoft Office Suite

Name: Matthew Nguyen

Email: reynoldsthomas@example.com

Phone: +1-421-475-3797x1904