Michael L. Register

www.linkedin.com/in/mregister

PROFESSIONAL PROFILE

Highly driven analyst with a passion for Security and Information Technology. Quick to pivot during incident investigations given new evidence discoveries. Intermediate level Windows Forensic concepts gathered from working cases involving Emotet, TrickBot, Ursnif, QBot, and Ulise malware families. Avid scripter constantly looking for ways to make remedial tasks more efficient, typically implemented via PowerShell or Python. Intermediate malware analysis capabilities covering basic static and behavioral analysis techniques, and actively learning debugging and disassembly concepts. Team player with a drive to mentor and skill share on a team for group growth. Co-author of “DFIR Against the Dark Arts” training course for entry level security analysts in local InfoSec community.

TECHNICAL SKILLS

Programming:	Python, PowerShell, VBA, Java (beginner level), Object Oriented Programming Concepts
Operating Systems:	Windows, Linux (Ubuntu, Kali, Red Hat), macOS (User/Troubleshooting experience)
Tools:	FTK Imager, Plaso, EnCase, Cylr, CDQR, REMnux, SIFT, Tanium, Splunk
Conceptual:	Windows Forensics, Incident Handling, Networking, Troubleshooting

CERTIFICATIONS

- CompTIA Security+
- CompTIA A+
- CIW Web Security Professional
- CySA+
- CCNA (exp. 09/2020)
- GCIH
- SSCP

PROFESSIONAL IT EXPERIENCE

Sr. Cyber Forensics Analyst (SOC Tier 3 - IR) Date: Jul. 2019 – Oct. 2020

Raytheon - Morrisville, NC

(Same client as Niksoft contract)

Tier 3 Analyst in the SOC to act as Incident Response during active Incidents. Provide mentoring to Tier 1 and 2 analysts to increase skillset. Assist in monitoring and triage of security events for country wide network belonging to Civilian Federal Agency. Investigate remote systems through Command Line interaction to determine or identify suspicious activity on hosts. Perform basic malware analysis and forensic investigations into identified malware events on user endpoints.

- Technical SME for forensic investigations on Windows workstations as part of malware infection response.
- EDR SME for the team to assist with reviewing and responding to security alerts on endpoints.
- Assisted in mentoring SOC analysts in malicious file analysis and handling for IOC discovery and mitigation.

Cyber Security Analyst (SOC Tier 3 - IR) Date: Dec. 2017 – Apr. 2019

Niksoft Systems Corp - Morrisville, NC

Tier 3 role included handling escalated cases from Tier 1 and 2 analysts in the SOC. Performed behavioral and basic static analysis on identified malware samples for IOC generation. Assisted as technical SME on concepts ranging from macro code de-obfuscation to network traffic analysis. Coordinated with peers to provide technical guidance on policies and procedures. Handled identified incidents and engage with Law Enforcement entities as necessary.

- Drastically improved basic automated process for administrative overhead on case notes through PowerShell scripting.
- Acted as the ad-hoc “DevOps” analyst in developing one-off tools specific to the enterprise environment and configuration.
- Performed in-depth analysis of .NET Framework versions and TLS version mismatches with PowerShell macro viruses to show failures in malware delivery specific to the enterprise.

Wi-Fi Solutions Engineer Tier 2 Date: Aug. 2017 – Dec. 2017

Spectrum Enterprise – Crossfire Consulting Contractor - Raleigh, NC

Received escalated tickets from Tier 1 group for advanced troubleshooting with end users as needed. Analyzed and resolved OSI Layer 1 and 2 problems. Assisted other Tier 2 Engineers with advanced configuration adjustments as needed, including but not limited to:

- Dynamic VLAN assignments
- ElevenOS Radius Integration
- MST Configurations
- ACL Adjustments/Implementations
- Port Security best practices
- Initializing and programming new switches and routers for deployment

Network Operations Center Engineer Date: Mar. 2017 – Aug. 2017
Cisco – Apex Systems Contractor - Morrisville, NC
Monitored Campus and Branch network infrastructures. Troubleshot network issues including but not limited to EIGRP, BGP, common L2 and L3 problems. Engaged various ISPs to resolve WAN connectivity issues as needed. Worked with on-site technicians to perform equipment change-outs and troubleshooting as necessary. Troubleshot Cisco Aironet series wireless APs and 5500 Series WLC platforms.

Network Operations Center Technician Date: Aug. 2016 – Feb. 2017
American Tower Corporation - Cary, NC
Monitored lighting and generator status on Cellular Tower sites throughout the continental U.S. Worked with site technicians to provide check in and check out times and tracking for record keeping. Troubleshot and validated working operation of lighting systems with site managers and repair technicians. Notified FAA in accordance with federal regulations on lighting issues to generate NOTAMs for pilot awareness of hazards.

EDUCATION

Bachelor of Science Cybersecurity and Information Assurance Anticipated Graduation: Feb. 2021
Western Governors University, Salt Lake City, UT

- Studies focused on Network Infrastructure Design and Security, Incident Handling and Digital Forensics
- Courses include IT Project Management, Data Management, Digital Forensics, and Cloud Foundations

Associate of Applied Science in Computer Technology Integration Graduated: Dec. 2016
Cape Fear Community College, Wilmington, NC

- Diplomas in Network Administration, Software Development, and Information Technology
- Courses included Cisco CNA, Linux and Windows Server Management, Beginner and Advanced Java programming, Object Oriented Programming fundamentals, Structured cabling, and Security Fundamentals