BRIAN T. CARR, MS, GCIA, GOSI

East Greenbush NY, 12061
briancarr.org | brian@briantcarr.com | linkedin.com/in/briancarrcyber/

SUMMARY

Driven Device Engineering Specialist and Cybersecurity Professional seeking full-time remote employment. Technically advanced through coursework, work experience, and self-taught knowledge in cybersecurity, digital forensics, network security monitoring, and detection engineering. Strengths include careful, detailed work and flexibility in quickly adapting to new projects. Proven ability to lead and collaborate with team members. Excellent verbal and written communication skills. Strong desire to continue to learn and grow as a professional within the cybersecurity field.

EDUCATION

Master of Science in Cybersecurity Utica University, September 2021
Specialization in Malware Analysis
Specialization in Computer Forensics

Bachelor of Science in Cybersecurity Utica University, May 2019
Specialization in Network Forensics and Intrusion Investigations

PROFESSIONAL SKILLS

GIAC Certified Intrusion Analyst (GCIA)	GIAC Open Source Intelligence (GOSI)	GIAC Certified Forensic Examiner (GCFE)
Linux System Administration	AccessData Forensics Toolkit	CrowdStrike EDR
Regular Expressions / Grep	IDS Rule Development	ClamAV Signature Development
Dynamic Malware Analysis	Splunk	Bash / Python Basic Scripting
Suricata / Snort	Volatility / Memory Forensics	Nmap / Nessus
YARA	CrowdStrike EDR	SIEM Detections

EMPLOYMENT EXPERIENCE

Device Engineering Specialist June 2021 – Present
Center for Internet Security, East Greenbush, NY

Associate Device Engineering Specialist January 2020 – June 2021
Center for Internet Security, East Greenbush, NY

- Onboarded Albert IDS sensors for the MS-ISAC and EI-ISAC.
- Performed support and maintenance on Albert IDS sensors.
- Resolved over 1500 support tickets.
- Wrote bash scripts to automate various steps in the onboarding process.
- Wrote a bash script to automate steps in the Albert support process.
- Tested newly written IDS rules to ensure functionality before implementation in production.
- Utilized Splunk to analyze and troubleshoot Albert sensors.
- Utilized Crowdstrike EDR.
- Wrote SQL queries to obtain data from an Oracle database.
- Participated in developing a Detectiong Engineering plan.
- Participated in developing monitoring and detection alarms in Splunk.

Computer Emergency Response Team Intern May 2019 – January 2020
Center for Internet Security, East Greenbush, NY

- Analyzed suspicious emails submitted to the MS-ISAC and EI-ISAC.
- Analyzed malware submitted to the MS-ISAC's and EI-ISAC's Malicious Code Analysis Platform (MCAP).
- Wrote a bash script that parses relevant email header information.
- Participated in incident response calls with the MS-ISAC CERT.
- Performed analysis on a system infected with ransomware and successfully determined how the infection occurred.
- Analyzed forensic images, memory captures, and various logs in both training scenarios and incidents.

COLLEGIATE AFFILIATIONS

Member, Utica College Cybersecurity Club 2017-2019
Athlete, Alfred State NCAA Division III Wrestling Team 2014-2015