Andrew Hogan

| Augusta, GA 30907 | (440) 821-6767 | hoganandrew620@gmail.com |
| --- |

# Objective

| Seasoned IT Security leader with experience implementing Department of Defense critical infrastructure security solutions in a demanding environment while providing top-level IT security leadership and direction focused on securing modernized IT security platforms, leading IT security functions for cybersecurity metrics for daily threat picture in both a classified and unclassified environment. This includes the management of cybersecurity metrics fort Owner/Operators, CISO’s, and Executive level dashboard and other reporting requirements, cybersecurity, and resiliency assessment reports to ensure all stakeholders are effectively informed, and review of risk management programs. |
| --- |

# Skills & Abilities

|  |  |  |
| --- | --- | --- |
| |  |  | | --- | --- | | Windows and Linux Forensics  ELK and Splunk Fundamentals  Tenable Nessus Security Center  Static/Dynamic Malware Analysis  MITRE ATT&CK Framework  VirusTotal  Living off the Land Binaries  Threat Management  Vulnerability Analysis | Risk Management  Sysinternal  Ghidra  Wireshark  TCPDump  Berkeley Packet Filter  Snort  Bash  PowerShell | |

# Experience

| December 2019-Present | Cyber Operations Specialist, US Army   * Served as the led Cyber Threat Analyst, Operation Security (OPSEC) Program Manager. * Developed and established the OPSEC program for senior leadership and all subordinate organizations. * Review violations of computer security procedures and developed mitigation plans * Assess the security impact of security alerts and traffic anomalies to identify malicious actions to escalate up to senior members of the team. * Create Cyber Threat Hunt hypotheses based of known tactics, techniques, and procedures (TTP) * Monitor Security Information and event Management (SIEM) solutions and analyze log data. * Generate static file fingerprints of suspicious files via PowerShell for analysis using OSINT tools such as VirusTotal. * Utilize discoveries from the incident response process to make significant and/or complex improvements to the existing detection capabilities, operational processes, and security controls. * Proactively and iteratively search through systems and networks to detect advanced threats. * Conduct Digital Forensics investigations n Malware Analysis to identify malicious activity and derive Indicators of Compromise (IOC) and associate detection rules. * Perform credentialed/non-credentialed scans on Windows host, servers, and routers and switches. |
| --- | --- |
| March 2016-December 2019 | Information Technology Specialist, US Army   * Used Remedy ticketing system to manage and process support actions and request. * Worked closely with senior management to plan, develop, coordinate, and execute technical strategies aligned to client’s vison, mission, and purpose. * Managed customers expectations of support and technology functionality to provide a positive user experience. * Defined and documented technical support best practices for networking and end user technologies. * Configured end users and administrative permissions through Active Directory. * Patched and mitigated software and hardware to eliminate security risks and protect data. |

# Education

| January 2023-Present | Bachelor of Science in Cloud Computing, *Western Government* *University* |
| --- | --- |

# Certifications

| (ISC)2 CISSP  CompTIA Cybersecurity Analyst  (ISC)2 Certified in Cybersecurity  CompTIA Security+  CompTIA Network+ |
| --- |

# Continuing educations

| Home lab for malware analysis, threat hunting, and SEIM projects  Enrolled in TCM Security Practical Malware Analysis & Triage |
| --- |