**Zackary Watson**

Active TS/SCI with CI Poly | IAT LVL 2

987 Glenhaven Dr, Evans GA 30809

**Cell: (813)-431-6599**

**Github:** https://github.com/zmwats

**Email:** [**zmwatson18@gmail.com**](mailto:zmwatson18@gmail.com)

(If you require additional information, please feel free to contact me via the above means to coordinate further discussion in a secured environment)

**Summary**

With over eight years of experience as a cleared professional, I have extensive experience in various roles supporting cybersecurity operations, technical instruction and technical writing/documentation, as well as systems administration with a working understanding of virtualization and networking. I constantly strive to solve and provide solutions to multifaceted and complex problems, as they arise in rapidly changing dynamic environments.

**Experience:**

**Athena Technology Group**

**Cyber Technical Instructor / Writer / Lead Offensive Security Content Developer**

**Fort Gordon, GA / U.S. Army Cyber Center of Excellence**

**(12/2021-Present)**

* Facilitates the instruction of cyber security concepts and foundational fundamentals necessary to equip incoming personnel with the knowledge required to function within their work role as Cyberwarfare Specialists. These fundamentals include networking, Windows and Linux related security, Unix operating systems and basic python programming and bash/powershell scripting, buffer overflow and injection attacks, security device evasion techniques, as well as application vulnerability identification and mitigation strategies..
* Develop technical documentation, consisting of key points of discussion during lecture for instructors to effectively facilitate learning of the required content within the learning module.
* Draft and develop various technical documents pertaining to the use of offensive security tools and tactics., utilizing ASCIIDoc and managing version control through the use of Git.
* Routinely utilize openstack technology to create virtualized environments for students.
* Routinely utilized and demonstrated the use of Wireshark, Nmap and other tools for the purposes of protocol analysis, target system enumeration, and other hacking methodologies.
* Consistently modify and update technical documentation to create a thorough module of learning, pertaining to offensive security concepts and fundamentals.
* Develop TRADOC cyber scenarios in order to educate students on the tactics, techniques and procedures utilized by adversaries in order to compromise network infrastructure and other high value targets
* Facilitate the instruction and learning of network security technologies such as firewalls, SIEMS and IDS/IPS devices such as Snort.
* Educate students on industry-standard best practices concerning IDS/IPS placement and explain various types of network infrastructure topologies that would result in a secure network, following a defense in-depth approach.
* Educate students on both the MITRE ATT&CK Framework, as well as the Lockheed Martin Cyber Kill Chain framework in order to fully comprehend the philosophy of attack planning from an offensive and defensive perspective.

**BAE Systems Inc**

**Active Geolocation Intelligence Analyst/Operator**

**Fort Gordon, GA**

**(09/2021-11/2021)**

* Possesses a strong knowledge base of GSM and RF communications and infrastructure.
* Supported a Joint aerial intelligence surveillance and reconnaissance operations mission focused on providing actionable intelligence and geolocational information to ground force command in various theaters of operation

**U.S. Army**

**Signals Intelligence Analyst**

**Fort Gordon, GA**

**(10/2014-10/12/2021)**

* Provide real-time and near real-time actionable intelligence to warfighters and combatant commands in support of strategic and battlefield operations in several AORs.
* Analyze large sets of data to create finished intelligence products.
* Author and edit serialized intelligence reports for further dissemination to senior leadership.
* Facilitates target prioritization and deconfliction.
* Conduct extensive research on persons, organizations, social networks, technologies and infrastructures of interest, to aid operational goals and efforts on a routine basis.
* Creates, presents and briefs tailored intelligence products to senior leaders in both physical and digital environments by both oral and written means of communication.
* Routinely analyze metadata that is significantly related to targets of interest.

**U.S. Army**

**Target Digital Network Analyst (Cyber Warfare Analyst)**

**Fort Gordon, GA**

* Support and enable Offensive Cyber Operations, performing analysis for target infrastructure exploitation activities.
* Gather and analyze open-source and all-source intelligence for intelligence value as it pertains to potential vulnerabilities against specific targets.
* Facilitates target prioritization and deconfliction.
* Routinely analyze metadata that is significantly related to targets of interest.
* Build operational and mission data trackers and other working aids.
* Conduct and document social network analysis.
* Develop target profiles for analysis and continuity.
* Identify intelligence gaps and analyze target communications to identify key CCIRs and PIRs in order to meet organizational objectives.
* Routinely utilize and query key intelligence collection databases.
* Facilitates target prioritization and deconfliction.
* Provide senior leadership with the actionable intelligence and expert assessments, required to make informed judgments and decisions in high-stress situations.
* Analyzes digital network intelligence and conducts header analysis, performs target development on social networks, network infrastructures and priority targets; finding credentials and potential vulnerabilities that cyber operators may use to exploit priority targets.
* Participated in the development and creation of new exploitation strategies and techniques, to be used by the cyber mission force in offensive operations, in order to penetrate adversarial infrastructure.
* Utilize a strong understanding of networking concepts such as DNS, DHCP, SSL, OSI Model, and TCP/IP.
* Maintains knowledge of cyber-attack stages within the MITRE ATT&CK and Lockheed Cyber Kill Chain frameworks.
* Conducts deep dive research on target tactics, techniques and procedures (TTPs).
* Strong understanding of phishing (including various sub-types of phishing), social engineering and other common threats.
* Author and edit detailed time-sensitive serialized and technical reports based on collected intelligence.
* Supports multi-discipline operations and contributes to cross-community meetings on a routine basis.

**U.S. Army**

**Systems Administrator**

**Fort Gordon, GA / U.S. Army Cyber Command Joint Mission Operations Center**

* Maintained situational awareness of network connectivity at all times.
* Managed, operated and maintained physical and virtual desktops, thin clients, WAN/LAN, VPN/VPS support and network infrastructure equipment, utilizing VMware, and running Linux and Windows operating systems.
* Experienced in virtualization administration utilizing VMWare Horizon, vSphere and ESXI.
* Routinely utilized PowerShell and bash scripts in order to access and transfer files, and conduct other daily activities.
* Managed user privileges and accesses utilizing active directory on a frequent basis.
* Utilized JIRA for ticket management.
* Conducted bi-daily briefs to provide frequent communication with team members and senior leadership regarding the status of mission-critical infrastructure.
* Independently managed required tasks and protocols to ensure operational success.
* Conducted routine operational checks on complex systems, networks and infrastructures.
* Performed troubleshooting techniques on physical and virtual desktop systems and network infrastructure, providing solutions and support to end-user clients.
* Assisted in the training of new personnel, in order to sufficiently meet mission requirements.

**U.S. Army (Theatre Support Activity)**

**Collection Manager/Auditor/Report Release Supervisor**

**Fort Gordon, GA**

* Maintained and managed a large ingest of collection to critical databases from various collection sites for further transcription and dissemination.
* Edited and released time-sensitive serialized intelligence reports, providing actionable intelligence and force protection warnings to service members in battlefield environments
* Performed routine audits against database queries to ensure regulatory, policy and legal compliance.
* Conducted daily briefs with coworkers and senior leadership in order to provide situational updates regarding the operational status of persistent data flow.

**U.S. Army (Operation Inherent Resolve)**

**Lead Targeting Analyst/Report Release Supervisor**

**Fort Gordon, GA**

* Created and briefed high-priority target packages to senior leadership and combatant commands, based on geolocation intelligence for nomination, effectively leading to the capture or elimination of several high-value targets.
* Build operational and mission data trackers and other working aids.
* Conduct and document social network analysis.
* Develop target profiles for analysis and continuity.
* Identify intelligence gaps and analyze target communications to identify key CCIRs and PIRs in order to meet organizational objectives.
* Routinely utilize and query key intelligence collection databases.
* Facilitates target prioritization and deconfliction.
* Authored, edited and released time-sensitive serialized intelligence reports, enabling force protection warnings and providing actionable intelligence for further development and analysis.
* Coordinated the analytic efforts of multiple teams, in order to cohesively provide timely and accurate intelligence products necessary to drive the operational process.
* Provided analytical assessments as a subject matter expert, to senior leaders and aid the decision making process.

**Technical Skills**

● Software: Experienced in the Microsoft Office Suite (Word, PowerPoint, Excel), Kibana, PFSense, SolarWinds, VMWare ESXi, Active Directory, JIRA, Sharepoint, Nmap, Wireshark, Snort, Splunk, Visio, Silo, Palantir, OSINT Framework, GITlab/GIThub, MSTeams, Confluence

● Operating Systems: Experienced in Windows (7,8, 10), various Linux Distros (Kali, Ubuntu, Mint, CentOS) and Unix environments.

● Computing Languages: Working knowledge of HTML, CSS, ASCIIDoc, BASH, Powershell, Python, YAML

● Certifications: Security+ (SY-601)

**Education**

2022-Present

**American Military University***-Pursuing BS Cybersecurity*

*(expected completion Spring 2024)*

2022

**Common Faculty Development Instructor Course (CFDIC) - U.S. Army**

*Fort Gordon, Ga*

2020-2021

**J7 Pipeline - U.S. Army**

*Fort Gordon, Ga*

2015- 2021

**National Cryptologic School***- Numerous courses*

January 2015-July 2016

**Basic Analysis and Reporting Course (BARC) 35N Signals Intelligence Analysis Course***- Goodfellow AFB, San Angelo, TX*