R. Alex Rhodes

(915) 207-6275 | alex.rhodes79@outlook.com | [Alex Rhodes, CISSP | LinkedIn](https://www.linkedin.com/in/alexrhodes79/)

**CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL | CYBERSECURITY | DIGITAL FORENSIC**

Strategic, innovative cybersecurity and Certified Information Systems Security Professional with extensive experience leading national and global security programs. Recognized for performance excellence and developing ''High Performing teams through creating a positive, supporting and work-working team culture built through trust, compassion, and humility. Brings over 15 years of progressive leadership experience in digital forensics, investigations, cybersecurity, including strategy, financials, team development, operations, growth, and compliance. Strong experience with NIST, DODI 8501 Risk Management Framework (RMF), Security Assessment Plan (SAP), Security Assessment Reports (SAR), System Security Plan (SSP), and Security Control Traceability Matrix (SCTM).

* **Active TS/SCI security clearance with a CI poly**
* Retired from the Army Dec 2018 after 15 years of service, including over 8 years in cyber security and information assurance, as a cybersecurity professional, digital forensic examiner, special agent, and intelligence analyst.
* Excellent verbal/written communication, with ability to communicate effectively with individuals at all levels of responsibility and authority; ability to prioritize, lead/support an environment driven by customer service and teamwork.
* Strong troubleshooting and organizational skills; ability to participate in resource planning processes based on defined organizational plans.
* Demonstrates excellent organizational direction, time management, problem-solving, prioritization, goal setting, leadership, motivation, negotiation, & interpersonal relations.

**PROFESSIONAL CERTIFICATIONS**

**CISSP**, Certified Information System Security Professional, ISC2 (current, Dec 2017)

**MCSA**, Microsoft Certified Solutions Associate, Server 2012, Microsoft, Dec 2015

**Security+**, CompTIA (current, Oct 2015)

**Certified Cyber Crime Investigator**-Department of Defense Computer Investigations Training Academy

**Certified Digital Forensic Examiner**-Department of Defense Computer Investigations Training Academy

**Certified Digital Media Collector** -Department of Defense Computer Investigations Training Academy

**PROFESSIONAL EXPERIENCE**

**Cyber Security Researcher**

**Stephenson Technologies Corporation 05/2021-Present**

Participates in the development of significant new concepts or novel approached to Cyber Security. Works with customers as part of a team to develop requirements, produce/test code, and provide necessary documentation.  Develops technical solutions for information operations and analysis related to national security topics, intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools and data visualization techniques.

* Researched and co-authored a research paper on the HiveNightmare vulnerability then used the information to conduct a penetration test on air-gapped network demonstrating the security of that project.
* Authored at least 10 research papers into vulnerabilities within security systems and medical devices (pending disclosure notifications and publication).
* Provided guidance and direction for cybersecurity research leading to two projects approved for research and one project pending publication.

**Senior Cyber Security Architect/Engineer**

**Northrop Grumman, Buckley AFB, Aurora, CO 02/2020-05/2021**

Served as the Cyber Architect to the U.S. Space Force. A key leader and primary point of contact for reverse engineering telemetry for the space platform cybersecurity project. Provided engineering assistance with creating an enterprise-wide logging solution with a centralized reporting service. Provided strategic thought leadership and tactical recommendations to drive the maturity of the overall program through improvements to the incident response function.

**Cybersecurity Leadership**

* Collaborated with developers to assist with creating Kibana dashboards from telemetry engineering documentation. This allowed for the automated processing and decoding of TT&C data so operators could monitor the satellites for the potential of compromise and the status of health in near real-time.
* Established the mission mapping cell by creating a database of IP addresses and hostnames from engineering documents, creating physical and logical network maps for over 23 enclaves, and providing training on these tasks to others.
* Created network diagrams and install checklists for installing Gigamon tap and aggregation hardware into a remote site for network monitoring.
* Created documentation to track IT asset lifecycle, monitors change requests and creates incident response sections.
* Assisted the system administrator with fixing several issues regarding Puppet, CentOS configuration, Gigamon configuration, and NTP issues related to an installation of Manticore.
* Provided executive guidance for the requirements to convert a watch floor into a SCIF. Drafted Standard Operating Procedure (SOP) for System Administrator section.
* Collaborates with other engineers to create a training plan to teach telemetry and satellite commanding to cybersecurity mission defense teams.

**Client Relationship Management**

* Analyzed the client's business culture, structure, processes, data, management, and performance criteria based on the scope of work, the sector in which it operates (including trends), as well as current political, economic, social, technological, legal, and environmental factors.
* Confidently presented/communicated with a diverse client and internal audience (including C-Level and Board), ensuring that the intent of presentation/communication is conveyed, which may include adapting presentation/communication style to suit the target audience.

**Key Highlights**

* Reverse engineered three satellite Tracking, Telemetry, & Commanding systems (TT&C) using the engineering documentation to create message data structures and signatures of satellite TT&C data traffic traversing the network. Decoded over five satellite command messages by hand, converting from hexadecimal to binary and decimal while cross-referencing the data structures created above to decode the messages. Message traffic was passed in binary or hexadecimal, and the engineering documents were written in binary, decimal, octal, and hexadecimal.
* Drafted requisite rack elevation and wiring diagram documentation to install three cybersecurity solutions, two in remote locations, during the Coronavirus lockdown
* Drafted and implemented the plan to install and maintain over 9 racks of hardware to monitor critical network infrastructure with minimal downtime
* Started implementation of Machine Learning within an Elasticsearch SIEM solution supporting over 23 enclaves in local and remote locations.

**Senior Cyber Security Engineer (ISSO)**

**Lockheed Martin, Waterton Campus, Littleton, CO 03/2019-02/2020**

Consistently Ensured that the technical administration of information security is in accordance with internal Lockheed Martin and government security requirements under the Risk Management Framework (RMF) and National Institute of Standards and Technology (NIST) standards. Created plan, which received customer approval, to sanitize all forms of digital media locally.

* Drafted and received tentative approval for the only sanitization plan for 3D-printed classified material in the industry.
* Created and implemented security measures for classified Information Systems in accordance with Government directives and facility procedures
* Functional knowledge of current Information Assurance (IA) policies as a contributor to the architecture and design of secure solutions to support government needs and requirements.
* Ensured approval of over 100 pieces of hardware and software to include advanced and prohibited technologies such as 3D printers, still and video cameras, High-Performance Computers, and wireless and drone capabilities.

**Key Highlights**

* Recipient of the Lockheed Martin 2020 Technical Innovation Award for pioneering work in developing and implementing a TSCIF within a large robotics lab allowing for a customer demonstration for one of the most daring space missions attempted.
* Fulfilled ISSO/ISSM, Information Assurance, Cyber Security Architect, System Administrator, and Network Administrator roles to ensure the mission success.
* Drafted, submitted, and received approval to turn an unclassified high-bay robotics lab (SOSC) into a temporary classified facility for testing within the first 4 months of employment. This included drafting both the physical and network security plans.

**Senior Cyber Security Engineer**

**ITEC / Raytheon, Buckley AFB, Aurora, CO 10/2018-03/2019**

Provided and integrated enterprise IT auditing tools and support, including the configuration of Linux and Windows systems to forward logs into SIEM tool RSA NetWitness.

Conduct collection, consolidation, de-confliction, and dissemination of metrics for multiple systems providing information systems security-related audit information to SIEM tools.

* QA/QC of collected audit information and providing direct customer support.
* Generated and reviewed of knowledge articles, process documentation, and SOPs.

**Key Highlights**

* Streamlined the Assessment and Authorization process according to the NIST RMF, metric consolidation, data parsing, and validation of ingested Audit information utilizing SIEM tools such as RSA NetWitness and HP ArcSight, of enterprise-level system audit information and provided compliance recommendations for a variety of computer operating systems and applications.
* Developed technical packages and adapted the packages to each organization's network architecture to streamline the onboarding of a SIEM system.

**Assistant Special Agent in Charge**

**Digital Forensics Research Branch, Computer Crimes Investigative Unit**

**U.S. Army Criminal Investigation Command, Quantico, VA** **07/2017-10/2018**

Supervised and mentored an assigned staff of 7 expert-level digital forensic examiners on the proper methods of **tool tests**, research projects, and digital forensic examinations. Guided the creation and maintenance of Standard Operating Procedures and similar documentation such as local and command-wide policies and regulations relating to digital forensics and Information Assurance.

* Reviewed the ISO standards and prepared guidance for DFRB to become **ANAB ISO/IEC 17025** Forensic Science Testing Laboratory accredited, allowing DFRB to move forward with an accreditation timeline.
* Investigated potential, successful, and unsuccessful intrusion attempts and compromises of Army networks through reviews and analysis of relevant event detail. Investigated intentional access or destruction of information from Army networks and made recommendations to increase the security posture of the affected networks.
* Performed preliminary and advanced forensic evaluations of internal and external computer systems and network

**Key Highlights**

* Demonstrated the Army CID digital forensics structure, current and future capabilities, and expert witness training to over 120 Department of Defense lawyers at the U. S. Army Judge Advocate General schoolhouse.
* Designed the next-generation forensic computer for all forensic examiners within Army CID.

**Senior Digital Forensic Examiner**

**Digital Forensics Research Branch 01/2016-06/2017**

Investigated potential, successful, and unsuccessful intrusion attempts and compromises of Army networks through reviews and analysis of relevant event detail and made recommendations to increase the security posture of the affected networks to include remediation of vulnerabilities, OS hardening, and policy and procedural changes.

* Guided the creation and maintenance of local SOPs. Researched emerging technologies to include a published joint study on the location of Cortana search artifacts within the Windows 10 Registry and Cortana app.
* Performed preliminary and advanced forensic evaluations of internal and external computer systems and networks.

**Key Highlights**

* Conducted 10 digital forensic examinations involving over 15 digital media items and approximately 10 Terabytes of data for evidence of intrusions into U.S. Army computer network systems comprised of Unix and Windows systems.
* Assessed and reported on three forensic tools enhancing the capabilities of all forensic examiners within U.S. Army CID.
* Trained over 120 Department of Defense lawyers on digital forensics and using expert witnesses at trial.

**INFORMATION SECURITY MANAGER**

**Digital Forensic Examiner 07/2018-09/2018**

**Field Investigative Unit 05/2015-07/2017**

**United States Army Criminal Investigation Command Alexandria, VA**

Designed and established or transform IT risk management, governance, and compliance programs based on clients’ business structures, strategies, and priorities. Advised on, developed, and implemented processes around risk identification, assessment, and remediation, including issues management, exception management, vendor risk management policy management, and security incident and vulnerability response. Performed Knowledge Transfer of incident handling, forensic Analysis, and Malware Triage in line with the NIST framework for incident response.

Information Security

* Maintained a functional knowledge of current IA policies to support customer needs and requirements.
* Prepared the documentation to support the Assessment and Authorization of a closed, restricted network at the TS//SCI//SAR with 2 stand-alone platforms IT systems.
* Managed the security of information systems assets on 7 networks of different classification levels from intentional or inadvertent access and destruction.
* Acquired authority to operate (ATO) certification by writing the System Security Plan (SSP) utilizing the JSIG - Risk Management Framework (RMF) with IC controls for a closed, restricted network while supporting 86 computers on 7 networks.
* Designed and built a thin-client Active Directory domain consisting of Dell Wyse clients and Windows Server 2012R2 server architecture for 16 clients and 7 servers, improving the security posture.
* Developed and published an incident response plan, POA&M, data transfer agent procedures, digital forensic examination Standard Operating Procedure, media control logs, and destruction of classified media guidance, increasing the readiness and capabilities of FIU.
* Administered Windows Server 2008R2 Active Directory Domain for 16 Windows 7 clients and 7 servers, receiving the highest patched rating for servers amongst all Army special access networks.
* Utilized SCAP vulnerability scanner to identify IAVM and DISA STIG vulnerabilities on Windows desktop and server OS requiring patching and hardening or remediation.

**Key Highlights**

* Conducted two digital forensic examinations of nine hard drives involving high-level national security with oversight by the Secretary of the Army.
* Supervised an assigned staff of 1 IT professional, developed schedules to meet deadlines and performed complex IT tasks.
* Assisted in designing the revamp of the electrical and HVAC systems to meet the demands of a growing data processing facility.
* Ensured the user community understood and adhered to the necessary procedures to maintain security by providing relevant and timely training.

**Special Agent**

**Digital Forensic Examiner**

**United States Army Criminal Investigation Command, Fort Bliss, TX 08/2009-05/2015**

Led managed investigations and digital forensic investigations for the US Army Criminal Investigation Command. Oversaw security incidents through gap analysis, plan and tabletop exercises, runbook design, knowledge transfers, and compromise assessment. Provided executive-level briefings to the Adjutant General of the New Mexico National Guard, the New Mexico Governor's Staff, and the Public Integrity Division, U.S. Department of Justice. Investigated, coordinated, resolved, and reported on security incidents (including OT) as they were escalated and identified Forensically analyzed end-user systems and servers with indicators of compromise and pursued security incident response activities.

**Digital Forensic Examiner/ Investigation**

* Forensically analyzed end-user systems and servers with indicators of compromise and pursued security incident response activities.
* Performed DFIR Incident Response Plan maturity gap assessments, determining risk rate, and recommended mitigation actions.
* Supervised the investigation, which identified and recovered stolen government property, including recovering six stolen HMMWV and locating a stolen fire truck.
* Provided on-scene digital forensics while responding to crime scenes at Forward Operating Bases within Afghanistan, providing case agents with real-time investigative leads.
* Developed and presented digital evidence collection and preservation training for 60 Special Agents and numerous commanders and lawyers.
* Executed outside the wire digital forensic and crime scene support during off-base raids to recover stolen U.S. Government property.
* Managed 63 investigations recovering over **$490,000** in U.S Government funds, and arresting multiple
* Conducted three digital forensic examinations involving four items of digital media and 1.5 Terabytes of data.

**Key Highlights**

* Managed 88 fraud cases across New Mexico and West Texas for Task Force Raptor, which recovered over $400,000 in U.S. Government Funds.
* Conducted a joint Army and FBI investigation arresting over eight members of a local militia group targeting civilians throughout El Paso, senior Army leaders, and Special Agents with the Army and the FBI.
* Conducted approximately 30 **digital forensic** examinations involving over 136 items of digital media and 21.2 Terabytes of data resulting in several courts martial and over 20,000 images submitted to the National Center for Missing and Exploited Children (NCMEC).
* Developed and presented digital forensic training on the recognition and proper collection procedure of current and emerging digital evidence to over 60 Special Agents and drug suppression investigators.

**EDUCATION**

**Master of Science, Cyber Security**

Excelsior College, Albany, NY Upsilon Pi Epsilon Honor Society member (4.0/4.0)

**Bachelor of Science**, Russian Studies

Excelsior College, Albany, NY

**Associate of Arts, Russian Studies**

Defense Language Institute Foreign Language Center, Presidio of Monterey, CA

**HONORS & AWARDS**

**2020 Technical Innovation Award Jul 2019 Employee of the Month 2019/2020-**Lockheed Martin Space, Littleton, CO

**Army Achievement Medal,** Fort Hood CID Battalion-Fort Hood Assistant Special Agent-In-Charge, Army CID, Fort Bliss, TX

**2013 Excellence in Public Service Award for Military Service**-Federal Executive Association of El Paso, El Paso, TX

**SELECTED TRAINING**

**Cyber Incident Response and Analysis**

**Federal Law Enforcement Training Center, Glynco, GA**

**Fundamentals of Networking, Department of Defense Computer Investigations Training**

**Advanced Crime Scene Investigative Techniques**

**Crisis Negotiators Basic Course**

**Federal Bureau of Investigation**

**Intermediate Incident Command Systems (ICS 300)**

**Federal Emergency Management Agency**

**CID Special Agent Warrant Officer Basic Course**

**United States Army Military Police School**

**Windows Forensic Examinations – EnCase**

**Department of Defense Computer Investigations Training Academy**

**Computer Incident Responders Course**

**Department of Defense Computer Investigations Training Academy**

**Special Agent Laboratory Training Course**

**Evidence Management Certification Course**

**United States Army CID Special Agent Course**

**TECHNICAL SKILLS & KNOWLEDGE**

Threat Management, threat Intel and MITRE attack, SIEM (Security Incident Event Management), Data Acquisition, forensic & IR best practices and forensic imaging tools, Vulnerability scanning and management, Endpoint Protection/Malware Protection, Technical Information Security Controls, Network Forensics and Digital Forensics, Malware Analysis and Log Analysis, Evidence Handling / Chain of Custody, Scripting (Python, Powershell), UNIX/Linux and Regular Expressions, VPN Communication Protocols