Aman Thanvi

https://amanthanvi.com

Email : contact@amanthanvi.com
Mobile : +1-301-538-7453

Executive Summary

Cybersecurity Specialist with active U.S. Secret clearance and a Master of Engineering in Cybersecurity. Over six years of progressive cybersecurity experience within federal agencies, federally funded research and development centers, and the private sector.

- Proven expertise in offensive and defensive security: vulnerability assessments, penetration testing, incident response, SIEM, DFIR, cryptographic protocol design, and industrial control systems security.
- Technical breadth across cloud (AWS, Azure, GCP), DevOps, secure SDLC, and compliance with NIST 800-53/800-171, complemented by enterprise-level security engineering and automation.
- Recognized leader: CyberCorps SFS recipient, Phi Kappa Phi member; strong collaborator with stakeholders, teams, and decision-makers. Fluent in English and Spanish, beginner proficiency in Hindi.
- Published author: "SocialCipher: A Multimodal Framework for Proactive Threat Detection with SentIntel" (IEEE CAI 2025), with hands-on experience in AI/ML threat intelligence, TTS evasion techniques, and advanced binary analysis.
- Seeking a strategic cybersecurity leadership role in areas including, but not limited to, offensive & defensive security, DevSecOps, and security engineering. Prepared to design and implement resilient security architectures, elevate enterprise threat intelligence and detection, and drive mission-critical security outcomes.

Experience

- **Department of Justice - U.S. Trustee Program** — Washington, D.C.
  Information Technology Cybersecurity Specialist (GS-07) — *Nov. 2024 – Present*
  - Providing technical support and cybersecurity oversight across DOJ's mission-critical systems within the Executive Office for U.S. Trustees (EOUST), ensuring system availability, data integrity & confidentiality, and risk mitigation.
  - Implementing and refining enterprise-level security protocols, incident response procedures, and data loss prevention strategies, aligning operations with NIST frameworks and DOJ policy standards.
  - Leading integration and quality assurance efforts for new system deployments, including application development environments, cloud infrastructure, and version control systems.
  - Conducting vulnerability and threat assessments and coordinating with stakeholders to remediate findings and ensure continuous security posture improvement across platforms.
  - Supporting DOJ cybersecurity initiatives through documentation, training, and advisory functions, ensuring alignment with DOJ's IT governance and strategic goals.
- **MIT Lincoln Laboratory** — Lexington, MA
  Summer Research Program Intern — *Jun. 2024 – Aug. 2024*
  - Designed and implemented software and hardware tools and methodologies to evaluate the cybersecurity resiliency of control systems and the related hardware devices that interface with infrastructure components.
  - Identified gaps in standardization across various program workflows, leading to the architecture and development of a comprehensive platform to centralize and optimize program operations, reducing inefficiencies and operational sprawl.
  - Developed new protocol parsers for Industrial Control Systems (ICS) and proprietary network protocols, improving the ability to monitor and secure critical infrastructure.
- **Kurtek** — College Park, MD
  Cybersecurity Research Intern — *Sep. 2023 – Dec. 2023*
  - Analyzed cybersecurity risks for NASA's Next Generation Network (NGN), focusing on integrating commercial cloud platforms and non-government entities, and developed strategies to mitigate identified threats.
  - Reviewed NASA's cybersecurity methods and adapted them to meet the unique challenges of the NGN architecture, ensuring compliance with federal cybersecurity frameworks such as NIST 800-53 and NIST 800-171.
  - Investigated mission-specific security challenges in space communications, applying insights from CCSDS reports to develop tailored cybersecurity solutions for the NGN, emphasizing operational availability during potential infrastructure degradation while ensuring compliance with NIST-based federal cybersecurity frameworks.
- **Cybersecurity and Infrastructure Security Agency (CISA)** — Arlington, VA
  Cybersecurity Intern — *May 2023 – Aug. 2023*
  - Collaborated with the Infrastructure team to execute critical service updates, leveraging cybersecurity best practices, ensuring seamless operations, and strict policy adherence.
  - Researched and integrated diverse and novel technologies to make existing infrastructure more modern, agile, and functional while maintaining reliability.
  - Leveraged Teleport, ThreatConnect, and Red Hat OpenShift to fortify essential infrastructure security, enabling persistent operational continuity.

- **Kurtek (contracted to NASA)** Greenbelt, MD
  Senior Cyber Security Intern *Feb. 2023 – May 2023*
  - Spearheaded development and implementation of security protocols for NASA's communications and navigation (SCaN) cloud infrastructure, ensuring alignment with federal cybersecurity policies and standards.
  - Developed security artifacts, user manuals, and capability brochures to enhance SCaN Cloud's readiness for independent assessments.
- **Nasdaq** Rockville, MD
  Information Security Intern *Feb. 2023 – May 2023*
  - Conducted comprehensive security assessments of internal applications using DAST and SAST tools, including OWASP ZAP, Burp Suite, Checkmarx, and Acunetix, leveraging MITRE ATT&CK to identify and report vulnerabilities of varying criticality.
  - Led offensive security assessments and penetration tests on communication platforms, integrating MITRE ATT&CK techniques and collaborating with IT and other departments to enhance access controls and ensure compliance with federal policies.
  - Utilized advanced tools like Splunk and ZScaler during red team exercises to identify and mitigate critical vulnerabilities, significantly enhancing Nasdaq's security posture across B2B and B2C channels.
- **National Aeronautics and Space Administration (NASA)** Greenbelt, MD
  Cryptography Intern *Jun. 2021 – Aug. 2021*
  - Implemented the CCSDS Space Data Link Security Protocol – Extended Procedures (SDLS-EP) to secure communications between the spacecraft's core Flight System (cFS) and ground station, utilizing the NASA Operational Simulator for Small Satellites (NOS3).
  - Analyzed cryptographic mechanisms and mission requirements, ultimately facilitating the incorporation of a proprietary cryptographic protocol.

  Security Intern *Jun. 2020 – Aug. 2020*
  - Enhanced existing security compliance tool capabilities through rigorous testing and analysis, leading to a more efficient compliance metrics reporting process.
  - Utilized multiple security frameworks to identify vulnerabilities within NCCS infrastructures and recommended enhancements.
- **Embedded Flight Systems Inc. (Contracted to NASA)** Greenbelt, MD
  Networking/System Administration Intern *Jun. 2019 – Aug. 2019*
  - Gained hands-on experience with various advanced computer hardware and operating systems used in NASA infrastructure and acquired experience managing and configuring advanced network devices.
  - Established and deployed a secure and service-rich private network infrastructure.

Education

- **University of Maryland, College Park** College Park, MD
  Master of Engineering in Cybersecurity; GPA: 4.00 *Aug. 2024 – May. 2025*
- **University of Maryland, College Park** College Park, MD
  Bachelor of Science in Computer Science; GPA: 3.3 *Aug. 2020 – May 2024*
  - **Minors**: Cybersecurity (Advanced Cybersecurity Experience for Students [ACES]), Science, Technology, Ethics, & Policy [STEP]
  - **Global Fellows Program**: International Security and Intelligence concentration

Skills

- **Cybersecurity**: Red & Blue Team, Vulnerability Assessment, Penetration Testing, Threat Intelligence, Network Security, MITRE ATT&CK, DFIR, SDLC Security, Cryptography, Reverse Engineering, Binary Analysis
- **Cloud & DevOps**: AWS, Azure, GCP, Docker, GitHub Actions, ZScaler, Teleport, Terraform, Agile, CI/CD, BitBucket, Bamboo, Jira, Confluence
- **Networking & Systems**: TCP/IP, Firewalls, Linux, Unix, pfSense, Shell Scripting, SIEM (Splunk), OSINT
- **Application Security**: SAST, DAST, Burp Suite, OWASP ZAP, Checkmarx, Acunetix, Secure Code Review, Static Analysis, Input Sanitization, SSRF/XSS/CSRF/SQLi, Snyk, Sonatype IQ, Sonarqube
- **Programming & Tools**: Python, C/C++, Bash, Java, HTML/CSS, JavaScript, Rust, Go, Git, VS Code, Wireshark, Ghidra, Binary Ninja, GDB, pwndbg
- **Data & AI/ML**: TensorFlow, XML/JSON, YAML, Elasticsearch, MongoDB, Pandas, scikit-learn, TTS/ML evasion research (Geneva)
- **Soft Skills**: Public Speaking, Technical Writing, Documentation, Cross-Team Collaboration, Training & Mentorship, Project Leadership
- **Languages**: English (native), Spanish (fluent), Hindi (beginner)

Honors, Awards, & Certifications

- **Secret Clearance** *Jun. 2024*
- **Phi Kappa Phi Honor Society** University of Maryland, College Park *Jan. 2025*
- **Alpha Lambda Delta Honor Society** University of Maryland, College Park *Nov. 2021*
- **Dean's List** University of Maryland, College Park *2021, 2022*
- **CyberCorps Scholarship for Service (SFS)** University of Maryland, College Park *Fall 2022*
- **CompTIA A+** *Dec. 2018*
- **Microsoft Certified: Azure Fundamentals** *Jul. 2022*
- **Microsoft Certified: Security, Compliance, and Identity Fundamentals** *Jul. 2022*

Publications & Research

- **SocialCipher: A Multimodal Framework for Proactive Threat Detection with SentIn-tel** Lexington, MA & Santa Clara,
  MIT Lincoln Laboratory & IEEE CAI 2025 *Jun. 2024 – May 2025*
  - Co-authored and presented a paper on proactive cyber threat detection using sentiment analysis and LLMs.
- **Geneva - Protocol Obfuscation** College Park, MD
  Breakerspace at the University of Maryland, College Park *Aug. 2023 – Present*
  - Researching utilizing Text-to-Speech (TTS) quirks for practical applications in circumventing censorship detection mechanisms.
  - Establishing a reliable baseline for detectability, focusing on optimizing the balance between detectability and data throughput.
- **Cyber Threat Intelligence Research** College Park, MD
  NSA in collaboration with the University of Maryland, College Park *Aug. 2023 – Dec. 2023*
  - Spearheaded in-depth threat intelligence project on Advanced Persistent Threats (APTs) 40 and 41 in collaboration with the NSA, utilizing industry-leading tools and best practices to identify potential security risks and devise robust defense strategies.
  - Developed comprehensive threat profiles for APTs 40 and 41, employing advanced analytical techniques to correlate data across multiple sources, providing a deeper understanding of cyber threat behaviors and tactics.
  - Crafted and delivered high-impact briefing and a thorough threat profile report to NSA leadership, significantly enhancing agency preparedness and response capabilities against sophisticated cyber threats through actionable intelligence and strategic insights.
- **Malware Detection & Classification** College Park, MD
  FIRE Program - AI & Deep Learning: Capital One ML stream *Aug. 2023 – Dec. 2023*

Leadership & Membership

- **Cybersecurity Club** University of Maryland, College Park
  Secretary *Jun. 2023 – May 2025*
- **Hindu Student Council** University of Maryland, College Park
  Events Co-Chair *Jan. 2023 – Aug. 2023*
- **Tech Fellow** College Park, MD
  CodePath *Jun. 2021 – Dec. 2021*
  - Facilitated hands-on learning experiences of cybersecurity concepts for the Fall 2021 semester at the University of Maryland, College Park.
  - Organized and presented learning materials effectively while maintaining regular communication with admins and supervisors regarding class progress, challenges, and student achievements.
- **University Senate** University of Maryland, College Park
  Undergraduate Senator, College of Letters & Science (LTSC) *Mar. 2021 – Jan. 2022*
- **Cybersecurity Club** University of Maryland, College Park
  Member *Sep. 2020 – Jun. 2023*