

Justin Dubin

Johnson City, TN

423-676-3529 | justin.n.dubin@pm.me | [linkedin.com/in/jdubin1417](https://www.linkedin.com/in/jdubin1417) | github.com/Jdubin1417 | justindubin.live

PROFESSIONAL SUMMARY

Information security analyst with skills in vulnerability management, coding, and IT architecture interested in a team-based, fast-paced security analyst role implementing security measures and controls. Available for full-time internship Winter 2024 and Summer 2025.

EDUCATION & TRAINING

- BS Computing | Minor Military Science | 3.8 GPA | Expected December 2025

CERTIFICATIONS

- CompTIA Security+ | Expires: 29 December 2026
- Google Cybersecurity Certification
- Cisco Junior Cybersecurity Analyst Career Path
- CEH Ethical Hacking Course Completion

INTERNSHIPS

U.S. ARMY CYBER COMMAND, FORT EISENHOWER, GA
INTERN; ROTC CADET

08/2024

- Contributed to a wide range of cyber activities with a high level of adaptability, and a solution-oriented mindset.
- Delivered a final capstone essay on the topic of Artificial Intelligence, and Quantum Computing and how they are relevant in Cyber Warfare today and in the future.
- Attended TechNet Augusta, gaining insights into emerging technologies and cybersecurity strategies relevant to military and government sectors.

ALPHA METALLURGICAL RESOURCES, BRISTOL, TN
INFORMATION SECURITY INTERN

05/2023 – 06/2024

(INTERMITTENT WITH SCHOOL SCHEDULE)

- Assisted in conducting phishing simulations, analyzing results to reduce employee click rates and enhance company-wide security awareness.
- Developed and standardized Standard Operating Procedures (SOPs), creating a framework to streamline team security processes and improve onboarding for new team members.
- Assisted in identifying and addressing security risks across multiple sites, ensuring effective remediation to enhance the company's overall security posture.
- Analyzed and mitigated threats on infected computers, utilizing sandbox environments to safely examine malware behavior and assess potential risks.

COMPETITIONS

DEPARTMENT OF ENERGY CYBERFORCE COMPETITION
CYBERBUCS - TEAM CAPTAIN

11/2024

- Coordinated practices and assignments for our team of six, focusing on hardening Windows and Linux environments throughout the competition to enhance defense against cyberattacks.
- Implemented security best practices, including system configuration, patch management, and access control measures, to secure critical infrastructure components in both Windows and Linux systems.
- Led efforts in continuous monitoring, establishing protocols for detecting and responding to breaches, ensuring rapid containment and mitigation of any attempted intrusions.
- Resolved anomalies in areas like forensics, phishing classification, and reverse engineering, applying these insights to fortify our defensive posture.
- Promoted strong collaboration and adaptability within the team, enabling cohesive and effective responses to evolving threats in a high-stakes, real-world simulation of critical infrastructure defense.

COLLIAGIATE PENETRATION TESTING COMPETITION

11/2024

CYBERBUCS - TEAM CAPTAIN

- Coordinated practices and assignments for a team of six, guiding our approach with the MITRE ATT&CK framework to systematically execute and document attack vectors in the simulated enterprise environment.
- Directed team efforts in identifying, exploiting, and documenting vulnerabilities across various systems, aligning findings with industry standards to create actionable security insights.
- Organized responses to competition injects, including technical reports, risk assessments, and presentations, ensuring our team delivered timely and accurate information to meet scenario requirements.
- Utilized CVSS scoring in reporting to prioritize vulnerabilities, providing a structured risk assessment and recommending effective remediation strategies.
- Fostered collaboration and communication within the team, enabling cohesive, well-coordinated actions that maximized effectiveness and adaptability in a high-stakes environment.

HIVESTORM

10/2024

CYBERBUCS - TEAM CAPTAIN

- Led a team of four, coordinating strategy, assigning roles, and managing communications under strict time constraints to optimize task efficiency.
- Focused on securing an Advanced Windows Server (Domain Controller) along with other Windows Servers by troubleshooting services, mitigating vulnerabilities, and maintaining up time for critical systems.
- Conducted password updates, audited administrative privileges, and applied essential group policy configurations to strengthen security and ensure compliance.
- Achieved 30th place out of 413 teams, ranking within the top 7% for exceptional performance and system resilience.

TECHNET CAPTURE THE FLAG

08/2024

- Competed in CTF solving challenges across digital forensics, reverse engineering, cryptography, and network security to simulate real-world cybersecurity threats.
- Focused efforts on Reverse Engineering, Network Traffic Analysis, and Exploitation, applying advanced analytical skills to uncover vulnerabilities and solve complex tasks.
- Collaborated effectively with team members, developing and executing strategies under time pressure to maximize scoring potential in each challenge area.

NATIONAL CYBER LEAGUE TEAM COMPETITION

03/2024

CYBERBUCS

- Competed in a Capture-The-Flag competition encompassing digital forensics, web application exploitation, cryptography, and network analysis, demonstrating advanced problem-solving abilities.
- Focused on Open-Source Intelligence, Network Traffic Analysis, and Enumeration/Exploitation, leveraging specialized skills to address complex challenges across diverse cybersecurity fields.
- Achieved 323rd place out of 4,199 teams (top 7%), earning 1st place nationwide in Open-Source Intelligence and placing in the 96th and 97th percentiles in Enumeration/Exploitation and Network Traffic Analysis, respectively.

SOUTHEAST COLLEGIATE CYBER DEFENSE COMPETITION

03/2024

CYBERBUCS

- Played a key role in defending a mixed-environment network with six machines (three Windows and three Linux), ensuring the security and stability of critical systems under active attack.
- Deployed and configured the open-source SIEM, Wazuh, to monitor system logs, detect anomalies, and provide real-time threat visibility across the network.
- Implemented security measures across both Windows and Linux systems, focusing on vulnerability mitigation, system hardening, and continuous monitoring to prevent unauthorized access.
- Collaborated with team members to develop and adapt defense strategies, ensuring efficient coordination and response to evolving threats throughout the competition.
- Contributed to maintaining service uptime and safeguarding data integrity, showcasing a proactive and resilient approach to cybersecurity defense in a high-pressure setting.

PERSONAL PROJECTS

HONEYPOT AND DIGITAL RESUME

- Developed a secure SSH honeypot to capture and log brute force attempts, providing real-time data on unauthorized access attempts for further analysis.
- Analyzed honeypot data to gain insights into attack patterns, login behaviors, and common threat actor techniques, contributing to a deeper understanding of cyber threats.
- Integrated live honeypot data into a professional digital resume and portfolio website, showcasing technical skills in real-time data presentation.
- Enhanced the website's design to highlight personal projects and achievements, creating an engaging platform for potential collaborators and employers.
- Planned version 2 update with the following updates:
 - Plan to implement enhanced data handling for faster load times, improving user experience and responsiveness of live data displays.
 - Plan to integrate a threat map with shaded regions indicating areas of frequent unauthorized login attempts, with darker shades representing higher concentrations of attack origins.
 - Plan to introduce a fake terminal to observe attackers' tactics, techniques, and procedures (TTPs) post-login, logging actions for insight into real-world threat behaviors.

SIEM IMPLEMENTATION PROJECT

- Built a dedicated lab environment emulating an Active Directory setup, allowing for the testing and simulation of real-world penetration testing techniques.
- Deployed Wazuh as an open-source SIEM within the lab to monitor security events, detect anomalies, and log pentesting activities for comprehensive analysis.
- Configured Active Directory with common misconfigurations to simulate vulnerabilities, creating a controlled setting to test enumeration, privilege escalation, and lateral movement techniques.

WORK HISTORY

ETSU, JOHNSON CITY, TN

11/2024 - PRESENT

IT SERVICE HELP DESK TECHNICIAN

- Provide technical support and troubleshoot hardware, software, and network issues for students, faculty, and staff.
- Assist with account management, including password resets and access troubleshooting.
- Ensure timely and effective resolution of IT-related inquiries via phone, email, and in-person support.
- Document and escalate complex issues to specialized teams when needed.
- Guide users in following best practices for cybersecurity and data privacy.
- Maintain a high level of customer service, enhancing user experience and satisfaction.

ETSU, JOHNSON CITY, TN

08/2024 - 11/2024

SHERROD LIBRARY LAB IT ASSISTANT

- Supported library patrons with computer and printer usage, software installations, and troubleshooting basic technical issues.
- Provided guidance on navigating library resources, online databases, and educational software.
- Maintained computer lab equipment, ensuring systems were operational and up to date.
- Assisted with logging and reporting technical incidents for prompt resolution.
- Educated users on digital literacy and responsible use of technology in a library setting.
- Fostered a positive and supportive environment to enhance user experience and accessibility to library resources.

BEST BUY, JOHNSON CITY, TN

10/2020 - 08/2023

SALES ASSOCIATE

- Engaged with customers to understand their unique needs, recommending tailored solutions across electronics, including PCs, mobile devices, home entertainment systems, and smart home security products.
- Guided customers through choosing and configuring PCs and accessories, ensuring optimal performance for gaming, productivity, or creative work.
- Delivered personalized assistance with product setup, compatibility advice, and troubleshooting, enhancing customer satisfaction and confidence in their purchases.

- Leveraged knowledge across all departments to provide comprehensive solutions that addressed both tech-focused and general household needs.
- Maintained a well-organized and inviting electronics section, collaborating with team members to meet seasonal demand and create a positive shopping experience.
- Achieved a 100% Customer Satisfaction Survey score at Best Buy, showcasing a dedication to delivering outstanding customer experiences and personalized product solutions.

INFOCISION, JOHNSON CITY, TN
SALES ASSOCIATE

07/2020 – 12/2020

- Engaged with a diverse range of customers, adapting communication style to meet varied needs and preferences across different client campaigns.
- Skillfully managed calls to balance meeting sales goals with providing personalized, empathetic customer service.
- Effectively navigated conversations to identify customer needs, tailoring solutions and product offerings to each unique interaction.
- Achieved productivity targets by completing calls efficiently while maintaining high-quality customer experience.
- Maintained 100% Customer Relations survey score, demonstrating exceptional customer service skills and a strong commitment to meeting client needs effectively.
- Developed strong interpersonal skills by interacting with customers from diverse backgrounds, enhancing adaptability and communication effectiveness.