Brandon Harris
brandonharrishidden@themail.edu | ***-***-**** | Stafford, VA | Blog: https://brandonerrorhidden.medium.com

Experience

Cybersecurity Intern |Leidos – Joint Base Andrews, MD | 05/2025 – present

- Conducted threat hunt operations using threat intelligence and indicators of compromise (IOCs) by crafting SQL and REGEX queries within the Air Force's Big Data Platform, ELICSAR.
- Reviewed closed and open-source intelligence to track adversary tactics, techniques, and procedures (TTPs)
- Monitor and analyze Microsoft Defender for endpoint alerts, Sysmon, and host logs, for suspicious activity and to rule out false positives.
- Supported cybersecurity efforts to protect over 30,000 end users in the Air Force District of Washington (AFDW)

Cybersecurity Engineer Intern (Co-Op) |Leidos – Bethesda, MD | 06/2024 – 12/12/2024

- Analyzed logs to detect and respond to security events and coordinated with cross-functional teams to resolve incidents and restore normal operations
- Ingested Logs into a Security Information Event Management System (SIEM) and created custom dashboards and alerts to reduce the time to detect and respond to security events
- Utilized Vulnerability scans to identify, patch, and mitigate security risk to Windows and Linux based systems
- Provided system analysis and engineering support for classified customers in the Department of Defense (DoD)

Amazon Warehouse Associate |Amazon Inc. – Fredericksburg, VA| 05/2023 – 07/2023

- Effectively troubleshot issues related to inventory discrepancies for a supply chain of over 70,000 packages daily.
- Implemented innovative technologies such as automated tracking systems to enhance warehouse operations.
- Utilized sophisticated inventory management systems to optimize the movement of products.

Certifications & Clearance

Splunk Certified Core User
CompTIA Security+
CompTIA CySA+
AZ-900 Microsoft Azure Fundamentals
Microsoft Office Specialist Excel (Office 2016)

Education

Old Dominion University | Norfolk, VA | Expected in 12/2025

Bachelor of Science in Cybersecurity

- ODU Collegiate Cyber Defense Competition (ccdc) Team Cybersecurity Club Member, 2022 to Present

Relevant course Work:

- **Basic Cybersecurity Programming and Networking** – Learned about network design, network security and network protocols and how to automate network security.
- **Cybersecurity Techniques and Operations** – Learned about vulnerabilities, Network Defense and attack information assurance, data security and data loss prevention, rule and role based access control.

Projects & Self Learning

Attack and defend lab

- Executed attacks by exploiting common vulnerabilities (e.g., misconfigured services, weak credentials) to gain unauthorized access and simulate real-world adversary tactics.
- Conducted defense by analyzing system logs and network traffic to detect, respond to, and mitigate active threats and intrusions.
- Monitored and interpreted SIEM alerts to investigate anomalies and respond to potential breaches during red team activity.
- implemented layered defense strategies including network segmentation, host hardening, and access control policies.

TryHackMe

- Did CTFs create a better understanding of computer network defense and computer network attack

Skills

Programing Languages: Python
Tools: Elk Stack, Nessus, Active Directory, Nmap, Snort, Volatility, ELICSAR
Operating systems: Windows, Ubuntu, Linux, Red Hat
Other: System Hardening, Active Directory, Analysis, System Administration, Vulnerability Remediation, Microsoft Excel, Customer Service, Problem Solving, Cyber defense, Attention to Detail, Team Oriented, Teamwork, Leadership, IT support, Software Impact Assessment, Networking, programming