Caleb Judy

Chesapeake, VA | 757-390-7105 | calebrjudy21@gmail.com

EDUCATION

Old Dominion University **Norfolk, VA**
Bachelor of Science in Cybersecurity Current GPA: 3.67
Expected Graduation: May 2026

ACTIVE CERTIFICATIONS

CompTIA Security+ SY0-701 **COMP001022865778**

WORK EXPERIENCE

City of Virginia Beach **Virginia Beach, VA**
Cybersecurity Analyst Intern August 2025 – December 2025

- Administered Microsoft Azure Directory B2C platform, reducing identity-based vulnerabilities by 10-15% weekly through vigilant threat analysts and risk assessment.
- Triaged and analyzed security incidents with the security operations team to update indicators of compromise, perform system monitoring, and further protect the environment from MITRE ATT&CK tactics.
- Created detailed reports and implemented rapid remediation strategies with Microsoft Defender for Endpoint, resulting in a 5-10% reduction in advanced threat vulnerabilities.
- Conducted thorough evaluations of software applications for using Open-Source Intelligence to identify and address security and privacy risks, ensuring new solutions to maintain compliance with security standards.
- Analyzed phishing email submissions for potential threats, utilizing SIEM (System Information and Event Management) data for event and system monitoring to research trends in cyber incidents and conduct strategic threat-hunting.
- Assessed APM (Application Portfolio Management) software evaluations, communicating with APM, the vendors and cybersecurity team to review potential software/applications for use in the organization.
- Wrote rough draft, reviewed, and revised the organization's Autopsy digital forensics SOP (Standard Operating Procedure) to develop clear and concise instructions aimed at explaining how to use the Autopsy digital forensics platform and defining proper, appropriate use of the platform.
- Utilized Cortex XSIAM (eXtended Security Intelligence and Automation Management), which is an AI-driven security platform that centralizes EDR (Endpoint Detection Response), XDR (Extended detection response), SOAR (System Orchestration, Automation, and Response), SIEM and automation solutions. Participated in configuring and troubleshooting the platform and made recommendations on how to tailor the platform to the organization's needs.

COURSEWORK

Cybersecurity Techniques and Operations

- Traced network traffic with tools like Wireshark
- Configured pfSense firewalls
- Performed penetration testing using the Metasploit framework
- Cracked passwords using dictionary attacks

Linux System for Cybersecurity

- Managed group and user accounts
- Managed file permissions and local storage
- Utilized automation, shell scripting

Cybercrime

- Summarized findings from academic research about cyber trespassing
- Conducted a case study of cybercrime by summarizing information from law enforcement affidavits and constructing a timeline of the cybercrime
- Identified impacts of cybercrimes using data from government agencies
- Classified instances of cybercrime into one of four categories (cybertresspassing, cyberfraud, cyberviolence, cyberpornography)

Cybersecurity Ethics

- Analyzed ethical problems related to cybersecurity
- Applied principles learned from ethical theories to cybersecurity cases
- Analyzed ethical issues and made decisions based on ethical dilemmas to solve them

Generative AI in Cybersecurity

- Focused on dual nature of AI systems as both enhancers and potential threats to security infrastructure
- Gained comprehensive understanding of principles, algorithms, and applications of generative AI models in the discovery of attack vectors, identification of cyber threats, and automation of security tasks
- Learned about defensive strategies in order to mitigate risks stemming from AI-driven cyberattacks
- Utilized chain-of-thought prompting to analyze exploitable python code, and devised a plan to address the vulnerabilities posed by the python code

SKILLS

Skills

- Linux
- Penetration testing
- Network scanning
- Network traffic analysis
- Configuration of firewalls
- Cortex XSIAM
- Windows Azure
- Windows Defender
- ServiceNow
- SolarWinds
- Chain-of-thought prompting