PAUL D. CUMISKEY

ASPIRING SOC ANALYST

Norfolk, VA

(434) 960-9691

pcumiskey77@gmail.com

KEY SKILLS

- SIEM (Splunk)
- Log Analysis
- Threat Detection
- Incident Response
- Penetration Testing
- System Hardening
- System Administration
- Networking Fundamentals
- Scripting (BASH, PowerShell, Python, SQL)
- Documentation

EDUCATION

B.S. CYBER SECURITY
Old Dominion University – 2026 expected

CERTIFICATIONS

SPLUNK CORE CERTIFIED USER
Splunk – 2026 expected

BLUE TEAM LEVEL 1
Security Blue Team – 2026 Expected

CYSA+
COMPTIA - 2026

SECURITY+
Comptia - 2026

PROFESSIONAL PROFILE

Motivated and professional cybersecurity learner with hands-on experience in Security Information and Event Management (SIEM), log analysis, threat detection basics, and security awareness practices. Graduating from Old Dominion University in May 2026 with a degree in CyberSecurity. Comptia Security+ and CySA+ certified. Pursuing Blue Team Level 1 and Splunk Core Certified User certifications.

CYBERSECURITY EXPERIENCE

Cybersecurity Intern
Old Dominion University **January 2026 - Present**

Employed to, with a team, conduct risk assessments, vulnerability evaluations and threat analysis for public and private sector clients contracted through the ODU School of CyberSecurity. Specifically, we identify, for our clients, any gaps we find with their overall information security posture and provide actionable cybersecurity recommendations to minimize risk exposure. Specific responsibilities include:

- Asset identification and classification
- Analysis of security controls and business practices
- Delivery of actionable CyberSecurity recommendations

Security Operations Labs & Projects
Home Labs **August 2024 - Present**

Built multi-system home labs using both VMWare and VirtualBox hypervisors. Each lab consisted of virtual machines designed to mimic production environments. Accomplishments:

- Designed and deployed virtual environments mimicking production environments with Windows workstations and a combination of file, web, email and database servers running Windows and Linux OSes.
- Deployed and configured Splunk to ingest and analyze authentication, system and network logs of the deployed virtual machines. Built multiple Splunk detections for brute-force and anomalous authentication behavior.
- Using Kali Linux conducted extensive penetration testing against deployed virtual hosts.
- Investigated Indicators of Attack (IoA) and Indicators of Compromise (IoC) using log correlation and time-based analysis.
- Identified and remediated vulnerabilities within the environment.
- Documented findings following incident response best practices.

Work History

SUB SHOP EMPLOYEE / LINE COOK / DISHWASHER
Wegman's / Tavern on the James **2020 - 2026**

Six (6) years of experience working a combination of part-time and full-time hours with two (2) different employers while completing a B.S in CyberSecurity and multiple InfoSec certifications. Top performer with each employer.

AWARDS

- Dean's List ODU
- Employee of the Month Wegman's
- Etc.