Jayden Williams

jwilliams.cyber@gmail.com | linkedin.com/in/jaydenwilliamscyber | github.com/jaydenwilliams-cyber | medium.com/@jwilliams.cyber

COMPETENCIES & SKILLS

Technical Skills: SIEM Analysis, Vulnerability Management, Threat Hunting, Network Traffic Analysis, Incident Response

Tools: Splunk, Sysmon, Wireshark, Tenable Nessus, T-Pot, Kibana, Elasticsearch, Suricata, Kali Linux, PEStudio, Process Monitor

Hardware / OS: Windows 10/11, Linux (Ubuntu, Kali), AWS EC2, Azure VMs, VirtualBox

Programming: Python, SQL, PowerShell, Bash, C++ (in progress)

Frameworks: MITRE ATT&CK, NIST CSF, CVSS, OWASP Top 10

Professional Skills: Technical Writing, Lab Documentation, Independent Research

EDUCATION & CERTIFICATIONS

University of South Florida Expected 2028

Bachelor of Science in Cybersecurity

Hillsborough Community College Aug. 2024 – Dec. 2026

Associate of Arts in Cybersecurity Pathway | GPA: 3.60 / 4.00 | Dean's List

Certifications

- CompTIA Cybersecurity Analyst+ (CySA+, CS0-003) — Earned April 2026
- CompTIA Security+ (SY0-701) — Earned March 2026

Awards & Recognition

- Microsoft Cybersecurity Talent Fund | Last Mile Education Fund — Spring 2026

EXPERIENCE

Guest Arrival Ambassador | Busch Gardens Tampa Bay May 2024 – Present

- Troubleshoot ticketing and access systems to restore service and maintain uptime in a high-traffic environment serving hundreds of daily guests, resolving access issues and escalating system failures to the appropriate team.
- Coordinated manual check-in procedures during a facility-wide power outage affecting ticketing infrastructure, maintaining guest flow until full system restoration.

Cybersecurity Club Member | HCC Cyberhawks — Hillsborough Community College Aug. 2024 – Present

- Practiced National Cyber League (NCL) CTF challenges covering cryptography, log analysis, open-source intelligence, and network forensics; attended BSides Tampa to network with security practitioners and learn from industry talks.

PROJECTS

Cowboy Bebop Threat Hunting Lab | Splunk, Sysmon, Kali Linux, Windows, MITRE ATT&CK May 2026 – Present

- Built a three-VM threat detection lab simulating four MITRE ATT&CK techniques across Initial Access, Persistence, Credential Access, and Lateral Movement; detected each attack using Splunk and Sysmon with documented SPL queries. Full writeup: medium.com/@jwilliams.cyber.

24-Hour AWS Honeypot Lab | T-Pot, AWS EC2, Kibana, Elasticsearch, Suricata Apr. 2026

- Deployed T-Pot 24.04.1 on AWS EC2, captured 63 attacks from 5 unique source IPs in 24 hours, detecting NMAP reconnaissance and SSH brute force attempts and mapping attacker TTPs to 5 MITRE ATT&CK techniques using Kibana and Suricata.

Azure VM Vulnerability Management | Azure, Nessus, PowerShell, GitHub Actions Mar. 2026

- Deployed a Windows VM in Azure, ran Tenable Nessus scans to identify vulnerabilities, remediated using PowerShell (PSWindowsUpdate), and built a GitHub Actions CI/CD pipeline to automate patch execution in a repeatable scan-patch-validate workflow.

Wireshark Traffic Analysis Automation | Wireshark, Python, Pandas Mar. 2026

- Captured and analyzed 24,834 packets using Wireshark, automating identification of top talker IPs, protocol distribution across TCP, UDP, QUIC, and TLSv1.3, and active port activity from raw CSV export using a Python/Pandas script.

Sysmon Detection Lab | Sysmon, PowerShell, Windows, MITRE ATT&CK Feb. 2026

- Configured Sysmon on Windows 10 VM with custom XML ruleset, capturing 7+ command executions via Event ID 1 and simulating LOLBAS techniques using encoded PowerShell.