Devin Young

devinl.young1@gmail.com | 301-804-8207 | Temple Hills, Maryland 20748 | Devin Young - LinkedIn

EMPLOYMENT HISTORY

Managed Funds Association, IT Support Intern   **Jan. 2025 - Present**
- Diagnosed and resolved hardware and software issues, including printers, desktops, and servers, ensuring operational continuity
- Provided technical support to staff, **troubleshooting** connectivity and application challenges to maintain productivity
- Executed and managed Windows **software updates** across user workstations in alignment with directives from the **VP of Information Technology**
- Facilitated the deployment and configuration of new hardware, mobile devices, and enterprise applications
- Oversaw software licensing, warranty management, and **asset inventory** to maintain compliance and optimize resource utilization

Federated Hermes, Information Security Analyst Intern   **May. 2024 - Aug. 2024**
- Investigated 320+ **phish** alert submissions on Microsoft Outlook to determine if emails that employees received were spam or targeted phish by using tools such as **CrowdStrike Falcon**, **Mimecast**, **Microsoft Defender**, VirusTotal, Email Hippo, etc.
- Created tickets within **Cherwell** for those phish alert submissions and documented the findings of each investigation
- Communicated with **end-users** to help determine the legitimacy of certain phish alert submissions
- Pitched a fully functional Outlook widget that gave employees the likelihood of emails they receive being phish or spam (internal group hackathon)
- Participated in server and endpoint meetings regarding the company's **vulnerability management** of software (with **Qualys** as the analysis platform)
- Customized the **benchmark scans** for "Federated Hermes Investments" to ensure that the hardware was configured for best practices (accessing **policies** within the security configuration assessment module of Qualys)
- **Shadowed** the desktop support, application support, identity and access management, cloud security, and domain architecture team
- Worked with a geographically distributed team (UK and US)

Booz Allen Hamilton (NASA CyPrESS Contract), Cybersecurity Co-Op   **Jan. 2024 - May. 2024**
- Supported senior cybersecurity professionals on the "Cyber **Incident Response** Team" in investigating **anomalous** activity and reporting findings to client leadership in a timely fashion.
- Shadowed **Digital Forensics** and Incident Response analysts in forensic analysis and detailed network investigations (tools that were used include **SentinelOne**, CrowdStrike Falcon, **Splunk**, etc.)
- Assisted in the development of **standard operating procedures** for an asset compromise within NASA's cybersecurity infrastructure
- Designed a visual workflow within PowerPoint that summarized the standard operating procedures for an asset compromise within NASA's cybersecurity infrastructure
- Participated in **tabletop exercises** lead by senior cybersecurity professionals to sharpen the team's incident response strategies

MITRE, Cyber Futures Intern (MITRE ATT&CK Defense Team)   **Jun. 2023 - Aug. 2023**
- Conducted research on 20 adversarial **techniques** within the **MITRE ATT&CK Framework** that are used to breach the cloud and network security of organizations, while also proposing a combined total of 48 new **detections** and **mitigations** to be listed under those techniques
- Gave full-time cybersecurity professionals on the "MITRE ATT&CK - Defense" team a unique approach that they could follow when suggesting their own detections and mitigations for adversarial techniques within the cloud and network realm
- Completed various capture-the-flag challenges through **picoCTF**
- Received 3 weeks of technical and professional training from cybersecurity experts at MITRE and **Prelude**

EDUCATION

Bowie State University, Department of Technology and Security   **Aug. 2022 - May. 2025**
- Bachelor of Science in Computer Technology **(**concentration in network enterprise infrastructure)
- Senior Classification - **3.9 Cumulative GPA** (baltimore gas and electric scholars program)

Prince George's Community College, Dual Enrollment (credits earned while enrolled high school)   **Jun. 2020 - May 2022**
- 18 Credits

SKILLS

- Computer Networking & Network Security (**TCP/IP**, OSI model, **NIST Framework**, CIA Triad, Zero Trust Architecture, etc.)
- Python, Java, & Powershell (programming/scripting languages)
- UNIX/**Linux** System Administration & **Windows** Server Administration (Active Directory, Hyper-V, etc.)
- **Operating System Installation** (multi-booting on endpoint devices & creating virtual machines)
- Familiar with **Intrusion Detection Systems** and **SIEMS** (SNORT, Splunk, SentinelOne, LogRhythm)
- Threat Analysis (**MITRE ATT&CK Framework**, open-source intelligence)
- Threat Hunting for Phishing (Mimecast, Microsoft Defender, **Crowdstrike Falcon Sandbox**)
- Microsoft Office & **Microsoft Access Database Development**

PROJECTS

- Used "**Cisco Packet Tracer**" to design a wide area network and security architecture for "Mayo Clinic" that would mitigate/detect cybersecurity attacks that could happen at each layer of the **OSI model** and align with the NIST framework (network administration, threat analysis)
- Proposed a specific network security architecture to reduce the risk of **SSL VPN** exploitation by threat actors leveraging a RootRot webshell to gain initial access to internal networks
- Installed and configured **Windows Server 2022** as a domain controller, managing **Active Directory**, user authentication, and group policies for a network of Windows 11 Home virtual machines deployed via **Hyper-V**
- Configured a dual-boot system on an Acer laptop with Ubuntu and Windows 11 using an external hard drive, installed **VirtualBox** on Ubuntu, and created a Ubuntu and Fedora Server **virtual machine** (managing partitioning, virtual hard disks, and external storage)