Arhum Zahid

571-523-8266 | U.S. Citizen | zarhum3@gmail.com | linkedin.com/in/arhum-zahid | arhumzahid.com

Education

George Mason University **Dec. 2024**
Bachelor of Science in Information Technology, Concentration in Cybersecurity *Fairfax, VA*

Technical Skills

Certifications: CompTIA Security+, CYSA+, AWS Cloud Practitioner, Microsoft Azure Fundamentals, CCNA, NCI, NCM
Tools: MS Office, Wireshark, Splunk, Nessus, Collection Commander, MECM, ServiceNow, Axonius, SentinelOne, VMware, Uber Agent, Crowdstrike Falcon, Power Bi, Active Directory, Nutanix, Nmap, Metasploit, Zeek, Burp Suite, Qualys WAS, ConnectWise, Tenable.io
Operating Systems: Windows, MacOS, Linux
Languages: Python, Windows Powershell, Java, MySQL

Experience

Arrow Electronics **June 2025 – Present**
Technical Solutions Engineer *McLean, VA*

- Sized and architected 10+ Nutanix HCI configurations for end customers migrating off legacy infrastructure, enabling multi-workload consolidation and reducing projected compute costs by an average of 30%.
- Led 5+ technical discovery sessions with end customers to assess existing environments and map requirements to optimal Nutanix solutions, accelerating time-to-proposal by 40%.
- Delivered enablement sessions to 50+ channel partners across NCI and NCM certifications, increasing partner-led Nutanix opportunity pipeline by 25%.
- Spearheaded NC2 (Nutanix Cloud Clusters on Azure) partner enablement, pioneering the first enablement session for Arrow's partner ecosystem and equipping partners to address global supply chain constraints through hybrid cloud solutions.

Institute for Defense Analyses **Mar. 2025 – Present**
Cybersecurity Engineer Intern *Alexandria, VA*

- Automated DNS-to-Active Directory mapping with PowerShell, streamlining workstation remediation and increasing turnaround by 70%.
- Remediated vulnerabilities across Windows Server 2012, 2016, 2019, and 2022 with the infrastructure team, improving server security posture by 30%.
- Consolidated vulnerability reports for leadership, prioritizing remediation across 2,000+ assets, improving visibility.
- Presented critical findings from Tenable, cutting manual vulnerability efforts by 40% and accelerating remediation.

Navy Federal Credit Union **May 2023 – Feb. 2025**
IT Governance Analyst Intern *Vienna, VA*

- Conducted a compliance audit of 3,400+ installations using Splunk, configuring AppLocker via GPO for application control, achieving 100% enterprise compliance.
- Refined SOPs, eliminating outdated information and integrating key metrics, resulting in a 40% boost in proficiency and standardized patching.
- Administered workstation admin access via CyberArk PAM, processing 2,551+ requests and enforcing least privilege in line with NIST SP 800-53 standards.
- Deployed a critical-severity zero-day hotfix, diligently securing 300+ endpoints within 3 hours of vulnerability disclosure, effectively mitigating crucial risks.

Vulnerability Management Analyst Intern *Vienna, VA*

- Upgraded Tenable Nessus agents to version 10.8.2 on 1,500+ endpoints, resolving critical plugin issues during a widespread outage.
- Integrated approved software into the continuous delivery pipeline, automating monthly patching and accelerating deployment speeds by 80%.
- Leveraged Splunk dashboards to monitor logs for endpoints, significantly enhancing end-to-end protection of assets.
- Implemented pre-deployment patch testing on test VMs, ensuring 100% functionality and minimizing disruptions, adhering to NIST SP 800-40 standards.
- Boosted Vulnerability Remediation Efficiency to 131% by resolving over 50 monthly tickets in ServiceNow, ensuring compliance with Service Level Agreement (SLA).

Projects

CrowdStrike Falcon EDR Threat Simulation Lab **May 2025**

- Simulated ransomware using PowerShell, triggering CrowdStrike Falcon detections mapped to MITRE ATT&CK T1486, resulting in a 100% detection rate.
- Conducted forensic analysis of Falcon's process tree and IOCs, reducing triage time by **60%** through early-stage behavioral insights and hash-based correlation.
- Built and executed automated scripts that generated, encrypted, and corrupted 10+ test files, leading Falcon to block the payload and quarantine malicious processes within seconds.