Zachary D. Henard

(423) 293-2364 - Zachary@Henard.tech
https://henard.tech - https://GitHub.com/zdhenard42
Clearance: Active DOD Sponsored Secret Clearance

EXPERIENCE

Tennessee Valley Authority Nashville, TN
Technology & Innovation Engineer January 2023 - Present

-Leveraged PowerShell to migrate 330 resource accounts into Entra (GCC High), resulting in $167,000 annual savings.
-Partnered with department heads and directors to design a service model for a smooth enterprise-wide transition.
-Integrated Graph API scripts into Azure Registered Apps allowing for on demand reports via webhooks.
-Created Ansible Playbooks to automate IOS upgrades for 523 Cisco devices reducing upgrade time by 95%.
-Deployed the playbooks to Ansible Automation Platform to leverage RBAC and management capabilities.
-Integrated verification tasks ensuring that failed upgrades would result in minimal network downtime.
-Conduct routine audits on Cisco gear, ensuring adherence to STIG guidelines and DISA standards.
-Utilize these assessments to highlight Cat-1 vulnerabilities found on devices supporting critical infrastructure.

Conquest Cyber Nashville, TN
SOC Analyst September 2022 – January 2023

-Developed “SOC Multitool”, a browser extension that aggregates 23 security tools for efficient investigations.
-Reached #22 on GitHub Trending and averages 3,000+ monthly users on Chrome Web Store.
-Received positive reviews from multiple security blogs and shared by industry leaders on social media.
-Utilized a combination of JavaScript, HTML, and ManifestV3 to create a seamless and effective user experience.
-Addressed 20+ daily security incidents using XSoar, Microsoft Azure/Sentinel, and QRadar.
-Developed 13 complex KQL queries increasing efficiency of evidence collection by 30%.

Intuitive Research & Technology Huntsville, AL
System Administrator Intern May 2022 – August 2022

-Developed “Thick2Thin Converter” script, utilizing Batch, PowerShell, and WinPE to automate desktop migration
-Deployed a login script that automated 14 tasks for user environment migration from thick to thin clients.
-Reduced user interruption by an average of 30 minutes per user for over 400 employees.
-Created a custom boot drive that automated re-imaging and conversion of desktops with WinPE and Wyse.
-Served as the primary contact for Virtual Desktop Infrastructure (VDI) issues for over 500 employees.

Army National Guard Knoxville, TN
Track Vehicle Mechanic April 2021 - Present

-Graduated as top of class from Advanced Individual Training, showing exceptional technical and leadership skills.
-Responsible for maintaining high-value military equipment ensuring they are in combat ready status.
-Trained in operational security and information security, applying these practices to secure communications and data.
-Collaborate in teams to solve complex technical problems, enhancing effectiveness in high-pressure situations.

EDUCATION

Tennessee Technological University Cookeville, TN
B.S Computer Science, concentration in Cybersecurity, 3.8 GPA May 2024

TECHNICAL EXPERTISE & CERTIFICATIONS

-Certifications: CompTIA Security+, AWS Solutions Architect Associate, Microsoft SC-200
-Cloud Technologies: Kubernetes, K3s, Rancher, Amazon Web Services, Microsoft Azure, and Entra ID.
-Programming Languages: C/C++, Python, JavaScript, SQL/KQL, YAML.
-Unix Tools: bash, Wireshark, Nmap, Metasploit, DirBuster, Ghidra, exploitdb, Kali, RHEL, and Ansible Tower.

PROJECTS

AWS Honeypot

-Deployed 19 Honeypots to an EC2 instance using a Debain 11 AMI to gather insights on modern attack methods.
-Leveraged Security groups to allow 19 vulnerable services to be exposed while keeping 3 internal services private.
-Created Kibana Dashboards allowing for a real-time attack map as well as attack analytics such as CVE used.
-Integrated daily reports showcasing the top results for over 40 metrics such as attacker IP and protocol used.

Majestic Million DNS Anomaly Detection

-Implemented real-time parsing of DNS queries using Logstash to detect anomalies outside the top 1M domains.
-Enriched logs with WHOIS info and IP metrics such as geolocation and reputation for comprehensive analysis.
-Stored the logs in OpenSearch Indices allowing for real-time alerts to detect suspicious queries being made.
-Created OpenSearch Dashboards allowing for a top-level view of top TLDs and Client FQDNs found in alerts.

Advanced QR-Code Analysis

-Collaborated with Virus Total to develop a machine learning model that identifies malicious QR codes through comprehensive data analysis, enabling automated decision-making based on the model's confidence scores.
-Leveraged JavaScript, Fetch API, and Cloudflare Workers for seamless integration and data presentation.
-Obtained 97% accuracy when tested on a 71,000 malicious QR code dataset, proving model accuracy.
-Integrated 6 threat analysis platforms, offering insight into QR content such as URL reputation and network data.

BuildLogix Construction Planning App

-Created a web app for a fencing company, integrating user accounts, payment processing, and real-time updates.
-Developed the user interface with Angular v16, API with Ruby on Rails, and managed data with MySQL.
-Integrated Stripe API and webhooks in Rails for payment confirmation, processing, and transaction logging.
-Utilized Atlassian Jira for agile project management and issue tracking throughout the development lifecycle.

Home Lab

-Designed and managed a sophisticated home lab with ESXi 6.5/8 for virtual machines and containers.
-Implemented OPNsense as a firewall, DHCP server, and router for network security and integrity.
-Integrated Rancher to deploy a self-hosted Kubernetes cluster running RKE2 to replicate a federal environment.
-Integrated NGINX Ingress controller with Let’s Encrypt to automatically obtain SSL certificates for my applications.
-Utilize Cloudflare Tunnels to securely serve self-hosted services to the internet.
-Deployed VMware VCenter allowing for cluster autoscaling via Rancher and the VCenter API.
-Utilized the simulated Cisco environments for robust testing of Ansible automation playbooks.
-Configured a managed switch for VLAN traffic segregation and network organization.
-Running Wazuh XDR on 5 OptiPlex PCs to implement complex endpoint security.

LinkedIn Connector

-Developed a Python script leveraging Selenium for automated LinkedIn connection requests.
-Utilized ‘undetected Chrome driver’, random intervals, and user-agent spoofing for bot detection evasion.
-Achieved up to 1,000 weekly connection requests without triggering security measures.
-Employed XPaths for personalized connection messages based on the target's job title.

Currency Converter

-Developed a Chromium browser extension to convert web page prices to user's preferred currency.
-Utilized a REST API for live exchange rates and JavaScript for currency identification.
-Supports **270** currencies including cryptocurrencies for simplified global currency conversions.