Zachary Henard

Cookeville, TN
(423) 293-2364
zdhenard42@tntech.edu

EXPERIENCE

Conquest Cyber, TN — *SOC Analyst Intern*
September 2022 - Present

- Monitor XSoar, Microsoft Sentinel, Qradar and other security tools for detection and identification of security events.
- Developed complex KQL queries to increase efficiency/effectiveness of evidence collection.
- Created CLI tool and browser extension to increase efficiency/effectiveness of investigations.
- Perform threat hunting in Microsoft Defender for Endpoint to identify potential security threats.
- Perform vulnerability and threat intelligence research via threat intelligence feeds.
- Document incidents, participate in War Room for compromises, breaches and notable events.

Army National Guard, TN
March 2021 - PRESENT

- Graduated from Advanced Individual Training as Valedictorian.
- Lead platoon of 40 trainees through basic training as a Platoon Guide

DOD Contractor, AL — *Sysadmin Student Hire*
May 2022 - August 2022

- Automated Thin Client migration (14 tasks)
- Automated Re-Imaging
- Automated Thick2Thin conversion
- Resolved ~120 Help Desk tickets
- Created scripts to resolve ~20% of daily help desk tickets
- POC for 500+ employees regarding VDI issues

Eastman Chemical, Kingsport, TN — *Lab Analyst*
January 2020 - May 2022

- Analyzed hundreds of samples a day to ensure that the automated process was running smoothly.
- Later moved to the pilot laboratory to test samples that will then be used in the world's largest methanolysis plant.

EDUCATION

Tennessee Technological University, Cookeville, TN — *Bachelor of Science, Computer Science; Concentration in Cybersecurity*
December 2021 - Expected May 2024
3.77 GPA, President's List

Northeast State Community College, Blountville, TN— *Associate of Science, Computer Science*
August 2019 - May 2021
3.8 GPA, President's List

SKILLS/CERTIFICATIONS

CompTIA Sec+ Certified
Secret Security Clearance
Penetration Testing
C++ & Python
Troubleshooting
Automation
Batch & Powershell scripting
Active Directory management
VDI configuration & security
IT Help Desk
PC Repair

AWARDS

"Above and Beyond"
Awarded by the VP of my previous employer for my contributions to the IT department.

Army Achievement Medal (AAM)
Graduated top of class in Advanced Individual Training and received an AAM Medal.

President's list
Maintained top 5% of class while attending Northeast State Community College

O-3 challenge coin
Received an O-3 challenge coin for management of a platoon during a simulated attack in basic training.

Philippine Army Challenge Coin
Received a challenge coin from soldiers of the Philippine army for repairing 5 year+ Inop M113A

Projects

SOC Multitool browser extension (JavaScript)

- Utilizes RegEX to automatically identify data type highlighted in browser by user (SHA256, IP Address, Domain, LOLBins, MAC Address, Base64, and Email Headers)
- Opens investigation summary from multiple sources based on data type identified.
- Utilizes Manifest V3

SOC Multi Tool CLI (Batch)

- Utilizes 5 APIs to automate investigations of IP addresses, hashes, domains, MAC Addresses, Filenames and LOLBins.
- Tracks investigators' cases and mean time to complete a case each day.
- Generates custom KQL queries based on the evidence provided

Thick Client Script (Batch + PowerShell)

- Back up user's mapped drives
- Generates login script for thin client
- Uploads Login Script to network drive
- Exports MsEdge Bookmarks
- Exports Chrome Bookmarks
- Empties User recycling bin
- Converts & exports all user DigiCerts into .pfx format
- Compress .PST/.TMP files to be compatible with OneDrive
- Exports Outlook Signatures

Thin Client Script (Batch + PowerShell)

- Imports MsEdge bookmarks
- Imports Chrome bookmarks
- Decompress .PST/.TMP files
- Imports Outlook Signatures

Custom Adobe Dynamic Stamps (JavaScript)

- 3 Dynamic Stamps created using JavaScript
- Imports stamps into Adobe Acrobat

Firefox Proxy Import (Batch + PowerShell)

- Generates Firefox profile
- Creates User.JS file in profile
- Configures 8 policies to implement proxy into browser
- Configures 3 policies to remove unnecessary bloatware
- Imports MsEdge bookmarks

Thick-To-Thin converter (Batch + PowerShell)

- Silently installs Dell Wyse Converter
- Installs VMware Horizon Client
- Configures System Preferences + Peripherals
- Configures Wyse Group Key
- Configures Horizon Connection Server
- Enrolls device into WMS
- Sends Device ID to network drive to notify SysAd it is ready to be accepted
- Restarts once device accepted to pull updates