Hyun Suk (Joseph) Shin

Pomona, CA | (310) 429-5231 | jshin1@cpp.edu | (310)429-5231 | linkedin.com/in/hsshin95

EDUCATION

California State Polytechnic University, Pomona *Expected Graduation 2025*
Masters of Science Information Security

University of California, Davis *Graduated 2019*
Bachelor of Science Computer Science

WORK EXPERIENCE

Field Engineer for the 127th Battalion, 1st Platoon, 1st Company, 1st Squad **Paju, South Korea**
Republic of Korea Army *February 2022-August 2023*

- Expertise in landmine and explosive installation and removal; Skilled in the operation and handling of the K2 rifle
- Proficient in the construction of Medium Girder Bridges to bolster support for both infantry and armored vehicles

BTSA2 Business Technical Support Analyst **Davis, CA**
UC Davis Phoenix IT Support *July 2021-January 2022*

- Achieved recognition as the highest-performing member of the Desktop Support Team
- Deployed the new USDA's greenhouse monitoring system to replace the old system. Successfully imported the old data into the new system to maintain data integrity
- Competent in the management of devices within an Active Directory environment, administration and configuration of DNS, DHCP, and IP addresses using Infoblox

ISA2 Phoenix Systems Client & Research Support Administrator **Davis, CA**
UC Davis Phoenix IT Support *July 2019-July 2021*

- Reimaged computers with Windows, MacOS, Ubuntu operating systems
- Rebuilt a Windows XP machine and installed specialized drivers to connect to a qPCR machine to save the department $5000
- Trained incoming students and emergency hires on diagnosing hardware and software skills

PROJECTS

SWIFT
CyberForce Competitor *September 2023-Present*

- Performed Nessus scans, configured Active Directory GPOs and installed SIEMs to harden Windows Servers, Active Directory and various linux distributions to protect against the red team
- Simulated attacks using Atomic Red Team scripts and detected them using and Bluespawn EDR to map the chain of attacks to the MITRE ATT&CK framework. Program scripts to automate using python and bash
- Created a report and presented the identified risks to a mock c-suite panel (CEO, CIO, CFO) to explain business impact and provided recommendations and solutions to mitigate risks

Threat Detection
Aurora Lite and Sigma *October 2023-Present*

- Knowledgeable in executing diverse offensive maneuvers using tools like Kali Linux, responder, crackmapexec, mimikatz, bloodhound, hashcat and more to simulate advanced adversary attacks
- Proficient in setting up an EDR Aurora Lite and incorporating Sigma rules to perform threat detection within a controlled virtual environment utilizing VMware Workstation Player

TryHackMe
Online cyber-security training, Ranked Top 3% *October 2022-Present*

- Learned how to use nmap to scan for vulnerable ports and gobuster to fuzz websites to find insecure websites
- Used Wireshark to identify sensitive data being leaked through unencrypted network traffic and burpsuite to find vulnerable injection points in websites
- Performed LLMNR poisoning, Kerberoasting, Golden/Silver ticket attacks, GTFO bins, crontabs, environment variables and public exploits to gain admin access on vulnerable machines to extract sensitive data

CERTIFICATIONS

- COMPTIA Security+
- COMPTIA Network+