# ZANDER WORK

www.linkedin.com/in/zanderwork

## Summary

Enthusiastic cybersecurity student with 4 years of relevant work experience. Driven analyst with experience working with industry standard tools (Zeek, Nessus, Elastic, Splunk) to analyze 40 Gbps of traffic for known and unknown threats. Experience with networking and virtualization via a home lab. Proven leader/self-starter from the NW Cyber Camp (over 100 participants, 95% positive feedback), and the OSU Security Club (with multiple high-placing finishes).

## Skills

**Security**

- Malware Analysis (IDA Pro/Hex-Rays Decompiler, gdb, radare2)
- Binary Exploitation (pwntools)
- Vulnerability Scanning (Nessus, OpenVAS)
- Network Security (Zeek, Wireshark, nmap)
- Log Management (Splunk, Elasticstack)

**Infrastructure**

- Virtualization (VMware vSphere, VMware Workstation, VirtualBox)
- Cisco Networking (IOS)
- Configuration Management (Ansible)
- Containerization (Docker)
- Rapid Prototyping (Vagrant)

**Programming**

- C, C++
- Python, *sh, PowerShell
- HTML/CSS/JavaScript
- Django/Flask
- x86 Assembly
- Git

## Education

**BS, COMPUTER SCIENCE (SECURITY) |** Oregon State University | 3.80 GPA | Est. Graduation June 2021 (Rising Junior)

- Honor Roll since Fall 2017
- Minoring in Asian Languages and Cultures (Chinese concentration)
- Key Courses: Intro to Digital Forensics, Operating Systems I and II
- Fall 2019 Courses: Intro to Security, Cyber Attacks and Defenses, Systems Security, Intro to Computer Networks, and Chinese

## Work Experience

**TECHNICAL INTELLIGENCE ANALYST INTERN |** FireEye, Inc. | June 2019 - Present

- Analyze and process intelligence on financial crime threat activity to write reports for customers
- Profile and manipulate attacker Command & Control servers to learn more their malware communications
- Hunt for and analyze malware samples from internal and external sources to support intelligence analysis
- Deploy and integrate a sandbox environment for automated Android malware analysis for use across the entire company
- Contributed to internal tracking of threat actors, malware samples/families, and TTPs

**SECURITY ANALYST |** Oregon Research & Teaching Security Operations Center (ORTSOC) | Oct 2017 – June 2019

- Work with Zeek, Nessus, Splunk, and the Elasticstack to perform network monitoring & analysis (average 40Gbps traffic)
- Design, deploy, and maintain production and development infrastructure
- Develop automation to improve analysis efficiency by over 50% (Python/Bash)
- Monitor and respond to end-user phishing incidents
- Contribute to documentation and training materials for other team members

## Activities/Awards

**OSU Security Club**

- President of the club since 2017
- Captain for competition teams
- Work with industry partners to bring recruitment events and presentations to our club members
- Work with the College of Engineering to secure funding for competitions and tools

**NW Cyber Camp**

- Co-founded in 2016
- 5 sessions with over 100 total participants
- Weekly management meetings
- Work with local high schools for recruitment
- Coordinate with industry partners to secure funding and guest speakers

**Awards**

- 3rd place, Pacific Rim Collegiate Cyber Defense Competition 2019
- 1st place regionally, 3rd place nationally at the Cyberforce Competition 2018