AXEL MUNOZ

Philadelphia, PA · (215) 800-6876

me@axelp.io

EXPERIENCE

1/2019 – CURRENT

SENIOR THREAT HUNTER, BOOZ ALLEN HAMILTON (DARK LABS)

Coordinate hunts with multiple customers simultaneously. Develop signatures and analytics to detect adversaries' tools and TTPs. Hunt threats and collect intelligence under time constraints.

10/2018 – 01/2019

ENDPOINT SECURITY CONSULTANT, USAA

Develop detections from both well-defined and open-ended security vulnerabilities. Develop Proofs of Concept to test vulnerabilities and exploits, as well as responsiveness and false-positive rates of detections. Use industry standard tools such as Phantom, HX, SysInternals Suite, and Wireshark to develop detections. Program and support software to assist in threat hunting and detection development. Hunt threats across a 50k endpoint environment to find evil. Reverse-engineer binaries to build detections and deny access to our environment.

06/2018 – 10/2018

CYBERSECURITY ENGINEER, L-3 TECHNOLOGIES

Worked with third-party vendors to stand up security products. From the first contact, to purchase, to installation and maintenance, bridged the gap between the vendor to best address security concerns in the enterprise environment to secure the network. Created signatures by identifying and reverse-engineering malicious files and malware. Reprogrammed the production Mail Filter from the ground up, adding additional features and workflows, and adding support for new scanning methodologies. Conducted Proofs of Concept of vulnerabilities and exploits to determine security risk to the enterprise. Increased speed and efficiency of scanning tools enterprise-wide.

09/2017 – 06/2018

CYBERSECURITY ANALYST, L-3 TECHNOLOGIES

Conducted analysis on malicious emails from following network flow to reverse-engineering malware. Identified code and security flaws in mail filter. Established as the point of contact for other analysts in reverse-engineering activities. Supported new SOC Transformation projects by working with multiple vendors to stand up security products.

09/2016 – 04/2017

INTRUSION DETECTION ANALYST, PFIZER

Automated analysis workflow revolving around endpoint detections, sandbox results, email scanning, and IMS platforms. Streamlined the phishing analysis to an almost analyst-free experience. Created scripts to execute actions based off analyst inputs from isolating endpoints, to hashing directory trees, to sandboxing malware and returning results. Worked with industry-standard investigation tools such as FireEye's HX and NX, Splunk, EnCase, FTK, IBM's Resilient, IDA Pro, tcpdump, and WireShark.

06/2016&17 – 09/2016&17
SOFTWARE DEVELOPER, LEMMA

06/2014&15 – 08/2014&15
BUDGET ANALYST INTERN, US ARMY AFRICA G-8

06/2012 – 08/2012
IT SUPPORT ANALYST, 414TH CONTRACTING BRIGADE

EDUCATION

06/2020
CRYPTOLOGY AND INTELLIGENCE ANALYSIS, DREXEL UNIVERSITY

Selected Courses

- CS 283 – Systems Programming
- CS 281 – Systems Architecture
- CT 388 - Penetration Testing and Ethical Hacking Lab
- CS T780 Special Topics in Cryptography (Graduate Course)
- CT 410 - Information Warfare
- CST 212 - Computer Investigations
- CS 475 – Computer and Network Security
- CS 380 – Operating Systems

SKILLS AND LANGUAGES

- Security Analysis and Engineering
- Programming
- Forensic Investigations
- Concurrent and Distributed Systems Programming
- Systems Administration
- Python (Expert)
- Bash (Intermediate)
- PowerShell (Intermediate)
- Perl/PHP (Intermediate)
- C/C++ (Intermediate)

ACTIVITIES

- Placed second at the Materials Research Society Hackathon; topic: Intelligent Materials Science Paper Term Interpreter for Reader Comprehension using Custom Hierarchical Data Structures.
- Placed first at the ASM Hackathon; topic: Reverse Engineering of Al 6061 Heat Treatment.
- Eagle Scout and Vigil Honor.
- Programming tutor for underprivileged kids.