# Axel Persinger

me@axelp.io | (215) 800-6876 | TS/SCI Active | Columbia, MD

## EXPERIENCE

### Invictus International Consulting — *Senior Software Engineer/Team Lead*

May 2020 - PRESENT

Key Accomplishments: Create indigenous catalog of capabilities to create new revenue streams by selling advanced software to mission-critical units. Mentor multiple junior employees on offensive security tradecraft. Lead and Manage workflow for 12 direct reports concurrently. Assign vulnerability research tasking for team members.
Analyze individual binaries, firmwares, and software systems for vulnerabilities. Research novel exploitation techniques in order to support existing CONOPS. Develop automation systems for increasing developer productivity in vulnerability research and exploitation activities. Lead a successful dynamic team that received accolades from end customers. Theorize, Research, and Develop state-of-the-art capabilities to ensure mission success. Plan and Orchestrate the creation of a secure, dynamic network to house developer activities.

### Booz Allen Hamilton — *Offensive Security Engineer and Researcher*

Jan 2020 - May 2020

Facilitate the creation of a technical blog to boost BAH's technical capital and reputation. Design and engineer CTF frameworks to administer challenges across national conferences. Design and engineer advanced CTF challenges. Mentor other teams/coworkers in BAH on offensive trends and methodologies. Rapidly prototype Proof of Concepts (POCs) to demonstrate market viability to firm executives. Research and exploit low-level Windows kernel structures and kernel drivers.

### Booz Allen Hamilton — *Senior Threat Hunter*

Jan 2019 - Dec 2019

Key Accomplishments: Discovered Advanced Persistent Threat (APT)-level malware. Automated repetitive tasks for an increase in analyst's productivity. Champion new tools and workflows.
Author reports and other deliverables for clients to notify them of malicious activity in their network. Hunt across multiple enterprise networks to detect nation-state authored malware. Develop signatures and analytics to detect adversaries' tools and Tactics, Techniques, and Procedures (TTPs). Hunt threats and collect intelligence under time constraints. Debrief team on relevant collected intelligence.

### HireVergence to USAA — *Endpoint Security Consultant*

Oct 2018 - Jan 2019

Key Accomplishments: Developed Proofs of Concept to test vulnerabilities and exploits, as well as responsiveness and false-positive rates of detections.
Developed detections from both well-defined and open-ended security vulnerabilities. Programmed and supported software to assist in threat hunting and detection development. Hunted threats across a 50k endpoint environment to find evil. Reverse-engineered binaries to build detections and deny access to the network.

### L3 Technologies — *Cybersecurity Engineer*

June 2018 - Oct 2018

Key Accomplishments: 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. Exploited vulnerability in key security software, showing critical vulnerabilities in the network.

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. Conducted Proofs of Concept of vulnerabilities and exploits to determine security risk to the enterprise. Increased speed and efficiency of scanning tools enterprise-wide.

### L3 Technologies — *Cybersecurity Analyst*

Sep 2017 - June 2018

Key Accomplishments: Decreased analyst workload as much as 70% by rewriting Indicators of Compromise (IOCs) and detection pipeline to eliminate false positives.

Established as the point of contact for other analysts in reverse-engineering activities. Conducted analysis on malicious emails from following network flow to reverse-engineering malware. Identified code and security flaws in the mail filter and was selected to fix the critical security appliance.

### Atrium Staffing to Pfizer — *Intrusion Detection Analyst*

Sep 2016 - April 2017

Automated analysis workflow revolving around endpoint detections, sandbox results, email scanning, and IMS (Incident Management System) platforms. Streamlined the phishing analysis to an almost analyst-free experience.

## EDUCATION

### Drexel University — *Bachelor's in Cryptology and Intelligence Analysis*

Custom-Designed and accredited degree specializing in cryptology, cybersecurity, and intelligence analysis. Over 120 hours of systems-level programming and design instruction, and over 210 hours of information security instruction including a graduate-level course in cryptography. Multiple intensive self-study courses ranging from pure mathematics to advanced hacking techniques.

## SKILLS & TECHNOLOGIES

| | | | | | |
|---|---|---|---|---|---|
| Ghidra | Python | C/++ | Windows Kernel | Linux Kernel | Splunk |
| Reverse Engineering | CNO Development | Vulnerability Research | Curriculum Development | Systems Exploitation | Software Engineering |

## MISC

Discovered multiple 0days in an application and wrote exploit kits for them, resulting in: CVE-2021-27569 - CVE-2021-27574.