Aaron **Lichtman**

SOFTWARE ENGINEERING · CYBERSECURITY

✉ aaronlichtman@gmail.com | 🏠 alichtman.com | alichtman | aaron-lichtman

Experience

Security Engineer — *Seattle, WA*
PRODSEC NATIVE ASSURANCE — FACEBOOK — *June 2022 - Present*

- Built continuous integration testing systems to detect security vulnerabilities and prevent security regressions in PortalOS.
- Created threat models and documented attack surfaces in order to effectively prioritize security review efforts.
- Conducted security reviews of high-risk surfaces. Created mitigations that eliminated vuln classes.
- Triaged whitehat reports, awarded bug bounty payouts, and created proof of concept exploits.

Rotational Security Engineer — *Remote*
RED TEAM X, INCIDENT DETECTION AND RESPONSE (IDR), PRODSEC — FACEBOOK — *Dec 2021 - June 2022*

- Expanded EDR capabilities, improved case investigation tooling, and triaged the IDR incident queue.
- Analyzed Unity engine to create signatures that could be used to hunt for and identify malware in 3P Oculus apps.
- Expanded coverage of automated vuln detection tools, resulting in vulns being detected and remediated before being deployed.
- Coordinated incident response at company-wide scale. Led day 0 log4j response – patched critical services, including Messenger.

Software Engineer — *Remote*
PORTAL KERNEL SECURITY — FACEBOOK — *Sept 2020 - Dec 2021*

- Led hardening efforts for PortalOS by using sanitizers, fuzzers, and modern security mitigations.
- Built the first PoC fuzzing harnesses for Portal using AFL. Used UBSAN / ASAN / MSAN / TSAN to find hundreds of bugs, including a set of memory corruption vulnerabilities in PJSIP: *CVE-2022-39244 (9.8 CVSS)*.
- Added Portal support to manufacturing platform. Built HSM integration, logging for security auditing, auto-escalation policies.
- Created factory resource monitoring pipelines to eliminate entire classes of manufacturing issues, saving millions of dollars.

Software Engineering Intern — *Menlo Park, CA*
AUTHENTICATION E2E TEAM — FACEBOOK — *Summer 2019*

- Worked on a team securing authentication across the entire Facebook universe of apps, including Whatsapp and Instagram.
- Designed, implemented and deployed a solution to prevent internal attackers from obtaining access to user accounts and data.
- Improved monitoring and auditing capabilities in C++ for more than 1 billion daily authentication attempts.

Open Source Software

Malware Techniques — *Champaign, IL*
A COLLECTION OF TECHNIQUES USED IN LINUX AND MACOS MALWARE — *2019*

- Researched Linux and macOS malware, and implemented anti-VM, anti-debugging, anti-analysis and persistence measures.
- Designed and developed a Linux LKM (14.4 - 14.8) rootkit that hooks syscalls, and is undetected by standard rootkit checkers.
- Developed educational malware in a variety of languages, including: C, x86, Bash, Python, and Objective-C.

Deadbolt — *Champaign, IL*
CROSS-PLATFORM FILE ENCRYPTION FOR HUMANS — *2019*

- Built a cross-platform (Linux, Windows, macOS) Electron app with a sleek UI to simplify encryption and decryption of files.
- Designed an intuitive user experience for secure encryption with AES-256, easily accessible to non-technical users.

Stronghold — *Champaign, IL*
MACOS HARDENING TOOL — *2018*

- Developed a command line interface that guides users through step-by-step secure configuration for macOS.
- Secured the workstations of more than 35,000 macOS users and earned ~1k stars on GitHub.
- Gained familiarity with macOS security architecture.

Education

University of Illinois at Urbana-Champaign — *Champaign, IL*
B.S. IN COMPUTER SCIENCE AND LINGUISTICS — *May 2020*

- **GPA**: 3.54/4.00; **Dean's List**: 2017, 2018, 2019, 2020
- Discrete/Data Structures, Algorithms, Computer Architecture, Systems Programming, Computer Security, Digital Forensics

Skills

Certs	OSCP
Languages	Python, C, C++, Swift, x86, Node.js, bash / zsh, AppleScript
Tools	macOS, Linux, radare2, Ghidra, Wireshark, VMware / VirtualBox, Volatility, Git