

System-level programming and research

EXPERIENCE

Cisco Systems / EDR team

Software Engineering Technical Leader

2025 - Now

Senior Software Engineer

2022 - 2024

Research and development of high-efficacy anti-malware engines within an EDR/EPP product.

- Transformed a Windows-specific behavioral engine into a cross-platform, generic event processing framework (Apache Flink like), now integrated across multiple Cisco products.
- Designed and delivered multiple features, enhancing detection quality and efficacy over time.
- Improved anti-ransomware efficacy by introducing sophisticated stateful event-matching capabilities.
- Researched many miscellaneous topics, including: running regex runtimes within a Windows kernel space; stateful, real-time log analysis; or implementing a [Sigma](#) rule transpiler.
- Handled DevOps-like duties such as managing CI infrastructure, creating automation scripts and handling release delivery.

Akamai Technologies / NOS team

Software Engineer Associate

2020 - 2022

Development of a specialized embedded Linux based network operating system (NOS) for routers deployed across the Akamai network.

- Added support for in-ASIC IP multicast routing by integrating the FRR routing daemon with the Linux networking stack and a proprietary routing chips.
- Introduced a syslog-based logging strategy and combined it with Splunk-based ingestors to facilitate better deployment monitoring and root cause analysis.
- Revamped configuration reloading logic, greatly cutting the time required to set up a new device.
- Great track record of finding and solving nuanced bugs spanning across hardware, software, and network layers.

SKILLS

- Good command of **C/C++**, **Rust**, **x86-64 assembly**, **Powershell**, **bash** and **Python**. Can quickly adapt to whatever is needed at the moment.
- Proficient in **Windows and Linux internals**, as well as **system-level programming**, both in **user and kernel space**.
- Ability to **research obscure and undocumented topics** through reverse engineering, reviewing sources, or any appropriate method for a given situation.
- Familiar with typical tooling, including **git**, **debuggers**, **virtualization technologies**, **containers**, **build systems**, **Linux/Windows utilities** and more.

CERTIFICATIONS

- [OSCP](#) (Offsec PEN-200): Penetration testing of Windows and Linux environments.
- [OSEP](#) (Offsec PEN-300): Exploitation of Active Directory and AV evasion methodologies.
- [OSED](#) (Offsec EXP-301): Binary exploitation and reverse engineering within the Windows environments.

EDUCATION

AGH University of Science and Technology

Bachelor of Computer Science

2017 - 2021

- [Bachelor's thesis project](#): Implementation of a RISC-V softcore CPU using Verilog and an FPGA chip, including tooling such as a bootloader, assembler, and C language support.