



whatthefox.dev



iansfox@pm.me



ian-fox



iansfox

Ian Fox

SKILLS

- Programming Languages: Rust, Python, Golang
- Technologies: Kubernetes, Terraform, Linux internals

EXPERIENCE

Cognite

Oslo, NO

Senior Security Operations Engineer

Feb 2025 - Present

- Automated incident response tasks through SIEM and SOAR tooling.
- Worked with infrastructure teams to implement new access solutions.

Defendable

Oslo, NO

Security Analyst

Nov 2024 - Feb 2025

- Developed automation for Palo Alto XSOAR to assist SOC analysts.
- Created a platform to give CTF participants access to a terminal in a container through their phones.

Omny Security

Oslo, NO

Senior Security Researcher

Oct 2021 - Aug 2024

- Created document parsing tools using OpenCV and GPT4-V.
- Created demonstrations of simulated ICS environments and attacks against them.
- Wrote and presented talks at DEFCON ICS Village, BSides Oslo, S4x2023.
- Developed and debugged CI/CD tooling and infrastructure.

Splunk

Waterloo, CA

Cloud Security Engineer

Jul 2020 - Sept 2021

- Developed and maintained automation for various security processes such as vulnerability scanning.
- Worked with stakeholders to plan and deliver enhancements to the vulnerability reporting process.
- Delivered webinar on using terraform to manage firewall rules with Signal Sciences

Cognite

Oslo, NO

Software Development Intern

Sep 2019 - Dec 2019

- Implemented new authentication mechanism using Hashicorp's Vault.
- Fixed security vulnerabilities related to authorization.

Splunk

San Jose, US

Software Engineering Intern

Jan 2019 - Apr 2019

- Designed and developed integrations between GitLab CI and static code analysis tools, streamlining developer workflow.
- Built systems to automate tool deployments for the Product Security team.
- Created and delivered training on CI best practices.

Oath

Sunnyvale, US

Technical Intern

Jan 2018 - Aug 2018

- Designed, implemented, and open sourced the yFuzz fuzzing orchestration tool.
- Developed a slack bot with Flask for a security engagement initiative encouraging employees to lock their computers.
- Conducted physical penetration tests and reconnaissance for Oath's red team.

Yahoo

Sunnyvale, US

Technical Intern

May 2017 - Aug 2017

- Added a new authentication mechanism for the Screwdriver CD tool with Ember.js and Hapi.js.
- Developed a plugin to queue Screwdriver jobs with Redis, enabling more complex pipeline structure.

OpenText Corporation*Junior Developer Intern***Waterloo, CA***May 2016 - Aug 2016*

- Developed features and fixed bugs in the OpenText Core desktop client

OpenText Corporation*High School Intern***Waterloo, CA***Jun 2014 - Aug 2014, Feb 2015 - Jun 2015*

- Developed web applications in a small team setting.
- Created integration allowing OpenText Core files to be opened in Google Docs for online editing with OAuth.

EDUCATION

University of Waterloo*Bachelor of Honours Computer Science***Waterloo, ON, Canada***June 2020*

PROJECTS

Crabtrap*Jun 2024*

- Proof of concept for syscall blocking similar to seccomp-bpf at the shared object level instead of process level.
- Runs a child process under ptrace and uses the proc filesystem to map stack traces for syscalls to shared objects, then allows or denies them based on policy.
- Blog post explaining the design at whatthefox.dev/posts/crabtrap

Vault JWT Backend*Oct 2019*

- JWT-signing plugin for Hashicorp's Vault, allowing JWTs to be signed without the private key ever leaving Vault.

yFuzz*Mar 2018*

- Tool to allow orchestration of parallel of fuzzing jobs with Docker and Kubernetes.
- Server and CLI written in Go, offering authentication through mutual TLS and RBAC through Yahoo's Athenz.

ADDITIONAL EXPERIENCE

BSidesLV Volunteer - Sponsor Ops*Aug 2024 - Present*

- Assisted in conference planning and on-site operations.

Øvelse Bukkesprang (Large simulated incident response exercise)*Nov 2023*

- Wrote a ransomware decrypting tool based on a threat intelligence report, enabling attribution of an attack.