

Simon Pinfold | Resume

simon@uint8.me • github.com/synap5e

Wellington, New Zealand

Security Engineer and Software Engineer focused on driving secure product delivery and implementing robust security architecture and practices across all technical domains.

Key Skills

- **Programming & DevOps:** Python, TypeScript, C#, Java, C. Familiar with containerization (Docker, Kubernetes), CI/CD pipelines (GitHub Actions, GitLab), and Cloud and Serverless tooling.
- **Architecture:** Design and deployment of secure, end-to-end solutions. Expertise in Threat Modeling and Zero Trust principles.
- **Offensive Security & Vulnerability Research:** Full-scope penetration testing, Red/Purple team engagements, 0-day vulnerability research.
- **Reverse engineering:** Vulnerability development focused on fault injection, fuzzing, and root cause analysis. Proficient with compiled binaries (x86/x64) and bytecode.
- **Agentic AI:** Engineered and using custom LLM-orchestration frameworks (LangChain/LangGraph, custom) for automated security research, vulnerability assessment, and triage.

Work Experience

- FirstCape: Cybersecurity Engineer 2024 - Present
- Led and executed comprehensive Red/Purple team engagements and application security testing
 - Discovered and reported many critical vulnerabilities to in-house software teams and to multiple international vendors.
 - Primary technical security professional for incident response and threat hunting.
 - Architected the security stack for a greenfields environment after divestment from Jarden Partners.
- Jarden: Cybersecurity Engineer 2022 - 2024
- Developed and utilised risk-based approaches for Jarden's Cybersecurity programme.
 - Performed IR and threat hunting, SDLC uplift, and broad security function.
- Jarden: Software Engineer 2020 - 2022
- Worked on cloud-native uplift from a legacy monolith system to modern microservices architecture.
- OverTrack: Startup Sole Founder 2017 - 2020
- Sole founder, architect, and full-stack developer of a B2C subscription SaaS.
 - Built and managed the entire stack: microservice AWS architecture with payment/subscription system.
 - Developed a custom client application able to track complete game statistics (kills, objective data, map data) for Overwatch and Apex Legends matches purely through Computer Vision and AI.
 - Demo: <https://overtrack.uint8.me>

Research, Published/Acknowledged Vulnerabilities, Projects, Open Source

ConnectWise Automate (Remote Management and Monitoring tool) RCE

- Reported multiple CVEs in ConnectWise Automate RMM. CVE-2025-11492 (9.6), CVE-2025-11493 (8.8).
- Writeup: <https://github.com/synap5e/connectwise-automate-AiTM-rce>
- Press Coverage: [ConnectWise fixes Automate bug allowing AiTM update attacks](#)

ZScaler Research

- Developed a bypass for *device policies*, enabling access via an unsanctioned device, discovery clash with [SynActiv](#).
- Ongoing novel work into a potential RCE.

Bug Bounties

- *Blizzard Entertainment*: discovered and reported a protocol based "auto win" exploit in Hearthstone.
- *Valve Software*: discovered and demonstrated two Remote Code Execution vulnerabilities in Source Engine (affecting online play), credited in [Valve's Security Hall of Fame](#).

Education

Victoria University of Wellington - B.Sc. (Computer Science) with Honours (First Class)

2013 - 2016