Dahvid Schloss, OSCP

Cybersecurity Executive · Offensive Security Leader · U.S. Special Operations Veteran

Raleigh, North Carolina · dahvidschloss@gmail.com

dahvidschloss.com · linkedin.com/in/dahvidschloss · github.com/dahvidschloss · youtube.com/@thecyberidiots

PROFILE

Cybersecurity Executive | Red Team Expert | U.S. Special Operations Veteran

Strategic cybersecurity executive and U.S. Special Operations veteran with 16+ years building security programs and the service lines that deliver them. Co-founded a red team firm that was later acquired, and helped grow another security firm from 3 to 40 employees. Has driven revenue growth of up to 300% while advising 100+ clients, from startups to the Fortune 500. Remains a hands-on operator by design, engineering custom AV-evasion tooling and uncovering 0-days to understand real attacker capability and translate cyber risk into business risk executives can act on. A DEF CON Black Badge holder, one of the conference's first seven official trainers, and a trusted expert commentator for national media.

SUMMARY OF QUALIFICATIONS

- Builds proactive, people-first security teams and lives by the Special Operations standard that leaders eat last.
- Co-founded and exited a U.S.-wide Red-Team-as-a-Service firm
- Grew U.S. revenue 300% while building a UK firm’s Americas operation from the ground up
- Grew revenue 100%+ YoY for three straight years and built a service line profitable in year one
- Scaled a security firm from 3 to 40 employees in under two years as its founding manager
- Trusted advisor and vCISO to 100+ clients, from startups to Fortune 500
- Engineered post-exploitation frameworks, kernel-level shellcode loaders, and a full-stack purple teaming platform
- Cut a recurring security workflow from 120 man-hours per week to 5 minutes through automation
- Former Special Operations offensive cyber operator, conducting real-world operations against live adversaries
- DEF CON Black Badge holder, one of seven inaugural DEF CON trainers, and frequent conference speaker

PROFESSIONAL EXPERIENCE

Chief Operating Officer · Suzu Labs

04/2026 – 10/2026 · Remote

- Led the post-acquisition integration of Emulated Criminals into Suzu Labs, including its IP, service lines, and delivery operations.
- Rebuilt core operating processes across sales, delivery, and contracting to improve repeatability and cut operational drag and risk.
- Overhauled the contracting framework, including MSAs and SOWs, to reduce the organization's legal and financial exposure.
- Authored company strategy and go-to-market positioning for offensive security and advisory services.
- Served as one of the company’s primary media voices, providing expert commentary in national outlets including The Register and AOL.
- Doubled as a lead operator, scoping, executing, and briefing penetration tests and red team engagements end-to-end while running company operations.

Co-Founder, CEO · Emulated Criminals (acquired by Suzu Labs)

09/2022 – 04/2026 · Remote

- Co-founded a red team tooling shop and grew it into a full-service Red-Team-as-a-Service firm, leading to its acquisition by Suzu Labs.
- Built and scaled a multi-state offensive security and development practice with workflows that outpaced competitors on reliability and repeatability.
- Architected and led development of EC RallyPoint, a three-part purple teaming platform built using Electron, React/Next.js, C#, Auth0, and gRPC.
- Advised clients on NYDFS, ISO-27001, SOC2, HIPAA, FDA Cyber guidance, PCI-DSS and FedRAMP, tailoring controls to business requirements.
- Served as a Red Team subject-matter expert, performing hands-on testing and incident validation.

Director, Offensive Security, Americas · CovertSwarm

07/2024 – 03/2025 · Remote

- Hired to establish a U.S.-based operation serving the Americas for the UK-based firm as part of its global expansion strategy, helping grow U.S. based revenue by 300%.
- Served as Americas Service Delivery Lead, owning the full sales lifecycle from unqualified lead to delivery handoff, closing subscription services with 10 new clients.
- Led a distributed sales and delivery team across four countries, holding one delivery standard across time zones, borders, and client environments.
- Acted as primary liaison between the UK executive team and Americas operations on strategy, compliance, and cross-border execution.

Director, Offensive Security · EchelonRisk+Cyber

04/2021 – 07/2024 · Remote

- Service Delivery Lead for sales of the Offensive Security service, achieving 165% YoY gross revenue growth, becoming profitable within one year of being a service.
- Founding manager, helped scale the firm from 3 employees to 40 in less than two years.
- Directed all offensive security services teams: physical, wireless, internal and external testing, social engineering, red and purple teaming and threat hunting.
- Advisor and vCISO to 100+ clients, from startups to the Fortune 500, guiding risk reduction and compliance with PCI-DSS, HIPAA, SOC 2, and ISO 27001.
- Led offensive security R&D, including a kernel-level shellcode loader built for AV evasion, reducing reliance on external tooling.
- Built and taught a 48-hour malware development training in C++ and Python supporting client Red Teams to improve their capabilities.

Senior Specialist, Red Team Operator/Lead · Deloitte Risk and Financial Advisory

09/2018 – 04/2021 · Remote

- Technical manager of an 8-person team delivering managed penetration testing, red team, and purple team services to a nationwide client.
- Led and managed a global team in devising and implementing strategic risk reduction initiatives, establishing 24/7 support to minimize external risk exposure for a key client.
- Directed a Python development team in creating and managing automation solutions for the RiskIQ platform, reducing time spent on required tasks from 120 man-hours per week to 5 minutes per week.

Information Operations Security Researcher · Joint Communications Unit, Cyber

07/2016 – 10/2018 · Fort Bragg, NC

- Conducted real-world offensive cyber operations supporting the targeting of high-value individuals in terrorist organizations.
- Routinely briefed both technical and non-technical audiences comprised of military commanders and civilian directors on mission capabilities, research projects, and development directions.

Special Operations Communicator · Joint Communications Unit, ECS

10/2013 – 07/2016 · Fort Bragg, NC

- Prepared for and conducted no-notice special operations missions in support of emergency response directed by the US Special Operations Command.

Enterprise System Administrator · U.S. Air Force, 561 Network Operations Center

03/2010 – 10/2013 · Hickam AFB, HI

- Managed and implemented security of a $650 million network spanning 13 time zones across 10 bases, servicing 40K command and control systems across the Pacific Air Force.
- Operated and maintained a $2.1 billion Air Force Network across 5 major enterprise networks comprising 525 servers and 1.2M e-mail accounts.
- Led a team of 5 administrators who migrated 9K legacy Windows PCs and 13K legacy Active Directory objects into the new Air Force Network forest with 100% uptime.
- Led a team of 5 conducting hardware and software upgrades on 350 Windows enterprise servers supporting 67K users.
- Served as point of contact for email warrants for the Air Force Office of Special Investigations in Hawaii; performed e-mail sanitization for Freedom of Information Act compliance.
- Responsible for asset management of $1.1 million in network and server equipment; wrote SOPs and knowledge articles for deploying Enterprise Exchange servers for the Air Force.

Additional roles

Course Developer and Instructor · Just Hacking Training (Contract)

01/2025 – Present · Remote

- Authored technical courseware translating complex Windows internals, C2 architecture, execution techniques, and malware tradecraft into practical, approachable lessons.
- Built a low-cost physical ICS training platform used to demonstrate Modbus exploitation and the kinetic impact of cyber attacks against industrial processes.
- Created and delivered the six-part Windows Malware Development (WMD) course series covering shellcode loaders, advanced execution and obfuscation, dynamic evasion, position-independent code, C2 development, and post-exploitation tooling.
- Instructed advanced malware development techniques including API resolution, PE manipulation, reflective loading, process injection, memory execution, and shellcode development.

EDUCATION

Certifications: Offensive Security Certified Professional (OSCP) · CompTIA Security+ · Network+ (expired) · Interconnecting Cisco Networking Devices 1 (expired)

Courses: Special Operations Radio Operators Course (JCU/JSOC) · Special Operations Network Operators Course (JCU/JSOC) · Offensive Cyber Network Operators Course (JSOC)