



Founder Biography

Alec Wood — Founder & Principal Security Engineer, Strata Security

Alec Wood is the founder and principal engineer of Strata Security, and a cybersecurity engineer with more than a decade of hands-on experience spanning federal offensive security, application security engineering, and mobile reverse engineering. His work sits at the intersection of two disciplines that are usually kept separate: the research background to understand how software actually breaks, and the engineering discipline to build software that holds up regardless.

That combination didn't come from a single career track. Alec's background begins in the U.S. Air Force, where more than a decade of service took him from installation defense and anti-terrorism program management to leading cyber workforce operations for a large enterprise population, and eventually into hands-on technical security work. A competitive Cyber Network Operations fellowship with Accenture Federal Services sharpened his offensive tradecraft — exploitation, reverse engineering, and vulnerability research across multiple platforms — and set the direction the rest of his career would follow.

From there, Alec moved into direct technical roles supporting national security missions. As a security engineering team lead within the National Security Agency, he owned web application security and vulnerability management for a live intelligence program, applying Python-based automation and CI/CD security integration to measurably reduce the program's exposure within months. He went on to serve in a security engineering role with Riverside Research Institute, supporting the U.S. Air Force, where he helped stand up enterprise-wide DevSecOps standards — static analysis, software composition analysis, and secrets scanning integrated directly into delivery pipelines — for Department of Defense engineering organizations that had none, and was selected as one of a small number of enterprise Software Assurance approval authorities for the Department of the Air Force.

The deepest chapter of that federal career was spent as a reverse engineer and vulnerability researcher supporting the Federal Bureau of Investigation, under an active Top Secret/SCI clearance with Counter-Intelligence polygraph. Over several years, that work meant taking apart real, production iOS, Android, and macOS applications under strict chain-of-custody and operational security requirements — performing reverse engineering, developing exploits, and conducting adversarial testing that supported federal law enforcement investigations. It also meant building tooling that didn't exist off the shelf: custom capabilities in Python, C/C++, and JavaScript for cryptographic analysis, dynamic instrumentation, and automated vulnerability identification, built because commercial tools stopped short of what the work required. As AI-integrated systems became part of the threat landscape, that same research discipline extended into assessing prompt injection, adversarial data manipulation, and agentic pipeline vulnerabilities in production AI systems — using frameworks including the OWASP LLM Top 10 and NIST's AI Risk Management Framework — with findings delivered directly to senior federal leadership.

What runs through all of it — the reverse engineering, the vulnerability research, the mobile security work — is the same instinct: don't take a system's behavior on faith. Read the binary. Instrument the runtime. Confirm it directly. That instinct, applied for years against real adversarial conditions, is what eventually led to Strata.



Strata Security exists because of a gap Alec saw from the inside, from both directions at once. Serious application security tooling has always been built and priced for large organizations with dedicated security budgets — out of reach for the smaller teams and independent developers who need it just as much. At the same time, the kind of security work that actually matters — reverse engineering an undocumented binary, running down a vulnerability in a mobile app, hardening a system that has to survive contact with a real adversary — takes direct engineering depth that no automated scan can substitute for. Strata was built to close both gaps with one practice: an engineering-first company that builds real, working software, and applies that same rigor directly to the federal and high-assurance programs that need it.

Alec designed, built, and has operated Strata as a solo founder — architecting a production multi-tenant SaaS platform end to end, including a mobile application security engine built on the same reverse-engineering discipline behind his federal work, the cloud infrastructure the platform runs on, and the production hardening that keeps it operating safely in front of real users. Notably, Strata was built while Alec was still actively engaged in federal contract work — engineered alongside a full-time federal caseload before recently becoming his full-time focus. That is a deliberate discipline, not a limitation: operating production software, and living with the consequences of its design decisions in front of real users rather than just describing them in a report, is what keeps the engineering judgment behind Strata's federal work honest.

Alec's approach to leadership was shaped by the same environments that shaped his technical judgment: leading security engineering teams under real operational pressure, mentoring junior engineers into reverse engineering and offensive research capability, and — in one case — being handed a failing intelligence program and given the job of finding out why, then fixing it. That experience produced a consistent leadership approach: diagnose before you act, be direct about what's actually wrong, and measure success by whether the system works, not by how the report reads. Alec leads the way he was led best — expecting direct ownership of outcomes, not deference to hierarchy for its own sake.

His engineering philosophy follows the same throughline. Security is a design constraint, not a compliance step bolted on at the end. A finding without a working fix is unfinished work. And nothing about a system's behavior is assumed — it is confirmed directly, against the artifact itself, the same way a reverse engineer confirms what a binary actually does rather than what its documentation claims.

Alec holds a **B.S. in Software Development & Security** and an **M.S. in Digital Forensics & Cyber Investigations**, both from the University of Maryland Global Campus, and is currently pursuing an **MBA in IT Management** alongside the **CISSP** certification — formal study layered onto more than a decade of applied practice, not a substitute for it.

Looking forward, Alec's focus is building Strata into the kind of company its own federal and commercial customers can rely on for the long term: a Commercial platform that keeps closing the affordability and depth gap for teams that have never had access to practitioner-grade security tooling, and a Federal Security Services practice built on the same direct, engineer-led model that defined his own career — engineers who scope the work and do the work, with no layer in between. Both sides of that mission are still run by the same person who has spent more than a decade finding out, directly, how software actually fails — and building the discipline to make sure it doesn't.