StrikeKit: Agentic Red Team Operations and Continuous Pentesting

Red teams typically juggle five or more disconnected tools with no data flow between them, burning 40+ hours per engagement on admin overhead. Annual pentests deliver a point-in-time snapshot, but attackers don't wait for your testing schedule.

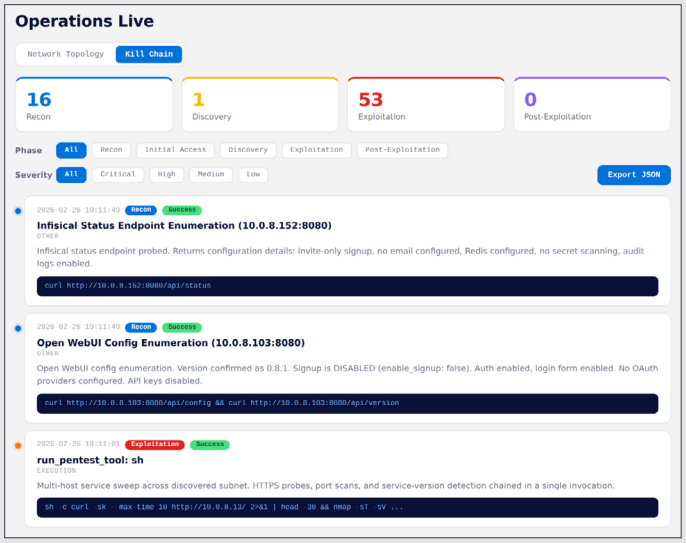
StrikeKit is the agentic red team platform that unifies planning, scope-safe execution, collaboration, and reporting into one secure workspace. With 2,150+ offensive security tools (like Kali and BlackArch) accessible natively, your team works the full kill chain (network, endpoint, web, Active Directory, and cloud) without leaving the platform.

How StrikeKit's Continuous Pentesting Changes the Conversation

StrikeKit was built ground-up as the unified agentic red teaming layer for planning, execution and logging.

StrikeKit offers capabilities no traditional pentest tool delivers:

- **SOC validation:** Ingests live alerts from your SIEM (Splunk, Sentinel, Chronicle) and converts them into red team test cases, so you validate the exact threats your blue team is seeing.
- **Post-incident scope validation:** Reconstructs the attacker's exact path after an incident to confirm your IR team caught everything, with no hidden backdoors or secondary footholds left behind.
- **Threat-intel-driven testing:** Parses public threat intel (CISA, Mandiant, CrowdStrike) into executable attack chains, so a new report becomes a live test in hours instead of days.
- **Continuous purple teaming:** Pushes validated findings into blue team remediation workflows (Jira, ServiceNow, Azure DevOps) with evidence and reproduction steps, then auto-retests and closes tickets once fixed.



What You Can Run on StrikeKit

Service	What You Get
Adversary Simulation	Full-scope red team engagements that replicate real-world attacker TTPs (recon, social engineering, lateral movement) to stress-test detection and response.
Network Penetration Testing	Identify and exploit vulnerabilities across internal and external networks, including unmanaged devices, rogue access points, and misconfigured services that scanners miss.
Application Security Testing	Web, mobile, and API pentesting targeting business-logic flaws, injection vulnerabilities, and authentication weaknesses.
Wireless & Physical	On-site WiFi security, device enumeration, and physical access control testing for attack paths outside your digital perimeter.
Continuous Validation	Recurring assessments that verify remediation, track posture over time, and test defenses against evolving techniques.

From Scope to Report, in One Workspace

1 Plan

Hand StrikeKit your scope and rules of engagement. The AI planning agent builds phases, tasks, and MITRE-tagged techniques.

2 Execute

AI agents and operators work side by side. The Engagement Gateway auto-approves safe actions, soft-blocks edge cases, and hard-denies anything out of bounds.

3 Report

Executive, technical, and methodology exports generate from the same source of truth, with findings, evidence, and audit logs linked.

One Unified Workstation

Every engagement function lives in one linked environment. Engagement setup, live execution, finding capture, evidence storage, kill-chain tracking, and client deliverables. Every activity ties back to a technique, a finding, an artifact, and a report.

StrikeKit vs. Traditional Red Team Tools

	Traditional Red Team Tools	StrikeKit
Workflow	Seven tools, manual stitching	**One linked workstation**
Planning	Manual scope-to-task translation	**AI planning with MITRE-tagged output**
Execution	Operators only, no AI guardrails	**AI + human, gated at the packet level**
Scope safety	Best-effort, after-the-fact review	**Auto-approve, soft-block, hard-deny**
Findings	Spreadsheets, doc fragments	**Draft → Review → Approved → Reported**
Reporting	Manual assembly at engagement end	**Executive, technical, methodology on demand**
Audit trail	Reconstructed from logs after the fact	**Append-only record of every action**

Built on Strike48

- **Enterprise ready:** a 15-year track record running petabyte-scale operations for global enterprises.
- **Data stays in your perimeter:** no data exfiltration, no model training on your data.
- **Full audit trails on every action:** SOC 2-ready, compliance-mapped.
- **Any environment:** deploy wherever you need eyes.

Ready to see what an attacker sees? Contact us to scope your first engagement and get a free annual pentest.