



External Penetration Testing

Sprocket Security | Continuous Offensive Security Platform

Test your perimeter the way real attackers do - continuously and comprehensively.

60%

of breaches start externally.
IBM Cost of a Data Breach, 2023

Traditional penetration tests give you a snapshot of your perimeter on one day of the year. Attackers don't work on your schedule. Sprocket Security's External Penetration Testing combines expert-driven manual testing with continuous attack surface monitoring so you know about exposures when they appear, not months later.

🔧 > SCOPE COVERED

Domains & Subdomains

Web Servers

APIs

Email Infrastructure

Cloud Services

VPN & Remote Access

Firewalls & Perimeter Controls

Credential Exposure

Key Capabilities

Reconnaissance & Asset Discovery

Sprocket enumerates all hosts, subdomains, and services associated with your apex domains and IP ranges using continuously refined OSINT, DNS analysis, and Attack Surface Management techniques. You can define your own scope or rely on Sprocket to autonomously discover company assets ensuring nothing is left untested.

Attack & Exploitation

Testers simulate real adversaries attempting to exploit public-facing vulnerabilities, brute-force authentication, bypass perimeter controls, and access sensitive data. Every technique reflects current real-world TTPs — not last year's playbook.

Continuous Monitoring & Retesting

After the initial engagement, Sprocket's ASM engine monitors for changes to DNS records, open ports, services, and newly discovered assets triggering expert human retesting whenever your perimeter evolves. Changes in your environment no longer go unverified.

Why It Matters



Business Risk

Internet-facing vulnerabilities are the most common initial access vector. Unpatched services, misconfigured cloud resources, subdomain takeovers, and forgotten assets can expose your entire organization to opportunistic and targeted attackers.



Compliance Driver

PCI DSS v4, SOC 2 Type II, HIPAA, ISO 27001, and CMMC all require regular external penetration testing. Sprocket's findings map directly to these frameworks for audit-ready reporting delivered on demand.



Operational Value

Findings are delivered in real time via the Sprocket Portal with role-based reporting for both security teams and leadership enabling faster, aligned remediation without waiting weeks for a static PDF.

ROI & Outcomes



Findings validated by human tester

100%



Alert on critical findings discovered

< 24 hours



Retesting included

Unlimited



Compliance-ready reporting

On demand via Sprocket Portal

Why Sprocket Security

- **OSCP & CISSP-certified consultants** with real-world attacker experience on every engagement
- **Continuous ASM engine** monitors your external footprint between engagements — no blind spots
- **Every finding includes** a full proof-of-concept, remediation steps, and attack narrative
- **Sprocket Portal** delivers live, role-based dashboards so your team always has current visibility
- **Unlimited retesting:** verify your fixes actually work without scheduling a new engagement

⚙️ Sprocket Security	Legacy / Point-in-Time
Continuous, always-on testing	Annual or quarterly testing
Live portal with real-time findings	Static PDF delivered weeks later
Monitoring & retesting continues year-round	Testing stops at engagement end
Proactive & security-driven	Reactive & compliance-driven
Subscription model with scalable scope	High cost, limited coverage

"A traditional external pen test is a single snapshot in time. Sprocket Security offers that testing on a continuous basis, so we always have an up-to-date view."

— IT Lead, Services Industry

