



Internal Penetration Testing

Sprocket Security | Continuous Offensive Security Platform

Simulate insider threats and post-breach attacker behavior across your entire internal environment.

30%

of security incidents involve insiders.

Verizon Data Breach Investigations Report, 2023

Once an attacker is inside your network - whether through a phishing email, a compromised credential, or a malicious insider - the question is no longer if they can get in, but how far they can go. Sprocket's Internal Penetration Testing answers that question before a real attacker does.

⚙️ > SCOPE COVERED

Active Directory

Lateral Movement

Privilege Escalation

File Shares

Credential Harvesting

Network Segmentation

ADCS / PKI

Workstations & Servers

Key Capabilities

Assumed-Breach Simulation via Dropbox

Sprocket deploys a preconfigured physical or virtual dropbox inside your network to serve as the attacker's launch point replicating exactly how a real threat actor operates after gaining initial access. All testing runs remotely over a secure channel, with no costly on-site visits required.

Advanced Credential Attacks & Privilege Escalation

Testers perform sophisticated Active Directory attacks including Kerberoasting, ADCS certificate template abuse (ESC1-ESC15), pass-the-hash, NTLM relay, DHCPv6 poisoning, and ZeroLogon - techniques that scanners will never catch and that lead directly to domain compromise.

Post-Exploitation & Attack Path Documentation

Every attack path is fully documented in a step-by-step narrative. Exploited paths are converted into structured Findings inside the Sprocket Portal - tracked through remediation with unlimited retesting to confirm vulnerabilities are genuinely resolved.

Why It Matters



Business Risk

Lateral movement and privilege escalation can turn a single compromised workstation into full domain administrator access. Without internal testing, you don't know your blast radius until it's too late.



Compliance Driver

PCI DSS v4 (Requirement 11.4), SOC 2 Type II, HIPAA, and CMMC require assessment of internal systems, network segmentation controls, and credential security. Sprocket's reports satisfy auditor requirements out of the box.



Operational Value

Receive a clear picture of exactly how an attacker would move through your environment, from initial foothold to crown jewels, with prioritized, actionable remediation guidance at every step.

ROI & Outcomes

 Findings include full attack narrative 100%	 Deployment method Via Dropbox	 On-site visits required None	 Retesting on remediated findings Unlimited
---	---	--	--

Why Sprocket Security

- **Dropbox-based deployment:** remote testing that mirrors real attacker behavior, no travel costs
- **Advanced AD techniques:** Kerberoasting, ADCS abuse, NTLM relay, DHCPv6 poisoning, and more
- **Continuous model:** internal assets are re-tested as your environment changes throughout the year
- **Full attack chain documentation** from initial foothold all the way to domain compromise
- **Unlimited retesting:** confirm your remediations actually close the attack paths identified

 Sprocket Security

Legacy / Point-in-Time

Continuous testing as your environment evolves	Annual or quarterly testing
Remote dropbox - no travel required	Requires on-site tester visits
Live portal with real-time findings	Static PDF delivered weeks later
Retesting continues as environment changes	Testing stops at engagement end
Proactive & security-driven	Reactive & compliance-driven

"With Sprocket it feels like it's an extension of my team. Things we only see every so often, they see twice a week. It reduces our time to remediate."

— Security Lead, Mid-Market Manufacturing

