Searchlight Cyber

Searchlight platform

Preemptive Threat Exposure Management

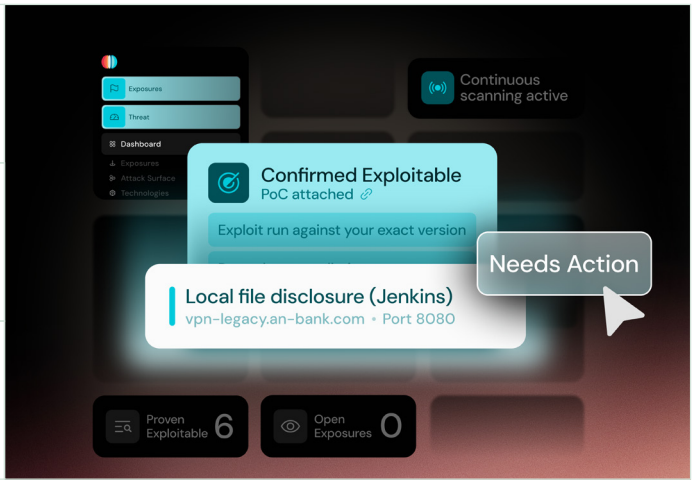
Searchlight unites exposure management and attacker intelligence in a single platform, comprised of two complementary capabilities. Searchlight Exposure finds what's exploitable on your attack surface and validates it by running the real exploit. Searchlight Threat shows who's targeting you, observed at the source. Where a confirmed exposure meets active attacker interest, it rises to the top and goes straight to remediation. That's preemptive security: acting before attackers move.

> The platform has well and truly paid for itself in what it's found and how it's helped us respond to incidents.
>
> Information Security Manager at an Insurance company

See both sides of the threat: Your exposure and your adversary in one view, so you prioritize based on real risk rather than theoretical severity.

Act before the CVE exists: Searchlight finds zero-days in the software you run and protects you before public disclosure and the patching scramble begins.

Rapidly remediate: Every finding is validated by exploitation, with proof of concept attached, so confirmed exposures can move straight to remediation without lengthy triage.



One preemptive platform. Two products. Three capabilities.

Searchlight Exposure

Exposure Management

- Continuous validated scanning across your entire external surface
- Alerts on verified exposures, with a proof of concept for every finding
- Zero-day alerts from Searchlight Labs, in-product

Searchlight Threat

Monitor

- Continuous clear, deep, and dark web monitoring
- Prioritized alerts matched to your organization, with MITRE ATT&CK mapping
- Pre-attack signals: Leaked credentials, exploit development, **and** dark web traffic **on your network.**

Searchlight Threat

Investigate

- Identify, preserve, and share dark web evidence
- Securely access Tor and I2P through a browser-based virtual machine
- Profile actors, **groups**, and monitor keywords across 15+ years of **archived data.**

From reactive to preemptive.

Most security runs on the same clock as the attacker: find, patch, respond after disclosure. Searchlight moves the whole timeline earlier, so you close exposures before they're weaponized.

Key Features

EXPOSURE VISIBILITY	ATTACKER REALITY	PREEMPTIVE ACTION
Continuous validated discovery The only ASM that scans your entire external surface every hour and confirms each exposure by running the real exploit, not matching CVEs.	**Intelligence from the source** Real-world adversary activity across the clear, deep, and dark web, matched to your organization and mapped to MITRE ATT&CK. Know what attackers will target next.	**Protection before disclosure** Searchlight's research team finds zero-days in the enterprise software you run and protects you before the CVE exists.
Signal, not noise Only alerts you to what is exploitable, so your team can act with confidence on the threats that matter, not the noise.	**Pre-attack early warning** Leaked credentials, exploit development, and targeting activity, spotted in their earliest stages, before the attack lands.	**Straight to remediation** Validated, prioritized findings route into the SIEM, SOAR, and ticketing tools your team already uses, with the mitigation attached.

96%

faster discovery and validation than other vendors

8 hours

mean time to exploit in 2026, down from 56 days in 2024 and 2.3 years in 2018.

32-40 hours

saved per month on threat investigation

QANTAS · Linktree · Canva · IMMUTABLE · afterpay · YUGALABS · TWILIO segment · OAKWOOD BANK · utmb Health · nccgroup · Vitality · CHECK POINT

See the platform in action. Learn how at slcyber.io/platform

Searchlight Cyber

Contact Us

sales@slcyber.io · slcyber.io

UK Headquarters

Suite 63, Pure Offices, 1 Port Way
Port Solent, Portsmouth PO6 4TY
+44 (0)345 862 2925

USA Headquarters

44 Merrimac Street
Newburyport, MA 01950
+1 (202) 684 7516