Christian Schneider
Security Architect, Hacker, Trainer

SERVICE INFO
Blackbox · Remote · Two-phase

ATTACK SURFACE MAPPING

Know what attackers see when they look at *your organization*.

You probably know what your company runs — but do you know what's actually visible from the outside? Attack Surface Mapping answers exactly that. I look at your organization through an attacker's lens: what can be found, what's exposed, and what shouldn't be. The goal is simple: identify everything reachable before someone with bad intent does.

christian-schneider.net/service/attack-surface-mapping ↗

HOW IT RUNS

1 Reconnaissance & scanning
Professional OSINT and dorking across public search engines and repositories — the same techniques a real attacker would use, minus the malicious intent. In-scope network segments are then analyzed and scanned: host detection, service fingerprinting, and component/version matching against CVE and exploit databases for direct vulnerability intelligence.

2 Deeper detail checks
A natural pause for a sync call: you see the first findings and we decide together where, and how deep, phase two should go. You stay in control of which discovered services get probed further, keeping side-effects on sensitive systems off the table.

3 Reporting & debrief
Compact overviews with statistics for trend-tracking against earlier mappings, plus detail reports per host, service and vulnerability category, directly usable for remediation. Followed by a remote debrief with the teams responsible for fixing.

Often surprises companies in phase one: forgotten staging environments, legacy subdomains nobody decommissioned, services running outdated software no one remembered. Exactly what attackers look for first.

FROM THE ATTACKER'S SEAT

Blackbox by default — little to no prior knowledge required. The two-phase approach also keeps targets aligned with your pentest scope, so probing stays clear of systems you'd rather leave untouched.

PREREQUISITES

- → In-scope IP ranges of your organization
- → Optional: domain names to include for closer review

WHAT YOU RECEIVE

- → Executive overview & trend-ready statistics
- → Detail reports by host, service & vuln category
- → CVE-mapped vulnerability intelligence per service
- → Mid-engagement sync to scope phase two together
- → Remote debrief with remediation owners

BONUS FINDING

This service also surfaces **phishing domains** impersonating your brand. I actively check for common name variations (typos, swapped TLDs, lookalike characters) ensuring squatters and active phishing infrastructure are identified alongside your legitimate assets.

Let's map your exposed surface.
Most attack-surface projects are tightly tailored to your organization. Every engagement starts with a free scoping call to align IP ranges, domains and depth.

GET IN TOUCH
mail@christian-schneider.net
christian-schneider.net