

Pentesting and Red-Teaming

Nineteen offensive services, from an external penetration test to an intelligence-led red team, each showing what an adversary could reach and whether your defenders would stop them.

The question it answers

Two questions decide which service fits: what can an attacker exploit, and would you notice them doing it. The services are organized by attack surface and engagement depth, the way a real adversary works: probe an asset for a weakness, chain weaknesses into a path, then pursue an objective.

A penetration test shows what can be exploited. Adversary simulation shows whether people, processes and technology detect and respond. The scope buys the depth the question needs.

How every test is run

Approved scope only

Only assets you explicitly approve are tested. Red team, threat-led and physical work run under a letter of authorization, and destructive actions and denial of service stay out unless approved.

Impact proven, damage avoided

Vulnerabilities are confirmed by controlled exploitation. Data exfiltration in a red team is simulated, and operations pause if a system shows instability.

Findings you can act on

Every finding carries an impact assessment and step-by-step remediation guidance. Identity and adversary work adds detection guidance mapped to MITRE ATT&CK.

Retest of critical findings

One retest within a year on the external, internal, cloud, web, mobile, API and container tests. A full retest of every finding is available as an add-on.

AT A GLANCE

SERVICES

19 in eight categories

DEPTH

Scan to threat-led red team

DURATION

2 days to 3 months

STANDARDS

OWASP, CIS, ATT&CK, TIBER-EU

BUNDLES

Six packages, or a custom one

DELIVERABLES

Report, summary, debrief

WHO THIS IS FOR

- Cloud-first organizations worried about initial access and lateral movement.
- Product teams shipping web, mobile and API applications.
- Security-mature teams that want to know whether an attacker would be stopped.
- Regulated organizations needing independent test evidence.

The services, and what each one is worth

SERVICE	WHAT IT DOES	BUSINESS VALUE
01 / INFRASTRUCTURE TESTING		
External penetration test 1 to 6 weeks	Adversary-style testing of the Internet-facing perimeter, from reconnaissance to controlled exploitation.	Shows how an external attacker could breach you under real conditions, and supplies perimeter evidence most frameworks require.
Internal infrastructure penetration test 1 to 6 weeks	Testing from inside the network, unauthenticated or as a standard user, through escalation and lateral movement.	Shows what an attacker achieves after an initial compromise, and the paths that lead to control of Active Directory.
Cloud penetration test 1 to 5 weeks	Configuration review and active testing of AWS, Azure and Google Cloud, centered on identity and access management.	Finds the identity and management-plane weaknesses network tests cannot see, mapped to provider best practice.
Active Directory and identity security assessment 1 to 5 weeks	Attack-path mapping and configuration review of Active Directory, Entra ID and the trust between them.	Reveals the routes from an ordinary user to Tier 0, and tells the SOC which identity attacks to detect, mapped to MITRE ATT&CK.
02 / APPLICATION AND API TESTING		
Web application penetration test 1 to 5 weeks	Authenticated and unauthenticated testing of web applications, their APIs and supporting cloud, sized per application.	Finds injection, access-control and business-logic flaws that scanners miss, in the layer where most modern breaches start.
Mobile application penetration test 1 to 5 weeks	iOS and Android testing to the OWASP MASTG: static and runtime analysis on instrumented devices, plus backend APIs.	Tests the app as it runs on a device the attacker controls, and confirms data on the device and in transit is protected.
API security testing 1 to 4 weeks	REST and GraphQL testing against the OWASP API Security Top 10, with depth on authorization across roles.	Targets the authorization and data-exposure flaws that dominate API breaches, and turns findings into developer backlog items.
Security code review 1 to 4+ weeks	Manual and automated source review for injection, hardcoded secrets, weak cryptography and access-control errors.	Finds weaknesses before code reaches production, with file and line references and fixes developers can apply.
03 / WIRELESS AND NETWORK TESTING		
Wireless security assessment 1 to 4 weeks	Onsite testing of wireless encryption, rogue and evil-twin access points, and guest, corporate and operational segmentation.	Confirms whether an attacker outside the building could reach the network, and whether segmentation holds.
04 / CLOUD-NATIVE AND CONTAINER SECURITY		
Container and Kubernetes security assessment 1 to 5 weeks	Cluster review to the CIS Kubernetes Benchmark, image and supply-chain analysis, and escape testing where authorized.	Shows whether workloads are isolated from the host and each other, and where RBAC and network-policy gaps open the control plane.

SERVICE

WHAT IT DOES

BUSINESS VALUE

05 / HUMAN-FOCUSED TESTING

Phishing simulation campaigns

2 to 6 weeks

Safe email simulations tailored to your context, with no malware or harmful payloads.

Quantifies your phish-prone percentage through open, click, data-entry and reporting rates, and targets training.

Social engineering

1 to 4 weeks

Vishing, smishing, pretexting and, where in scope, physical intrusion under a signed letter of authorization.

Shows how staff, help desks and physical controls respond under pressure, beyond email behavior alone.

06 / ADVERSARY SIMULATION

Assumed-breach assessment

1 to 4 weeks

Starts from a standard account or planted foothold and pursues agreed objectives through escalation and lateral movement.

Delivers much of a red team's value in less time, and shows whether segmentation and tiering would slow an attacker.

Purple team exercise

1 to 4 weeks

Offensive specialists run ATT&CK-mapped techniques beside your defenders, confirm telemetry and alerts, and tune on the spot.

Gaps are closed and validated during the exercise, leaving a detection coverage matrix and new or tuned detections.

Red team / adversary emulation

4 weeks to 3 months

A covert, goal-driven simulation of a stealthy advanced persistent threat pursuing agreed objectives without detection.

Tests whether people, processes and technology detect and stop a real attacker, with indicators of compromise for tuning.

Threat-led red teaming

6 to 10 weeks

Intelligence-driven emulation of the actors most likely to target you, against live production under a control group (TIBER-EU, CBEST).

Regulator-grade evidence and a board-ready account of resilience against the threats you actually face.

07 / SUPPLY CHAIN AND THIRD PARTY

Supply-chain and third-party security testing

1 to 5 weeks

Mapping and testing of vendors, software dependencies, integrations and the trust relationships between them.

Makes inherited risk visible, with findings you can act on and share with your suppliers.

08 / CONTINUOUS ASSESSMENT

Vulnerability scanning

2 days to 2 weeks

Automated discovery of known weaknesses and misconfigurations across external, internal and cloud assets.

A fast, repeatable health check with false positives removed and findings ranked by risk and business context.

Vulnerability management as a service

2 to 4 weeks onboarding

Recurring scans, expert triage, remediation tracking against agreed service levels and trend reporting.

Drives exposure down over time and keeps the continuous-assessment record auditors and regulators increasingly expect.

Request an engagement

Tell us the assets in scope, the starting position and the objective, and we will tell you which service and depth answers the question.

contact@alexsta-cybersecurity.com

+41 76 76 44884

alexsta-cybersecurity.com