

OFFENSIVE SECURITY PROPOSAL

Red Teaming as a Service

KEY FEATURES

Professional proposal for offensive security testing

Core Workflow Overview



ITERATIVE • RISK-DRIVEN • COMPREHENSIVE

Reconnaissance

- Asset and attack-surface discovery
- Domain and subdomain enumeration
- Technology identification — software, versions, services
- Open Source Intelligence (OSINT) gathering



Vulnerability Assessment & Initial Access

VULNERABILITY ASSESSMENT

- Identify weaknesses and misconfigurations
- Web, API, and network vulnerability scanning
- Risk prioritization for remediation focus

INITIAL ACCESS TESTING

- Validate exposed attack paths
- Authentication and authorization testing
- Controlled phishing simulations
- External attack-surface testing

Network & Infrastructure Testing

01

**Internal & external
network assessments**

02

**Network segmentation
testing**

03

**Firewall & security
control validation**

04

**Privilege escalation
& lateral movement**

Web & API Testing

- Authentication mechanism testing
- Access control and authorization validation
- Input validation to prevent injection attacks
- Session management and business logic testing

```
POST /api/v2/session
{ token: ..... }

200  authorization: validate
403  privilege: denied

// test every trust boundary
```

Adversary Simulation & Social Engineering

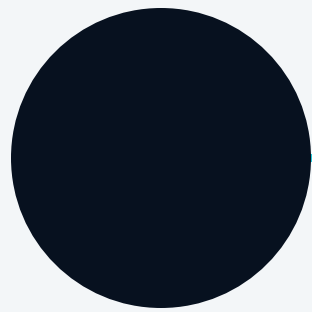
ADVERSARY SIMULATION

- Realistic attacker behavior emulation
- Detection and response capability testing
- Controlled lateral movement
- Persistence and defense evasion assessment

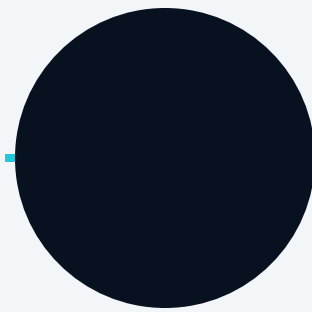
SOCIAL ENGINEERING

- Phishing simulations
- Security awareness testing
- Physical security assessment — where authorized
- Employee response evaluation

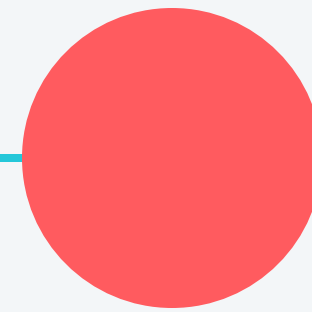
Cloud & Identity Testing



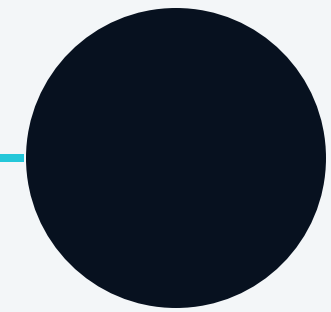
**Cloud configuration
assessment**



**IAM & security
policy testing**



**Privilege & access
path analysis**



**Identity security
validation**

Detection & Response Validation

SIEM + EDR

Alert validation

SOC

Detection testing

PATH

Attack tracking

TTR

Response time

Can your team see the attack — and respond before impact?

Reporting & Dashboard

- Executive summary for leadership
- Detailed technical findings for security teams
- Attack path visualization
- Risk ratings and remediation priorities
- Evidence collection and recommendations



Retesting



CONTINUOUS IMPROVEMENT, NOT A ONE-TIME CHECK