

# Red Teaming

Test how your people, processes and technology hold up against a real adversary

Most organisations have invested in firewalls, endpoint protection and a security operations centre. Few know whether those controls would stop a determined attacker who has weeks to work and needs only one way in. A penetration test checks a fixed scope for known weaknesses. It does not tell you how long an intruder could stay inside your network before anyone noticed.

A red team engagement answers that question. We emulate a real threat actor against objectives agreed with your leadership, such as reaching customer data, payment systems or domain admin, using the tactics, techniques and procedures attackers use in the wild.

You get a measured view of your detection and response, from the first phishing email to the final objective, with every action mapped to MITRE ATT&CK.

## OBJECTIVE-DRIVEN ADVERSARY EMULATION

Every engagement starts from agreed objectives, and the scope is the whole organisation: the external perimeter, your people, physical access where approved, and the internal network. We build the campaign around threat actors relevant to your sector and region, and choose initial access techniques the way they would, with tooling and infrastructure built for your engagement.

- |                            |                                   |                                     |
|----------------------------|-----------------------------------|-------------------------------------|
| ■ OSINT and reconnaissance | ■ Phishing and social engineering | ■ Initial access and C2             |
| ■ Active Directory attacks | ■ Privilege escalation            | ■ Lateral movement and exfiltration |

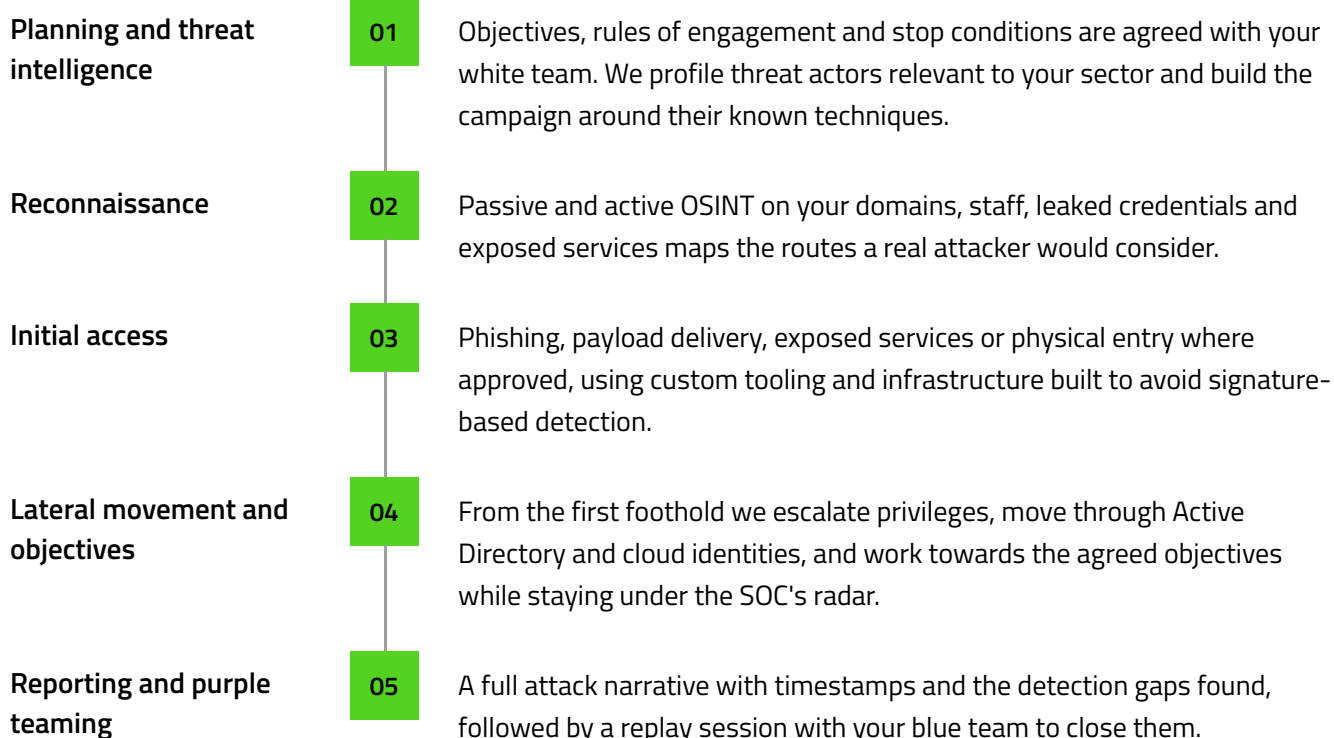
## MEASURING DETECTION AND RESPONSE

Stealth is part of the test. We record a timestamp for every action and compare it with what your SOC saw and when. Where an action went undetected, we name the log source or detection rule that would have caught it. Optional purple team sessions replay the attack chain with your blue team, so new detections can be built and verified on the spot.

All activity runs under signed rules of engagement, with a named white team contact on your side and agreed stop conditions for any risk to production systems.

## ASSESSMENT DETAILS AND METHODOLOGY

Our red team methodology follows the full attack lifecycle and maps every action to MITRE ATT&CK. Each engagement is planned with your white team, run under strict rules of engagement and documented action by action, so results can be reproduced and replayed with your defenders.



## The engagement includes

- Executive summary for leadership
- Detection and response gap analysis
- Prioritised remediation and detection steps
- Attack narrative mapped to MITRE ATT&CK
- Objectives achieved and data accessed
- Purple team debrief with your SOC

## ABOUT SENTRYARK

SentryArk is a team of security engineers and offensive security specialists. Our consultants hold OSCE, CRYPTO and CEH certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Our focus is offensive security that shows the real-world risk to your business.