BUYER'S GUIDE

Offensive Security

SAEPIO.CO.UK

SAEPIO

CREST PEN TEST

CYBER ESSENTIALS PLUS

Assured Service Provider

in association with National Cyber Security Centre

CHECK Penetration Testing
Cyber Advisor

TABLE OF

Contents

OFFENSIVE SECURITY

Understanding Your Needs and Key Considerations

This guide helps organisations select the right mix of offensive security services and technologies by defining their objectives, required coverage, operating model, assurance needs and evaluation criteria.

OFFENSIVE SECURITY

What is Offensive Security?

Offensive security proactively simulates real-world attack techniques to help organisations identify and validate weaknesses before adversaries exploit them. Unlike defensive controls such as endpoint detection and response and firewalls, offensive security activities assess how an attacker could gain initial access, escalate privileges, move laterally and affect critical business operations.

Offensive security is not about fixing every vulnerability; it is about determining which weaknesses are exploitable, how they could be chained and what business impact could result. It includes penetration testing, red teaming and increasingly automated validation platforms that continuously assess exposed assets, attack paths and security controls.

Most offensive security testing can be broken down into a standard sequence:

- **Reconnaissance:** gathering information about attack surfaces and mapping potential vulnerabilities.
- **Scanning:** automatically scanning systems to identify potential access points such as open ports, live hosts, weak credentials, and running services.
- **Vulnerability analysis:** validating identified weaknesses, removing false positives, assessing exploitability and determining whether individual issues can be combined into viable attack paths.
- **Exploitation:** targeting identified vulnerabilities to gain access, escalate privileges, access functionality and files, and execute attack goals such as stealing data.
- **Post-exploitation:** demonstrating the potential impact of a compromise while operating within agreed safety boundaries.
- **Remediation validation:** confirming that corrective actions close the identified attack path without introducing new risk.
- **Reporting:** documenting the vulnerabilities, assessing risk priorities and recommending mitigations based on the findings.

OFFENSIVE SECURITY

Why is Offensive Security important?

As organisational infrastructure becomes more complex, it is increasingly difficult to understand risk across cloud, on-premises, SaaS and identity environments. Vulnerabilities will always exist, and attackers often exploit chains of weaknesses rather than isolated issues. Organisations therefore need to validate that security controls work as intended, identify blind spots across the estate and prioritise remediation according to exploitability and business impact, rather than relying solely on the number or severity of CVEs and CVSS scores. Offensive security also gives leaders evidence that critical risks are understood and gives security teams clear, prioritised actions, reducing the likelihood and potential impact of a serious security incident

Since the advent of FrontierAI a new found focus on testing exploitability is vital due to the speed and scale of exposures being identified and weaponised. This is also driving the development of automated, AI-native testing platforms to address the machine-speed challenge of modern cyber security, without of course replacing the need for expert human-led assessment

OFFENSIVE SECURITY

Identifying Your Core Needs

Before comparing specific solutions or providers, define the problems you need to solve, the outcomes you expect and the constraints that will shape the programme.

- **Primary purpose:** Is the objective to meet a compliance or assurance requirement, identify exploitable attack paths, emulate relevant threat actors or validate controls such as endpoint detection and response, email security and identity protection? Define the required outcome before selecting the engagement type or platform.
- **Coverage:** Will testing be internal, external or both? Which environments are in scope, including cloud, identity, SaaS, on-premises systems, applications, APIs, endpoints, networks and third parties? Also define geographic, business-unit and data-residency constraints.
- **Security maturity:** At a minimum, organisations should understand their external attack surface, conduct baseline penetration testing and take prioritised action based on the findings. As maturity increases, testing should become more frequent and threat-informed, with adversary emulation and rigorous exercises focused on systems that are critical to business operations.
- **Ownership and policy:** Define who owns the programme, who accepts the risk of testing, who is responsible for remediation and how findings will be tracked to closure. Establish the testing frequency, rules of engagement, escalation paths, emergency stop procedures, approved testing windows and safeguards required to prevent unintended disruption.

- **Current capability:** Assess whether the existing team, processes and security stack can meet the requirements. Consider available skills, testing capacity, licences, integrations, data access and the ability to remediate and retest findings.
- **In house, outsourced or hybrid:** Determine whether the organisation has the skills, capacity, independence and specialist expertise to achieve its objectives internally. A hybrid model may combine internal ownership with external assurance, specialist testing or surge capacity.
- **Legal, privacy and authorisation:** Confirm written permission to test, data-handling requirements, privacy obligations, third-party approvals, evidence-retention periods and any restrictions imposed by cloud or SaaS providers. Agree on clear rules of engagement, including in-scope targets, prohibited techniques, testing windows, communications and emergency contacts.

OFFENSIVE SECURITY

Navigating the Offensive Security Landscape

Choosing the Right Approach for Your Organisation

Offensive security is a broad discipline, so buyers should distinguish between service engagements, managed programmes and technology platforms, then compare each option against the outcomes they need.

Penetration testing services

Attack surface management

Security control validation & threat-informed testing

Specialist testing based on specific threats, such as ransomware

Automated red teaming

Red teaming

Vulnerability assessments

Purple teaming (combining external support in the attack and defence phases of an exercise)

Breach and attack simulations

It is also important to balance tool-based activities that use AI and machine learning with human-led testing, which provides creative thinking, contextual judgement and real-world experience.

Additional categories may include web application and API security testing, mobile application testing, cloud and identity security assessments, social engineering, physical security testing, wireless testing, source-code review and secure configuration assessments. The appropriate mix should reflect the organisation's attack surface, critical services and threat model.

The market includes professional services, managed programmes and technology platforms. Buyers should first decide whether they need an independent point-in-time assessment, continuous validation, internal enablement or a blended approach, as these models differ significantly in scope, expertise, evidence and operational effort.

OFFENSIVE SECURITY

Comparison Criteria and Metrics

To compare offensive security services and platforms objectively, use a consistent set of criteria aligned to your objectives, environment, risk appetite and operating model.

- **Technical efficacy:** Evaluate the depth and breadth of testing, supported environments and techniques, ability to validate complete attack paths, false-positive management, evidence quality, safe exploitation controls and alignment to recognised methodologies. For automated platforms, assess coverage of relevant tactics and techniques, credentialed testing, customisation and the transparency of validation logic.
- **Commercial model:** What drives the price, such as asset count, application count, testing days, frequency, users or consumption? Assess annual cost, minimum commitments, overage charges, retesting fees, price predictability and termination terms.
- **Total cost of ownership:** Include implementation, onboarding, integration, internal administration, training, managed-service support, remediation effort, retesting, travel and any specialist consultancy required beyond the base price.
- **Delivery performance and service levels:** Compare mobilisation time, test completion time, critical-finding notification, report turnaround, retest turnaround and achievement against agreed service levels. For platforms, also assess scan or validation frequency, coverage, reliability and time to evidence.
- **Communication and customer service:** Assess contract governance, named points of contact, escalation routes, reporting cadence and available communication channels. Confirm compatibility with existing ticketing, SIEM, vulnerability management and governance workflows, including APIs and export formats.

- **Compliance and assurance:** Confirm whether the provider and individual testers hold relevant certifications or accreditations, such as CHECK and CREST, where required. Review testing methodology, professional indemnity and cyber insurance, data location, security certifications, personnel vetting and the suitability of evidence for regulatory or audit purposes.

- **Reporting and remediation support:** Assess executive and technical reporting, evidence quality, attack-path visualisation, business-impact context, prioritisation, remediation guidance and retesting. Confirm whether findings can be tracked to closure and whether reports can be tailored for technical teams, risk owners, auditors and executives.

OFFENSIVE SECURITY

Next Steps

Choosing the right offensive security approach is important, and often the 'right' outcome is a blend of processes and tooling to achieve the right blend of speed and scale, alongside the context-aware expertise of human-led approaches. Saepio helps organisations move from initial requirements to a confident, evidence-based selection through the following five-step process.

Step 1. Define your requirements

We work with you to understand your environment, challenges and goals, ensuring the engagement delivers the outcomes you need.

Step 2. Build a shortlist of providers

Using our extensive market knowledge and vendor-neutral approach, we narrow the offensive security landscape to providers aligned with your needs, highlighting the strengths and trade-offs of each option in the context of your environment.

Step 3. Use the Saepio Offensive Security Evaluation Matrix

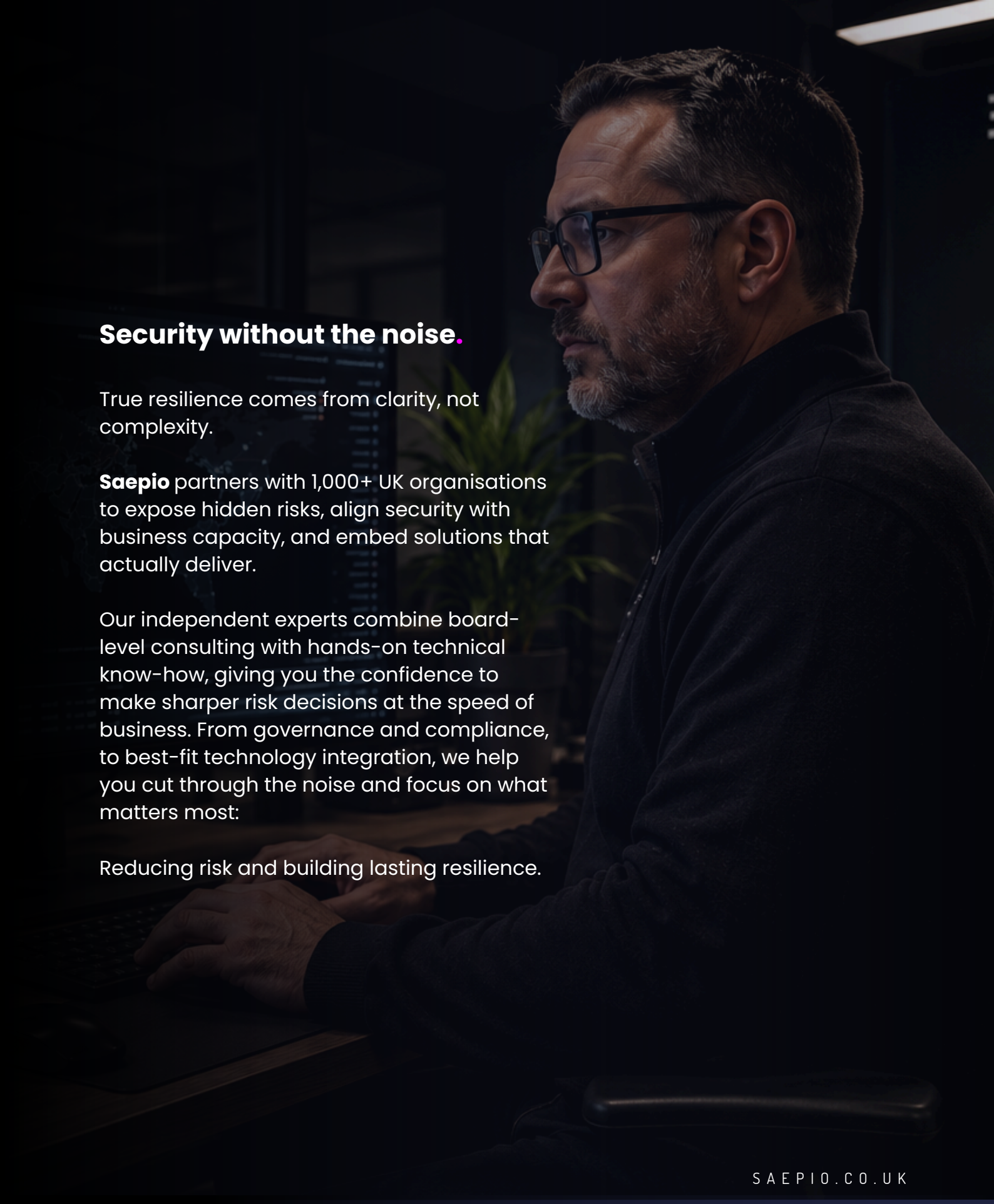
We provide a structured framework for comparing providers across technical, operational, assurance and commercial dimensions, with weightings and scores aligned to your priorities.

Step 4. Facilitate introductions and demonstrations

We coordinate technical deep dives, demonstrations and proof-of-concept engagements so you can assess how each solution or service would perform in your environment.

Step 5. Support procurement and onboarding

Once a solution or provider is selected, we assist with contract negotiation, commercial alignment, implementation planning, governance and onboarding, ensuring the delivery plan is realistic and aligned with internal timelines.



Security without the noise.

True resilience comes from clarity, not complexity.

Saepio partners with 1,000+ UK organisations to expose hidden risks, align security with business capacity, and embed solutions that actually deliver.

Our independent experts combine board-level consulting with hands-on technical know-how, giving you the confidence to make sharper risk decisions at the speed of business. From governance and compliance, to best-fit technology integration, we help you cut through the noise and focus on what matters most:

Reducing risk and building lasting resilience.

SAEPIO.CO.UK

SAEPIO

CREST PEN TEST

CYBER ESSENTIALS PLUS

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing
Cyber Advisor