eSENTIRE

SOLUTION BRIEF

Technical Testing

Tactical and strategic assessments of your prevention, detection and response capabilities

A DIFFERENTIATED APPROACH

With thousands of security vendors in the market, how can you ensure your defenses are being tested against the latest threats vs. pre-canned engagements designed for mass distribution that only scratch the surface level? At eSentire, we treat every simulated threat exercise as a challenge to test the efficacy of your security defenses using the latest techniques designed to evade security controls. Our testing experts leverage decades of experience, threat intelligence from over 200+ sources and evasive measures seen in our Managed Detection and Response engagements, that result from hunting and identifying threats that other technologies miss.

Whether testing prevention, detection or response capabilities for your applications, networks, employees or security team, our portfolio of tactical and strategic assessment ensures you can identify areas of greatest risk, both broadly and focused, and determine how to strengthen your security posture against the latest cyber threats.

TECHNICAL TESTING SERVICES

External Vulnerability Assessment

Internal Vulnerability Assessment

Penetration Testing

Phishing Campaigns

Wireless Penetration Testing

Web Application Testing

Mobile Penetration Testing

Red Team

SOLUTION AT A GLANCE

	Vulnerability Assessment (Internal or External)	Phishing	Web App Test	Wireless Pen Test	Penetration Test (Internal or External)	Red Team
Stealth	Low	Low	Low	Low	Low	High
Scoping	Reports on all systems and vulnerabilities found on in-scope systems	Reports on all target users	Reports on all web applications and vulnerabilities found on in-scope web applications	Threat modeling (from a wireless perspective)	Threat modeling (includes suitable testing scenario)	Customized engagement goals
Target Users		•				•
Objective	Broad scan	Test users	Goal seeking	Goal seeking	Goal seeking	Goal seeking/ Test response
Can be performed on premise				•	•	•
Can be performed remotely	•	•	•		•	•
Vulnerability Scanning	•		•		• (as necessary)	• (as necessary)
Detailed Report	•	•	•	•	•	•
Post-exploitation			•		•	•
Recon on in-scope targets					•	•
Manual testing to simulate attacker methods and techniques			•	•	•	•
Review compromised system for any data that allows further compromise					•	•
Port scanning	•				•	•
Exploitation			•	•	•	•
Escalation			•	•	•	•
Pivoting					•	•
Continue post-exploitation as necessary					•	•
Review compromised or target systems for business-critical data			•		•	•
Report narrative			•	•	•	•
Attack planning and preparation					•	•
Crack "decrypt" any obtained passwords				•	•	•
Phishing		•				•
Vishing						•
OSINT to gather additional targets					•	•
Perimeter breach: Wireless (as necessary)						• (as necessary)
Perimeter breach: Physical testing and drop box placement (as necessary)						• (as necessary)

SERVICES

HEALTH CHECK

A point-in-time exercise utilizing a scanning tool that deliberately probes a network or system to discover its weaknesses. Results are analyzed by security experts and prioritized by severity with remediation guidance.

- Catches low-hanging fruit
- Validates your patching/hardening program
- Establishes a security baseline
- Identifies known, surface-level security issues and misconfigurations

PENETRATION TEST (INTERNAL AND EXTERNAL)

Simulates the actions of an external and/or internal attacker. Using the latest tactics, techniques and procedures, the penetration tester attempts to infiltrate and exploit systems and gain access to data. Exercise results in identification of systematic weaknesses with areas of remediation ranked by criticality.

- Tests prevention and detection capabilities
- Simulates threats including pivoting and post exploitation
- Validates internal and/or external security controls
- Identifies areas of greatest risk and remediation
- Satisfies compliance needs, including HIPAA, SEC, NYCRR, PCI 3.x.

PHISHING

Tests end users through customized simulated phishing engagements. Users that present potential risks via exploitation of the human element are identified and remediation guidance is provided to implement into security awareness programs.

- Validates security awareness training program effectiveness
- Identifies employees of greatest risk
- Satisfies regulatory requirements
- Prioritizes areas of remediation

WIRELESS PENETRATION TEST

Tests if an unauthorized user is able to sniff or connect to wireless access points and retrieve information. Exercise results in confirmation of and/or identification of potential areas of risk in both physical and virtual security controls and recommendations for remediation by severity.

- Determines risk related to potential access to wireless networks
- Identifies insecure wireless encryption standards and passphrases
- Identifies presence of unknown access points
- Prioritizes hardening and remediation efforts

WEB APPLICATION PENETRATION TEST

Tests security of software/libraries on which the application runs. Exercise results in identification of vulnerabilities such as injections, broken authentication, broken authorization and improper error handling and recommendations for remediation by severity.

- Identifies security issues resulting from insecure development practices
- Tests against injection vulnerabilities (e.g. SQL, Cross-site, etc.)
- Measures security controls against OWASP Top 10
- Prioritizes remediation of most critical vulnerabilities

MOBILE PENETRATION TEST

Tests mobile application for input validation vulnerabilities, sensitive data in code and memory/ local storage, communications issues such as Bluetooth or NFC, platform-specific vulnerabilities, issues around jailbroken devices, etc. Exercise results in identification of risk and recommendations for remediation by severity.

- Identifies security issues resulting from insecure development practices
- Measures security controls against OWASP Mobile Standard
- Prioritizes remediation of most critical vulnerabilities

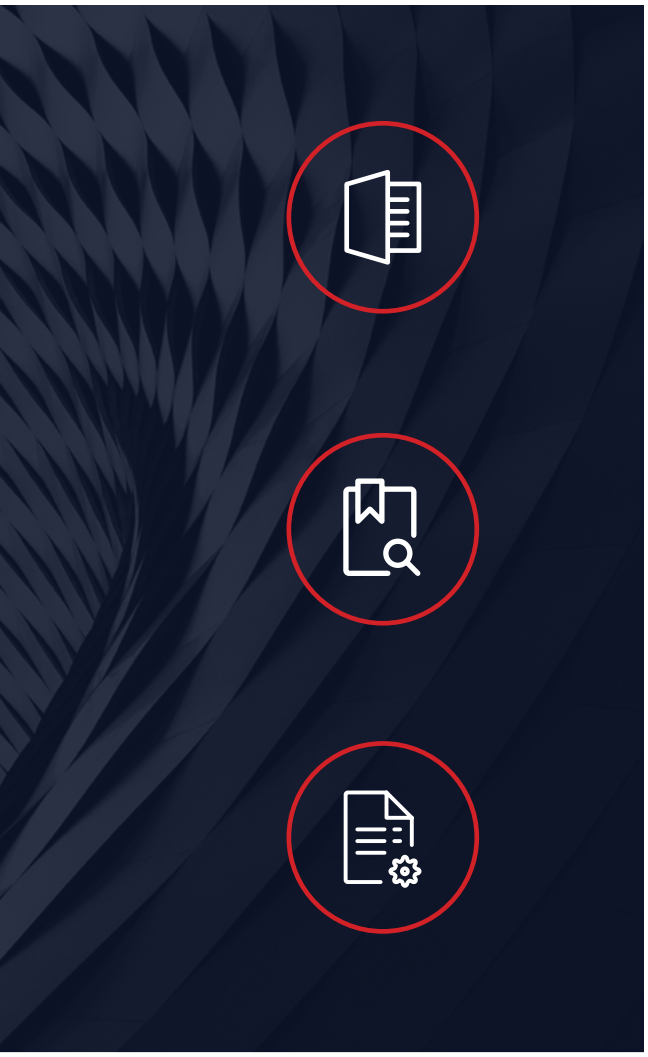
RED TEAM

Combines various techniques to evade detection and prevention capabilities, including OSINT, phishing, wireless and covert physical and network attack tactics, techniques and procedures. Exercise results in assessment of prevention, detection and response capabilities against real-world scenario and identifies areas of greatest risk and remediation recommendations.

- Tests prevention, detection and response capabilities
- Validates both virtual and physical security controls
- Measures effectiveness against phishing
- Simulates a real-world scenario against a threat actor designed to evade detection
- Identifies areas of greatest risk and remediation
- Satisfies compliance needs, including HIPAA, SEC, NYCRR, PCI 3.x.

DELIVERABLES

All eSentire technical testing engagements are designed to test the effectiveness of your security defenses and demonstrate how the engagement was carried out. Vulnerabilities identified in each step of the engagement are used to illuminate areas of risk and, in turn, our experts provide remediation guidance and prioritization so you can prevent future exploitation.



WHAT TO EXPECT IN YOUR REPORT

To ensure the information is valuable and applicable to the appropriate audience, eSentire summarizes all findings into both an Executive level and technical report.

EXECUTIVE SUMMARY REPORT

Targeted toward a non-technical audience so they are apprised of risks and mitigation strategies as a result of the test:

Executive Summary: Brief description of the results of the engagement

Findings and Recommendations: Describes scope, approach, findings, high-risk and systemic issues, and recommendations to remedy issues or reduce risk.

DETAILED TECHNICAL REPORT

Targeted toward technical staff and provides detailed findings and recommendations:

- Methodology employed
- Positive security aspects identified
- Detailed technical findings
- An assignment of a risk rating for each vulnerability exploited
- Supporting detailed exhibits when appropriate
- Technical remediation steps

After the reports are created, we can set up a meeting to share and discuss the findings.

MAKE THE CASE FOR AN eSENTIRE TECHNICAL TESTING

- Applies tactics and techniques used to bypass traditional security controls as seen through the eSentire Managed Detection and Response platform
- Leverages latest threat intelligence from over 200+ sources
- Continuous communication and establishment of goals
- Testing conducted via experienced and certified professionals (e.g. CEH, OSCP, CISSP, etc.)
- Clear reporting with risk prioritization and detailed findings
- Includes detailed discussion with eSentire Advisory Services team members on findings and remediation

NEXT STEPS

Put eSentire MDR to the test

Learn more about eSentire Advisory Services

Learn more about eSentire MDR

Access free cybersecurity tools and resources

eSENTIRE

eSentire, the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire.**