DATA SHEET

Risk Assessment

Holistic identification of organizational, programmatic, human and technical risks

Many security services providers offer assessments that are only designed to look at specific areas of risk leaving you without a holistic view from the top down. Rather than taking a siloed approach, eSentire's Risk Assessment is designed to identify risk across four key areas: organizational, programmatic (security), human and technical.

As these areas require specialization to assess, we employ multiple security teams with expertise in their individual fields, combined with intelligence from our Managed Detection and Response (MDR) platform which identifies attacks that bypass traditional security controls. This combination uniquely enables us to identify your organization's risk measured via assessments against industry standard frameworks, technical testing, phishing and malicious network activity monitoring.

Once the assessment is complete, our experts will provide a combined view into all areas of risk with detailed analysis and recommendations for addressing critical gaps to meet compliance demands and protect your business from threats.

RISK ASSESSMENT APPROACH

BENEFITS

- Identifies areas of greatest risk and prioritizes remediation of what was discovered
- Aligns business objectives and security risks
- Measures effectiveness of your existing technical security controls
- Identifies threats that have bypassed preventative methods
- Validates security awareness training
- Pinpoints employees of greatest risk
- Satisfies compliance needs, including HIPAA, SEC, NYCRR, PCI 3.x.

COMPONENTS

Security Program Maturity & Risk Analysis

Provides an in-depth assessment of the maturity and associated risks of the client's information technology environment. It uses the eSentire Security Framework, which is based on the NIST Cybersecurity Framework, a comprehensive set of policies, procedures and security controls.

Benefits

- Identifies measures to manage and mitigate risk
- Aligns business objectives and risks to security strategy
- Defines action plans and justifies increased security investment
- Examines the organization's unique environment, architecture, operations, culture and threat landscape against an industry standard framework

Focus	✓ Prevention	✓ Detection	✓ Response
Risk Area	✓ People	✓ Process	✓ Technology

Malicious Activity Assessment

Implementation of a single esNETWORK™ sensor in watch-only mode into the client premises for thirty (30) days, to identify malicious activity with near real-time alerts for any potentially malicious activity from the eSentire 24/7/365 Security Operations Center.

Benefits

- Monitors network traffic for known and unknown threats
- Identifies exploits that have bypassed preventative methods
- Measures effectiveness of your existing security controls
- Alerts client to malicious activity landscape against an industry standard framework

Focus	✓ Prevention	✓ Detection	✗ Response
Risk Area	✗ People	✓ Process	✓ Technology

Spear-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.

Benefits

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

Focus	✓ Prevention	✗ Detection	✗ Response
Risk Area	✓ People	✗ Process	✗ Technology

COMPONENTS

Vulnerability Assessment (Internal and External)

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.

Benefits

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

Focus	✓ Prevention	✗ Detection	✗ Response
Risk Area	✗ People	✓ Process	✓ Technology

Penetration Test (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.

Benefits

- 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.

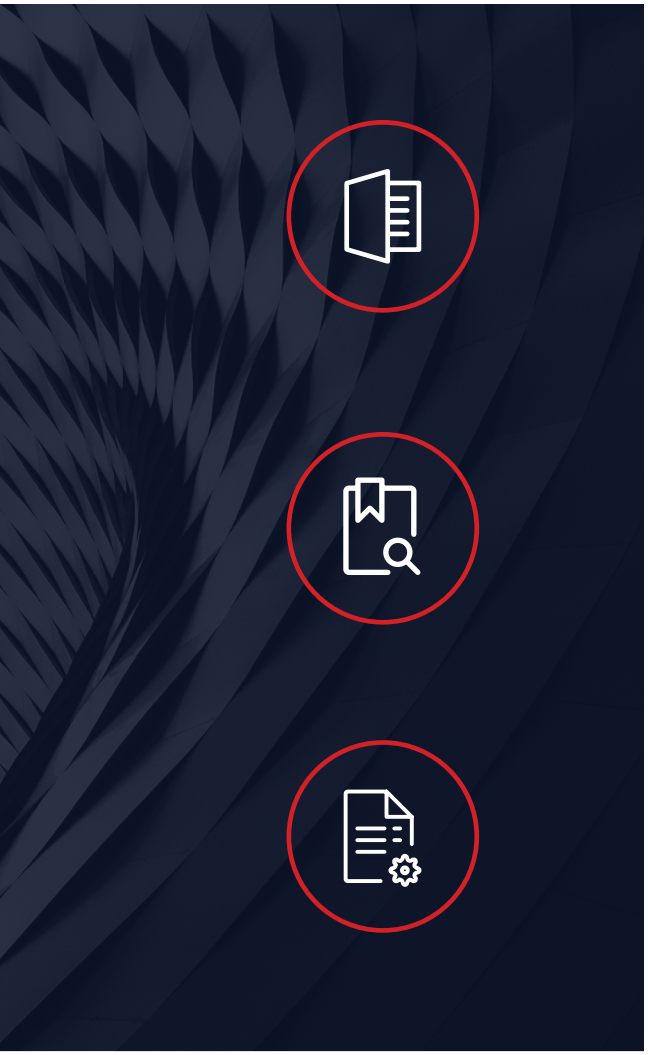
Focus	✓ Prevention	✓ Detection	✗ Response
Risk Area	✗ People	✓ Process	✓ Technology

HUMAN RISK AND TECHNICAL TESTING DETAILS

	Vulnerability Assessment (Internal or External)	Phishing	Penetration Test (Internal or External)
Stealth	Low	Low	Low
Scoping	Reports on all systems and vulnerabilities found on in-scope systems	Reports on all target users	Threat modeling (includes suitable testing scenario)
Target Users		•	
Objective	Broad scan	Test users	Goal seeking
Can be performed remotely	•	•	•
Vulnerability Scanning	•		• (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			•

DELIVERABLES

Throughout the Risk Assessment, eSentire will present clients with reports that include both summary findings and technical detail findings as part of the individual Risk Assessment components. At the conclusion of the engagement, an Executive Summary of the organization's overall results and risk will be provided, in-person or remotely, to the client's executive team as a final deliverable.



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 engagement:

- 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 area
- Supporting detailed exhibits when appropriate
- Remediation steps

MAKE THE CASE FOR AN eSENTIRE RISK ASSESSMENT

- Organizational assessments conducted by certified professionals with experience from the C-level to technical implementation and controls
- Technical testing conducted by experienced penetration testers (e.g. CEH, OSCP, CISSP, etc.)
- Applies tactics and techniques used to bypass traditional security controls as seen through the eSentire Managed Detection and Response platform
- Clear reporting with risk prioritization and detailed findings
- Includes detailed discussion with eSentire Advisory Services and Technical Testing team members
- Satisfies compliance requirements

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, Inc., 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 $6 trillion AUM, 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**.