eSENTIRE

DATA SHEET:

eSentire Virtual CISO (vCISO) Services

Cybersecurity Advisory Services To Develop Your Cybersecurity Strategy and Keep It On Track

We evaluate your strategy

We complete a 15-point cybersecurity program assessment to understand your current strategy and inform your future strategy.

Build your action plan

We align your cybersecurity strategy, business objectives and risk enabling efficient roadmap development.

Set your program objectives & support execution

Your refined strategy will be delivered by a named eSentire vCISO who becomes an extension of your team and builds a program tailored to your business.

Demonstrate value & clear results

Gain buy-in for a comprehensive program development at the board level while meeting and exceeding compliance mandates.

Many organizations find themselves stuck between ever-evolving cyber threats and tightening regulatory requirements. This can force organizations to piece together and execute informal programs that check the compliance box, but don't necessarily align and address the greatest areas of cyber risk.

Our vCISO team approach includes a NIST based organization-wide cybersecurity maturity assessment as part of every engagement. This ensures our experts understand your strengths, weaknesses and greatest areas of cyber risk.

Additional services in the vCISO portfolio such as policy guidance, incident response planning and security architecture review are aligned to one singular strategy, road mapped & measured across a multi-year engagement. This allows your organization to mature with a tailored, comprehensive cybersecurity program that meets the stringent requirements of your industry regulations & business objectives.

Our vCISO program supports you in building a more responsive security operation by:

- ✓ Aligning to your business objectives, risks and cybersecurity strategy
- ✓ Promoting organization-wide buy-in with effective resource allocation
- ✓ Demonstrating measurable success to your executive management and board
- ✓ Defining action plans for a new cybersecurity program or updating your existing cybersecurity program
- ✓ Examining your organization's unique environment, architecture, operations, culture and cyber threat landscape against industry standard frameworks
- ✓ Identifying and prioritizing your cybersecurity architecture risk and subsequent control & remediation opportunities
- ✓ Meeting and exceeding your compliance mandates

Why eSentire vCISO Services

Our vCISO portfolio contains modules that address each component of your cybersecurity posture, including: policy guidance, incident response planning and security architecture reviews. These are all aligned to one singular strategy and measured across a multi-year engagement.

Program	Details	Deliverables
Security Program Maturity Assessment (SPMA)	In-depth appraisal of your information security maturity against industry standards.	• eSentire Security Framework Playbook. • Client report detailing your current security program maturity ratings and comparison to industry norms. • Client roadmap with executive overview and recommendations.
Security Incident Response Planning (SIRP)	Focused, pragmatic strategy on key steps to take when an event occurs.	• Initial (baseline) assessment and Cybersecurity Incident Response Plan development. • Annual re-assessment and testing of Cybersecurity Incident Response Plan identifying necessary changes required. • Annual tabletop exercise to test the efficacy and accuracy of the response measures that are in place. • Update to Cybersecurity Incident Response Plan based on any new findings, environmental or business changes, etc.
Security Policy Review and Guidance (SPG)	Best practices for policies and procedures from NIST Cybersecurity Frameworks.	• Development of updated Information Security policies based on assessment and findings. • Guidance and direction on Information Security policy adoption within your organization. • Annual re-assessment and review of Information Security policies. • Annual review of Information Security policies to identify gaps based on any applicable business, regulatory or legal changes. • Findings and recommendations report based on annual review.
Security Architecture Review (SAR)	Evaluation and audit of your current technologies, security controls and system criteria.	• Assessment and review of security architecture with executive summary and detailed recommendations report based on findings. • Annual re-assessment and review of security architecture.
Vendor Risk Management Program (VRM)	Establish a process to track third-party and vendor risks to your business.	• Assessment and review of existing vendor due diligence processes. • Development of a pragmatic Vendor Risk Management Program including vendor classification and due diligence questionnaires. • Annual reassessment and review of Vendor Risk Management program to identify opportunities for improvement. • Executive summary on findings and recommendations for future changes to Vendor Risk Management Program.
Vulnerability Management Program (VMP)	Create and refine procedures to account for emerging vulnerabilities.	• A documented program to identify, manage, and report on the security posture of systems and applications, and also on systemic security issues. • A vulnerability tracking mechanism, to capture vulnerability data across the environment over time. • Metrics for evaluating the overall effectiveness of the program itself and managing improvement. • Templates for executive reports regarding risks arising from vulnerabilities and from program deficiencies, risk trending, overdue vulnerabilities, and exception reporting. • A summary report of the VMP Development Project.

The eSentire vCISO Difference

While most security service providers deliver a one-and-done approach without understanding an organization's business objectives, cybersecurity strategy and overall cyber risk profile, we operate with insight and context, including a NIST based organization-wide security maturity assessment as part of every engagement. This ensures our experts understand your strengths, weaknesses and greatest areas of cyber risk.

Our vCISO experts:

- ✓ Are industry certified professionals with decades of experience from the C-level to technical implementation and controls
- ✓ Have an average of 17 years of security experience
- ✓ Hold numerous certifications including CISSP, CISM, CISA, and more

The results you can expect from eSentire vCISO consulting services include:

- ✓ Alleviate resource constraints in your organization
- ✓ A comprehensive security program with strong policies and procedures
- ✓ Meet or exceed your compliance requirements
- ✓ Align business objectives with your unique risk and exposure

Ready to get started?

We're here to help! Submit your information and an eSentire representative will be in touch to further discuss our vCISO services

Contact Us

If you're experiencing a security incident or breach contact us ☎ 1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.