SOLUTION BRIEF

Virtual CISO

Security programs that prepare you for tomorrow's threats today

Organizations often find themselves in a vise between ever-evolving threats and regulatory requirements that tighten in response to new attacks. Due to resource constraints, this can force organizations to piece together and execute informal programs that check the compliance box, but don't necessarily align with their areas of greatest risk.

Most security providers deliver a one-and-done approach without understanding an organization's business objectives, security strategy and overall risk profile. Instead, we designed an approach that includes a NIST based organization-wide security maturity assessment in every engagement. This ensures our experts understand your strengths, weaknesses and greatest areas of risk.

Additional components in the Virtual CISO (vCISO) portfolio such as policy guidance, incident response planning and security architecture review are aligned to one singular strategy and road mapped and 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 business and industry.

☆ Build Your vCISO Service

Components

- Security program maturity assessment
- Security incident response plan
- Security policy guidance
- Security architecture review
- Vendor risk management
- Vulnerability management program

Included with all components

- Annually updated plans
- vCISO named contact
- Quarterly health check
- Annual executive briefing

BENEFITS

- Aligns business objectives, risk and security strategy
- Promotes organization-wide buy-in with effective resource allocation
- Demonstrates measurable success to Executive Management and the Board
- Defines action plans for a new security program or updates the existing security program
- Examines the organization's unique environment, architecture, operations, culture and threat landscape against industry standard frameworks
- Identifies and prioritizes security architecture risks and subsequent controls and remediation opportunities
- Meets and exceeds compliance mandates

FRAMEWORK

The eSentire Security Framework is built atop of the NIST framework to address the most critical and practical elements of information security programs in today's technology-driven business world. Integrating the standards, regulations and requirements found across all industries and business sizes, the eSentire Security Framework provides clients with a detailed and easy-to-digest understanding of their current information security posture as it corresponds to the following 15 security program areas.

Security strategy and governance

Human resources

Security architecture

IT/Security risk management

Monitoring and operations

Incident response, DE and BCP

Information management

Asset management

Vulnerability and patch management

Third party risk management

Compliance and audit

Secure network and perimeter security

Authorization and access

Malicious code prevention

Secure build

COMPONENTS

Security Program Maturity Assessment (SPMA)

Security Program Maturity Assessment (SPMA) is the foundation for the vCISO program, providing an in-depth assessment of the maturity 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.

DELIVERABLES

- eSentire Security Framework Playbook
- Client report detailing their current security program maturity ratings and comparison to industry norms
- Client roadmap with executive overview and recommendations

Security Incident Response Planning (SIRP)

Security Incident Response Planning (SIRP) is designed to develop a focused and pragmatic plan to assist you with the key steps to take when a security event happens. This program includes an annual tabletop planning exercise and mock drill testing to assess readiness and any necessary updates to the response plan based on the results of the exercises.

DELIVERABLES

- 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 Guidance

Security Policy Guidance (SPG) builds on the Security Program Maturity Assessment guidance, creating a fully realized information security program by providing specific best practices for policies and procedures based on the eSentire Security Framework and NIST Cybersecurity Framework.

DELIVERABLES

- Development of updated Information Security policies based on assessment and findings
- Guidance and direction on Information Security policy adoption within client's 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

The Security Architecture Review looks at specific technologies used and provides detailed security controls and audit assessment criteria which should be implemented to secure the system. The eSentire Security Framework, which is used as the baseline, is based on the NIST Special Publication 800-53 and 20 Critical Security Controls, which can be translated into related industry specific technical requirements put forward by regulators.

DELIVERABLES

- 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

Vendor Risk Management ensures an organization can review and assess third party providers to mitigate any risk that may currently exist or be introduced by new vendors.

DELIVERABLES

- 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

The Vulnerability Management Program aids in the creation and refinement of procedures to account for and mitigate the risk of emerging vulnerabilities.

DELIVERABLES

- 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

ADDITIONAL FEATURES INCLUDED WITH ALL vCISO SERVICES

HEALTH CHECK

A Health Check is a quarterly service where the client meets with their vCISO to discuss Managed Detection and Response (if applicable) performance and any ongoing Advisory Services as it pertains to their entire cybersecurity program. This is done as an extension of the quarterly MDR review and offered as a value-add to vCISO clients.

EXECUTIVE BRIEFING

An Executive Briefing is an annual service where the client works with their vCISO to create executive level materials they can use to brief their leadership team. The content can be customized to include any ongoing Health Check or related information.

NAMED CONTACT

A primary benefit of the vCISO program is that the client will receive all Advisory Services from a dedicated Advisory Services strategist. This relationship can be leveraged over the course of the contract to provide specific and knowledgeable guidance. The reach of the vCISO into the client environment can also provide guidance on how the relationship and overall information security program can be further developed.

MAKE THE CASE FOR eSENTIRE vCISO

As experts in the small and medium business space, we understand the unique challenges faced by organizations commonly presented with resource availability constraints. Whether that's a lack of time, expertise or resources, our approach is designed to fit organizations that traditionally grapple with scaling security program efforts at this level.

- ✓ vCISO experts leverage intelligence and lessons learned from what attacks bypass traditional security controls from our MDR platform
- ✓ vCISO experts are industry certified professionals with decades of experience from the C-level to technical implementation and controls
- ✓ vCISO experts are dedicated specifically to your organization with a direct line of continuous and clear communication and establishment of goals

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**.