Four Top Emagined Security Services

Emagined Security offers a variety of Security Services designed to support growing security needs. This brochure highlights four key Emagined Security services.

- CISO On-Demand
- Security Risk Assessments
- Network Penetration Test
- Web Application Penetration Test

Together with Emagined Security's other services we can help companies solve a multitude of security challenges.

CISO On-Demand

Overview

CISO On-Demand service is designed to allow organizations to supplement their security expertise. By adding security expertise, at various levels from technical to executive, organizations can conduct a variety of security analyses including business programs, product selections and corporate services.

Benefits

It is important that executive information regarding operation of the business, mergers and acquisitions, personnel, etc., be prudently protected. Simple technique and deliberate attention to this matter can save a company from embarrassing and costly exploitation of this data. By allowing Emagined Security's CISO On-Demand assist you, you can mitigate potential risks associated with sensitive data, reduce executive risk and increase awareness of vulnerabilities.

Emagined Security's CISO On-Demand can help save your company time and money by proactively assessing and improving your security programs. In addition, by using Emagined Security's CISO On-Demand, your organization can obtain the most accurate and unbiased evaluation of your strengths and vulnerabilities in the information security arena.

Description of Service

Emagined Security's CISO On-Demand can be responsible for conducting a variety of technical security analyses of programs, products and services, as your organization deems necessary. Emagined Security's CISO On-Demand's can interview key personnel and review security services, products, and networks. Emagined Security's CISO On-Demand can be responsible for managing your security programs, using your own or Emagined Security's resources, including:

- Policies & Programs
- Mobile Solutions
- Data Protection Services
- Virtual Private Networks (VPNs)
- Data Loss Prevention
- Public Key Infrastructures
- Encryption

- Audit Support
- Etc.

Based on acquired information, Emagined Security's CISO On-Demand can conduct analyses and generate reports from a business perspective.

Security Risk Assessments

Overview

Security Risk Assessment includes an analysis of the effectiveness of a company's or specific system's security controls. Our service includes adaptive techniques to work with organizations to review the risk associated with a company's overall security design, implementations of sensitive e-commerce applications, and overall risk identification to ensure that proper security controls are utilized.

Benefits

A Risk Assessment can help save your company time, money and the embarrassment of a bad audit by finding discrepancies before an audit occurs and before an attacker does. In addition, by allowing Emagined Security to perform the assessment for you, you receive the most accurate and unbiased report of your strengths and weaknesses in the information security arena.

Emagined Security has developed this process to assess information security processes and controls in order to ensure that organizations preserve the integrity, confidentiality and availability of their information and computing resources.

Description of Service

Risk Assessments start by evaluating crucial components at the corporate and technical levels. These reviews are broken into the following categories:

- Security Program Assessment
- Security Technology Assessment
- Configuration Reviews

In order to perform the Risk Assessment, we will follow a methodology that will proceed through seven stages:

Phase	Description
1	Review Existing Security Policies, Processes, and Practices
2	Interview Staff Members
3	Assess Current Controls
4	Identify Technical Vulnerabilities and Business Risks
5	Determine Proposed Recommendations or Solutions
6	Document Current Security Posture
7	Prioritize High-Level Roadmap

The Security Program Assessment provides an analysis of the effectiveness of a company's security controls based upon ISO 27001, 27002. This task will assess the current security posture, contrast it against industry standards and best practices, and make recommendations to attain your security goals. Emagined Security recommends that you periodically assess your security environment to ensure that you are in compliance with each regulation that governs your industry.

- Review of current documentation, policies and practices
- Interviews with key personnel
- Comparisons against "best practice"

The security categories that we examine include:

- Security Policies, Standards & Guidelines
- Security Organization & Infrastructure
- Security Asset Classifications
- Personnel Security & Training
- Physical & Environmental Security
- Network, Communications & Operations Management
- Telecommunications Security
- Systems Development & Maintenance
- Security Administration & Access Control
- Anti-Virus Protection
- Incident Response Identification & Response
- Business Continuity Planning

- Legal Compliance
- Privacy

The Security Technology Assessment performs a high-level security review of the external security boundary along with selected key areas and systems to determine potential vulnerabilities and risks. The primary systems and areas of interest include:

- Internet Connectivity
- Remote Access
- Business Partner Connections
- Critical Internal Network Infrastructure
- Application Security Infrastructure

For these areas, the topics on which we will typically focus are:

- Identification And Authentication
- Password Management
- Resource Access Control
- Data Security
- Security Event Logging
- Intrusion Detection And Reporting
- Virus Protection
- Operating System Patches
- Emergency Response
- Data Backup And Archiving
- Contingency Planning
- Operations Procedures
- Vendor Access Control
- Software Development Standards
- Change Control

The Configuration Reviews will perform key Technology Equipment reviews (e.g., firewalls, routers, servers) and make cost effective recommendations. This review provides an internal perspective of technology to determine if configurations are adequate.

Network Penetration Test

Overview

Network Penetration Testing enables clients to quickly identify, assess and remedy security holes. Devices attached to the network are evaluated to detect technical vulnerabilities. Penetration Testing is accomplished by performing scheduled and selective probes of the network's communication services, operating systems, key applications, and network equipment in search of those vulnerabilities. Our specialists analyze the vulnerability conditions and provide a detailed report including corrective actions.

Benefits

Penetration Testing is a battle simulation to determine what vulnerabilities have not been addressed in your network. By locating vulnerabilities before the bad guys do, Penetration Testing will increase the level of confidence of the company's security measures. In particular, Penetration Testing:

- Provides a "battle-test" for your network, systems, and applications
- Provides a more "realistic" test than a paper-based assessment
- Provides a proactive approach to mitigating risk
- Enhances the quality assurance process
- Demonstrates the need for and effectiveness of security