



Progressive Ethical Hacking

Overview

Bringing together Emagined Security's Ethical Hacking, Threat Warning Service, Vulnerability Alert Service, and Penetration Test Research Lab, Emagined Security offers Progressive Ethical Hacking. This unique service is available to select companies that continually need to be at least one step in front of the organized crime and professional black-hat hackers.

Benefits

This exclusive service is designed to support internet based companies that a single compromise can have devastating effects on their revenue stream. This service combines many Emagined Security services into a unique offering designed to be one step ahead of the hacker community. Thus, exclusive service is for organizations that do not feel that a point in time review is sufficient. In particular, Progressive Ethical Hacking provides:

- Ethical Hack Comprehensive Baseline
- Internet Monitoring
- Static Binary Analysis
- Regular reviews for application and associated asset changes
- Dedicated research of your potential vulnerabilities
- Validation of newly discovered attack vectors

Description of Service

Ethical Hack Comprehensive Baseline

Combining our External Network Penetration Testing and Web Application Penetration Test service, Emagined Security offers an initial comprehensive baseline review. This initial review will identify existing vulnerabilities in an organizations web application service and infrastructure. Using this review as the baseline the remaining components of the Progressive Ethical Hack program will be established.

Internet Monitoring

Emagined Security Internet Monitoring is designed to identify newly discovered vulnerabilities and malicious discussions. Protecting vital information in today's online environment requires an intelligence-led approach to security an approach that focuses on identifying risks early for effective prevention and mitigation. This is accomplished using three separate approaches:

- Continual review of Internet communication channels
 - Ethical Hacking techniques
 - Proprietary information leaked by employees
 - Malicious discussions involving your organization
- Review of Security Alert information that offers the most comprehensive and customizable alert services for environment-specific vulnerabilities and malicious code alerts.
 - The Alert Services components will be customized around your systems.
- Review of Threat Analysts review threat data as it comes available to support zero day threat detections.
 - This information is vital to being able to obtain information just in time to remediate eminent malicious security events.

Regular reviews for application changes

Emagined Security will periodically review your website to determine if any significant security changes have been made. If the changes are logged as high risk, they will be reviewed ASAP. Other changes will be validation during the remaining two phases to determine if they pose significant threats.

Dedicated research of your potential vulnerabilities

Emagined Security will use information from the prior phases and proven white-hat hacker techniques to periodically research your organization and its potential vulnerabilities. This research designed to simulate black-hat techniques is divided into the following components:

- Penetration Test Lab Research
- Internet Research for Company Proprietary Information
- Social Engineering
- Vulnerability Analysis
- Threat Analysis
- Laboratory Testing
- Potential Risk Identification
- Etc.

Validation of newly discovered attack vectors

Using all the information from the previous phase, on a monthly basis, Emagined Security will attempt highly sophisticated attack vectors to attempt to subvert protection methods. This phase will employ knowledge gathered from each of the prior phases and thus creates a concerted effort to bypass an organizations electronic defense.