

Healthcare vulnerability assessment and penetration testing

PROACTIVELY MANAGE RISK

Meeting the minimum compliance obligations may mean you've got the boxes checked, but it most likely won't reveal critical vulnerabilities that could put your organization at risk. Additional steps should be taken to safeguard electronic protected health information (ePHI).

Through healthcare vulnerability assessment and penetration services, Coalfire Labs simulates malicious intent to reveal hidden weaknesses in your IT and physical environments that could leave your organization exposed.

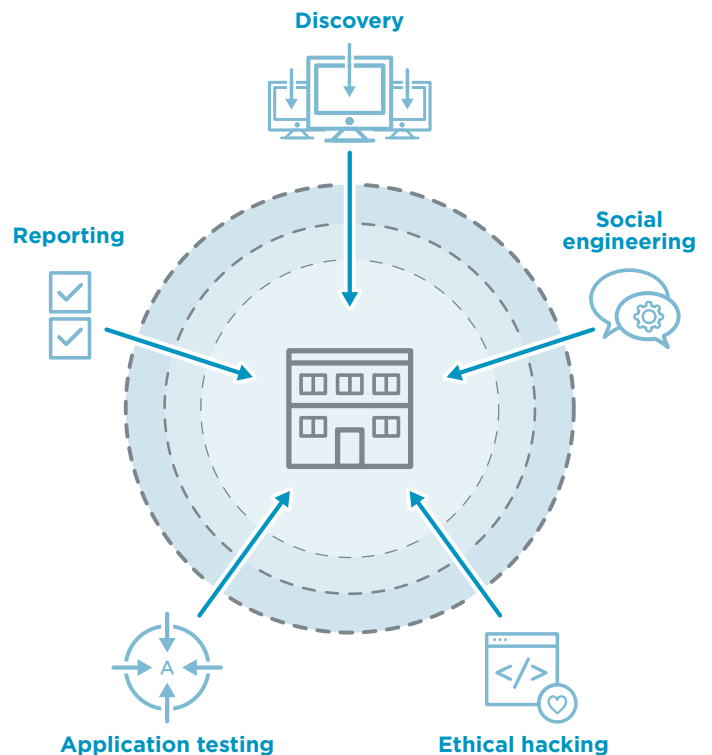
Our team uses CoalfireOneSM to consistently manage projects and identify compliance challenges so they can be addressed quickly and cost effectively. CoalfireOne is designed for collaboration, so you can play an integral part of the assessment process.

COALFIRE SERVICES

Compliance is often measured against the results of automated vulnerability scanning. While technical testing is effective in finding some security weaknesses, it is no guarantee of protection. The most effective vulnerability assessment and penetration tests are performed by a human tester supported by the latest technologies. Coalfire Labs uses expert testers and consultants who have comprehensive knowledge of IT security best practices and healthcare-related compliance issues. This team challenges your environment, explains the results, and offers recommendations on next steps.

- **Discovery:** Our experts conduct methodical reconnaissance, scanning, vulnerability, validation, and reporting to discover, verify, and report security flaws.
- **Social engineering:** We attempt to manipulate the users of critical data into unintentionally performing specific IT-related actions or divulging confidential awareness. In doing so, we test the security awareness of your employees and the physical security of your environment.

- **Ethical hacking:** Our experts use automated and manual techniques to gain access to your vital information.
- **Application testing:** Through automated vulnerability scans, we identify unintentional programming and configuration errors in web applications that can be exploited to compromise the application and the data it stores.
- **Reporting:** We provide the results of the scans and penetration tests, including interpretations and recommendations. This report helps you quickly identify and implement an action plan to close gaps and protect your valuable information.



INCIDENT RESPONSE AND RECOVERY

Despite your diligence, a breach may still occur. If one does, Coalfire offers full response and recovery services to:

- Minimize the impact.
- Stabilize the situation.
- Repair security vulnerabilities.
- Implement malware protection.
- Manage configuration.
- Develop a recovery plan.
- Provide critical information on compliance regulations

TAKE THE COMPLEXITY OUT OF ASSESSING CONTROLS AND RISK.

www.coalfire.com | 877-224-8077

COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com

Copyright © 2014-2017 Coalfire Systems, Inc. All Rights Reserved. Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.