COALFIRE.

Hunting for vulnerabilities in a healthcare company's infrastructure

AT A GLANCE

An international Fortune 100 managed healthcare organization with more than $29 billion in revenue and 38,000 employees has an ongoing critical need for cybersecurity measures that extend beyond the scope of most providers.

CLIENT CHALLENGE

With growing public concern about the security of health-related personal information, the company sought a thorough analysis of its past, current, and future security posture. The company reached out to Coalfire because of our established, experienced team of highly skilled professionals.

APPROACH

In addition to penetration testing and red team operations, Coalfire proposed a two-phase hunt assessment to look for breaches that may have already occurred inside the system. In the first phase of hunt operations, Coalfire conducted a strategic analysis of network traffic to pinpoint potential indicators of a network breach and identified egress and ingress points.

Building on the results of phase one, Coalfire conducted a tactical assessment of potentially compromised hosts, the presence of malware, and any other already compromised systems within the established boundary.

As well-known industry contributors and thought leaders, the Coalfire technical testing team used open source hunt operations tools, such as PowerShell Digital Forensics, that were actually created and released by the team.

RESULTS

Coalfire's hunting capabilities are recognized in the industry because of the methodology of execution and the team's ability to flex to meet customers' needs.

Coalfire provided the healthcare company with scheduled windows of engagements ranging from two weeks for penetration testing to three to six weeks for the more complex red team and hunting operations. This schedule allowed maximum efficiencies for individuals on the client side who were involved in the project. Coalfire's analysis included strategies and specific recommendations for remediating vulnerabilities that could be implemented immediately, thereby increasing the security of the client's networks and valuable data.

About Coalfire

As cybersecurity risk management and compliance experts, Coalfire delivers cybersecurity advice, assessments, testing, and implementation support to IT and security departments, executives, and corporate directors of leading enterprises and public sector organizations. By addressing each organization's specific challenges, we're able to develop a long-term strategy that improves our clients' overall cyber risk profiles. Armed with our trusted insights, clients can get to market faster with the security to succeed. Coalfire has offices throughout the United States and Europe.
Coalfire.com

COALFIRE.