COALFIRE

CASE STUDY

Coalfire advises on breach containment and helps remediate vulnerabilities for an international retailer

AT A GLANCE

An international retailer was breached by two sophisticated foreign advanced persistent threat (APT) teams. When the FBI notified the retailer of the breach, the enterprise reached out for assistance to eradicate the attackers from its network. Subsequently, the retailer engaged Coalfire to help strengthen its network security posture. Coalfire advised on how to neutralize the attackers and secure the network environment.

CHALLENGE

Initially, the international retailer hired another third party to investigate the breach, but the provider's recommended remediation approach proved to be costly and difficult to execute. Based on the recommendation of its cyber law firm, the retailer hired Coalfire to provide incident response, eradication advise, and network security remediation services.

APPROACH

Coalfire provided subject matter expertise along with incident response and remediation services to help the retailer respond to the breach. Coalfire guided the analysis of the malware tools used by the attackers and then removed them from the network. Then, Coalfire developed a strategy to conduct a global password change across the retailer's networks. The retailer lacked the processes and tools to manage global password resets, so Coalfire identified and implemented the necessary technology. Coalfire deployed the appropriate tools and generated an asset inventory, which provided the retailer and its cyber law firm the confidence that the breach had been contained and the incident could be closed.

Coalfire further assisted by providing cybersecurity guidance, planning, and expertise to fix other critical vulnerabilities within the retailer's IT infrastructure and enhance its incident response readiness posture so that it would be better prepared in the event of a future breach.

Today, Coalfire offers clients a single point of contact and seamless expertise for end-to-end breach response and remediation.

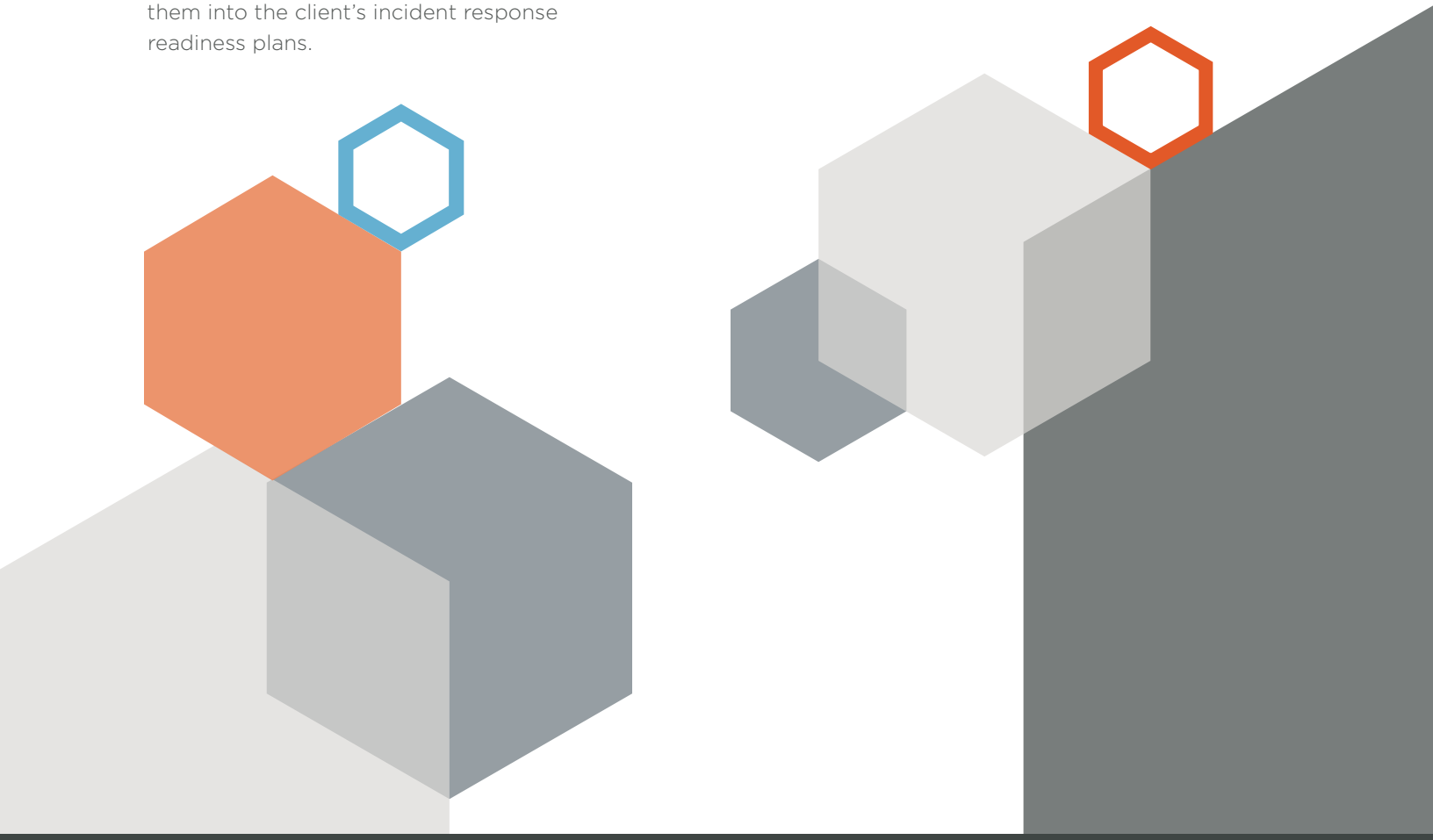
RESULTS

As a result of Coalfire's work, the retailer implemented the lessons learned and dramatically redefined its incident response plan. Coalfire effectively:

- Eradicated the attackers from the victim's network.
- Generated the critical asset inventory that allowed the incident to be closed.
- Enhanced the client's network security through implementation of new technologies.
- Identified cybersecurity control gaps and enhanced in-place controls.
- Documented "lessons learned" and incorporated them into the client's incident response readiness plans.

"I've partnered with at least a dozen cybersecurity firms as I led large-scale incident response operations over the past decade. The teamwork, professionalism, and performance demonstrated by Coalfire on this breach far exceeds anything I've seen. This is our go-to team for the future."

- CIO OF THE INTERNATIONAL RETAILER



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 nearly 20 years and has offices throughout the United States and Europe. **Coalfire.com**

CS_IntlRetail_030419