HEXEON
BY COALFIRE

DATA SHEET

Offensive security

Integrated and aligned to deliver desired security outcomes

Offensive security that defines defensive priorities and establishes urgency requires engaging in a continuous, collaborative process from an adversarial perspective. This process should focus on validating and improving your organization's ability to defend against real-world threats. These efforts prioritize testing probable scenarios over spending time demonstrating the possible.

Introducing Hexeon, Coalfire's new offensive security SaaS solution

Hexeon is a new, modern, and agile standard for managing vulnerabilities throughout their lifecycle. By integrating human intelligence with automation, Hexeon provides continuous and actionable insights into your threat exposures, enabling you to prioritize responses that strengthen your organization's cyber resiliency.

Hexeon's engaging, user-friendly experience features seamless, real-time communication; shared dashboards; and unified reporting. The solution allows you to collaborate with your Coalfire team in real time, leading to positive business outcomes.

Our approach leveraging Hexeon

Our unique blend of human intelligence and automation provides real-time visibility into the way organizations manage threat exposures. We customize each offensive engagement to meet your needs and goals, designing and developing offensive security programs that are proven to scale with even the most complex environments. Hexeon, our new offensive security platform, enables our expert team to provide the comprehensive services we're known for – asset discovery, vulnerability identification, adversary emulation, offensive security testing, and remediation guidance – all in one easy-to-use solution.

Comprising the industry's top penetration testers, our team performs each test, leveraging experience with thousands of global engagements across more than 1,500 organizations. The engagement we shape for your organization may include:

Penetration testing

A targeted, focused approach that seeks to identify specific vulnerabilities in your environment, penetration testing involves using known vulnerabilities and attack vectors to attempt to exploit weaknesses in a limited scope of systems. Penetration testing is typically used to assess the security of a specific system or application and is often applied as part of a compliance program or to validate a system's or application's production readiness.

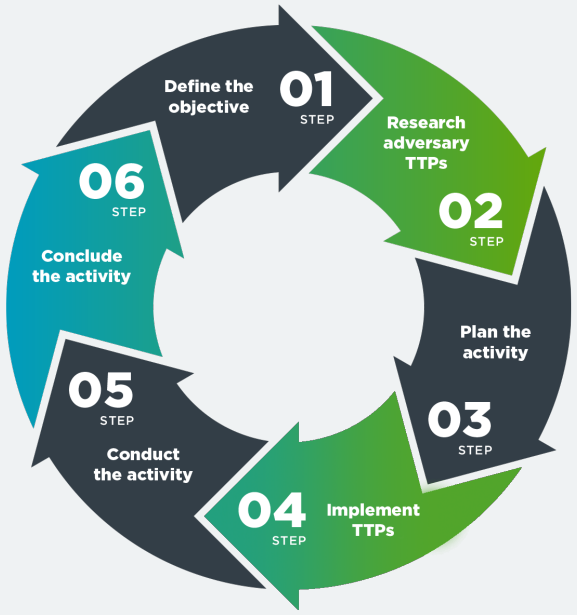
Red teaming

A more comprehensive approach to testing your security posture, red teaming involves simulating a real-world attack scenario to test your ability to detect and respond to an attack. Red teaming tests your overall security posture and identifies weaknesses in detection and response capabilities. It also tests your ability to withstand a coordinated, multi-vector attack.

Adversary emulation

In this offensive security technique, our security professionals simulate the tactics, techniques, and procedures (TTPs) of real-world attackers. The goal is to identify and test your ability to detect and respond to an actual attack performed by real threat actors, mimicking the TTPs used in documented attacks.

Six steps to Coalfire's adversary emulation process



Following the MITRE ATT&CK principles, our process for adversary emulation spans six steps:

1. **Define the objective:** Our team assesses the current threat landscape in the context of your business concerns to determine the threat to be replicated. This includes identifying your organization's most valuable systems and data, the TTPs that will be used, and your response capabilities.
2. **Research adversary TTPs:** Once a threat is selected, TTPs are assessed to determine alignment with engagement objectives, available cyber threat intelligence (CTI), and complexity.
3. **Plan the activity:** After TTPs have been selected for emulation, our testers develop a detailed schedule, rules of engagement, and communication plan for the engagement.
4. **Implement TTPs:** We then collect and prepare TTPs into a usable format, which may include writing code, collecting tools, etc.
5. **Conduct the activity:** We execute the plan by using the same tools and techniques as real-world attackers, such as phishing, vulnerability exploitation, and malware, to gain access to systems.
6. **Conclude the activity:** We then provide results, including analytics, mitigations that were effective in the exercise, and required mitigations to address identified gaps.

Careful planning and execution of the adversary emulation approach result in the most holistic view of your security program. While this approach is highly effective and best conducted as a part of a larger program, it can sometimes be used as a standalone exercise, as long as the objective is clearly defined. There may be certain situations when adversary emulation is not the right approach; this often depends on the scope, timing, and follow-on resources available for mitigation.

Improve your organization's ability to defend against threats.

Learn more about Coalfire's offensive security services.

Coalfire.com | 877-224-8077

COALFIRE

About Coalfire

The world's leading organizations – including the top five cloud service providers and leaders in financial services, healthcare, and retail – trust Coalfire to elevate their cyber programs and secure the future of their business. Number one in compliance, FedRAMP®, and cloud penetration testing, Coalfire is the world's largest firm dedicated to cybersecurity services, providing unparalleled technology-enabled professional and managed services. To learn more, visit **Coalfire.com**.

DS_OFFSec_073123