COALFIRE

DATASHEET

Threat modeling and attack simulation

Maximize your security investments.

As the threat landscape continues to become more sophisticated, security professionals around the world are challenged to look beyond the typical list of attacks and think about new threats – even those that have never been considered.

Coalfire has developed a proprietary threat modeling and attack simulation (TMAS) approach to help your organization prove the effectiveness of your security investments and justify the decisions made when establishing a security operations strategy.

Our threat modeling and attack simulation (TMAS) approach begins by evaluating the strategy and threat model that your organization has undertaken to build out your security operations team. Armed with your organization's prioritized decisions, our team will carry out purple-team-styled attacks that emulate the attackers and threat vectors you established your operations to protect against, as well as emulate attacks that target those environments and threat vectors you chose to de-prioritize.

The objective of this engagement is to:

- Optimize security technologies and systems.
- Optimize security operation workflows.
- Establish a baseline and advanced command of the security operations toolsets.

Aligning security testing in this manner provides validation that your cyber program is effectively securing your business objectives.

OUR APPROACH

- **Evaluate** the risk management strategy to determine how to prioritize security investments.
- **Identify** threat actors and threat vectors that could leave the organization vulnerable.
- **Attack** simulation.
- **Execute** attacks and identify security program gaps.

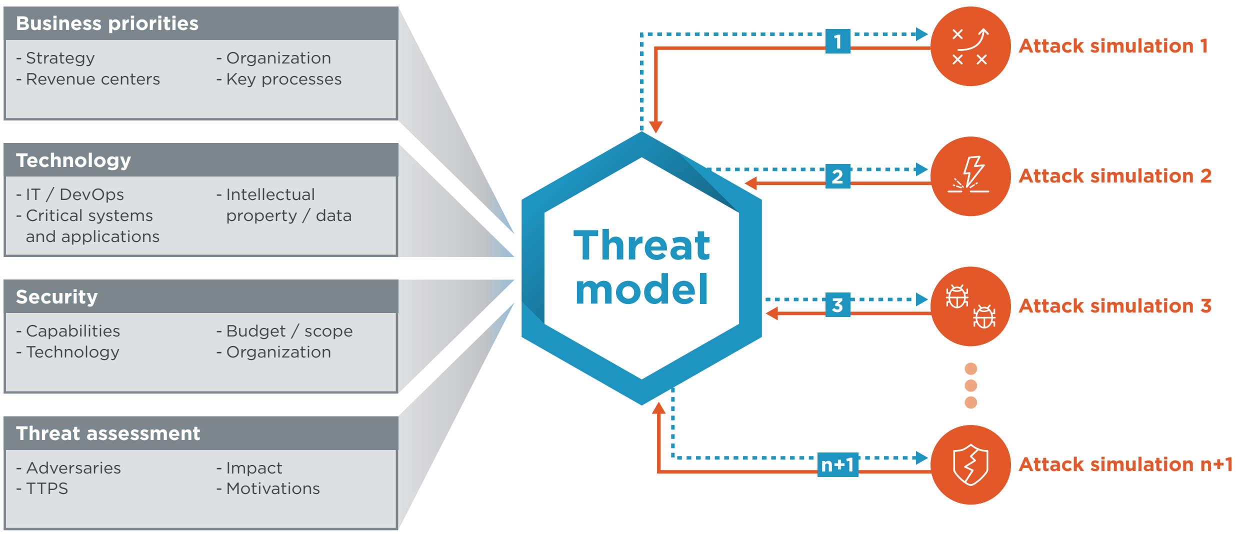
SAMPLE ATTACK SCENARIOS

- Insider threat access to sensitive data
- Compromised customer account used to attack application interfaces
- Supply-chain / software dependency compromise
- "Malware-infected" workstations controlled by an attack on the internal network
- Spear-phishing attacks, targeting high-profile individuals
- Physical attacks to breach the perimeter and gain access to the network

WHY CHOOSE COALFIRE?

- **Broad capabilities**
  - Our testers can carry out any attack vector against any organization including via physical access, social engineering, technical attacks, or non-traditional IoT solutions.
- **Industry thought leaders**
  - Coalfire Labs was awarded the prestigious CREST accreditation, which recognizes our team's skills and proficiency in penetration testing, as well as the consistently high standard of service we provide.
  - Our team members regularly speak at leading industry events and conferences, including Black Hat, DEF CON, DerbyCon, and BSides, to teach others about advanced tradecraft.
- **Cutting-edge research and development**
  - We constantly research new and emerging technologies to equip our team with the latest techniques and solutions to demonstrate risk for our clients.
  - Our team comprises developers of industry-leading tools including, RedBaron, Icebreaker, iOS 11.1.2 Jailbreak, Dissonance, Hwacha, DeathStar, and Malrule.

COALFIRE'S APPROACH TO THREAT MODELING AND ATTACK SIMULATION



Business priorities
- Strategy
- Revenue centers
- Organization
- Key processes

Technology
- IT / DevOps
- Critical systems and applications
- Intellectual property / data

Security
- Capabilities
- Technology
- Budget / scope
- Organization

Threat assessment
- Adversaries
- TTPS
- Impact
- Motivations

Threat model

1 Attack simulation 1

2 Attack simulation 2

3 Attack simulation 3

n+1 Attack simulation n+1

DS_TMAS_040920

MAKE THE MOST OF YOUR SECURITY INVESTMENTS WITH HELP FROM COALFIRE.

Learn more about Coalfire's threat modeling and attack simulation services.

Coalfire.com | 877.224.8077

About Coalfire

Coalfire is the trusted 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. For more information, visit **Coalfire.com**