BUILD CYBERSECURITY READINESS WITH LIVE FIRE EXERCISES

Building cybersecurity readiness by conducting a live fire simulation of today’s sophisticated and advanced targeted attacks is key for any organization. It helps train you to reduce reaction time to real-world attacks with well-orchestrated, rehearsed processes. CrowdStrike® Live Fire exercises take response simulations beyond discussion-based tabletops by pressing participants to take action in a fully immersive experience. These exercises can involve the full spectrum of responders from analysts to executives and focus on using real tools and capabilities for investigating, communicating and coordinating. For organizations that are confident in their ability to respond or those that have completed tabletop exercises with ease, the live fire exercise can take security preparedness to the next level.

HOW A LIVE FIRE EXERCISE IS CONDUCTED

CrowdStrike Services begins by reviewing your incident response processes and protocols as well as the tools you use to investigate and coordinate the response to a cybersecurity incident.

After reviewing your response capability, CrowdStrike team members examine your network with the goal of understanding the strengths and weaknesses of your defensive posture. The team then devises an attack scenario that exploits those weaknesses while avoiding your strengths, working with you to meet the appropriate level of difficulty and complexity. Based on these reviews, the Services team works with a small subset of your security and response teams to develop an exercise scenario and anticipate your team’s likely response. A series of injections are developed that simulate real-world inputs, including security tool alerts, media inquiries, customer interactions and more.

THE CROWDSTRIKE LIVE FIRE EXERCISE PROVIDES THE FOLLOWING BENEFITS:

- Take your response planning and exercising to the next level with a fully immersive and interactive simulation, using your company’s own infrastructure
- Participate and take actions as you would in a real incident, rather than simply discussing what you would have done
- Use data injects that simulate real-world inputs, including security tool alerts, media inquiries, customer interactions and more
- Adjust the level of realism to suit your needs — stay at your desk until you’re called in or have the command center already assembled
- Conduct activities throughout the exercise that give your teams an opportunity to put their policies into action: writing a holding statement, doing an indicator search and more
- Experience positive outcomes: CrowdStrike helps you deal with the latest attacks, extracting lessons-learned to improve your security posture going forward
KEY CAPABILITIES

- **Action oriented**: Unlike a tabletop exercise, where participants have a facilitated discussion about how they should or would respond to different situations, participants in a CrowdStrike Live Fire exercise must act. These actions may include examining forensic data, searching for indicators of compromise across an environment, communicating key findings or new developments with the necessary stakeholders, writing press releases, briefing executives and more.

- **Flexible and tailored approach**: The format is dictated largely by your own organization’s standard response process and the degree to which you want to simulate it. Setup of the exercise varies depending on what is needed from the simulation: Participants may be in the same room; separate rooms for technical and management responders; breakout rooms based on different functions; or they can all start at their desks and figure out where they need to be.

- **Cross-functional approach**: The live fire exercise involves an organizationwide response, including information security, communications, legal, compliance, HR and business leaders.

- **Positive outcomes**: In addition to the comprehensive live fire exercise, CrowdStrike provides two written deliverables:
  - A copy of all materials used in the exercise, including any scripts, timelines, injects, etc.
  - A detailed list of key takeaways and observations identified during the scenario by both your organization and the CrowdStrike team.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services security team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

Learn more at www.crowdstrike.com/services/
Email: services@crowdstrike.com

© 2019 CrowdStrike, Inc. All rights reserved.