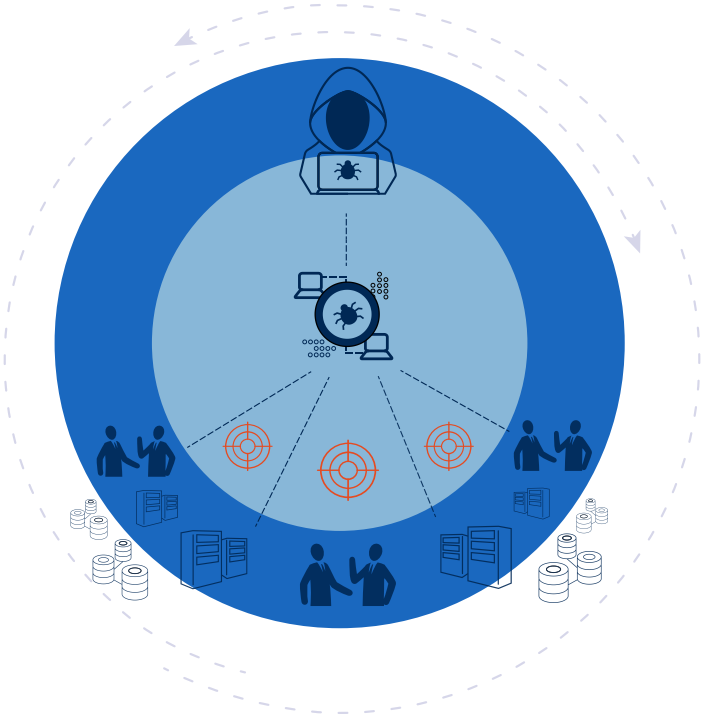
BREACH RESPONSE WARGAME

Assess capabilities to detect and respond to adversial threats

Enterprises are constantly looking to improve their security posture beyond the traditional, compliance-driven penetration testing. One popular method is to deploy advanced services that can protect their environments more effectively by emulating sophisticated cyber attacks that are becoming increasingly common. No organization is immune and many are still vulnerable to even the simplest and most common techniques and exploits, let alone the more sophisticated attacks that can remain undetected in the network for weeks and months. To make matters worse, cyber criminals are continuously upping the stakes by repurposing and combining existing techniques and malware into new exploits that are increasingly difficult to detect and prevent from penetrating your existing defenses.

Optiv can help. With a slow and deliberate approach, we experiment with an array of breach simulation tactics and conduct war room-style exercises to assess your organization's processes, defenders, and overall security controls. Collaborating in interactive working sessions with stakeholders from your Security, IT Operations, and Incident Response teams, wargaming helps teams more effectively identify security strengths and weaknesses during live breach simulations. By the end of the engagement, your team will have a clear understanding of the current incident response strengths and gaps, so you can evaluate your holistic defense plan.



Optiv consultants have the expertise to utilize non-attributable and evasive techniques to assess clients' infrastructure while gaining access and persistence on those targeted systems. Optiv uses this knowledge to provide both tactical and strategic recommendations for our clients' security programs.

How Do We Do It?

EVALUATION PHASE:
We evaluate your organization's attack surface and begin to develop attack scenarios for your organizations.

ANONYMOUS, NON-ATTRIBUTABLE INFRASTRUCTURE:
We deploy a non-attributable Command and Control ("C2") infrastructure and custom artifacts ("Malware") to assess threat hunt-and-detection readiness.

DECONSTRUCTED BREACH APPROACH:
We conduct a phased covert-to-overt malware execution attack that replicates those done by sophisticated attackers, such as nation states and cybercrime syndicates, until detected by countermeasures.

DEFENDER ANALYSIS:
Optiv will document each activity that is executed during the attack scenarios while working with your team to monitor how defenders and incident responders react.

SITUATIONAL DEBRIEF:
Onsite executive review encompassing all aspects of the Wargame and Breach Simulation, highlighting strengths and weakness across your defensive processes.

Benefits of a Breach Response Wargame

Increased Confidence in Operational Staff
Ensure that incident responders are fully prepared for sophisticated real-world threats

Prioritize and Tune Threat Detection and Response Capabilities
Fine tune automated tool indicators and configurations with a phased breach simulation

Improve Analysis and Response
Reduce the amount of time it takes to identify and triage a cyber threat incident

Choose the Right Partner

Optiv's Attack and Pen team continues to earn accolades from clients across many industries with our proven methodology and innovative attack approach. We offer a wide variety of offensive security solutions from standard vulnerability scans to sophisticated, nation state-level breach assessments and simulations. As the largest commercial Attack and Pen team in the world, we have the skills and experience to validate the effectiveness of your layered security defenses so you know exactly what is working and what needs to change.

The Optiv Advantage

Optiv can help businesses in every industry connect information security policies, procedures and practices with business goals. Our security leadership experts, backed by our team of consultants, can provide the experience you need to take your program to the next level.

Expert Minds

Optiv's security professionals are dedicated to helping you achieve results and realize value. Our team of 1,000+ highly skilled client managers and security practitioners work hard to deliver superior results and cutting-edge research to solve your complex, real-world security problems.

Leading Best Practices

Our knowledge of leading best practices helps Optiv formulate security recommendations tailored to meet your specific business objectives.

Client-First Culture

Optiv's passion for security and our commitment to quality results means we focus on the right solutions to meet your specific needs.

Proven Methodologies

Optiv has developed proven methodologies to help ensure superior outcomes for your projects and programs.

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.