

ALWAYS-ON PENETRATION TESTING

Challenge your organization to practice like it fights

Traditional point-in-time assessments are instrumental in validating an organization's security posture, but they often overlook dynamic security controls in production environments – including network defenders and incident response processes.

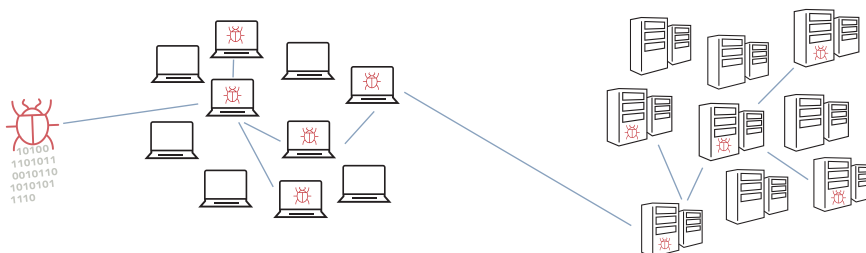
Always-On Penetration Testing addresses these challenges with an ongoing testing cycle using real-world attack techniques and testing conditions. This helps validate your organization's ability to identify, evaluate, and defend against previously unknown attackers that may engage when you least expect it.

The service can be paired with compliance-based penetration tests and other specialized tests as part of your larger penetration testing program. Offered in both bi-annual and quarterly delivery options, both choices provide an evasive penetration test from Optiv's anonymous, non-attributable attack infrastructure. These attacks may be triggered at random times during the period or triggered by an opportunistic change in the client's perimeter, such as newly deployed systems or applications that the Optiv team is periodically searching for.

Are you prepared to practice like you fight?

Example Attack Scenario

Attack Surface Analysis	Perimeter Interrogation	Gain Foothold	Lateral and Vertical Movement	Achieve Goal
Through passive reconnaissance, analysts identified four publicly facing login portals, as well as a list of potential defensive controls in a job posting.	Through active, manual testing, analysts identified a variety of exposed services and were able to identify a potentially exploitable weakness in ABC application/system.	Analysts were able to exploit the identified weakness by utilizing a SQL injection technique and gain shell access on the underlying operation system.	Utilizing the foothold on ABC system, analysts were then able to extract XYZ domain user names and ultimately their credentials by exploiting ABC vulnerability on XYZ system, which had a logged in system administrator.	Utilizing domain administrator privileges, analysts were able to move a compromised user into the "Payroll" domain group and ultimately gain access to employee SSN's, payment, and tax information.



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?

- ENGAGEMENT PLANNING:**
 Project management engagement, stakeholder and timeline development, and de-confliction processes are established to allow prompt separation of our attacks and potential threat actors.
- OPPORTUNISTIC ATTACKS:**
 Optiv attacks are scheduled to occur at seemingly random times throughout the testing cycle, and our attacks periodically review changes in your organization's attack surface to launch new attacks.
- ANONYMOUS, NON-ATTRIBUTABLE INFRASTRUCTURE:**
 Our opportunistic attacks are launched from an environment unknown to your organization to simulate real attacks.
- EVASIVE TECHNIQUES:**
 All tactics utilized during the opportunistic attacks are evasive in nature. There will be no vulnerability scanning or obvious sign that we are conducting operations.
- REPORTING:**
 At the conclusion of each performance period, Optiv will provide a debrief on the attack(s) that includes a detailed attack scenario, successful defensive actions, and suggested remediation.

Benefits of Always-On Penetration Testing

Increased Confidence in Defensive Capabilities

There are only two ways to know how defenders and controls can respond to an attack. Either they are attacked by a malicious attacker or from a non-malicious offensive security team. Optiv suggests the latter.

Prioritize and Tune Detection Capabilities

We use time-stamped testing results to enable the correlation and fine tuning of your detection and response capabilities.

Mature Penetration Testing Program

Always-On Penetration Testing provides the framework for a formal program that can include compliance testing, endpoint assessments, and full Optiv Breach Simulation.

Focus Your Security Teams

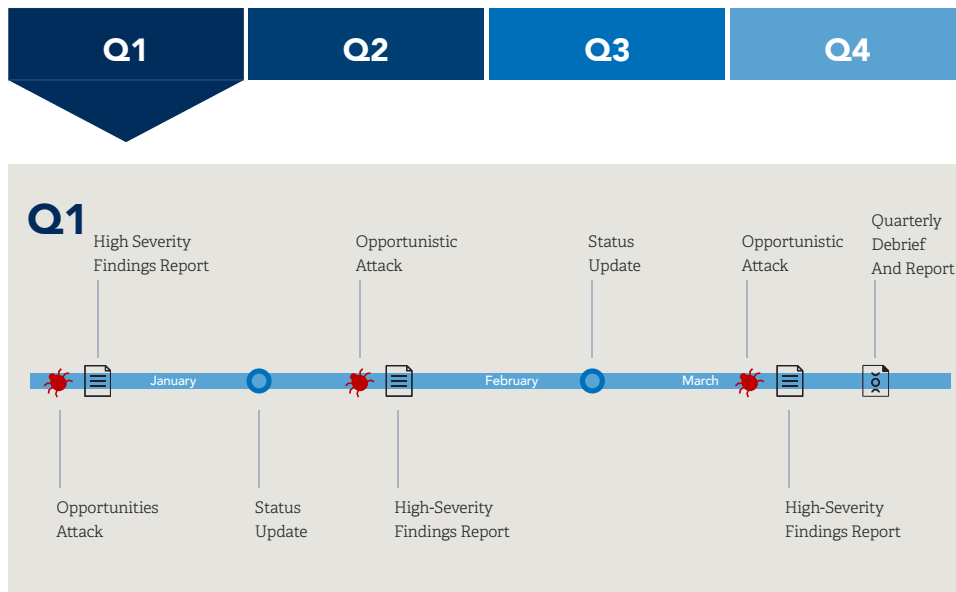
Ongoing preparation and testing for inevitable attacks keeps your defenders focused and ready.

Start Practicing Like You Fight

Attackers are not going to give notice. Your defenders need to be constantly ready. Optiv's offensive security specialists provide a friendly adversary in the fight who also provide concise and programmatic guidance.

Ongoing Flow of Testing in Real Time

Optiv's Attack and Pen (A&P) team is leading the industry in tradecraft advancement and methodology. Optiv's A&P consultants focus solely on being objective offensive security experts, rather than asking clients to meet certain administrative or project management requirements. Our team of specialists provides a wide variety of offensive solutions from standard vulnerability scans to nation state level breach assessments.



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.



1144 15th Street, Suite 2900
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](https://twitter.com/optiv), www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

© 2018 Optiv. All Rights Reserved. Optiv is a registered trademark of Optiv Security Inc.