Attack and Penetration

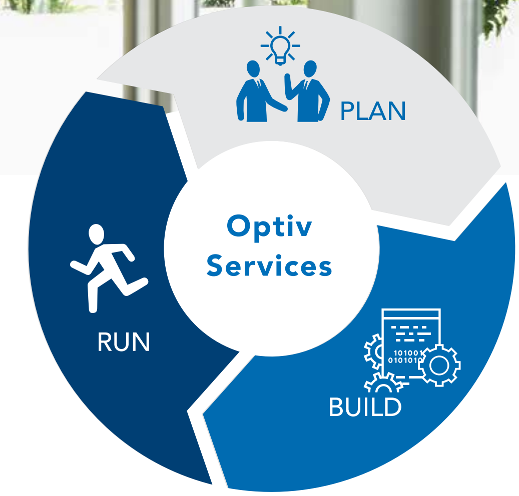
Third-Party Validation of Your Existing Security Defenses

Despite millions of dollars, thousands of man hours, and scores of technologies most organizations spend on securing their IT environments, vulnerabilities are ever-present. With new applications, network devices, and systems coming online every day and the frequent configuration changes to keep all of it operational, a single change can undermine your existing defenses and introduce new vulnerabilities that can remain hidden from even the most sophisticated vulnerability scanning tools.

Optiv has helped thousands of organizations reduce the risks around their ever-changing environments. With a proven methodology to identify, analyze, and prioritize new and existing vulnerabilities, we validate and help ensure your layered security defenses continue to protect against external and internal threats and meet compliance requirements. Whether you require white, grey, or black box services, we provide peace of mind with experienced third-party validation of your extended security environment.

Why Choose Optiv Attack and Penetration Services

- **Proven Experience** – Our Attack and Penetration consultants bring unrivaled experience to address the unique needs of organizations of all sizes and industries
- **Risk-Based Insight** – We analyze all relevant technical and business implications to ensure our recommendations and outcomes align with your specific risk profile
- **Parallel Testing** – Our specialists use a variety of commercial and open source tools for complete and methodical assessment results
- **Flexibility** – We use an adaptable approach and methodology to meet your organization's distinct business requirements
- **Detailed Action Plan** – We provide a detailed roadmap and specific steps to strengthen your overall security program and defense posture



Optiv Services

Optiv provides a wide range Attack and Penetration Testing services and offers the expertise to help plan, build and run your Threat and Vulnerability Management program.

PLAN

Adversarial Breach Simulation – Using deception and distraction while identifying points of weakness, we exploit data and mimic an actual breach.

Vulnerability Assessment - Comprehensive evaluation of your security controls to identify weaknesses and provide detailed recommendations for mitigation.

Penetration Testing – Through simulated attack scenarios, we exploit vulnerabilities in critical systems to breach the organization and identify weaknesses for remediation. Pen Test services include:

- Target Pen Testing
- Comprehensive Pen Testing
- Physical Security Pen Testing
- Specialized Pen Testing

Social Engineering – We perform a variety of methods to identify the "human element" risk introduced by your employees.

VoIP Technology Assessment – Assessment of Voice over Internet Protocol solutions to identify vulnerabilities common in network devices.

War Dialing Assessment – Optiv experts simulate a war dialing attack to locate available modems and identify security gaps.

Wireless Security Assessment – We execute a vulnerability assessment on your wireless network to uncover weaknesses that could lead to a security incident.

BUILD

Product Security Assessment – Comprehensive security assessment for new products (single devices and entire systems of devices) to identify weaknesses and potential attack vectors.

Breach Response Wargame – Optiv offensive security experts conduct covert-to-overt attacks to trigger real-time Incident Response processes and work closely with clients to improve their response programs.

RUN

Vulnerability and Attack Surface Management – Services for managing or supplementing a client's vulnerability management program by implementing offensive security methods and a regular cadence of testing to maintain a secure attack surface across your environment.

Always On Penetration Testing – Service providing on-going protection with offensive attacks from anonymous, non-attributable environments conducted randomly by Optiv experts throughout defined testing cycles.

Public Information Profile – Utilizing public information, our experts create a profile on your organization and individuals to identify security concerns.

OPTIV

1144 15th Street, Suite 2900 Denver, CO 80202 | 800.574.0896 | www.optiv.com