Threat Management: Attack and Penetration
Identifying Weaknesses to Strengthen Your Security Program

Unknown weaknesses in your software, hardware and end-user environments are exploitable targets for attackers. Regular testing helps, but where does it leave your organization’s security posture if your team lacks the resources to respond to identified issues?

Optiv’s threat experts can perform both comprehensive and targeted penetration testing through adversarial simulations against your environment. From straightforward vulnerability assessments to product penetration tests and advanced breach simulations, we can help you design and implement a proactive and comprehensive threat management program to meet your adversaries head on and ensure your staff is confidently prepared in the event of an attack.

Keep it Simple
Core Offerings
Security assessments and penetration testing to identify, quantify and rank the vulnerabilities in your system

Targeted Testing
Replicate real-world attack chains to identify and focus on the chinks in your armor to understand your true exposure

Social Engineering
Evaluate user security awareness through tried-and-true pretexting methods such as spear phishing, media drops and tailgating

Prepare for the Unknown
Outside your Network
Assess physical security controls and cloud configurations to identify tangential threats to your network and information

Insider Threat (Purple Team)
Interactive engagement between advanced offensive and defensive operators that identifies and remediates critical flaws in real-time

Breach Simulation
Use proprietary technologies with evasive, non-attributable operations outside of traditional testing methodologies to assess even the most hardened security programs

Think Outside the Box
Vulnerability and Attack Surface Management
Differential testing to assess your most critical weaknesses and provide recommendations over a regular schedule

Endpoint Protection
Compare and contrast the effectiveness of selected controls to enable informed decisions about your security investments

Everything but the Kitchen Sink
Employ targeted testing to identify security flaws in products that don’t fit traditional testing methods including embedded systems, kiosks, SCADA, VDI and VoIP environments
Why Clients Choose Optiv

We deliver a security-first perspective, with a holistic approach to infrastructure and programs

**Proprietary technology** to collaborate, analyze, deliver and report on your engagements

**Manual testing and verification methods** that supplement automated scanning to ensure a comprehensive assessment of your entire security program

Dedicated teams comprised of only 4% of top applicants exclusively performing attack and penetration services

**Annual Attack and Pen Experience**
- 600+ engagements
- 108,000+ testing hours

Leverage **market-leading attack and penetration R&D** that identifies and exposes the newest attack vectors

Program-level **root cause analysis and remediation** to identify and address underlying security program deficiencies

**75% of vulnerabilities** exploited by the Optiv team were not identified by automated tools

**Industry leaders:** 50+ consultants with over 110 certifications, over 500 years combined offensive security experience

We deliver Threat Management services to >60% of Fortune 500 companies

---

Breach Simulation Methodology

**THREAT INTELLIGENCE**
- Planning and Requirements
- Collection
- Analysis and Production
- Dissemination and Integration

**THREAT MODELING**
- Determine Assets
- Understand Threat Agents
- Derive Position/Relevance
- Build Strategy
- Operationalize
- Monitor and Adapt

**RED TEAM/BREACH**
- Information Profiling
- Discovery (Passive/Active)
- Solicitation
- Exploitation/Post Exploitation
- Covert/Surreptitious
- Attack Chain Analysis

**THREAT HUNTING**
- Hypothesize
- Investigate
- Discover
- Remediate
- Augment

---

Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2020 Optiv Security Inc. All Rights Reserved.