Why Mandiant
Mandiant, a FireEye company, has over 14 years of experience at the forefront of cyber security and cyber threat intelligence. Our incident responders have been on the frontlines of the world’s most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures.

Our penetration tests leverage deep knowledge of advanced persistent threats (APTs) and attacker behavior, using the same tools, tactics and procedures (TTPs) we see every day during our incident response engagements.

Service Overview
Mandiant’s penetration tests are custom-tailored to an organization’s environment and needs, assessing specific aspects of the security program and the state of security of an organization’s critical systems, networks and applications. We take advantage of the intelligence gained from our years of experience responding to the most sophisticated threat actors worldwide.

Approach

canvass
- Understand the environment, system or application being assessed.
- Search for exploitable vulnerabilities that may exist in exposed services or APIs, applications or firmware, or social engineering.
- Attempt to exploit identified vulnerabilities using a combination of publicly available exploit code, commercial penetration testing tools and internally developed exploit code and tools.
- Gain access to the internal environment from the Internet, steal data from segmented environments, or take control of a device and issue malicious commands.

Assessments can be performed black box (starting the assessment with zero knowledge of the environment) or white box (starting with knowledge of the environment).
### Table 1. Range of customizable penetration testing services

<table>
<thead>
<tr>
<th>Penetration Test</th>
<th>Objective</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Penetration Tests</td>
<td>Identify and exploit vulnerabilities on systems, services and applications exposed to the Internet</td>
<td>Understand risk to assets exposed to the Internet</td>
</tr>
<tr>
<td>Internal Penetration Tests</td>
<td>Simulate a malicious insider or an attacker that has gained access to an end-user system, including escalating privileges, installing custom-crafted malware or exfiltrating faux critical data</td>
<td>Understand risk from a breach</td>
</tr>
<tr>
<td>Web Application Assessments</td>
<td>Comprehensively assess web or mobile applications for vulnerabilities that can lead to unauthorized access or data exposure</td>
<td>Understand the security of applications that broker access to critical data</td>
</tr>
<tr>
<td>Mobile Device Assessments</td>
<td>Comprehensively assess the security of mobile devices and installed applications</td>
<td>Understand risk introduced to an organization through newly developed mobile applications or company-issued cell phones</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Assess the security awareness and general security controls with respect to human manipulation, including email, phone calls, media drops and physical access</td>
<td>Understand how an organization reacts to exploitation of human beings</td>
</tr>
<tr>
<td>Wireless Technology Assessments</td>
<td>Assess the security of your deployed wireless solution (e.g., 802.x, Bluetooth, Zigbee, etc.)</td>
<td>Understand how secure data in transit and systems communicating via wireless technology actually are</td>
</tr>
<tr>
<td>Embedded Device Internet of Things (IoT) Assessments</td>
<td>Assess the security of your device by attempting to exploit the embedded firmware, control the device by passing or injecting unsolicited malicious commands, or modify data sent from the device</td>
<td>Understand the security of devices and the ability to guarantee that the commands issued to and information received from the device are legitimate</td>
</tr>
<tr>
<td>ICS Penetration Tests</td>
<td>Combine penetration testing and exploitation experience with ICS expert knowledge to prove the extent an attacker can access, exploit or otherwise manipulate critical ICS/SCADA systems</td>
<td>Understand the vulnerabilities in an ICS environment before an attacker exploits them</td>
</tr>
</tbody>
</table>

### WHAT YOU GET

- Summary for executive- and senior-level management
- Technical details that include enough information to recreate our findings
- Fact-based risk analysis to confirm a critical finding is relevant to the targeted environment
- Tactical recommendations for immediate improvement
- Strategic recommendations for longer-term improvement

Suspect an incident? Email us at investigations@mandiant.com or visit https://www.fireeye.com/company/incident-response.html

---

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. M-EXT-DS-US-EN-000016-02

**FireEye, Inc.**

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

**About FireEye, Inc.**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.