ThreatSpace is a technology-enabled service that allows your organization to assess and develop its security team’s ability to respond to real-world threats in a consequence-free environment. Using a virtualized environment that simulates typical IT infrastructure such as network segments, workstations, servers and applications, teams use ThreatSpace to assess their technical capabilities, processes and procedures as they investigate simulated attack scenarios.

The scenarios, based on Mandiant’s extensive incident response experience responding to thousands of breaches, include the latest adversary tactics, techniques and procedures (TTPs) and test an organization’s ability to detect, scope and remediate a targeted attack. Throughout the process Mandiant incident response experts provide real-time feedback and coaching to help improve your security team’s ability to respond to cyber attacks.

Our analysis-focused and technology-agnostic approach tests your security team’s ability to identify and prioritize systems and forensic artifacts to analyze including:

- Affected systems, networks, user accounts and applications
- Malicious software and exploited vulnerabilities
- Information accessed and/or stolen

ThreatSpace scenarios go through all phases of the targeted attack life cycle.

**Figure 1. Attack lifecycle.**
Service Delivery
Remote Preparation

Identify scenarios
Review goals, expectations and logistics
Discuss incident response processes and procedures

Remote
Scenario identification and range configuration

Onsite: 1/2 day
Team preparation and range familiarization

Onsite: 2 days
Hands-on scenario investigations

Onsite
Scenario debriefs

Figure 2. Workflow for remote preparation and onsite service delivery.

Onsite Scenarios
- Half-day training and range familiarization.
- Two days of hands-on investigation of a simulated attack that progresses through the phases of the attack lifecycle. Mandiant incident responders provide real-time feedback and coaching to your incident responders and cyber threat analysts throughout the scenario.
- Debriefs to review team achievements and strengths as well as gaps in training, processes and procedures, with recommendations for improvements.

Deliverables
After the engagement, you receive a report that identifies observed strengths and recommended enhancements to your organization's incident response capabilities.

To learn more about FireEye, visit: www.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.