ThreatSpace

Benefits

- **Identify gaps and opportunities for improvement.** Investigate real-world, complex incidents to identify gaps in training, processes, procedures, and communication plans.
- **Learn from incident response experts.** Work closely with experienced Mandiant incident responders who draw on years of intelligence-led investigative expertise to assess and provide real-time feedback and coaching.
- **Investigate critical security incidents.** Familiarize your response and intelligence teams with the latest attack scenarios and attacker TTPs relevant to your organization, as learned from Mandiant advanced persistent threat (APT) investigations.
- **Gain experience with different attack scenarios and threat actors.** Evaluate and improve the abilities of your incident response and intelligence teams as they respond to various attack scenarios and actors.
- **Research and analyze identified threats.** Learn to research attacker TTPs and identify indicators of compromise from host-based artifacts and network-based artifacts.

Practice responding to real-world threats without the real-world consequences

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 extensive Mandiant 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:

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

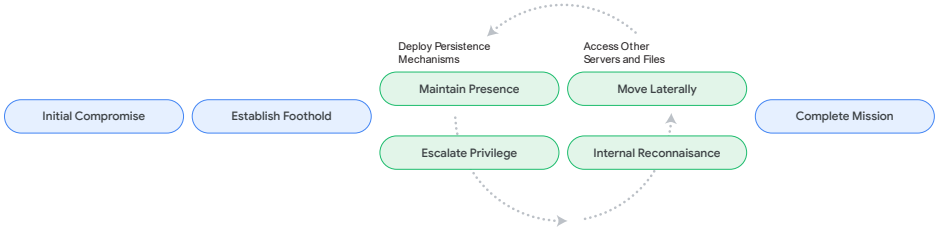

FIGURE 1. Attack lifecycle.

Service Delivery

Remote Preparation

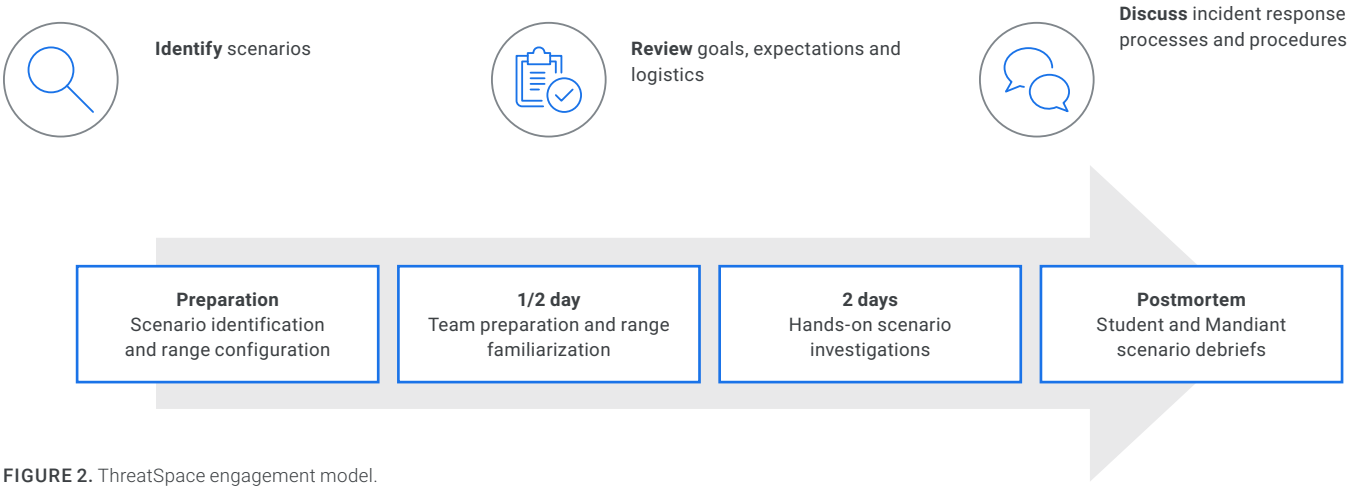

FIGURE 2. ThreatSpace engagement model.

ThreatSpace scenario samples

Reconnaissance by Insider Threat

This scenario emulates an insider threat with a valid user already on a system. This user opens a reverse shell session on the initial access host and uses it to discover information about the entire network.

Beaconer Deployment

This scenario imitates an attacker gaining access to a host via a spearphishing attachment. It opens a bypass session on that host and gathers information and deploys a beacon.

Ransomware

A domain user is compromised allowing the threat to access the system before moving laterally, conducting internal reconnaissance and establishing persistence. Once initial compromise is secured, the attacker deploys ransomware and runs malware on multiple mission critical systems.

Active Directory

A threat actor gains access to a host and begins discovery before conducting a Kerberoast attack and further reconnaissance of the domain. The actor then compromises the domain controller, exfiltrates passwords and disrupts normal business operations.

Deliverables

- 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, and processes and procedures, with recommendations for improvements.

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