Mandiant

Datasheet

ThreatSpace™ Cyber Range

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 cyber range that assesses and develops your security team's technical capabilities, processes, and procedures when responding to real-world cyber threats. The scenarios are based on extensive Mandiant incident response experience from responding to thousands of breaches and include the latest adversary tactics, techniques, and procedures (TTPs).

This is done in a consequence-free environment, through a simulated infrastructure that includes network segments, servers, and applications.

Students investigate and respond to simulated attacks with real-time coaching from our expert instructors. Your team will receive feedback on their strengths and weaknesses, along with an actionable best-practices roadmap for improvement.

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.

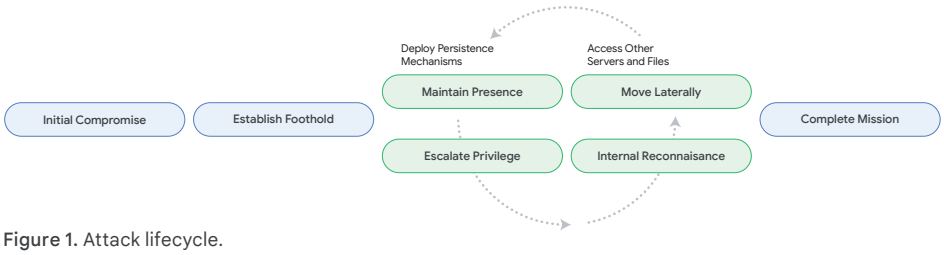

Figure 1. Attack lifecycle.

Service Delivery

Remote Preparation

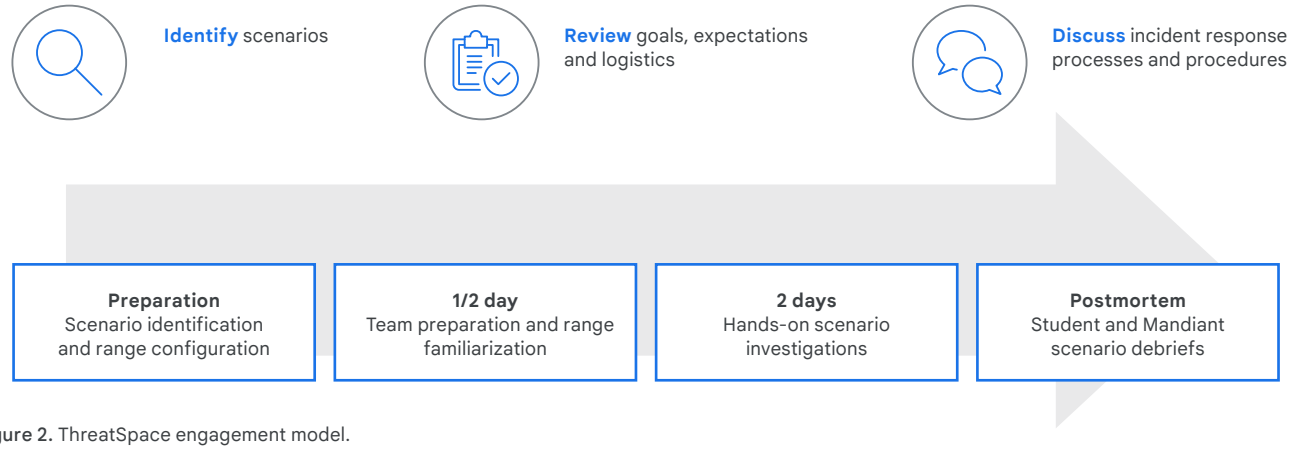

Figure 2. ThreatSpace engagement model.

ThreatSpace scenario samples

While these are our most popular exercises, we can also develop custom scenarios to address your unique challenges.

Insider threat

This multi-level scenario simulates an insider threat, from an employee misusing standard permissions to one acting under the direction of an external threat actor to exfiltrate data.

Phishing and deployment of ransomware

This scenario starts with a phishing attack to gain access, then moves to privilege escalation, data exfiltration, and finally, ransomware deployment on key systems.

Compromise through malicious download

A scenario where a threat actor uses a compromised website to deliver malware. This allows the attacker to establish a foothold, maintain persistence, and conduct reconnaissance.

Unauthorized access and data theft

This multi-level scenario involves an attacker exploiting a public-facing service to gain access, and then moving laterally to target Active Directory, compromise critical assets, and exfiltrate data.

Threat actor emulation

Live scenarios simulate the latest adversary TTPs to challenge your team's detection and response capabilities. We emulate real-world threat actors, from financially motivated criminals like FIN6 and Lapsus$ to state-sponsored groups like APT40 and APT41 engaged in espionage and service disruption.

Threat Hunting with Google

This workshop focuses on the top ten MITRE ATT&CK techniques identified in the latest Mandiant M-Trends report. Learn how to identify critical artifacts, apply detection methods, and actively engage across the six critical functions of Cyber Defense: Intelligence, Detect, Respond, Validate, Hunt, and Mission Control.

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.