Datasheet

Mandiant

ThreatSpace™: Threat Hunting with Google

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

ThreatSpace: Threat Hunting with Google covers the fundamentals of each MITRE top ten techniques identified by Mandiant M-Trends report, including artifact examples and methods for detection and engagement.

Learners are invited into the ThreatSpace range for the practical application of finding artifacts associated with the techniques to uncover threat actor activity. Throughout the course, learners will gain hands-on experience hunting for threat actor activity and will be able to apply these skills in their daily operations. ThreatSpace is an engaging state-of-the-art cyber range using Google Cloud Security tools and a virtualized enterprise within Google Cloud for detecting and responding to threat actor activities. In this delivery, security professionals access a virtual environment that simulates real-world IT infrastructure, including network segments, workstations, servers, and applications. This environment enables responding to cyber threats in a controlled environment without incurring actual consequences.

This engagement is intended for individuals with some knowledge in security operations, incident response, analysis, network traffic, security architecture, or system administration duties. This engagement can be delivered virtually, or onsite at customer's location.

Benefits:

- Improve individual skills by investigating real-world, complex incidents in a controlled environment, discussing triage processes, and response procedures.

- Learn from incident response experts who draw on years of intelligence led investigative expertise to assess and provide real-time feedback and coaching.

- Experience critical security incidents based on the latest attack scenarios and attacker TTPs.

M-Trends 2025 Top 10 Techniques*

1. T1059: Command and Scripting Interpreter
2. T1027: Obfuscated Files or Information
3. T1021: Remote Services
4. T1083: File and Directory Discovery
5. T1070: Indicator Removal
6. T1082: System Information Discovery
7. T1140: Deobfuscate/Decode Files or Information
8. T1486: Data Encrypted for Impact
9. T1071: Application Layer Protocol
9. T1133: External Remote Services

* M-Trends 2025 has a tie for ninth place to make out the top 10 techniques