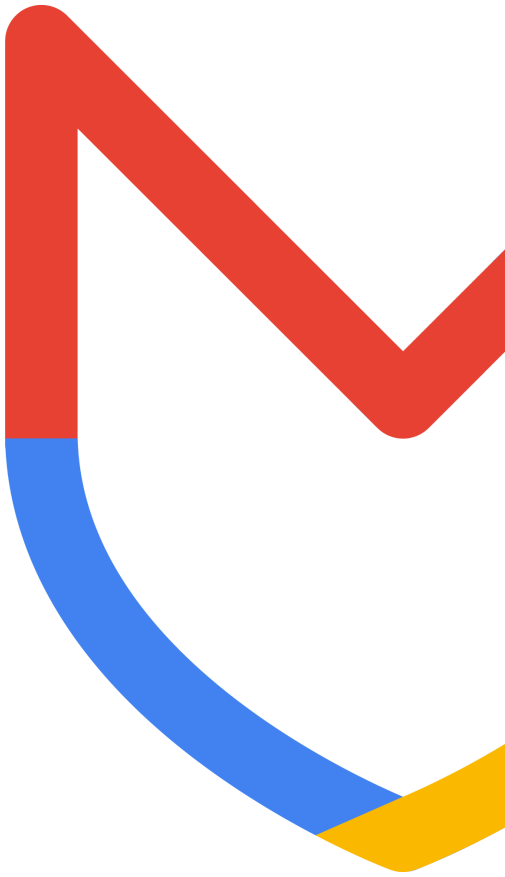
Google Cloud
Security

ThreatSpace™

Catalog - 2026



For more information visit https://cloud.google.com/learn/security/mandiant-academy-threatspace

Mandiant

Welcome to ThreatSpace™ 2026

On behalf of Mandiant, a Google Cloud company, I am pleased to present this catalog for ThreatSpace. We understand cyber drills, and fighting an asymmetrical battle often against unknown adversaries with seemingly limitless resources. This engagement can be incorporated into workforce readiness programs and maturity journeys to support in preparing for these challenges.

Mandiant is the globally renowned Incident Response and Cyber Security company, and we help organizations around the world develop and uplift cyber capabilities and respond when incidents occur. We know more about cyber security incidents because:

- We respond to the world's largest, most complex and most important breaches in the world giving us real world insight into the minds of the hackers and defenders, their tooling, tactics, techniques and procedures.
- Mandiant Intelligence tracks cyber actors all around the world, modelling worldwide cyber activity and engaging with cyber actors on the dark web or wherever else they may be, and
- Mandiant fuses this intelligence into all our products giving us a truly intelligence led capability where we know more about the attackers than anyone else.

We believe Threatspace will help your staff gain the confidence and experience to tackle cyber security incidents and experience real world threats enhancing their readiness now and in the future.

If you have any questions after reviewing this catalog, please contact me. Furthermore, please let me know if there is anything more that Mandiant can do to support you during the decision-making process.

I look forward to supporting your ongoing dedication to this mission.

Sincerely,

Nadean H. Tanner
Head of ThreatSpace
Technical Director
Mandiant, a Google Cloud Company
nadeantanner@google.com

Executive Summary

Mandiant is proud to present this ThreatSpace catalog, designed to strengthen your organization's cybersecurity readiness. Through this cyber range, we aim to provide an environment that sharpens your resilience against the most pressing cybersecurity threats. Our extensive expertise across diverse industry segments enables us to understand the unique cybersecurity challenges you face and provide targeted, effective solutions. We are committed to being your trusted partner as you navigate the complexities of safeguarding your critical infrastructure.

ThreatSpace is a technology-enabled, hands-on cyber range that allows an organization to assess and develop its security team's ability to respond to real-world threats. Using a virtualized environment that simulates typical IT infrastructure with network segments, workstations, and servers, teams will exercise their analysis skills, and response processes and procedures as they investigate simulated attack scenarios. ThreatSpace offers a unique experience for organizations to look to reduce the complexity and burden of improving and assessing their security team's maturity to prepare for, detect and respond to cyber-attacks.

ThreatSpace Options

Whether you are seeking to enhance your team's core defensive capabilities, build incident response skills with guided instruction, or provide a comprehensive, immersive experience that challenges the full spectrum of your security team's abilities, ThreatSpace has an option to fit your needs. Each is defined in the catalog.

ThreatSpace

A customizable delivery that can be tailored to organizational priorities and existing skill levels. Live scenarios in the range simulate the latest adversary tactics, techniques, and procedures (TTPs), challenging an organization's ability to detect, scope, and remediate a targeted attack.

Threat Hunting with Google

A set delivery covering the M-Trends top techniques and sub-techniques as identified by Mandiant. A workshop where attendees spend time in the ThreatSpace range with hands-on experience threat hunting. Instruction provides a lab guide for identifying techniques, the artifacts left by threat actors performing them, and potential false positives in those detections.

ThreatSpace

- **Purpose:** To provide a full-scope, immersive drill designed to mature an organization's cybersecurity capabilities progressively over three days of threat hunting.
- **Format:** Multi-day engagement that includes increasingly challenging scenarios to build team capabilities step-by-step.
- **Scope:** ThreatSpace provides exposure to a wide range of realistic threat scenarios, cutting-edge tools, intel, and techniques, all designed to push participants beyond their comfort zones.

Schedule

- **Day 1:** Scenario that includes familiarization with ThreatSpace tools and environment while working through an initial scenario to set the foundation for the engagement.
- **Day 2:** A scenario focused on specific threats, chosen from a range of industry-relevant threat options, helping teams deepen their skills.
- **Day 3:** Progressively more difficult scenario designed to be highly challenging, simulating sophisticated adversary tactics, including (but not limited to) those used by APT actors.

ThreatSpace Storyboard Example

Day 1	Time
Threatspace Course Introduction	9am
Accessing Range, Tool Intro, and Hands on Threat Hunting	9:30am
LUNCH	12pm-1pm
MITRE ATT&CK Discussion Initial Attack Tactics	1pm
Hands on Threat Hunting	1:30pm-4pm
Participant Scenario Debrief Purple Team Reveal	4-5pm
Scenario: Insider Threat	

Day 2	Time
MITRE ATT&CK Discussion Maintaining Access Tactics	9am
Hands on Threat Hunting	9:30am
LUNCH	12pm-1pm
MITRE ATT&CK Discussion Enterprise Discovery Tactics	1pm
Hands on Threat Hunting	1:30pm-4pm
Participant Scenario Debrief Purple Team Reveal	4-5pm
Scenario: 3rd Party Compromise	

Day 3	Time
MITRE ATT&CK Discussion Attacker Action Tactics	9am
Hands on Threat Hunting	9:30am
LUNCH	12pm-1pm
MITRE ATT&CK Discussion End Game Tactics	1pm
Hands on Threat Hunting	1:30pm-4pm
Participant Scenario Debrief Purple Team Reveal	4-5pm
Scenario: Ransomware	

Evaluation

Throughout the immersive engagement, Mandiant incident response and intelligence experts provide real-time feedback and coaching to improve team communication, threat hunting, and remediation skills. Our analysis-focused and technology-agnostic approach empowers security teams to identify attacker activity, prioritize systems for response, and analyze live-response artifacts. At the conclusion of an engagement, Mandiant delivers actionable feedback to help pinpoint areas of strength and opportunities for improvement, ensuring the security team can effectively enhance their incident response capabilities based on these criteria.

Evaluation Criteria	Description
Communication	Evaluate internal and external information exchanges during the incident and the debrief.
Technical Response	Assess the technical prowess and skills of the team during the event based on the incident response life cycle.
Operational Response	Analyze procedural adherence by following set protocols during the event from detection to containment to remediation.
Intelligence Integration	Evaluate the team's ability to request and assimilate threat intelligence on malware, threat groups, and other indicators.
Adversarial Learning	Assess the team's ability to determine and adapt to the adversary's tactics throughout the event.

ThreatSpace Scenarios

ThreatSpace offers a multitude of threat scenarios available for delivery in the engagement. These scenarios focus on key TTPs threat actors use during the specific compromise. Most scenarios can be adjusted to fit a specific difficulty level. This is usually determined during the engagement, based on the skills and abilities of the team observed by the coaches. A beginner difficulty level will include almost all activity done on disk and recorded in the available logs. Normally, the exercise delivered on day one will be a beginner level difficulty to evaluate the team's capabilities. The other end of the difficulty scale is advanced. The advanced difficulty includes almost all actions performed in memory, leaving little evidence of their actions on disk, thus relying on other logs and sources for evidence of compromise. Intermediate difficulty will leave some key items on disk but start to perform operations in a way to leave little evidence on disk.

Malicious Download

In this scenario, a threat actor leverages a website to deliver malware to a user's system. Once executed, the malware establishes a covert foothold and creates a communication channel back to the threat actor. This access allows the threat actor to maintain persistence on the compromised machine and begin reconnaissance, and potentially the network for valuable information and further opportunities.

Website Compromise

This scenario depicts a threat actor exploiting a vulnerability in a public-facing service web server to gain initial access into the network. From this initial foothold, the threat actor works to escalate their privileges and move laterally. They perform reconnaissance to identify valuable accounts and systems. The threat actor then compromises critical assets, ultimately leading to the exfiltration of sensitive data.

3rd Party Compromise

This scenario emulates an attack where a threat actor breaches the network by compromising a trusted partner or third-party vendor with existing access. The threat actor establishes a secure and covert channel back to their infrastructure. Once inside, they move to compromise internal systems, systematically searching for sensitive data, and prepare it for exfiltration. The scenario culminates with the threat actor stealing staged data using encrypted methods, highlighting the risk posed by compromised external relationships.

Phishing Compromise

This scenario begins with a threat actor gaining initial access through a targeted phishing campaign, utilizing various lures such as malicious attachments or links. Upon successful execution on a user's system, the threat actor establishes a persistent presence and a covert communication channel. The threat actor then works to elevate their privileges, aiming for lateral movement to critical systems.

Developer Compromise

This scenario emulates a user downloading a malicious extension which compromises the device. With this access, the threat actor then performs discovery which leads to privilege escalation and lateral movement throughout the network. Ultimately access to critical systems results in stealing of data and impact to the organization.

Insider Threat

This scenario shows the actions of an insider threat operating with legitimate user access within the network. It depicts an employee utilizing their standard permissions to perform malicious activities, potentially accessing, modifying, or attempting to exfiltrate sensitive internal data. Depending on difficulty level, this may include the insider working with an external threat actor which scales up the impact. This highlights the risks posed by trusted individuals acting against the organization's interests illustrating the challenges of detecting insider threats.

ThreatSpace Threat Actors

ThreatSpace offers a selection of known threat group scenarios. These scenarios focus on specific TTPs the threat groups used in their campaigns. ThreatSpace does not cover every possible campaign, and the team built the scenarios out based on capabilities and techniques that can be demonstrated in the range. The range does use the same IP addresses, domains, and where possible the same hashes used by the threat groups to provide a chance for the attendees to attribute the scenario to the threat group. As before, the difficulty level of these groups can be adjusted during the delivery based on the coaches observations of the attendees. However, most threat groups in this section use techniques in the intermediate to difficult side of the scale.

UNC Groups - Uncategorized

UNC3236 (Volt Typhoon)
UNC3236 is a suspected China-nexus cluster of activity that has been active since at least May 2020. The threat group heavily relies on Living Off The Land (LOTL) techniques, leveraging legitimate system tools and infrastructure to blend in. Through these stealthy methods, the adversary focuses on collecting sensitive information, including intellectual property, and actively works to remove indicators of their presence to maintain long-term, undetected access.

UNC3569 (Cinnamon Tempest)
UNC3569 is a suspected China-nexus cyber actor of unknown motivation. The threat group has used multiple malware variants and has leveraged public vulnerabilities. Reportedly, they deployed a variety of ransomware payloads in affected environments and ostensibly has historical infrastructure links to a backdoor used to enable Chinese espionage operations.

UNC3661 (Lapsus$)

UNC3661 is a threat group active from at least mid-2021 to late 2022 that appeared to be motivated by both financial gain and a desire for notoriety. While the threat group stole data from victims and attempted to monetize it by extorting the compromised organization, it also sometimes leaked the data for free. During their intrusions, the threat group relied mainly on stolen credentials to access corporate environments and several publicly available tools and utilities, as well as built-in operating system tools. The group also resorted to some attention-grabbing techniques, including public shaming, interacting with victims within the victim environment, and defacement attacks.

UNC3944 (Scattered Spider)

UNC3944 is a financially motivated threat cluster that has been active since at least early 2022 and commonly gains initial network access using stolen credentials obtained from phishing operations or through interactive social engineering of IT help desk employees. In early 2023 the associated threat actors also began to leverage access to victim environments for eventual ransomware deployment. They demonstrated a stronger focus on stealing large amounts of sensitive data for extortion purposes.

Temp.Isotope (Berserk Bear / DragonFly)

TEMP.Isotope is a cluster of cyber espionage activity that has been active since at least 2015. They rely on gaining initial access through strategic web compromises, such as watering hole attacks, and targeted spear-phishing campaigns. A consistent technical method employed by the adversary involves the abuse of Server Message Block (SMB) callouts. This technique is central to their objectives of harvesting credentials and conducting data theft for espionage purposes.

FIN Groups - Financially Motivated

FIN6

FIN6 is a financially motivated intrusion set that has operated since at least mid-2014. As of mid-2018, actors associated with the threat group began to deploy various ransomware payloads. Since at least mid-2019, FIN6 campaigns have leveraged resume-themed lures and job-themed files, which have more recently been hosted on domains that appear to be fake personal websites.

FIN11

FIN11 is a financially motivated threat group that has been active since at least 2016. In 2019 the threat group shifted to deploying ransomware and in 2020 they began conducting data theft extortion operations. In addition to adopting new monetization methods, the threat group has shifted from obtaining illicit access via malicious email campaigns to instead exploiting public-facing servers.

APT Groups - (Advanced Persistent Threat)

APT29 (Russia)

APT29 is a cyber espionage actor with a Russia nexus. The group appears to have formidable capabilities, to include a range of custom developed tools, extensive command-and-control infrastructure, and significant operational security. The threat group demonstrated a high regard for operational security but were also fairly aggressive in their continued operations and efforts to evade investigators and remediation attempts.

APT40 (China)

APT40 is a Chinese cyber espionage group that has been active since at least 2013. The threat group creates infrastructure mimicking agencies, defense contractors, and multinational corporations to provide operational relevance and legitimacy. The threat group has used a variety of tactics and techniques and a large library of custom and open-source malware to establish initial access, enable lateral movement, and locate high value assets in order to exfiltrate data.

APT41 (China)

APT41 is a Chinese state-sponsored espionage group that also conducts financially motivated activity for personal gain. The threat group has used spear-phishing campaigns which led to system compromise through the download and execution of payloads. The threat group also carried out operations for financially motivated intrusions as well as to steal source code and digital certificates.

APT43 (DPRK)

APT43 is a prolific cyber operator that supports the interests of the North Korean regime. The group combines moderately sophisticated technical capabilities with aggressive social engineering tactics. In addition to its espionage campaigns the threat group is believed to fund itself through cyber crime operations to support its primary mission of collecting strategic intelligence. The group creates numerous spoofed and fraudulent personas for use in social engineering.

APT44 (Russia)

APT44 is a dynamic and operationally mature threat actor that has carried out the full spectrum of espionage, influence, and attack operations since as early as 2009. The group's long-standing center focus has been Ukraine, where it has carried out a campaign of disruptive and destructive attacks. Beyond Ukraine, the group continues to sustain espionage operations that are global in scope and illustrative of the Russian military's far-reaching ambitions and interests in other regions.

APT45 (DPRK)

APT45 is a moderately sophisticated cyber operator that supports the interests of the Democratic People's Republic of Korea (DPRK). APT45 initially engaged in traditional cyber espionage activity targeting government and defense entities and subsequently expanded its remit to the financial vertical and suspected ransomware development. The threat group relies on a mix of publicly available tools, malware modified from publicly available malware, and custom malware families.

Threat Hunting with Google

- **Purpose:** To improve technical incident response knowledge, skills, and abilities in a guided setting.
- **Format:** Two-day instructor-led workshop includes a blend of lectures and hands-on labs focusing on detecting the top MITRE ATT&CK techniques and sub-techniques as defined in M-Trends. The workshop also includes additional popular tactics and techniques used by threat actors. This workshop can be delivered in-person or virtually and publicly or delivered as a private session to an organization.
- **Scope:** Threat Hunting with Google uses a cyber range to experience real-world attack scenarios to rehearse and refine incident response capabilities.

What You Get:

- Two hands-on days to sharpen response knowledge, skills, and abilities
- Facilitation from subject matter experts
- 39 different techniques covered across 12 different tactics

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.

**M-Trends 2026 will debut in April 2026 and content will be updated at that time.