Google Cloud
Security

ThreatSpace

Catalog - 2025

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

Welcome to ThreatSpace

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 drill, 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 drill 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 single 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.

Engagements are customizable and 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.

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 this 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 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.

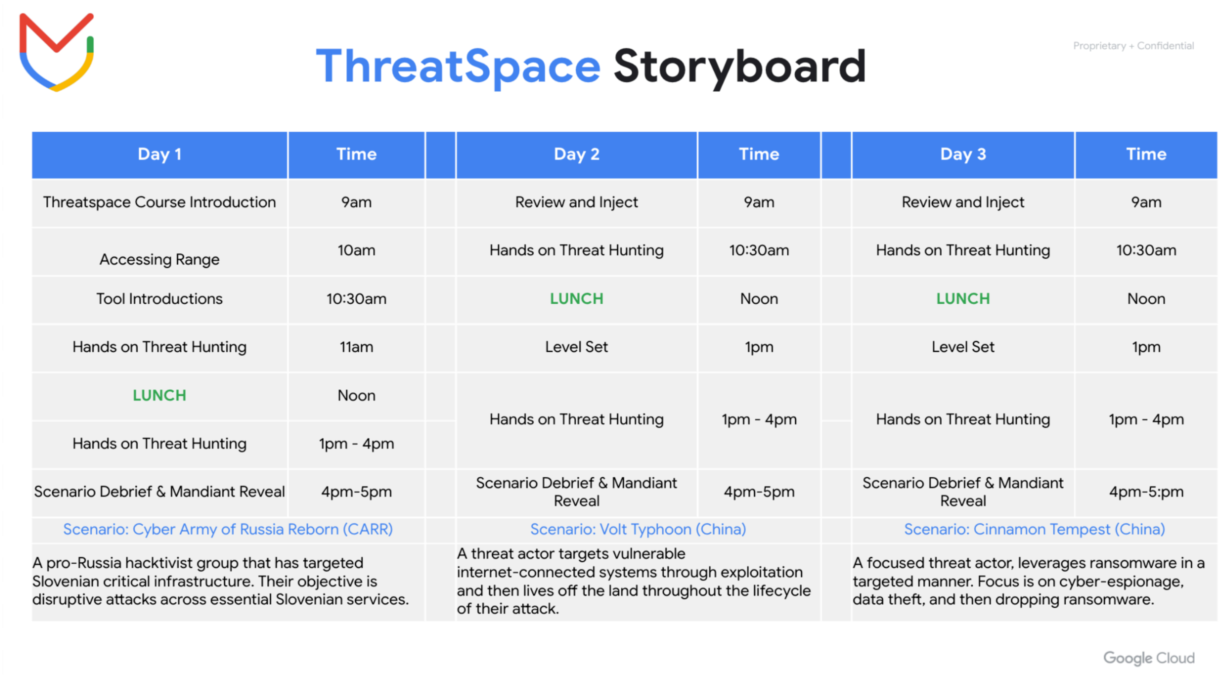
Option 1: ThreatSpace

- **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.

What You Get:

- **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 understanding.
- **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.



Proprietary + Confidential

ThreatSpace Storyboard

Day 1	Time	Day 2	Time	Day 3	Time
Threatspace Course Introduction	9am	Review and Inject	9am	Review and Inject	9am
Accessing Range	10am	Hands on Threat Hunting	10:30am	Hands on Threat Hunting	10:30am
Tool Introductions	10:30am	LUNCH	Noon	LUNCH	Noon
Hands on Threat Hunting	11am	Level Set	1pm	Level Set	1pm
LUNCH	Noon	Hands on Threat Hunting	1pm - 4pm	Hands on Threat Hunting	1pm - 4pm
Hands on Threat Hunting	1pm - 4pm				
Scenario Debrief & Mandiant Reveal	4pm-5pm	Scenario Debrief & Mandiant Reveal	4pm-5pm	Scenario Debrief & Mandiant Reveal	4pm-5:pm
Scenario: Cyber Army of Russia Reborn (CARR)		Scenario: Volt Typhoon (China)		Scenario: Cinnamon Tempest (China)	
A pro-Russia hacktivist group that has targeted Slovenian critical infrastructure. Their objective is disruptive attacks across essential Slovenian services.		A threat actor targets vulnerable internet-connected systems through exploitation and then lives off the land throughout the lifecycle of their attack.		A focused threat actor, leverages ransomware in a targeted manner. Focus is on cyber-espionage, data theft, and then dropping ransomware.	

Google Cloud

Option 2: 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.

Threat Scenarios

Compromise via Malicious Download	
Difficulty	Beginner
	In this scenario, a threat actor leverages a compromised website to deliver malware to an unsuspecting user's system. Once executed, the malware establishes a covert foothold and creates a communication channel (beacon) 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.

Unauthorized Access and Data Theft	
Difficulty	Beginner / Intermediate / Advanced
	This scenario depicts a threat actor exploiting a vulnerability in a public-facing service, such as a web server or router, 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, potentially targeting Active Directory to identify valuable accounts and systems. The threat actor then compromises critical assets like database servers and domain controllers, ultimately leading to the exfiltration of sensitive data. This scenario simulates the preparatory steps often taken by attackers before deploying ransomware.

Trusted Partner/3rd Party Compromise	
Difficulty	Beginner / Intermediate
	This scenario simulates a sophisticated 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 and Deployment of Ransomware	
Difficulty	**Intermediate**
	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. They then work to elevate their privileges, aiming for high-level credentials, and move laterally through the network, targeting critical infrastructure like domain controllers. The scenario progresses to include the exfiltration of sensitive data before the threat actor executes the final stage: deploying ransomware on key systems to cause widespread disruption and impact availability.

Insider Threat	
Difficulty	**Multi-level (Beginner to Advanced)**
	Beginner: This scenario simulates 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. This highlights the risks posed by trusted individuals acting against the organization's interests. **Advanced:** This more advanced scenario involves an employee acting under the direction of an external threat actor. It simulates the employee establishing covert communication with the threat actor via a secure channel and being guided to systematically locate and exfiltrate sensitive data. The data theft is conducted using uncommon protocols designed to evade standard monitoring, illustrating the challenges of detecting coordinated insider threats with external backing.

Election Security	
Difficulty	Multi-level (Beginner to Advanced)
	This three-day immersive engagement helps participants understand the purpose and roles of various election systems (such as the Voter Registration System, Election Management System, and Vote Tallying). The exercise focuses on detection, mitigation, and response processes the blue team must engage in when facing threats, without real-world attribution or political discussions. **Day 1: Disenfranchising the Voter Base** Objective: Simulate an attack on the voter registration system to disrupt voters' ability to participate by manipulating or deleting voter data. **Day 2: Election Management System (EMS) Compromise via Phishing** Objective: Simulate a phishing attack targeting election staff to gain unauthorized access to the EMS. **Day 3: Vote Tallying and Reporting System** Objective: Simulate an attack on vote tallying and/or reporting systems to manipulate election results and alter public reporting.

Threat Actor Emulation

APT40 (China)	
Difficulty	Intermediate / Advanced
	The adversary gains initial access and establishes a persistent foothold within the network. Following this, they conduct detailed network enumeration to map the environment and identify targets. The threat actor then moves to acquire high-level privileges, including domain administrator credentials, enabling them to compromise critical data repositories, specifically focusing on database exfiltration. The simulated attack concludes with the initiation of service disruptions, reflecting the multi-objective nature often observed with this group.

APT41 (China)	
Difficulty	Intermediate / Advanced
	The adversary commences with initial access gained through a phishing campaign. Following successful compromise, the threat actor bypasses user controls and introduces additional malicious tools and files into the environment. The adversary then leverages legitimate protocols like RDP for lateral movement across the network. A key objective is the compromise of domain credentials, achieved through techniques such as performing a DCSync attack to obtain information for all domain accounts. The final stage involves the widespread execution of ransomware, impacting systems across the domain.

APT29 (Russia)	
Difficulty	Advanced
	The adversary gains initial access into the network and quickly leverages legitimate system tools, such as PowerShell, to harvest domain credentials. Demonstrating their focus on stealth and persistence, the threat actor establishes novel persistence mechanisms, including the compromise and addition of devices configured for ActiveSync. They also utilize common utilities like 7-Zip as part of their operational setup within the environment, maintaining a covert and persistent presence to achieve their objectives.

FIN6	
Difficulty	Advanced
	The adversary gains initial access into the network. Upon establishing a foothold, the adversary performs rapid reconnaissance to understand the environment and identify valuable targets and pathways. They then focus on identifying and exploiting privilege escalation opportunities to gain higher levels of access, enabling swift lateral movement across the network. The ultimate objective of the adversary in this scenario is the execution of ransomware across targeted systems for financial gain.

FIN11	
Difficulty	Intermediate / Advanced
	FIN11 typically initiates its attacks through high-volume phishing campaigns or by exploiting vulnerabilities, often casting a wide net before selecting specific victims. Once initial access is achieved, the group employs various malware, including ransomware like CLOP, to move laterally, steal sensitive data, and disrupt operations. Ultimately, FIN11's primary objective is financial gain, achieved through deploying ransomware, extorting victims by threatening to publish exfiltrated data, or a combination of both tactics.

VoltTyphoon	
Difficulty	Advanced
	The adversary, a state-sponsored threat actor known for targeting U.S. critical infrastructure, gains access and establishes a covert presence. They utilize web shells for persistent access and heavily rely 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.

Lapsus$	
Difficulty	Advanced / Expert
	The adversary specializes in leveraging social engineering and other access methods, primarily for the purpose of extortion. Their attacks target various sectors and often involve disruptive actions designed to pressure victims. These actions can include defacing websites, causing loss of control by removing administrative accounts, and in some instances, deploying ransomware, all aimed at forcing compliance with their demands.

Cyber Army of Russia Reborn	
Difficulty	Intermediate / Advanced / Expert
	The adversary is a pro-Russia hacktivist threat actor demonstrating capabilities and targeting aligned with state interests, particularly posing a risk to Operational Technology (OT) environments. The adversary explicitly targets internet-accessible OT assets, showcasing the ability to gain access and manipulate these critical systems. Their typical activities include conducting disruptive Denial-of-Service (DDoS) attacks and using platforms like their Telegram channel for communication and broadcasting their actions.

Cinnamon Tempest	
Difficulty	Advanced
	The adversary is a focused threat actor whose operations involve a distinct multi-stage approach. Their initial focus is on cyber-espionage and the systematic theft of data. Following these objectives, the adversary then leverages ransomware, deploying it in a targeted manner within the compromised environment.

DragonFly (Berserk Bear / Temp.Isotope)	
Difficulty	Advanced
	The adversary represents a cluster of cyber espionage activity, active for many years. 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.

APT44 (Voodoo Bear,Sandworm)	
Difficulty	**Advanced/Expert**
	The adversary, the advanced persistent threat group APT44, focuses this attack campaign on entities in Eastern Europe. The attack chain begins with the deployment of a stealthy backdoor onto a target system. This backdoor is designed to collect detailed system information, identify the compromised user and machine, and establish communication with the adversary's command-and-control (C2) infrastructure to transmit the gathered intelligence.