



MITRE | ATT&CK[®]

SIMULATION SCENARIOS

A joint initiative between CYBER RANGES and MITRE Engenuity, giving learners access to the CYBER RANGES next-gen cyber range platform

CYBER RANGES fully supports ATT&CK[®] across its entire cyber range architecture



On April 19th 2022 MITRE Engenuity, MITRE's tech foundation for public good, announced that MITRE ATT&CK Defender™ (MAD), the cybersecurity community's MITRE ATT&CK® training and certification program, is to launch new Purple Teaming offerings, including threat hunting and adversary emulation credentials along with version 2.0 of its platform, now with a cyber range, to empower threat-informed defenders.‡

This has been made possible thanks to the joint initiative between CYBER RANGES and MITRE Engenuity, giving learners access to the CYBER RANGES next-generation cyber range platform.

Through public-private partnerships and federally funded R&D centers, MITRE Engenuity works across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.



The MAD certification and training program, with more than 33,000 users and counting from across 90 countries and more than 1,600 companies, helps to close the persistent cybersecurity skill gap to enable defenders to gain the advantage over adversaries.

These new MAD training and certification resources come in addition to the 10 learning modules and two certifications that were already offered: ATT&CK® SOC Assessments and ATT&CK® Cyber Threat Intelligence.

With the new offerings, MAD delivers cyber practitioners the ability to demonstrate their mastery of using MITRE ATT&CK® in practical ways for SOC assessment, cyber threat intelligence, adversary emulation, threat hunting and purple teaming.



learning
modules



certifications

MITRE ATT&CK® provides a common language for each discipline to communicate with each other more effectively and better understand real-world adversary behaviors to better defend their networks and critical systems.

**MITRE
ENGENUITY**
A Foundation for Public Good

‡ <https://mitre-engenuity.org/blog/2022/04/19/mad-purple-teaming-initiatives-and-cyber-range/>

Why MITRE ATT&CK® and CYBER RANGES

- CYBER RANGES fully supports ATT&CK® across its entire cyber range architecture.
- Through its Injector Engine, CYBER RANGES automatically can emulate the latest cyber threat intelligence-based attacks, advanced persistent threats (APTs), and specific tactics and exploits.

“Not only will these hands-on training resources greatly benefit cybersecurity professionals on an individual basis, they also will provide greater peace of mind for organizations as a whole. The whole idea behind Purple Teaming is enhanced collaboration, and now, with the new training capabilities, security teams can work more closely together to successfully defend their organizations from the latest adversarial tactics and techniques.”

Chriss Knisley, General Manager, MITRE ATT&CK Defender™, MITRE Engenuity

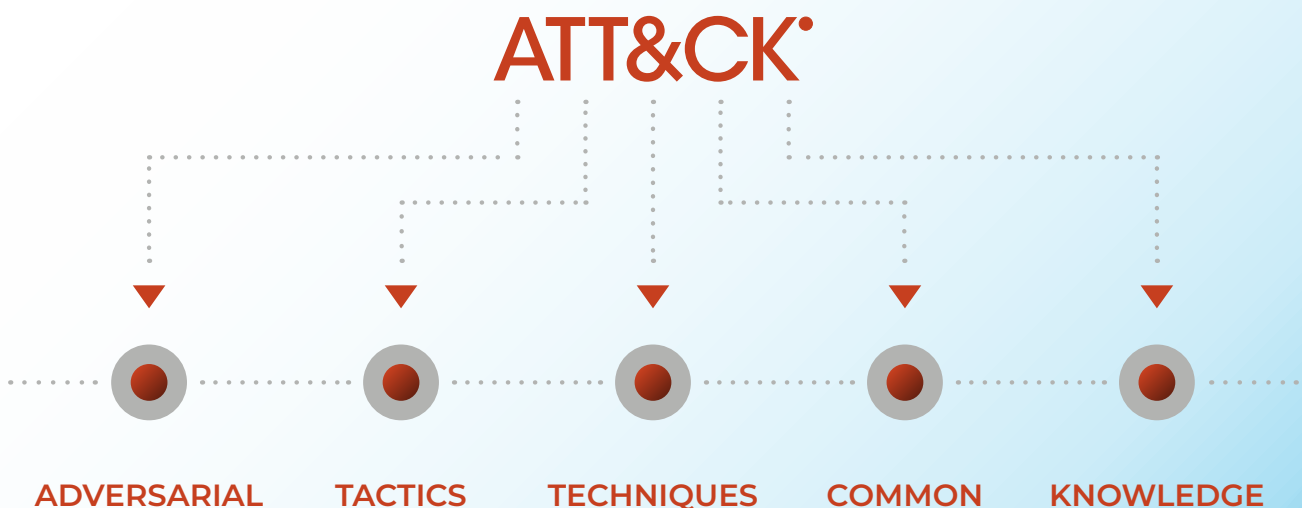
“We are delighted that MITRE Engenuity has selected CYBER RANGES as the cyber-range-of-choice for MAD 2.0. Our research, innovation, and community values very closely align with those of MITRE Engenuity’s MAD team. Our collaboration stems from our novel ‘Top 10 Abilities’ approach, which focuses on observable, measurable abilities to validate cybersecurity talent, and the underpinning TOAR platform, which supports strong cyberdefense development ecosystems based on threat intel, next-gen cyber ranging and incident response.”

Dr. Al Graziano, Chief Executive Officer for CYBER RANGES

About the MITRE ATT&CK® Framework

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK® knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge), MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK® is open and available to any person or organization for use at no charge.



The ATT&CK® framework describes how attackers penetrate networks and then move laterally, escalate privileges, create a persistent state, or generally evade your defenses. The ATT&CK® framework looks at the issue from an attacker's point of view and helps cybersecurity professionals identify what is the goal of an attacker and what are the techniques and procedures the attacker will use to attain their goal.



ATT&CK® helps you understand how attackers might operate so that you can plan and build response playbooks to mitigate attacker incidents.

Another important use of ATT&CK® is to help you learn how to detect an attacker's actions on your network. The ATT&CK® Framework includes resources that are purpose built to help you develop analytics that detect the techniques used by attackers as they attempt to breach, explore, and exfiltrate data from your databases. ATT&CK® will also provide information on hacking collectives or groups and the campaigns they have conducted, allowing you to be as prepared as possible for a future attack.

Armed with this knowledge and “attack playbooks” you are now better prepared to understand how your adversaries prepare for, launch, and execute their attacks to achieve specific desired objectives.

Successful and comprehensive threat detection requires understanding common adversary Tactics, Techniques and procedures (TTPs) especially those that pose a threat to your organization, and how to detect and mitigate these attacks.

Each technique describes one way an attacker may attempt to achieve their objective.

Tactics represent the “why” of an ATT&CK® technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action.

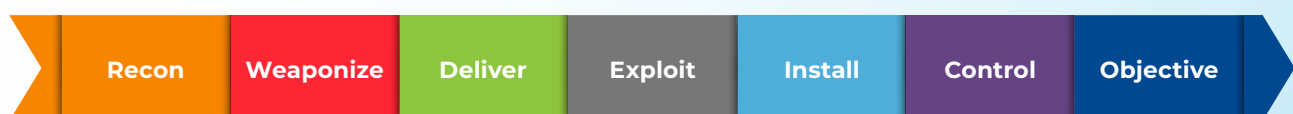
For example, an adversary may want to achieve credential access, that's a tactic. Within each tactic category ATT&CK® defines a series of techniques.

Enterprise Matrix in the ATT&CK Framework

ATT&CK® Enterprise and PRE-ATT&CK combine to form the full list of tactics that align with the Cyber Kill Chain. While PRE-ATT&CK mostly aligns with the first three phases of the Cyber Kill Chain, ATT&CK® Enterprise aligns with the final four phases.

PRE-ATTACK

ENTERPRISE



The Enterprise Matrix included in the ATT&CK® Framework consists of 14 tactics that attackers may use to breach and exfiltrate data from your network.

The Matrix includes techniques spanning Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office365 and SaaS tools. You can use the MITRE ATT&CK® Navigator to filter through the different tactics and their assigned MITRE ATT&CK® Techniques.

This framework is on the MITRE Git and makes navigating attack techniques significantly easier.

MITRE ATT&CK® Simulation Scenarios by CYBER RANGES

Available by subscription, this MITRE ATT&CK® training library is designed to introduce students to the MITRE ATT&CK® Framework and to cover the process of utilizing it for adversary emulation with Atomic Red Team tests. Initially, MAD subscribers can access practice labs running on CYBER RANGES.

New practitioner-level assessments and certifications are coming soon and will offer MAD subscribers a new way to prove their mastery of adversary emulation and threat hunting concepts.

The MITRE ATT&CK® Library is made of several Playlists to suit students' interests and objectives.

MITRE | ATT&CK® TRAINING





Description

This Library will introduce you to the fundamentals of using the MITRE ATT&CK® Framework for threat intelligence and will teach you how to use the MITRE ATT&CK® framework in conjunction with Atomic Red Team tests to automate an adversary emulation campaign.

This playlist also contains challenge-based hacking scenarios that are tied to specific MITRE ATT&CK® techniques and sub-techniques and are designed to improve your knowledge of the techniques used by adversaries and threat actors.

Outcomes

After completing this playlist, student will be competent in the following areas:

-  The ability to use the MITRE ATT&CK® Framework and Navigator.
-  The ability to perform threat intelligence with the MITRE ATT&CK® Framework.
-  Knowledge on how to setup and automate an adversary emulation campaign with Atomic Red Team tests.
-  Comprehensive knowledge of the techniques and sub-techniques used by adversaries/threat actors during their campaigns.

 **Nº of Playlists**
5 (five)

Playlists in this Subscription






1 MITRE | ATT&CK® FUNDAMENTALS

Description

This playlist is designed to introduce students to the MITRE ATT&CK® Framework and covers the process of using the MITRE ATT&CK® Navigator, performing threat intelligence with MITRE ATT&CK® and using SIGMA rules.

Outcomes

After completing this playlist, students will be competent in the following areas:

-  Using MITRE ATT&CK® Framework.
-  Using MITRE ATT&CK® Navigator.
-  Performing threat intelligence using MITRE ATT&CK®.
-  Using SIGMA rules.
-  Threat Hunting and Threat Intelligence.

 **Nº of Scenarios**
8 (eight)

   **Difficulty**
Intermediate

Playlists in this Subscription

2 ATOMIC RED TESTS WITH MITRE | ATT&CK®

Description

This playlist will teach you how to use Atomic Red Team tests for adversary emulation. This playlist and covers the process of hunting and detecting IOCs with ELK and the MITRE ATT&CK® Framework.

Outcomes

After completing this playlist, students will be competent in the following areas:

- 🛡️ Using and running the Atomic Red Team tests.
- 🛡️ Analysing Windows and Sysmon Events.
- 🛡️ Hunting for Indicators of Compromise.



Nº of Scenarios
10 (ten)



Difficulty
Intermediate

3 MITRE | ATT&CK® RED TEAM CHALLENGES • EASY

Description

This playlist contains easy challenge-based CTFs that require students to use specific MITRE ATT&CK® techniques to gain access to a vulnerable system and perform post exploitation. This playlist is ideal for penetration testers and red teamers looking to improve their exploitation skills and knowledge of various initial access, persistence, and privilege escalation MITRE ATT&CK® techniques.

Outcomes

After completing this playlist, students will be competent in the following areas:

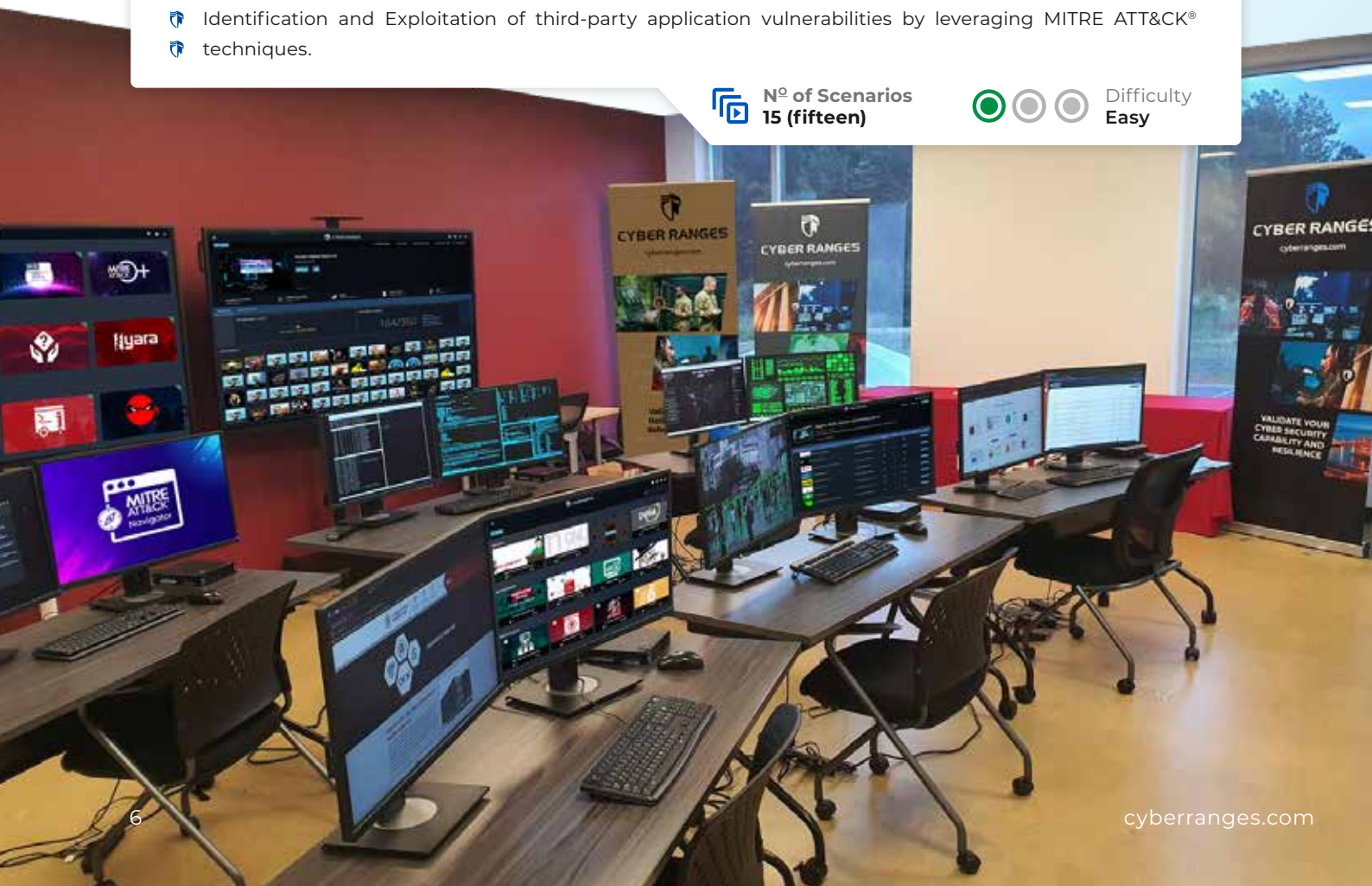
- 🛡️ Identification and Exploitation of system vulnerabilities by leveraging MITRE ATT&CK® techniques.
- 🛡️ Identification and Exploitation of third-party application vulnerabilities by leveraging MITRE ATT&CK® techniques.



Nº of Scenarios
15 (fifteen)



Difficulty
Easy



4 MITRE | ATT&CK® RED TEAM CHALLENGES • MEDIUM

Description

This playlist contains intermediate challenge based CTFs that require students to use specific MITRE ATT&CK® techniques to gain access to a vulnerable system and perform post exploitation. This playlist is ideal for penetration testers and red teamers looking to improve their exploitation skills and knowledge of various initial access, persistence and privilege escalation MITRE ATT&CK® techniques.

Outcomes

After completing this playlist, students will be competent in the following areas:

- 🔒 Identification and Exploitation of system vulnerabilities by leveraging MITRE ATT&CK® techniques.
- 🔒 Identification and Exploitation of third-party application vulnerabilities by leveraging MITRE ATT&CK® techniques.



Nº of Scenarios
15 (fifteen)



Difficulty
Intermediate

5 MITRE | ATT&CK® RED TEAM CHALLENGES • ADVANCED

Description

This playlist contains advanced challenge based CTFs that require students to use specific MITRE ATT&CK® techniques to gain access to a vulnerable system and perform post exploitation.

This playlist is ideal for penetration testers and red teamers looking to improve their exploitation skills and knowledge of various initial access, persistence, and privilege escalation MITRE ATT&CK® techniques.

Outcomes

After completing this playlist, students will be competent in the following areas:

- 🔒 Identification and Exploitation of system vulnerabilities by leveraging MITRE ATT&CK® techniques.
- 🔒 Identification and Exploitation of third-party application vulnerabilities by leveraging MITRE ATT&CK® techniques.



Nº of Scenarios
15 (fifteen)



Difficulty
Advanced

For all queries specific to this Library
mitre@cyberranges.com

For all general queries
subscriptions@cyberranges.com





About Us

CYBER RANGES is the ISO27001 certified next-generation military-grade full-content-lifecycle simulation platform for the validation of threat-informed defense capability and cyber resilience. Built on powerful cloud technology, CYBER RANGES is available as subscription-based, as managed service, as On-Premise and Portable rugged deployment options.

CYBER RANGES applies high automation, high orchestration and high scalability to the delivery of even complex large-audience deep-dive management tabletop and technical exercises based on high-fidelity IT/OT infrastructure replicas. CYBER RANGES fully supports MITRE (PRE-)ATT&CK across its entire cyber range architecture. Through its proprietary Injector Engine CYBER RANGES automatically emulates user traffic and the latest intel-based attacks, APTs and specific tactics and exploits from the MITRE ATT&CK Matrix™.

CYBER RANGES powers the international CyberStars™ initiative (www.cyberstars.pro) run in private-public collaboration with national focal points and regulatory authorities from around the world. CyberStars provides a turnkey project package for participating countries to organize national cybersecurity competitions and to participate in international ones, while at the same time meeting the objectives of national cybersecurity strategies in terms of talent growth.

CYBER RANGES actively participates as a key member organization in the European Cyber Security Organization (ECSO) WG5 on Cyber Ranges, Education and Training and Technical Exercises, advancing best practice in the domain of cybersecurity capability and resilience. CYBER RANGES also spearheads the "Top 10 Abilities" initiative, which helps CISOs to focus on pertinent, observable, measurable abilities for the development and assessment of job-specific capabilities in the workplace.

CYBER RANGES is also an active Partner of the Global Cyber Alliance – GCA (New York, Brussels, London) in its worldwide mission to sustain a trustworthy Internet by reducing cyber risk. CYBER RANGES is a founding member of the Canada-based Cyber Security Global Alliance (CSGA). CYBER RANGES is an ecosystem partner of the Quantico Cyber Hub in Virginia.

Call us toll-free (North America)
1-800-959-0163

cyberranges.com