MITRE
TECHNOLOGY APPLIED

Course Library Detail

MAD20
MAD20 ARENAS
POWERED BY CYBER RANGES

Module and Certification Roadmap

MAD20

ATT&CK® Fundamentals

MITRE's own ATT&CK subject matter expert, Jamie Williams, produced this course. It is the first and fundamental piece of the MAD20™ online training series

ATT&CK Fundamentals…

- Introduces the MITRE ATT&CK framework, a globally accessible knowledge base, and a cyber adversary behavior model based on real-world observations
- Familiarizes learners with how ATT&CK documents real-world adversary tactics, techniques, and procedures (TTPs)
- Demonstrates various ways to exploit this understanding of adversary TTPs to address current (operational) and future (strategic) threats

ATT&CK Cyber Threat Intelligence (CTI)

MAD20

Course Overview

MITRE's own ATT&CK subject matter experts produced MAD20's *ATT&CK for Cyber Threat Intelligence* course. This training may be completed solo or as a team. The authors recommend viewing the video for each module first. When prompted, pause the video to access the associated exercise documents, complete the exercises, and then view the video to go over the exercise. This training will:

- Introduce learners to MITRE ATT&CK and why it's useful for CTI
- Show learners how to map to ATT&CK from both finished reporting and raw data
- Share why it's challenging to store ATT&CK-mapped data and what to consider when doing so
- Visualize how to perform CTI analysis using ATT&CK-mapped data
- Familiarize learners with making defensive recommendations based on CTI analysis

Narrative Reporting

ATT&CK subject matter experts develop the training and mastery assessment built for the ATT&CK Cyber Threat Intelligence (CTI) from the **Narrative Reporting Badge**. The focus is to validate:

- Applying ATT&CK in mapping a threat report.
- Identifying ATT&CK tactics, then techniques and extracting those from a finished threat report.

Raw Data

The focus of the **CTI Raw Data Badge** is to validate:

- Mapping raw data and translating behaviors seen on a system or in raw data into TTPs.

Storage and Analysis

The focus of the **CTI Storage and Analysis Badge** is to validate:

- Creating layers in ATT&CK Navigator.
- Producing heatmaps and sharing coverage of specific TTPs, adversary groups, and more.
- Comparing layers by looking at two different APT groups or software and finding overlapping techniques between them.

Defense Recommendations

The **CTI Defense Recommendations Badge** validates a defender's mastery of using ATT&CK mapped data to make defensive recommendations for an enterprise. Completion of the program certifies:

- Mastery of the defensive recommendation process.
- Understanding techniques and sub-techniques are used in ATT&CK CTI.
- Mastering constraints and tradeoffs within organizations.

Certification

ATT&CK Cyber Threat Intelligence Certification is an intermediate level program that affirms your ability to identify, develop, analyze, and apply ATT&CK-mapped intelligence. You must earn five distinct badges to be eligible for the *ATT&CK for Cyber Threat Intelligence (CTI) Certification*.

Click the badge to enroll now

ATT&CK Security Operations Center (SOC) Assessment

MAD20

Course Overview

MITRE's own ATT&CK subject matter experts produced MAD20's *ATT&CK SOC Assessments* course to familiarize learners with how to implement ATT&CK for visibility into where a SOC needs improvements, and inform how to apply ATT&CK to design a rapid, low overhead, and broad SOC Assessment. This training will:

- Provide tips on how to analyze SOC technologies like tools and data sources
- Share best practices for performing interviews and leading discussions on ATT&CK with SOC personnel
- Educate on how to recommend changes based on assessment results

Fundamentals

Professionals must show their mastery of the foundational elements of ATT&CK-based SOC assessments to earn the **SOC Fundamentals Badge**. The focus is to validate:

- Understanding the types and tradeoffs of different assessment methodologies, including the general methodology of a hands-off ATT&CK-based SOC assessment.
- Determining whether an ATT&CK-based SOC assessment is appropriate for a given SOC.
- Properly scoping and communicating the value of an assessment for a given SOC.

Analysis

The **SOC Analysis Badge** test students' abilities to map common SOC components back to the ATT&CK framework; those who've passed the exam have shown themselves to be proficient in understanding SOC components as they relate to the framework. The focus is to validate:

- Setting and customizing a coverage scheme for an assessment.
- Evaluating different data sources, tools, and analytics that might be found in a SOC and assess how well each one covers the techniques in ATT&CK.
- Navigation from component to component within a SOC and running it against the ATT&CK framework

Synthesis

Practitioners must demonstrate an ability to form a full ATT&CK-based SOC assessment to earn the **SOC Synthesis Badge**. They must understand the big picture of assessments and how assessments should be composed and delivered. The badge tests:

- Fusing together a holistic view of security operation coverage of ATT&CK.
- Using current coverage and other SOC information to make prioritized recommendations.
- Aggregation of heatmaps from different sources to paint a complete picture of SOC coverage.
- Choosing a heatmap scoring scheme best geared towards a specific audience.
- Interviewing SOC personnel and understanding how that impacts coverage and recommendations.

Certification

The *ATT&CK SOC Assessments Certification* affirms your ability to conduct Security Operations Center (SOC) assessments that are rapid, have low overhead, and are broad enough to help the SOC get on their feet with ATT&CK. The certification affirms your mastery at analyzing SOC technologies, like tools and data sources, savviness at interviewing and discussing ATT&CK with SOC personnel and recommend improvements based on the assessments' results. You must earn four distinct badges to achieve *the ATT&CK for SOC Certification*.

Click the badge to enroll now

ATT&CK Adversary Emulation Methodology

MAD20

Course Overview

This course prepares you to apply ATT&CK to adversary emulation activities. You will learn foundational adversary emulation concepts, as well as how to research, implement, and ethically execute adversary TTP's based on ATT&CK. Additionally, you will be prepared to succeed in earning the MAD20 Adversary Emulation certification.

Fundamentals

The **Adversary Emulation Fundamentals Badge** certifies an understanding of foundational adversary emulation concepts and the ability to execute an adversary emulation plan based on ATT&CK. This badge verifies an ability to:

- Leverage ATT&CK and adversary emulation as part of their assessment and improvement practices.
- Understand foundational concepts about adversary emulation (its purpose, the adversary emulation framework, and how to execute an adversary emulation plan).

TTP Research

The **Adversary Emulation TTP Research Badge** certifies an ability to research adversary TTPs, select an adversary to emulate, and develop a TTP outline. This badge verifies an ability to:

- Understand how to research adversary TTPs to support adversary emulation activities that are representative of real-world threats.

Planning

The **Adversary Emulation Planning Badge** certifies an ability to plan adversary emulation engagements that are representative of real-world threats and aligned with the organization's cybersecurity objectives. This badge verifies an ability to:

- Understand how to plan professional adversary emulation engagements to include defining objectives, scope, and rules of engagement.

TTP Implementation

The **Adversary Emulation TTP Implementation Badge** certifies an ability to implement adversary TTPs based on ATT&CK. This badge verifies an ability to:

- Understand how to implement adversary TTPs based on real-world adversary behaviors documented in ATT&CK.

Execution

The **Adversary Emulation Execution Badge** certifies an ability to execute adversary TTPs based on ATT&CK to assess and improve cybersecurity. This badge verifies an ability to:

- Understand how to execute adversary TTPs that are representative of real-world threats while also balancing realistic emulation against project objectives and time and safety constraints.

Certification

The *ATT&CK Adversary Emulation Methodology Certification* validates a practitioner's ability to conduct adversary emulation activities based on real-world threats. The certification affirms mastery at researching, implementing, and ethically executing adversary TTPs to help organizations assess and improve cybersecurity.

Click the badge to enroll now

ATT&CK Threat Hunting Detection Engineering

MAD20

Course Overview

This course teaches students how to utilize knowledge of adversary TTPs as described in the MITRE ATT&CK framework to develop, test, tune, and employ robust analytics to detect and investigate malicious cyber activity. Students taking this course will learn how to leverage ATT&CK to develop hypotheses, determine data collection requirements, identify and mitigate collection gaps, test and tune analytics using purple-teaming, and conduct a threat-informed hunt.

Fundamentals

The **Threat Hunting Fundamentals Badge** verifies an understanding of how ATT&CK can be used as a malicious activity model to conduct the six steps of the TTP-based threat hunt methodology. This badge verifies:

- Understanding of how to contrast key elements of TTP-based hunting with complimentary approaches and fundamental considerations for characterizing malicious activity or behavior.
- Use that information to execute a TTP-based hunt.

This process shapes information needs and data requirements to develop continual hunt efforts focused on advanced cyber adversary behaviors.

Hypotheses

The **Threat Hunting Hypotheses Badge** certifies an ability to develop and refine hypotheses and abstract analytics that can be used to hunt for evidence indicative of malicious presence. This badge covers the ability to:

- Develop a well-formed hypothesis while avoiding common traps such as cognitive bias that can impact hunting efforts and fine-tuning hypotheses to focus on potential attack behaviors.
- Discuss and formulate abstract analytics that help conduct research to find candidate invariant behaviors.

Data Collection Requirements

The **Threat Hunting Data Collection Requirements Badge** verifies an understanding of how to identify data requirements necessary to conduct TTP-based hunts. This badge covers the ability to:

- Describe various types of data types, how to identify data collection requirements, and how they map to analytics.
- Create a collection plan.

Addressing Data Collection Gaps

The **Threat Hunting Addressing Data Collection Gaps Badge** certifies an ability to identify gaps in a data collection strategy and develop a plan for addressing those gaps. This badge covers the ability to:

- Reconfigure existing tools, deploy new sensors, establish new data flows, and use alternative analytic approaches to close existing data gaps, resulting in new data collection configurations.
- Explain potential impacts to network owners to inform security-based decisions.

Tuning Analytics

The **Threat Hunting Tuning Analytics Badge** certifies an ability to convert hypotheses and abstract analytics into concrete analytics that can effectively find malicious adversary behaviors within a given environment. This badge covers the ability to:

- Optimize precision and recall through modification of Time, Terrain, and Behavior aspects of developed analytics.

Certification

The *ATT&CK Threat Hunting Detection Engineering Certification* verifies an ability to demonstrate foundational knowledge that supports the execution of a six-step TTP-based hunting methodology centered on use of the ATT&CK Framework. This program is designed for practitioners who can apply a solid understanding of the ATT&CK Framework, adversarial behaviors of interest, and possess the ability to articulate hunt-directing hypotheses that inform the development of written analytics that drive information needs and data collection requirements. The ability to apply the TTP-based hunting methodology, as demonstrated by successful completion of this program, supports a dedication to securing critical networks and systems against attacks from advanced cyber adversaries.

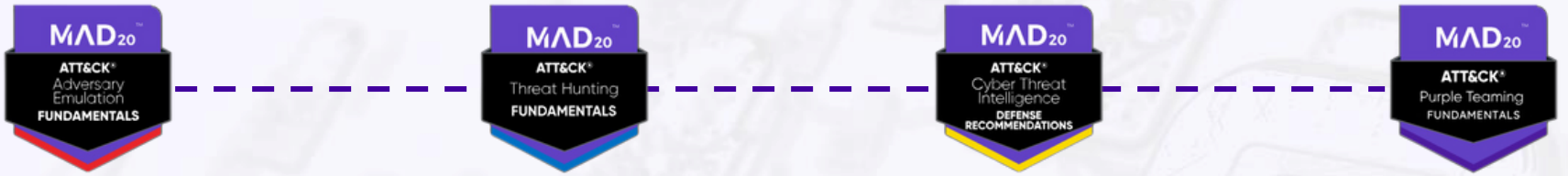
Click the badge to enroll now

ATT&CK Purple Teaming Methodology

MAD20

Course Overview

Do you want to learn the exciting discipline of Purple Teaming? In this MAD20 Purple Teaming Fundamentals course, you'll learn to do collaborative purple teaming focused on prioritized malicious behaviors. Experts from MITRE show you the actionable defensive rewards that only come when red and blue teams work together.



Adversary Emulation Fundamentals

The **Adversary Emulation Fundamentals Badge** certifies an understanding of foundational adversary emulation concepts and ability to execute an adversary emulation plan based on ATT&CK. This badge validates an ability to:

- Leverage ATT&CK and adversary emulation as part of cybersecurity assessment and improvement practices.
- Understand foundational concepts about adversary emulation, including its purpose, the adversary emulation framework, and how to execute an adversary emulation plan.

Threat Hunting Fundamentals

The **Threat Hunting Fundamentals Badge** verifies an understanding of how ATT&CK can be used as a malicious activity model to conduct the six steps of the TTP-based threat hunt methodology. This badges verifies an ability to:

- Contrast key elements of TTP-based hunting with complimentary approaches, as well as fundamental considerations for characterizing malicious activity or behavior
- Use that information to execute a TTP-based hunt.

Knowledge of this process continually shapes information needs and data requirements to inform and develop continual hunt efforts focused on advanced cyber adversary behaviors.

Cyber Threat Intelligence Defense Recommendations

The **Cyber Threat Intelligence Badge** validates a defender's mastery of using ATT&CK mapped data to make defensive recommendations for an enterprise. The focus is to validate:

- Mastery in how the defensive recommendation process works.
- Mastery in how techniques and sub-techniques are used in ATT&CK CTI.
- Proficiency in understanding constraints and tradeoffs within organizations.

Purple Teaming Fundamentals

The **Purple Teaming Fundamentals Badge** verifies the holder knows how to effectively prepare for, execute, and leverage purple teaming.

Certification

This certification verifies that the holder knows the fundamentals of how to leverage purple teaming to emulate adversarial behavior, and deliver actionable, robust defensive recommendations, such as new data collection requirements, mitigations, system reconfigurations, and analytics.

Click the badge to enroll now

ATT&CK Access Token Manipulation Courses

MAD20

Course Overview

These token manipulation courses are for advanced practitioners aiming to receive more nuanced training on access token manipulation.

ATT&CK Detecting Access Token Manipulation

The **Detection Engineering Technique T1134.001 Certification** affirms an understanding of the lessons and tactics taught in the MAD20™ ATT&CK Threat Hunting Course and applies it to detecting T1134.001: Token Impersonation and Theft. Badge holders are able to:

- Walk through the steps of the TTP Threat Hunting Methodology and apply it for specific technique detection engineering
- Understand what access tokens are, how they can be manipulated through token impersonation and theft, and implement research to emulate behaviors
- Analyze and identify low variance behaviors to build and implement analytics into their analytical environment

ATT&CK Emulating Access Token Manipulation

This course analyzes real-world examples of adversaries performing Access Token Manipulation and discusses how we can emulate this behavior. The course is broken down into modules, with each module focusing on a specific sub-technique for Access Token Manipulation. The first module focuses on the token impersonation/theft sub-technique, and it dives into two real world examples from FIN8 and Shamoon.

Click either badge to enroll now

MAD20 ARENAS
POWERED BY CYBER RANGES

MAD20 ARENAS Exclusive Content

CYBER RANGES Partnership

MAD20 ARENAS
POWERED BY CYBER RANGES

Why CYBER RANGES?

MAD20 has chosen to partner with CYBER RANGES due to the organization's global standard of excellence. Since 2014, CYBER RANGES has delivered hands-on cyberdrills to CERTs/CSIRTs and SOC teams worldwide in collaboration with the International Telecommunication Union (ITU). More recently CYBER RANGES has developed the latest ITU Cyberdrill Framework and is their official cyber range platform for the delivery of global cyberdrills targeting national CERTs as well as CSIRTs from critical infrastructure and financial institutions. In 2020 and 2021, CYBER RANGES was used to power the ITU Global Cyberdrill bringing together hundreds of incident responders from around the world.

Also, CYBER RANGES Cross-Cyberdrill (C2 Drill) service is the only type of cyberdrill combining both managerial tabletop and operational exercises on a single platform to test the end-to-end incident response process of an organization as well as to assess that organization's cyber resilience. MAD20 ARENAS harnesses the power of the CYBER RANGE platform to provide users a hands-on curriculum uniquely designed to train teams on the MITRE ATT&CK framework.

CYBER RANGES Experience & References

CYBER RANGES was chosen by the ITU as the platform for the delivery of their 2020 and 2021 Global Cyberdrills, where CYBER RANGES held the following roles:

- Development of CyberDrill Scenarios
- Support of other ITU Partners in the development and publication of their CyberDrill scenarios onto CYBER RANGES
- Provision of the CYBER RANGES platform for the whole duration of the International CyberDrills for all participating United Nations member states.

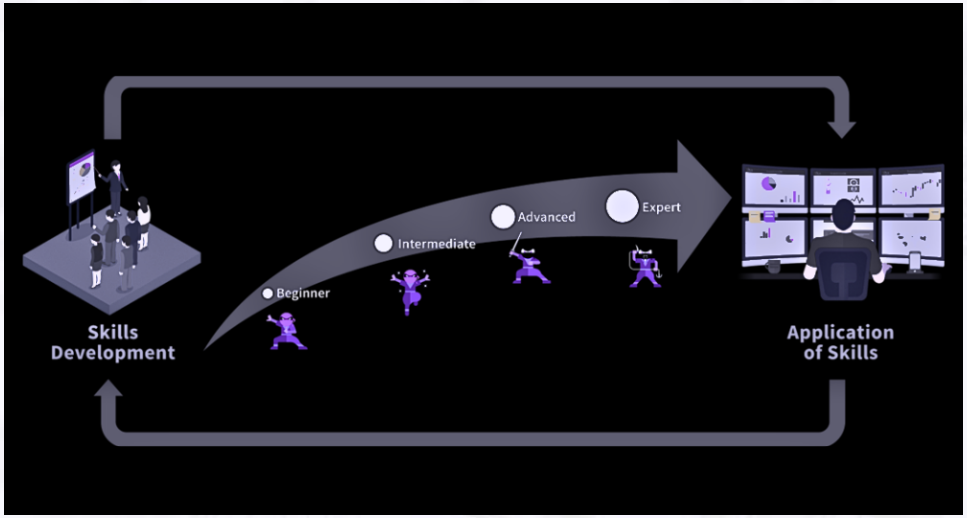
CYBER RANGES is used and trusted by organizations worldwide across Military, Government, Financial, Telecommunication and Education sectors:

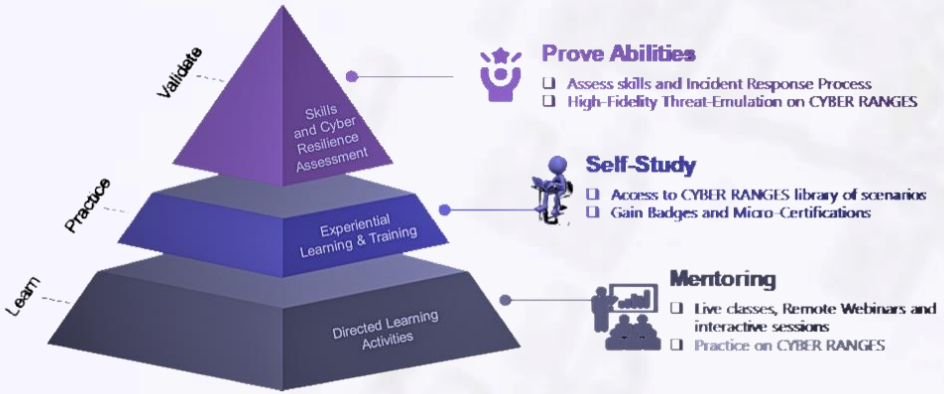
MAD20 ARENAS Skill Development

Critical Path of Skill Development

MAD20 ARENAS, powered by CYBER RANGES, is designed for skill development and gamified application. Playlists are available to Blue team, Red team, Purple team activities and functionalities to support white team operations via our MAD20 ARENAS standard bundle.

MAD20 ARENAS **currently includes over 60 simulations across five playlists on MITRE ATT&CK** and is expected to expand to include more. More broadly speaking, the full CYBER RANGES library of **over 1,000 labs can be accessed upon request for additional cost**.





Structure + Guidance

MAD20 ARENAS is designed around the idea that simply giving access to a vast list of videos, training scenarios and labs for self-use is not sufficient for upskilling professionals, especially when talking about beginners and intermediate professionals.

Our methodology for upskilling and workforce development is illustrated by our pyramid. MAD20's MITRE ATT&CK training platform guides Defenders step by step through the concepts covered in the ranges, preparing them for all exercises. Following simulation completion, Defenders are then provided detailed feedback regarding their performance, providing a basis for continued improvement.

MAD20 ARENAS Playlists

MAD20 ARENAS
POWERED BY CYBER RANGES

MAD20 ARENAS Library

The MAD20 ARENAS library consists of five simulation playlists today, with **over 60 simulations and 180 hours (8+ days) of content across the five playlists below**, this being in excess of MAD20 MITRE ATT&CK Basic subscription learning track content.

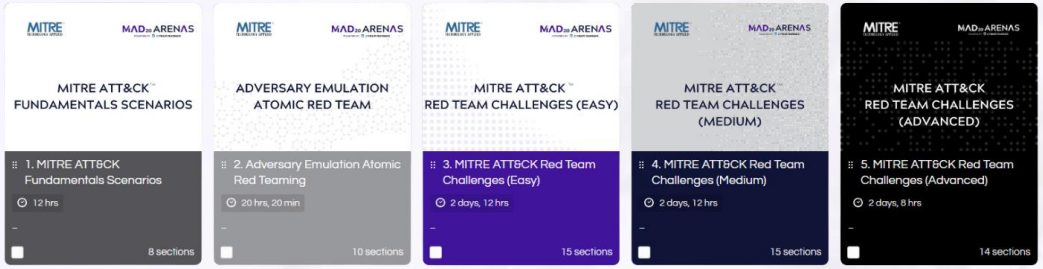
Learners will have access to all content available and can work towards a practitioners' certification on MITRE ATT&CK, soon to be announced.

Example – CTI with MITRE ATT&CK

Duration: 2hrs

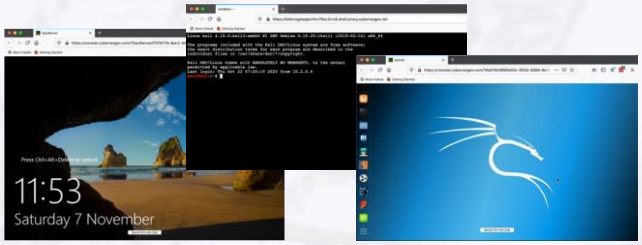
Difficulty: Intermediate

Objectives: Learn to heat map multiple APT groups to MITRE ATT&CK Navigator, conduct a CTI analysis on an organization, and determine priority TTP's for the organization.

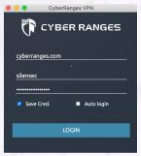


Simulation	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
1	Exploit Public Facing Application		Valid Accounts	Valid Accounts		Brute Force	File and Directory Discovery	Exploitation of Remote Services	Data from Local System		Exfiltration Over Web Service	Account Access Removal
2	Valid Accounts					OS Credential Dumping	File and Directory Discovery	Remote Services	Data from Local System		Scheduled Transfer	Data Destruction
3	External Remote Services				Hijack Execution Flow	Credentials from Password Stores	Remote System Discovery	Remote Services		Application Layer Protocol	Exfiltration Over C2 Channel	Data Encrypted for Impact
4	Phishing	User Execution	Boot or Logon Initialization Scripts	Access Token Manipulation		Man-in-the-Middle	Domain Trust Discovery	Remote Services	Data from Local System	Encrypted Channel		Defacement
5	Exploit Public Facing Application			Exploitation for Privilege Escalation		OS Credential Dumping	File and Directory Discovery	Remote Services		Encrypted Channel		Service Stop

Tactic/Technique Scenario Grid Examples

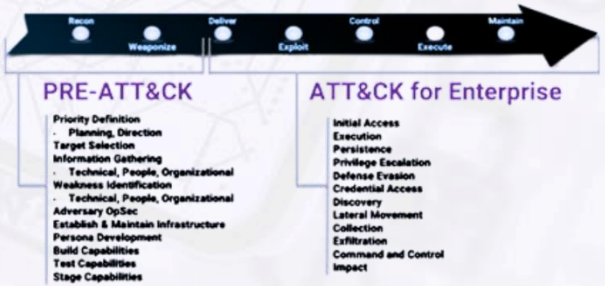


In-Browser Access to the Simulation Environment



Access via VPN for for BYOD Engagements

Individual access to the VMs



MITRE®
TECHNOLOGY APPLIED

MAD20

MAD20 ARENAS

POWERED BY CYBER RANGES