MITRE
TECHNOLOGY APPLIED

MAD20 Library Detail

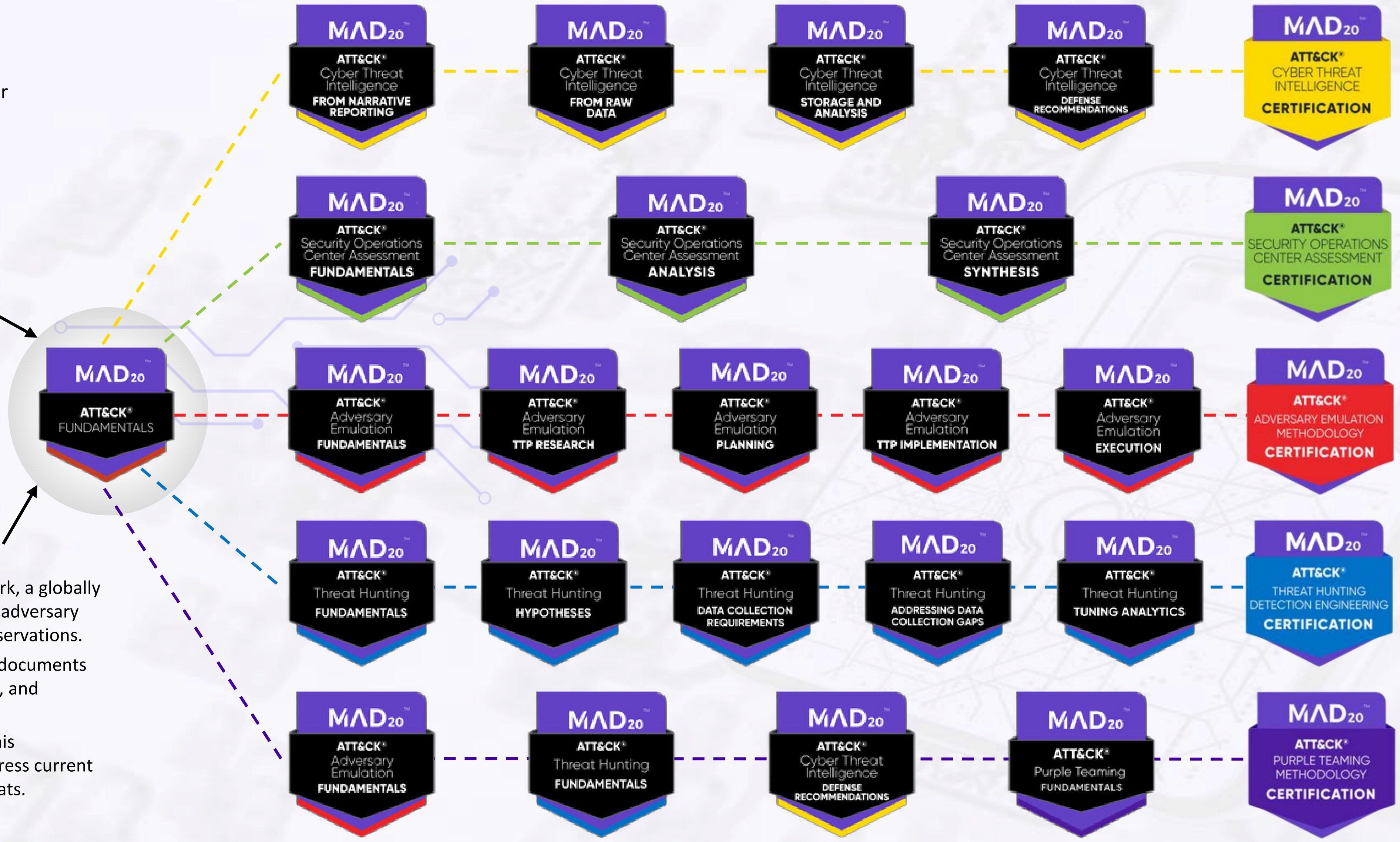
MAD20

MAD20 ARENAS
POWERED BY CYBER RANGES

Module and Certification Roadmap

ATT&CK® Fundamentals

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



MAD20 ATT&CK® FUNDAMENTALS

MAD20 ATT&CK® Cyber Threat Intelligence FROM NARRATIVE REPORTING

MAD20 ATT&CK® Cyber Threat Intelligence FROM RAW DATA

MAD20 ATT&CK® Cyber Threat Intelligence STORAGE AND ANALYSIS

MAD20 ATT&CK® Cyber Threat Intelligence DEFENSE RECOMMENDATIONS

MAD20 ATT&CK® CYBER THREAT INTELLIGENCE CERTIFICATION

MAD20 ATT&CK® Security Operations Center Assessment FUNDAMENTALS

MAD20 ATT&CK® Security Operations Center Assessment ANALYSIS

MAD20 ATT&CK® Security Operations Center Assessment SYNTHESIS

MAD20 ATT&CK® SECURITY OPERATIONS CENTER ASSESSMENT CERTIFICATION

MAD20 ATT&CK® Adversary Emulation FUNDAMENTALS

MAD20 ATT&CK® Adversary Emulation TTP RESEARCH

MAD20 ATT&CK® Adversary Emulation PLANNING

MAD20 ATT&CK® Adversary Emulation TTP IMPLEMENTATION

MAD20 ATT&CK® Adversary Emulation EXECUTION

MAD20 ATT&CK® ADVERSARY EMULATION METHODOLOGY CERTIFICATION

MAD20 ATT&CK® Threat Hunting FUNDAMENTALS

MAD20 ATT&CK® Threat Hunting HYPOTHESES

MAD20 ATT&CK® Threat Hunting DATA COLLECTION REQUIREMENTS

MAD20 ATT&CK® Threat Hunting ADDRESSING DATA COLLECTION GAPS

MAD20 ATT&CK® Threat Hunting TUNING ANALYTICS

MAD20 ATT&CK® THREAT HUNTING DETECTION ENGINEERING CERTIFICATION

MAD20 ATT&CK® Adversary Emulation FUNDAMENTALS

MAD20 ATT&CK® Threat Hunting FUNDAMENTALS

MAD20 ATT&CK® Cyber Threat Intelligence DEFENSE RECOMMENDATIONS

MAD20 ATT&CK® Purple Teaming FUNDAMENTALS

MAD20 ATT&CK® PURPLE TEAMING METHODOLOGY CERTIFICATION

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

MAD20
ATT&CK® Cyber Threat Intelligence
FROM NARRATIVE REPORTING
MAD20
ATT&CK® Cyber Threat Intelligence
FROM RAW DATA
MAD20
ATT&CK® Cyber Threat Intelligence
STORAGE AND ANALYSIS
MAD20
ATT&CK® Cyber Threat Intelligence
DEFENSE RECOMMENDATIONS

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*.

ATT&CK Security Operations Center (SOC) Assessment

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*.

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.

MAD20 ATT&CK Adversary Emulation FUNDAMENTALS
MAD20 ATT&CK Adversary Emulation TTP RESEARCH
MAD20 ATT&CK Adversary Emulation PLANNING
MAD20 ATT&CK Adversary Emulation TTP IMPLEMENTATION
MAD20 ATT&CK Adversary Emulation EXECUTION

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.

ATT&CK Threat Hunting Detection Engineering

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.

MAD20
ATT&CK®
Threat Hunting
FUNDAMENTALS
MAD20
ATT&CK®
Threat Hunting
HYPOTHESES
MAD20
ATT&CK®
Threat Hunting
DATA COLLECTION REQUIREMENTS
MAD20
ATT&CK®
Threat Hunting
ADDRESSING DATA COLLECTION GAPS
MAD20
ATT&CK®
Threat Hunting
TUNING ANALYTICS

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

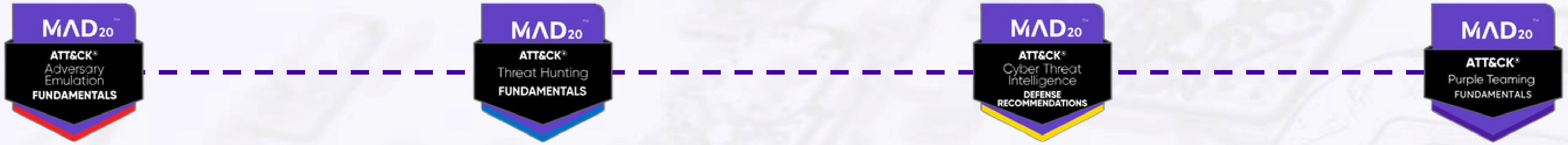
The *ATT&CK Threat Hunting Detection Engineering Certification* verifies an ability to demonstrate foundational knowledge that supports the execution of a six-step TTP-based hunting methodology centered on use of the ATT&CK Framework. This program is designed for practitioners who can apply a solid understanding 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.

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.

Information contained herein is confidential and not to be distributed. For pricing or questions, please contact info@mad20.com.

ATT&CK Access Token Manipulation Courses

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.

Information contained herein is confidential and not to be distributed. For pricing or questions, please contact info@mad20.com.

MAD20 ARENAS
POWERED BY CYBER RANGES

MAD20 ARENAS Content Overview

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.

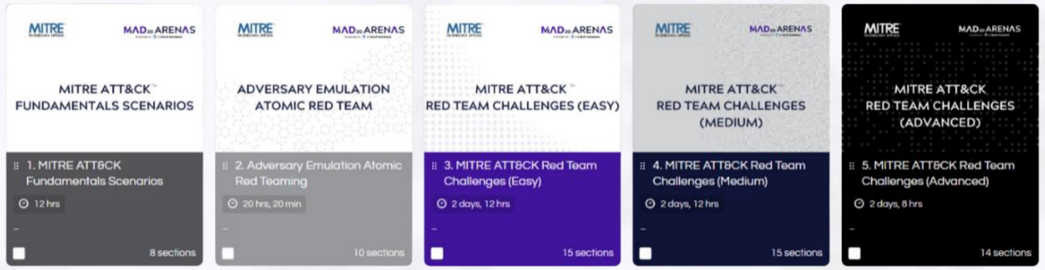
Learners will have access to all content available and can work towards a practitioners' certification on MITRE ATT&CK, soon to be announced.

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.



MITRE ATT&CK™ FUNDAMENTALS SCENARIOS
1. MITRE ATT&CK Fundamentals Scenarios
12 hrs
8 sections

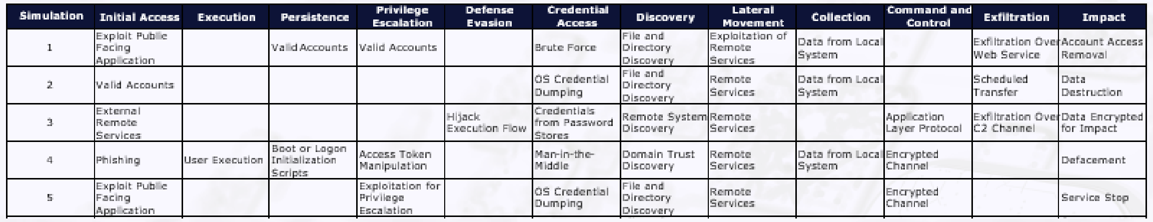
ADVERSARY EMULATION ATOMIC RED TEAM
2. Adversary Emulation Atomic Red Teaming
20 hrs, 20 min
10 sections

MITRE ATT&CK™ RED TEAM CHALLENGES (EASY)
3. MITRE ATT&CK Red Team Challenges (Easy)
2 days, 12 hrs
15 sections

MITRE ATT&CK™ RED TEAM CHALLENGES (MEDIUM)
4. MITRE ATT&CK Red Team Challenges (Medium)
2 days, 12 hrs
15 sections

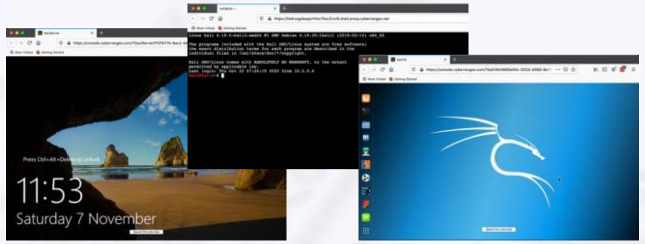
MITRE ATT&CK RED TEAM CHALLENGES (ADVANCED)
5. MITRE ATT&CK Red Team Challenges (Advanced)
2 days, 8 hrs
14 sections

MITRE
MAD20 ARENAS

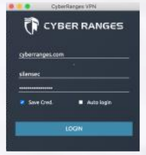


Simulation	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
1	Exploit Public Facing Application		Valid Accounts	Valid Accounts		Brute Force	File and Directory Discovery	Exploitation 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

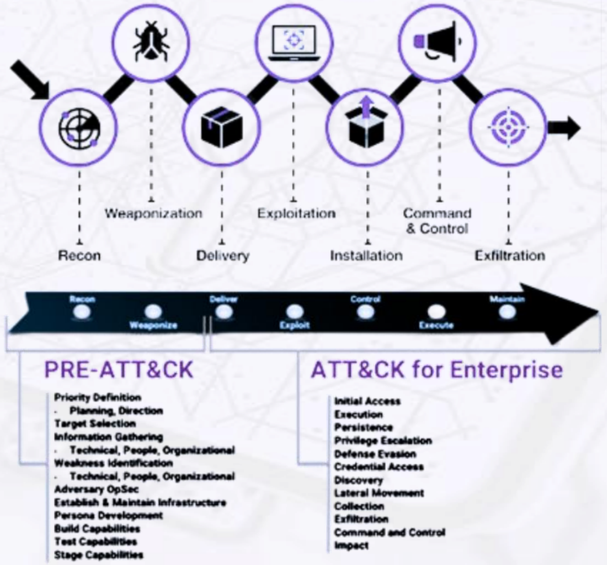


In-Browser Access to the Simulation Environment



Access via VPN for for BYOD Engagements

Individual access to the VMs



PRE-ATT&CK

Priority Definition
- Planning, Direction
Target Selection
Information Gathering
- Technical, People, Organizational
Weakness Identification
- Technical, People, Organizational
Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ATT&CK for Enterprise

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

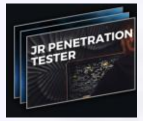
Information contained herein is confidential and not to be distributed. For pricing or questions, please contact info@mad20.com.

MAD20 ARENAS Courses

MAD20 ARENAS Library – Continuous RED Team Training

The MAD20 ARENAS library also provide learners access to various range-based dynamic courses that work to build upon MAD20’s Adversary Emulation Methodology certification, continuously developing skills and validating abilities in accordance with NICE’s NIST skills framework. The assessment for each training course is mapped to the NIST/NICE Competence Framework for detailed job role assessment.

Level 1 - Practitioner



Junior Penetration Tester

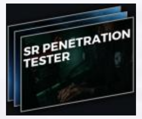
This training covers the fundamentals of cybersecurity, networking and penetration testing and provides students/professionals with the knowledge, skills and abilities required to become a Junior Penetration Tester.

Web Pentesting Professional

This training course is designed to provide penetration testers with the knowledge and skills required to assess and exploit vulnerabilities in web applications.

MAD20 ATT&CK® ADVERSARY EMULATION METHODOLOGY CERTIFICATION

Level 2 - Advanced



Senior Penetration Tester

This course is designed for SOC Tier 2 analysts. It covers knowledge domains like log management, Windows Registry, HIDS/NIDS solutions, Elastic stack, and malware analysis.

Citadel

The Citadel is a red team/offensive security training range where you will learn about tradecraft frequently used by offensive security professionals in the field today. You will be required to gain access to Citadel Corp’s corporate environment and laterally move through the network, with the objective of compromising the Domain Controller.

Collective Bank of Cyber (CBC)

The Collective Bank of Cyber is. A training range where students are are tasked with simulating an external threat actor whose goal is to compromise the CBC infrastructure and exfiltrate data from the CEO's personal workstation.

Level 3 - Expert

Red Team Operator

This training course is designed to make students competent Red Team operators. In this training course students will practice with all the tools and techniques needed to become an effective Red Team Cyber Security expert.

Red Teaming Active Directory

This training course is designed to make students competent Red Team operators. In this training course students will practice with all the tools and techniques needed to become an effective Red Team Cyber Security expert.

Information contained herein is confidential and not to be distributed. For pricing or questions, please contact info@mad20.com.

MAD20 ARENAS Courses

MAD20 ARENAS Library – Continuous BLUE Team Training

The MAD20 ARENAS library also provide learners access to various range-based dynamic courses that work to build upon MAD20's Theat Hunting & Detection Engineering certification, continuously developing skills and validating abilities in accordance with NICE's NIST skills framework. The assessment for each training course is mapped to the NIST/NICE Competence Framework for detailed job role assessment.

Level 1 - Practitioner

SOC Analyst Level I
This course covers the fundamentals of networking, traffic analysis, incident response, threat intelligence and scripting for SOC analysts.

Level 2 - Advanced

SOC Analyst Level II
This course is designed for SOC Tier 2 analysts. It covers knowledge domains like log management, Windows Registry, HIDS/NIDS solutions, Elastic stack, and malware analysis.

Cyber Threat Intelligence and Active Defense
This course addresses cyber threat intelligence to improve proactive defense. It also addresses active defense tools and techniques to deter and slow down cyber attacks.

Introduction to Malware Analysis
This course introduces the students to the fundamentals of malware analysis across a range of real examples.

Defending Corporate Networks
In this course students are tasked with detecting and responding to a wide range of cyber attacks from both outside and inside the perimeter.

Level 3 - Expert

SOC Analyst Level III
This course is designed for SOC Tier 3 analysts. It covers knowledge domains such PowerShell, network traffic monitoring, memory forensics, reverse engineering, and adversary emulation.

Adversary Emulation for Purple Teaming
Bootcamp will introduce you to Adversary Emulation and Atomic Red Team, how to use Atomic Red Team Tests for adversary emulation and how to detect and defend against adversarial TTPs with Wazuh.

Malware Analysis and Reverse Engineering
Covers advanced static and dynamic reverse engineering techniques with tools such as IDA Pro & OllyDBG through a number of practical examples.

MAD20 ARENAS Courses

MAD20 ARENAS
POWERED BY CYBER RANGES

MAD20 ARENAS Library – Continuous OT/ICS Team Training

The MAD20 ARENAS library also provide learners access to various range-based dynamic courses that work to build upon MAD20's upcoming OT/ICS certification, continuously developing skills and validating abilities in accordance with NICE's NIST skills framework. The proposed training courses are aimed at building cyber defense capabilities from beginner level up to expert level.

Level 1 - Practitioner

OT Security Practitioner
This course introduces participants to the domain of OT/ICS security along with a range of OT attack techniques through hands-on examples.

Level 2 - Advanced

Defending OT Environments
In this course participants are taken through a number of practical case studies to develop the practical experience to detect and respond to attacks to the OT infrastructure

Level 3 - Expert

Adversary Emulation for ICS Purple Teaming
This purple teaming course focuses on understanding specific techniques targeting the OT infrastructure and the associated IoCs generated by the attacks in order to develop stronger defense capabilities.

MAD20 ARENAS Courses

MAD20 ARENAS
POWERED BY CYBER RANGES

MAD20 ARENAS Library – Continuous GRC Team Training

The MAD20 ARENAS library also provide learners access to various range-based dynamic courses that work to build upon MAD20's upcoming GRC certification, continuously developing skills and validating abilities in accordance with NICE's NIST skills framework. The proposed training courses are aimed at building cyber defense capabilities from beginner level up to expert level.

Level 1 - Practitioner

Risk Management
This course introduces participants to the risk management process, from the risk assessment methodologies to risk treatment using ECC and OTCC standards

Developing Security Awareness Training Programme
This course introduces participants to the risk management process, from the risk assessment methodologies to risk treatment using ECC and OTCC standards

Level 2 - Advanced

Internal Auditor
This course helps participants develop the competences required to develop security metrics programme and improve the security maturity of the organization

Developing an Internal Audit Programme
This course helps participants develop the competences for the development and execution of internal audit programmes as well as to conduct effective security audits

Level 3 - Expert

Measurable Security and Maturity Models
This course helps participants develop the competences required to develop security metrics programme and improve the security maturity of the organization

Information contained herein is confidential and not to be distributed. For pricing or questions, please contact info@mad20.com.

MITRE®
TECHNOLOGY APPLIED

MAD20®

MAD20 ARENAS
POWERED BY CYBER RANGES