## Course Syllabus

### MITRE ATT&CK Defender™ (MAD) ATT&CK® Fundamentals Badge Training

Instructor Name: Jamie Williams

Instructor Website: N/A

Instructor Contact: jcwilliams@mitre.org

Course Creation Date: 12/04/2020

## Course Description and Goals

**Course Description:** This course will serve as the first and fundamental piece of the MITRE ATT&CK Defender™ (MAD) series which will explore how ATT&CK® and a threat-informed mindset can help focus our efforts towards understanding and improving how our defenses actually fare against real-world adversaries. This journey begins with the MITRE ATT&CK® framework, a globally-accessible knowledge base and model for cyber adversary behavior based on real-world observations.

ATT&CK® Fundamentals will not only familiarize you with how the ATT&CK® knowledge base documents real-world adversary tactics, techniques, and procedures (TTPs), but also introduce the various ways we can exploit this understanding of adversary TTPs to address current (operational) and future (strategic) threats. Together we will explore how ATT&CK® enables us to produce measurable and trackable answers to the hard questions we face every day as defenders (such as "how does our decision to make us better/worse at defending against threats?"), making us more threat-focused and informed security practitioners.

**Target audience:** Anyone involved or interested in threat modeling and applying this knowledge to improve how you and your organization defends against adversaries.

**Prerequisites:** A general understanding of information security and technology as well as their associated threats (i.e. malicious actors and malware).

**Supplementary Materials:**

- ATT&CK® Website
- MITRE ATT&CK®: Design and Philosophy
- Getting Started with ATT&CK®

**Course Goals:** By the end of this course, students should be able to:

- ❏ Understand the structure and philosophy that continually shapes ATT&CK®
- ❏ Identify the available ATT&CK® resources and operational use cases
- ❏ Recognize how ATT&CK® empowers defenders through understanding threats

## Course Outline

**Module 1** | Understanding ATT&CK®

- Lesson 1.1: Introduction to ATT&CK®
- Lesson 1.2: Matrices/Platforms
- Lesson 1.3: Tactics
- Lesson 1.4: Techniques & Sub-Techniques
- Lesson 1.5: Mitigations
- Lesson 1.6: Data Sources & Detections
- Lesson 1.7: Groups & Software
- Lesson 1.8: How ATT&CK® Grows & Evolves

**Module 2** | Benefits of Using ATT&CK®

- Lesson 2.1: Community Perspective
- Lesson 2.2: Common Language
- Lesson 2.3: Quantitative Scorecard
- Lesson 2.4: ATT&CK® Navigator

**Module 3** | Operationalizing ATT&CK®

- Lesson 3.1: Cyber Threat Intelligence
- Lesson 3.2: Detection & Analytics
- Lesson 3.3: Threat Emulation
- Lesson 3.4: Assessment & Engineering
- Lesson 3.5: Putting It All Together into Threat-Informed Defense