English

Help Us Translate

0:01 Hello, and welcome to this learning path for Python for cybersecurity. So in the intro video for this path, we talked about how the structure of the PAC is based off of the mitre attack and shield frameworks. In this video we're going to start out with an introduction to MITRE ATT&CK and shield Before we dive into the Python, so you feel a bit more comfortable about what to expect in this path.

0:29 So, let's start out by talking about MITRE ATT&CK. So the MITRE ATT&CK framework is a tool that was developed by the MITRE Corporation. And the goal of MITRE ATT&CK is to improve cybersecurity understanding, communications, etc. So it brings structure to the life-cycle of the cyber attack, and how attackers can achieve various goals throughout this life cycle. Also by standardizing vocabulary, it helps to support discussions about cybersecurity. And so how the MITRE ATT&CK matrix does this is by mapping the different goals, techniques and ways of accomplishing these goals to the cyber attack life-cycle. So, we see an example of the ATT&CK matrix for enterprise at the bottom of the screen here. And so, across the top are columns, outline the various goals that an attacker might want to achieve. So, things from performing initial reconnaissance through gaining initial access to moving laterally. To achieving an impact on the target system.

1:45 And so the first part of our course here is going to be based heavily off MITRE ATT&CK, the Python code we'll be taking a look at is designed to accomplish different goals in each course. And the code will be designed to implement certain techniques for accomplishing these goals. But that's only half of our course. We're also going to be taking a look at the MITRE shield framework. Work which is designed to complement the MITRE ATT&CK framework. And so the goal of MITRE shield is to provide some of the same insight to defenders as it does for the attack side of cybersecurity. And so it's designed to promote ways that defenders can engage in active defence. So taking action to gain some control over an attackers actions on their networks. And so like the MITRE ATT&CK framework, it has certain goals that the defender wants to achieve and outlines methods that the defender can use to achieve those goals.

2:59 And so in both of these frameworks, there's some important terms that we should talk about first. And so MITRE uses its own terms for the goals methods of accomplishing things and specific implementations. So later on when we talk about a MITRE ATT&CK tactic or a shield tactic, we're discussing the tactical goal at the particular stage of a cyber attack, or a goal an active defense. So for example, in the MITRE ATT&CK framework, lateral movement is an example of a tactic. Or, as we see at the bottom of the screen here, we'd say that credential access is a tactic.

3:42 A technique is a way that an attacker or defender can achieve the goal outlined in a particular tactic. So

in our example at the bottom of the screen here, brute force attacks are a way of accomplishing the goal or tactic of credential access.

4:01 We might have multiple different methods of accomplishing out a particular technique. So for example, you could use password guessing, password cracking, etc, for a brute force attack on passwords. And so we'll call those sub techniques that fall under a particular technique. And then finally, MITRE uses the term procedure to discuss a specific implementation of a particular technique or sub-technique. So these are things like particular malware variants, different tools, etc that have been observed to implement a particular technique. Or sub technique in the wild.

4:45 And so, now that we have some of the terminology down, let's talk through the various tactics we'll be looking at in this learning path. So the attack portion of this learning path is going to be broken down into 13 sections.

5:02 We're going to talk about the PRE-ATT&CK tactics, which are reconnaissance and resource development, and then we'll have a course for each of the remaining tactics, and the MITRE ATT&CK framework. So initial access, execution, persistence, privilege escalation, defensive evasion, credential access discovery, lateral movement, collection, command and control exfiltration and impact. And so for each of these courses, we're going to take a look at two particular techniques. And then look at Python code for sub techniques that fall under those techniques. And so we'll get a broad viewpoint of how to apply Python to the MITRE ATT&CK framework and the cyber attack lifecycle.

5:57 Once we've worked through the attack side, we'll take a look at MITRE shield. And so there's a few tactics that are defined for MITRE shield, channel collect, contain, detect, disrupt, facilitate, legitimize and test. And so all of these are actions that an active defender can take to help protect their network. And the second part of the course is going to be focused on these tactics. But we'll be structuring this one a little bit differently. So many of the techniques in MITRE shield apply to many different tactics. So we're going to organize the MITRE shield part of the course into three courses based of the specifics of the techniques that can be used.

6:49 And so the structure of this learning path is based on the purpose that we wish to demonstrate how Python can be applied to cybersecurity. And so, as I mentioned, each of the courses in this path focuses on an area of the MITRE ATT&CK. Or shield frameworks. So for attack, we'll be having a course for each tactic with the exception of preattack where we'll bring both tactics together into one course, and we'll explain that shortly. For the shield framework, we're going to be talking about specific applications of active defense. Talking about the use of decoys performing active defense at the network level and how to employ monitoring for network defense and active defense. And so each course is going to discuss some techniques and sub techniques in detail. For MITRE ATT&CK, we'll look at two techniques per course and MITRE shield we'll look at three per course. And so we'll start

out with an introduction to the course discussing either the MITRE ATT&CK tactic or the MITRE shield topic decoys, network level or monitoring.

8:06 After that intro to the course, we'll have our sets of techniques, where we'll have an introduction to the technique and describe how the technique works. And then we'll have a video where we use Python to demonstrate the application of that technique or sub technique.

8:27 And so that's how this course is going to work. And so let's get started.