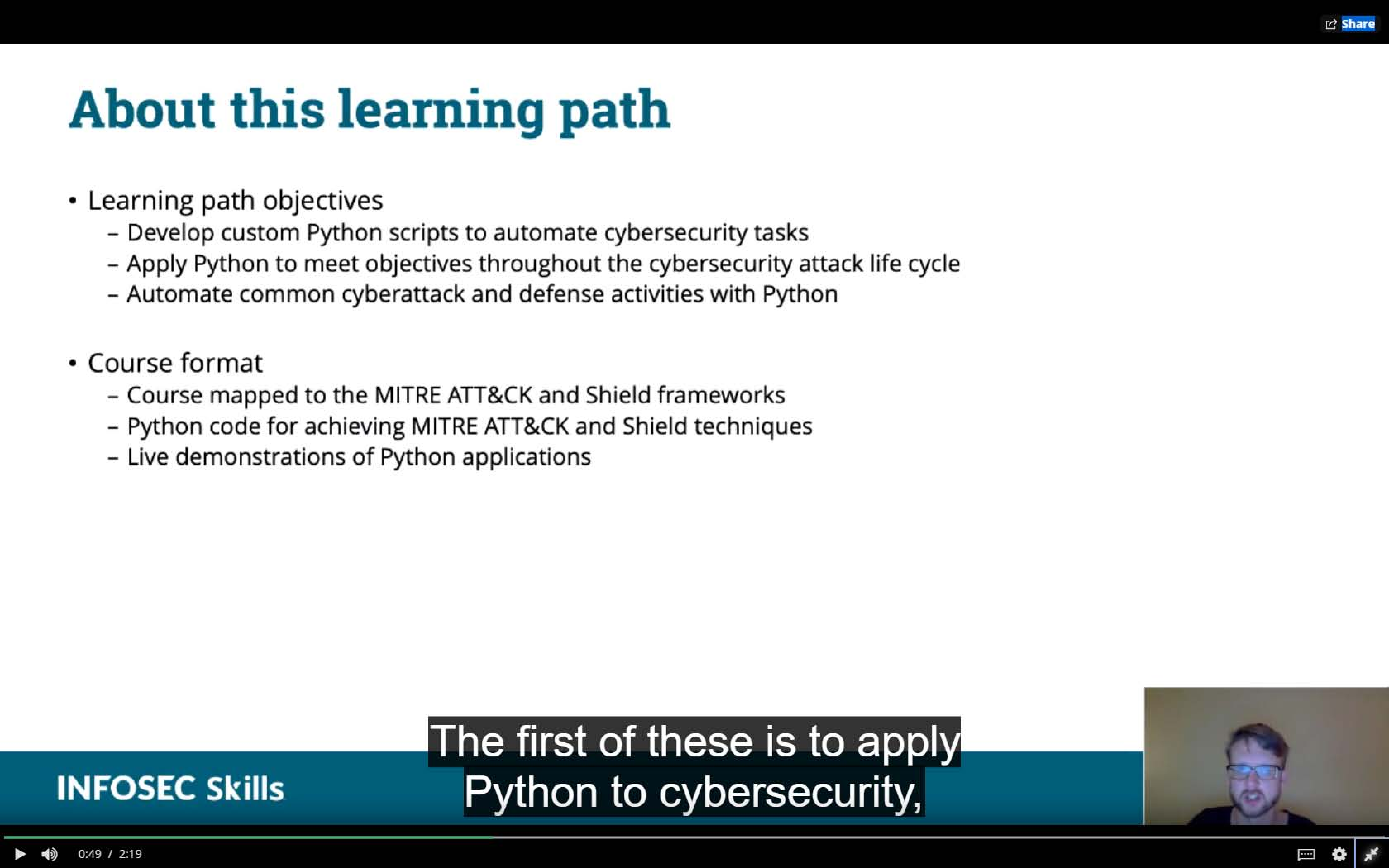


About this learning path

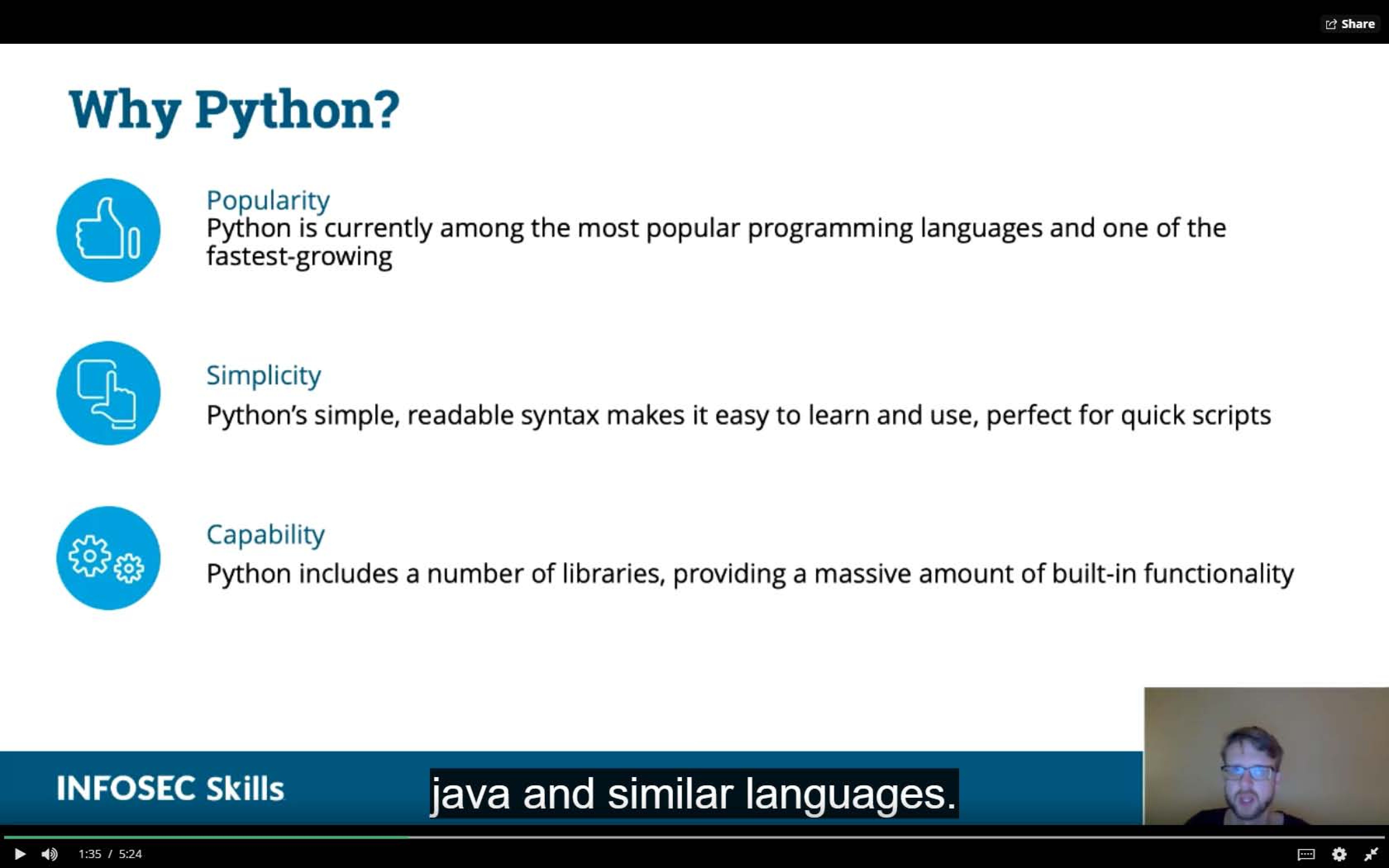
- Learning path objectives
  - Develop custom Python scripts to automate cybersecurity tasks
  - Apply Python to meet objectives throughout the cybersecurity attack life cycle
  - Automate common cyberattack and defense activities with Python
- Course format
  - Course mapped to the MITRE ATT&CK and Shield frameworks
  - Python code for achieving MITRE ATT&CK and Shield techniques
  - Live demonstrations of Python applications

The first of these is to apply
Python to cybersecurity,

INFOSEC Skills

Course 1: Introduction to Python

Hello and welcome to this python for cybersecurity learning path.



Why Python?

Popularity

Python is currently among the most popular programming languages and one of the fastest-growing

Simplicity

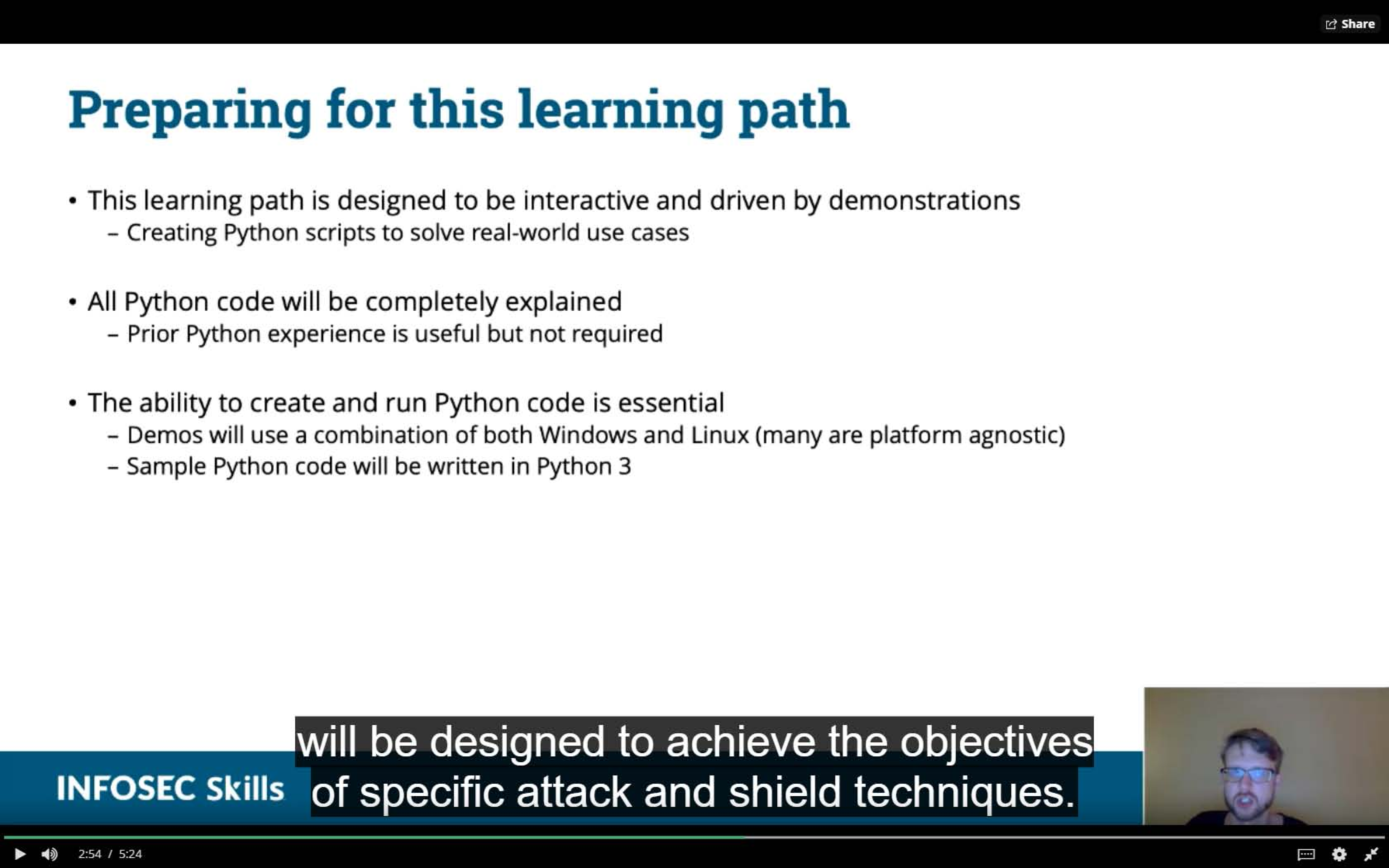
Python’s simple, readable syntax makes it easy to learn and use, perfect for quick scripts

Capability

Python includes a number of libraries, providing a massive amount of built-in functionality

INFOSEC Skills

java and similar languages.



Preparing for this learning path

- This learning path is designed to be interactive and driven by demonstrations
  - Creating Python scripts to solve real-world use cases
- All Python code will be completely explained
  - Prior Python experience is useful but not required
- The ability to create and run Python code is essential
  - Demos will use a combination of both Windows and Linux (many are platform agnostic)
  - Sample Python code will be written in Python 3

will be designed to achieve the objectives
of specific attack and shield techniques.

Section 1: Introduction to MITRE ATT&CK and Shield

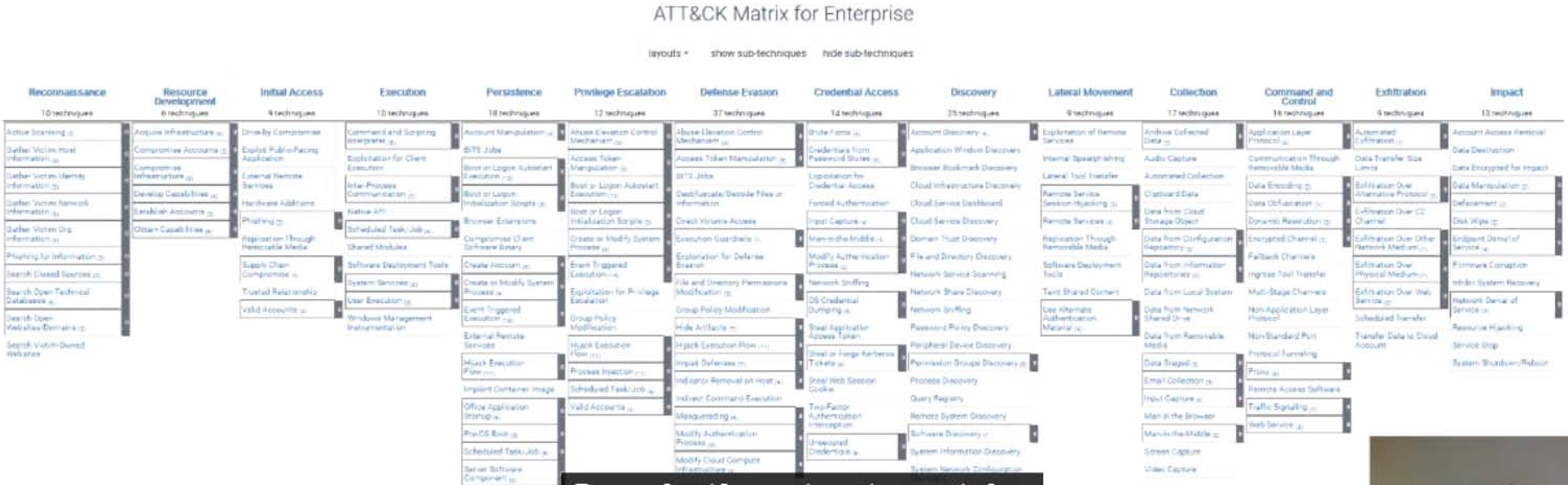
INFOSEC Skills

Hello, and welcome to this learning path for Python for cybersecurity.

Share

What is MITRE ATT&CK?

- MITRE ATT&CK is a tool developed by the MITRE Corporation to improve cybersecurity understanding
- It maps different attacker techniques and procedures to the cyberattack life cycle and an adversary's goals



So, let's start out by talking about MITRE ATT&CK.

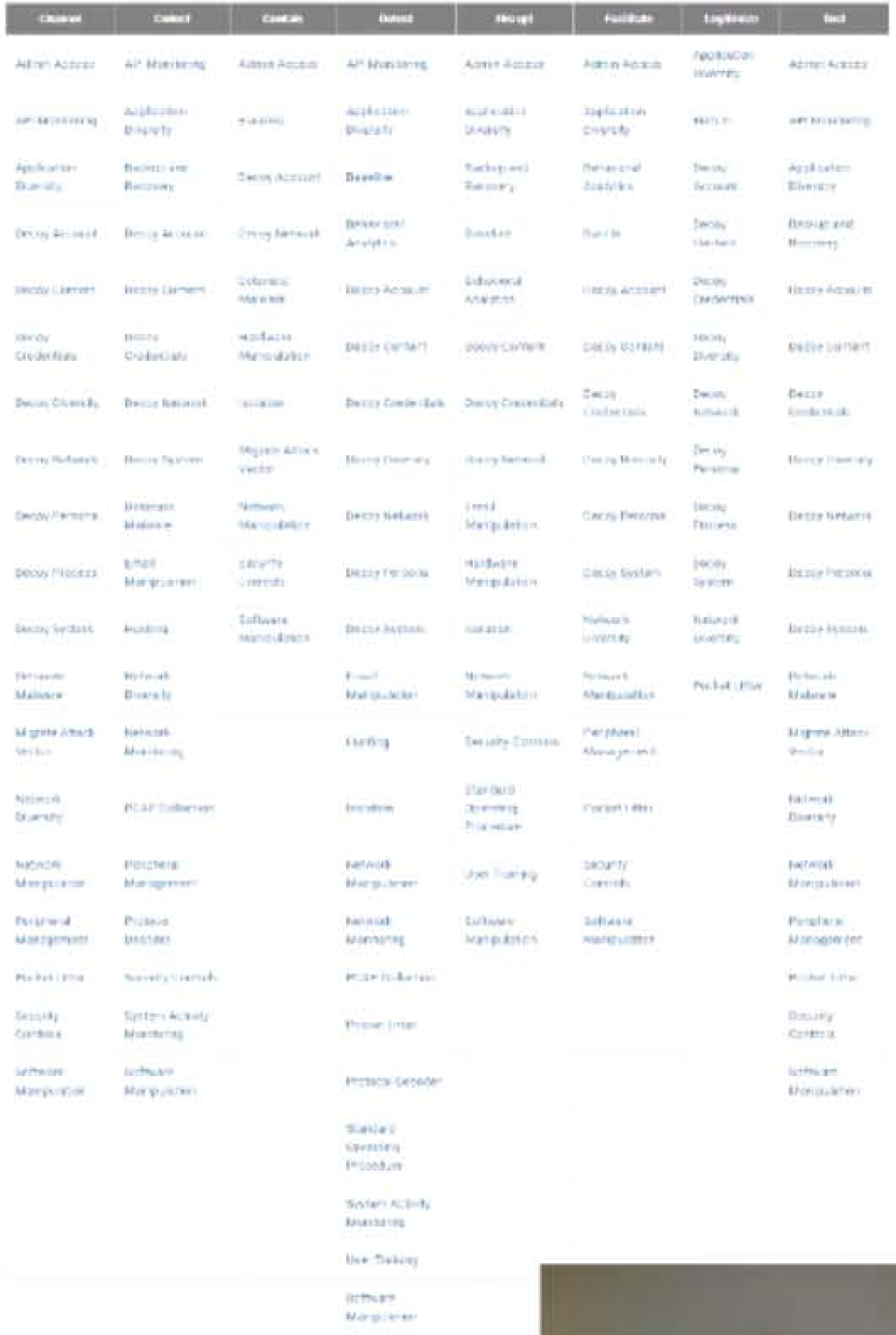
INFOSEC Skills

0:30 / 8:32

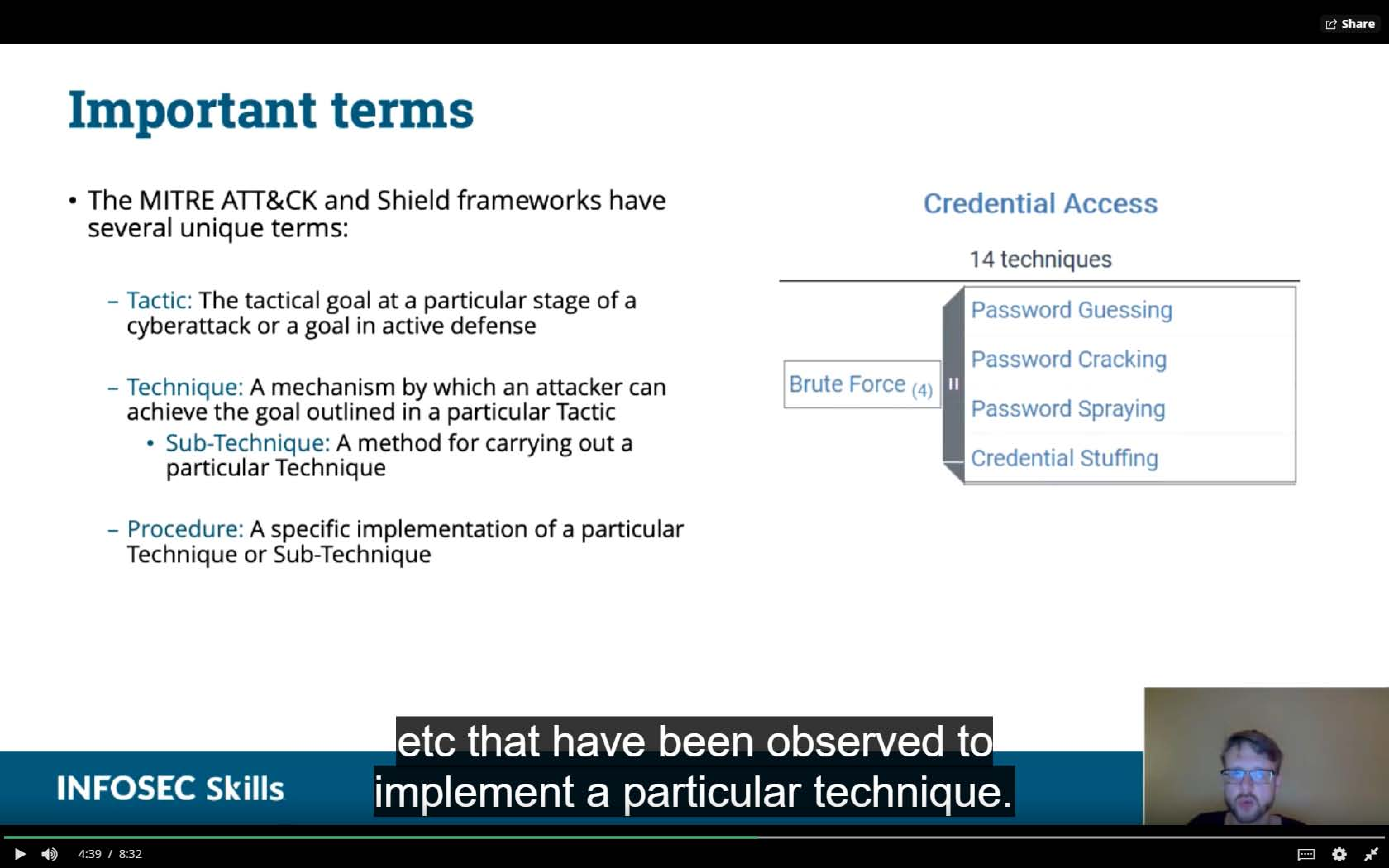
Share

What is MITRE Shield?

- MITRE Shield was developed by MITRE to promote active defense
- It identifies different goals that an active defender may have and outlines methods for achieving those goals



2:59 / 8:32



Important terms

- The MITRE ATT&CK and Shield frameworks have several unique terms:
  - Tactic: The tactical goal at a particular stage of a cyberattack or a goal in active defense
  - Technique: A mechanism by which an attacker can achieve the goal outlined in a particular Tactic
    - Sub-Technique: A method for carrying out a particular Technique
  - Procedure: A specific implementation of a particular Technique or Sub-Technique

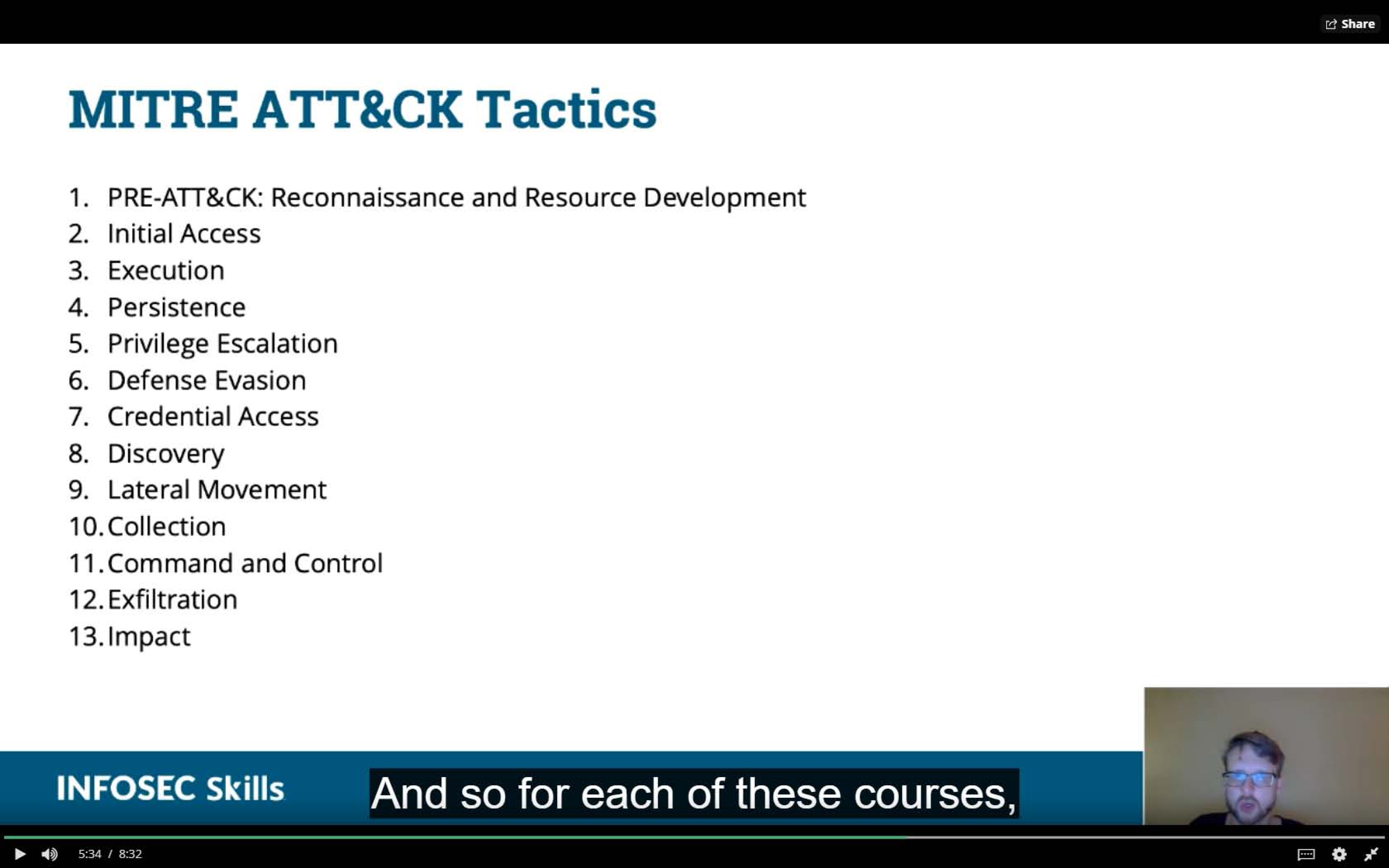
Credential Access

14 techniques

Brute Force (4)	Password Guessing Password Cracking Password Spraying Credential Stuffing

INFOSEC Skills

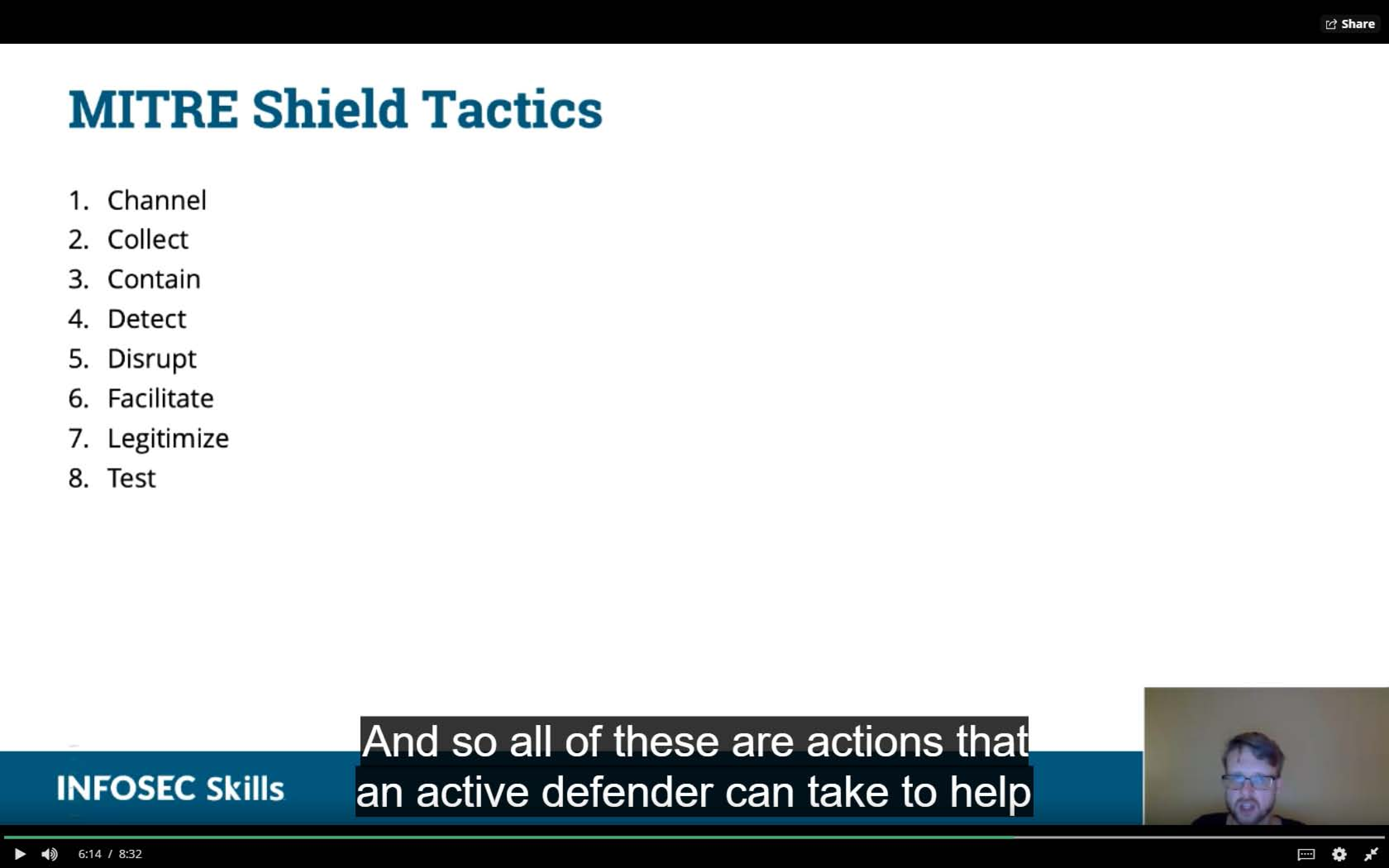
etc that have been observed to implement a particular technique.



MITRE ATT&CK Tactics

1. PRE-ATT&CK: Reconnaissance and Resource Development
2. Initial Access
3. Execution
4. Persistence
5. Privilege Escalation
6. Defense Evasion
7. Credential Access
8. Discovery
9. Lateral Movement
10. Collection
11. Command and Control
12. Exfiltration
13. Impact

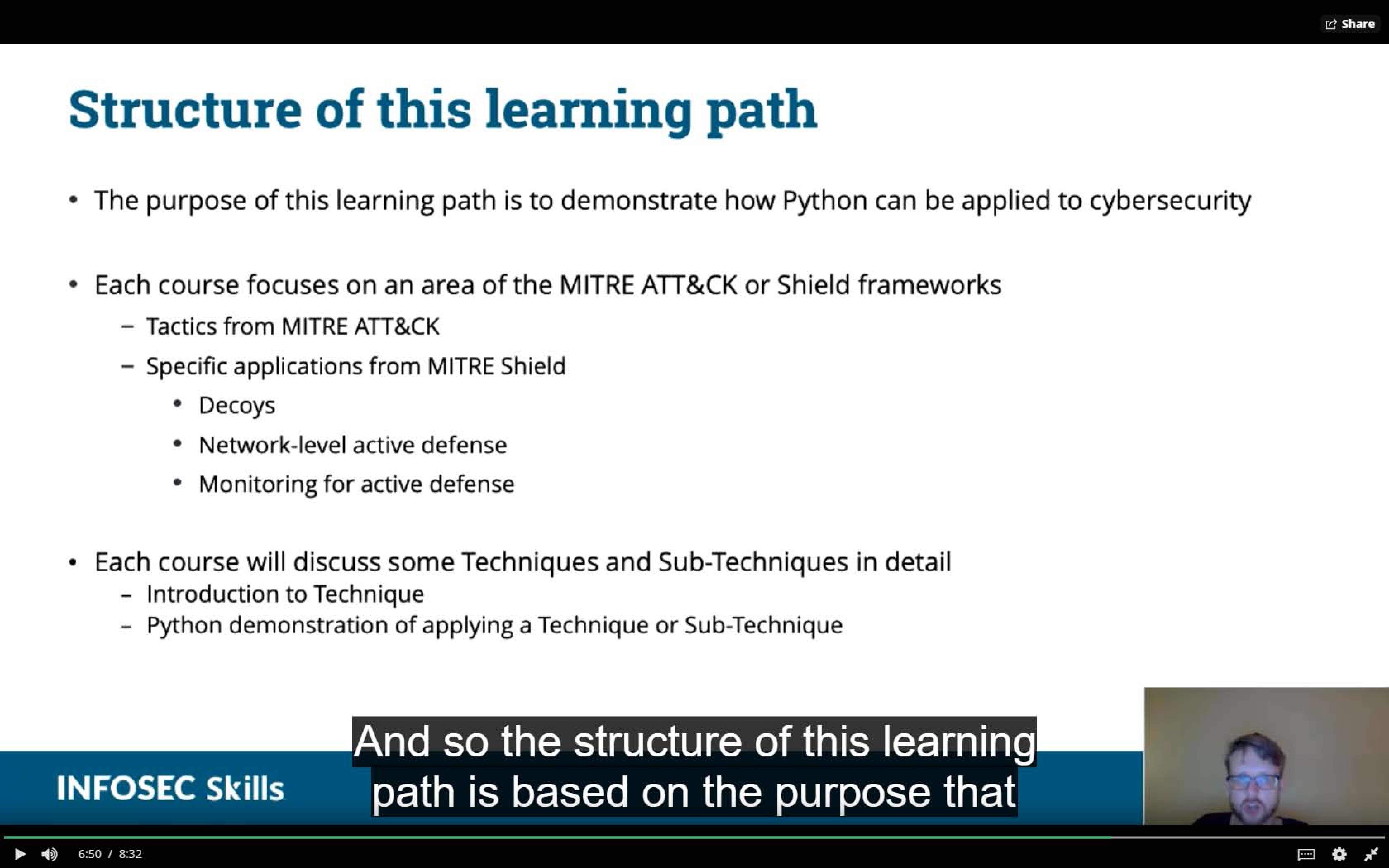
And so for each of these courses,



MITRE Shield Tactics

1. Channel
2. Collect
3. Contain
4. Detect
5. Disrupt
6. Facilitate
7. Legitimize
8. Test

And so all of these are actions that
an active defender can take to help



Structure of this learning path

- The purpose of this learning path is to demonstrate how Python can be applied to cybersecurity

- Each course focuses on an area of the MITRE ATT&CK or Shield frameworks
  - Tactics from MITRE ATT&CK
  - Specific applications from MITRE Shield
    - Decoys
    - Network-level active defense
    - Monitoring for active defense

- Each course will discuss some Techniques and Sub-Techniques in detail
  - Introduction to Technique
  - Python demonstration of applying a Technique or Sub-Technique

INFOSEC Skills

And so the structure of this learning path is based on the purpose that