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,







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



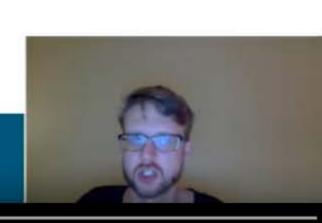
java and similar languages.



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 INFOSEC Skills of specific attack and shield techniques.





Section 1: Introduction to MITRE ATT&CK and Shield

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

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





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

Chimel	Centr	Contain	Direct	Recipi	fulltate	Logitimin	feet
Altre Actors	Air Montering	Altern Access	All Monthlys	Admit Amoun	Admin Appaid	reportation inverse;	Abres Action
ne princing	Aughtralian Binawity	7-8100	Aughorites Distant	MARKS IN	Sophiston Courty	NO F	
Application Districts	Receives	Sworthermal	Decello:	tacique) tamey	Mehanichal Josephin	Swin, Scount	Applicates Electry
(teory 41 month	Dency McCount	Strong Saltmoods	Behaviorel Analytics	Santas	Numerola	Sensy the hair	Deplacand Harmon
Decay Liener	herry (armer)	Colorese Majorie	інер Асмат	Educació Antigent	HED Account	DESTINATION	tieny écolit
covered to the control of the contro	CradeCate	Merculatur	\$4111 (WTM*)	DWG/Contex	DICH KIMIN	HOON; Diversity	Batteriories
Decay Chernilly	Designation	-	Decry Crede Sale	Davy Crewellish	Cecip Codectals	Decey formació	0+119 ()b116.0k
Ckyrn Mediatric	Henry System	Major Arios Vector	Here beenly	(Lary lane) - E	Contraction (set)	Decay Paratrop	House transaction
Decoy/errors	Denovate Medico e	Newson Mangalaker	Denny Nethanis	i est Marguletur	Cacry Electris	Second Entiresis	Detry Network
Decay Placess	gradi Margrunner	sacy/fe sweets	District Twiston	Haldware Mespulation	Disciplination	(MON) System	Basis Person
Sector Systems	Austra)	Software regroupers	Decre bytom	had at an	Marin, sar is programa	National R Level Title	Rette System
Malloca	Brans by		Board pro-later	Navquistics	Notes to Adjust to the state of	Projet (flor	Perturate Rindorsen
Migrata Attach Nel hoo	bjehjunek. Meserkering		Turbig	Security Commission	Perphoni Newspeed		Magney Alter Service
Notice of Disposity	PLAP Collectors		transferm.	Darbut Steeling Fix stan	Cocurt (May		(alma) Disertos
Menteron. PROVIN	Politicale Management		tarrech Margo, texes	Use Turky	security Coerrols		pochecky descripationers
Pergrand : Management	Proteon: Motifet		harmed Averaging	Eurhwer Wanpukston	Delivate Number		Persitoral Managaryan
Pickel Inc.	Society Certable		ecce in being				Probabilities
Cordona	System Activity Monthship		Present from				Dosawy Corects
settwise Mangarities	terbuare Mar parame		Promov Secretar				tomore Bringsalders
			Statie C System (*1000/cm				
			Society Activity Ameniating				
			New Trabers				
			(critical) Morpileran				

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

Password Guessing
Password Cracking
Password Spraying

Credential Stuffing

etc that have been observed to implement a particular technique.



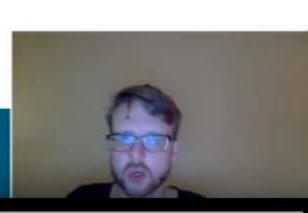


MITRE ATT&CK Tactics

- 1. PRE-ATT&CK: Reconnaissance and Resource Development
- Initial Access
- 3. Execution
- 4. Persistence
- 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,



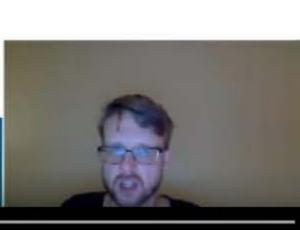


MITRE Shield Tactics

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

INFOSEC Skills

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

