Python and cybersecurity

Security professionals use a variety of tools.
One of those tools is computer programming.
Programming is used to create a specific set of instructions for a computer to execute tasks.
Let's take an example of a vending machine.
Think of a vending machine as a computer that supplies food or drinks to customers.
To receive an item, the customer inserts the money into the machine and then select the item they want.
Let's say the customer provides the machine with a value of $5.
The machine stores this value while you make your selection.
If you select a candy bar that costs $2, the machine takes this input, otherwise known as an instruction, and then understands to output your candy bar for $2 and provides the change back of $3.
There are many programming languages in existence.
Here, we'll focus on Python.
Python is considered to be a general-purpose language.
This means that it can create a variety of different programs, and it isn't a specialized in any particular problem in fields such as web development and artificial intelligence.
Python is typically used to build websites and perform data analysis.
In security, the main reason we use Python is to automate our tasks.
Automation is the use of technology to reduce human and manual effort to perform common and repetitive tasks.
Python is generally best for automating short, simple tasks.
For example, a security analyst who's dealing with a security incident might have a log with necessary information.
Reading through these manually would take too much time, but Python can help sort through this so the analysts can find what they need.
As another example, an analyst might use Python to manage an access control list, the list that controls who can access the system and its resources.
It would be potentially less consistent if the analysts had to manually remove an employee's access every time they left the company.
However, a Python program can periodically monitor this instead.
Or, Python could also perform some automated tasks like analyzing network traffic.
Though these tasks can be done through outside applications, they are also possible through Python.
In addition to automating individual tasks, Python can combine separate tasks into one workstream.
For example, imagine a playbook indicates that an analyst needs to resolve a certain situation by delivering a file and then notifying the proper individuals.
Python can connect these processes together.
So why exactly might a security professional choose Python for these tasks?
There are several advantages Python has as a programming language.

For one, Python is user-friendly because it resembles human language, it requires less code, and it's easy to read.
Python programmers also have the benefit of following standard guidelines to ensure consistency with the design and readability of code.
Another great reason for learning Python is that there's a large amount of online support.
Python also has an extensive collection of built-in code that we can import and use to perform many different tasks.
These are just some of the reasons why Python continues to be in high demand across different industries throughout the world.
You'll most likely use it in your security career.
Wow!
All of this sounds great.
Let's take a short break, and next, we'll finally get to run some Python code.
I'll meet you in the next video.

Revision #1
Created 8 December 2023 23:14:41 by naruzkurai
Updated 19 December 2023 03:38:35 by naruzkurai