Python Study- Sprint 1

Week 0: Group Basics

Learn Python through hands-on projects leading to AWS CloudTrail analysis.

When: Saturdays - 10:00 AM - 11:30 AM EST

How long? November 1, 2025-January 17, 2026 (w/ breaks for holidays)

Where: CSOH Zoom

Connect: CSOH Discord in the Learning channel section

Special thanks to Cloud Security Office Hours for providing the space.

This will be our shared drive: CSOHP Open Share

*Warning: This link is available to anyone who has it so please be mindful of what you share.

Week 1: Python Basics

(November 1, 2025)

Focus: Install Python, set up an environment, and run your first scripts.

Objectives:

- Print messages, work with variables and strings, understand numbers.
- Run scripts in Python
  Project: Write a small script that asks for input and prints a message.
  Resources: Python Official Docs, W3Schools Python

Week 2: Reading and Filtering Logs

(November 8, 2025)

Focus: Open text files, filter keywords, detect patterns like "DROP" or "DENY" in fake firewall logs.

Objectives:

- Read files line by line
- Filter lines with keywords
- Write filtered results to a new file
  Project: Create a fake firewall log and filter blocked traffic.
  Resources: Python Morsels Reading Files, W3Schools File Handling

Week 3: Lists, Dictionaries, and Loops

(November 15, 2025)

Focus: Store structured data and process it using loops.

Objectives:

- Create and iterate through lists
- Use dictionaries for key-value data
- Count occurrences of event types
  Project: Threat Hunting mini-project counting event names in logs.
  Resources: W3Schools Lists, W3Schools Dictionaries, Real Python For Loops

Week 4: Flask Basics

(November 22, 2025)

Focus: Create a simple web server using Flask and understand routes.

Objectives:

- Serve content via Flask routes
- Create dynamic pages
- Understand app.run() and debug mode
  Project: Flask Hello World with multiple routes.
  Resources: Flask Docs Quickstart, Real Python Flask Tutorial

Week 5: User Input and Forms in Flask

(December 6, 2025)

Focus: Handle user input on web pages and store data locally.

Objectives:

- Use GET and POST requests
- Capture form data using Flask
- Persist data in a file
  Project: Simple To-Do App with forms and local storage.
  Resources: Writing To File in Python, File Write

Week 6: JSON Crash Course

(December 13, 2025)

Focus: Read, parse, and write JSON files in Python.

Objectives:

- Use json.loads() and json.dump()
- Open sample CloudTrail log
- Extract key fields like eventName, userIdentity.userName, and sourceIPAddress
  Project: Load JSON and print selected fields.
  Resources: Python JSON Module, W3Schools Python JSON

Week 7: Analyzing Local Logs

(December 20, 2025)

Focus: Parse JSON logs and extract insights.

Objectives:

- Count top 5 eventNames
- Identify specific events like failed ConsoleLogin
- Optional: write results to CSV
  Project: Analyze CloudTrail JSON and summarize findings.
  Resources: Pandas JSON, Real Python JSON

Week 8: Intro to Boto3 and S3

(January 3, 2025)

Focus: Access S3 buckets using boto3.

Objectives:

- Set up AWS credentials
- List buckets and objects
- Download files and print content
  Project: Download test.txt from S3 and display contents.
  Resources: Boto3 S3, SDK For Python

Week 9: CloudTrail + Boto3 Part 1

(January 10, 2026)

Focus: Fetch and parse CloudTrail logs from S3.

Objectives:

- List bucket objects
- Download and unzip .gz files
- Parse JSON events
  Project: Count events in a CloudTrail file and print first 5 eventNames.
  Resources: gzip Module, Boto3 S3 Download

Week 10: CloudTrail + Boto3 Part 2

(January 17, 2026)

Focus: Build a CloudTrail analyzer summarizing activity.

Objectives:

- Count top users, eventNames, and source IPs
- Detect IAM changes like CreateUser or PutRolePolicy
- Export results to CSV
  Project: Full CloudTrail analysis with summary output.
  Resources: Real Python CSV, AWS IAM Monitoring