→ Use a Python script to analyze security logs .

```python
import json
import csv

# Load the sample log file
with open("SIEM_Log_Analyzer/sample_logs.json", "r") as file:
    logs = json.load(file)
suspicious_events = []

# Events we want to track
flagged_events = ["DeleteUser", "DetachUserPolicy", "DeleteAccessKey", "PutBucketPolicy"]

# Go through each event
for event in logs.get("Records", []):
    event_name = event.get("eventName")
    if event_name in flagged_events:
        user = event.get("userIdentity", {}).get("userName", "Unknown")
        event_time = event.get("eventTime", "Unknown")
        suspicious_events.append({
            "User": user,
            "Event": event_name,
            "Time": event_time
        })

# Write the output to a CSV file
with open("suspicious_activity.csv", "w", newline="") as csvfile:
    writer = csv.DictWriter(csvfile, fieldnames=["User", "Event", "Time"])
    writer.writeheader()
    writer.writerows(suspicious_events)

print(f"✅ Analysis complete! {len(suspicious_events)} suspicious events found.")
print("Report saved as suspicious_activity.csv")
```

→ Created sample JSON test data in the folder, then extracted data user, event and timestamp.

```json
{
    "Records": [
        {
            "eventTime": "2025-09-08T12:30:00Z",
            "eventName": "DeleteUser",
            "userIdentity": {"userName": "test-admin"}
        },
        {
            "eventTime": "2025-09-08T13:15:00Z",
            "eventName": "CreateBucket",
            "userIdentity": {"userName": "dev-user"}
        },
        {
            "eventTime": "2025-09-08T14:00:00Z",
            "eventName": "PutBucketPolicy",
            "userIdentity": {"userName": "root"}
        }
    ]
}
```

→ Output showing User, event and timestamp as CSV format for review.