[1]:

```
import re
import datetime
from collections import defaultdict
```

[2]:

```
# Function to capture logs from a file
def capture_logs(file_path):
    logs = []
    with open(file_path, 'r') as file:
        logs = file.readlines()
    return logs
```

[3]:

```
# Function to correlate events based on predefined rules
def correlate_events(logs, rules):
    correlated_events = defaultdict(list)

    for log in logs:
        log_time = extract_log_time(log)
        for rule in rules:
            if re.search(rule["pattern"], log, re.IGNORECASE):
                correlated_events[rule["event_type"]].append((log_time, log.
 ↪strip()))

    return correlated_events
```

[4]:

```
# Helper function to extract timestamp from log
def extract_log_time(log):
    match = re.search(r'\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}', log)
    if match:
        return datetime.datetime.strptime(match.group(), '%Y-%m-%d %H:%M:%S')
    else:
        return None
```

[5]:

```
# Sample log file path (replace with your log file)
log_file_path = "system_logs.txt"

# Sample correlation rules (define more as needed)
correlation_rules = [
    {"pattern": r"Failed password", "event_type": "Failed Login Attempt"},
    {"pattern": r"error", "event_type": "System Error"},
    {"pattern": r"access denied", "event_type": "Unauthorized Access"}
]
```

[6]:

```
# Main logic
logs = capture_logs(log_file_path)
correlated_events = correlate_events(logs, correlation_rules)

# Display correlated events
```

```
for event_type, events in correlated_events.items():
    print(f"\nEvent Type: {event_type}")
    for event in events:
        log_time, log = event
        print(f"Time: {log_time}, Log: {log}")
```

```
Event Type: Failed Login Attempt
Time: 2024-08-24 10:15:23, Log: 2024-08-24 10:15:23 Failed password for user
root from 192.168.1.1 port 22 ssh2
Time: 2024-08-24 10:20:00, Log: 2024-08-24 10:20:00 Failed password for user
guest from 192.168.1.3 port 22 ssh2

Event Type: System Error
Time: 2024-08-24 10:16:45, Log: 2024-08-24 10:16:45 error: unable to connect to
database

Event Type: Unauthorized Access
Time: 2024-08-24 10:17:30, Log: 2024-08-24 10:17:30 access denied for user
'admin'@'localhost' (using password: YES)
```

[ ]:

```

```