SIEM Log Simulator Guide

# 🧪 SIEM Log Simulator

\*\*Author:\*\* Charles G. | Auroch Security

\*\*Purpose:\*\* Generate synthetic Windows-style security events to test SIEM pipelines or log ingestion.

---

## ⚙️ Features

- Outputs fake logs to a `.txt` file and console.

- Mimics real-world log patterns (failed logins, suspicious PowerShell, malware alerts).

- Adjustable number of events with CLI args.

---

## 🚀 Usage

python siem\_log\_simulator.py -n 100 -o logs.txt

- `-n`: Number of logs to generate (default: 50)

- `-o`: Output file name (default: `simulated\_logs.txt`)

---

## 🔒 Sample Output

[2025-04-22 10:01:23] SECURITY - Failed login attempt for user 'jsmith' from IP 192.168.1.12

[2025-04-22 10:01:25] ALERT - Suspicious PowerShell command execution: 'Invoke-Mimikatz'

[2025-04-22 10:01:28] MALWARE - Detected malware hash match on file 'backdoor.vbs'

---

## 📦 Integration

Pipe these logs into a syslog server or ingest into ELK/Graylog for simulated traffic.

---

## 📁 Save as

`siem\_log\_simulator.py`

---