

SOAR EDR Playbook

Message with details contains

- Time
- Computer Name
- Source IP
- Process
- Command Line
- File Path
- Sensor ID
- Link to the detection (if applicable)

