Manual de Execução — Fawkes Anti-Ransomware

1. Introdução

Este manual tem como objetivo orientar o usuário na execução, utilização e verificação do funcionamento do **Fawkes** , demonstrando como realizar testes, interpretar alertas e confirmar a detecção de ameaças.

2. Inicialização do Sistema

1. Acesse a pasta onde o Fawkes foi instalado ou onde o executável foi gerado (exemplo):

C:\Fawkes_AntiRansomware

2. Caso esteja utilizando o código Python, execute:

python fa.py

3. Se estiver usando o executável gerado:

dist\fa.exe

4. Ao iniciar, o sistema exibirá a interface gráfica principal (GUI) do Fawkes, mostrando os módulos de monitoramento e logs em tempo real.

3. Estrutura de Pastas do Sistema

Durante a primeira execução, o Fawkes criará automaticamente as seguintes pastas no diretório principal do sistema:

FAWKES_AV_Logs	Armazena os registros de eventos e alertas de segurança.
FAWKES_AV_Quarantine	Guarda os arquivos suspeitos ou maliciosos isolados automaticamente.
FAWKES_AV_Honeypots	Contém arquivos isca monitorados para detecção de ransomwares.

Importante: não altere ou exclua os arquivos da pasta *Honeypots*, pois eles são essenciais para o funcionamento da detecção.

4. Interface e Operação

A interface principal do Fawkes exibe:

- **Botão "Iniciar Monitoramento"** – ativa a vigilância em tempo real nas pastas configuradas;
- **Botão "Parar Monitoramento"** – pausa o sistema sem encerrá-lo;
- **Área de Log** – mostra eventos recentes (arquivos modificados, acessos suspeitos etc.);
- **Indicador de Status** – mostra se o sistema está "Ativo" (verde) ou "Inativo" (vermelho).

Durante a operação, o Fawkes monitora as alterações nos arquivos em tempo real e identifica qualquer comportamento suspeito.

5. Visualização de Logs

Os eventos registrados ficam salvos na pasta:

C:\FAWKES_AV_Logs

Cada log é nomeado com a data e hora da execução (exemplo: log_2025-10-04.txt).

Os logs incluem informações como:

- Data e hora do evento

- Caminho do arquivo afetado
- Tipo de ação detectada (criação, modificação, exclusão)
- Processo responsável pelo evento
- Status da resposta do Fawkes (bloqueado, isolado, ignorado)

É recomendável revisar periodicamente os logs para identificar padrões de comportamento suspeito.

7. Quarentena

Arquivos detectados como suspeitos são movidos automaticamente para:

C:\FAWKES_AV_Quarantine

Nessa pasta, eles são renomeados e não podem ser executados.
O usuário pode limpar manualmente a quarentena se tiver certeza de que os arquivos são falsos positivos.

8. Encerramento e Manutenção

Para encerrar o sistema de forma segura:

1. Clique em **“Parar Monitoramento”** na interface.
2. Feche o programa normalmente.