



INSIDE THREAT

MANUAL DE UTILIZAÇÃO

1. INSTALAÇÃO

Para executar o programa é necessário instalar o Java na sua máquina, caso não esteja já instalado. Caso você não tenha instalado você pode encontrar em https://www.java.com/pt_BR/download/

2. INICIALIZAÇÃO

Após a instalação do programa é necessário que você tenha realizado o download dos arquivos de log, especificamente os da pasta r1 no seguinte link: <ftp://ftp.sei.cmu.edu/pub/cert-data/r1.tar.bz2>. Após estar com os arquivos baixados na sua máquina é hora de inicializar o programa, abra o arquivo Inside Threat.jar, é ele quem realizará as análises.

Figura 1 – Programa inicializado.

3. UTILIZAÇÃO

Antes de clicar para buscar insiders ou realizar comparações de análises é necessário carregar os arquivos de logs informados anteriormente. Inicialmente é necessário carregar o arquivo contendo as informações dos usuários. Clique no primeiro botão **Selecionar...**

INSIDE THREAT

1. Selecione todos os arquivos de log:

Users:

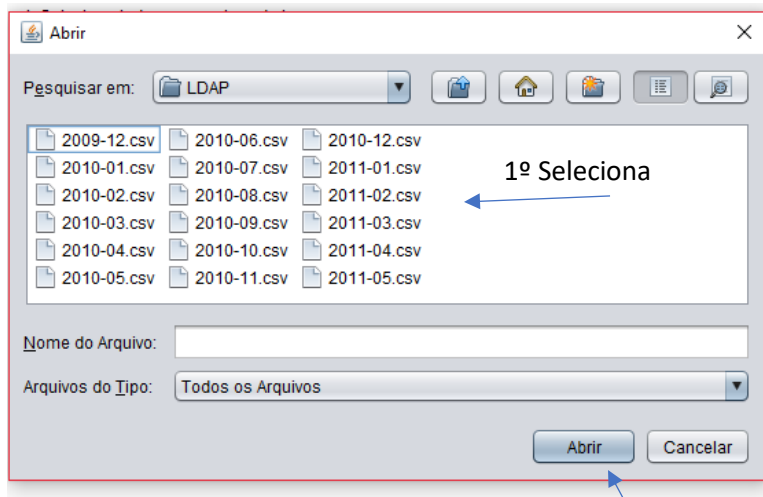
Selecionar...

Obs.: Para selecionar todos os arquivos pressione a tecla CTRL.

Selecione os arquivos com os dados de usuários.

Figura 2 – Clique no botão Selecionar...

Ao clicar irá abrir uma caixa de diálogo para você selecionar os arquivos, navegue até a pasta com os logs com os dados dos usuários e **pressionando CTRL** clique sobre cada arquivo que possua os logs. *Caso na sua pasta possua arquivos de logs apenas com os dados dos usuários então você pode clicar CTRL+A que todos os arquivos serão selecionados.* Após selecionar todos os arquivos necessários basta **clicar em Abrir**.



2º Clica em Abrir

Figura 3 – Selecionar os arquivos e abrir eles.

Agora que você selecionou os arquivos é necessário escolher um período a ser analisado. O programa lhe oferece 3 (três) possibilidades: Período entre datas, Data específica e Tudo.

2. Como deseja filtrar? ☒ Período entre datas ☐ Data específica ☐ Tudo

Data (início):

Data(fim):

Ler dados dos usuários

Insira as datas no formato: MM/dd/yyyy

Figura 4 – Selecionar as datas a serem analisadas.

- Período entre datas: Você pode informar duas datas para fazer um filtro, em que só será analisado os logs dentro daquele período.
- Data específica: Informa apenas uma data, ou seja, a análise será realizada apenas naquela data informada.
- Tudo: Todo o período dos logs será analisado.

Nessa etapa é importante que você informe a data seguindo o formato: Mês/Dia/Ano. Após selecionar o período de análise, basta clicar no botão **Ler dados dos usuários** e esperar realizar a leitura dos dados.

Agora que você realizou a leitura dos dados sobre os usuários é necessário enviar os dados de utilização de cada usuário. Basta clicar no botão **Selecionar...** e selecionar os arquivos necessários quando abrir a caixa de diálogo, como ocorreu com os dados dos usuários. Cuidado para não selecionar outros arquivos que não sejam com os dados de utilização.

Insira as datas no formato: MM/dd/yyyy

Dados: **Selecionar...** **Enviar**

1º Clica no Botão

4º Clica no Botão

Selecione os dados de utilização dos usuários.

Figura 5 – Selecionar os logs contendo as ações dos usuários.

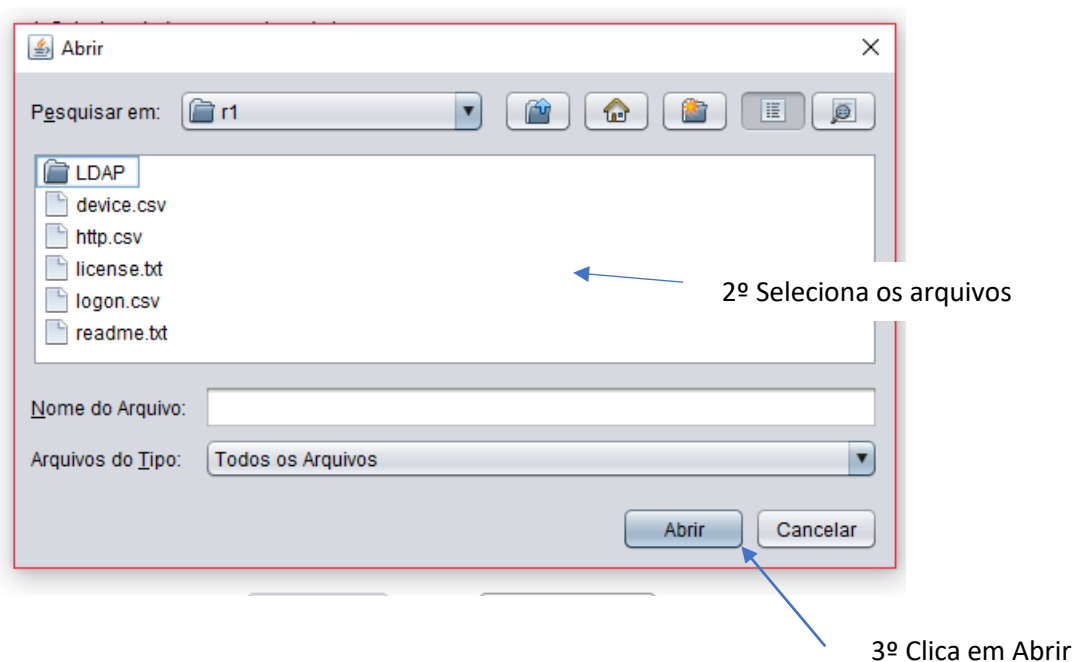
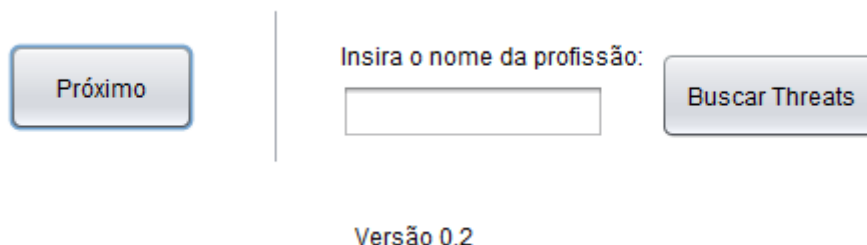


Figura 6 – Selecionar os arquivos.

Após selecionar os arquivos e clicar em **Abrir**, basta clicar no botão de **Enviar**. Então é só esperar que todos os arquivos sejam carregados. Ao finalizar o carregamento o botão **Próximo** estará disponível.



The interface consists of a horizontal layout. On the left is a button labeled 'Próximo'. To its right is a vertical line. Further right is a text label 'Insira o nome da profissão:' followed by an empty text input field. To the right of the input field is a button labeled 'Buscar Threats'. Below the input field, centered, is the text 'Versão 0.2'.

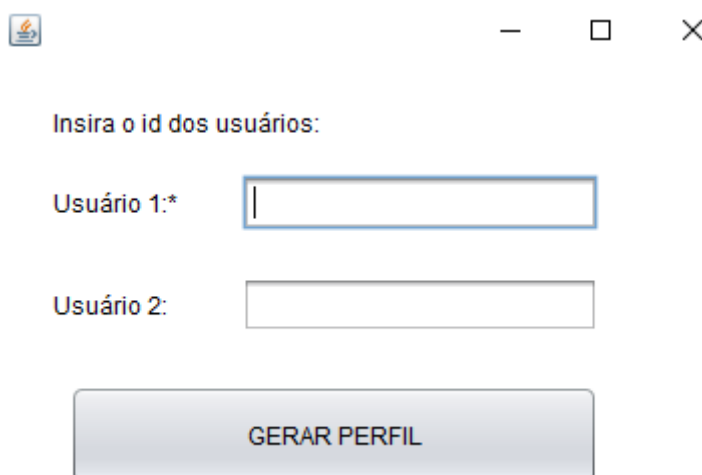
Figura 7 – Ações a serem realizadas.

O botão **Próximo** serve para realizar a análise de usuário(os) com comparações, enquanto o botão **Buscar Insiders** é para buscar quem pode ser o usuário infiltrado no sistema.

Comparar usuários:

Ao realizar todos os procedimentos acima e clicar no botão Próximo, irá surgir uma nova tela, em que você poderá inserir o ID de 1 (um) ou 2 (dois) usuários para realizar a comparação.

No caso de ter inserido apenas 1 usuário o sistema irá comparar o usuário com a média dos que possuem o mesmo cargo que ele. E em caso de 2 usuários, o sistema irá comparar o histograma de cada um. Então basta inserir os Ids e depois clicar no botão **GERAR PERFIL**.



The interface is a window with a title bar containing a logo and window controls. Below the title bar is the text 'Insira o id dos usuários:'. There are two text input fields. The first is labeled 'Usuário 1:*' and the second is labeled 'Usuário 2:'. Below the input fields is a large button labeled 'GERAR PERFIL'.

Figura 8 – Informar usuários a serem analisados.

Ao clicar no botão GERAR PERFIL será gerado um gráfico igual a este:

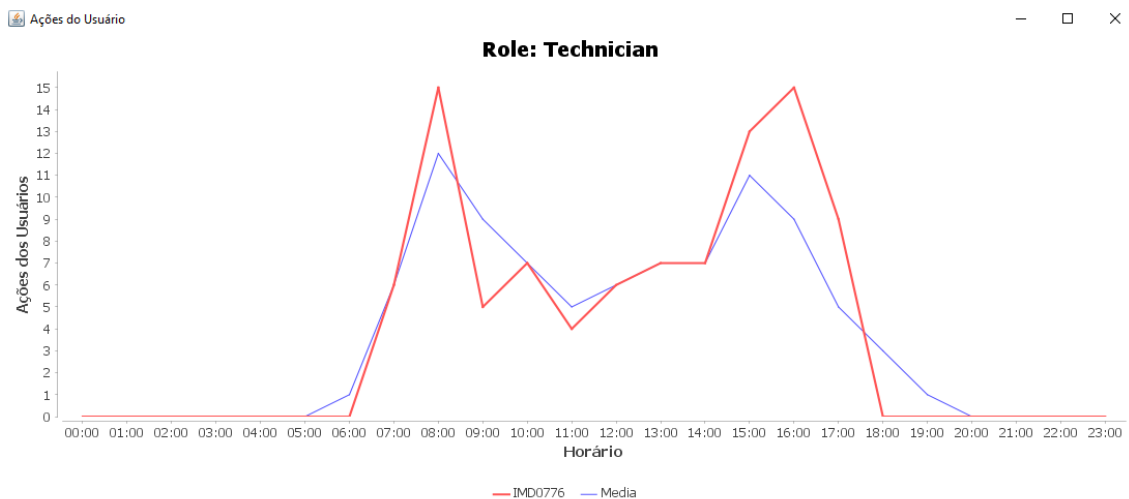


Figura 9 – Gráfico amostra de histograma de usuário e a média do papel dele.

Mostrando a média da pessoa e a média daquela profissão na empresa (foi informado apenas o nome de um usuário).

Ao gerar o gráfico, é possível analisar intervalos de tempos, digamos que desejamos analisar apenas a partir das 05:00 até as 20:00, basta clicar e arrastar o mouse da esquerda para a direita, formando um retângulo sobre a região desejada e para voltar ao normal basta clicar e arrastar para cima ou para a esquerda.

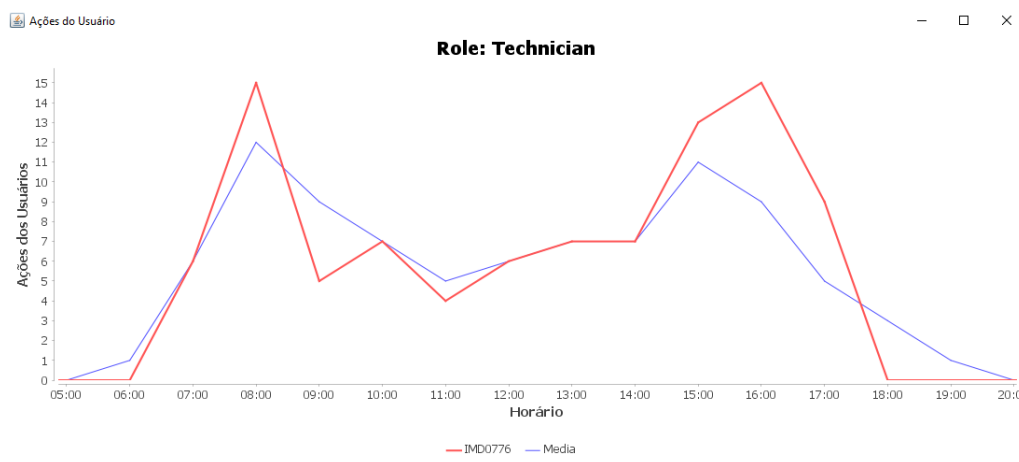


Figura 10 – Gráfico analisando período específico.

Buscar Insiders:

Para encontrar quem são os infiltrados basta inserir qual papel na empresa você deseja filtrar e clicar no botão **Buscar Insiders**, o programa irá realizar a análise e irá aparecer uma nova janela com uma lista dos Ids dos infiltrados em ordem crescente, ou seja, em primeiro quem possui mais chance de ser o infiltrado. Caso a lista não tenha nenhuma informação é porque não existe infiltrado naquele papel. Também é possível obter as informações dos usuários, basta clicar no id do usuário infiltrado, assim retornará todas as informações daquele usuário.