SECDAY - BEGINNER MONITOR

SDBM

WHOAMI?

- Analise e desenvolvimento de sistemas
- 9 anos de experiência em tecnologia e segurança da informação, atuando em órgãos governamentais, instituições financeiras, empresas de consultoria e telecomunicações, tanto nacionais quanto internacionais
- Principais certificações
  - ECIH – EC-Council Certified Incident Handler
  - ECIR – ElearnSecurity Certified Incident Responder
- Apaixonado por tecnologia
- Viciado em CTF
  - Campeão regional Hackaflag 2017
  - Campeão do CTF das forças armadas em 2017 – MANDABYTE
- Fundador do canal Security Every Day

DESAFIO

A SecDay, empresa especializada em treinamentos, contratou seus serviços para realizar o monitoramento de sua rede. O objetivo principal é assegurar um monitoramento eficiente da rede, priorizando a detecção de ameaças, coleta de logs e estabelecendo cenários para identificação de ataques.

AGENDA

OBJETIVOS DE APRENDIZADO

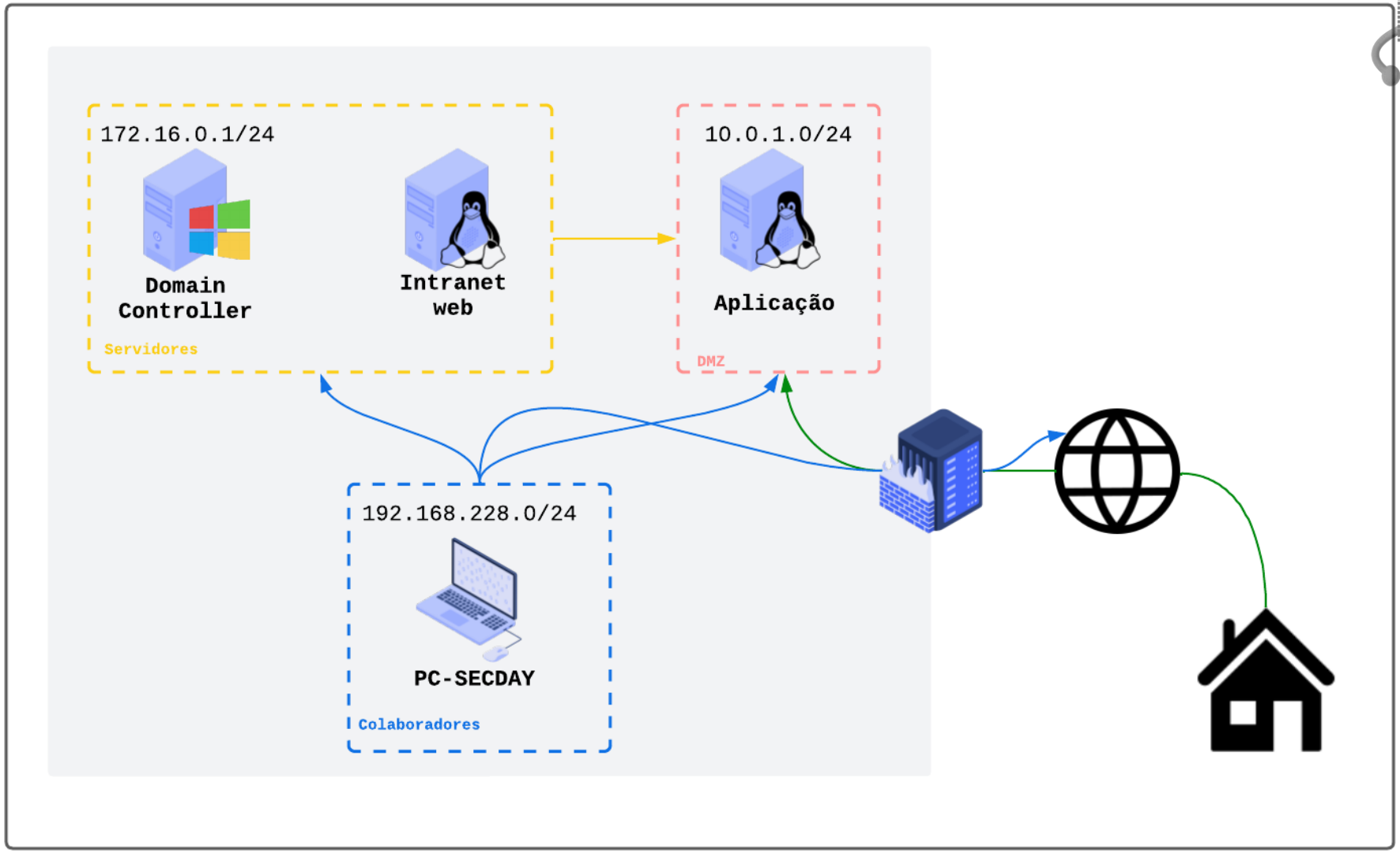
INTRODUÇÃO

PREPARAÇÃO DO AMBIENTE

PRATICA

OBJETIVOS DE APRENDIZADO

- Fundamentos de segurança defensiva
- Visão simplificada da arquitetura de rede e segurança corporativa
- Básico de monitoramento e configuração de sistemas operacionais Windows e Linux
- Firewall/IDS: Configuração e monitoramento básico
- Entendimento do processo de centralização de logs e sua importância no monitoramento
- Noções básicas de implantação do SIEM
- Visão geral do framework MITRE ATT&CK e sua utilidade
- Desenvolvimento de casos de uso simples para detecção de ataques
- Integração do Slack


172.16.0.1/24
Domain Controller
Intranet web
Servidores
10.0.1.0/24
Aplicação
DMZ
192.168.228.0/24
PC-SECDAY
Colaboradores

PRÉ-REQUISITOS

8GB de RAM

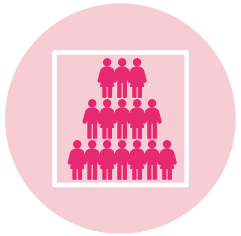
100 GB espeço em disco

Conexão com a internet

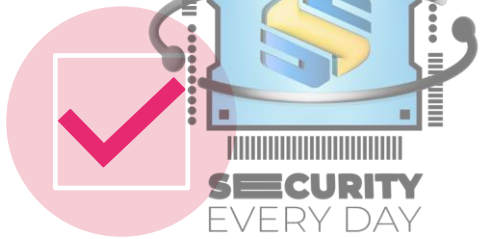
CPU Core I3 ou equivalente

INTRODUÇÃO

O QUE É SEGURANÇA DEFENSIVA?



QUAIS SÃO AS EQUIPES QUE COMPÕEM?

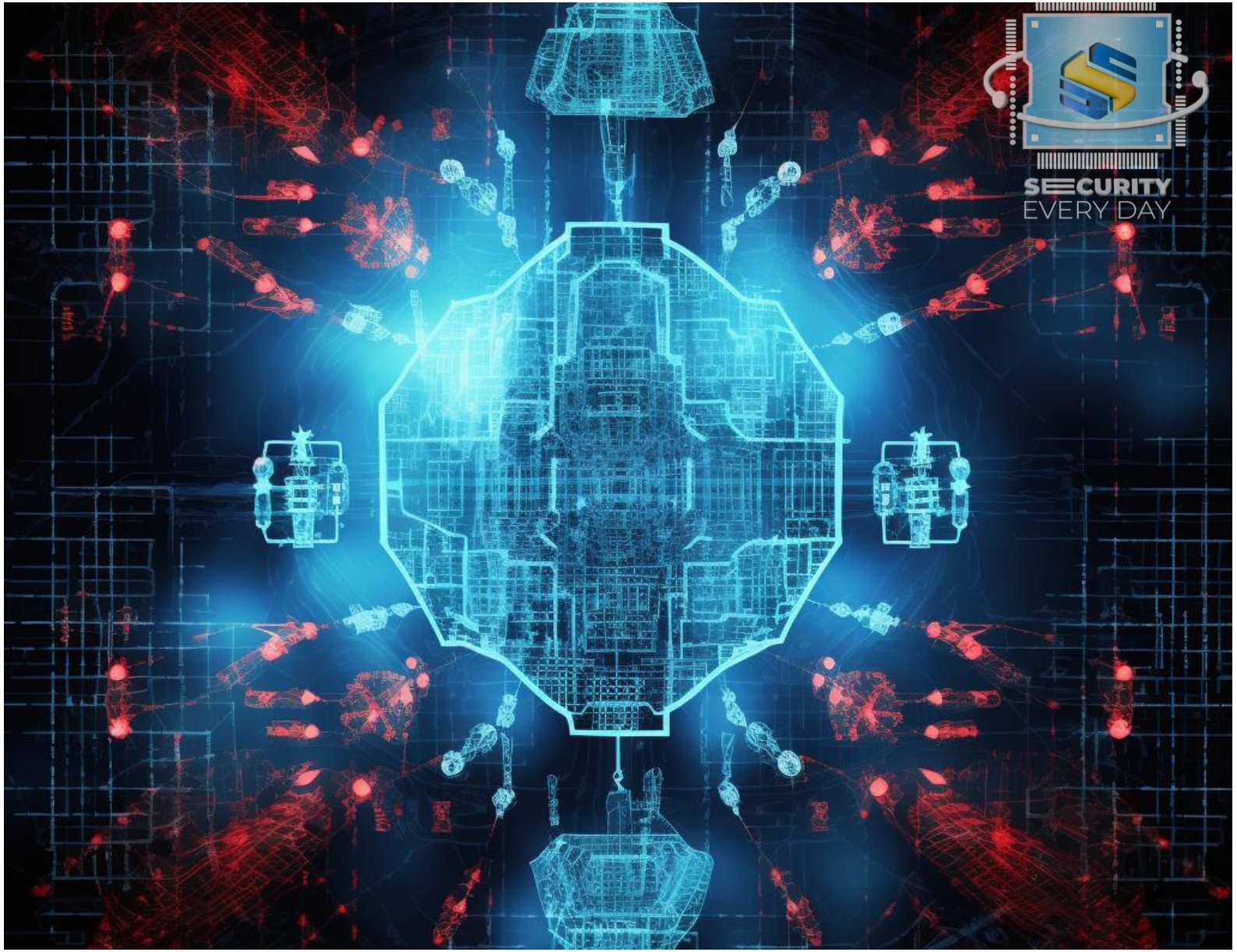


PREVENÇÃO X DETECÇÃO

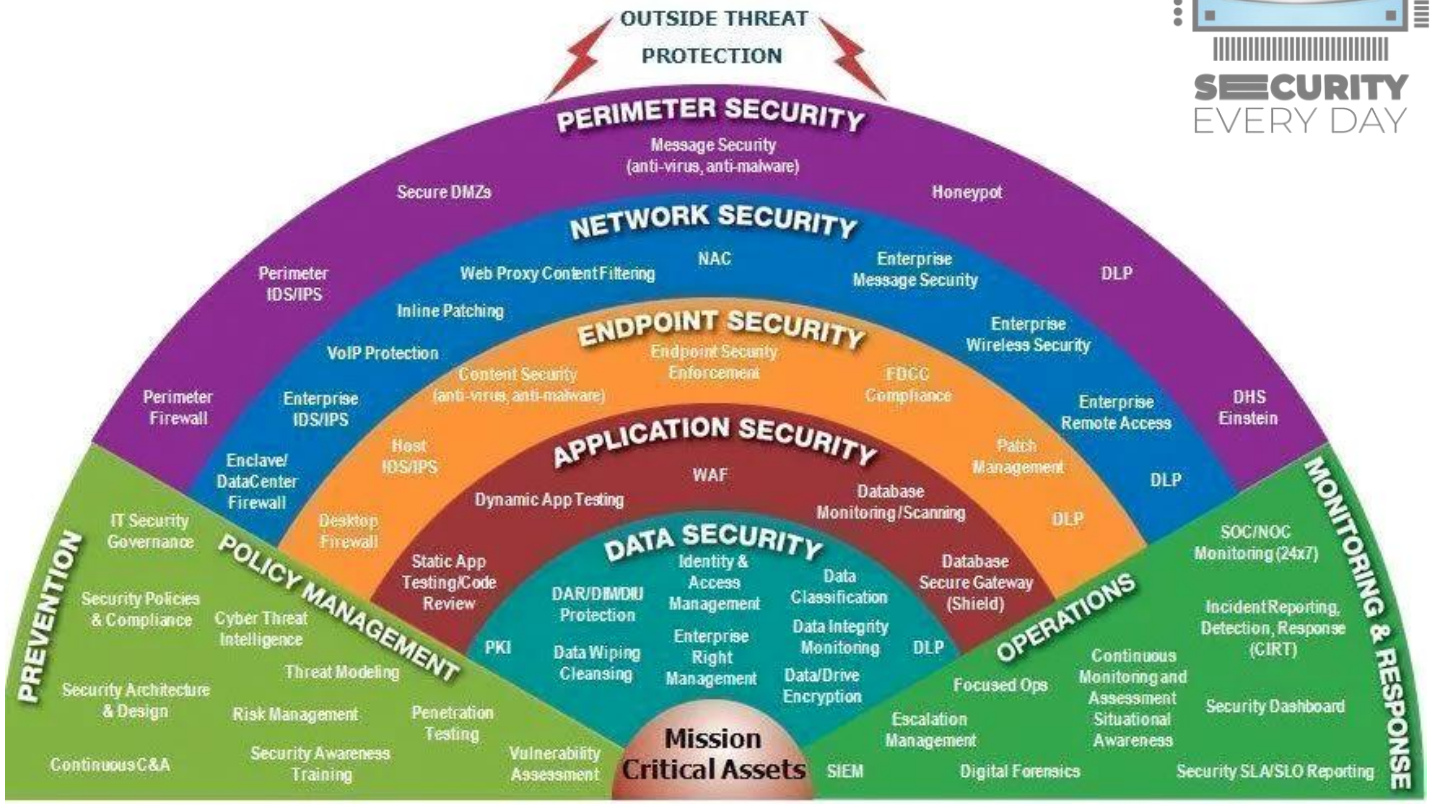
POR QUE MONITORAR?

O QUE É SEGURANÇA DEFENSIVA?

- Proteção do perímetro de rede
- Segurança de aplicativos
- Controle de acesso
- Monitoramento e detecção de ameaças
- Resposta a incidentes e recuperação
- Criptografia de dados
- Gestão de vulnerabilidades
- Defesa em profundidade
- Conscientização e treinamento em segurança



DEFESA EM PROFUNDIDADE

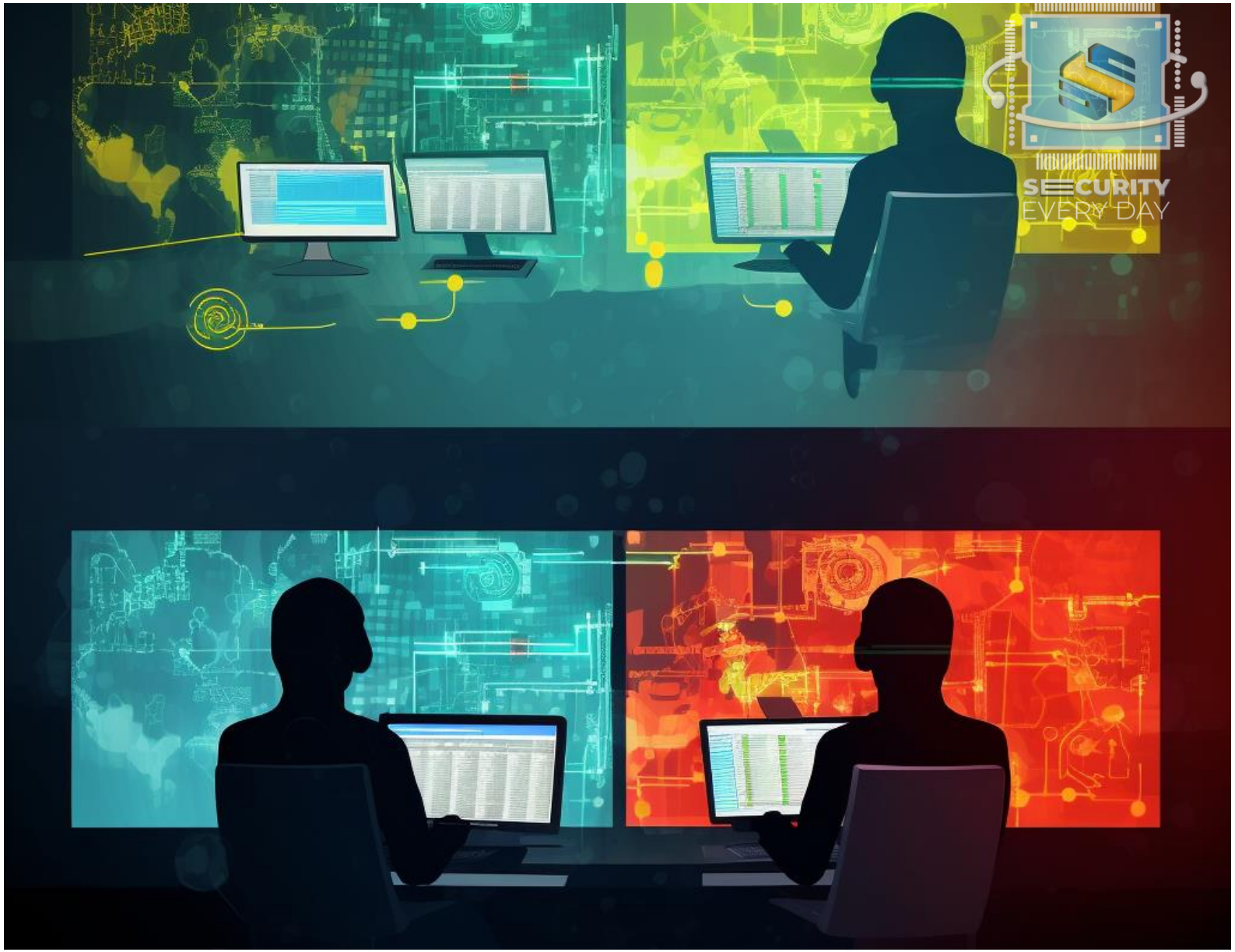


QUAIS SÃO AS EQUIPES QUE COMPÕEM?

- SOC
- CSIRT
- Gestão de vulnerabilidades
- SecOps
- Network Security
- AppSec
- Governança
- Threat Intelligence
- CloudSec
- Red Team

PREVENÇÃO VS DETECÇÃO

- Prevenção
  - Controle de acesso
  - Proteção de perimetro
  - Criptografia de dados
  - Gestão de vulnerabilidades
- Detecção
  - Monitoramento de eventos
  - Sistemas de detecção de intrusão
  - Ferramentas de SIEM
  - Análise de tráfego de rede



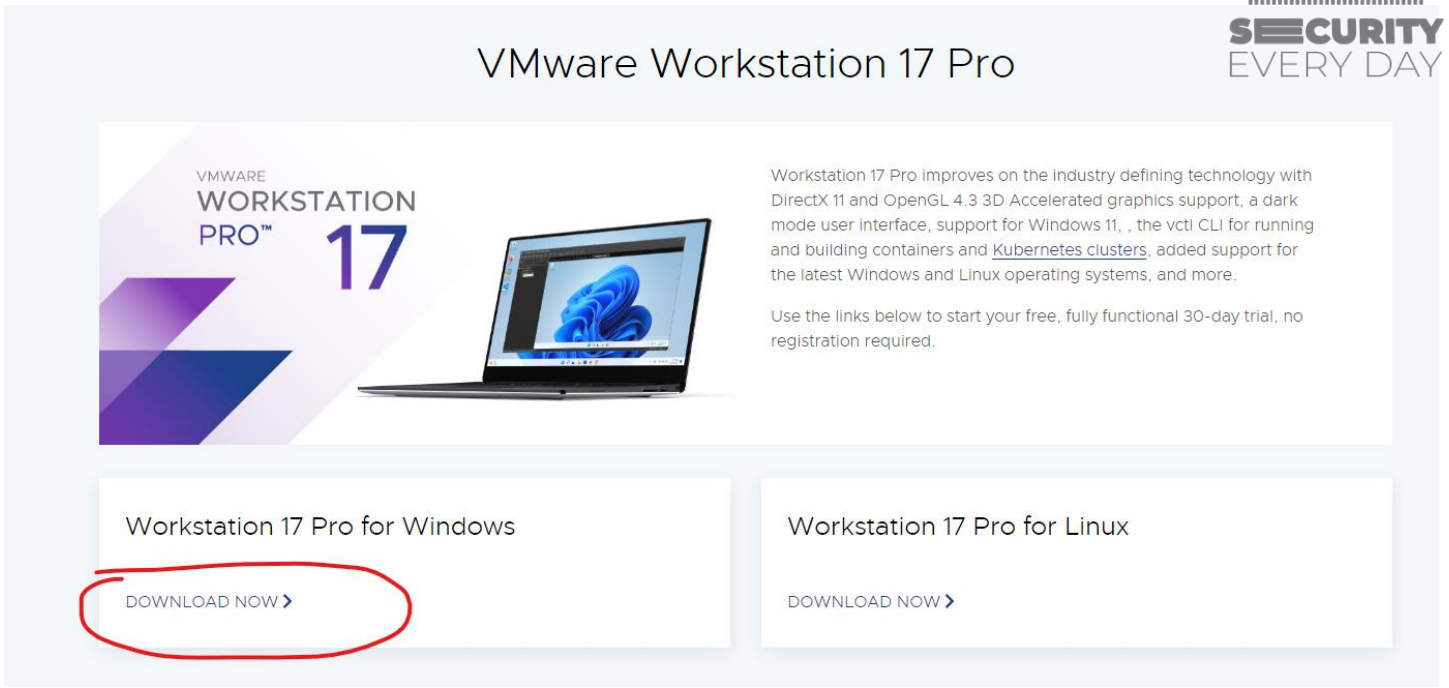
POR QUE MONITORAR?

- Detecção de ameaças e incidentes
- Identificar cenários não mapeados
- Prevenção a falhas e tempo de inatividade
- Rastreamento e responsabilização
- Conformidade e auditoria

PREPARAÇÃO DO AMBIENTE!

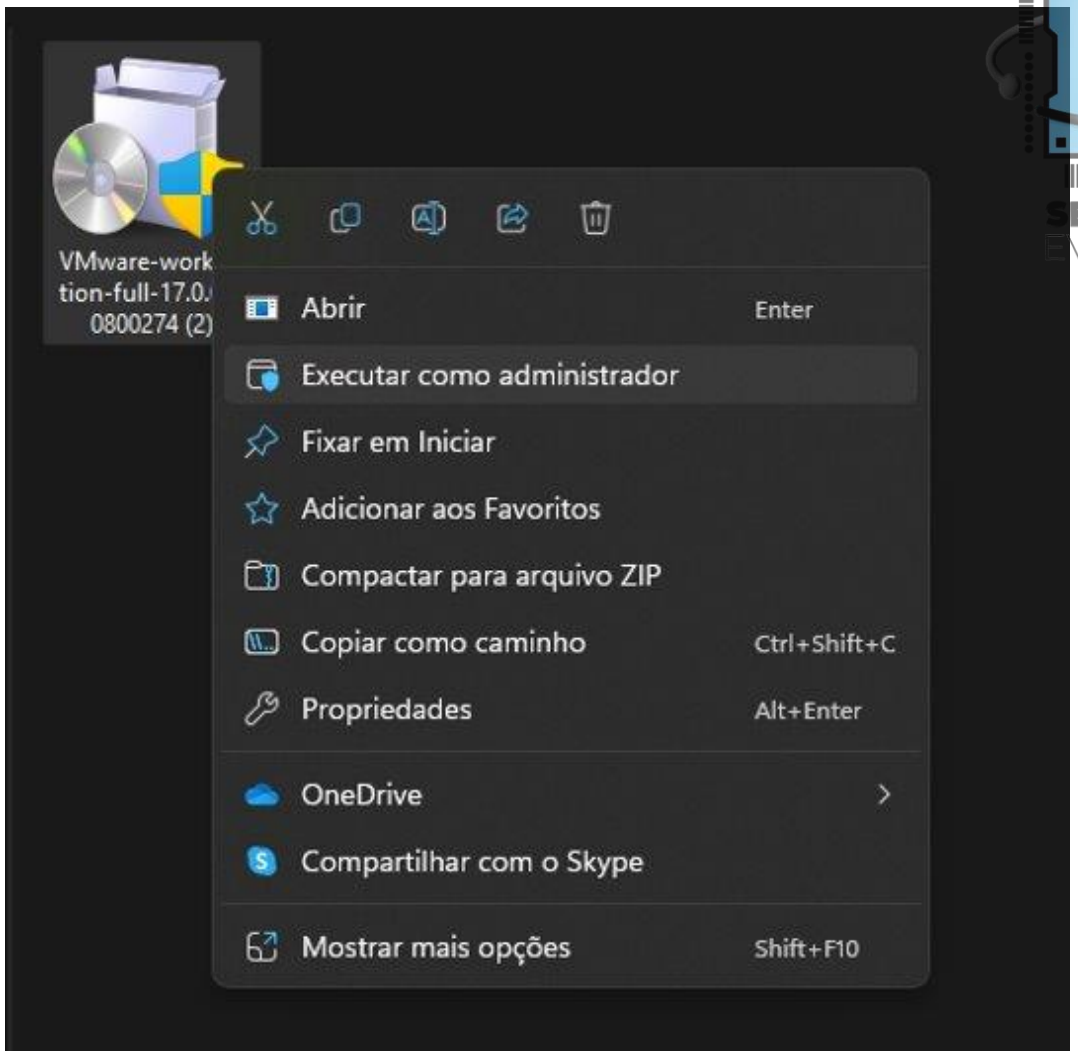
INSTALAÇÃO DO VMWARE WORKSTATION

- Faça o download do VMware Workstation no link
  - https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html



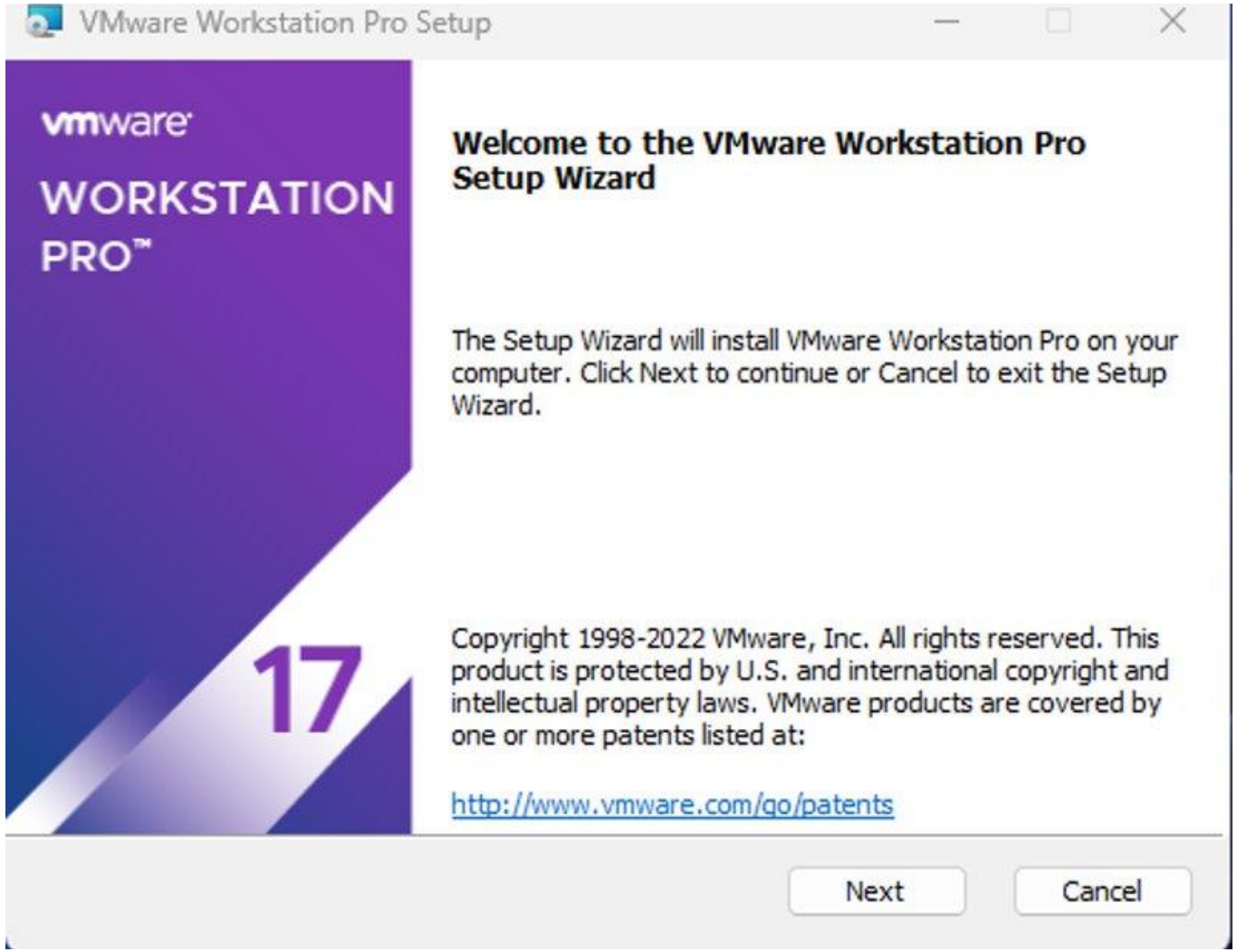
INSTALAÇÃO DO VMWARE WORKSTATION

- Vá até o executável e clique com o botão direto, escolha a opção "Executar como administrador"



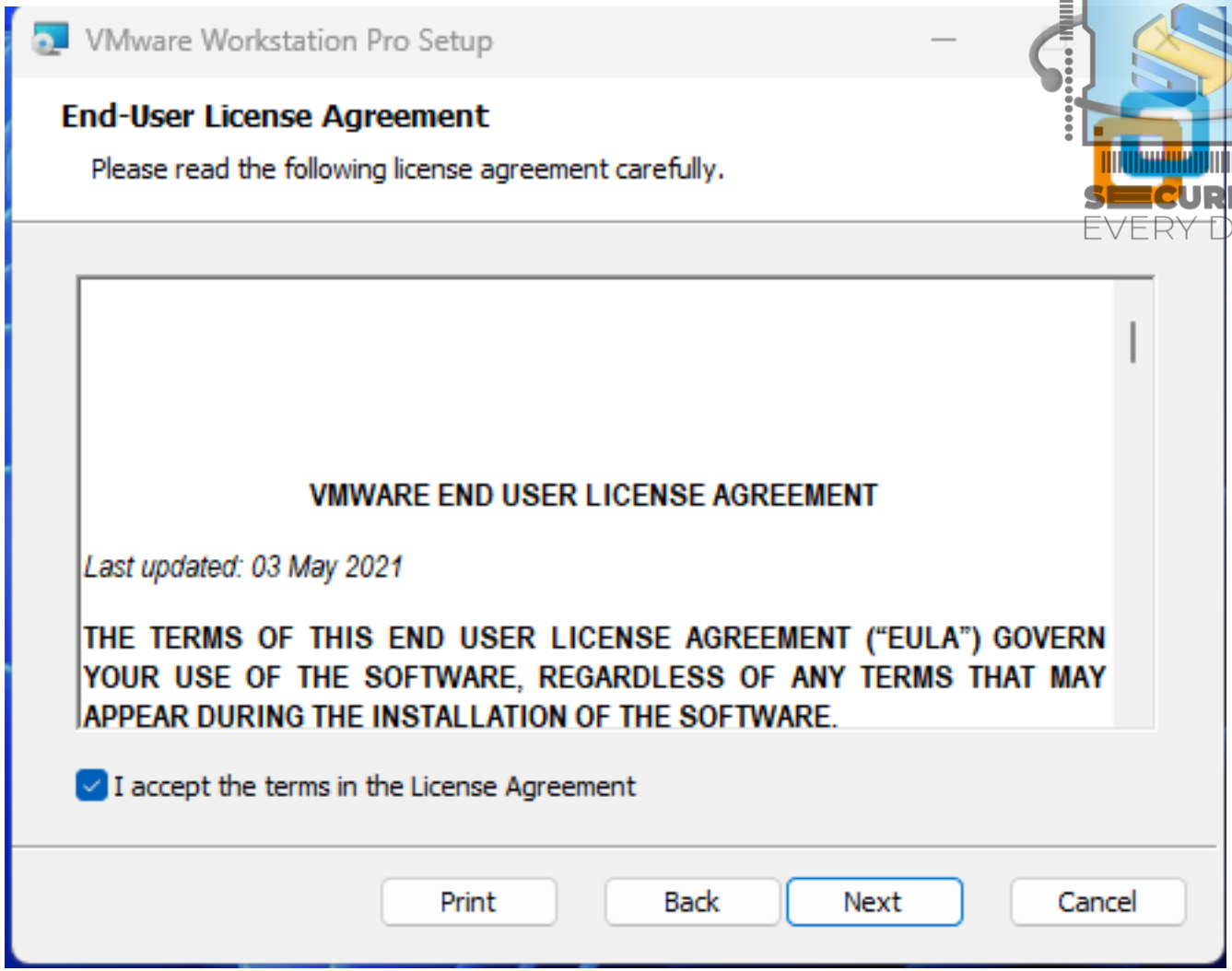
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



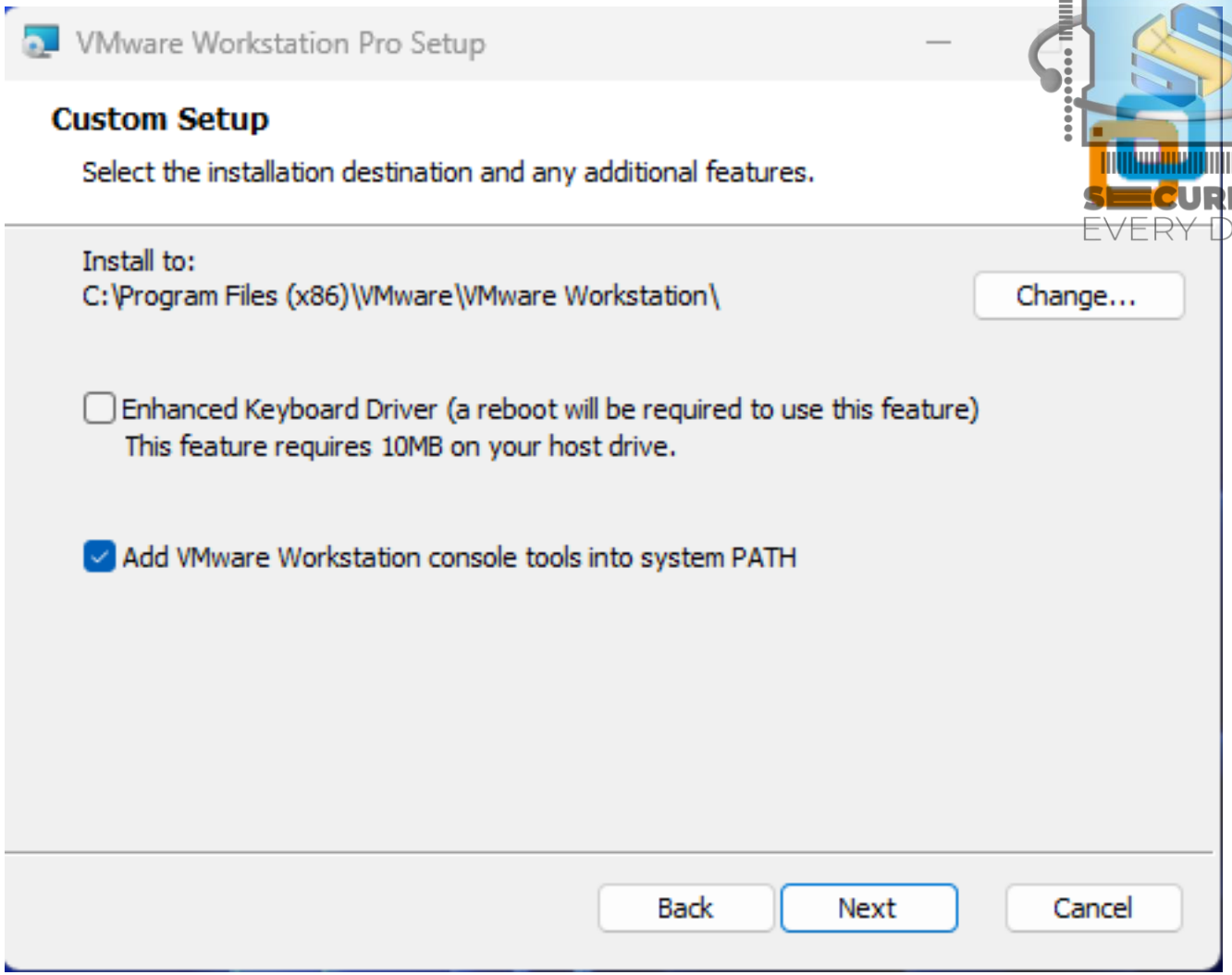
INSTALAÇÃO DO VMWARE WORKSTATION

- Aceite a licença e clique em "Next"



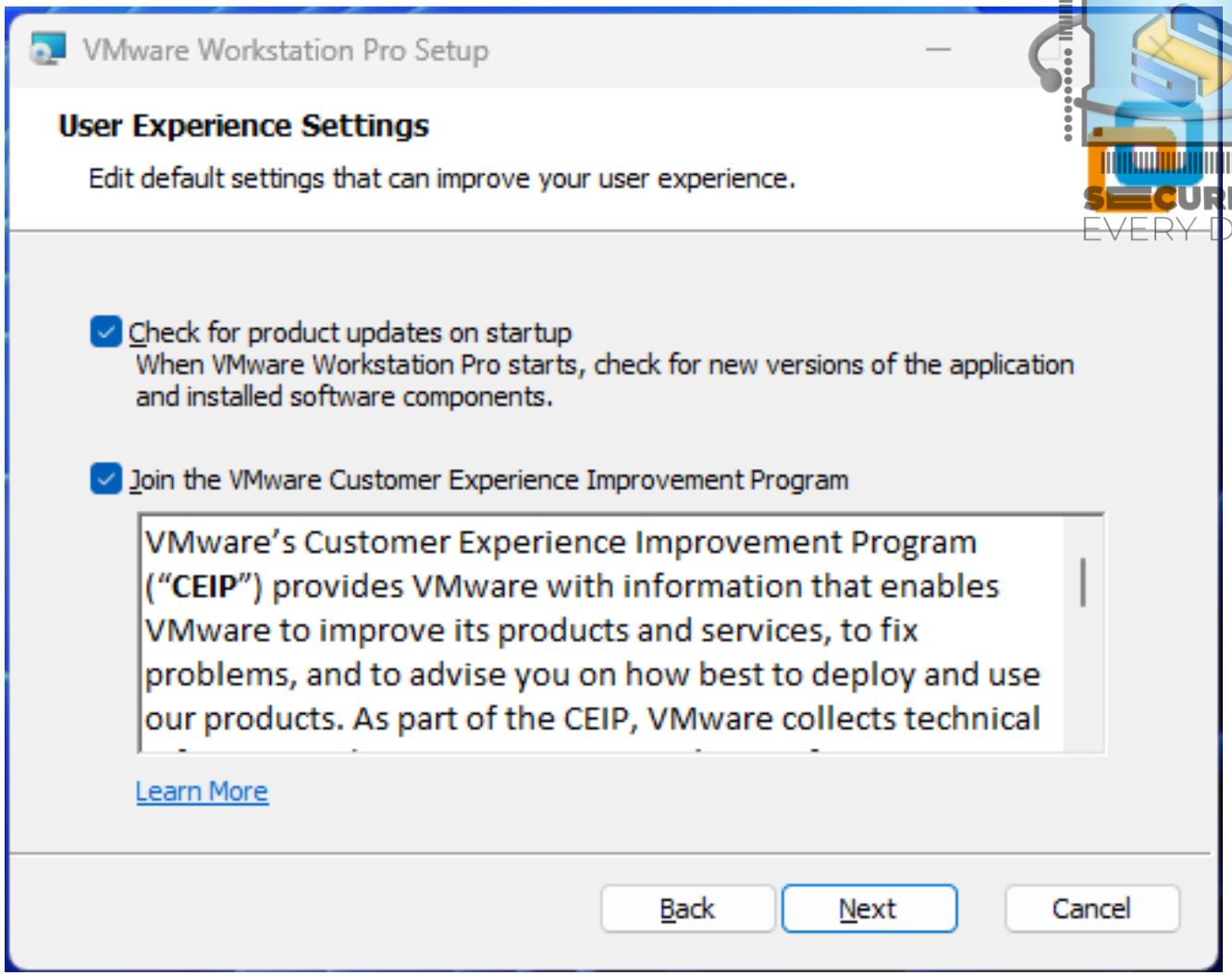
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



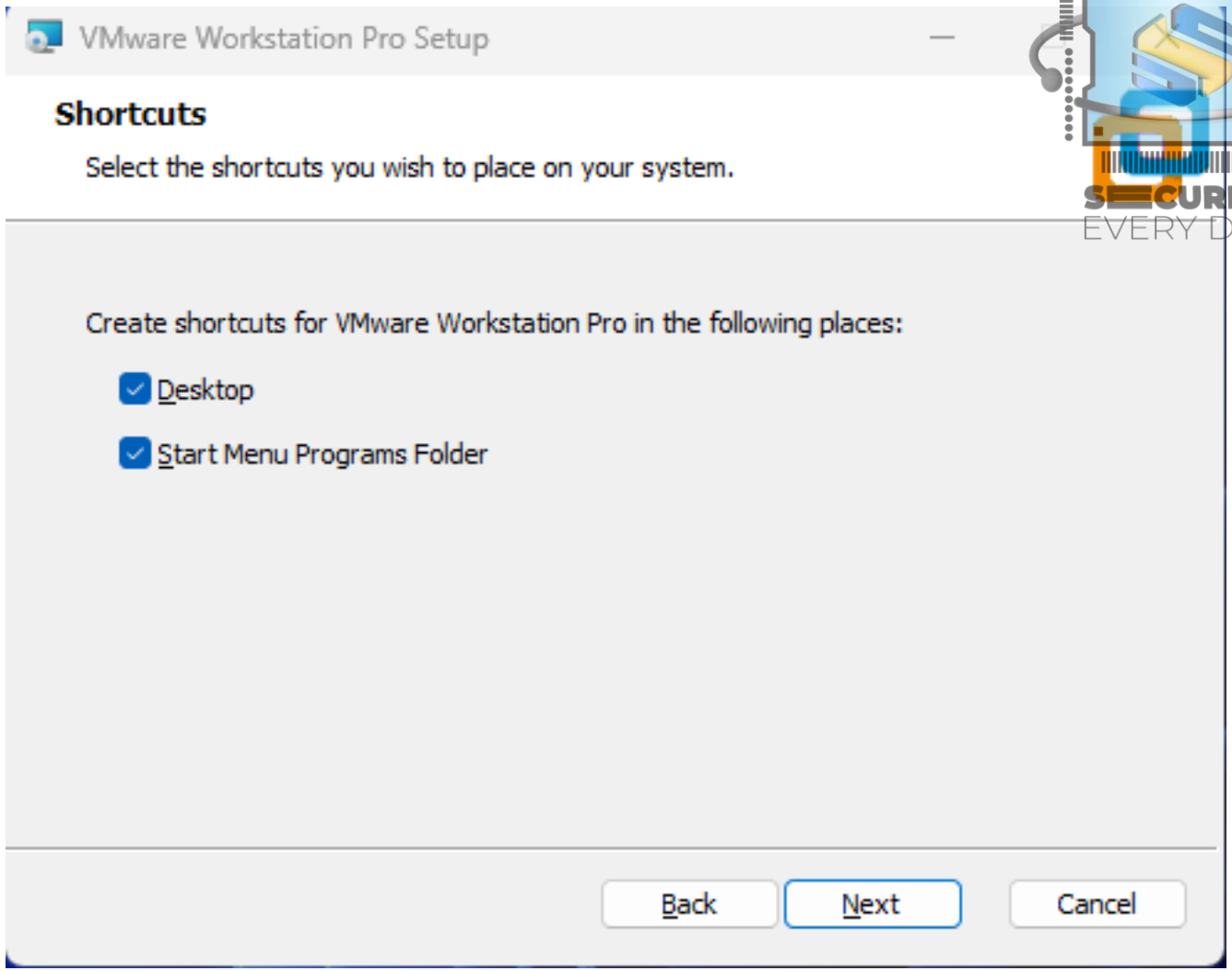
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



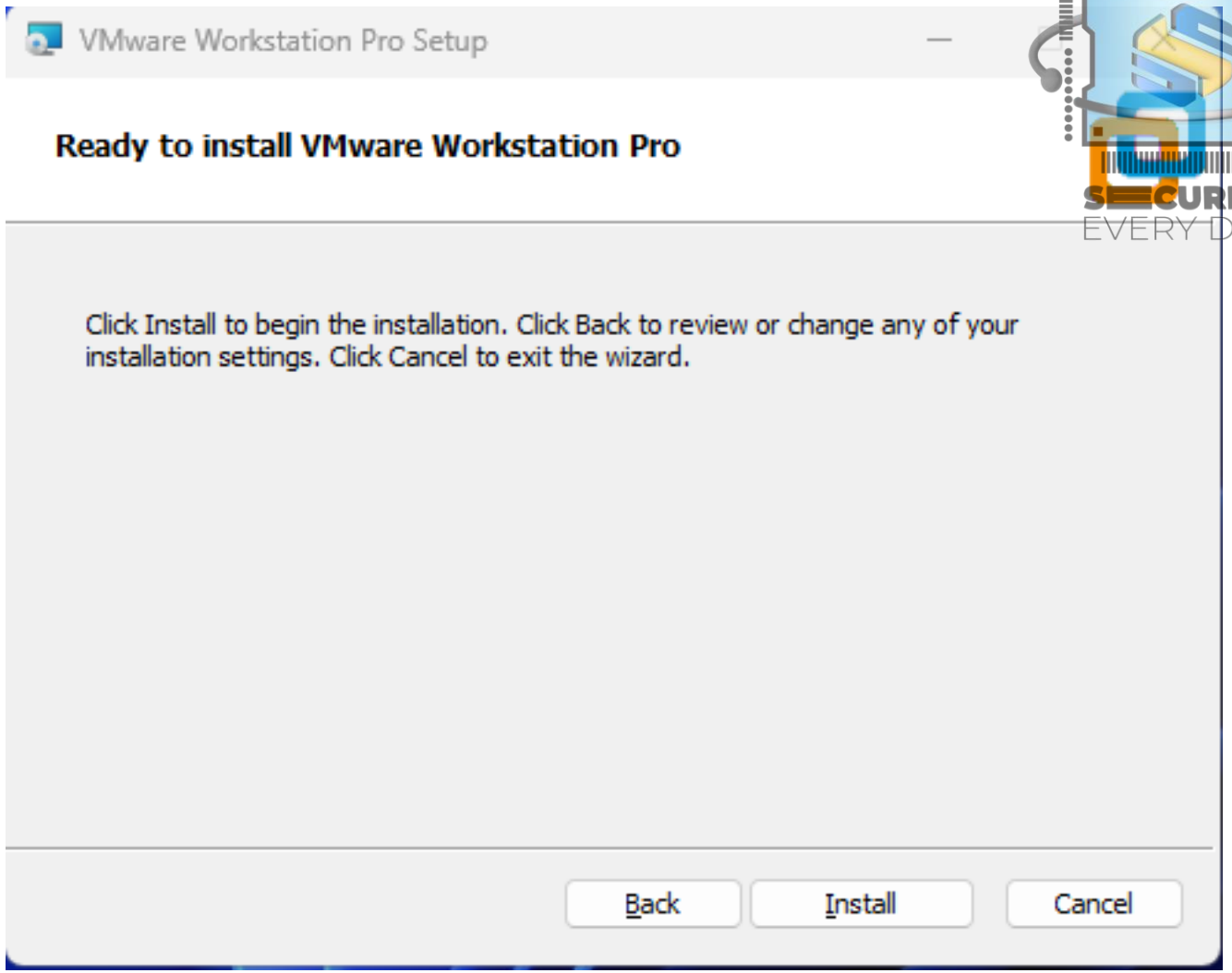
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



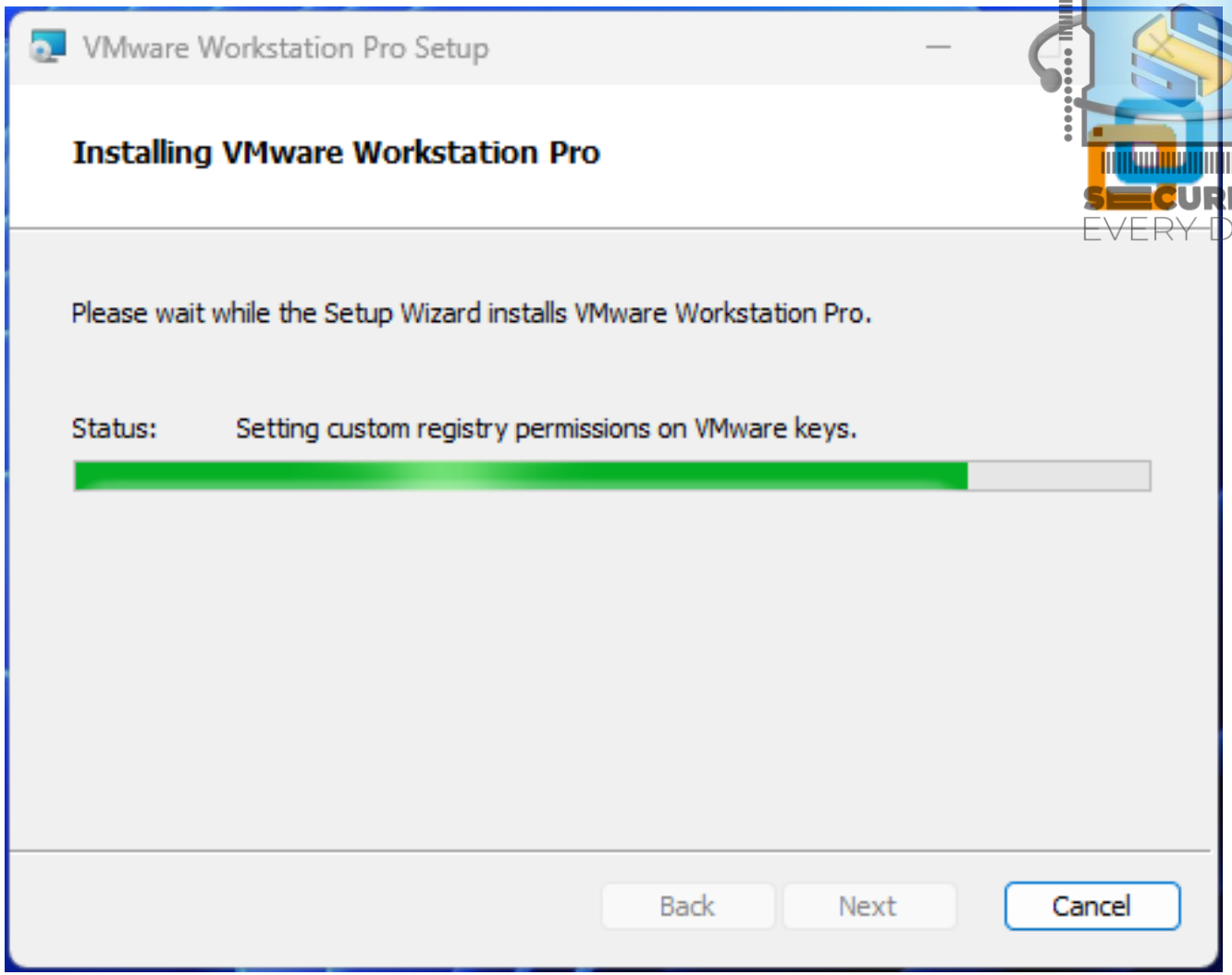
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Install"



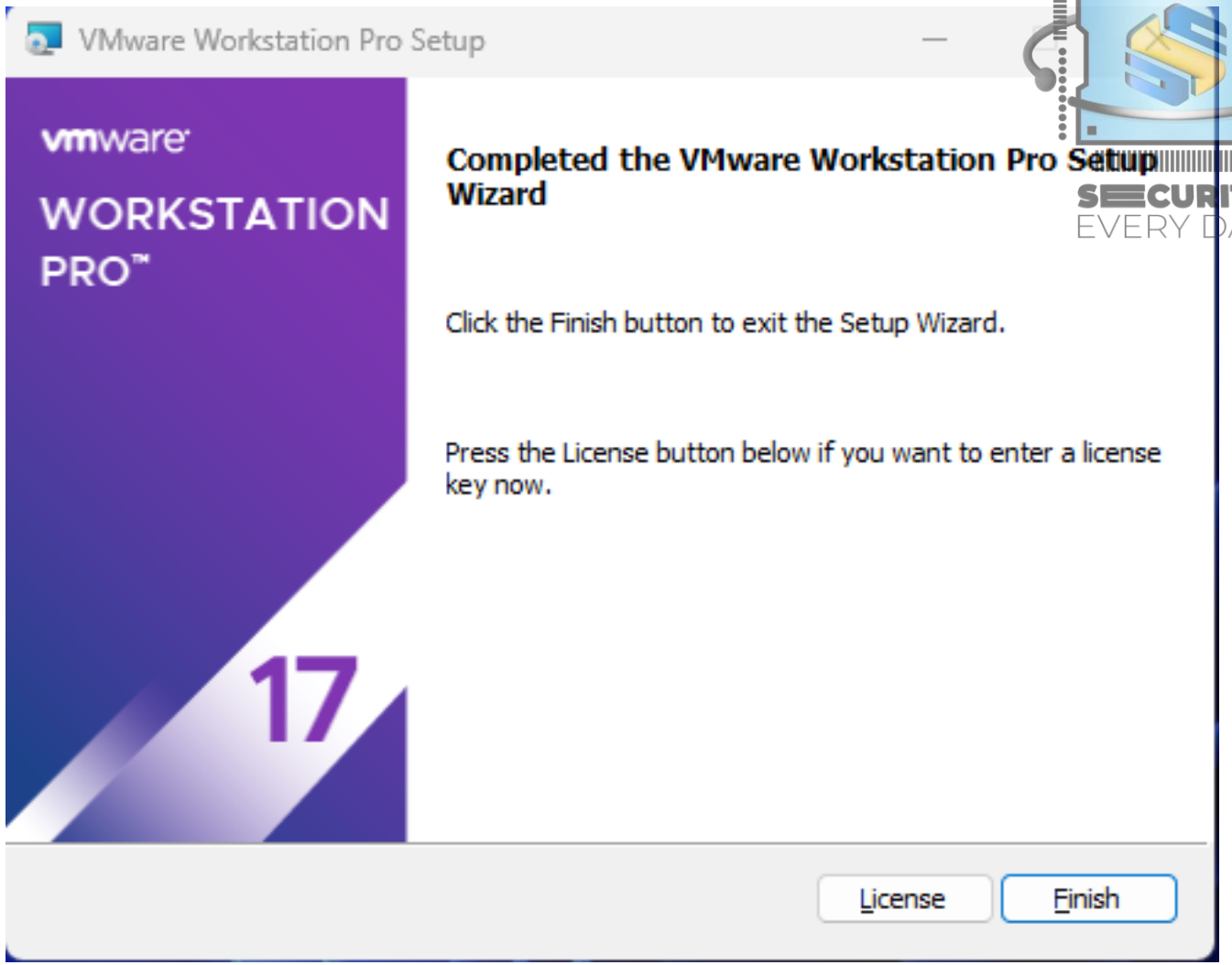
INSTALAÇÃO DO VMWARE WORKSTATION

- Aguarde a instalação ser finalizada



INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Finish"

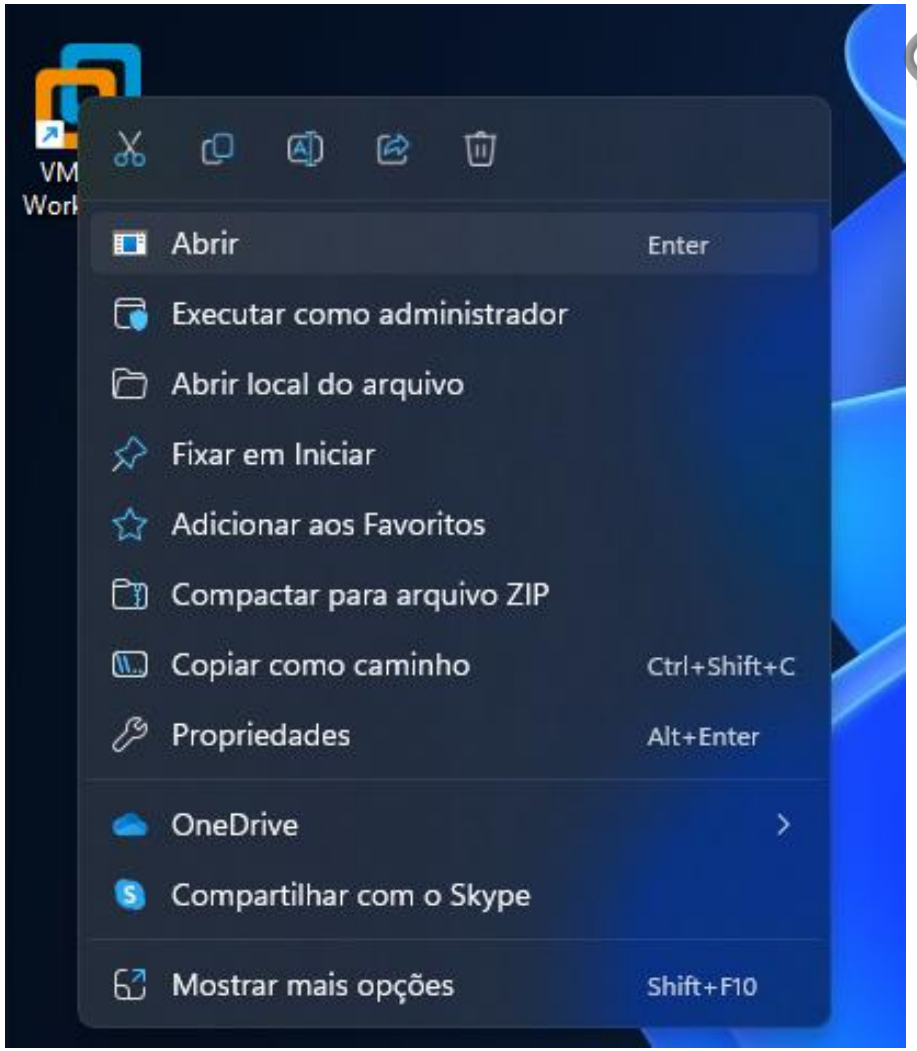


INSTALAÇÃO DO VMWARE WORKSTATION

AGORA, VOCÊ TEM 30 DIAS FREE PARA UTILIZAR O VMWARE WORKSTATION:)

CONFIGURAÇÃO DO VMWARE WORKSTATION

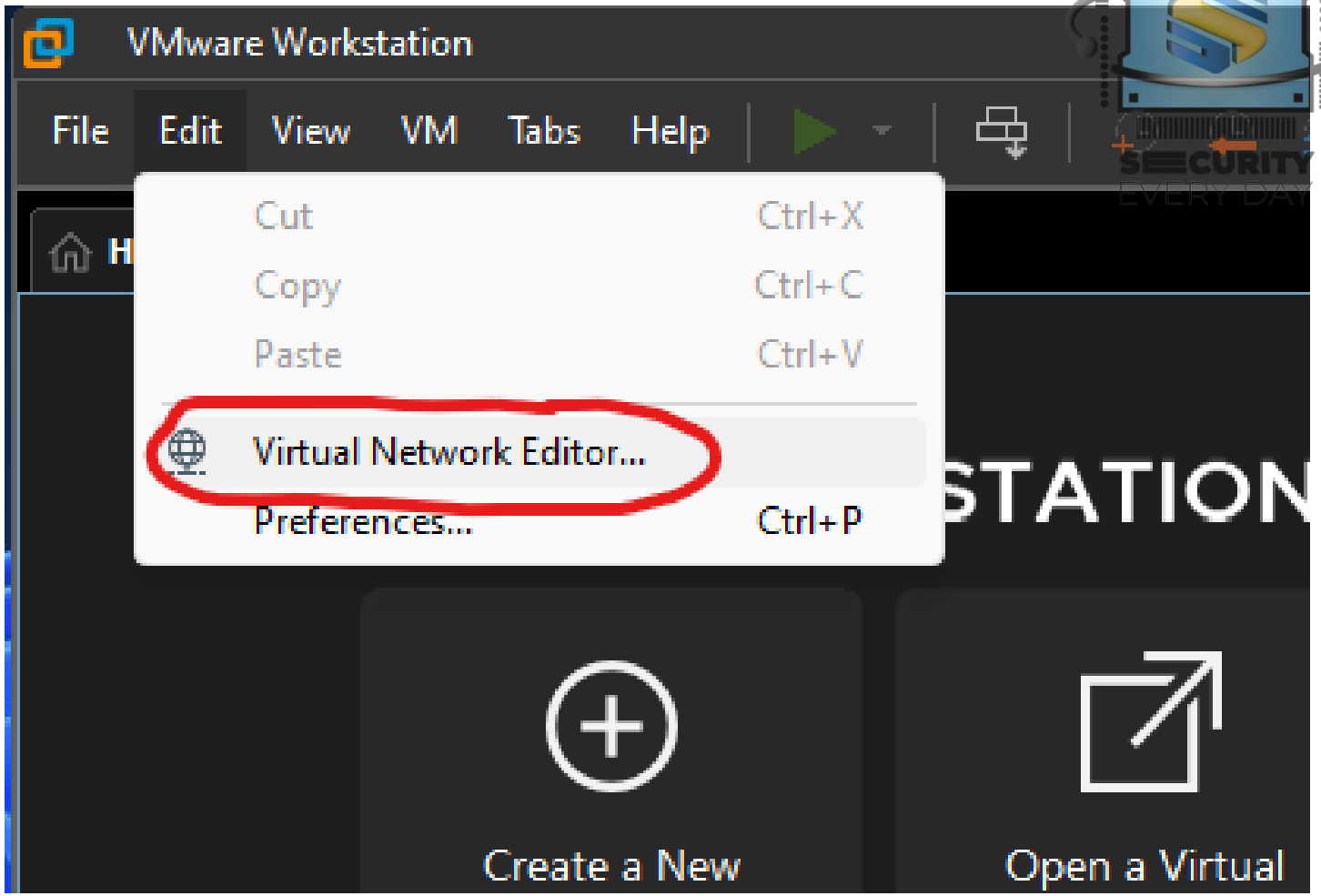
- Abra o VMware Workstation, clique com o botão direito e escolha a opção "Abrir"



SECURITY EVERY DAY

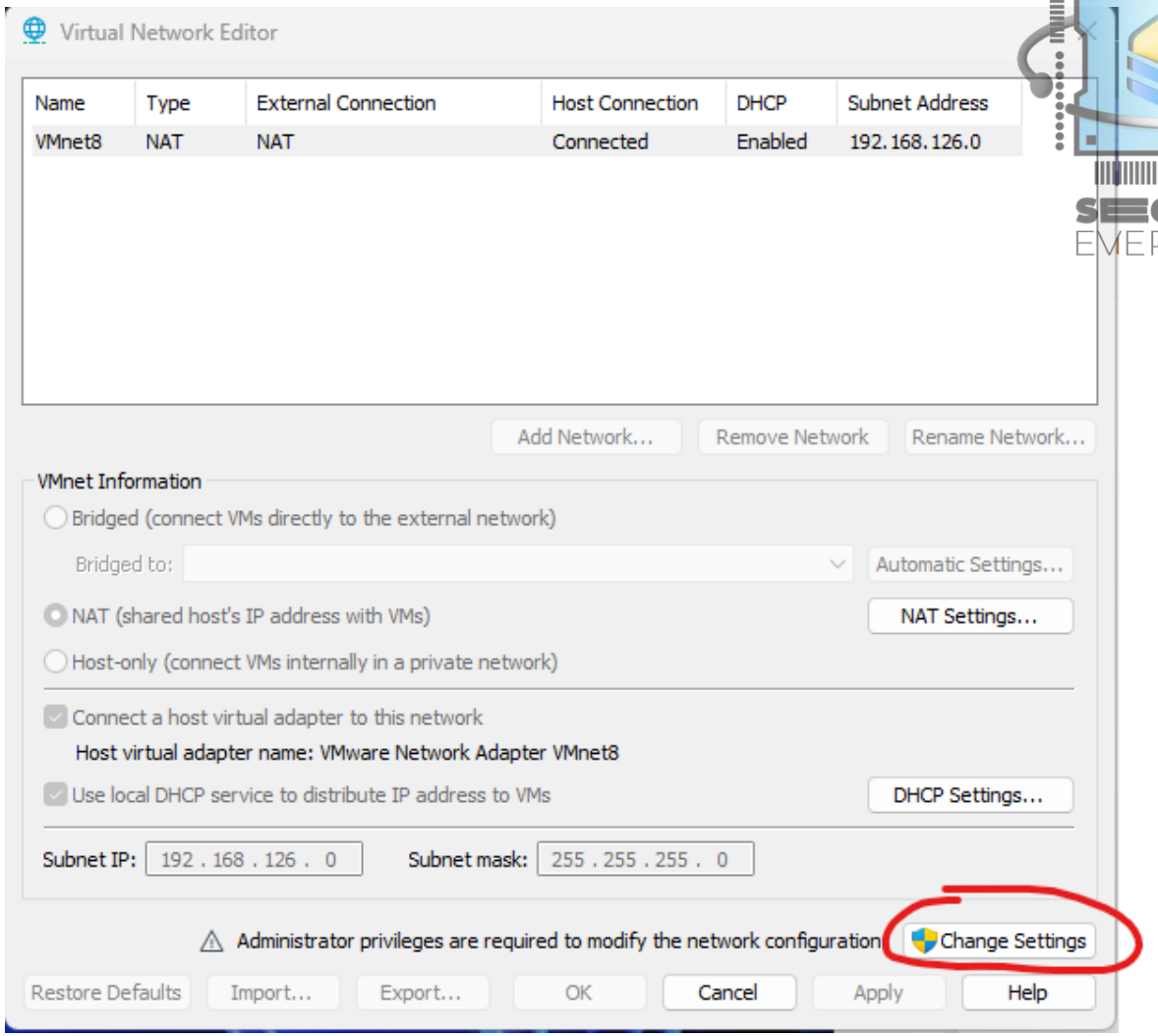
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Abra a opção "Edit" > "Virtual Network Editor..."



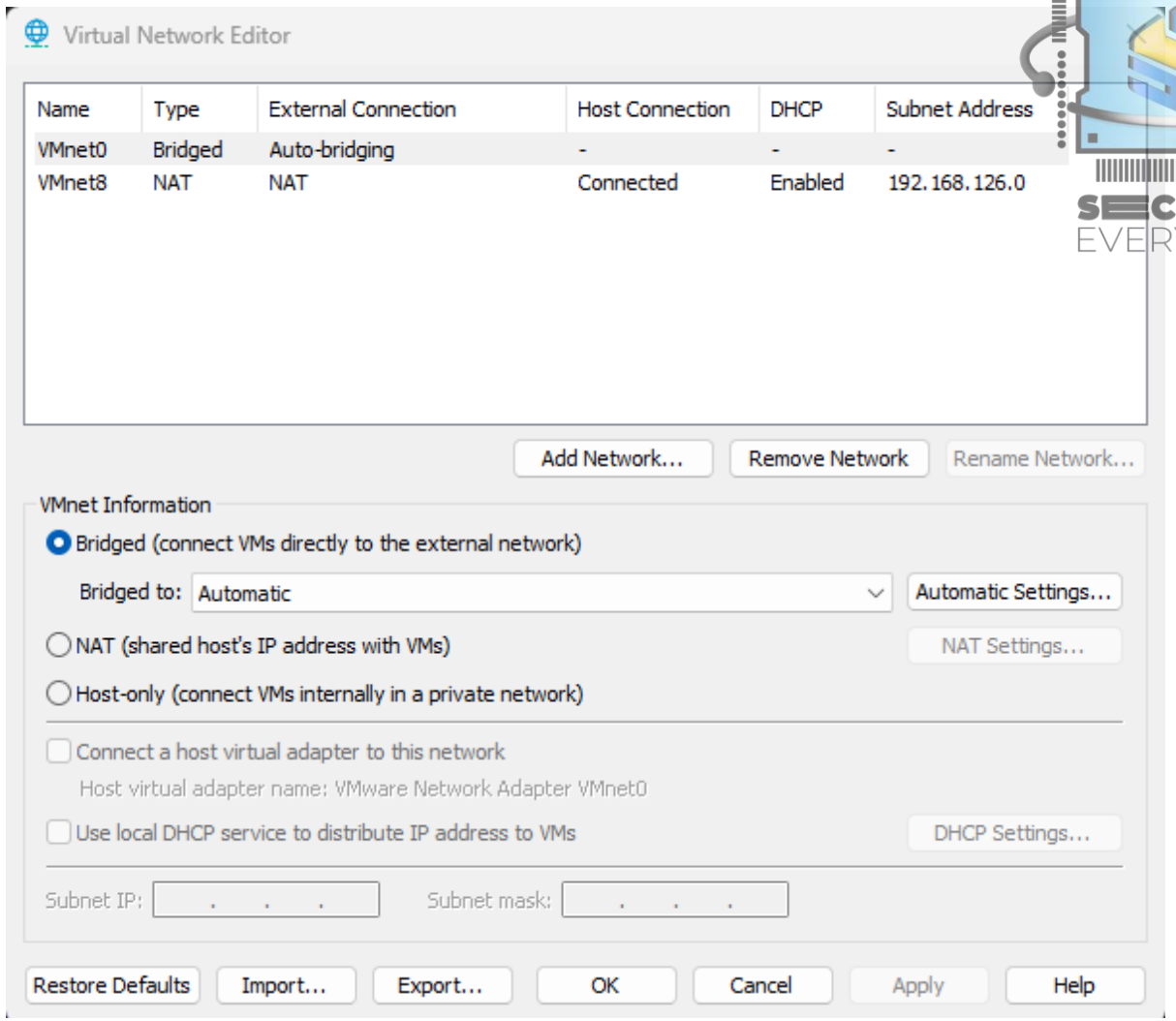
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Deve aparecer uma tela similar a está, clique em "Change Setings" para poder adicionar novas interfaces



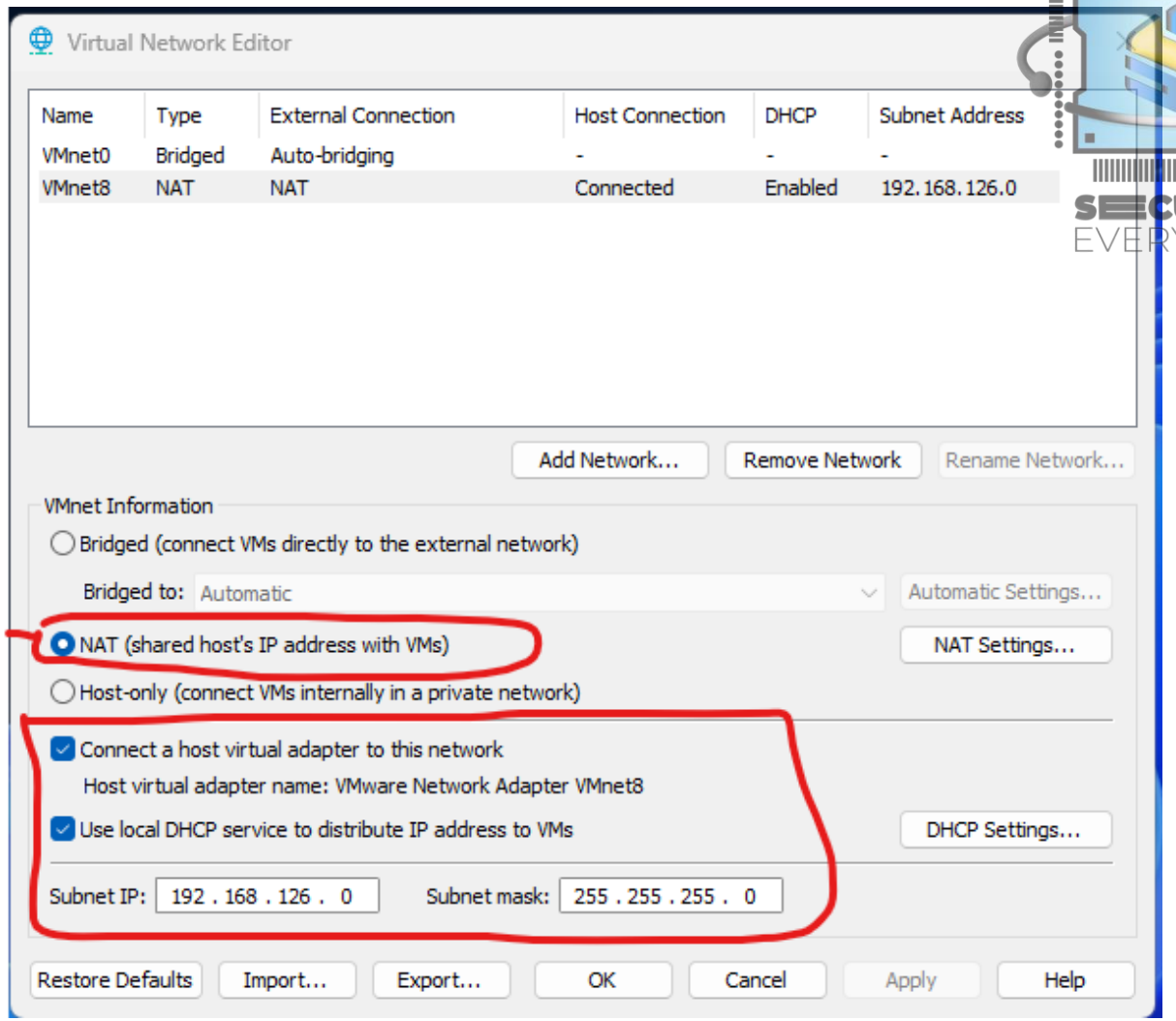
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, as opções de "Add Network.." E as outras opções devem aparecer desbloqueadas para edição, vamos editar a interface type "NAT", note que, o nome "VMnet8" pode ser diferente para você, não tem problemas.



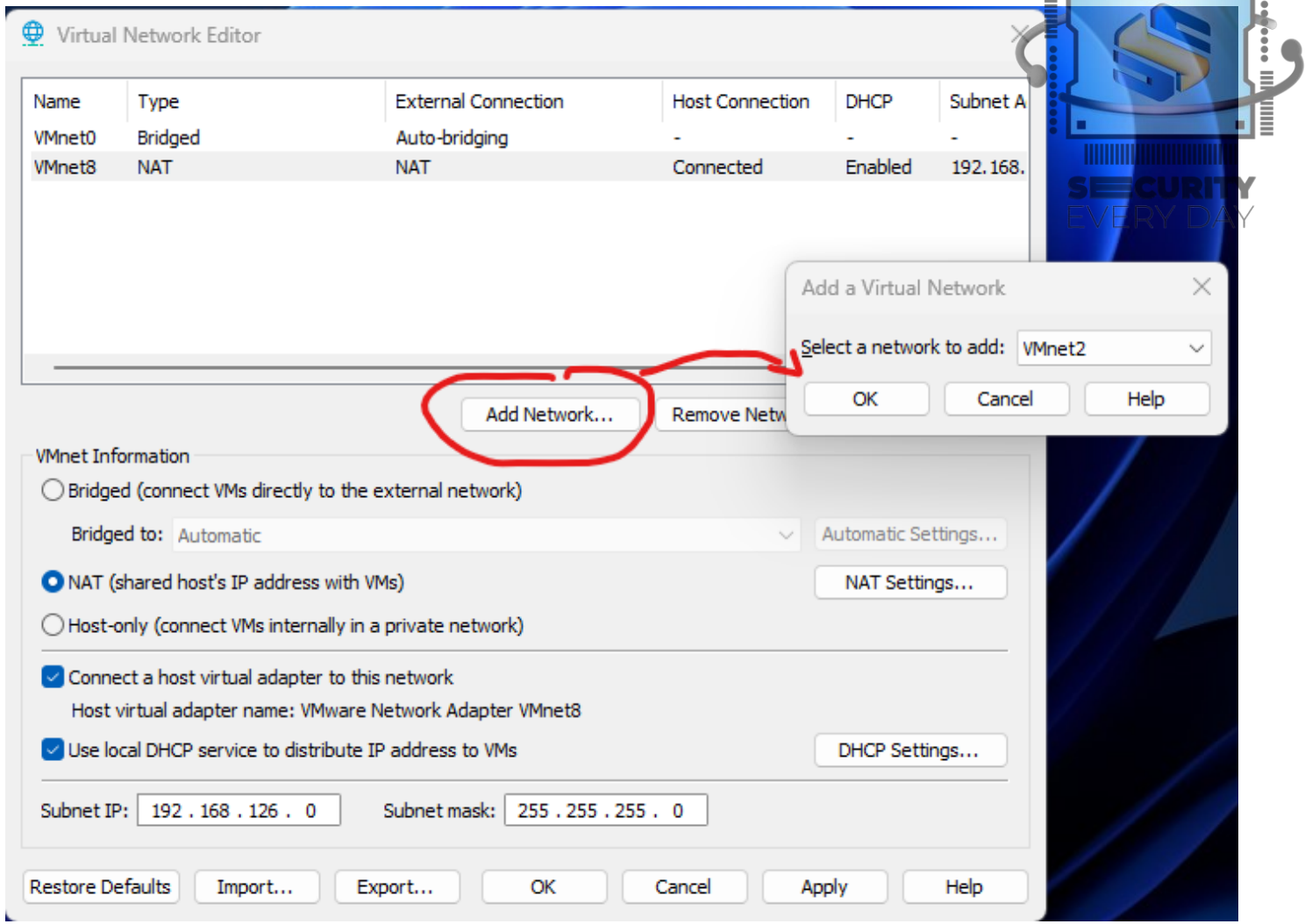
CONFIGURAÇÃO DO VMWARE WORKSTATION

- A sua configuração deve ficar exatamente igual as destacadas na imagem ao lado, feito isso, clique em aplicar e vamos para a próxima configuração



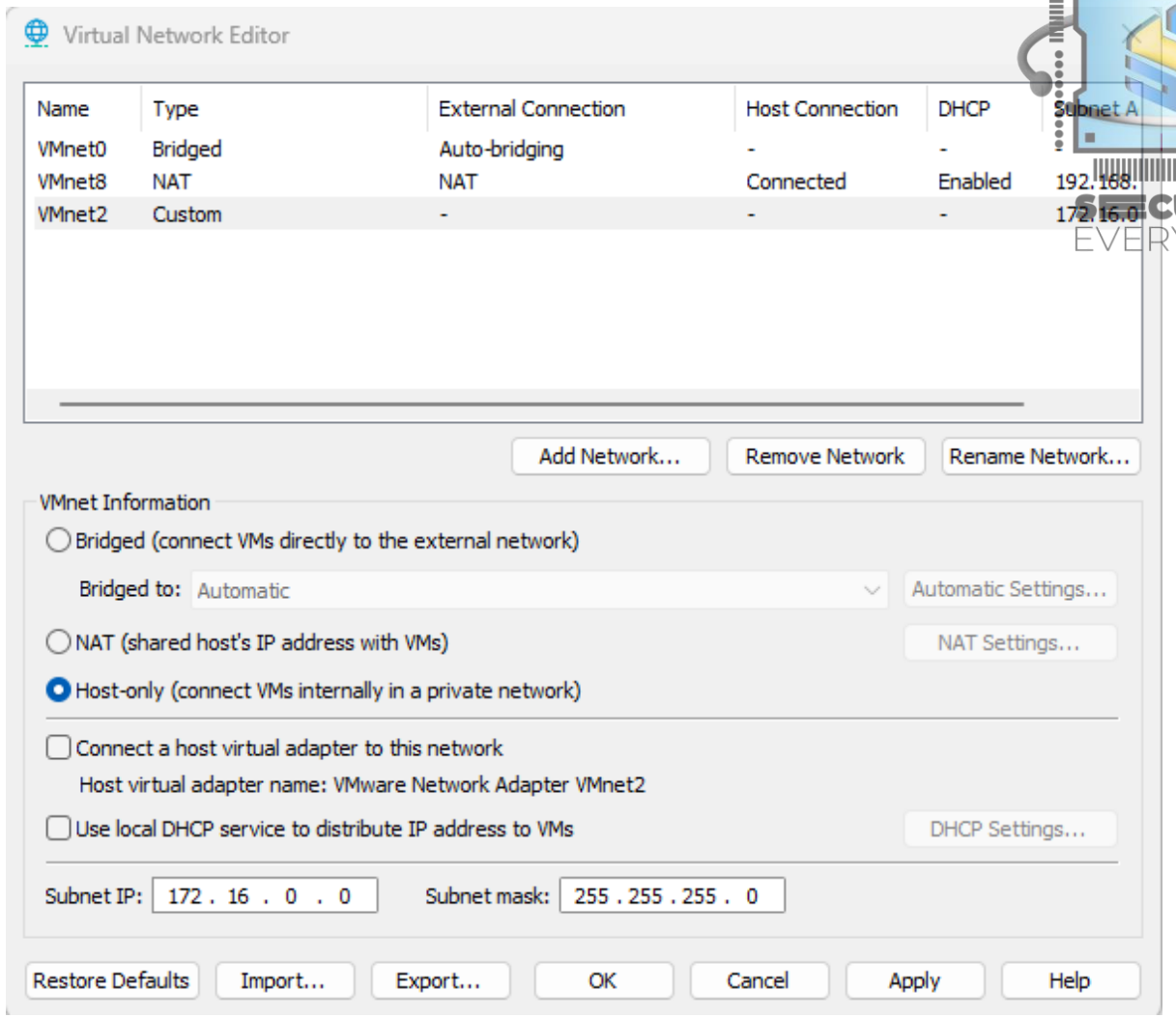
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, vamos adicionar uma nova interface, clique em "Add Network.." E em seguida, clique em "OK"
  - Obs: não escolha a VMnet1



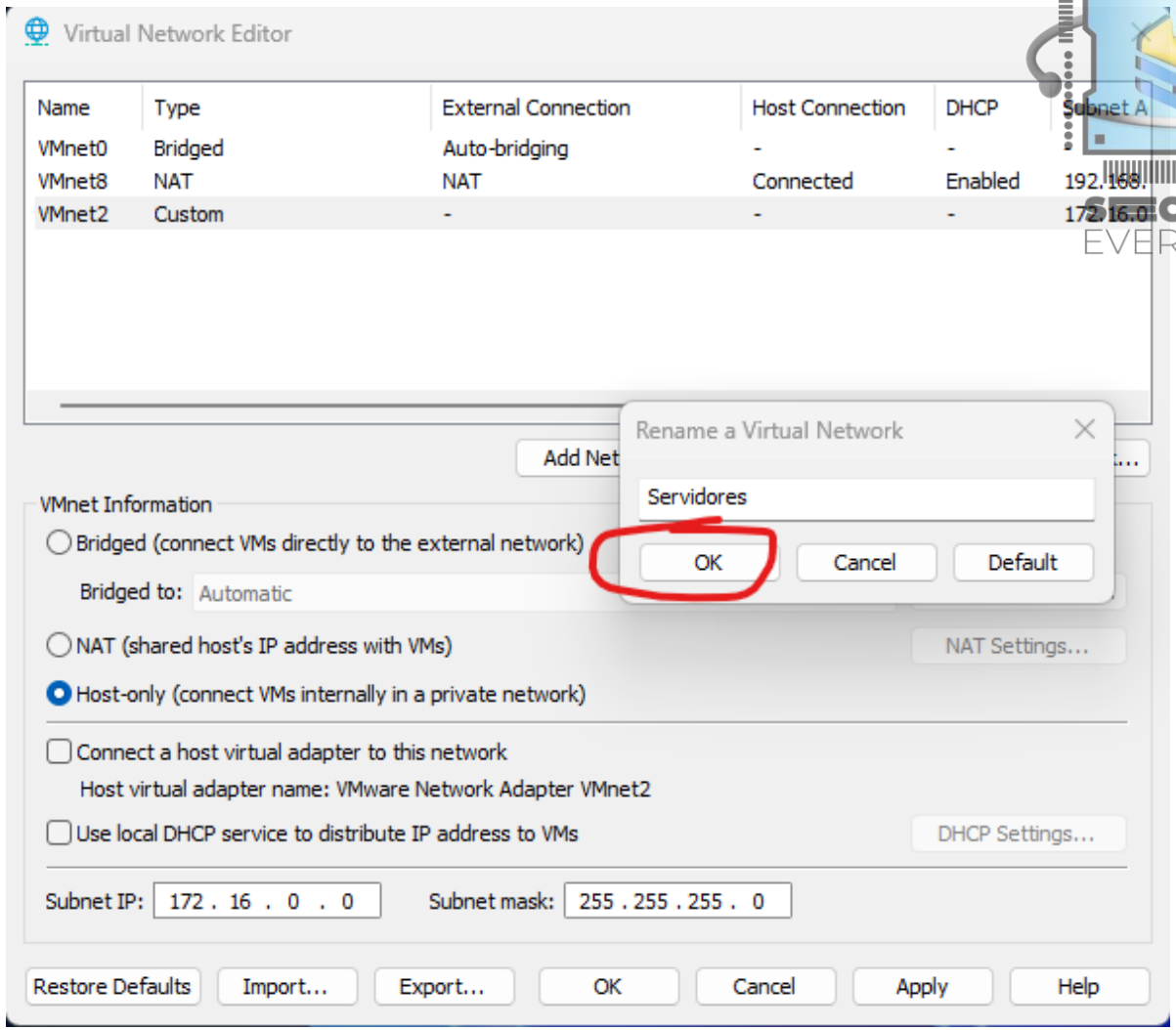
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Configure a nova interface para ficar exatamente igual a imagem ao lado, feito isso, clique em "Rename Network..." e vamos renomear essa interface para "Servidores"



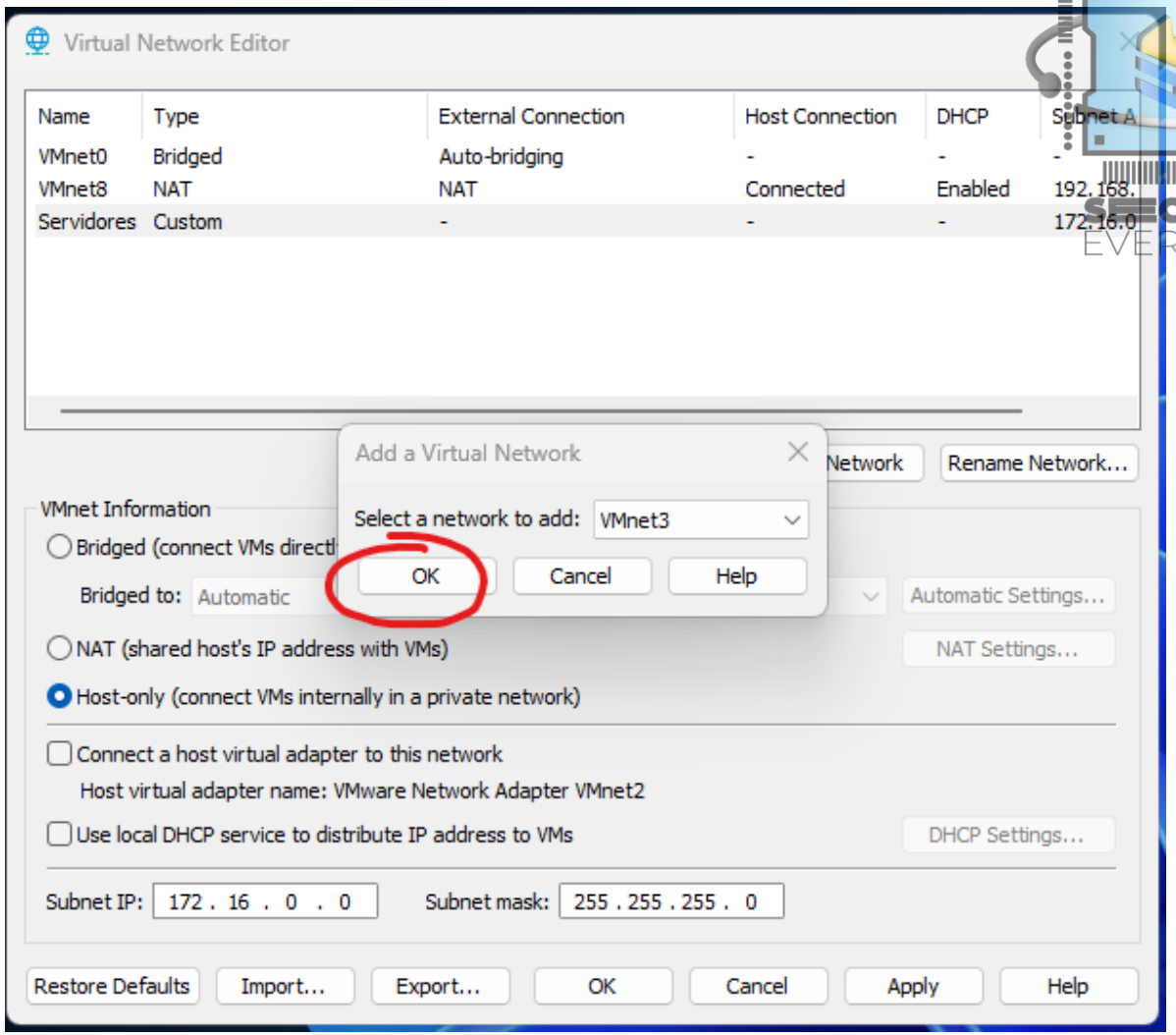
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Configure a nova interface para ficar exatamente igual a imagem ao lado, feito isso, clique em "Rename Network..." e vamos renomear essa interface para "Servidores"



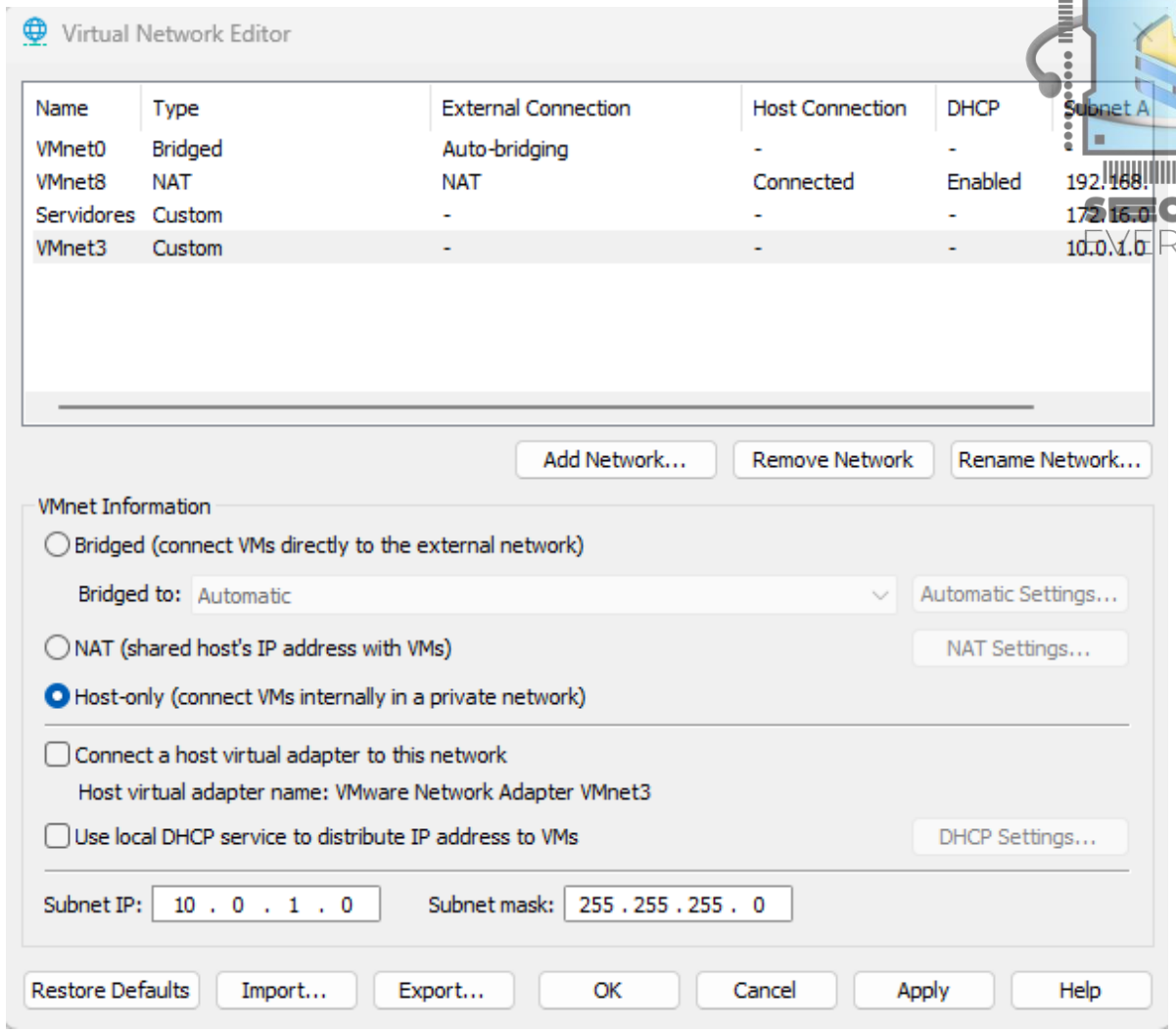
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, vamos seguir os mesmos passos para criar a interface "DMZ" e "Colaboradores"



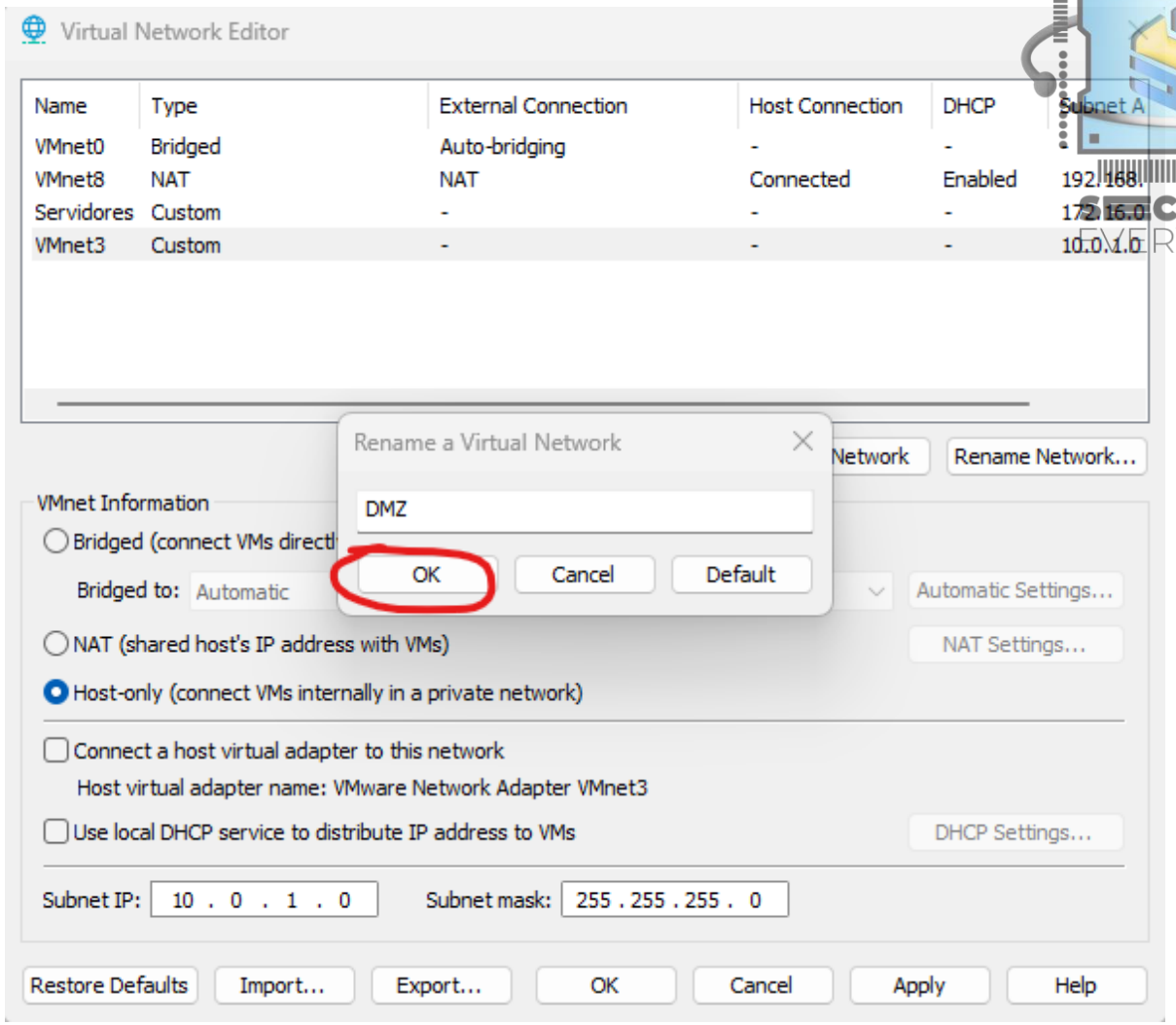
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, vamos seguir os mesmos passos para criar a interface "DMZ" e "Colaboradores"



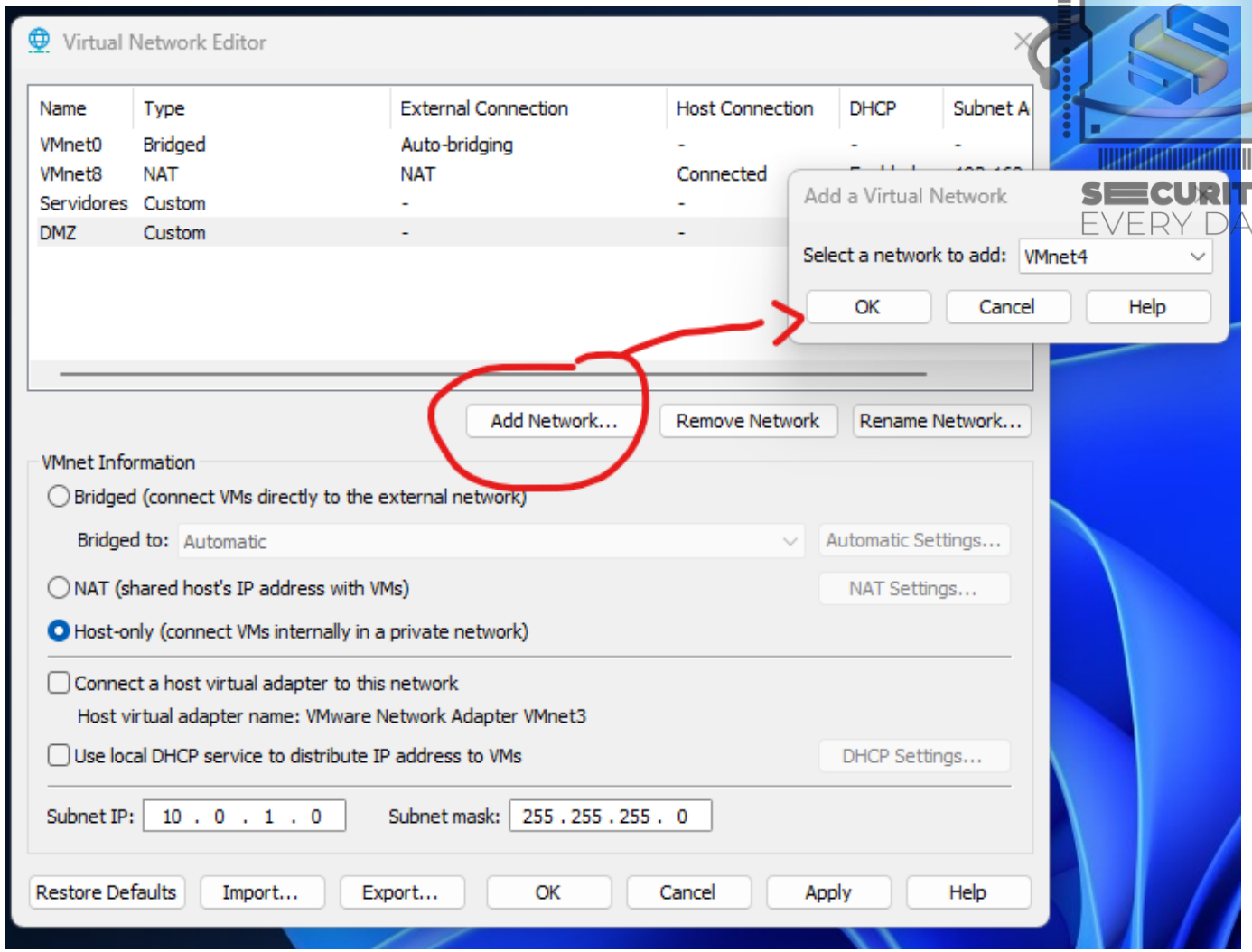
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, vamos seguir os mesmos passos para criar a interface "DMZ" e "Colaboradores"



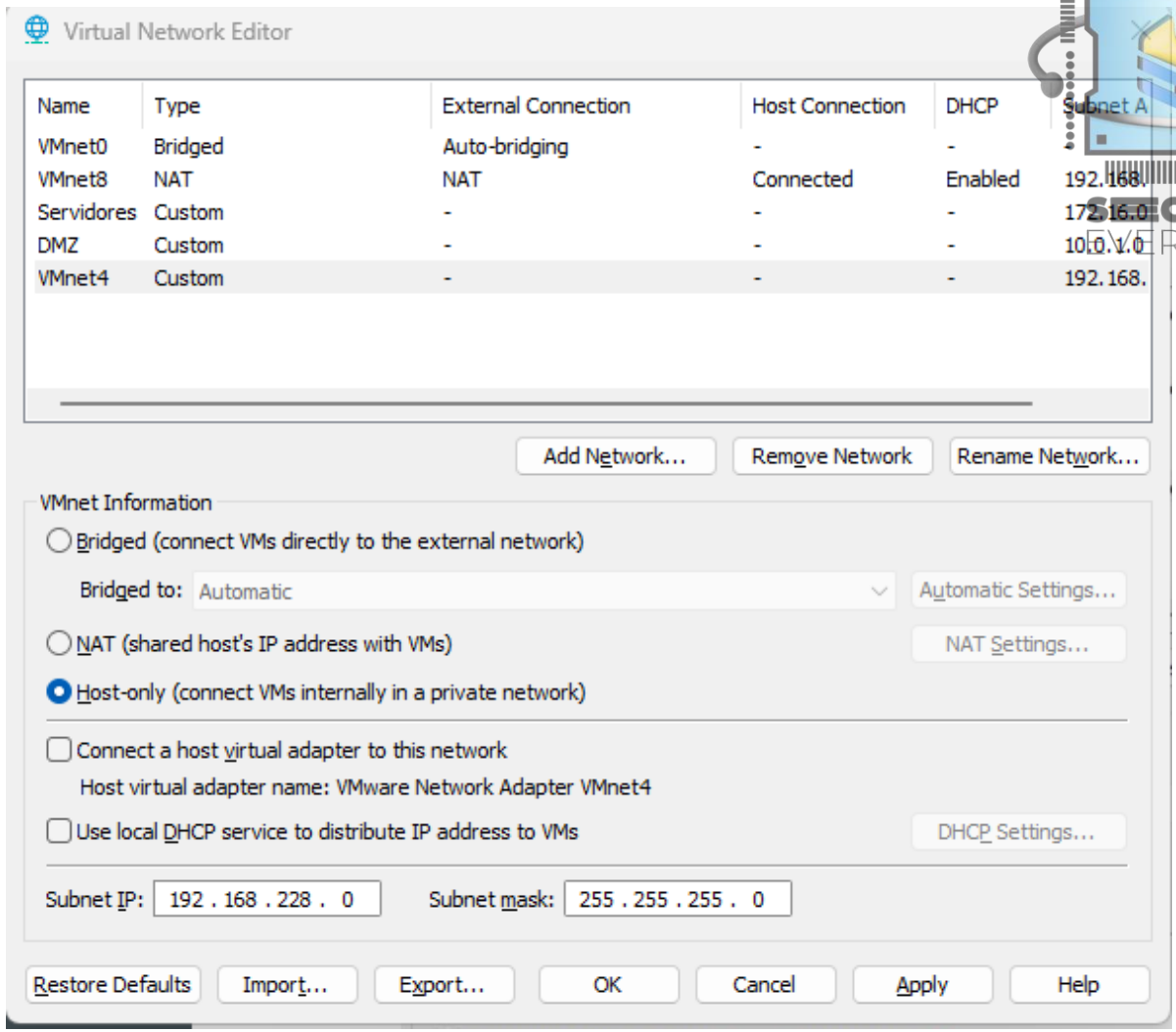
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, vamos seguir os mesmos passos para criar a interface "DMZ" e "Colaboradores"



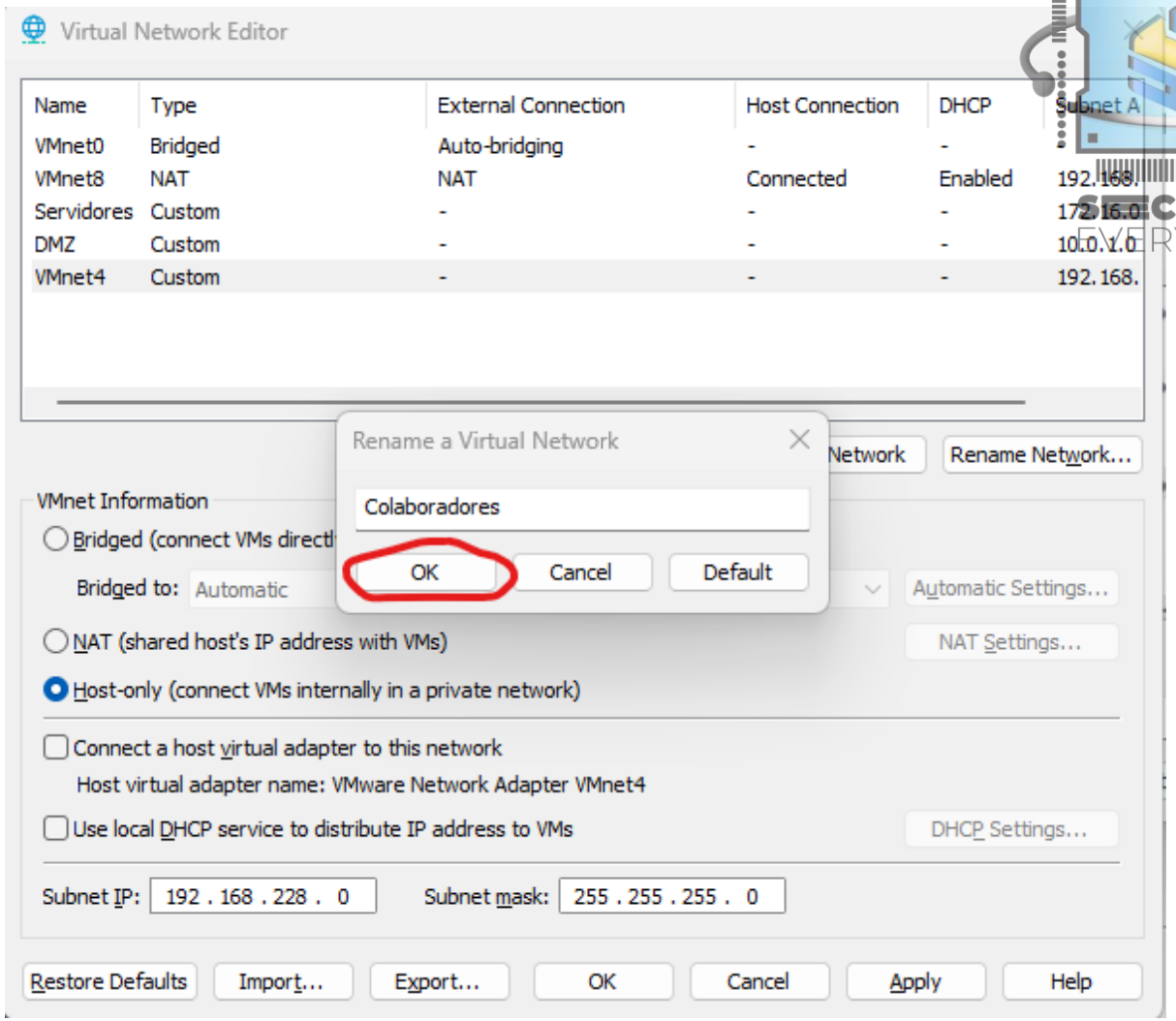
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, vamos seguir os mesmos passos para criar a interface "DMZ" e "Colaboradores"



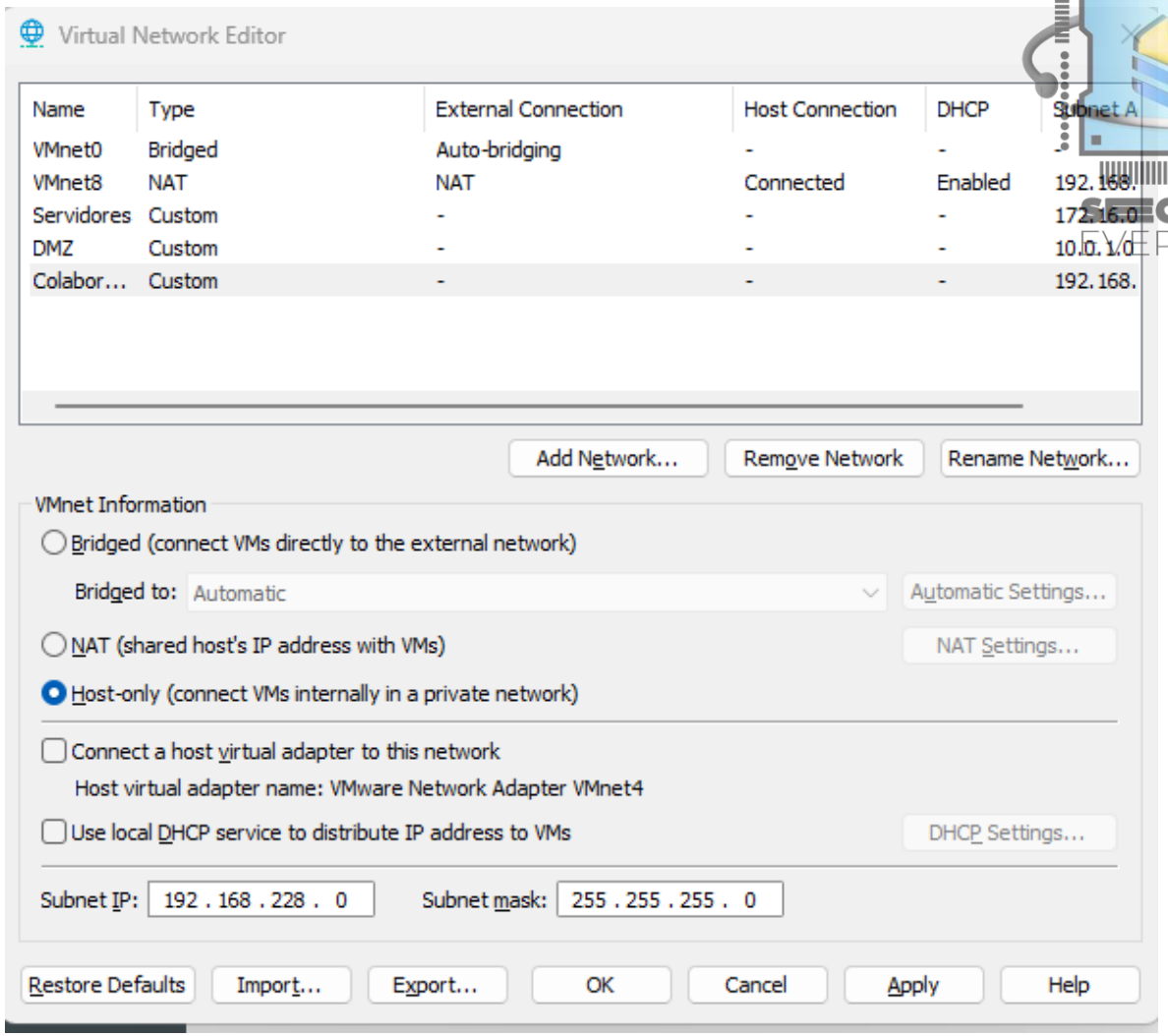
CONFIGURAÇÃO DO VMWARE WORKSTATION

- Agora, vamos seguir os mesmos passos para criar a interface "DMZ" e "Colaboradores"



CONFIGURAÇÃO DO VMWARE WORKSTATION

- Pronto!! Feito isso, suas interfaces devem estar assim:
- Clique em "Apply" e depois em "OK"

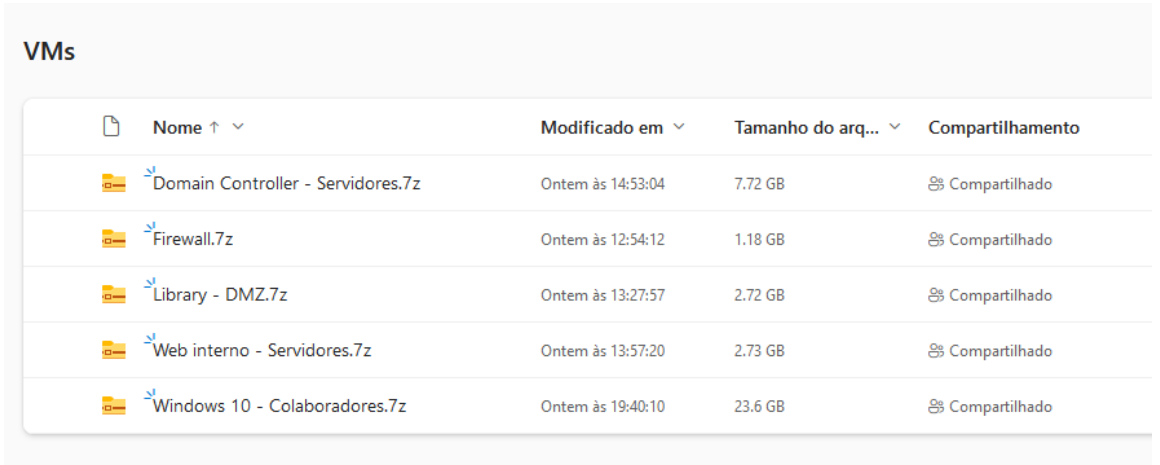


CONFIGURAÇÃO DO VMWAR E WORKSTATION

AGORA ESTAMOS PRONTOS PARA SUBIR AS MAQUINAS VIRTUAIS

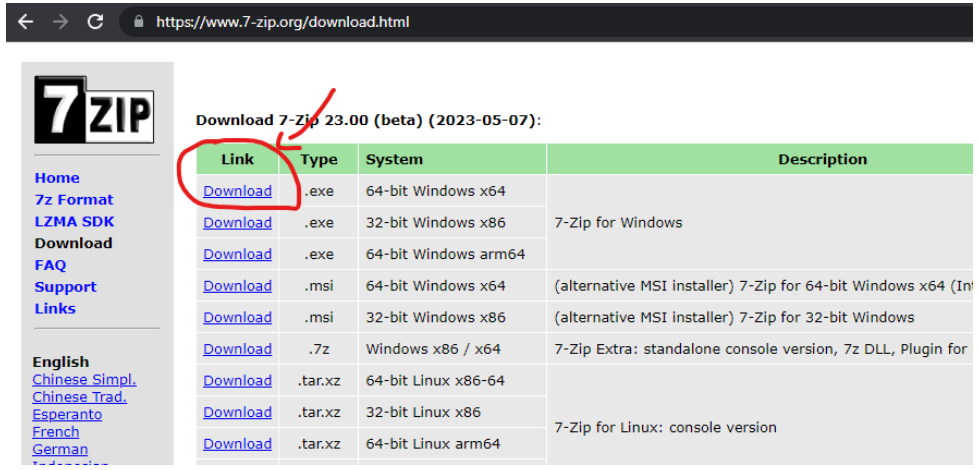
CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

- Realize o download das maquinas no link
  - https://1drv.ms/f/s!Asw32WKX_XOWiPFuTs1_XoEsiC2bKw



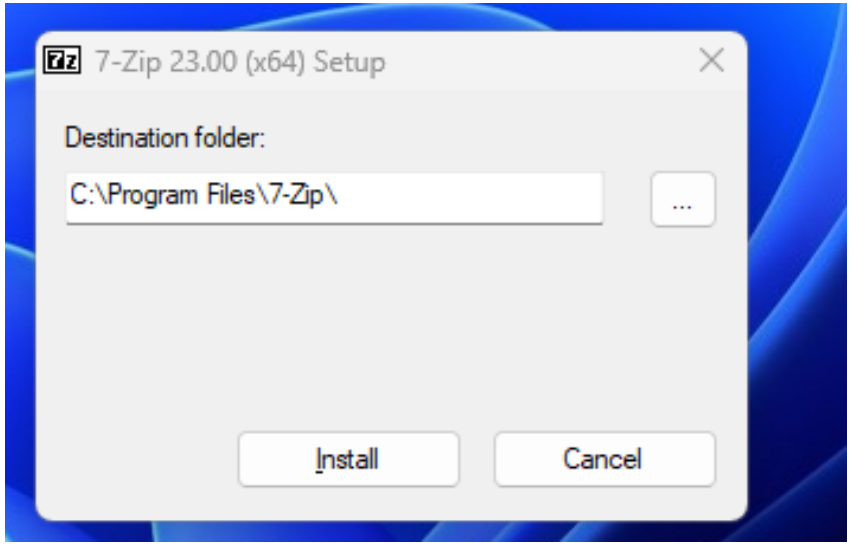
INSTALAÇÃO DO 7-ZIP

- Enquanto as VMs são baixadas, vamos instalar o 7-zip :)
  - Link https://www.7-zip.org/download.html



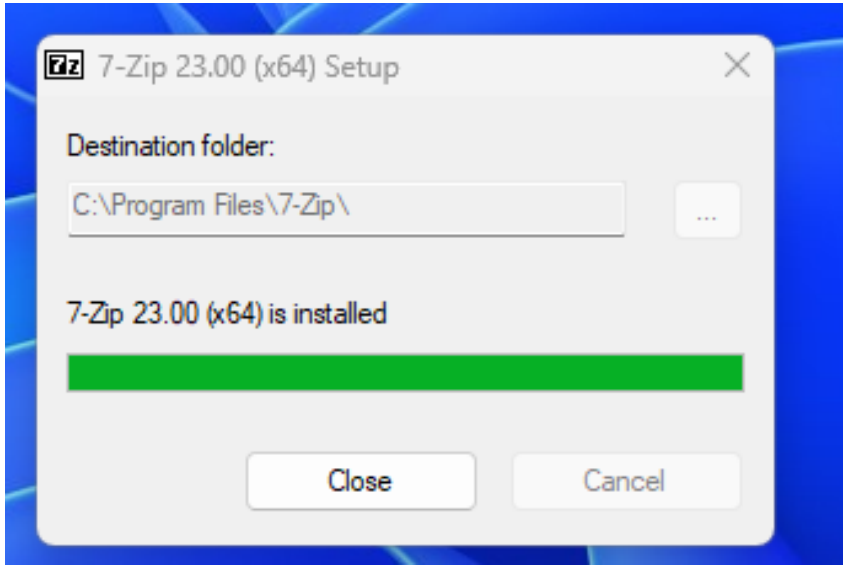
INSTALAÇÃO DO 7-ZIP

- Basta clicar 2x no executável e escolher a opção "Install"



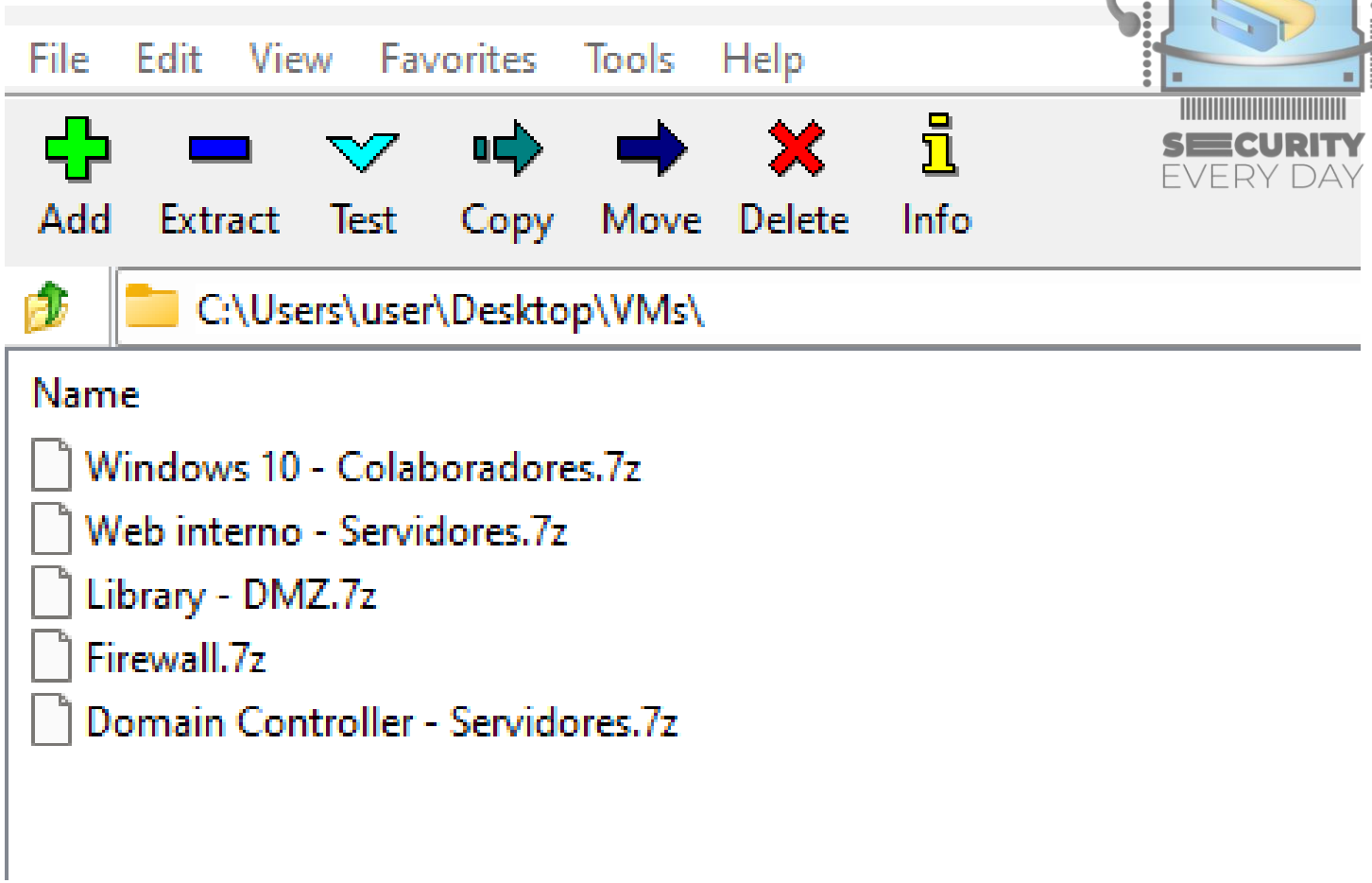
INSTALAÇÃO DO 7-ZIP

- Clique em "Close", pronto, 7-zip instalado, vamos utiliza-lo para extrair as maquinas virtuais



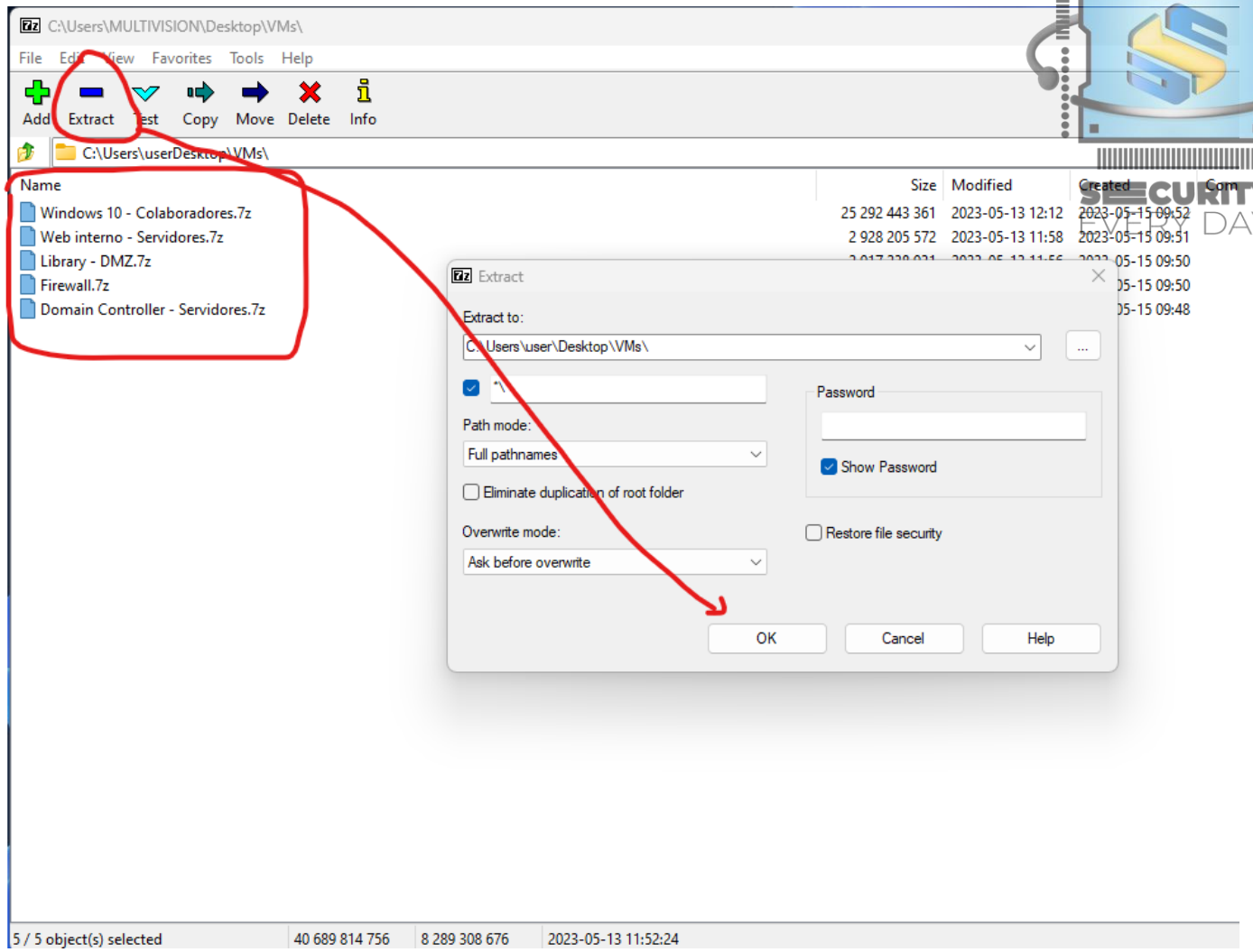
CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

- Abra o 7-zip e navegue na ferramenta até a pasta onde você salvou as maquinas virtuais



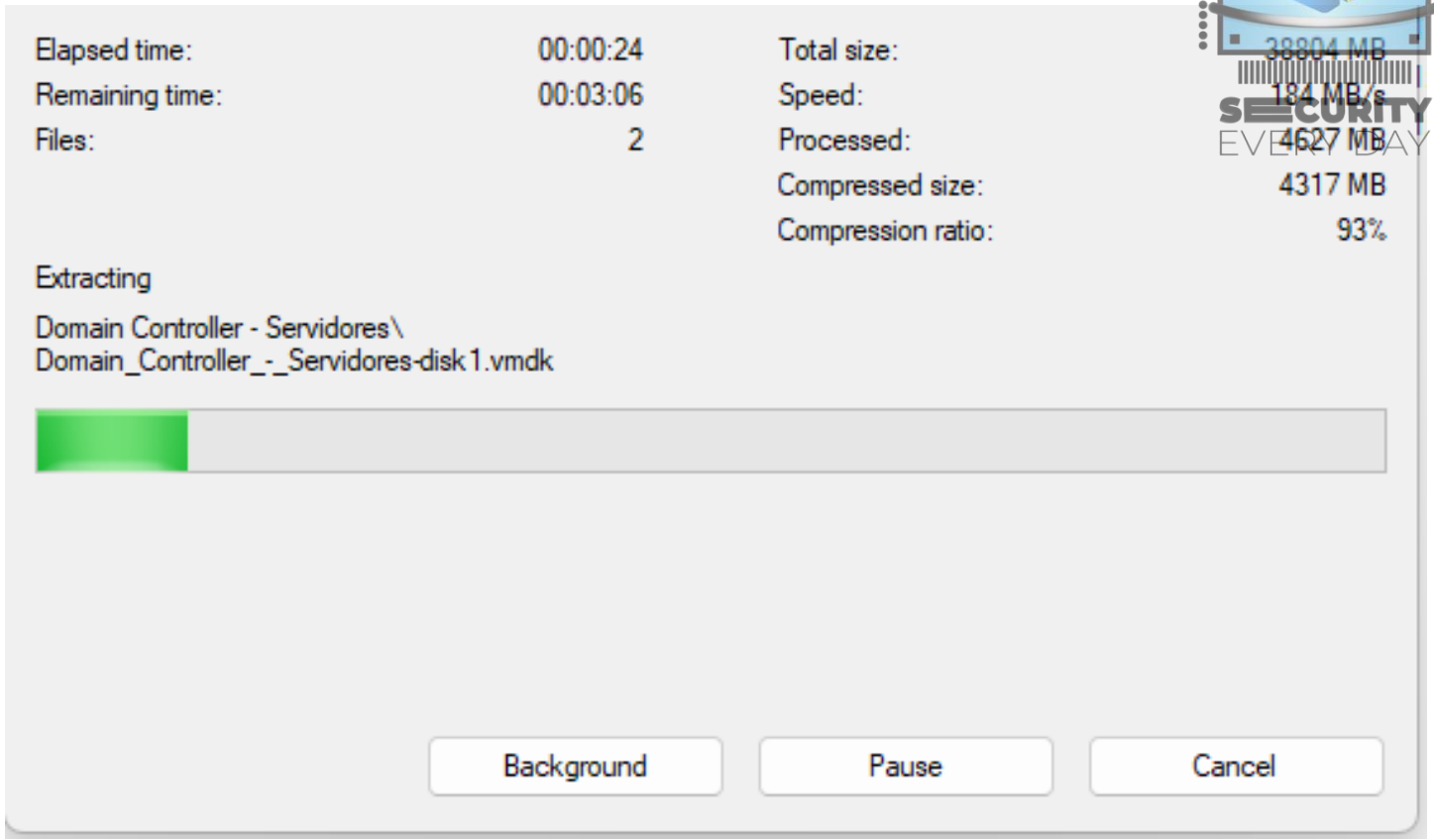
CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

- Precione a tecla shift e selecione todas as vms, após isso, clique em "Extract" e depois em "OK"



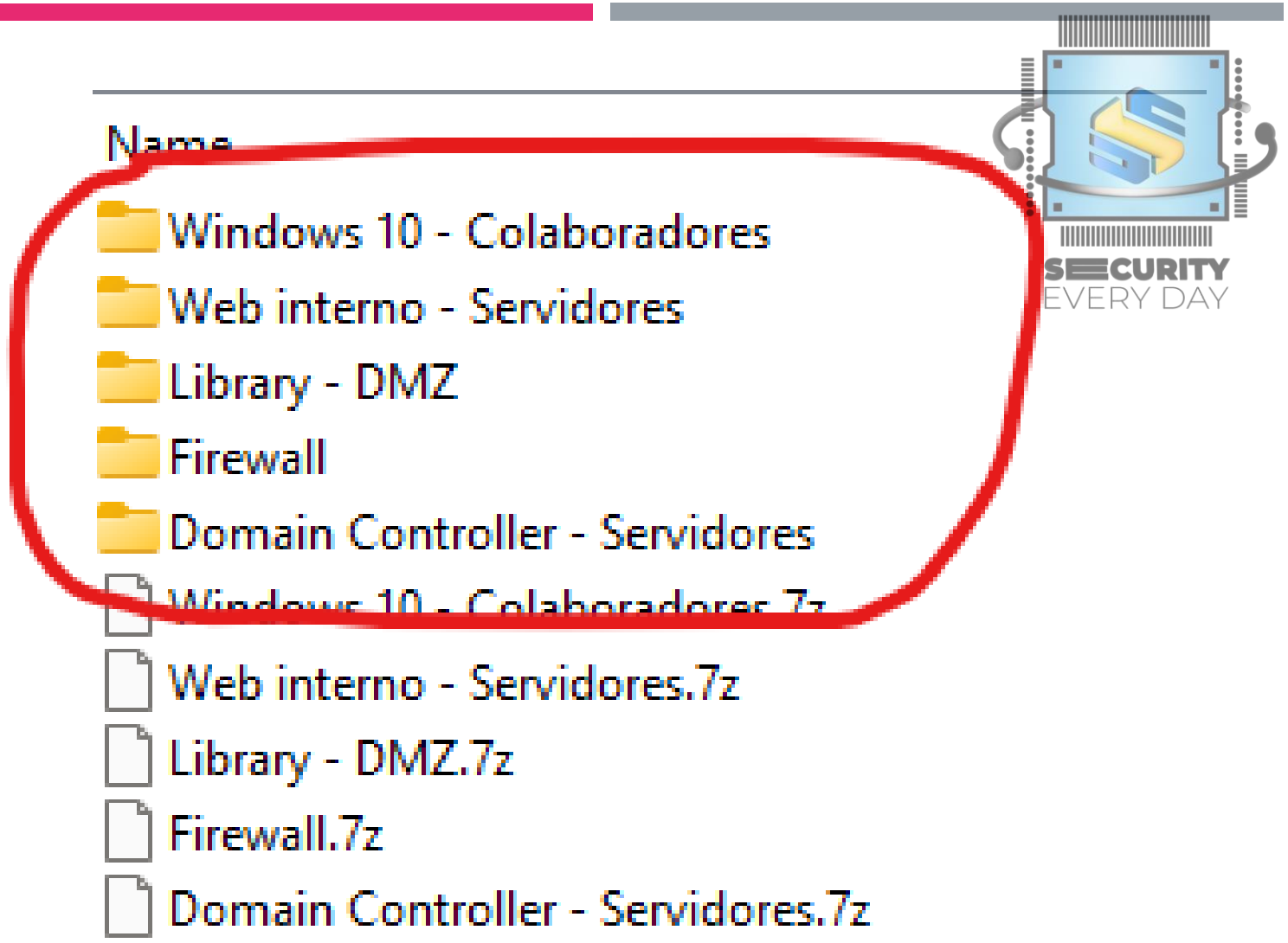
CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

- Aguarde até que todas as vms sejam extraidas



CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

- Após finalizar, as pastas das VMs devem aparecer, pode fechar o 7-zip
  - Obs: você pode deletar os arquivos .7z para economizar espaço na sua maquina.

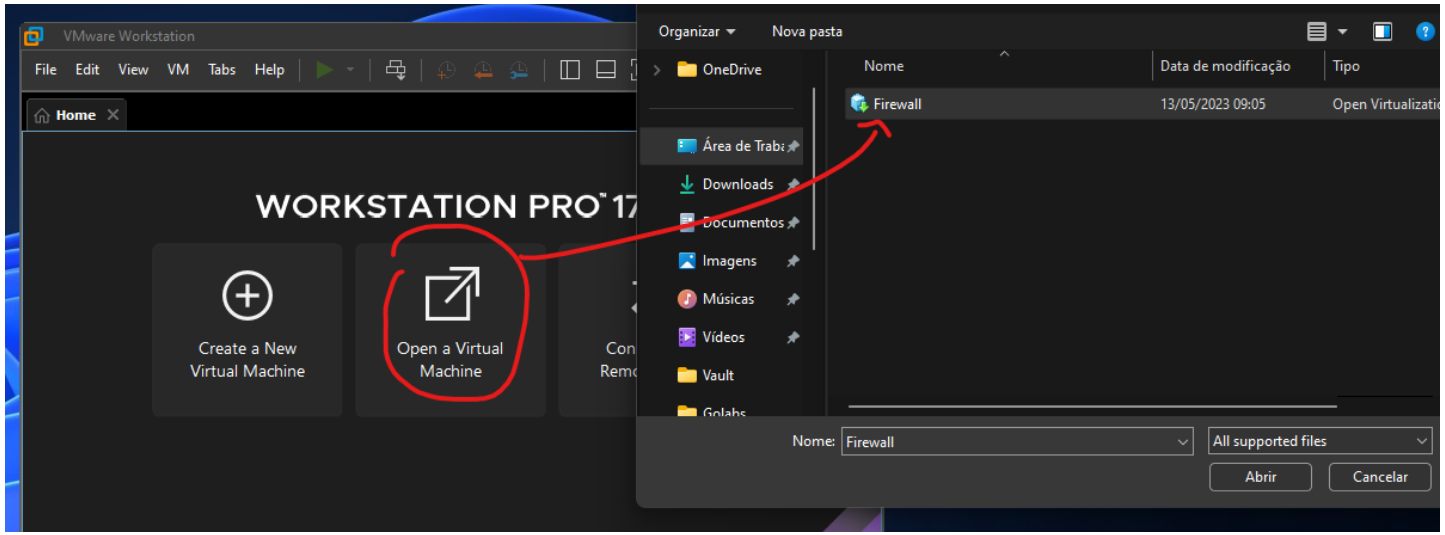


CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

TEMOS NOSSAS MAQUINAS AGORA, SÓ FALTA SUBIR :)

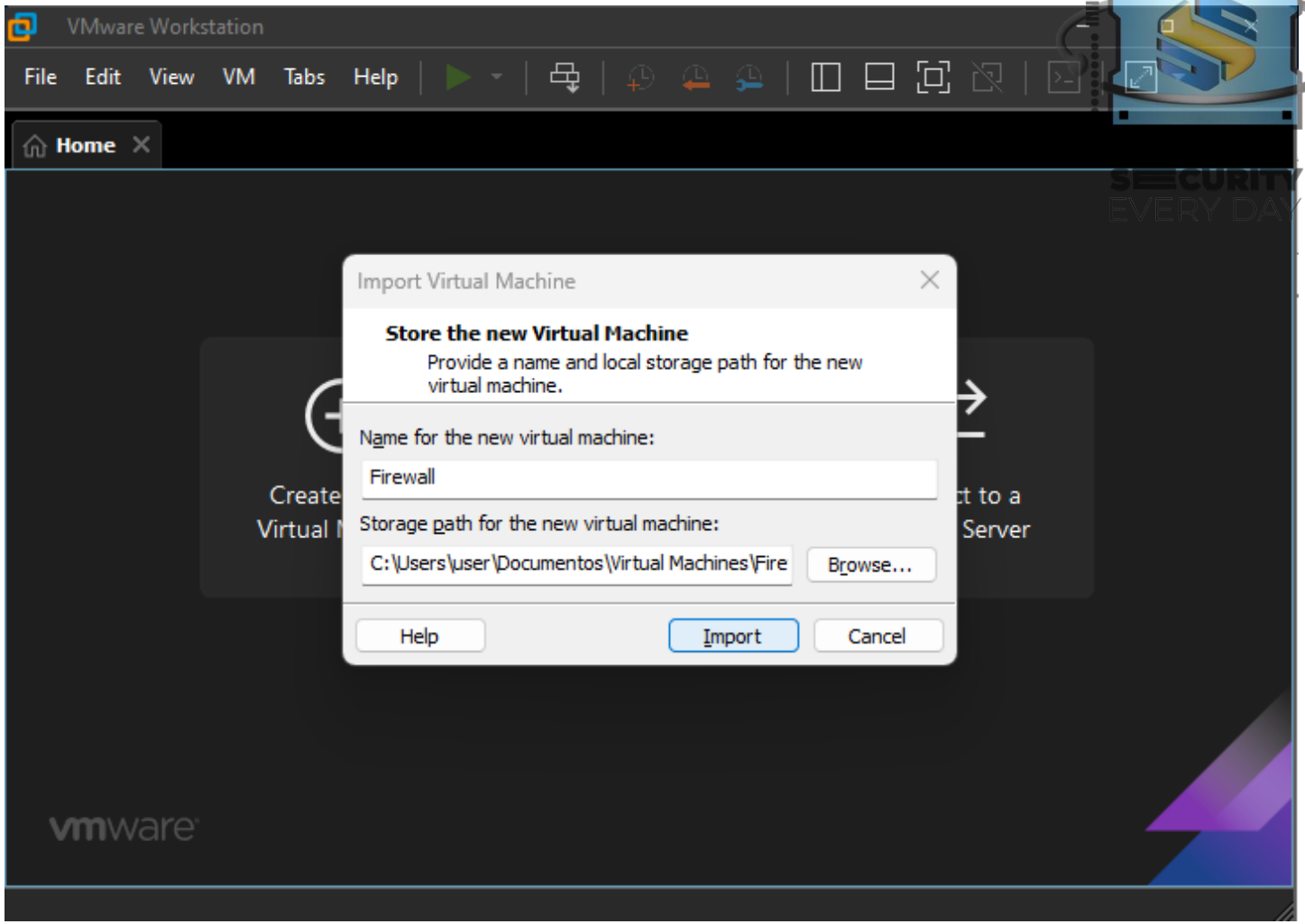
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Vamos começar pelo Firewall
  - Primeiro abra o VMware Workstation
  - Clique em "Open Virtual Machine" e vá até a pasta do Firewall (extraída anteriormente) e clique em "Abrir"



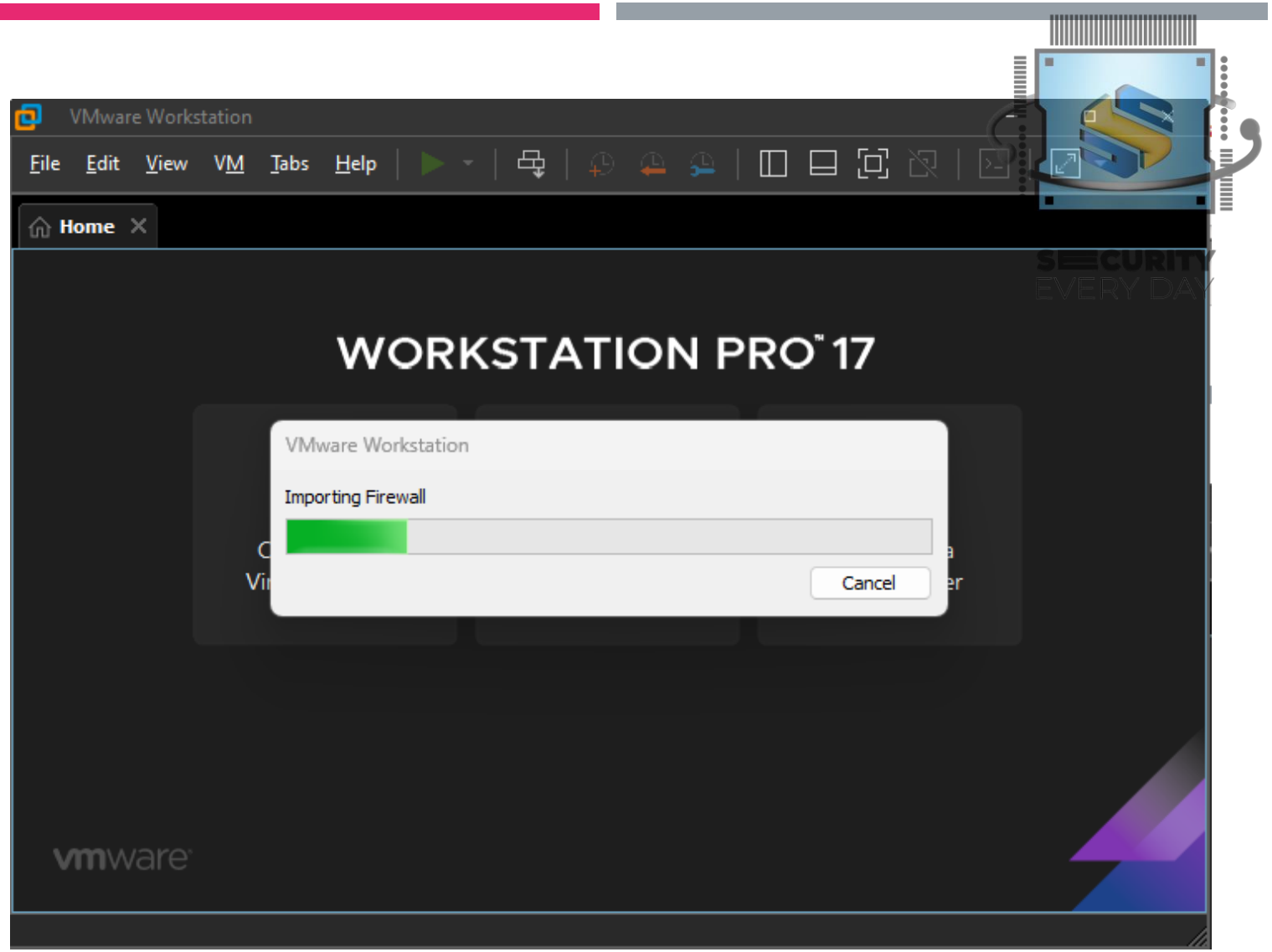
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Defina um nome para a VM, para fins de organização, recomendo utilizar "Firewall", após isso, clique em "Import"



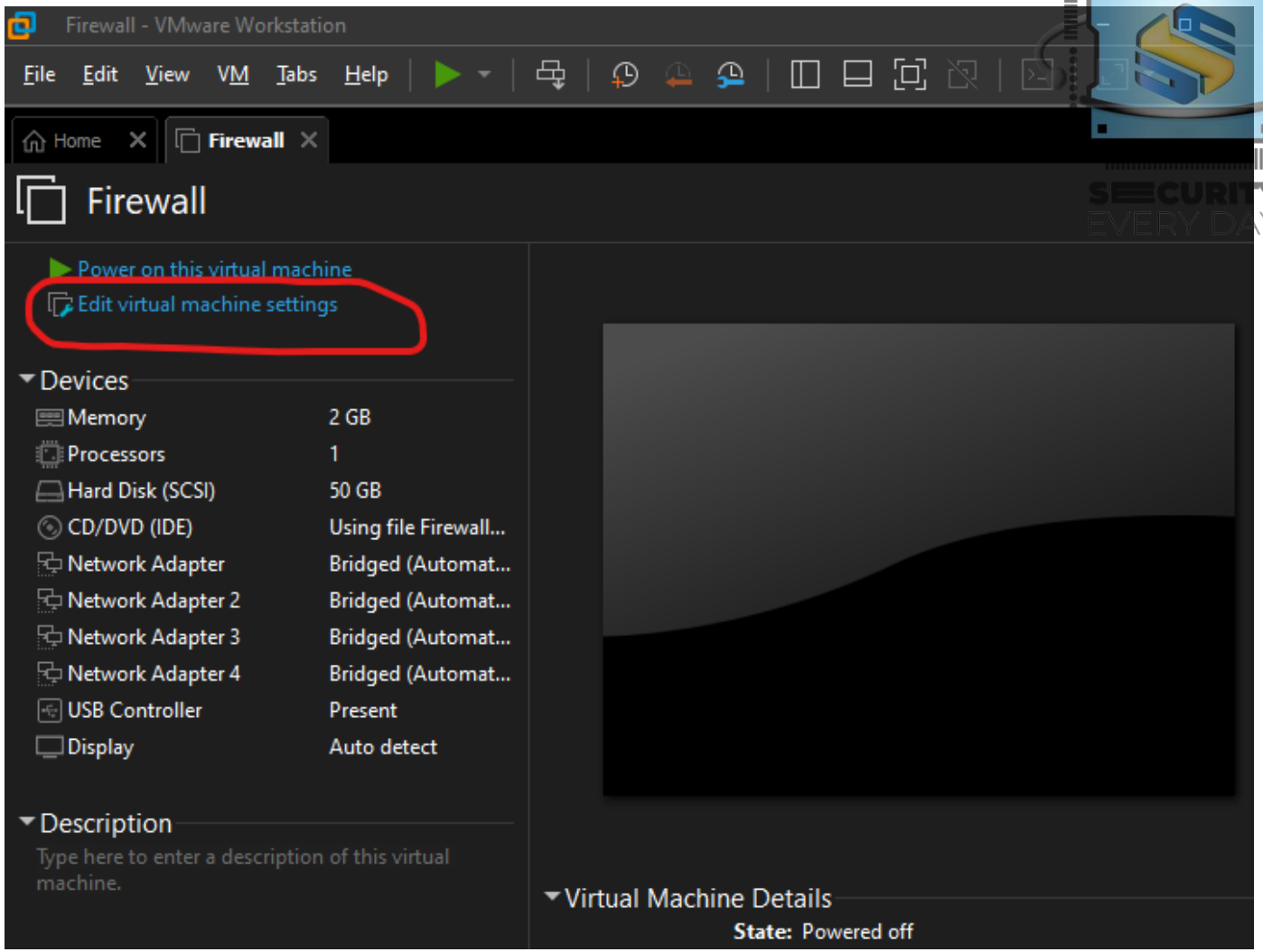
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Aguarde até que a VM seja importada



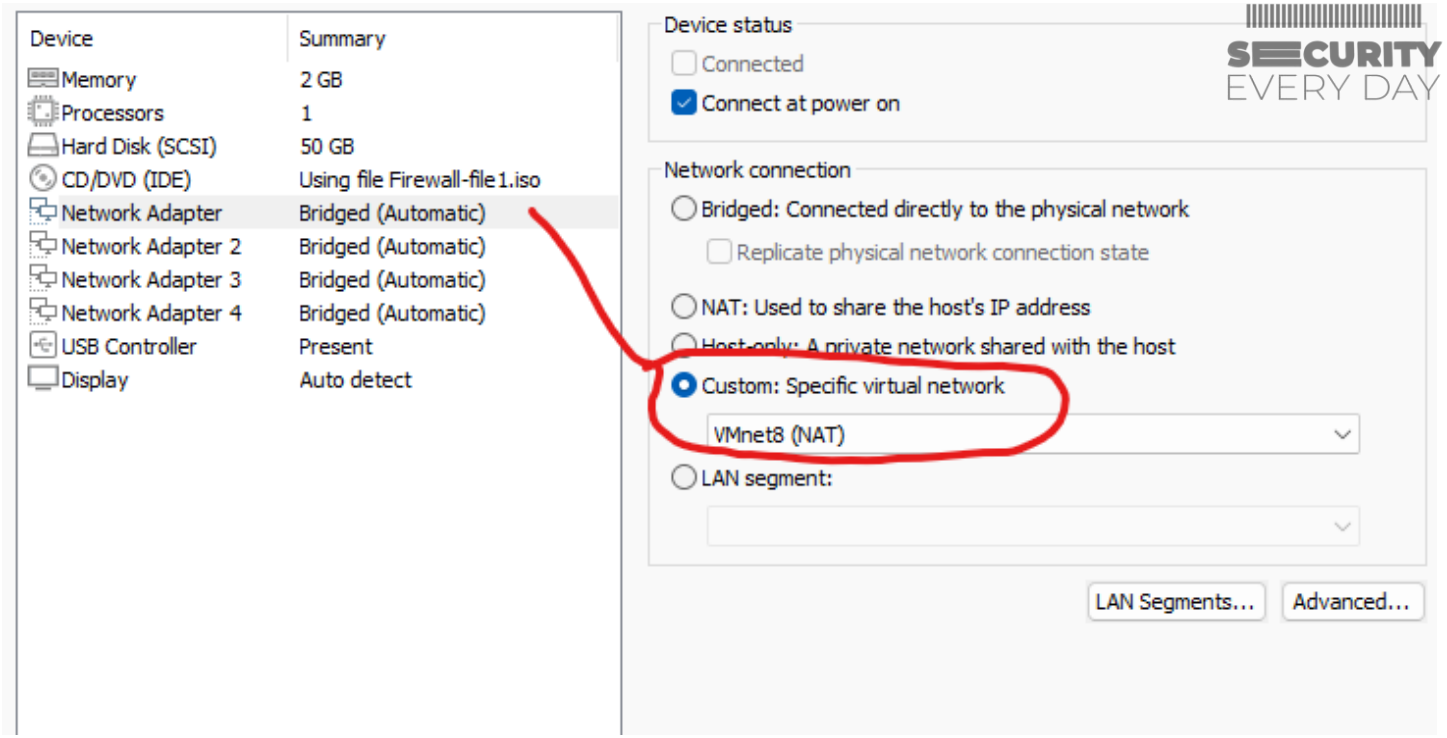
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Após o import, clique em "Edit virtual machine settings"



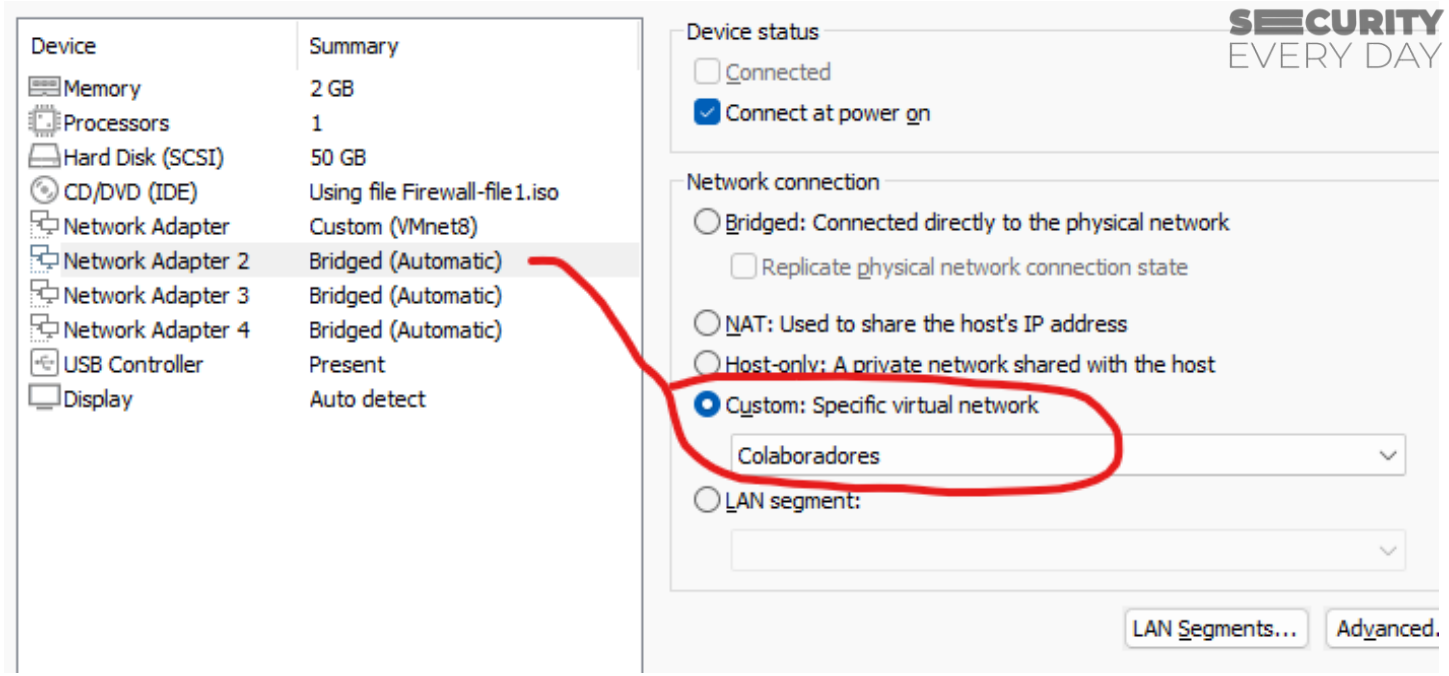
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Navegue até "Network Adapter" e deixe exatamente com essa configuração na mesma ordem para cada adpitador de rede:
  - Network Adapter



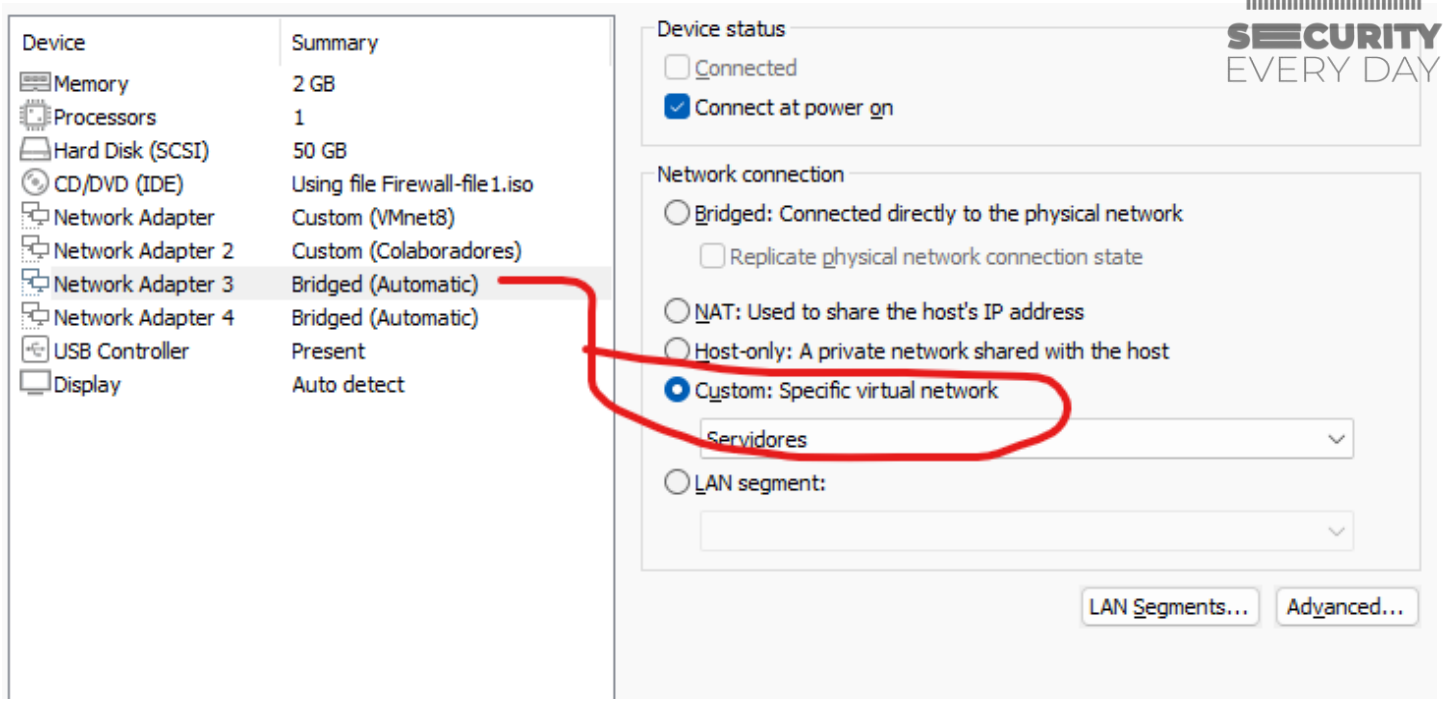
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Navegue até "Network Adapter" e deixe exatamente com essa configuração na mesma ordem para cada adpitador de rede:
  - Network Adapter 2



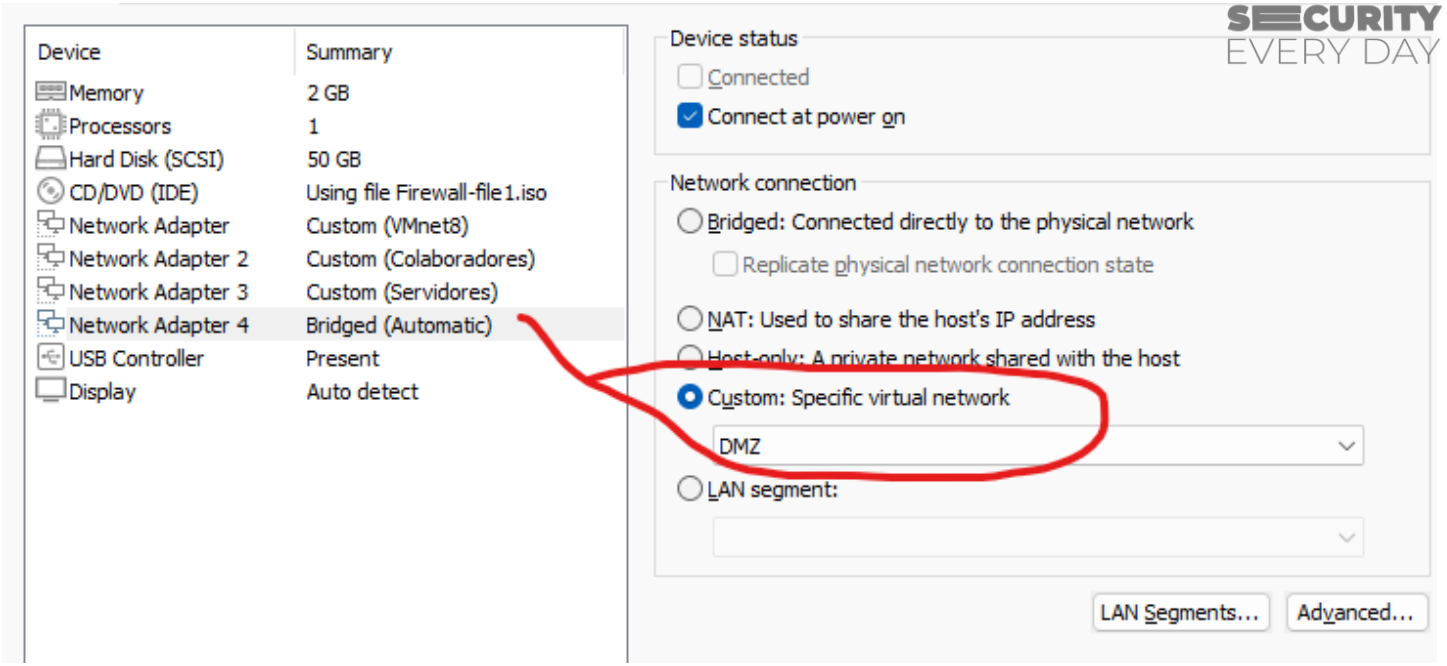
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Navegue até "Network Adapter" e deixe exatamente com essa configuração na mesma ordem para cada adpitador de rede:
  - Network Adapter 3



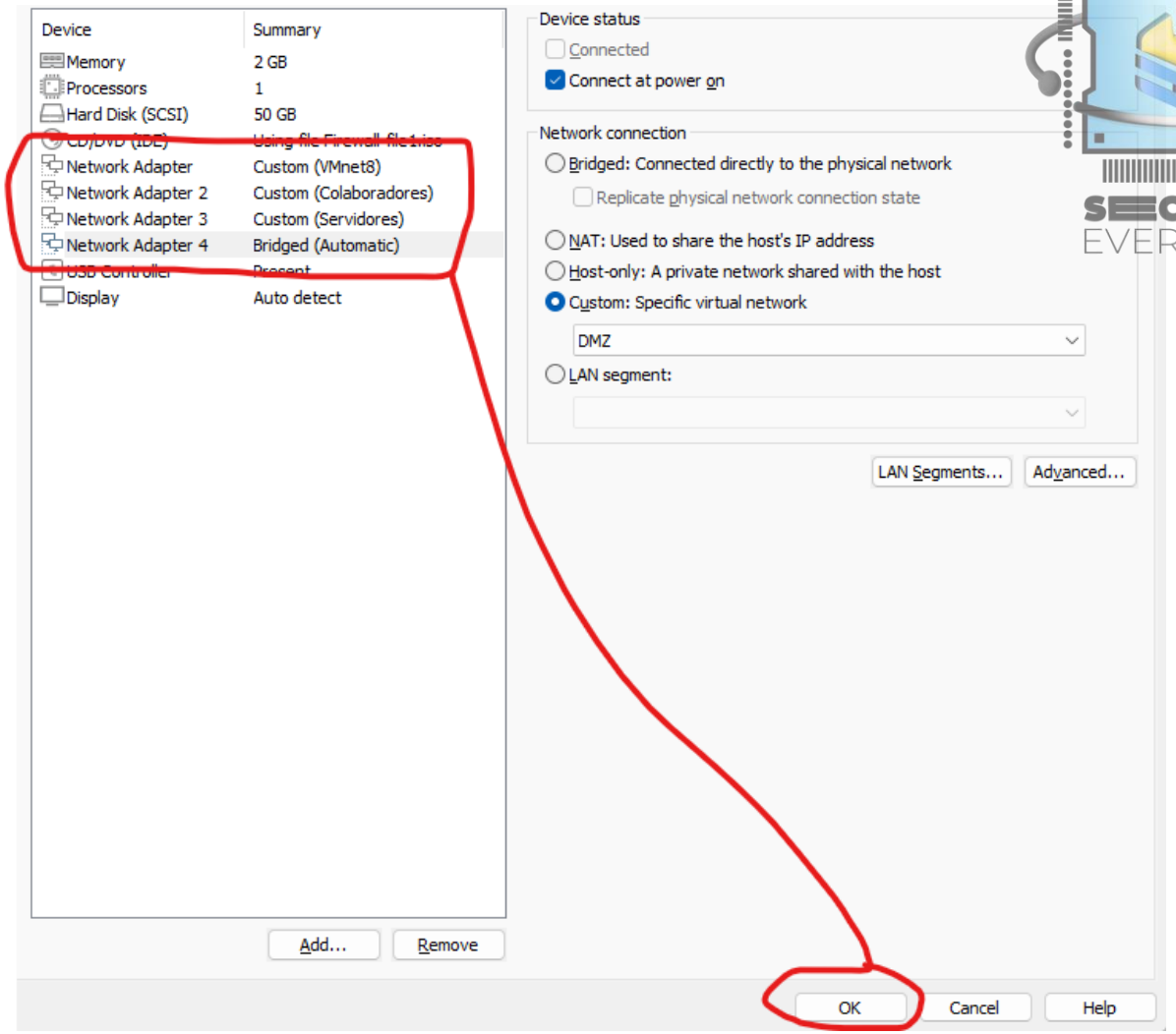
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Navegue até "Network Adapter" e deixe exatamente com essa configuração na mesma ordem para cada adpitador de rede:
  - Network Adapter 4



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

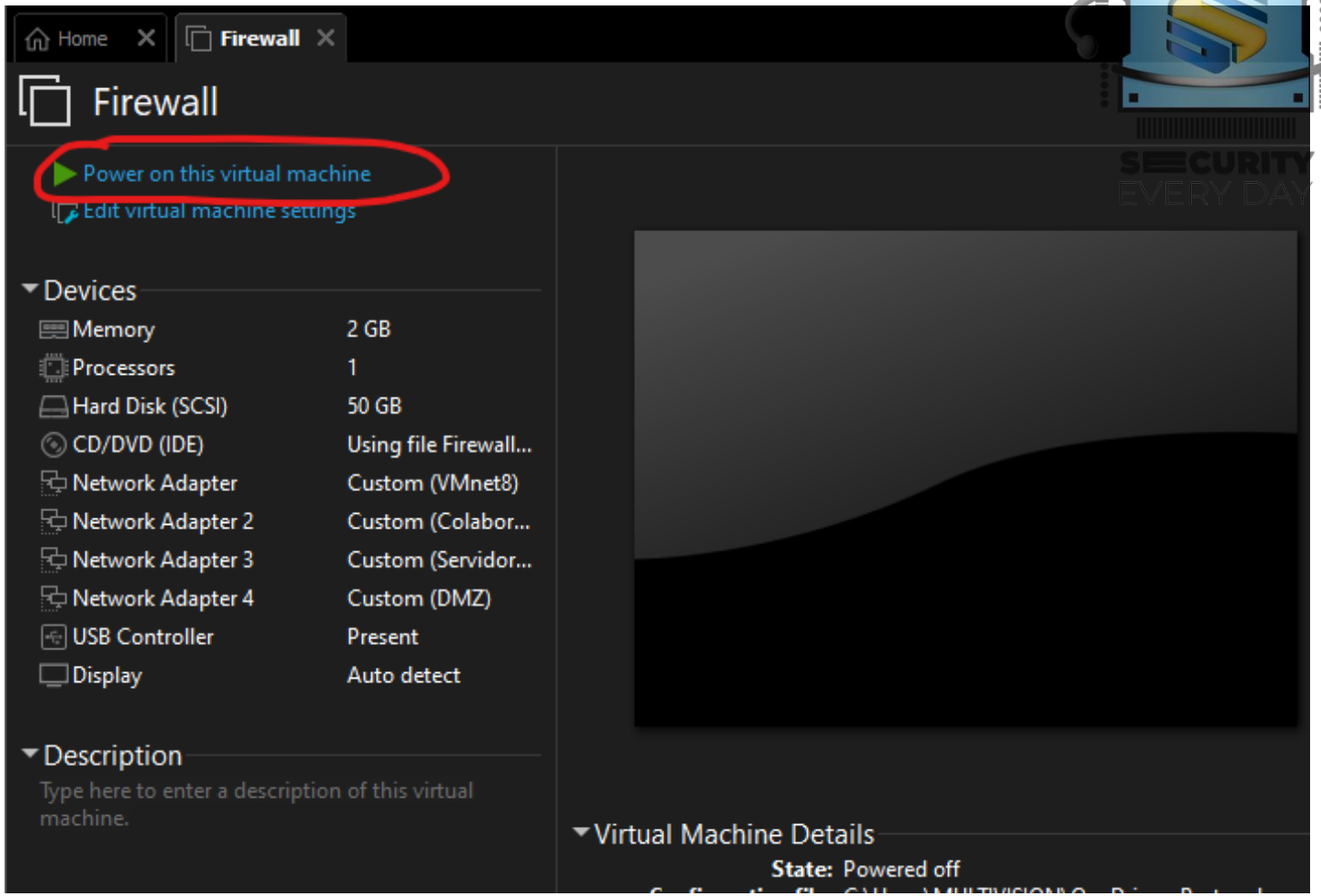
- Feita as alterações, basca clicar em "OK" e iniciar a maquina



SECURITY EVERY DAY

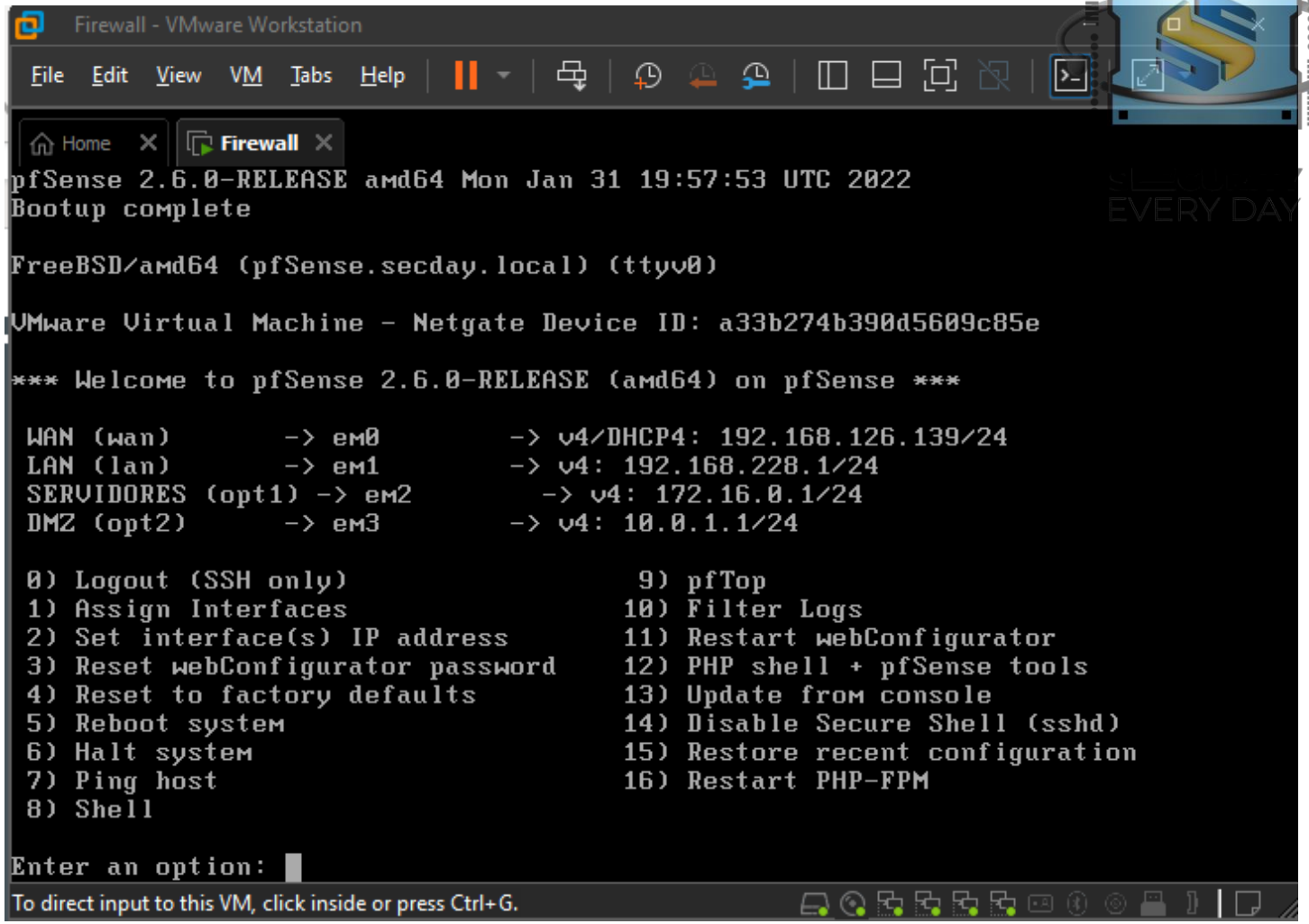
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Feita as alterações, basca clicar em "OK" e iniciar a maquina



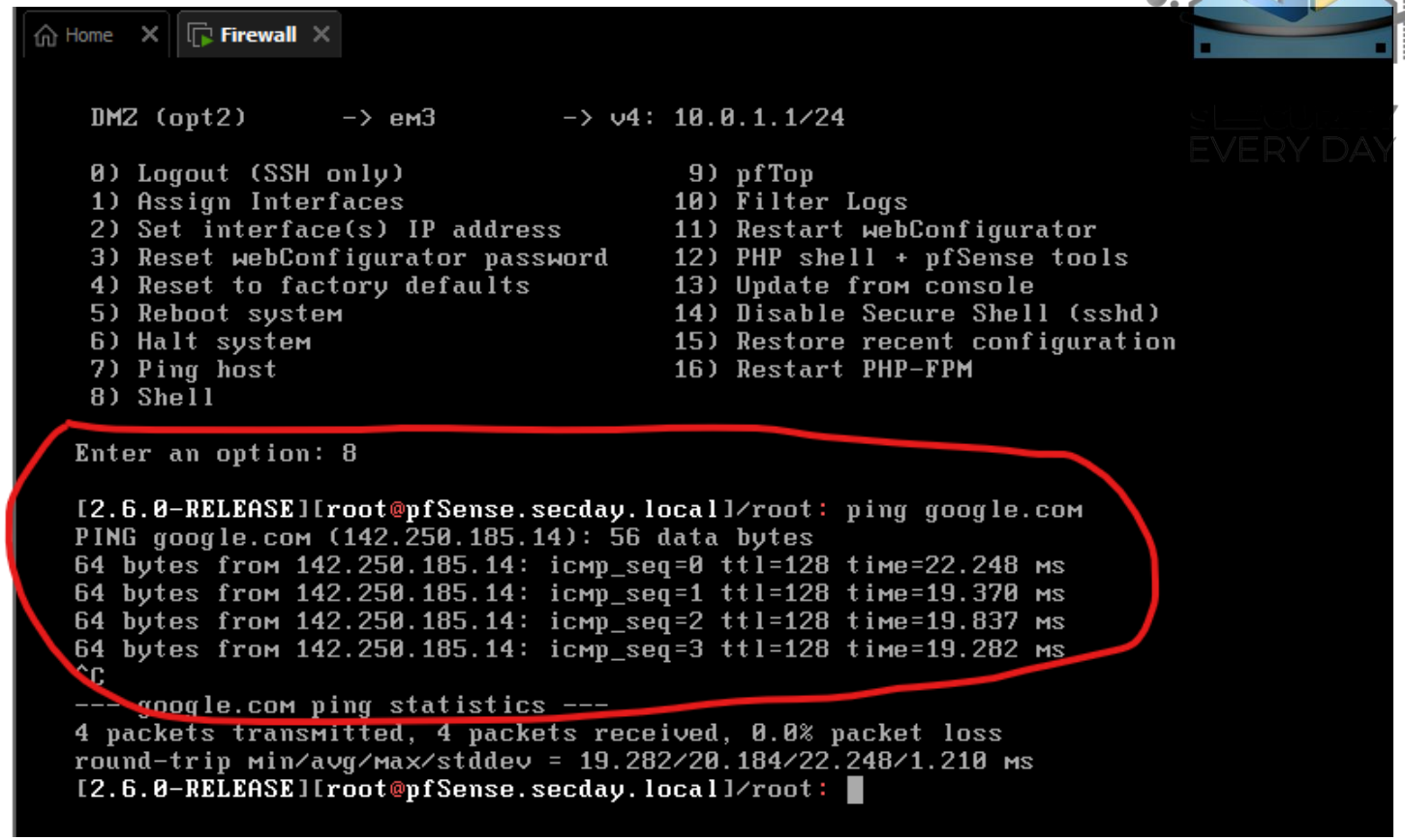
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Ao iniciar o firewall, você deve ver uma tela similar a essa, vamos testar se temos acesso a internet, aperte a tecla "8" e "Enter" para entrar no CLI do pfsense e execute o comando "ping google.com"
  - Obs: aperte "CTRL + C" para parar o comando
  - Obs2: aperte "CTRL (lado direito) + Alt Gr" para tirar o mouse de dentro da VM :)



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Se o retorno for similar a esse, significa que deu tudo certo.



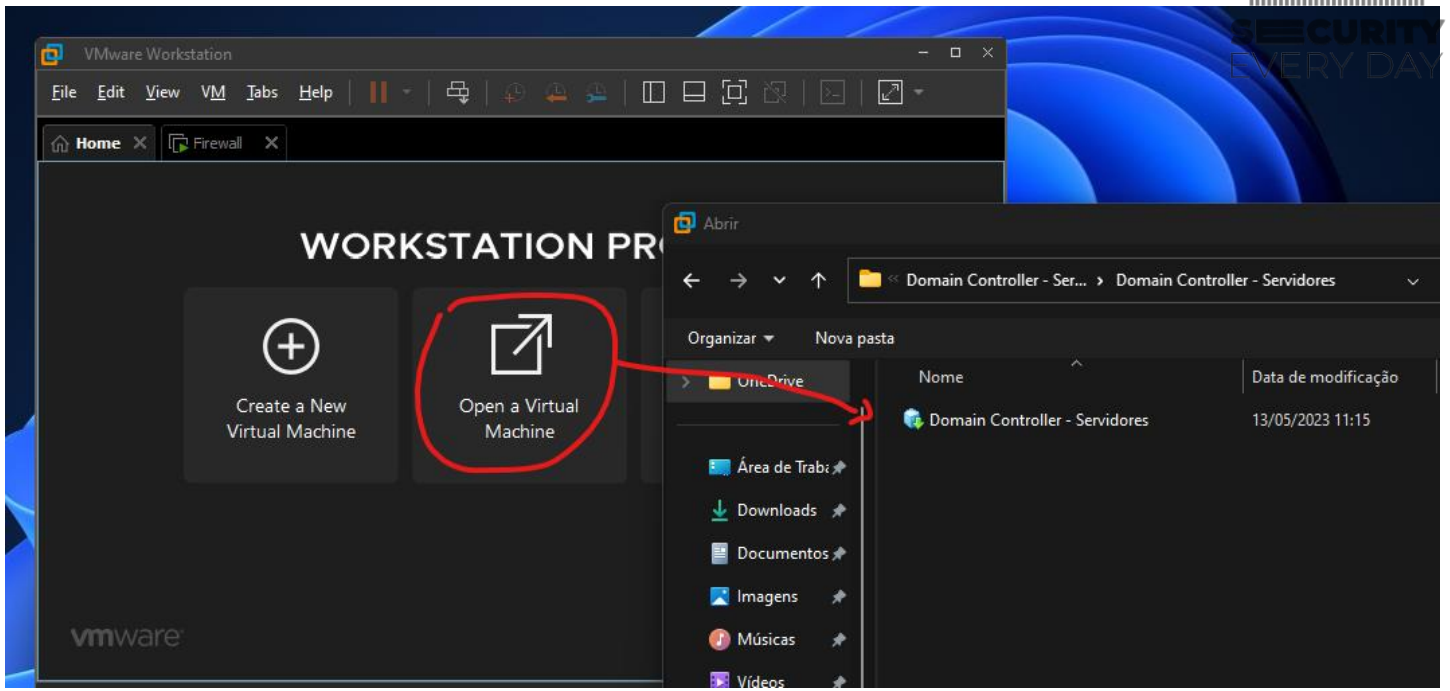
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Vamos fazer o mesmo para todas as maquinas
  - Atenção, altere o Network Adapter antes de iniciar a VM, a seguir vou adicionar os prints em sequencia da configuração de cada vm

VMs	Network Adapter
Domain Controller - Servidores	Servidores
Library - DMZ	DMZ
Web interno - Servidores	Servidores
Windows 10 - Colaboradores	Colaboradores

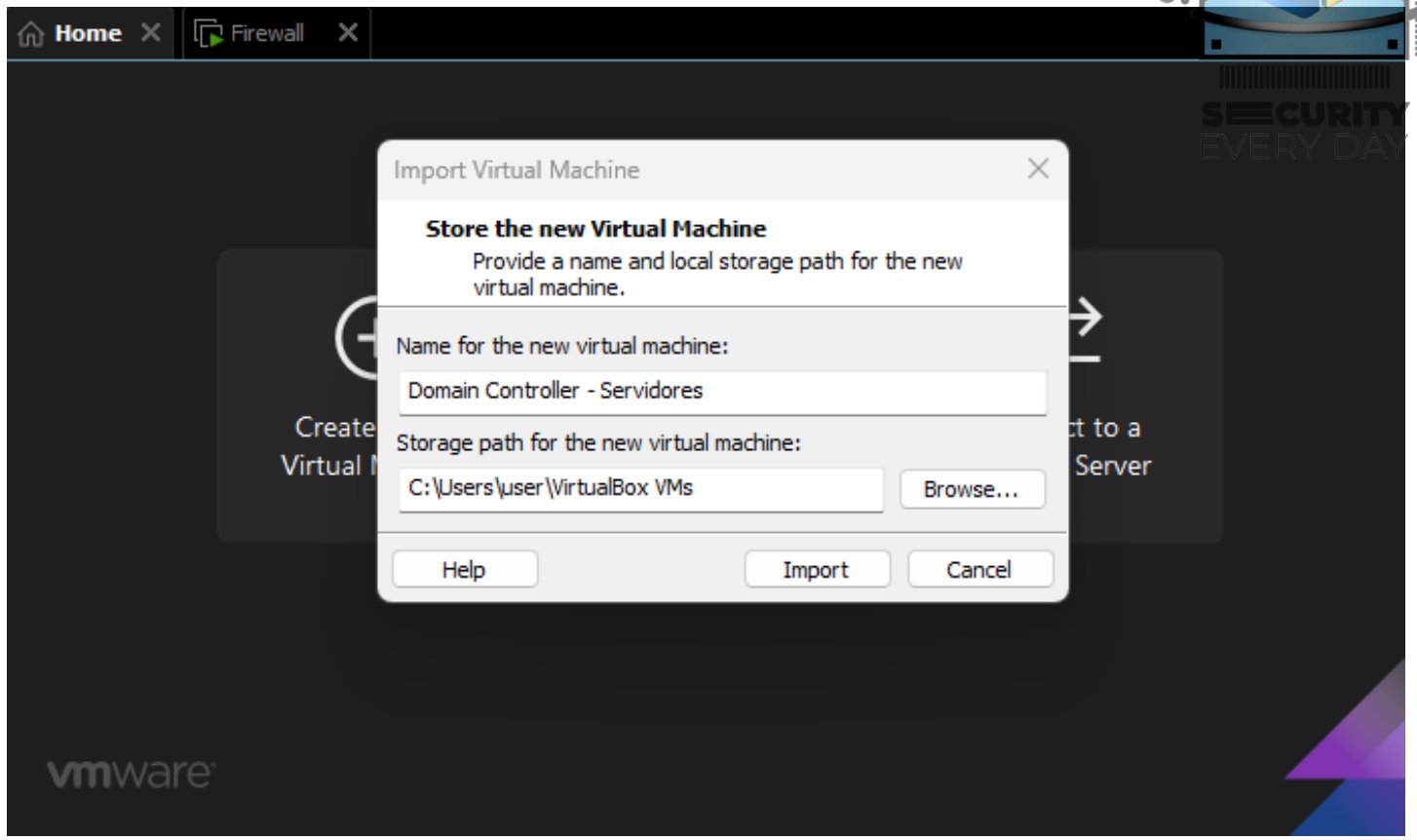
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



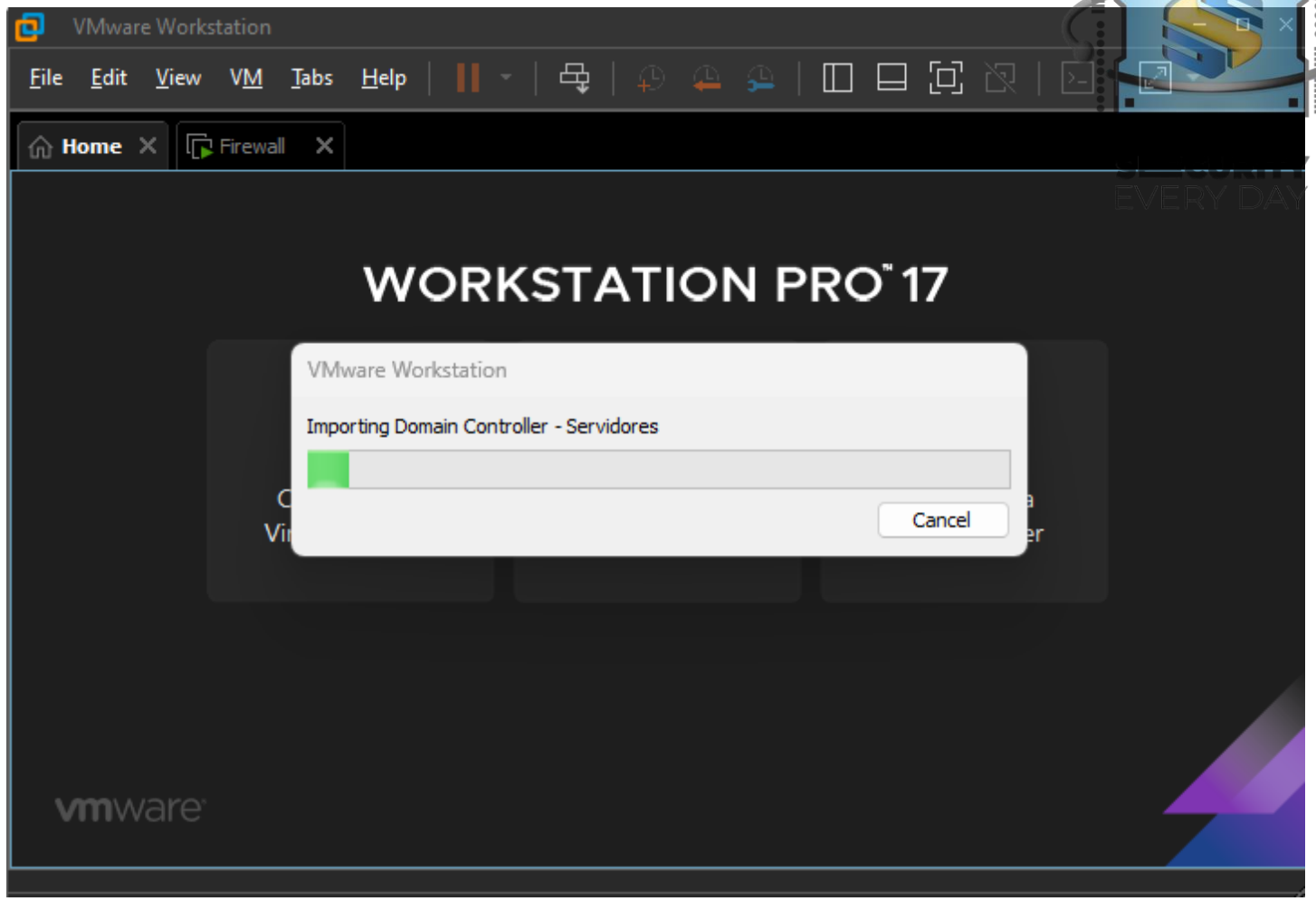
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



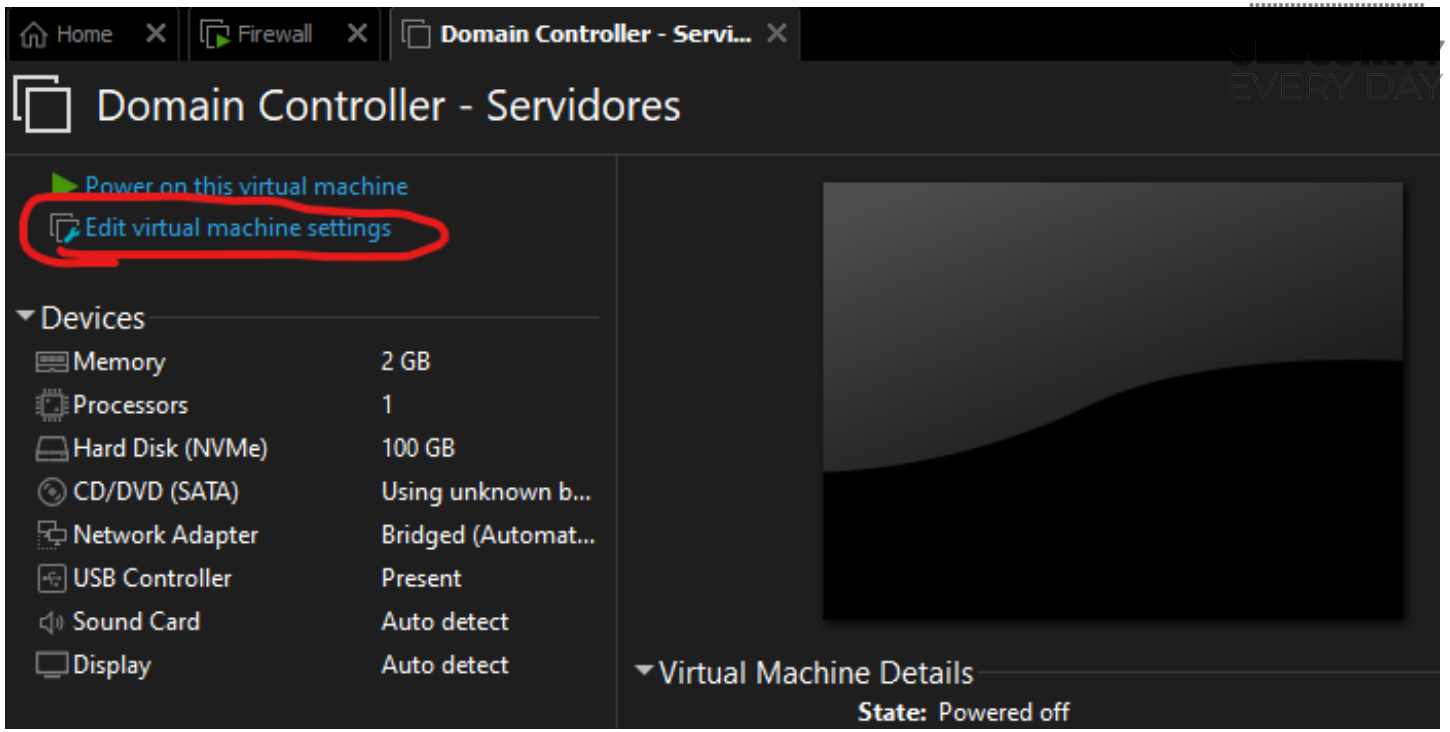
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



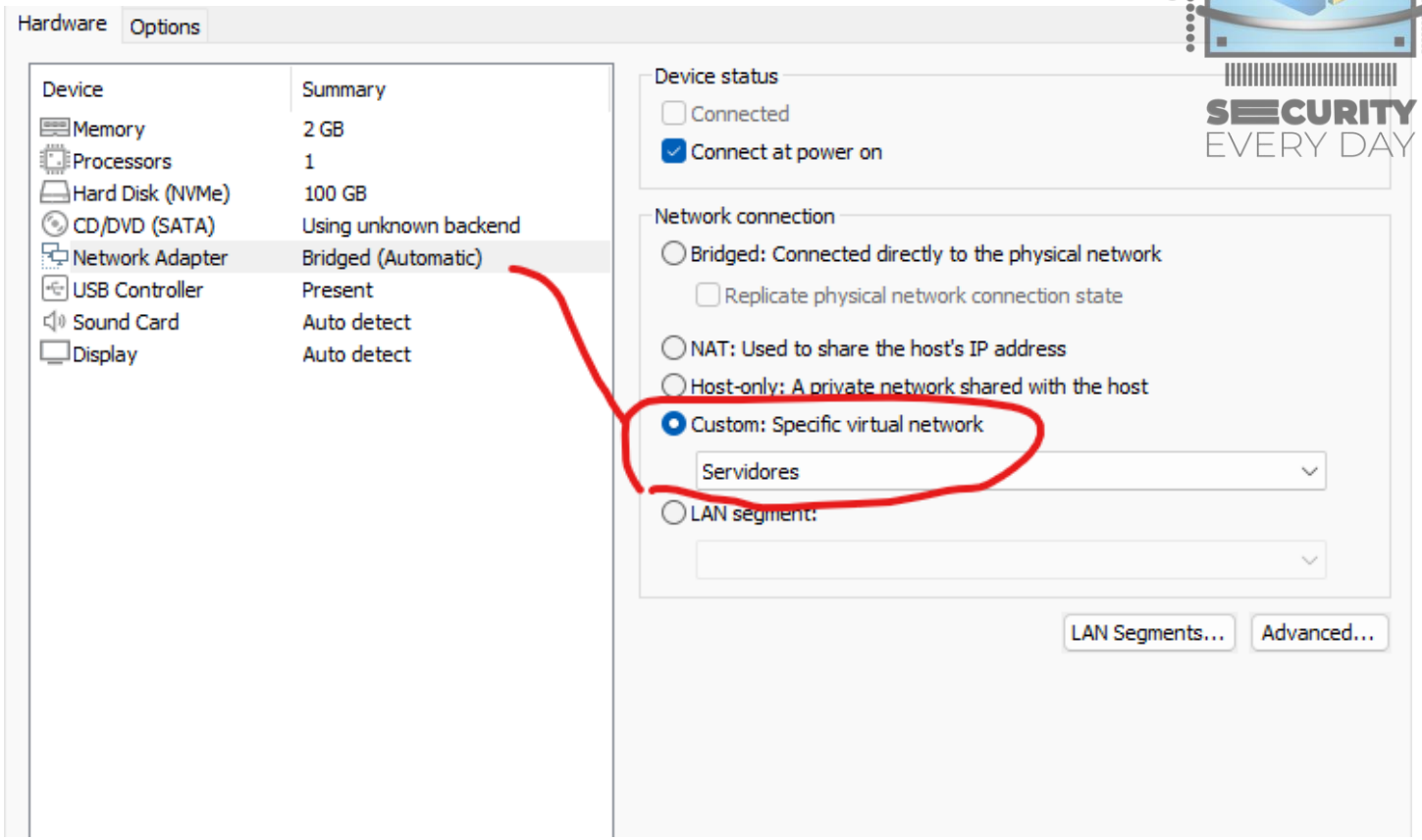
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



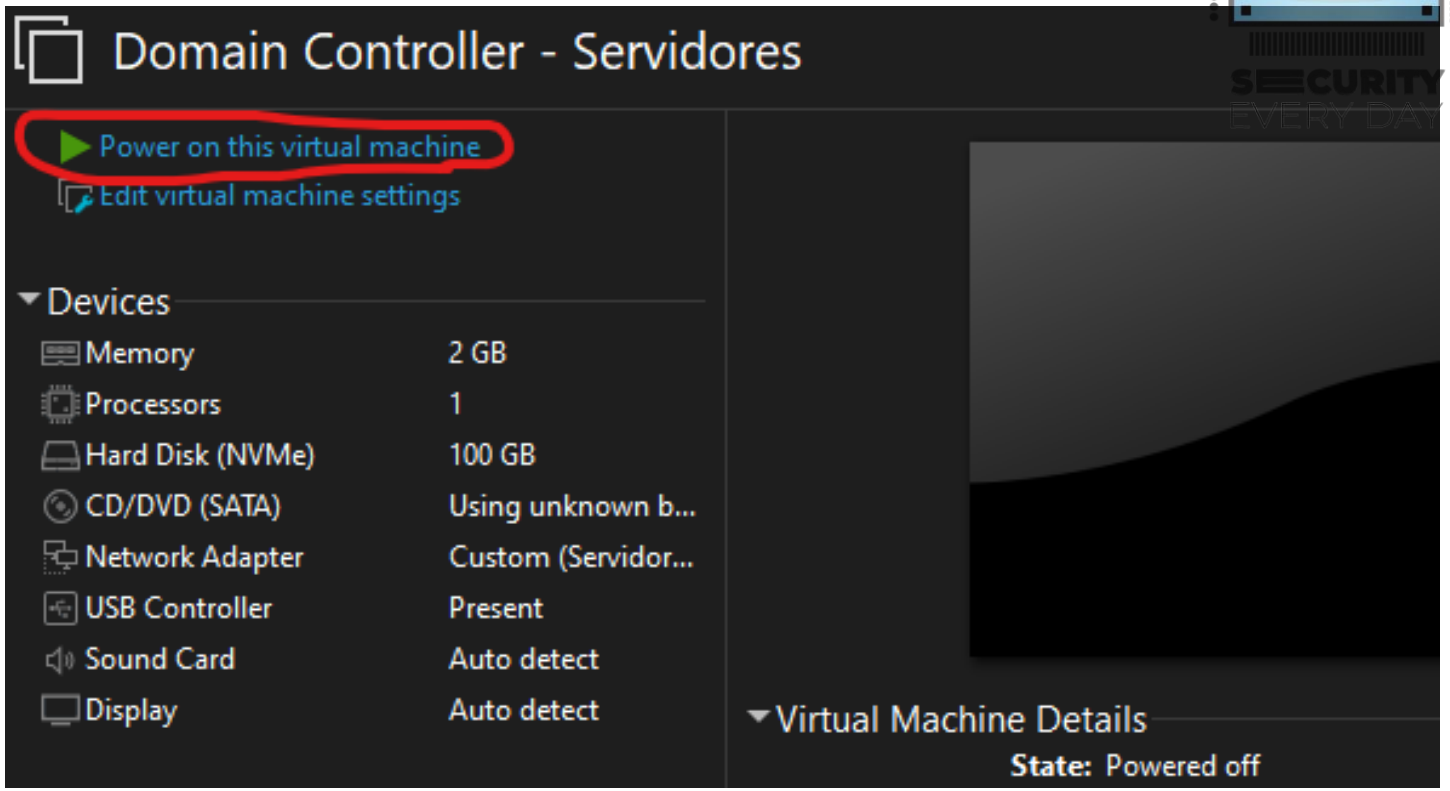
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



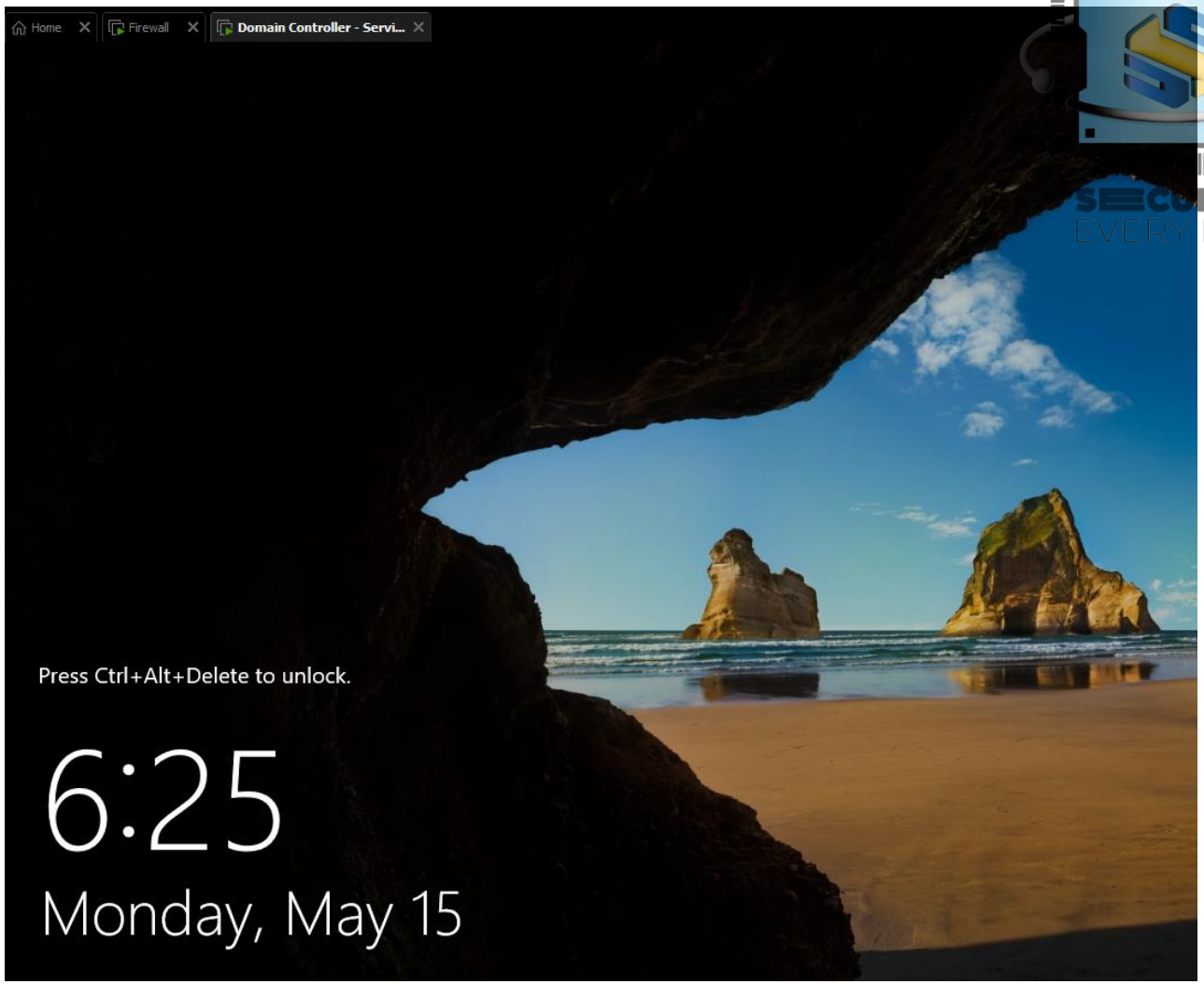
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



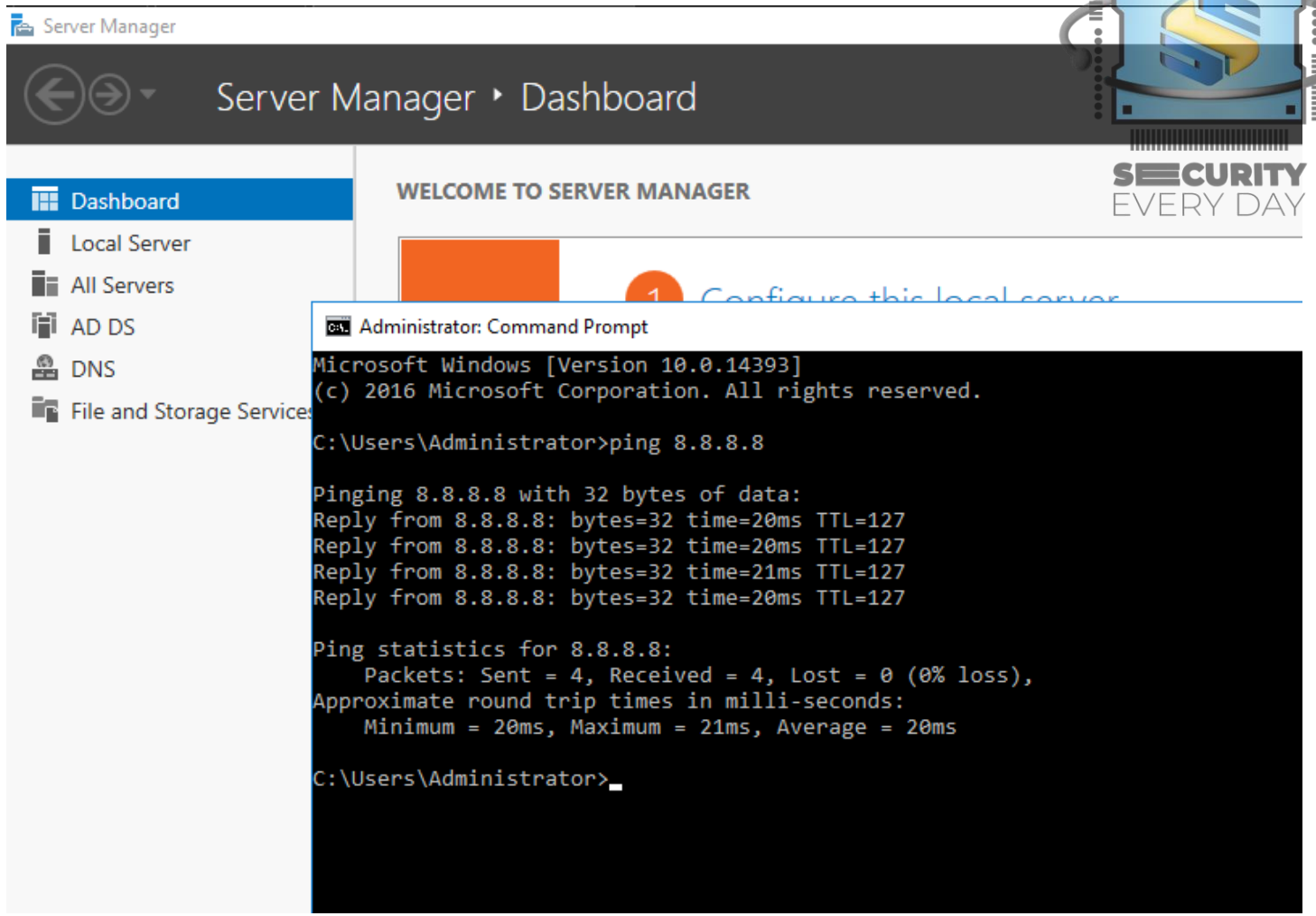
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



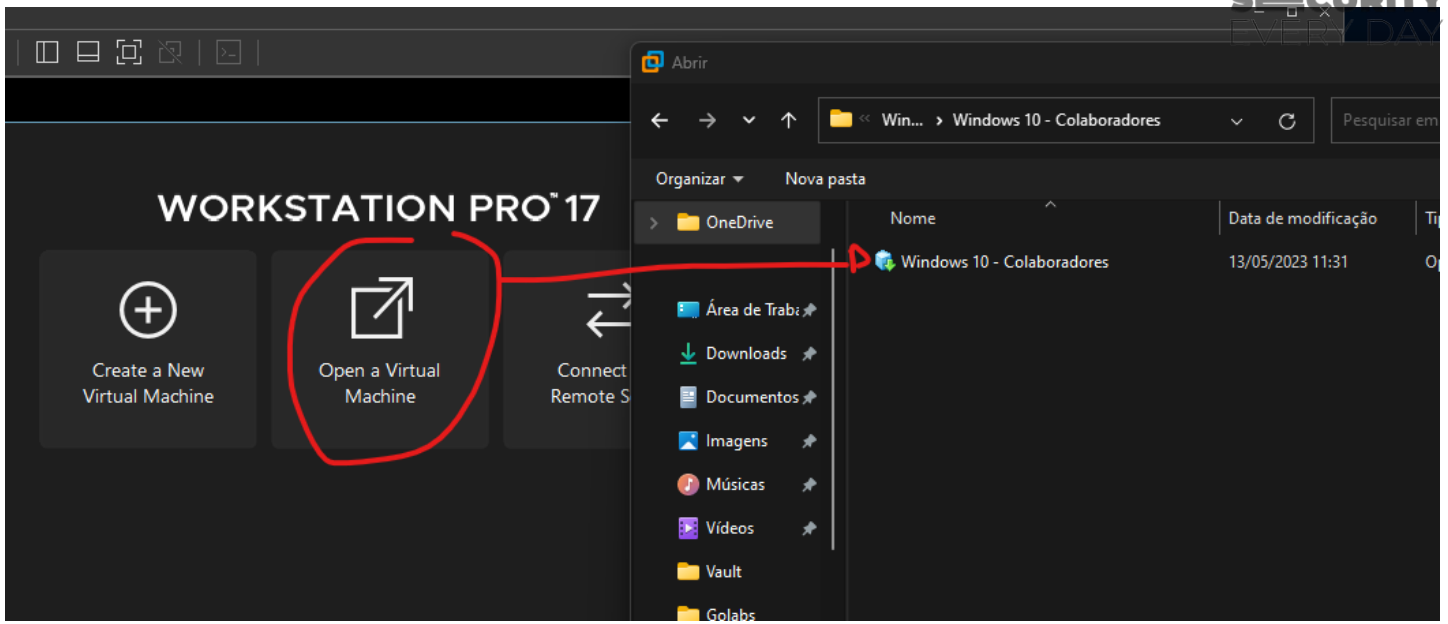
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores
- Entre com o usuário "Administrator" senha "Admin@mudar" e execute um "ping 8.8.8.8", se a conexão foi estabelecida com sucesso, significa que tudo deu certo



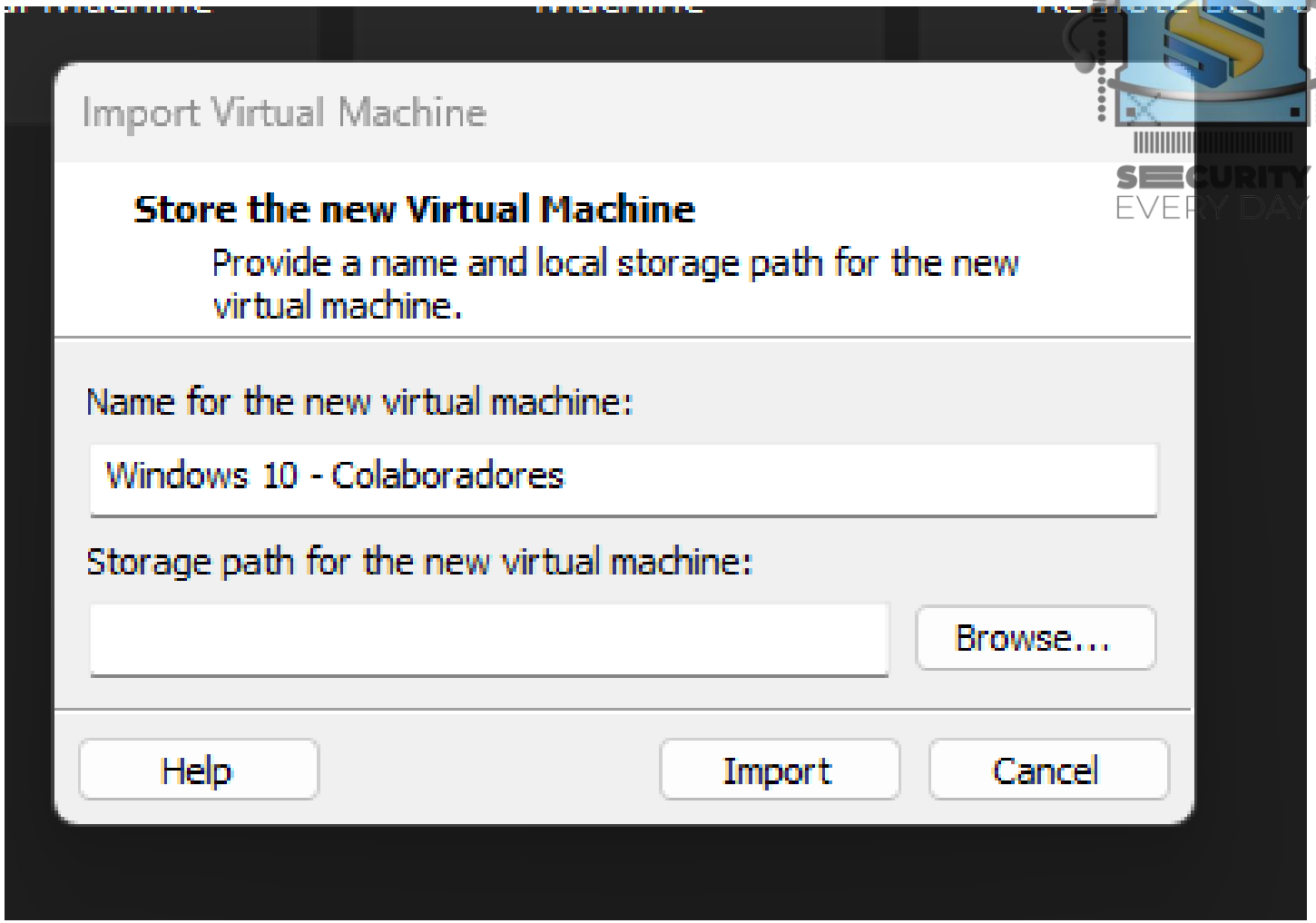
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



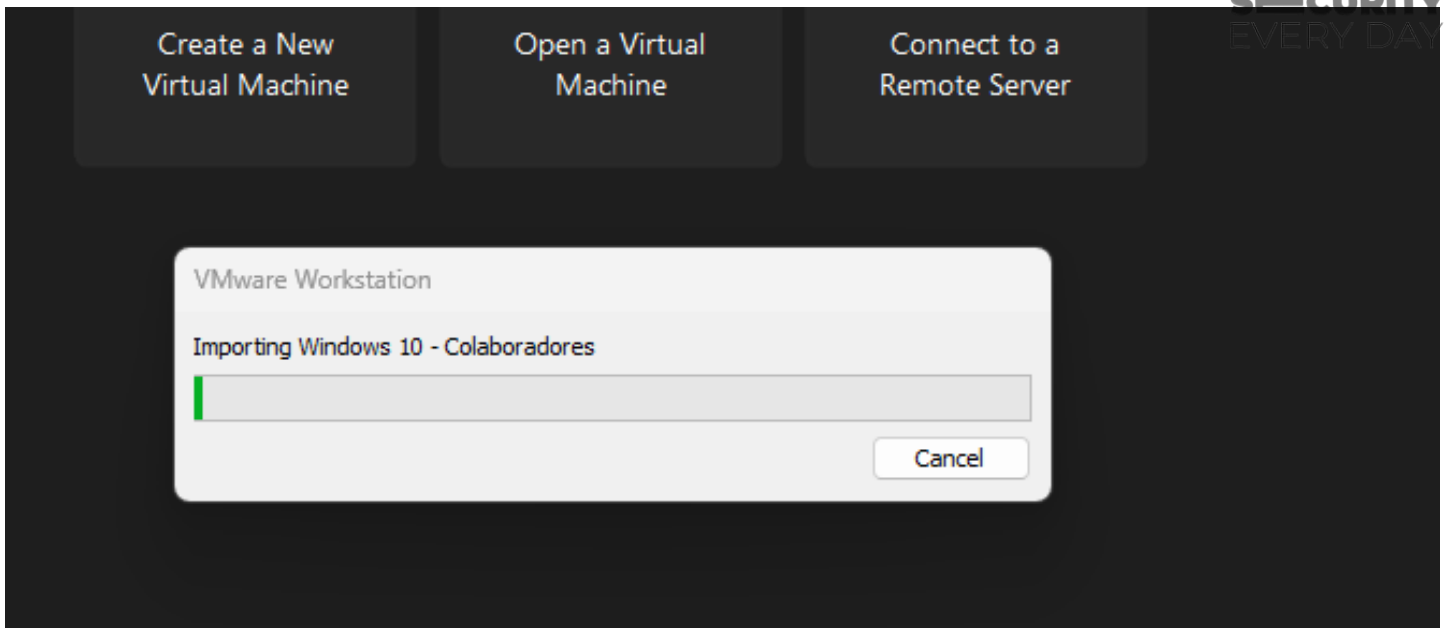
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



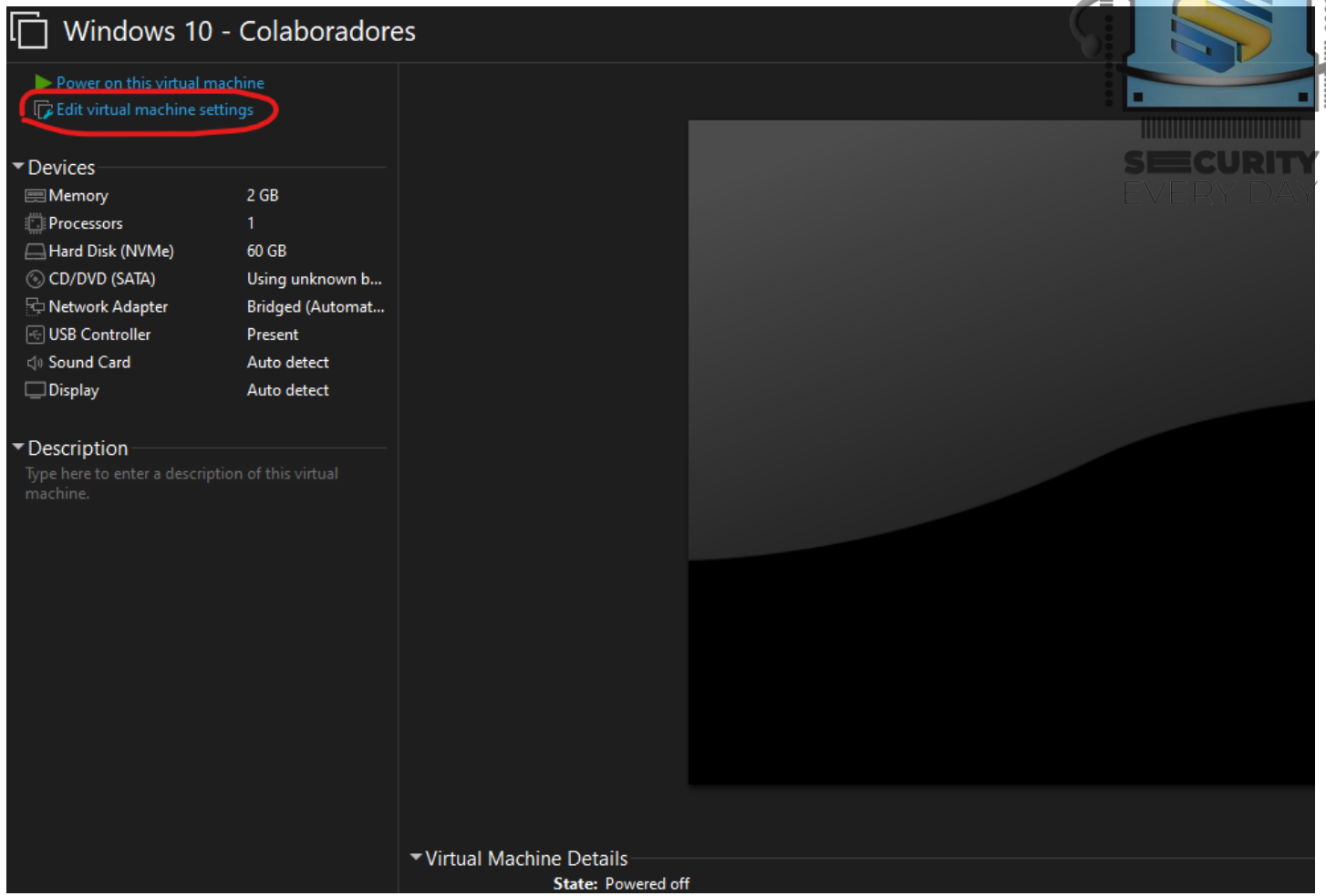
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



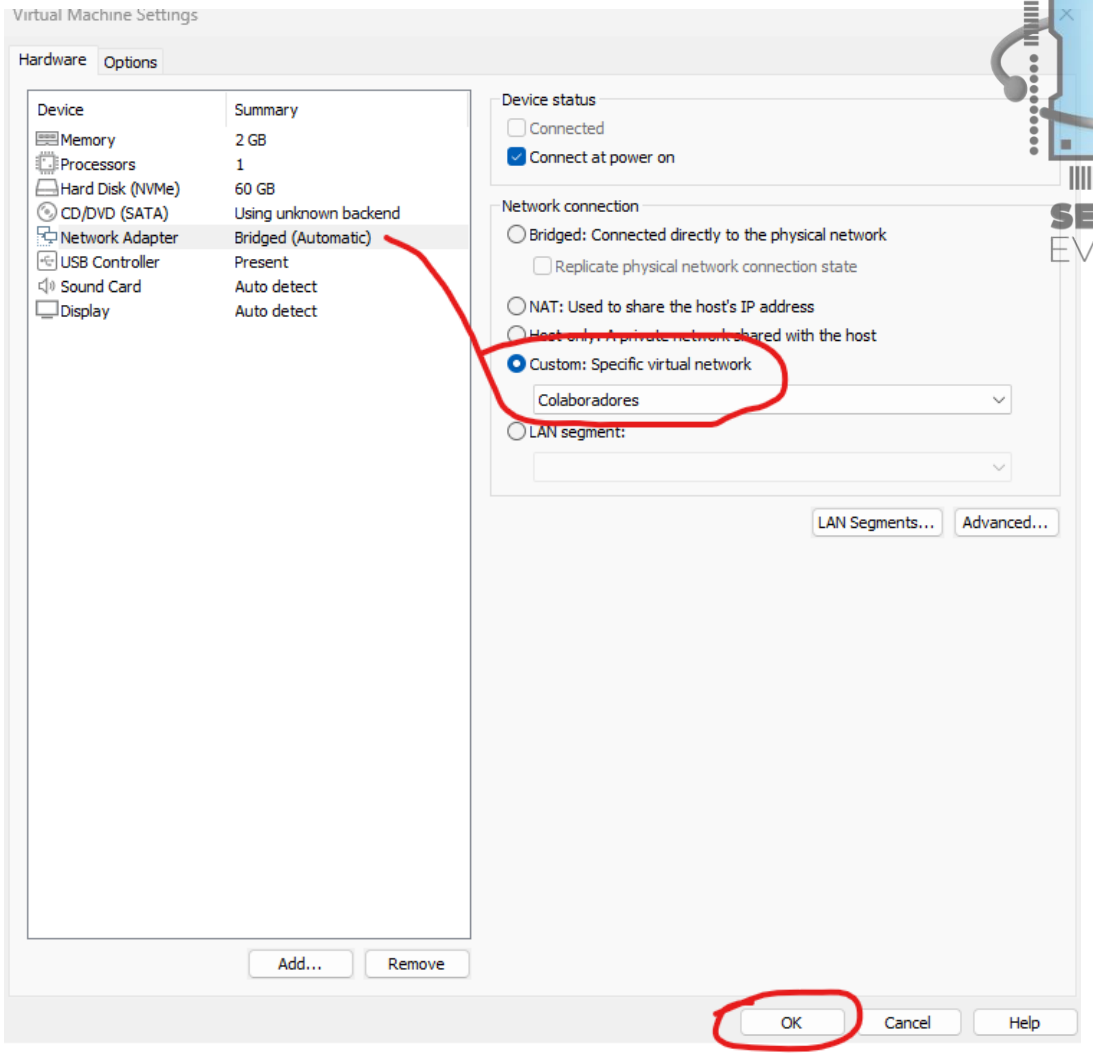
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



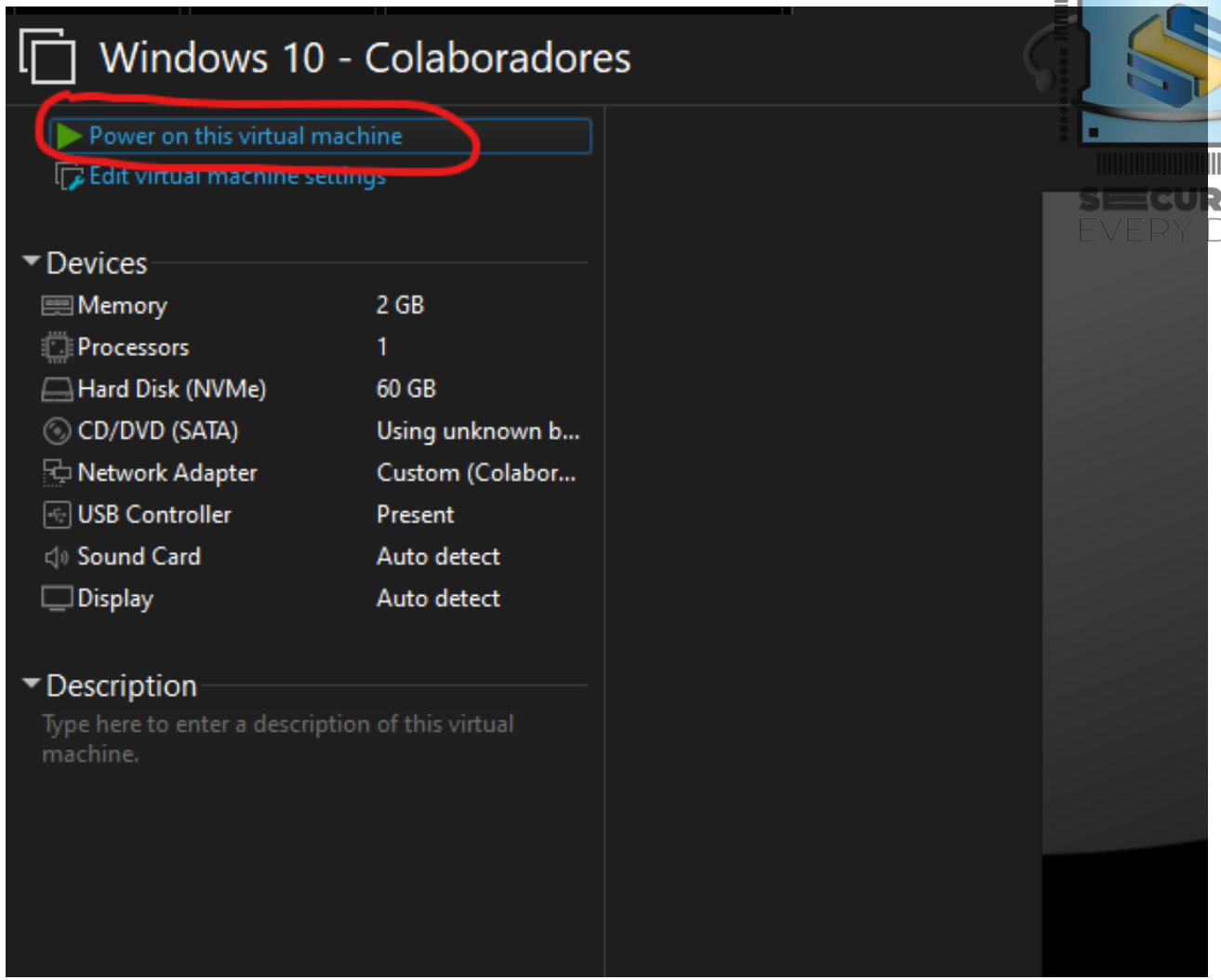
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



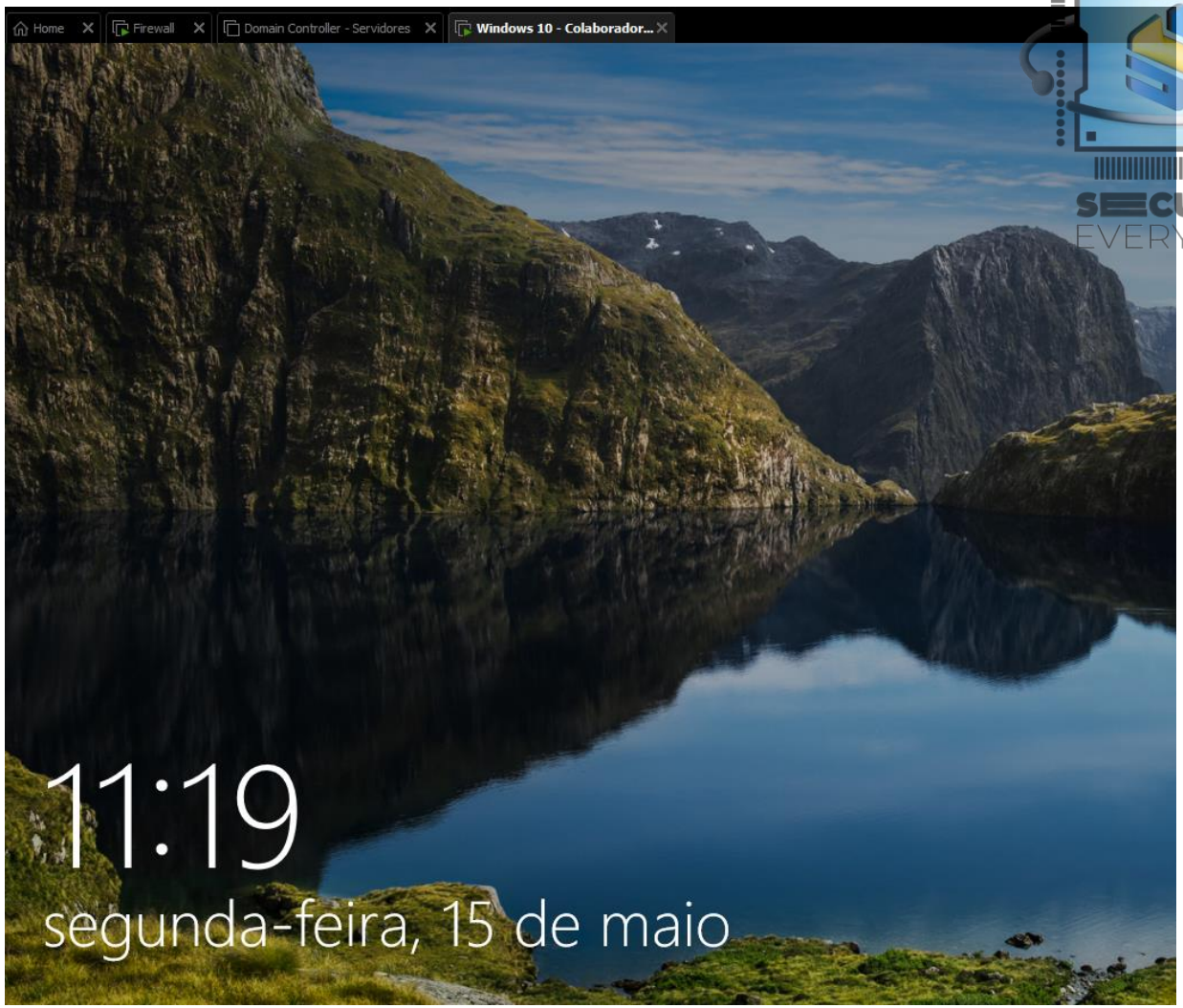
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

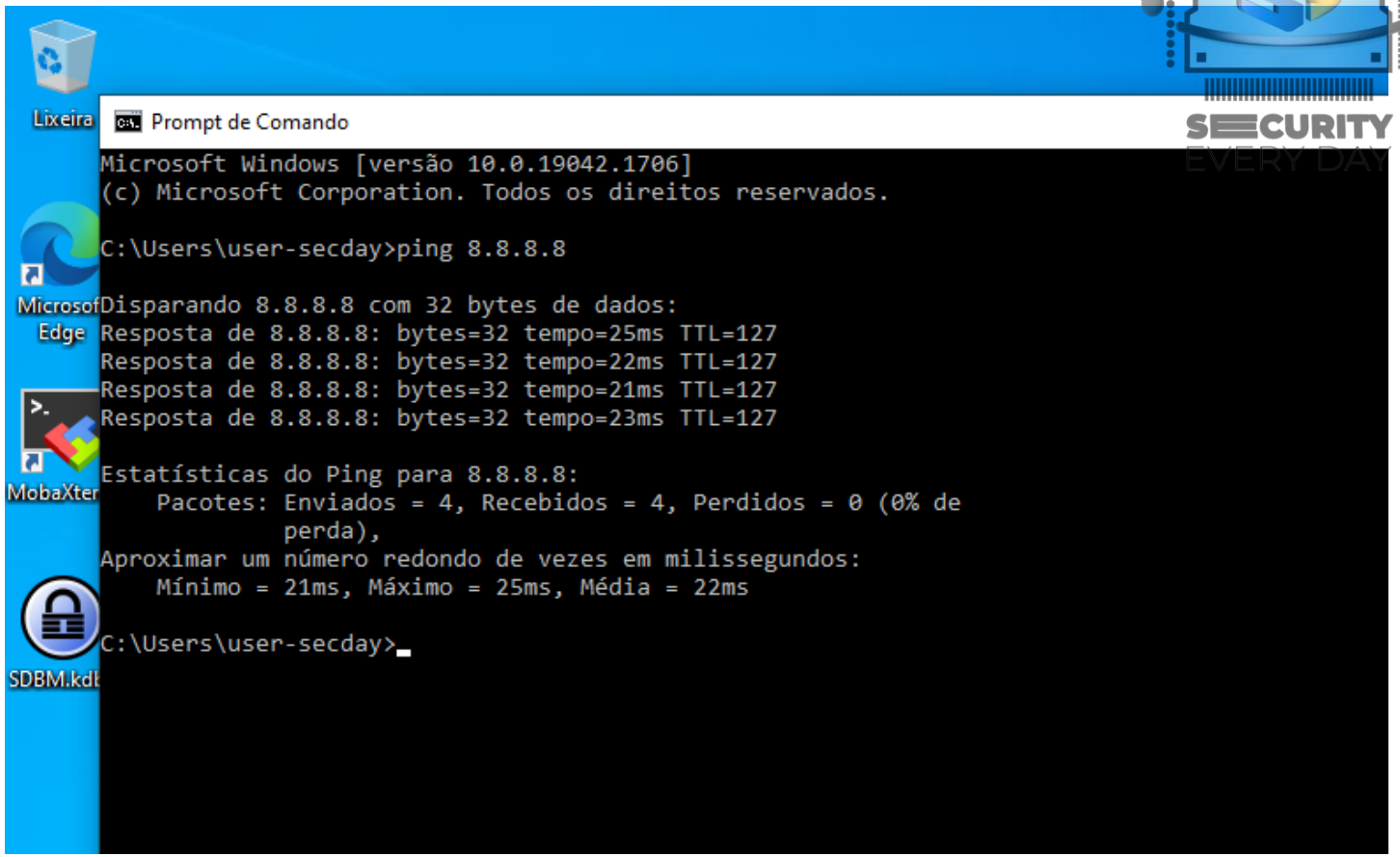
- Windows 10 - Colaboradores



SECURITY
EVERY DAY

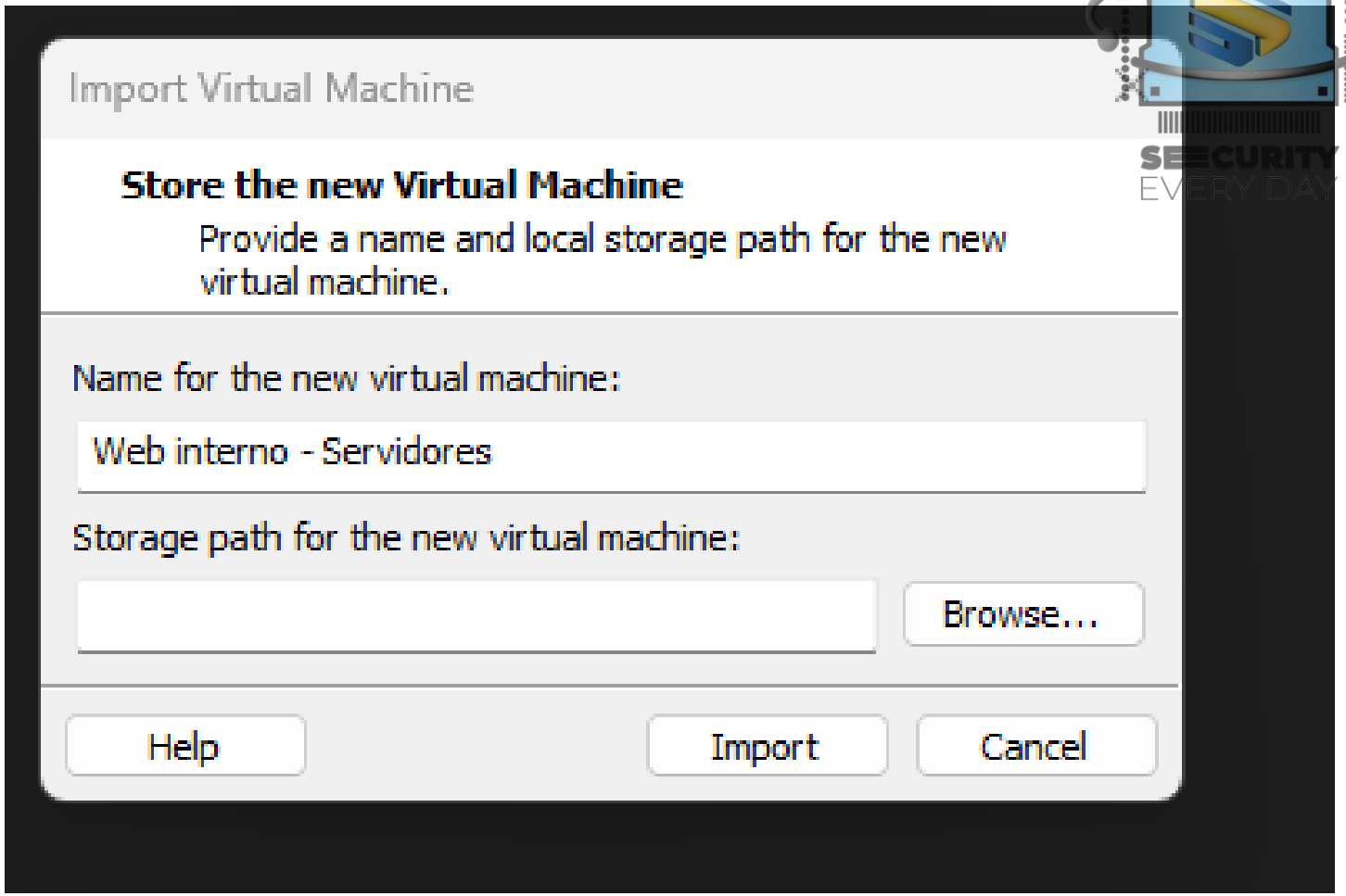
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 – Colaboradores
- Entre com o usuário "user-secday" senha "Admin@mudar" e execute um "ping 8.8.8.8", se a conexão foi estabelecida com sucesso, significa que tudo deu certo



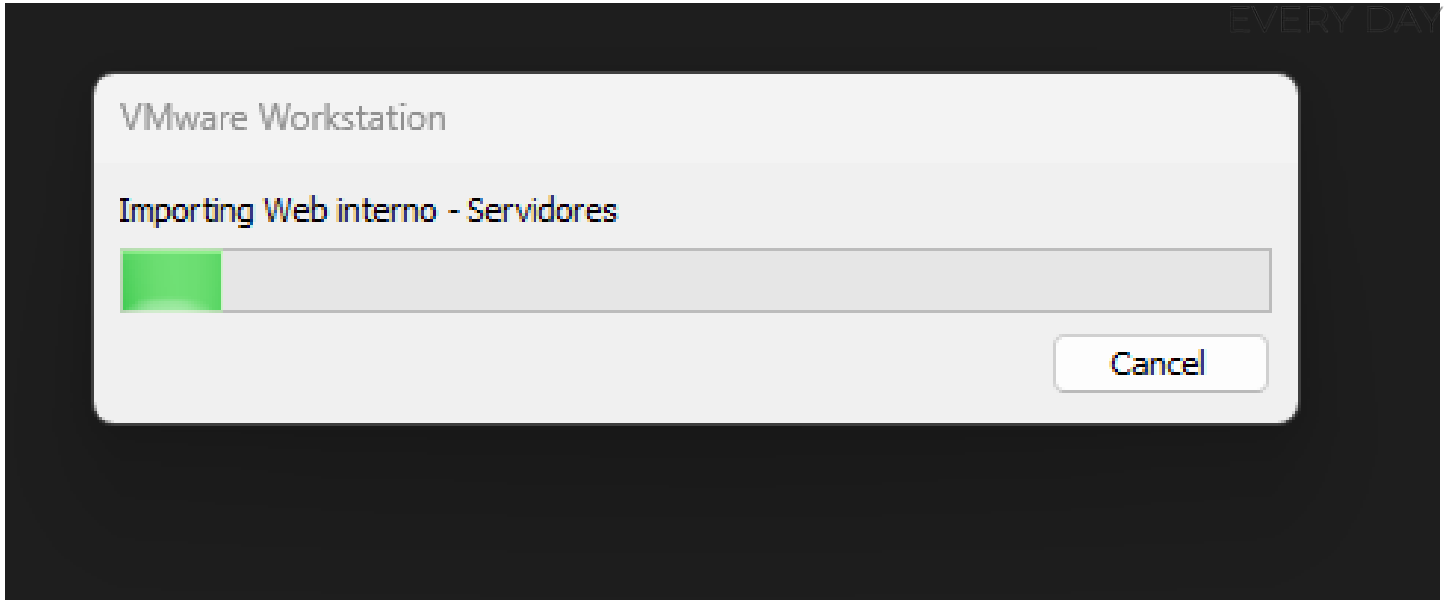
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



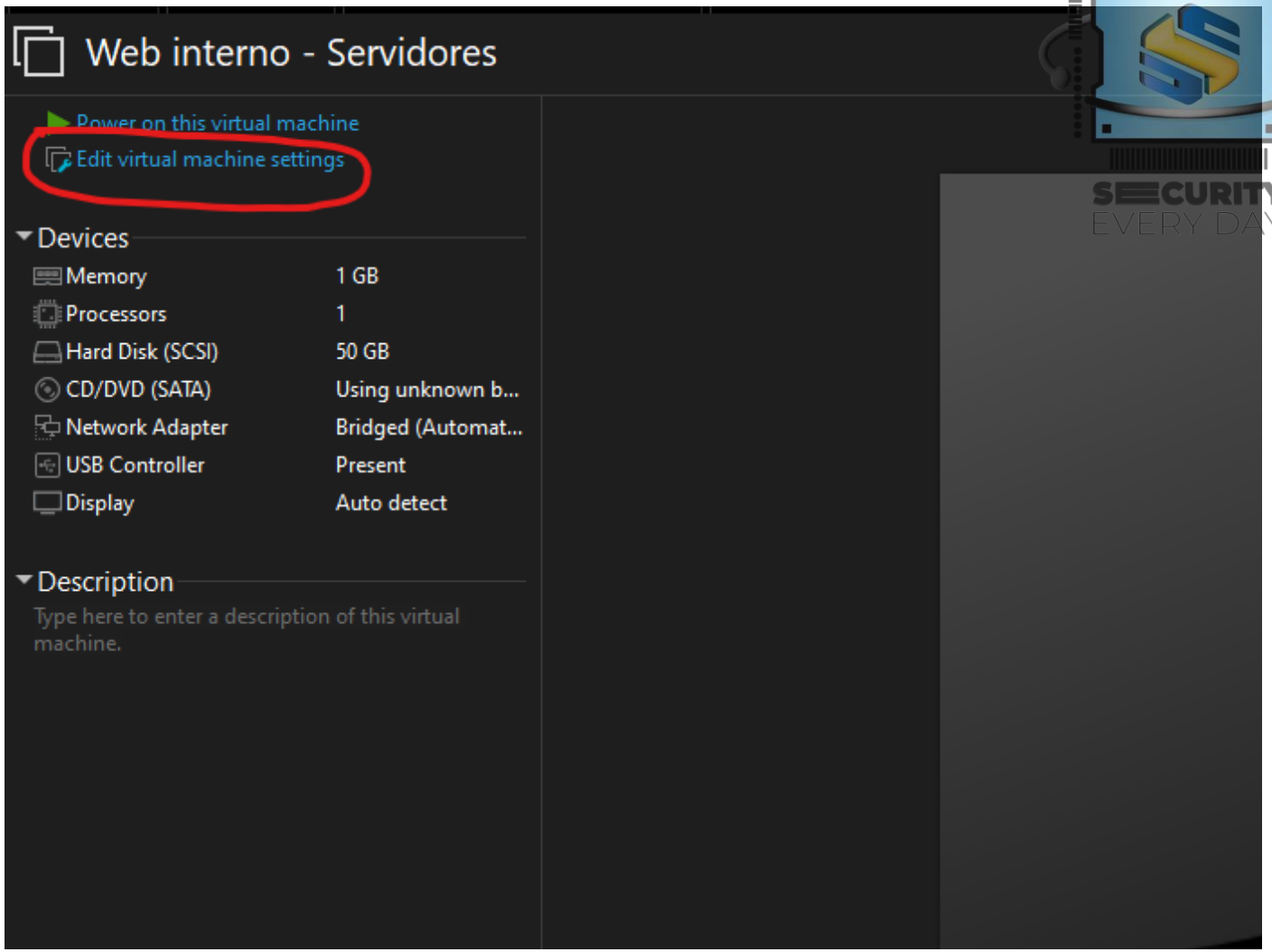
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



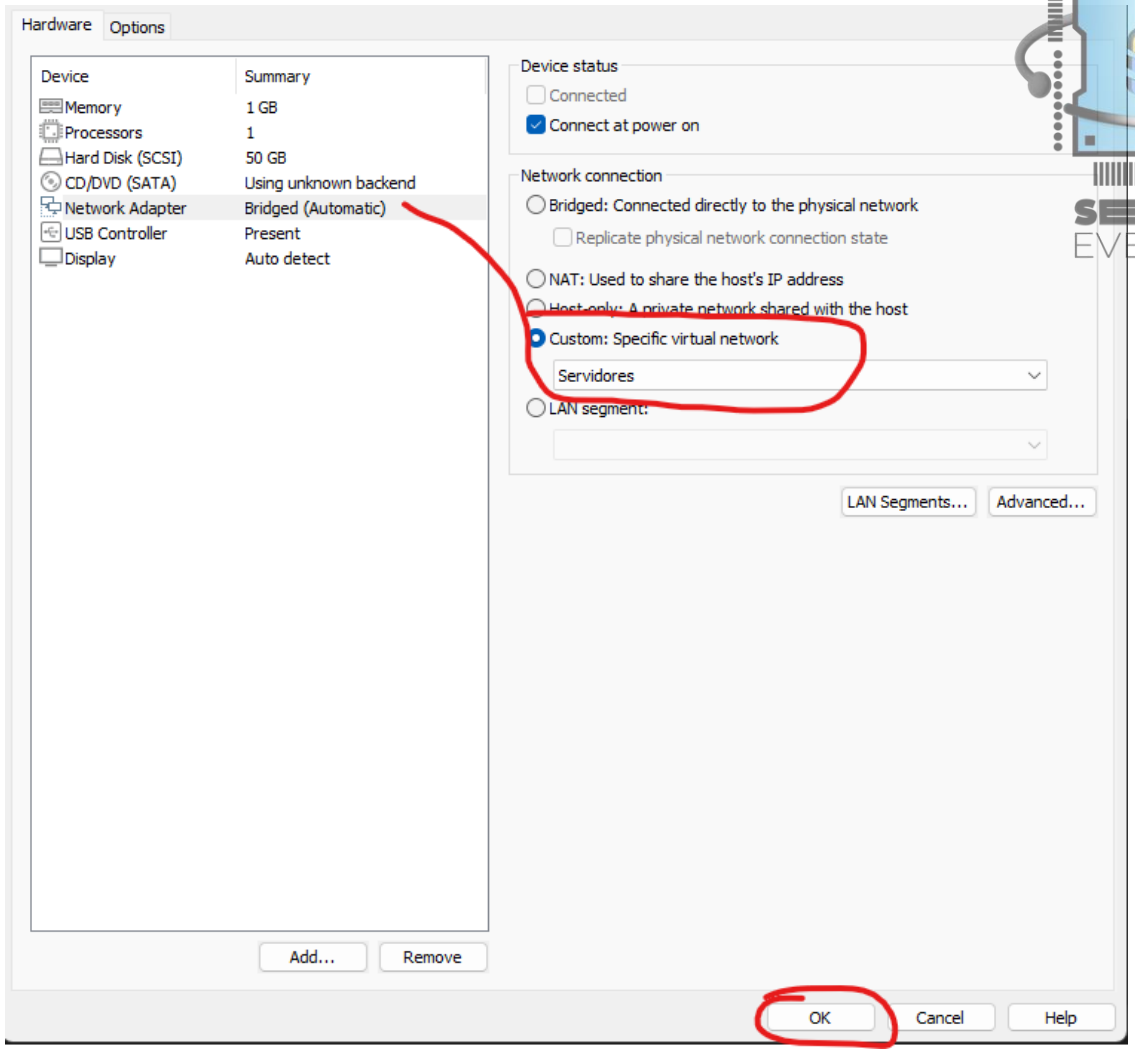
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



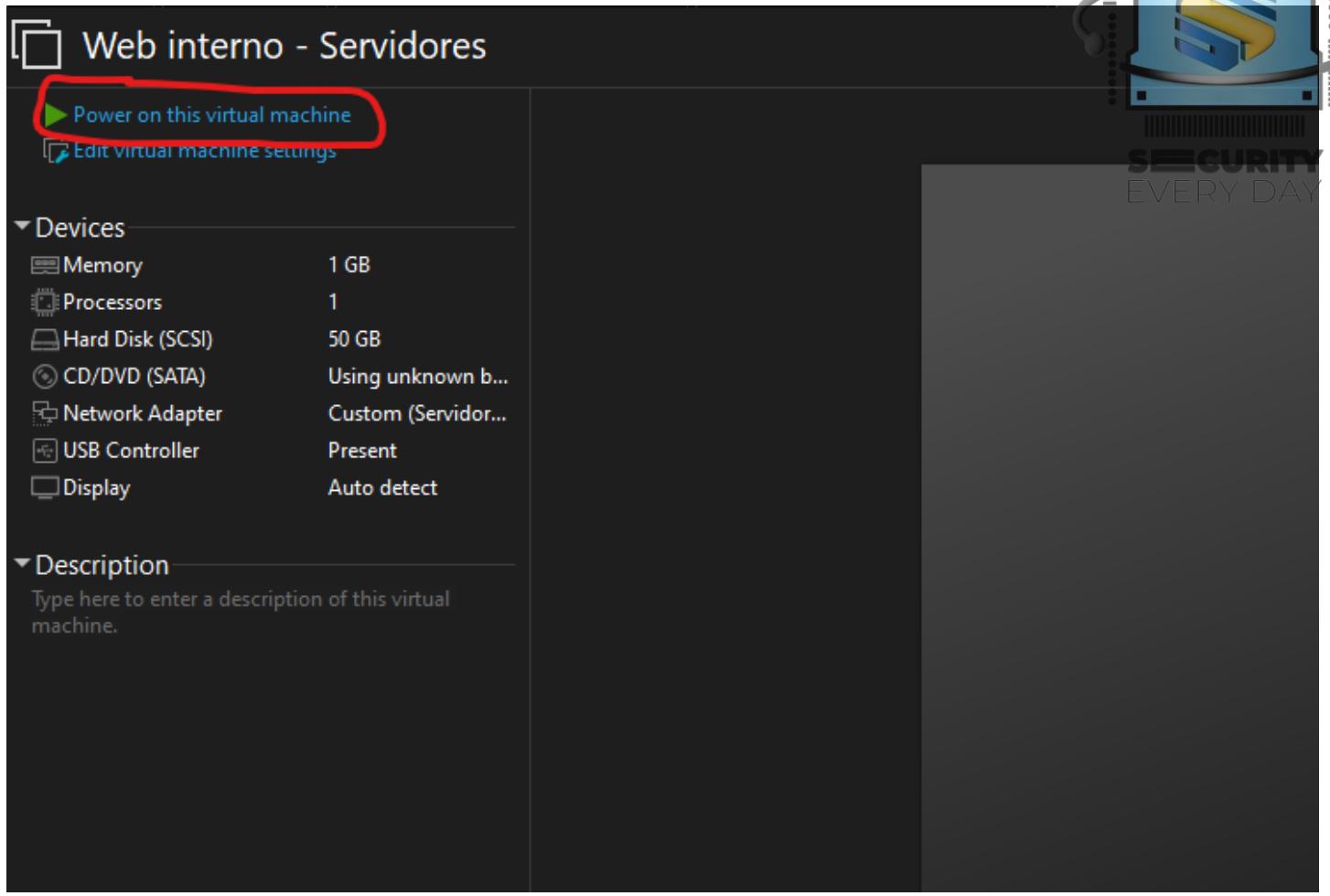
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



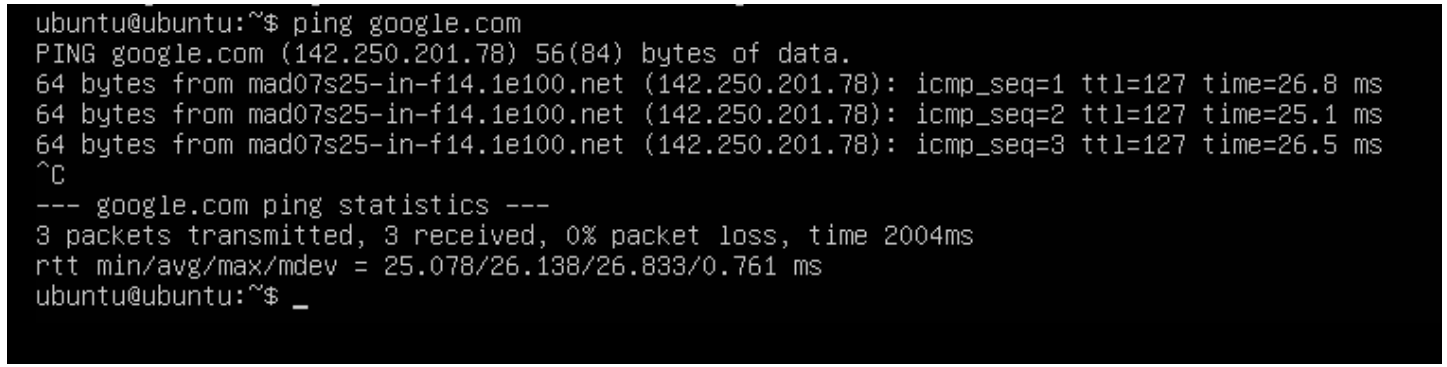
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



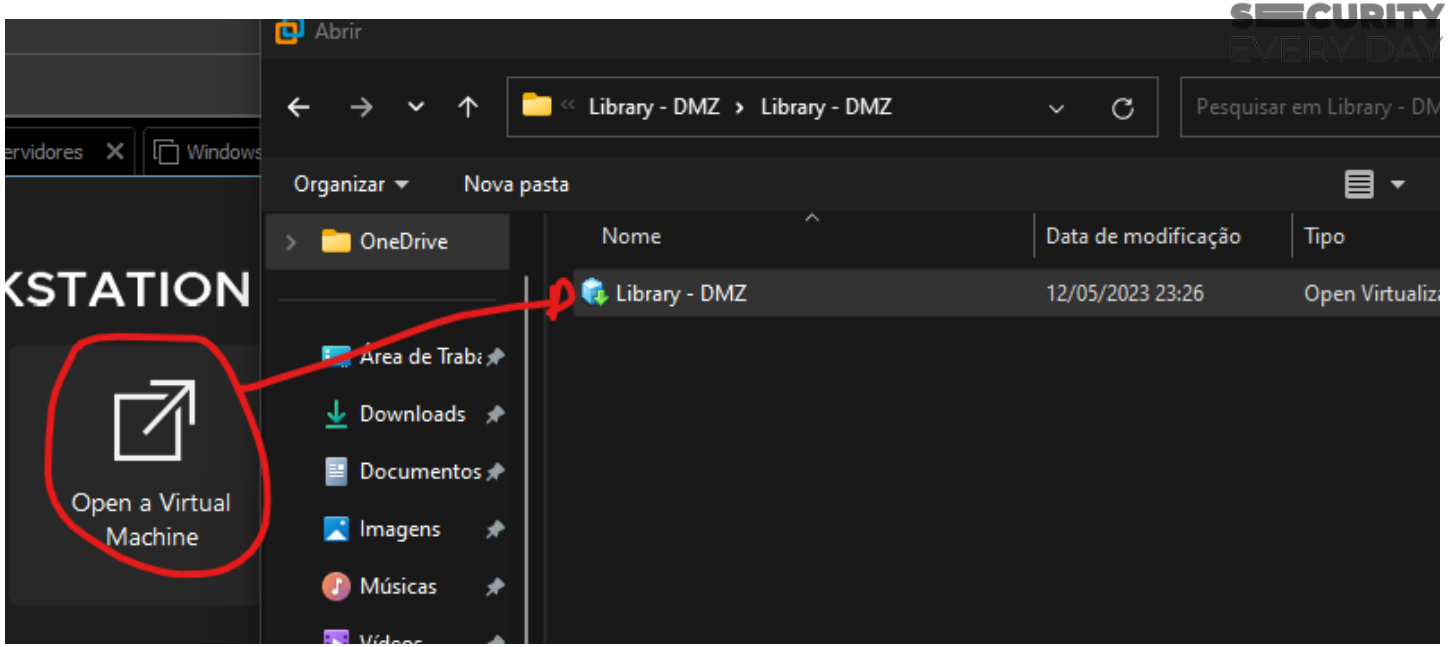
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno – Servidores
- Entre com o usuário "ubuntu" senha "ubuntu" e execute um "ping google.com", se a conexão foi estabelecida com sucesso, significa que tudo deu certo



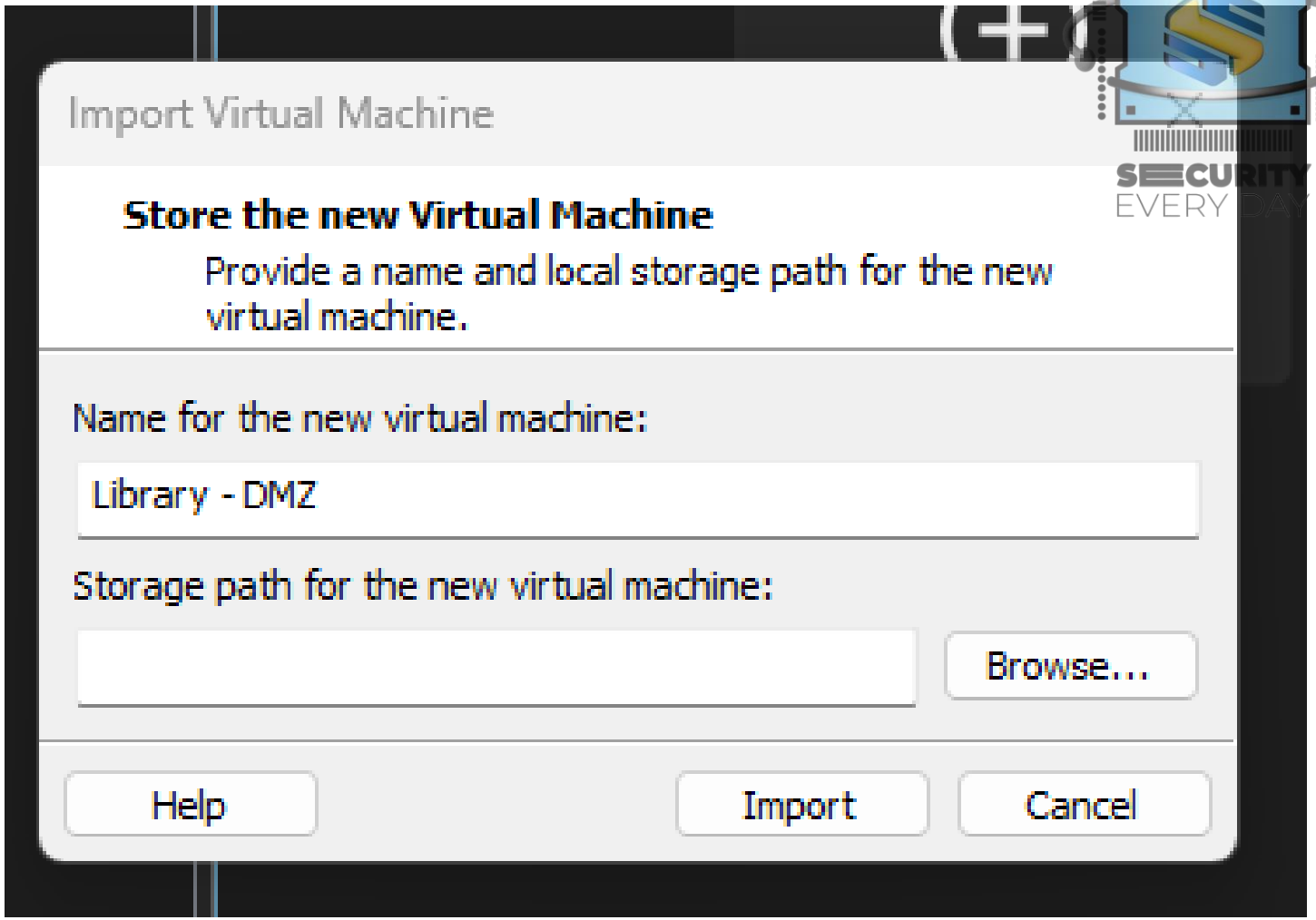
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



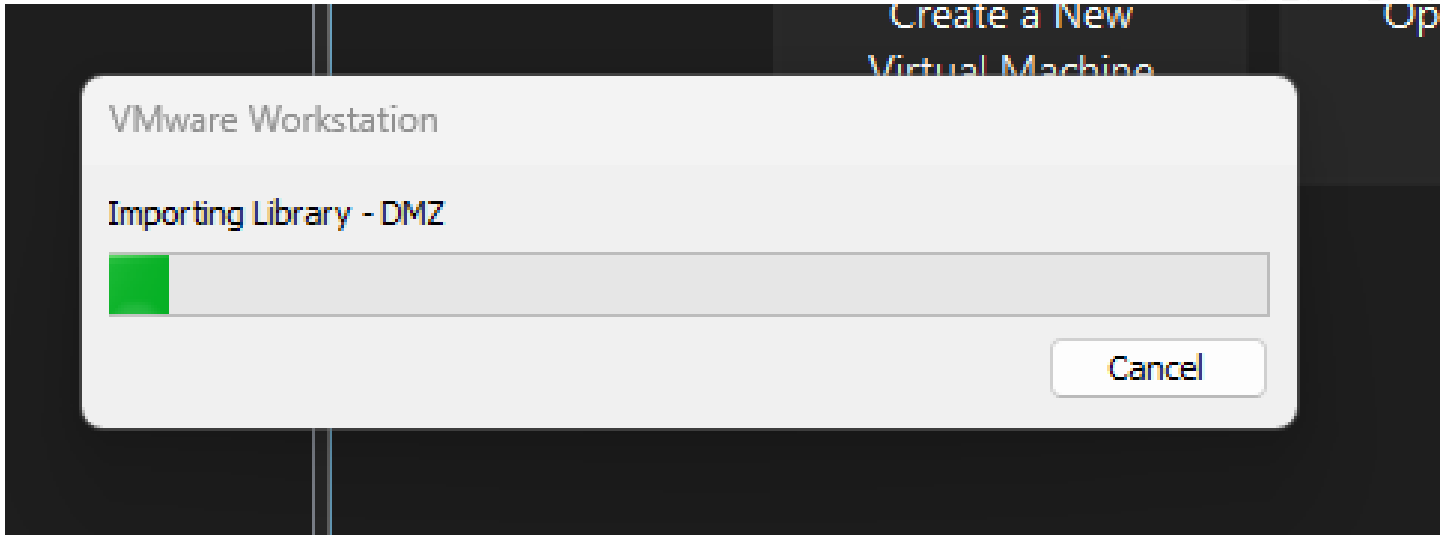
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



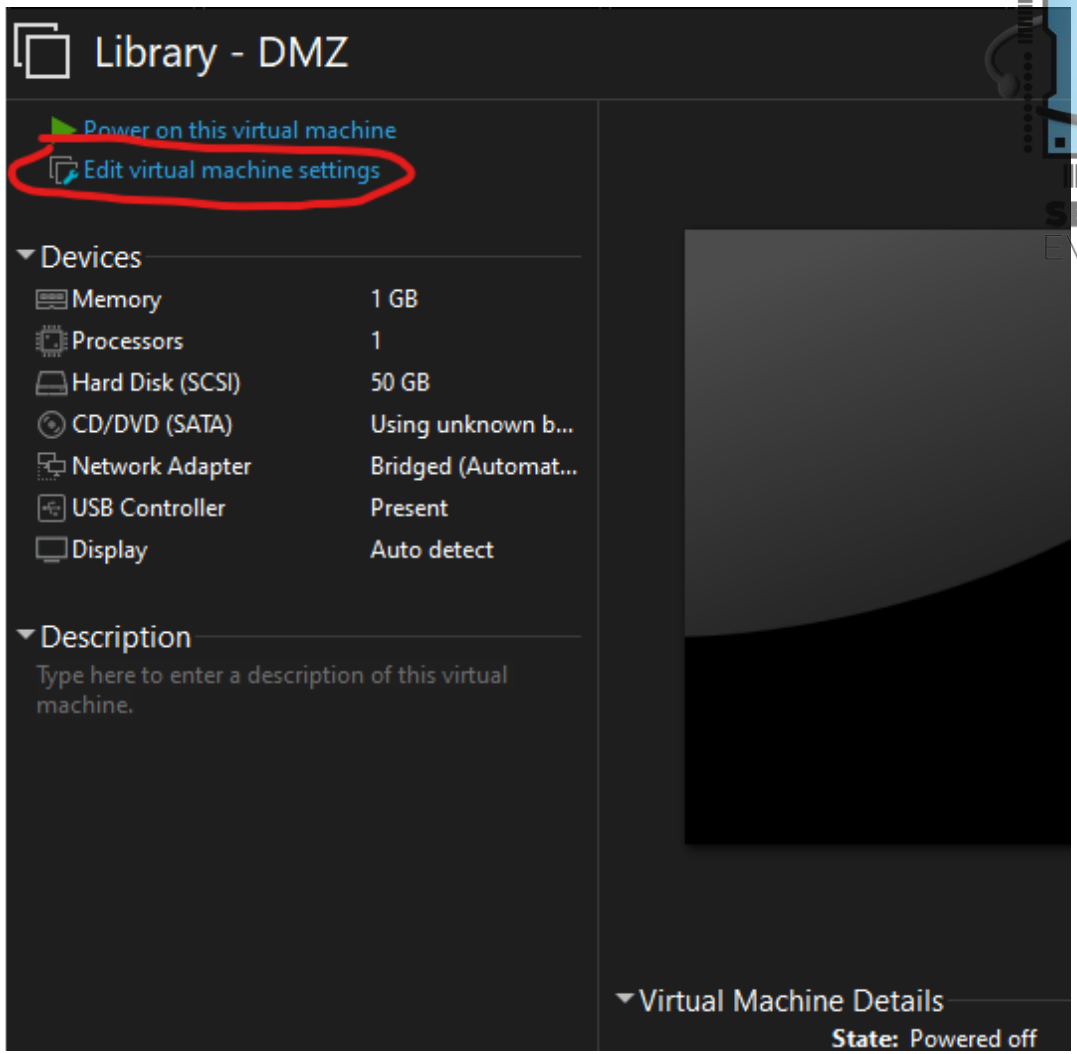
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



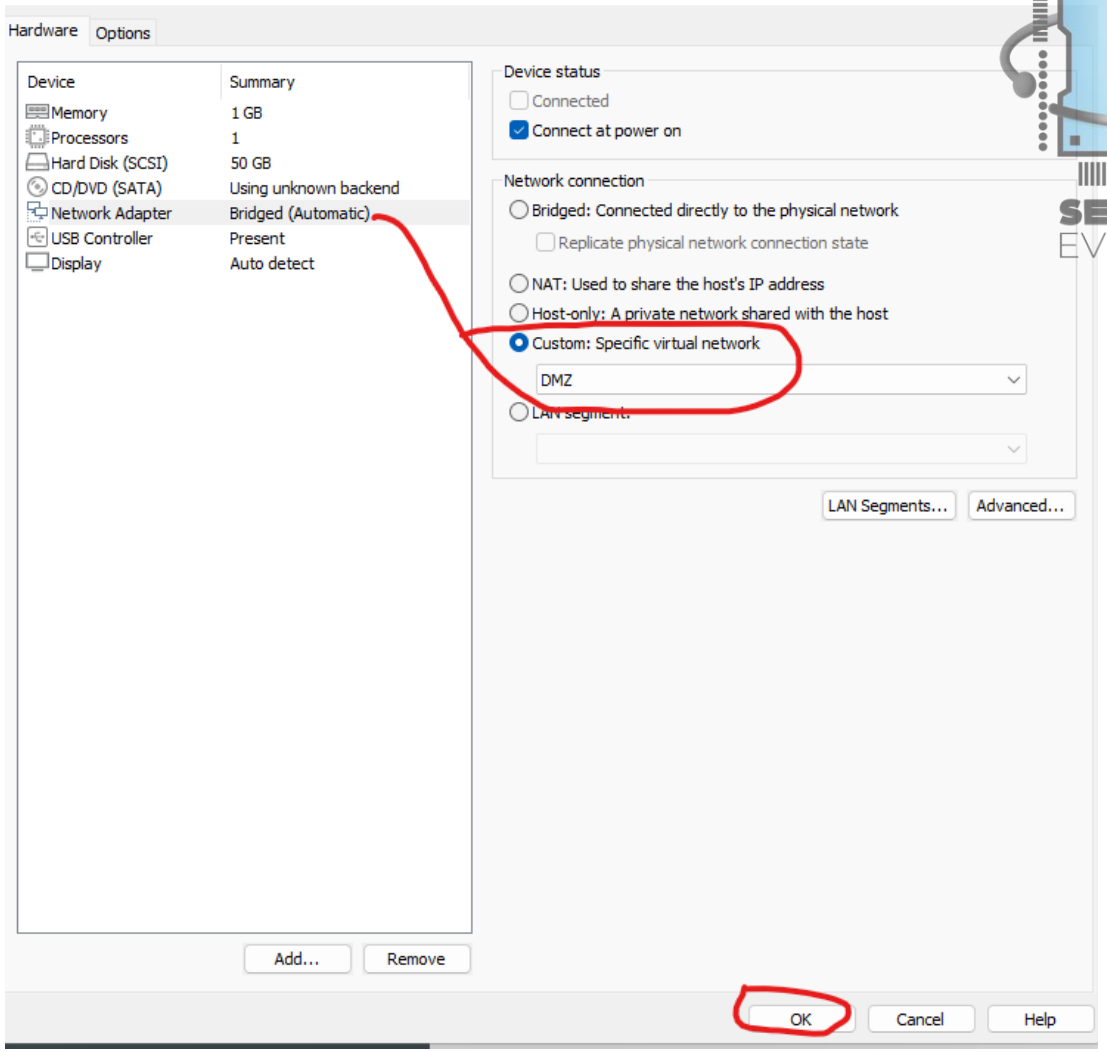
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

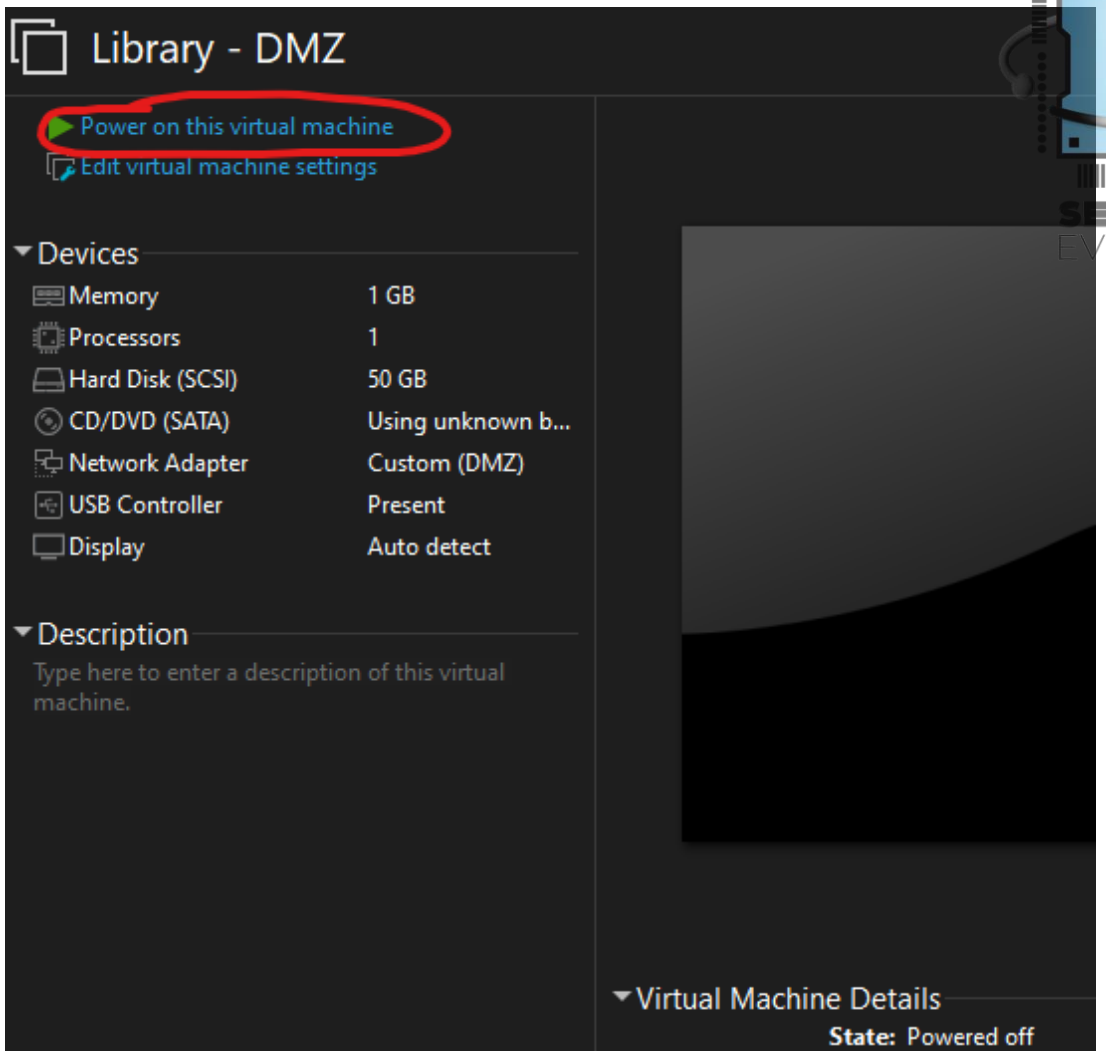
- Library - DMZ



SECURITY EVERY DAY

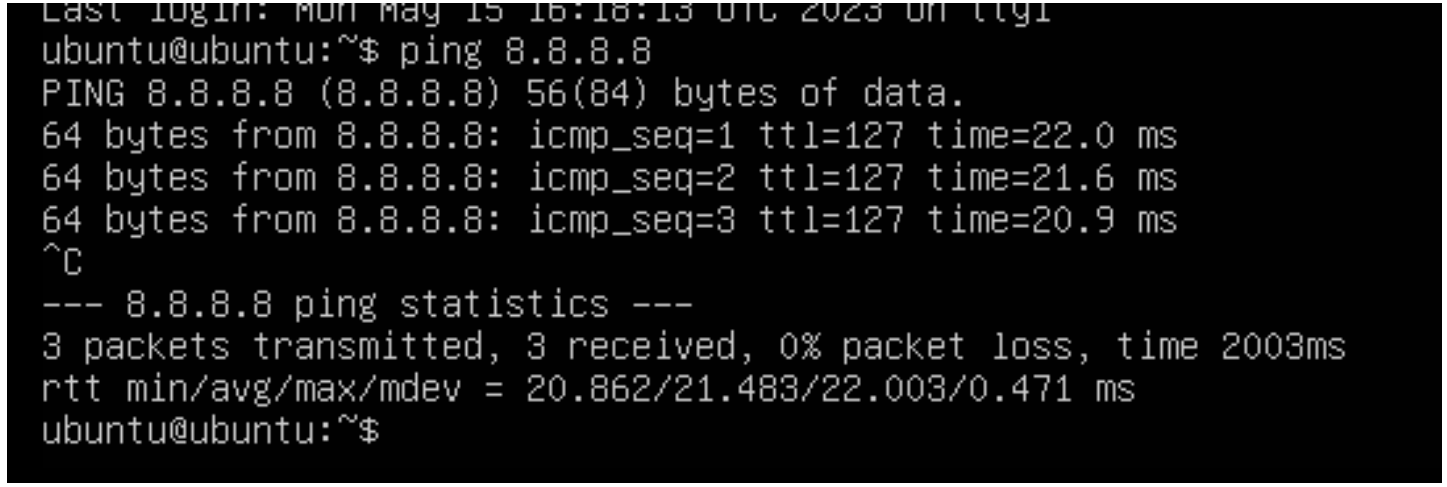
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ

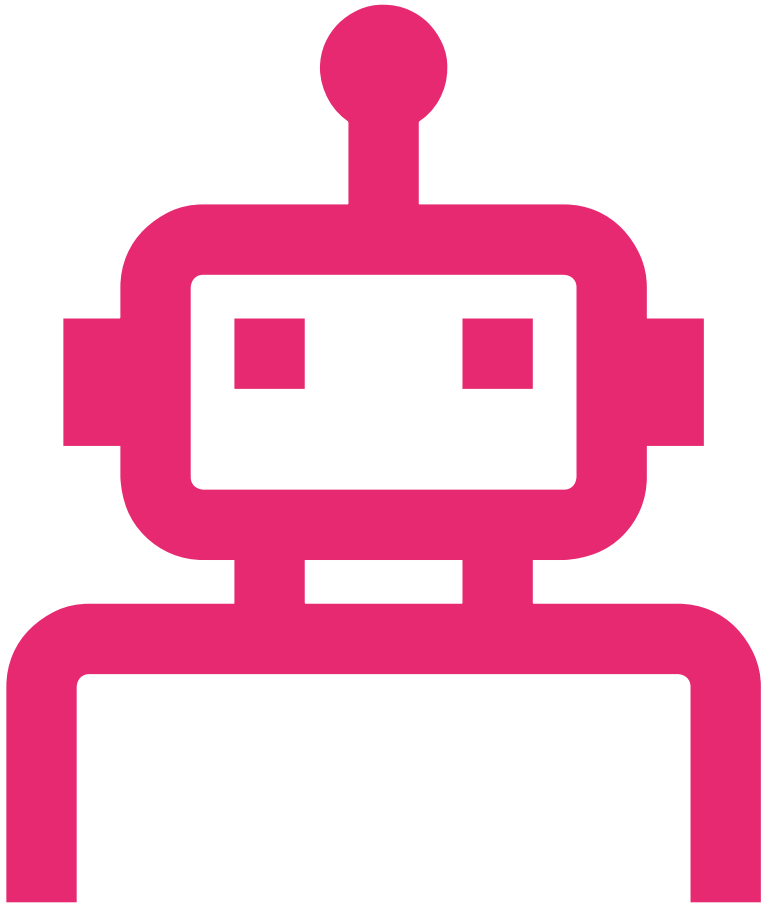


IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library – DMZ
- Entre com o usuário "ubuntu" senha "ubuntu " e execute um "ping 8.8.8.8", se a conexão foi estabelecida com sucesso, significa que tudo deu certo



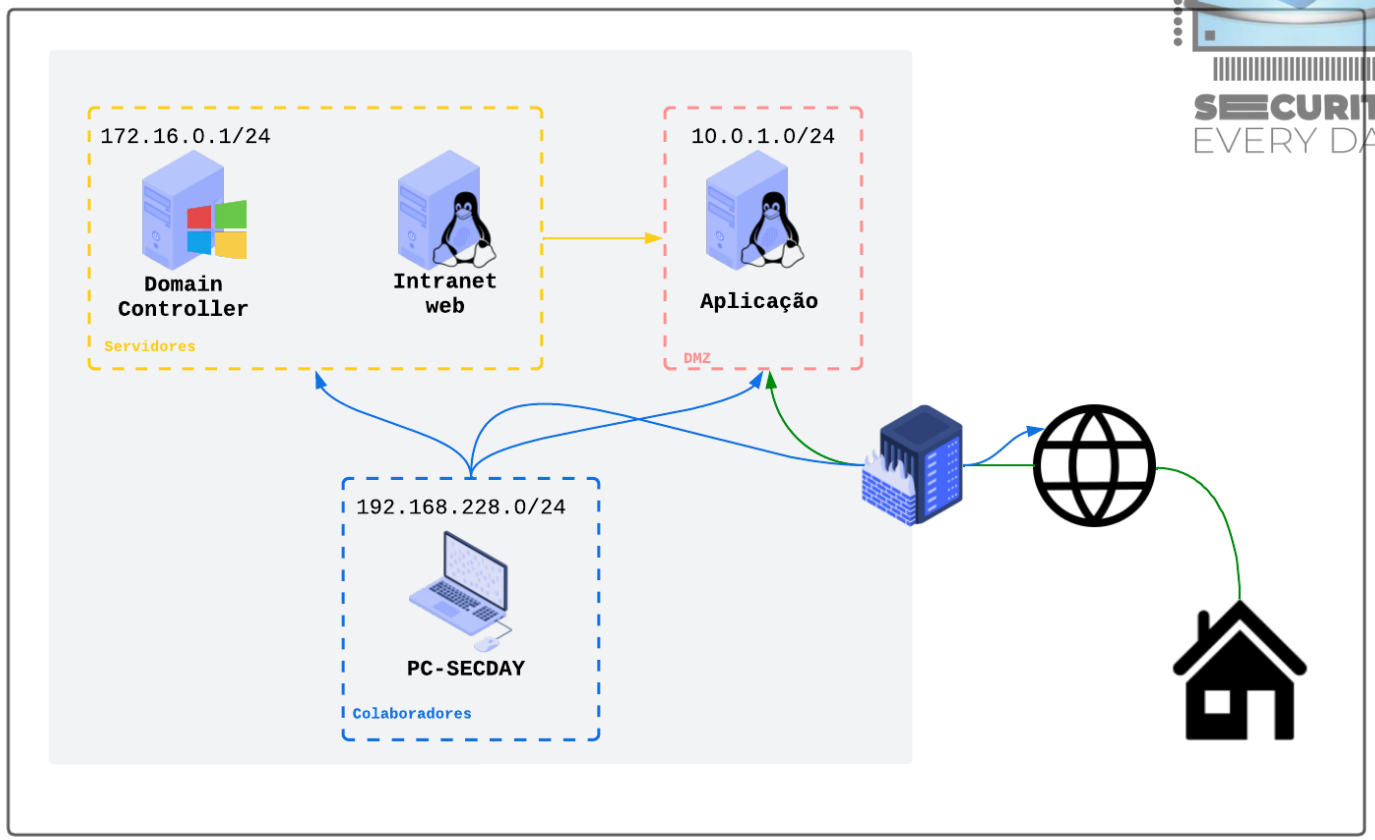
TUDO PRONTO! AMBIENTE CONFIGURADO, VAMOS POR A MÃO NA MASSA?



SECURITY EVERY DAY

REDE DO LABORATÓRIO

- Firewall
  - 172.16.0.1 (Servidores)
  - 192.168.228.1 (Colaboradores)
  - 10.0.1.1 (DMZ)
  - 192.168.126.139 (WAN)
  - User: Admin
  - Pass: secday
- Domain Controller
  - 172.16.0.5 (Servidores)
  - User: Administrator
  - Pass: Admin@mudar
- Intranet Web (Web interno)
  - 172.16.0.60 (Servidores)
  - User: ubuntu
  - Pass: ubuntu
- Aplicação
  - 10.0.1.101 (DMZ)
  - User: ubuntu
  - Pass: ubuntu
- PC-SECDAY
  - 192.168.228.100 (Colaboradores)
  - User: user-secday
  - Pass: Admin@mudar



ESTRATÉGIAS DE MONITORAMENTO

Identificação das Joias da Coroa

Instalação do SIEM

Coleta dos logs

- Configuração do NTP
- Logs da aplicação exposta para internet
- Logs do Firewall
- Logs da aplicação da Web da intranet
- Controlador de Domínio
- Logs de endpoints

Exercício de Purple team

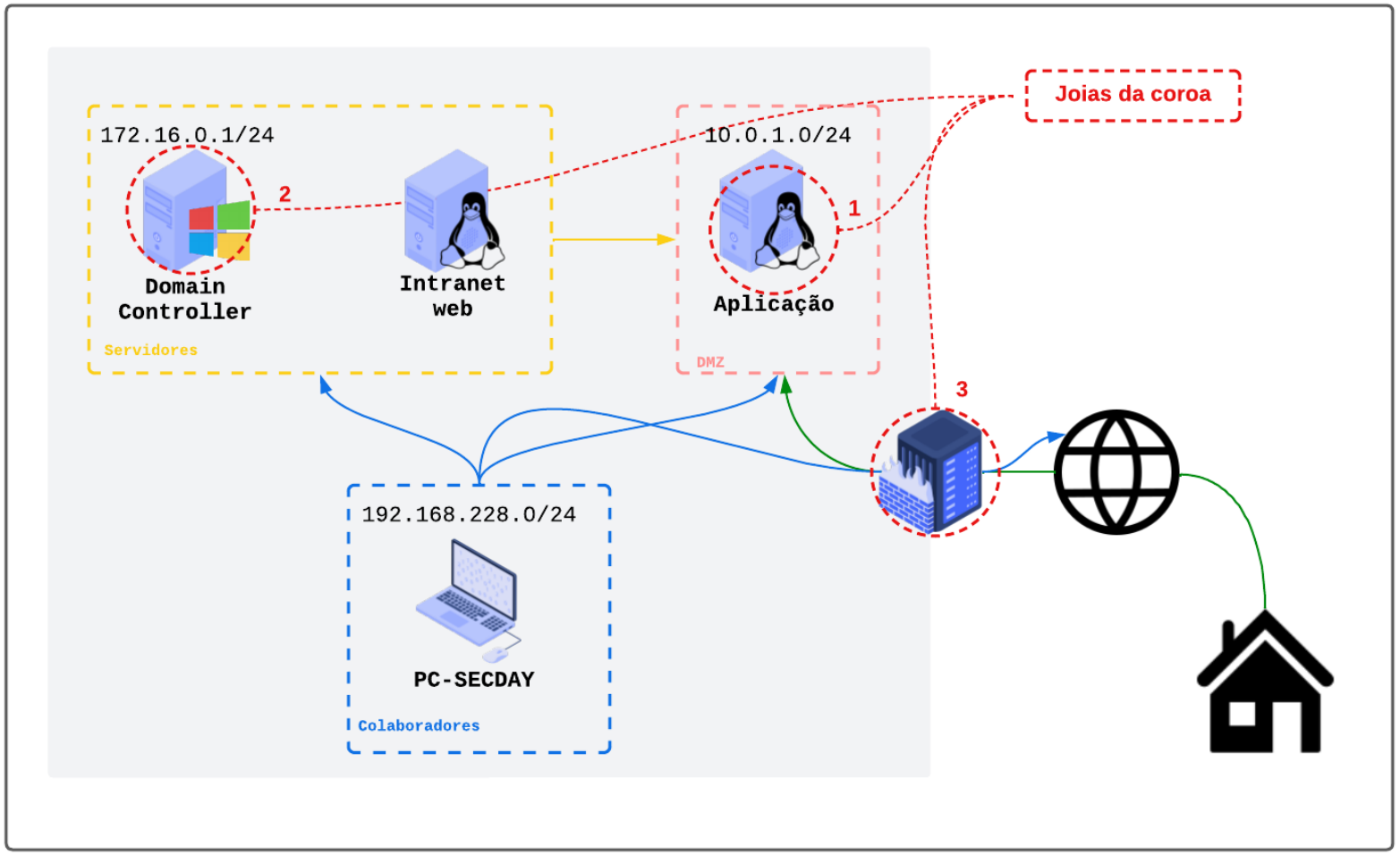
- Realização de ataques
- Criação de regras
- Teste de efetividade

IDENTIFICAÇÃO DAS JOIAS DA COROA

O QUE SÃO “JOIAS DA COROA”?

EXEMPLOS DE “JOIAS DA COROA”

- Aplicação exposta para internet
- Controlador de domínio
- Bancos de dados de clientes
- Propriedade intelectual
- Servidores de email corporativos
- Sistemas de Recursos Humanos



JOIAS DA COROA - SECDAY

SIEM

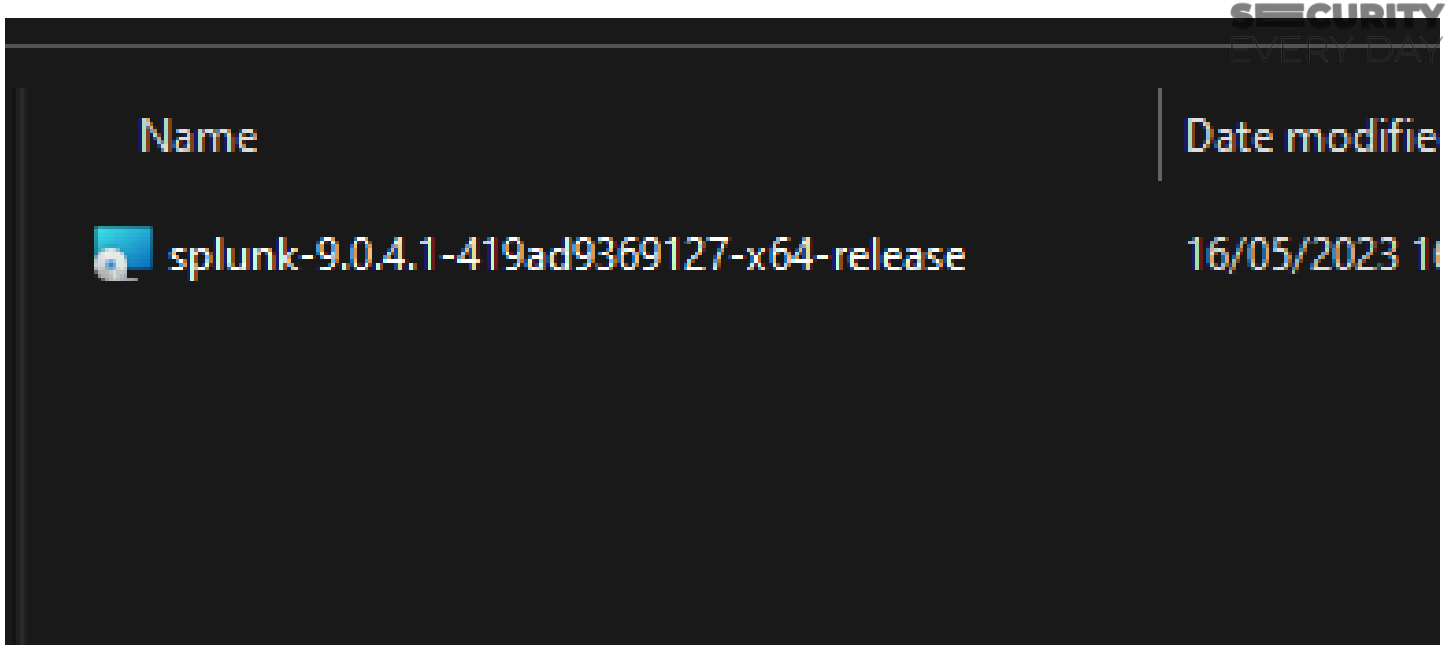
- Utilizaremos o Splunk como nosso SIEM, instalando-o na máquina host em vez de uma VM, para evitar o consumo desnecessário de recursos com várias máquinas virtuais

INSTALAÇÃO DO SIEM

- Link para o download do Splunk (Windows)
  - https://download.splunk.com/products/splunk/releases/9.0.4.1/windows/splunk-9.0.4.1-419ad9369127-x64-release.msi

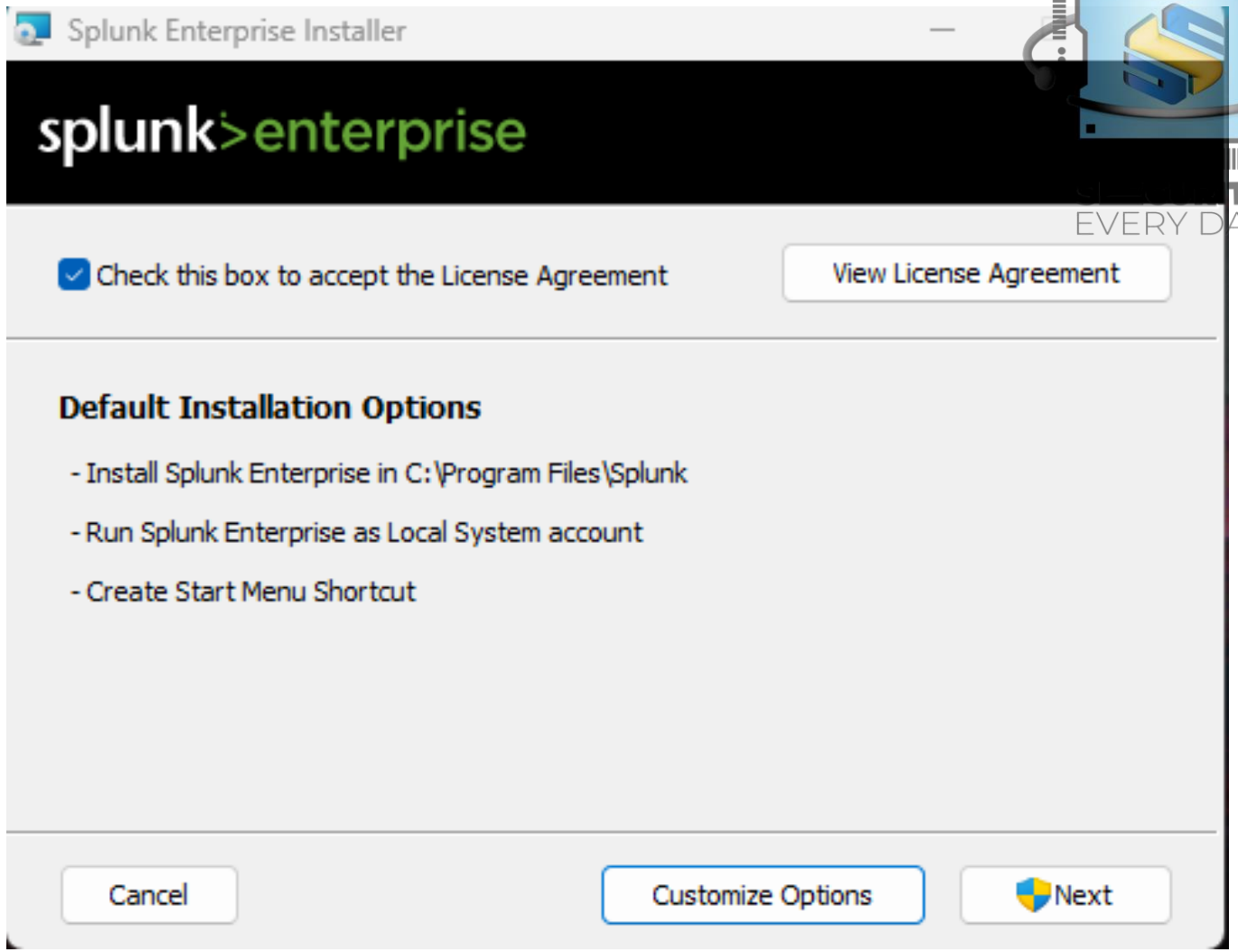
INSTALAÇÃO DO SIEM

- Para iniciar a instalação, clique 2x sobre o arquivo de instalação do Splunk



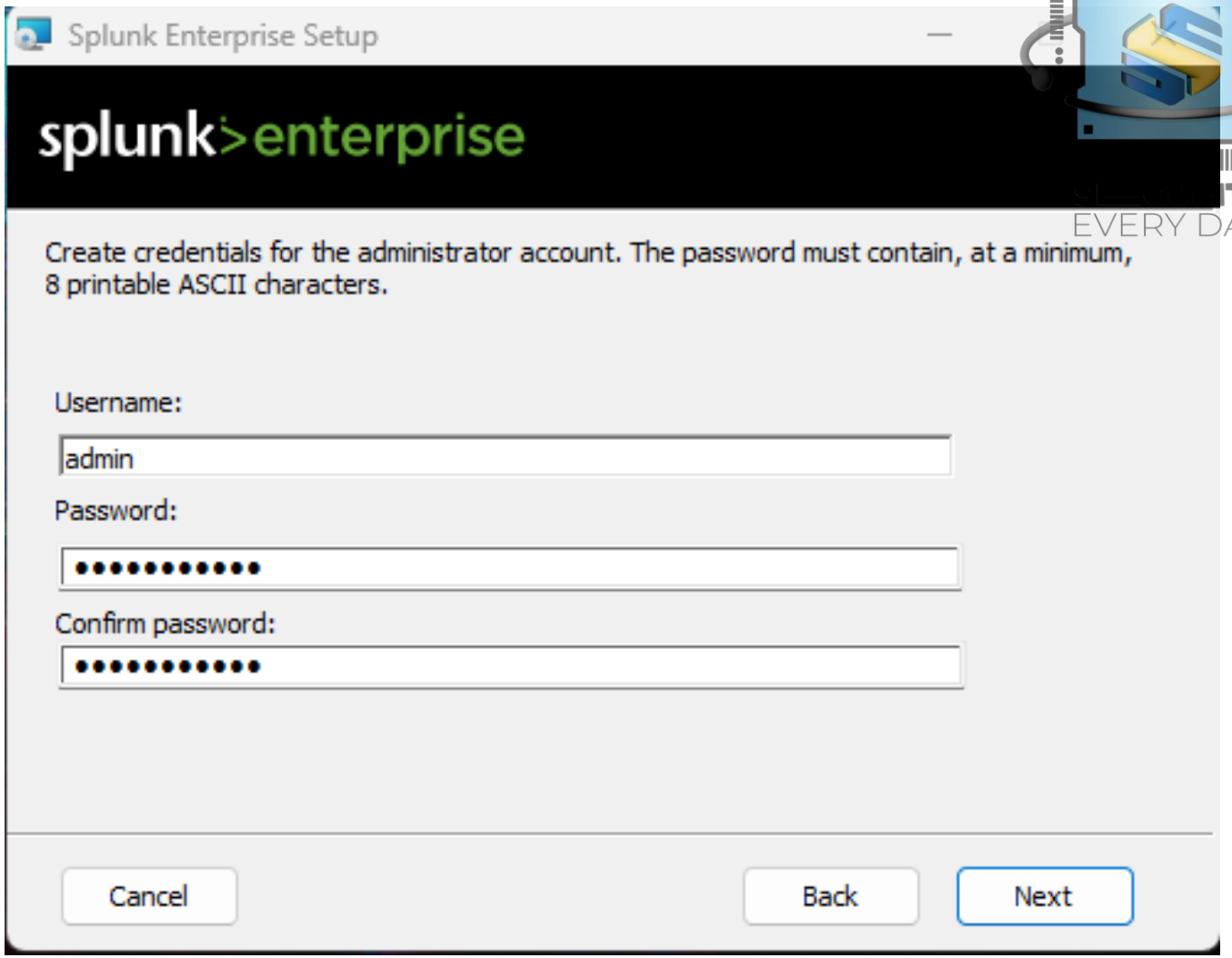
INSTALAÇÃO DO SIEM

- Marque o “Check” para aceitar a licença e clique em “Next”



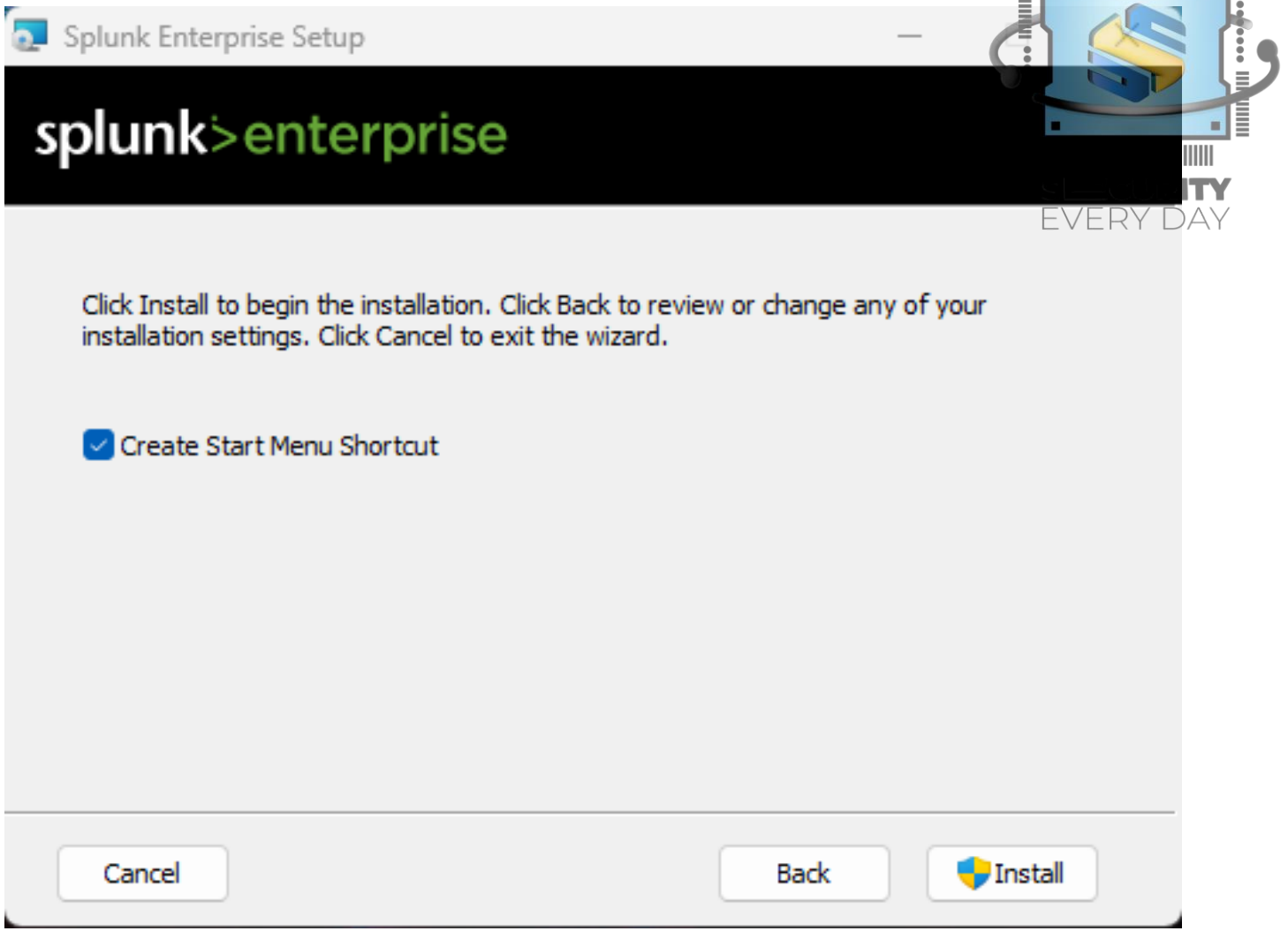
INSTALAÇÃO DO SIEM

- Defina um usuário e senha para acesso ao Splunk e clique em “Next”



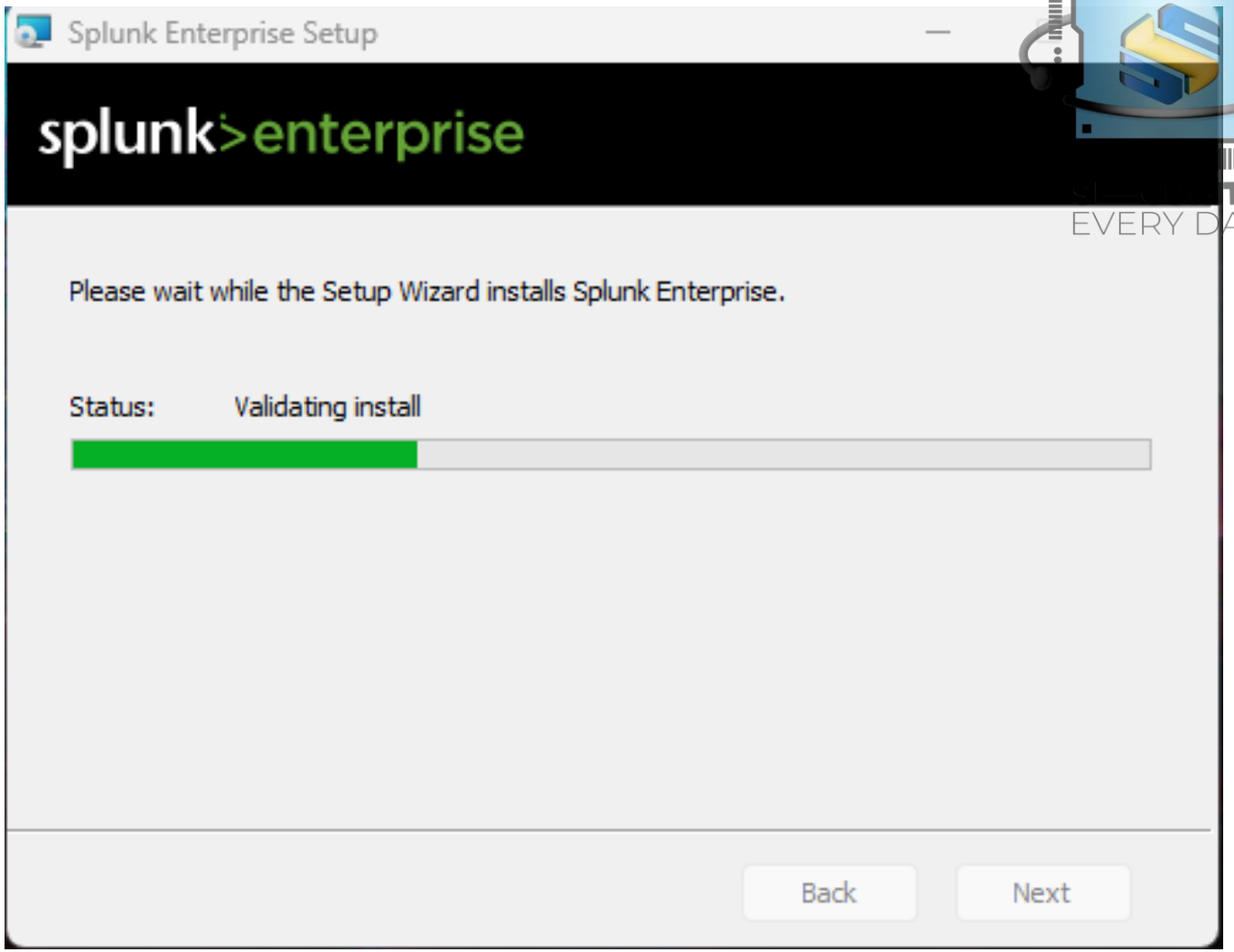
INSTALAÇÃO DO SIEM

- Clique em “Install”



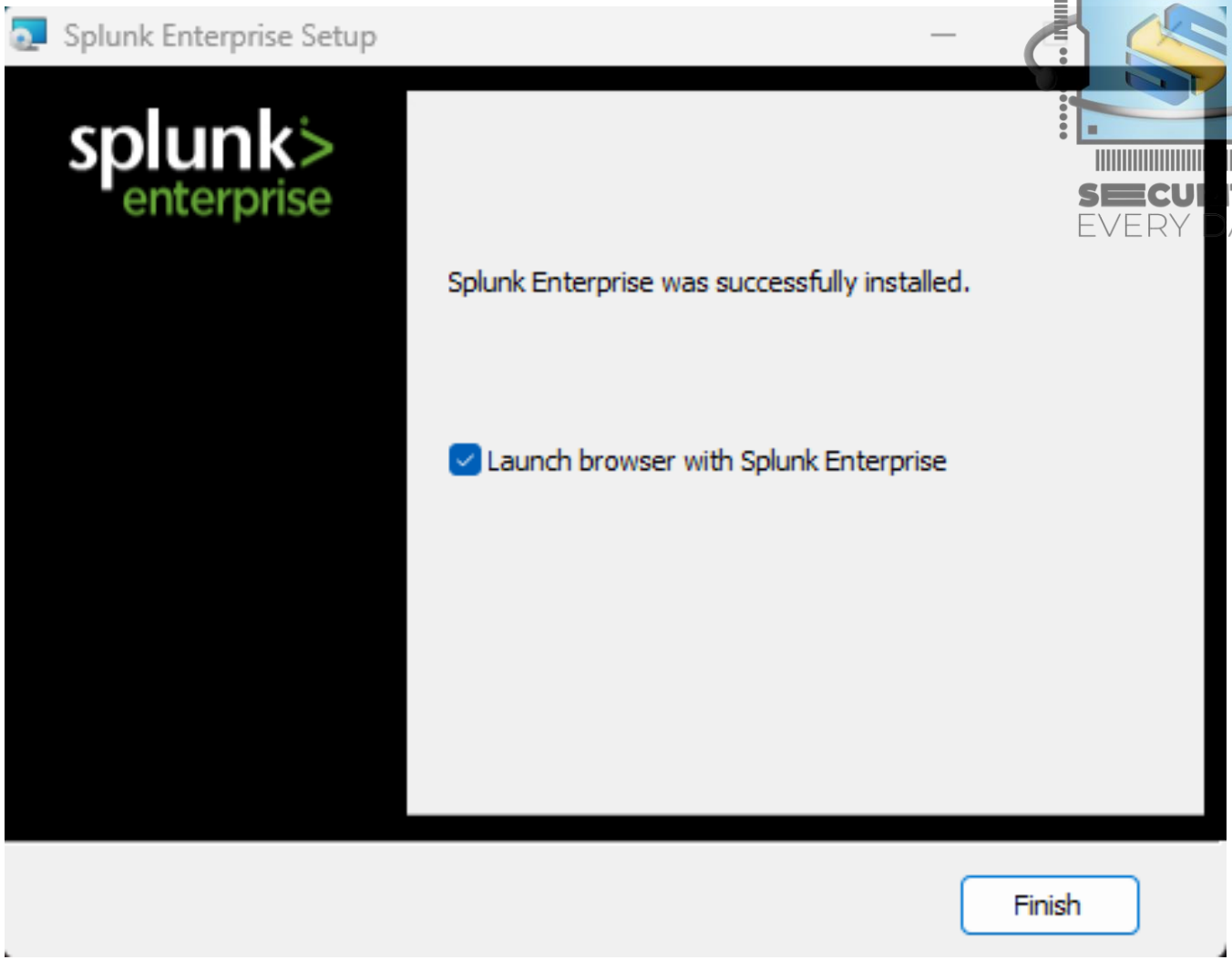
INSTALAÇÃO DO SIEM

- Aguarde até que a instalação seja finalizada e clique em “Finish”



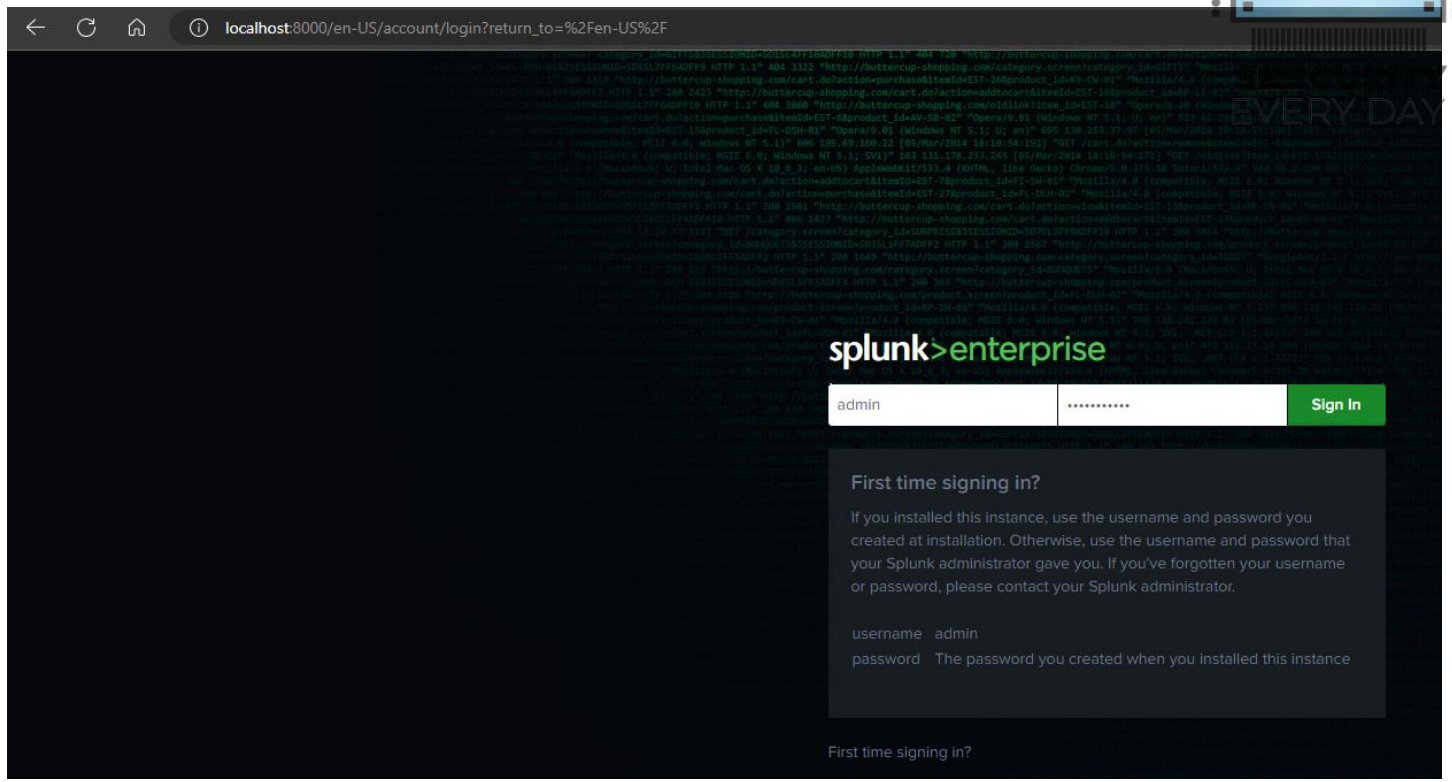
INSTALAÇÃO DO SIEM

- Aguarde até que a instalação seja finalizada e clique em “Finish”



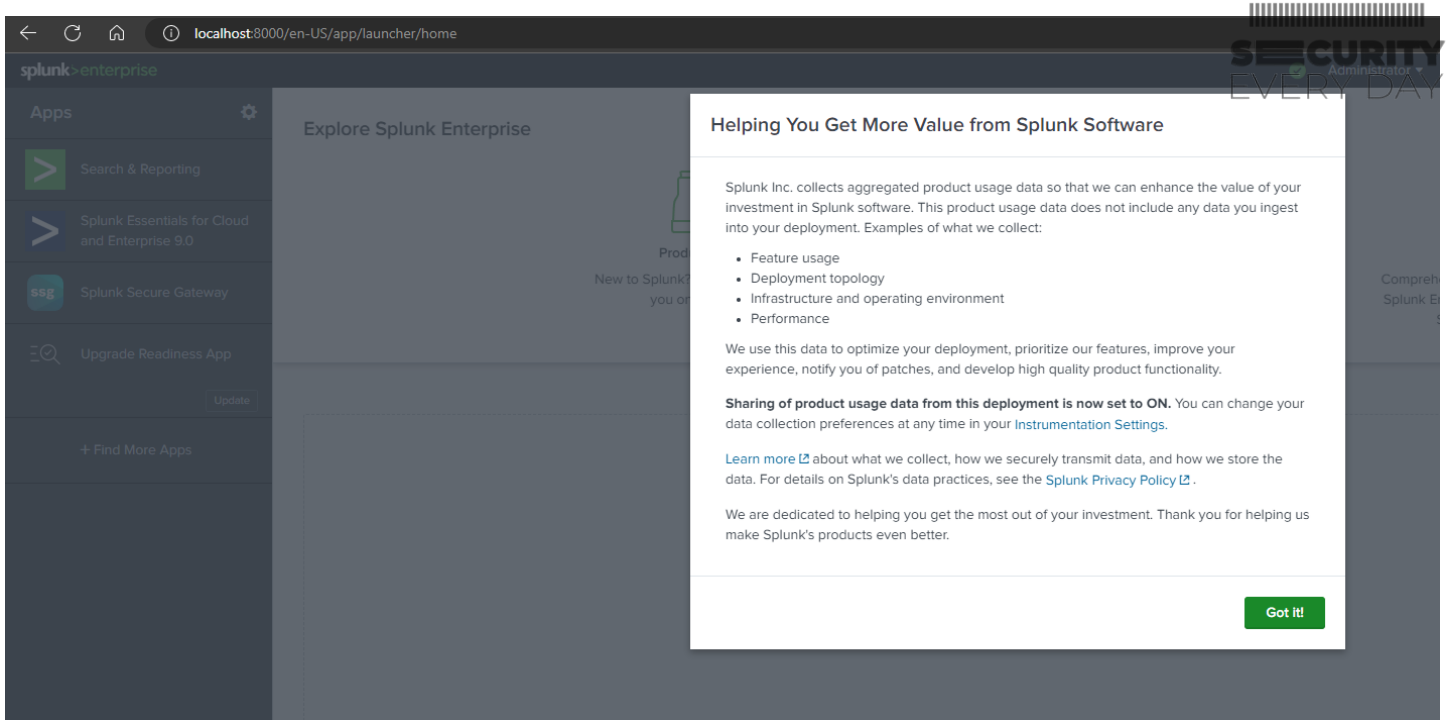
INSTALAÇÃO DO SIEM

- Agora, se você acessar seu navegador em http://localhost:8000/ , deverá conseguir acessar o aplicativo web Splunk, digite o nome de usuário e a senha definidos na instalação e clique em “Entrar”



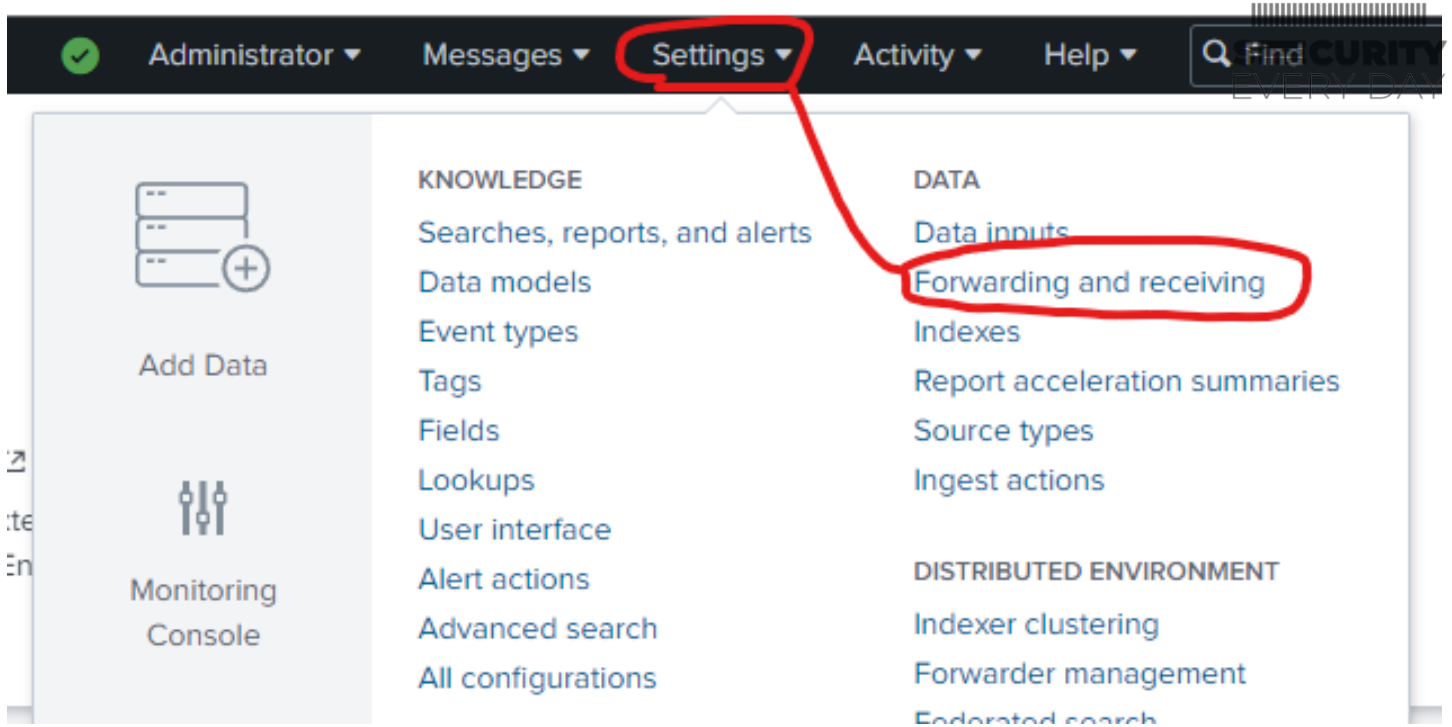
INSTALAÇÃO DO SIEM

- Clique em “Got it!”



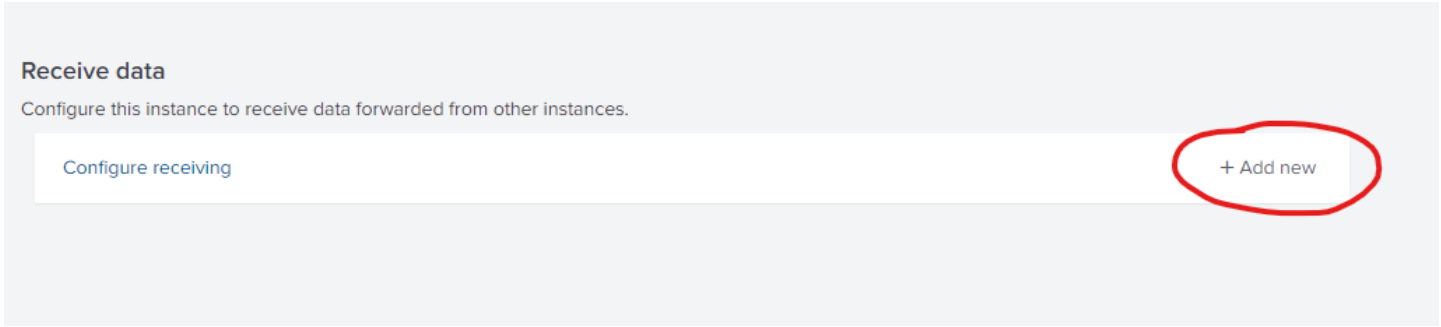
INSTALAÇÃO DO SIEM

- Agora, vamos abrir a porta do Splunk, para que ele possa se comunicar com o agente Splunk, clique em “Settings” e depois em “Forwarding and receiving”



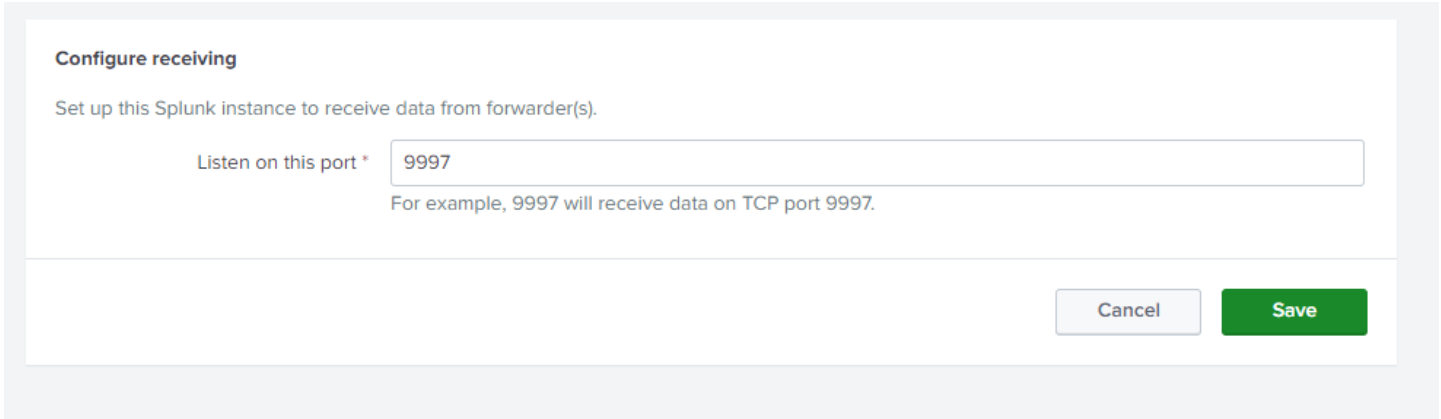
INSTALAÇÃO DO SIEM

- Em “Receive data”, clique em “+ Add new” e vamos configurar a porta 9997



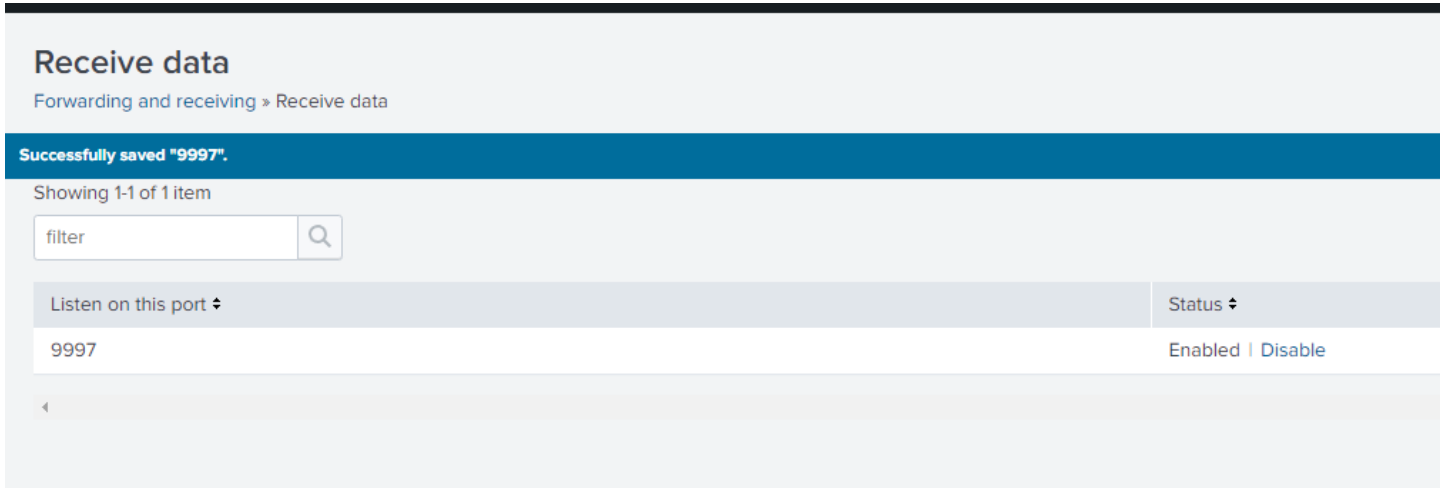
INSTALAÇÃO DO SIEM

- Clique em “Save”



INSTALAÇÃO DO SIEM

- Pronto, porta configurada



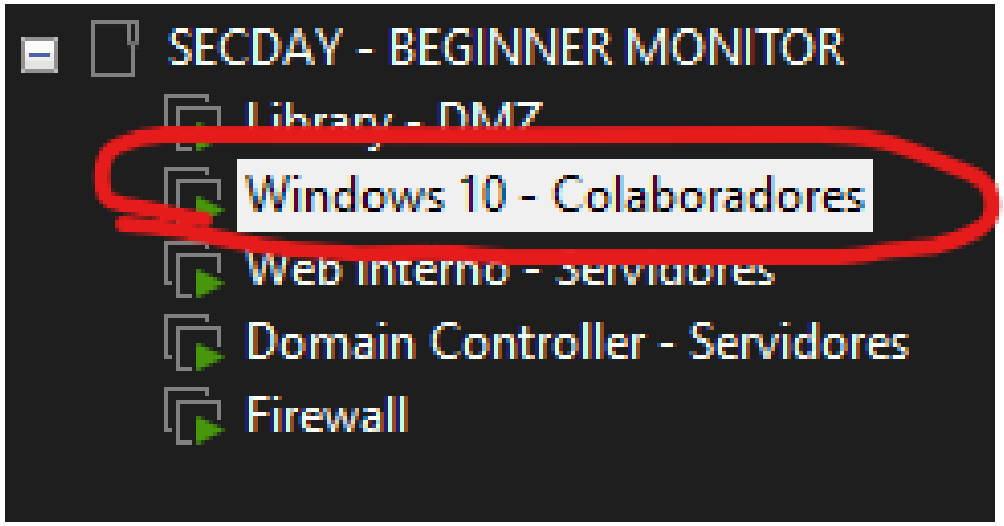
COLETA DE LOGS

CONFIGURAÇÃO DO SERVIDOR NTP

PORQUE O NTP É IMPORTANTE?

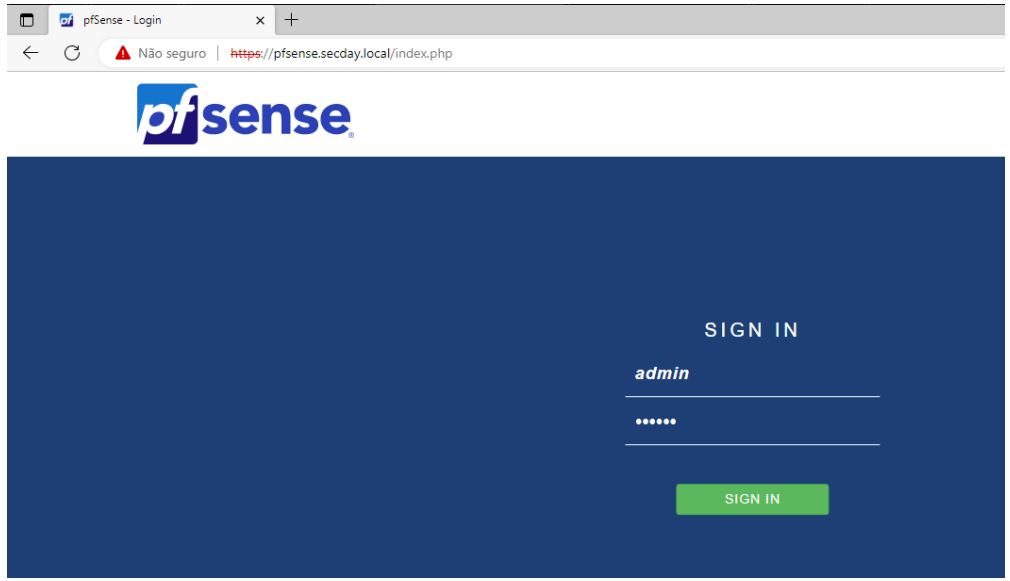
- Correlação de logs
- Análise forense
- Integridade de transações
- Etc...

CONFIGURANDO O SERVIDOR NTP



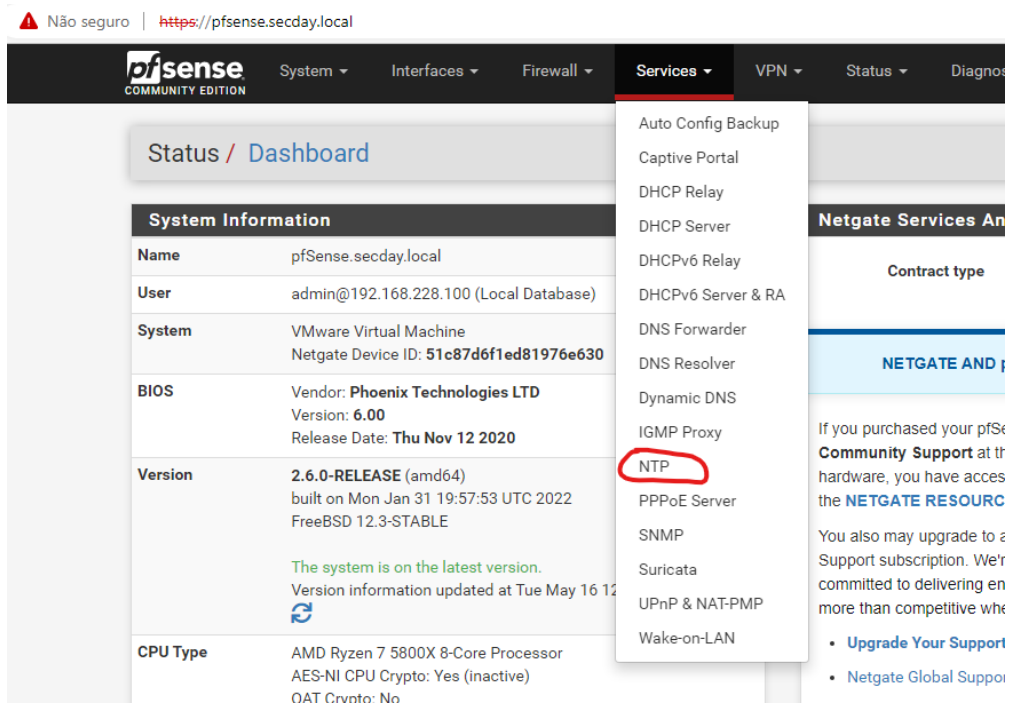
- Vamos configurar o nosso Firewall como nosso servidor NTP, para isso, precisamos acessar a maquina “Windows 10 – Colaboradores”
  - User: user-secday
  - Pass: Admin@mudar

CONFIGURANDO O SERVIDOR NTP



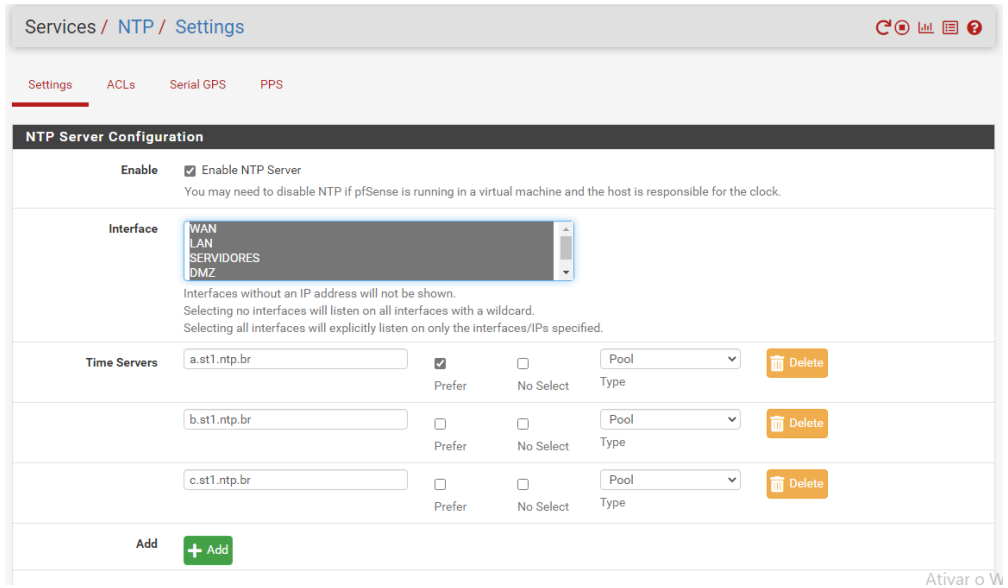
- Abra o navegador e acesse a url https://pfsense.secday.local/index.php e logue com
  - User: admin
  - Pass: secday

CONFIGURANDO O SERVIDOR NTP



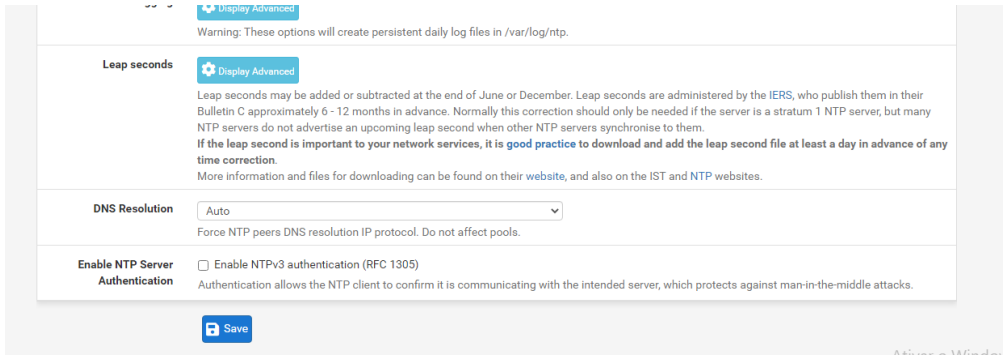
- Vá até “Services → NTP”

CONFIGURANDO O SERVIDOR NTP



- Em “Interface” selecione todas as interfaces
- Em “Time Servers”, vamos utilizer os seguintes servidores
  - a.st1.ntp.br
  - b.st1.ntp.br
  - b.st1.ntp.br
- Agora, vá até o final da pagina e clique em “Save”

CONFIGURANDO O SERVIDOR NTP

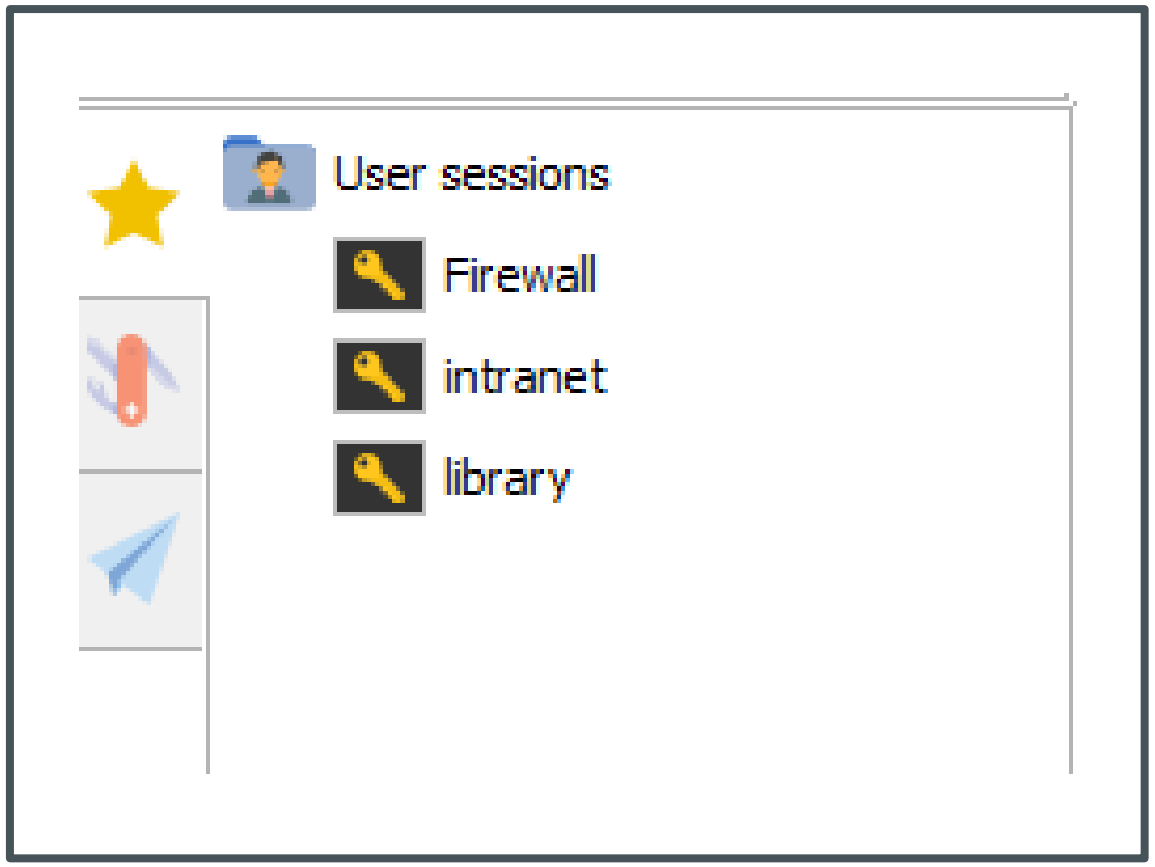


- Em “Interface” selecione todas as interfaces
- Em “Time Servers”, vamos utilizer os seguintes servidores
  - a.st1.ntp.br
  - b.st1.ntp.br
  - b.st1.ntp.br
- Agora, vá até o final da pagina e clique em “Save”

COLETA DE LOGS

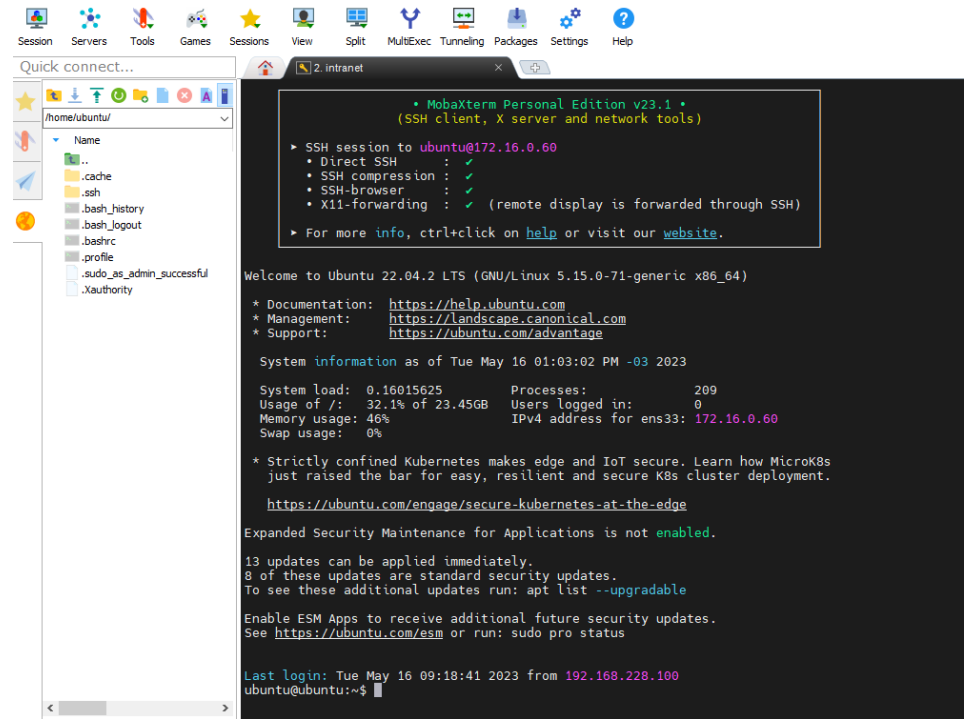
SINCRONIZAR NTP NOS SERVIDORES

SINCRONIZAR NTP NOS SERVIDORES



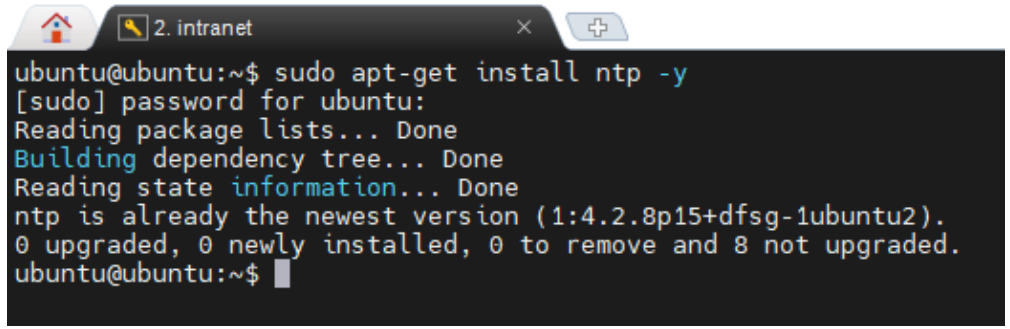
- Abra o “MobaXterm” na maquina “Windows 10 – Colaboradores” para acessarmos via SSH os servidores e configurarmos o NTP
  - Intranet (Web interno – Servidores)
  - Library (Library – DMZ)

SINCRONIZAR NTP NOS SERVIDORES



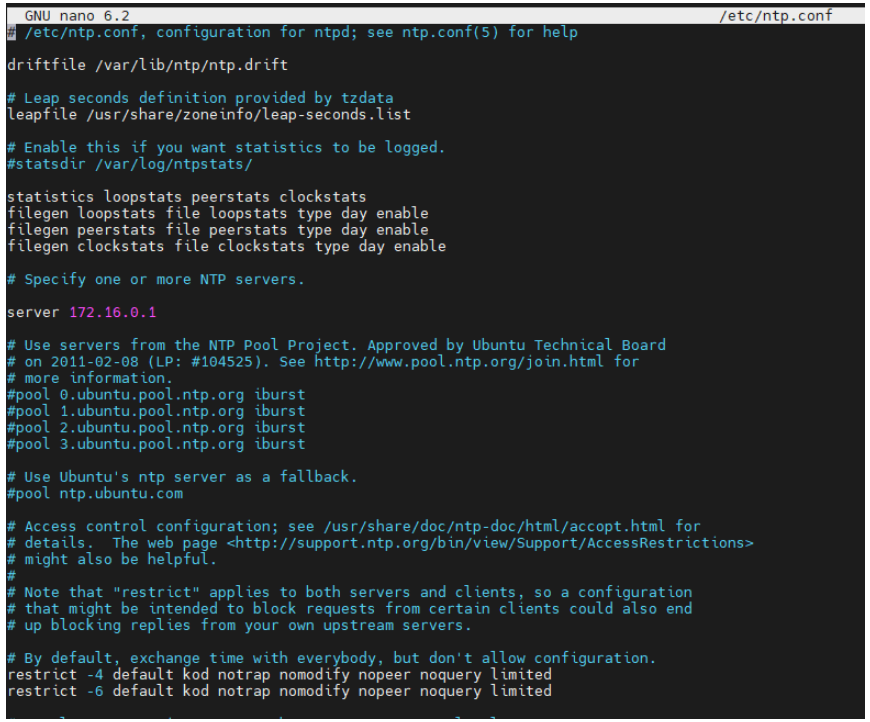
- Vamos começar pela “Intranet”, clique 2x sobre a conexão da intranet para acessar SSH
  - User: ubuntu (já configurado)
  - Pass: ubuntu

SINCRONIZAR NTP NOS SERVIDORES



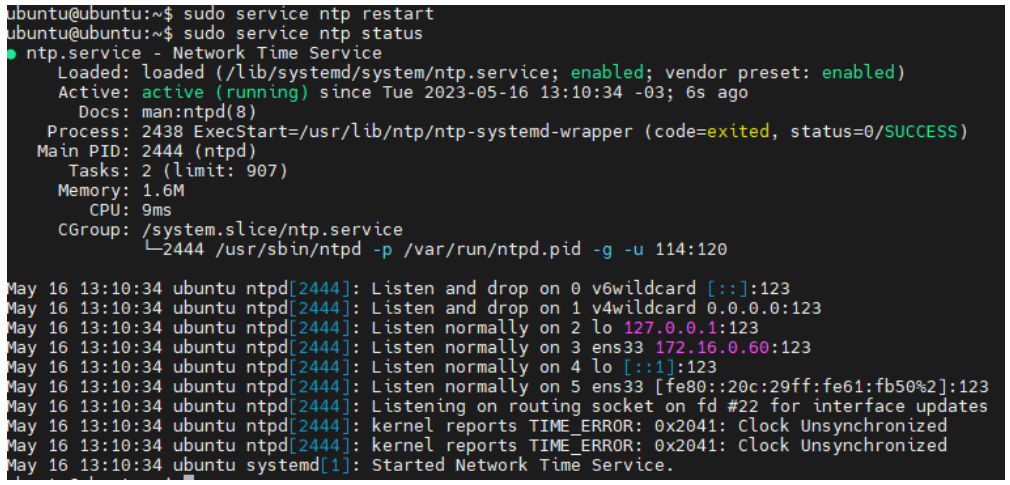
- Instale o pacote NTP com o commando
  - sudo apt-get install ntp -y

SINCRONIZAR NTP NOS SERVIDORES



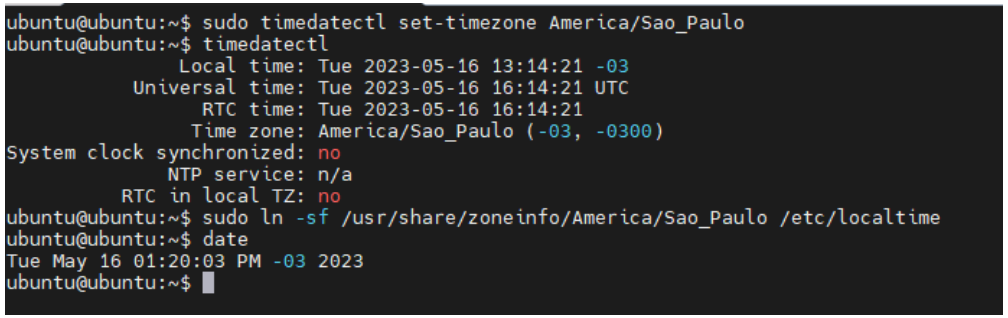
- Edite o arquivo de configuração do NTP com o seguinte comando
  - sudo nano /etc/ntp.conf
- Adicione um # no começo de cada linha que contem os servidores NTP do ubuntu (conforme a imagem)
- Adicione o endereço da interface “Servidores” do Firewall para ser o NTP (conforme a imagem)
  - server 172.16.0.1
- Salve o arquivo e saia do editor (Ctrl+X, depois Y e Enter)

SINCRONIZAR NTP NOS SERVIDORES



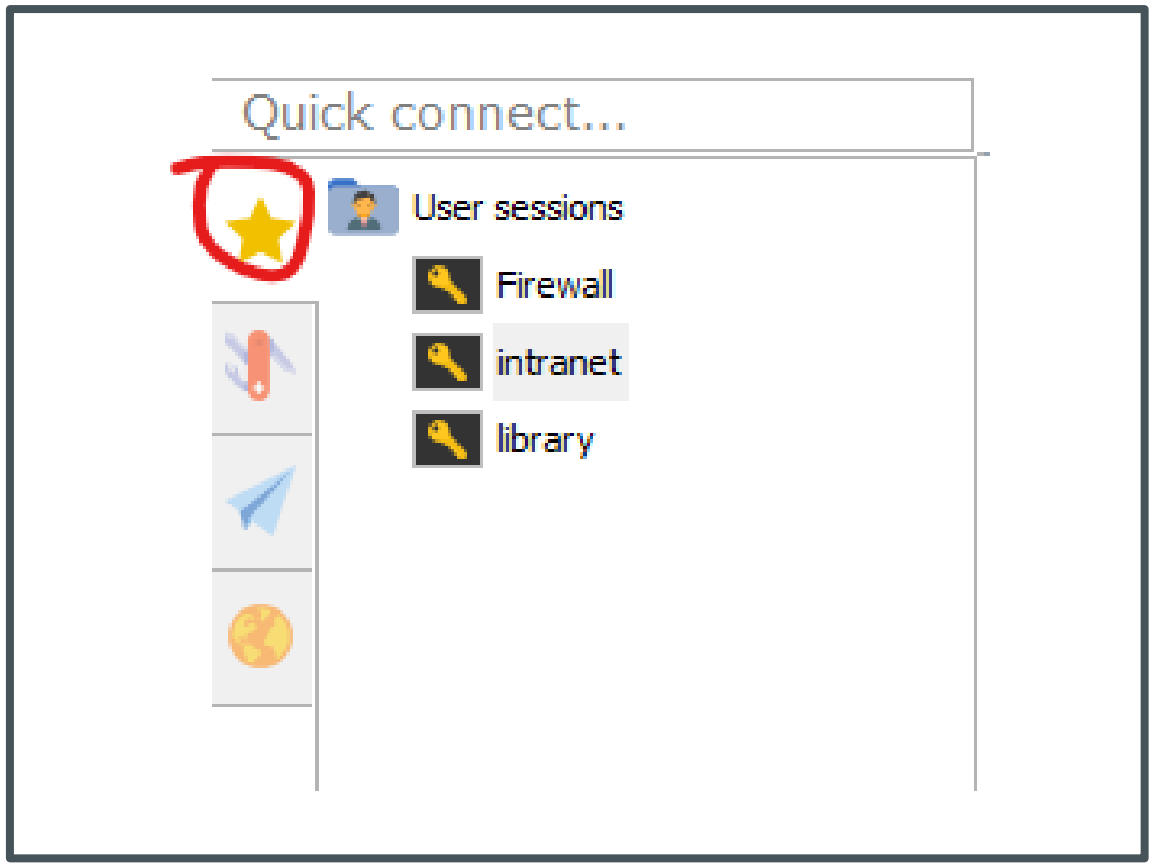
- Reinicie o serviço NTP com o seguinte comando
  - sudo service ntp restart
- Verifique o status do serviço com o seguinte commando
  - sudo service ntp status

SINCRONIZAR NTP NOS SERVIDORES



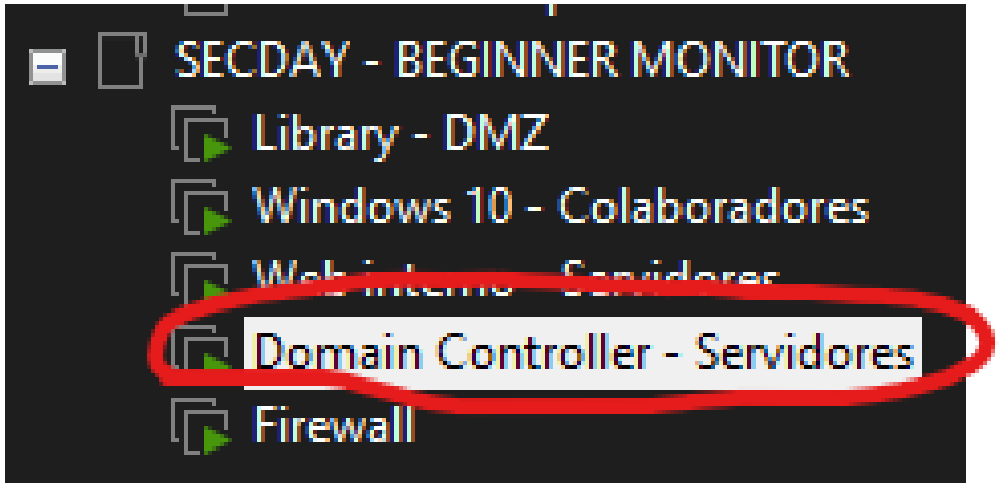
- Execute a sequência de comandos abaixo para o fuso horário do Brasil no Ubuntu, o ultimo comando deve refletir seu horário atual
  - sudo timedatectl set-timezone America/Sao_Paulo
  - timedatectl
  - sudo ln -sf /usr/share/zoneinfo/America/Sao_Paulo /etc/localtime
  - date

SINCRONIZAR NTP NOS SERVIDORES



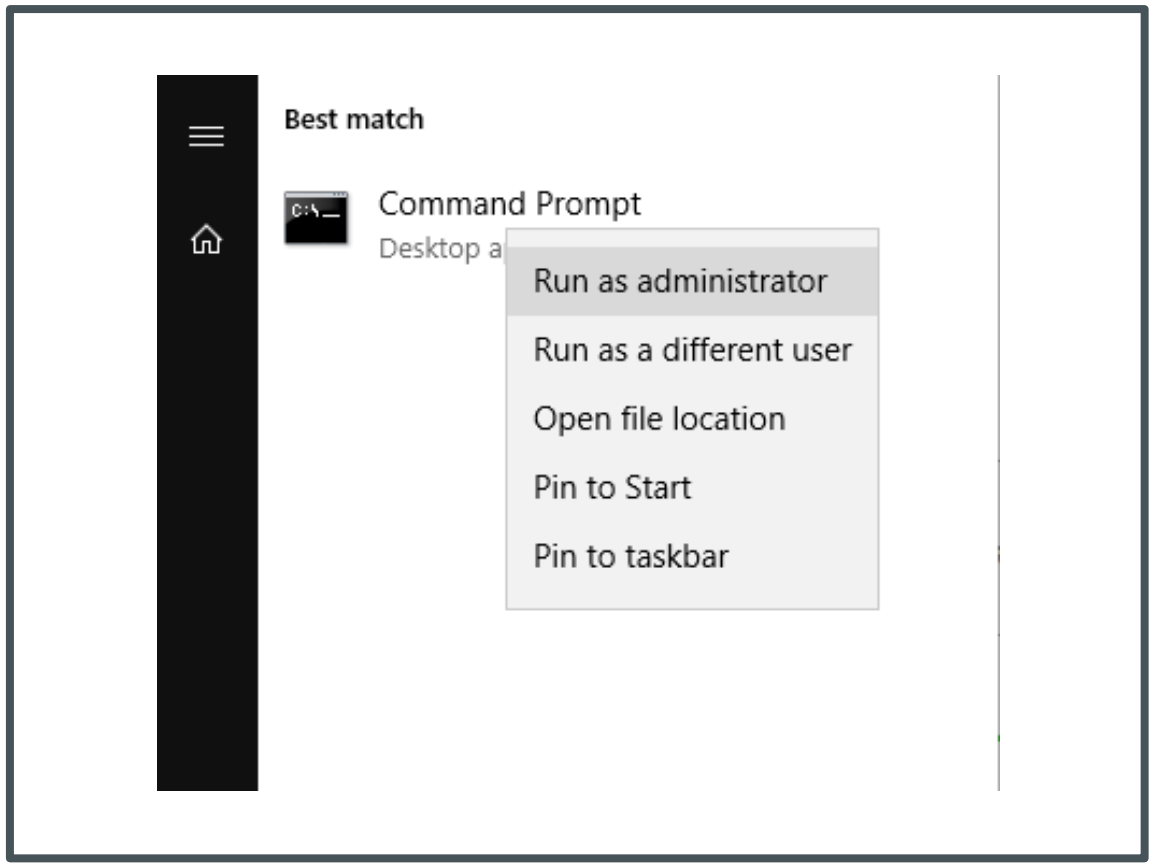
- Clique na “estrela” para voltar a ver a lista das conexões SSH, acesse o “library” e repita novamente os passos realizados na maquina anterior

SINCRONIZAR NTP NOS SERVIDORES



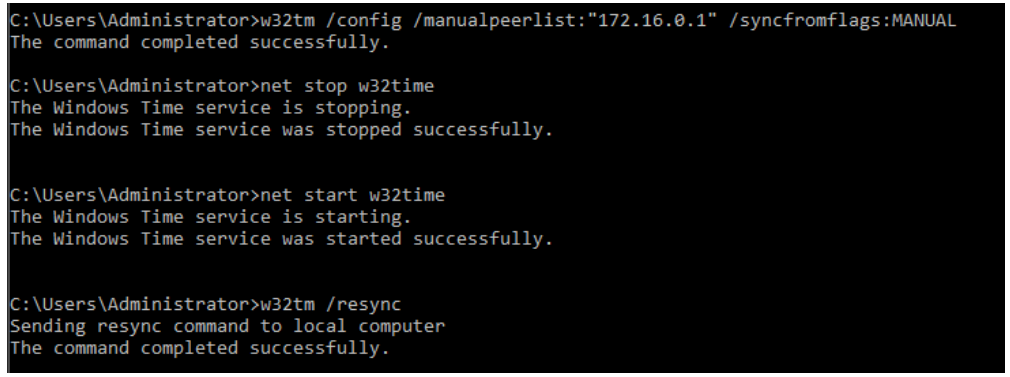
- Agora, vamos configurar o NTP no “Domain Controller – Servidores”, acesse a maquina com
  - User: Administrator
  - Pass: Admin@mudar

SINCRONIZAR NTP NOS SERVIDORES



- Abra o prompt de comando como administrador

SINCRONIZAR NTP NOS SERVIDORES



- Execute o seguinte comando para configurar o Windows Time Service para usar um servidor NTP 172.16.0.1 (Interface de Servidores do Firewall)
  - w32tm /config /manualpeerlist:"172.16.0.1" /syncfromflags:MANUAL
  - net stop w32time
  - net start w32time
  - w32tm /resync

SINCRONIZAR NTP NOS SERVIDORES

- Para configurar o time zone, execute o commando
  - tzutil /s "E. South America Standard Time"

PRONTO, NTP CONFIGURADO NA REDE, VAMOS COMEÇAR AS COLETAS?

- Firewall – é o Servidor NTP
- Web Interno – Configurado
- Library – Configurado
- Domain Controller – Configurado
- Windows 10 – Recebe a hora do Domain Controller

CAMADAS DE MONITORAMENTO

HARDWARE

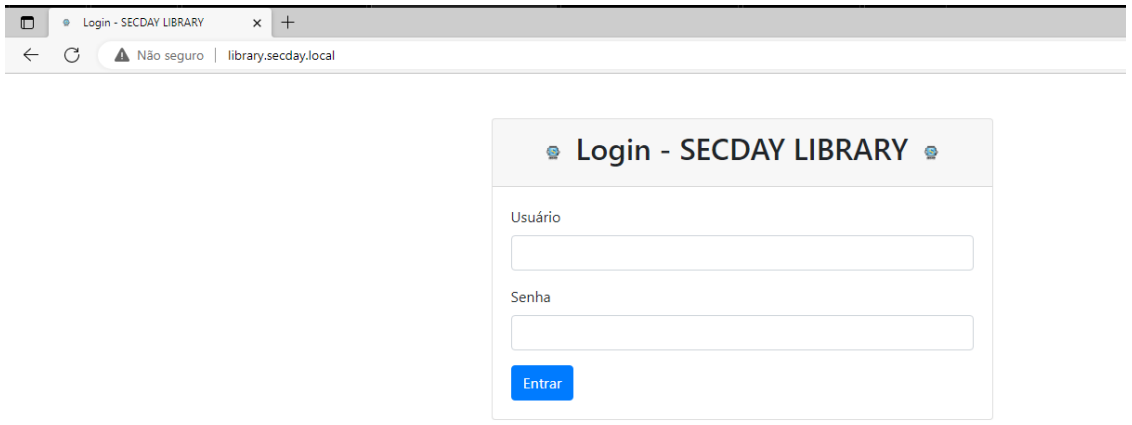
SISTEMA OPERACIONAL

REDE

APLICAÇÃO

DADOS

SEGURANÇA

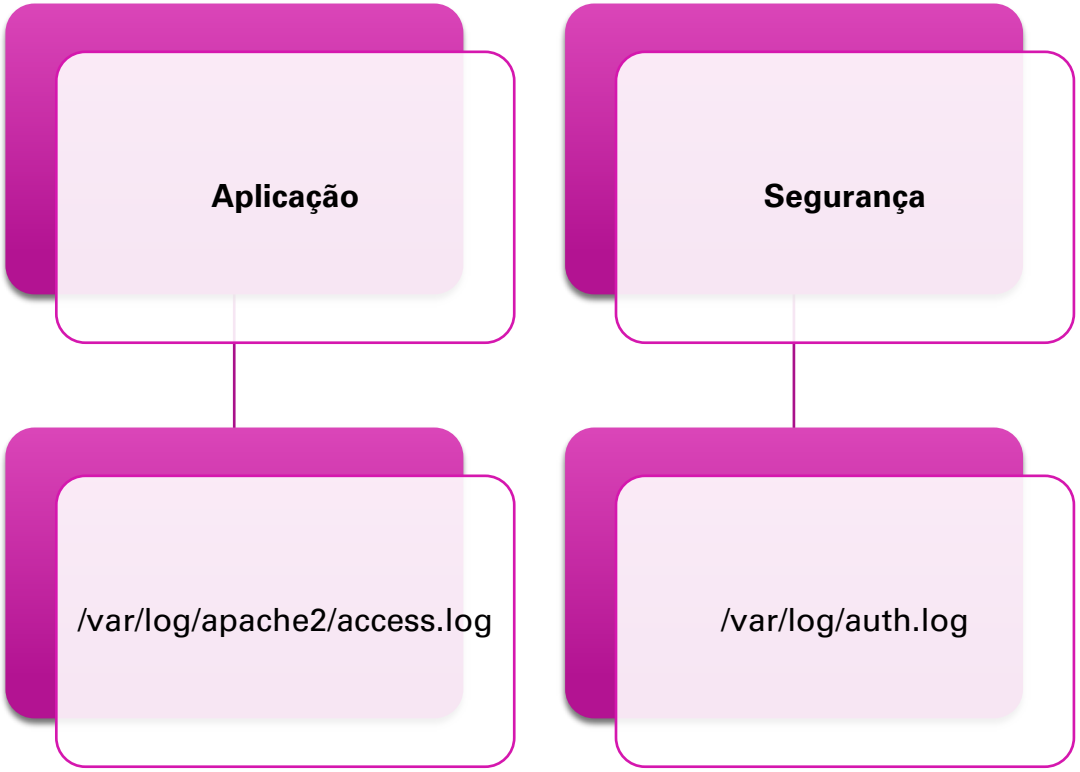


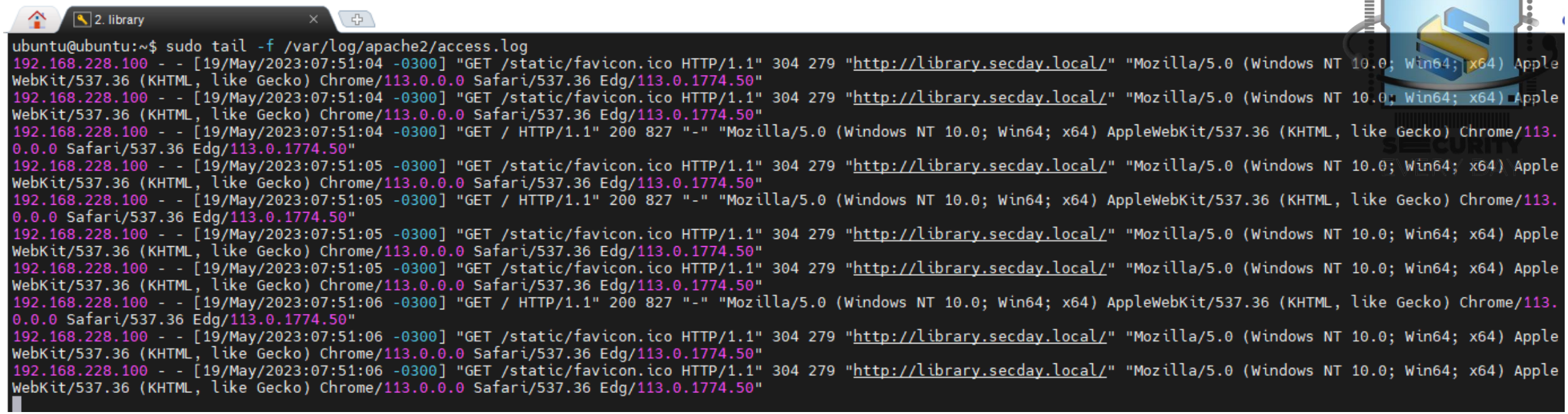
COLETA

- Acesse http://library.secday.local para ver a aplicação web

COLETA

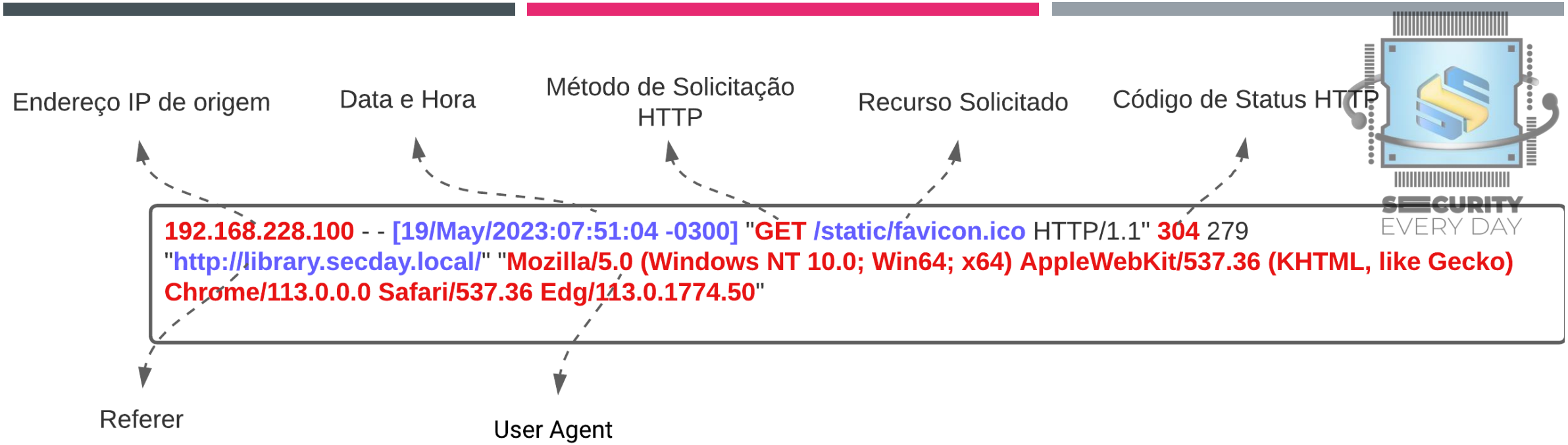

10.0.1.101
Aplicação


Aplicação
Segurança
/var/log/apache2/access.log
/var/log/auth.log



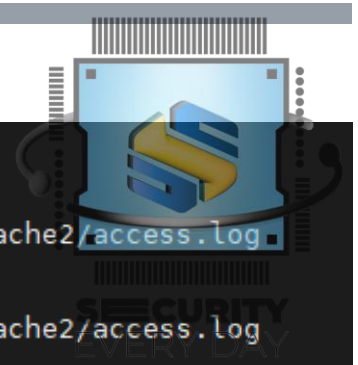
COLETA

- Acesse a máquina “library” via SSH para identificar os logs que queremos coletar, use o comando abaixo para identificar os logs de aplicação
  - sudo tail -f /var/log/apache2/access.log



COLETA

- Informações relevantes no log




```
ubuntu@ubuntu:~$ sudo tail -f /var/log/auth.log
May 19 07:50:29 ubuntu sshd[1419]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by (uid=0)
May 19 07:50:29 ubuntu systemd-logind[869]: New session 6 of user ubuntu.
May 19 07:50:52 ubuntu sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/apache2/access.log
May 19 07:50:52 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
May 19 07:50:55 ubuntu sudo: pam_unix(sudo:session): session closed for user root
May 19 07:51:12 ubuntu sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/apache2/access.log
May 19 07:51:12 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
May 19 07:53:30 ubuntu sudo: pam_unix(sudo:session): session closed for user root
May 19 07:53:35 ubuntu sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
May 19 07:53:35 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
May 19 07:53:45 ubuntu sshd[1651]: Accepted password for ubuntu from 192.168.228.100 port 57850 ssh2
May 19 07:53:45 ubuntu sshd[1651]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by (uid=0)
May 19 07:53:45 ubuntu systemd-logind[869]: New session 7 of user ubuntu.
May 19 07:53:45 ubuntu sshd[1653]: Accepted password for ubuntu from 192.168.228.100 port 57851 ssh2
May 19 07:53:45 ubuntu sshd[1653]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by (uid=0)
May 19 07:53:45 ubuntu systemd-logind[869]: New session 8 of user ubuntu.
```

COLETA

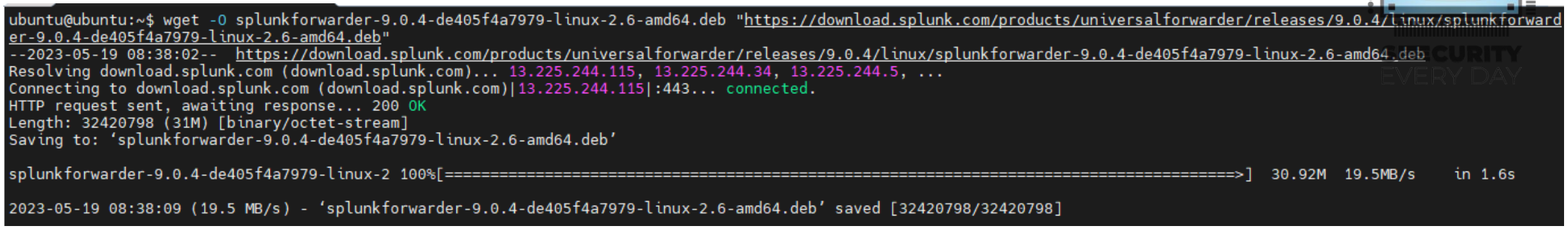
- Use o comando abaixo para identificar os logs de segurança que queremos monitorar
  - sudo tail -f /var/log/auth.log

COLETA

- Algumas informações relevantes que conseguimos ver com os logs /var/log/auth.log
  - Tentativas de login
  - Uso de sudo
  - Mudanças de senha
  - Adição/Remoção de usuários e grupos
  - Logins e logouts de usuários
  - Atividade do servidor SSH
  - Crond jobs

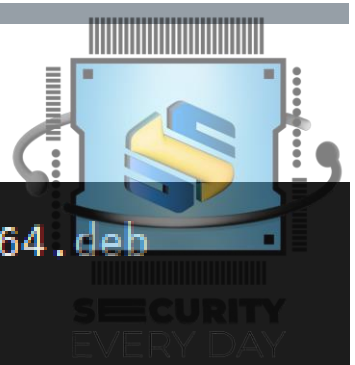
COLETA

- Instalando o Splunk Universal Forwarder na máquina “library” e encaminhando os logs



INSTALAÇÃO SPLUNK UF - LIBRARY

- Para baixar o instalar do Splunk UF, utilize o comando
  - wget -O splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.0.4/linux/splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb"




```
ubuntu@ubuntu:~$ sudo dpkg -i splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 117141 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb ...
Unpacking splunkforwarder (9.0.4) ...
Setting up splunkforwarder (9.0.4) ...
complete
ubuntu@ubuntu:~$
```

INSTALAÇÃO SPLUNK UF - LIBRARY

- Para instalar o Splunk UF, utilize o comando
  - sudo dpkg -i splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb

```
provided at no charge, and their use will be for a limited duration.

(ii) Beta Licenses. Some Offerings and features may be available to you as a
preview, or as an alpha, beta or other pre-release version (each, a "Beta
Offering"). All rights for Beta Offerings are solely for internal testing and
evaluation.  Your use of a Beta Offering will be for the term specified by us,
Do you agree with this license? [y/n]: y
```

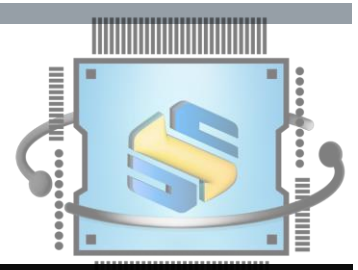
INSTALAÇÃO SPLUNK UF - LIBRARY

- Para iniciar o splunk, use o comando
  - sudo /opt/splunkforwarder/bin/splunk start
    - Aperte “**q**” e depois “**y + Enter**” para aceitar a licença

```
Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunk
The unit file has been created.


Splunk> Like an F-18, bro.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
```

INSTALAÇÃO SPLUNK UF - LIBRARY

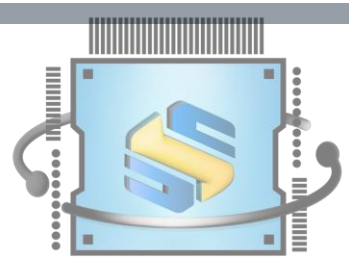
- Defina um nome de usuário e senha para o agente



```
PS C:\Users\kelve> Get-NetIPConfiguration | Where-Object { $_.NetAdapter.Status -eq "Up" } | Select-Object InterfaceAlias, IPv4Address

InterfaceAlias                IPv4Address
--------------                -----------
Ethernet 4                    {192.168.56.1}
Ethernet                      {192.168.1.8}
VMware Network Adapter VMnet8 {192.168.126.1}
```

COLETA - SPLUNK UF - LIBRARY

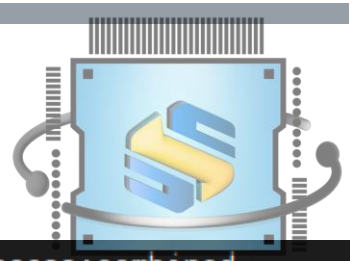
- Vamos configurar o envio de logs para nosso servidor Splunk (que é o IP da sua maquina host)
  - Para descobrir o IP da sua maquina de forma “facil”, basta abrir o powershell e executar o commando abaixo, no meu caso, o IP é 192.168.1.8
    - Get-NetIPConfiguration | Where-Object { $_.NetAdapter.Status -eq "Up" } | Select-Object InterfaceAlias, IPv4Address



```
ubuntu@ubuntu:~$ sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.1.8:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: admin
Password:
Added forwarding to: 192.168.1.8:9997.
ubuntu@ubuntu:~$
```


COLETA - SPLUNK UF - LIBRARY

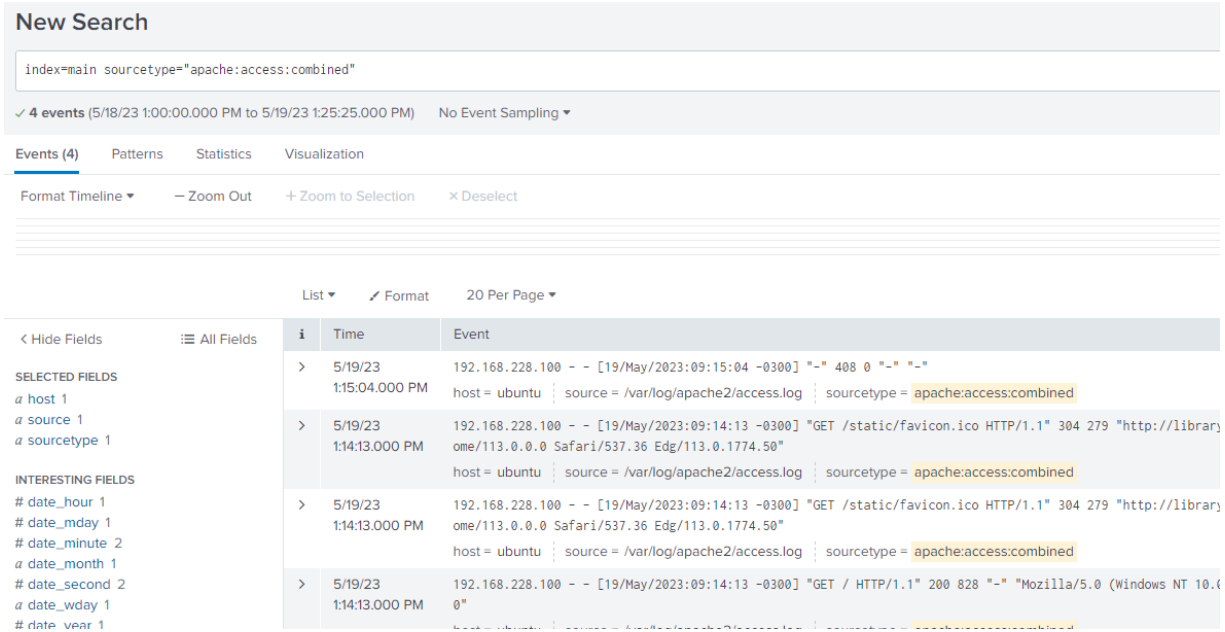
- Novamente, na maquina “library”, execute o seguinte comando para configurar o encaminhamento dos logs para o Splunk
  - sudo /opt/splunkforwarder/bin/splunk add forward-server SeuIP:9997




```
ubuntu@ubuntu:~$ sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/apache2/access.log -sourcetype apache:access:combined
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Your session is invalid.  Please login.
Splunk username: admin
Password:
Added monitor of '/var/log/apache2/access.log'.
ubuntu@ubuntu:~$
```

COLETA - SPLUNK UF - LIBRARY

- Agora, vamos configurar o envio dos logs de acesso ao apache para o Splunk com o comando
  - sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/apache2/access.log -sourcetype apache:access:combined



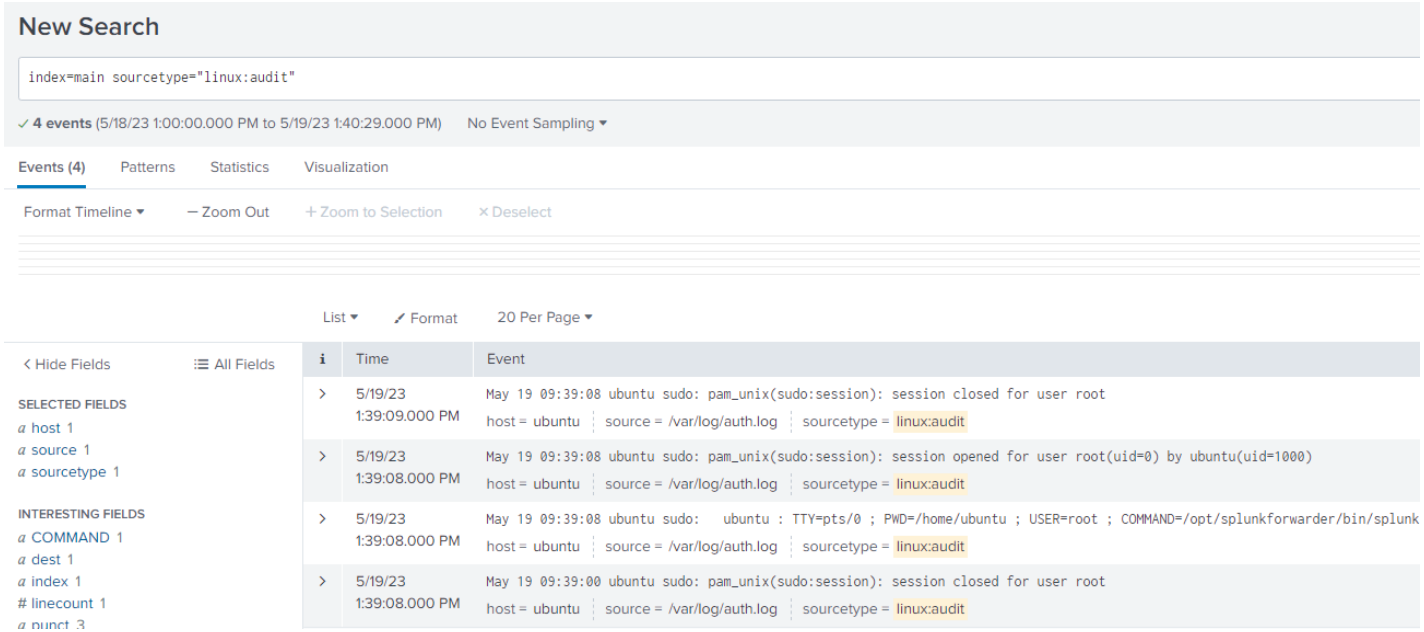
COLETA - SPLUNK UF - LIBRARY

- Acesse o splunk e envie a pesquisa abaixo para ver os logs chegando
  - index=main sourcetype="apache:access:combined"


```
ubuntu@ubuntu:~$ sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -sourcetype linux:audit
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Added monitor of '/var/log/auth.log'.
ubuntu@ubuntu:~$
```

COLETA - SPLUNK UF - LIBRARY

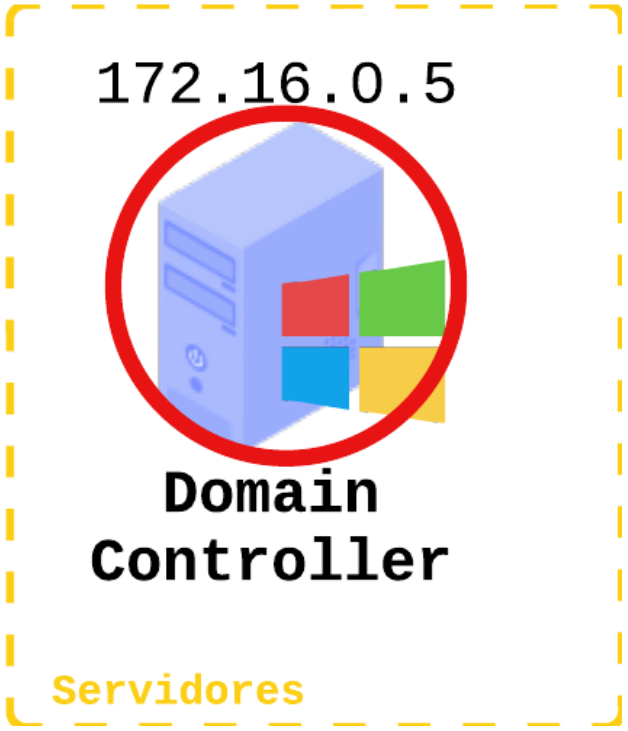
- Agora, vamos configurar o envio dos logs do auth.log para o Splunk com o comando
  - sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log –sourcetype linux:audit

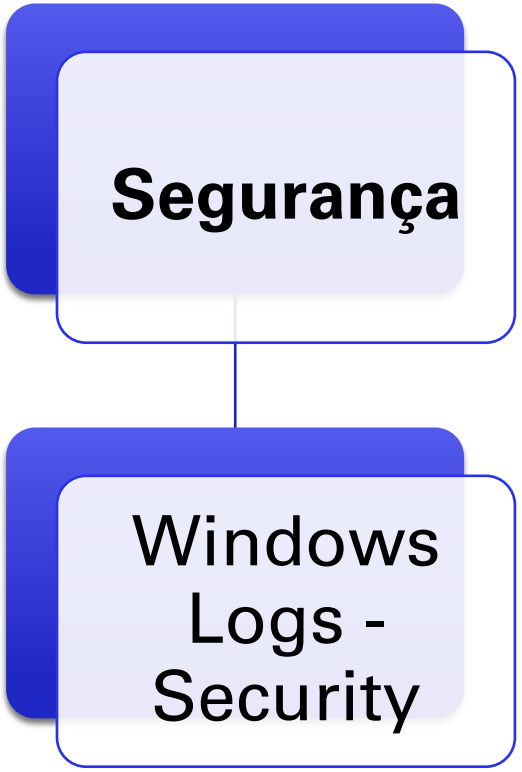


COLETA - SPLUNK UF - LIBRARY

- Acesse o splunk e envie a pesquisa abaixo para ver os logs chegando
  - index=main sourcetype="linux:audit"

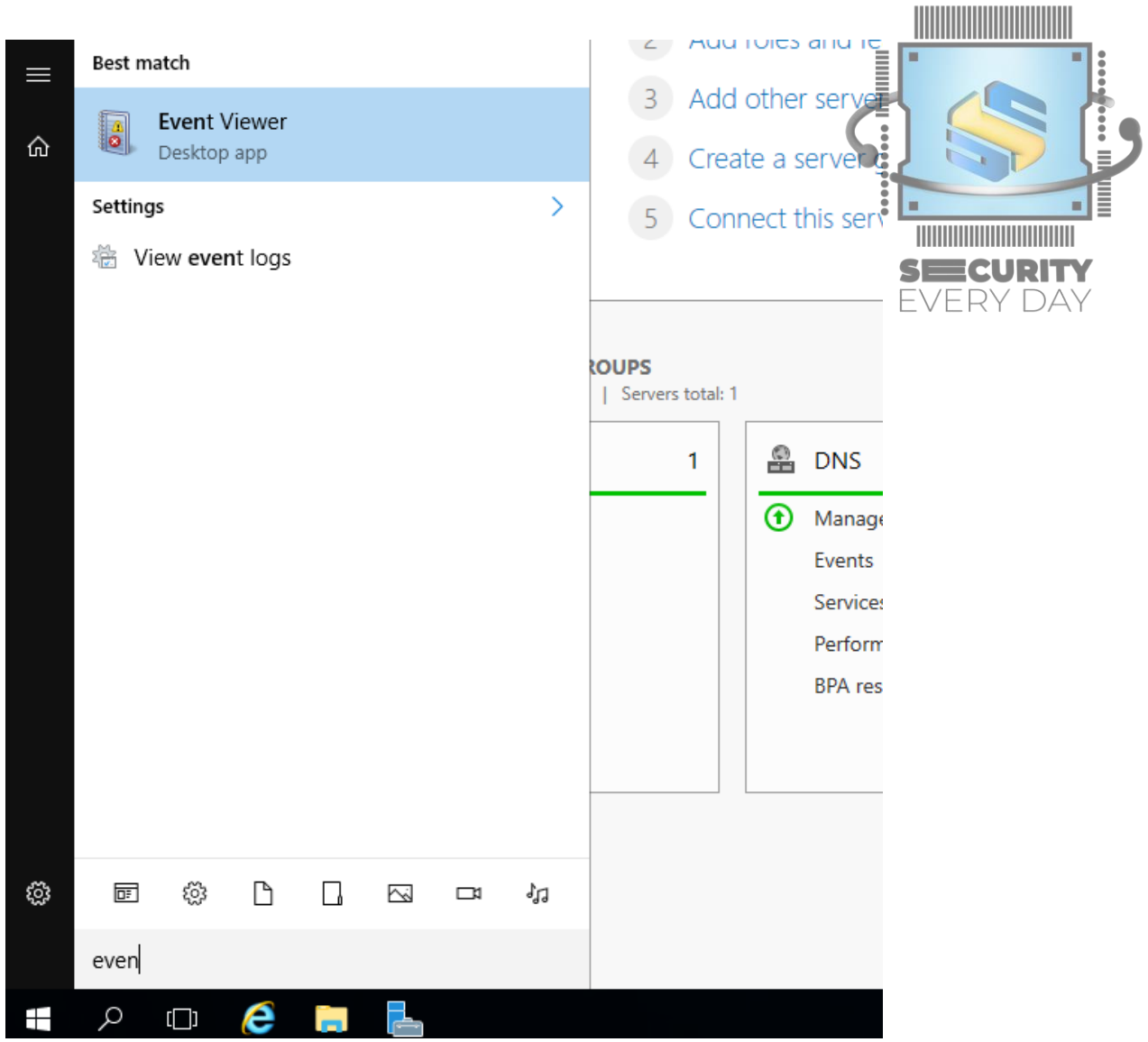
COLETA


172.16.0.5
Domain Controller
Servidores


Segurança
Windows Logs - Security

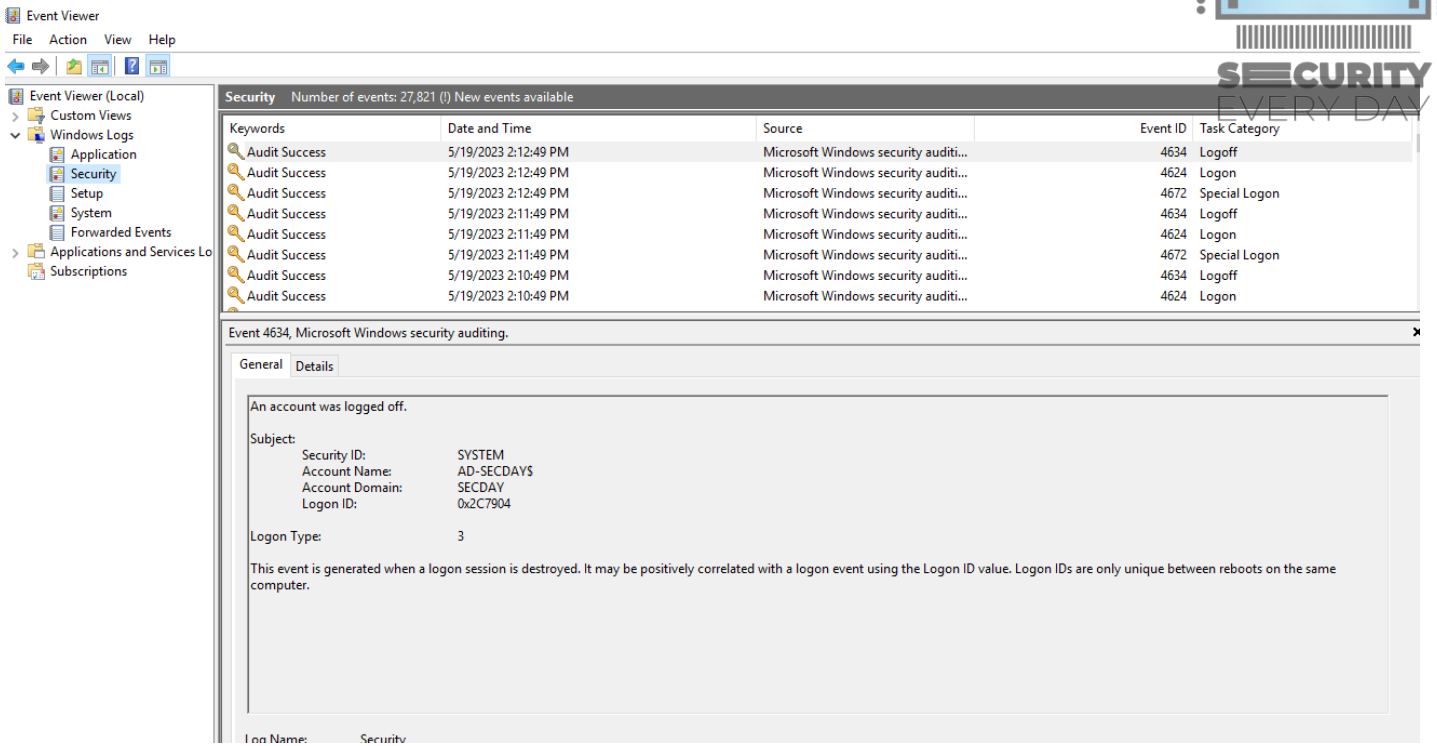
COLETA

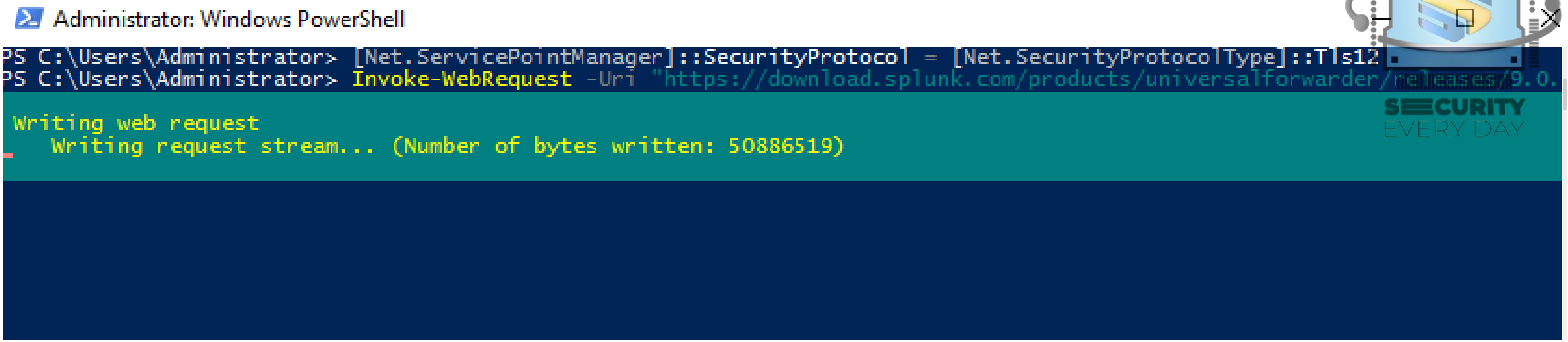
- Acesse a maquina “Domain Controller” e na barra de pesquisa digite “Event Viewer"



COLETA

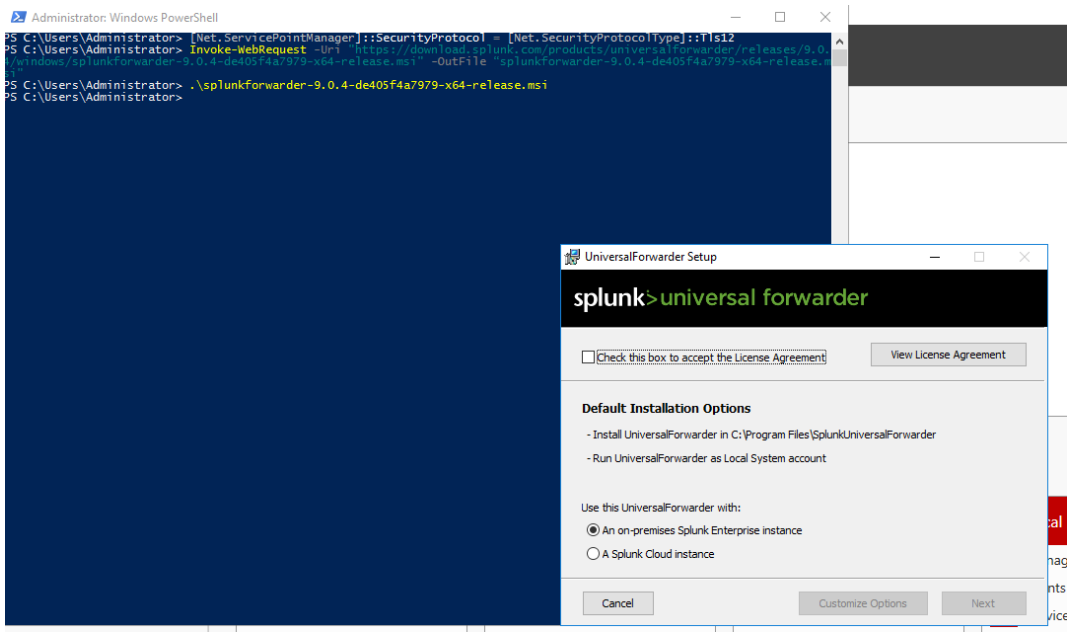
- Navegue até “Windows Logs → Security”
  - Nesses logs são registrados eventos como logins, logoffs, falhas de login, criação de novos usuários, mudanças de senha, entre outros.





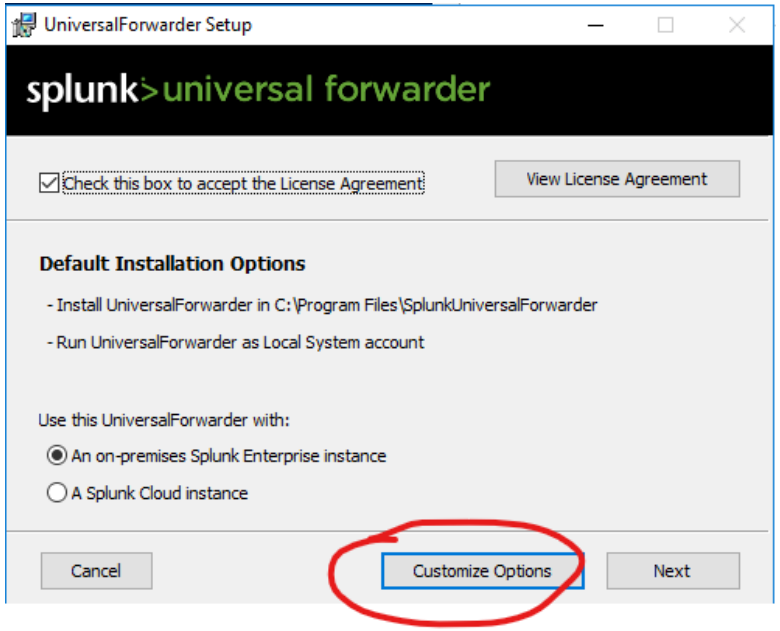
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Para baixar o instalar do Splunk UF, utilize os commando abaixo em sequencia via powershell:
  - [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
  - Invoke-WebRequest -Uri "https://download.splunk.com/products/universalforwarder/releases/9.0.4/windows/splunkforwarder-9.0.4-de405f4a7979-x64-release.msi" -OutFile “splunkforwarder-9.0.4-de405f4a7979-x64-release.msi"



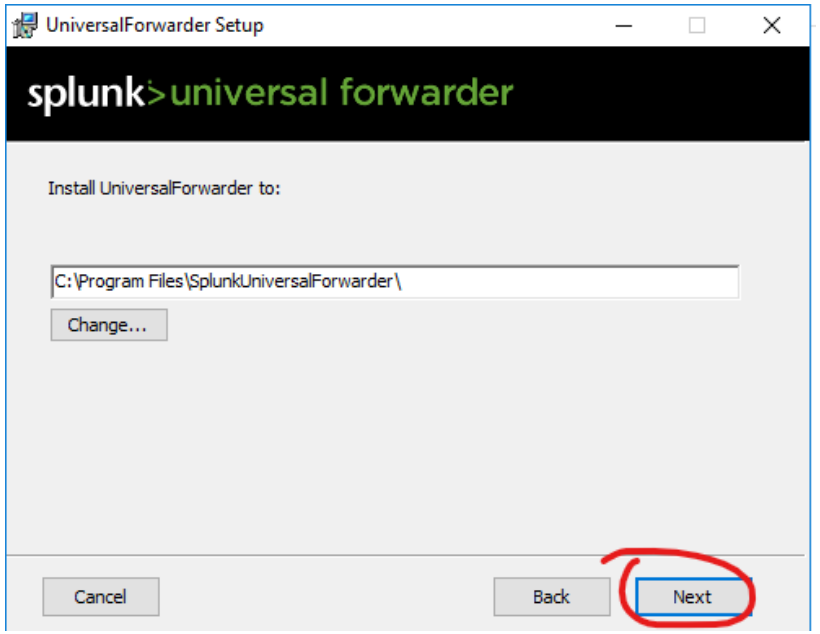
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Use o comando abaixo para iniciar a instalação
  - .\splunkforwarder-9.0.4-de405f4a7979-x64-release.msi



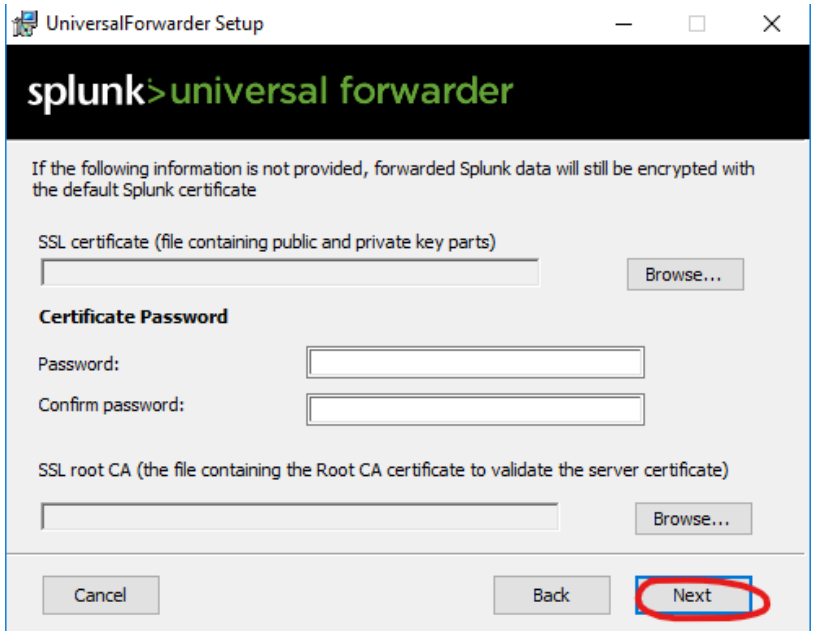
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Aceite a licença e clique em “Customize Options”



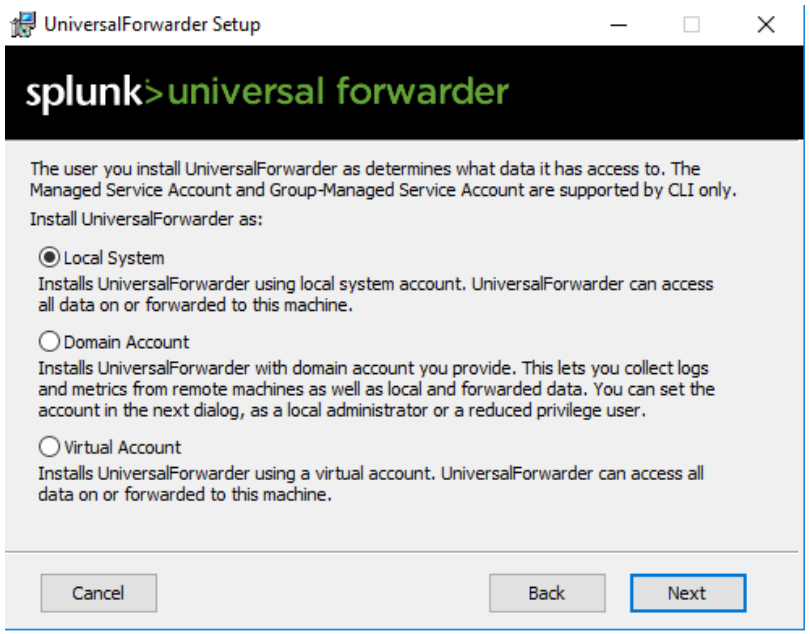
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Clique em “Next”



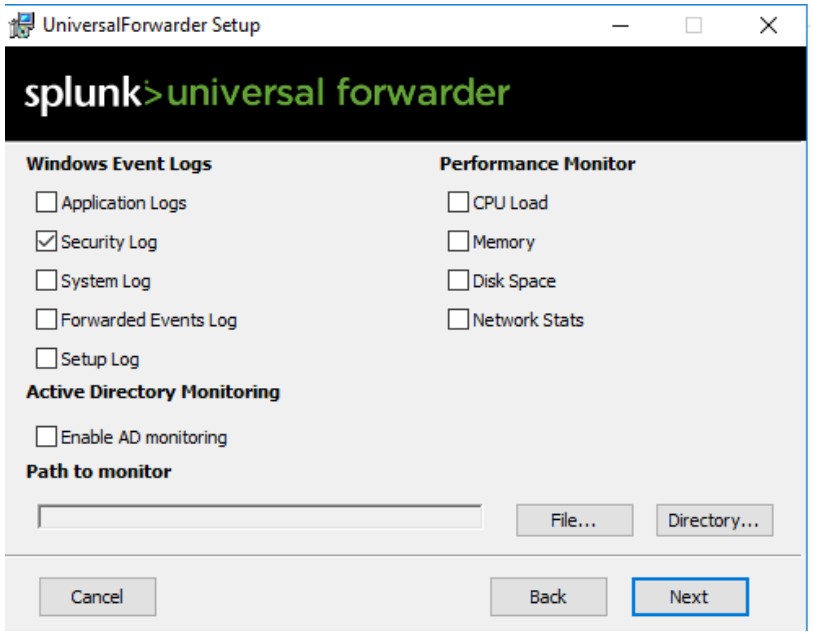
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Clique em “Next”



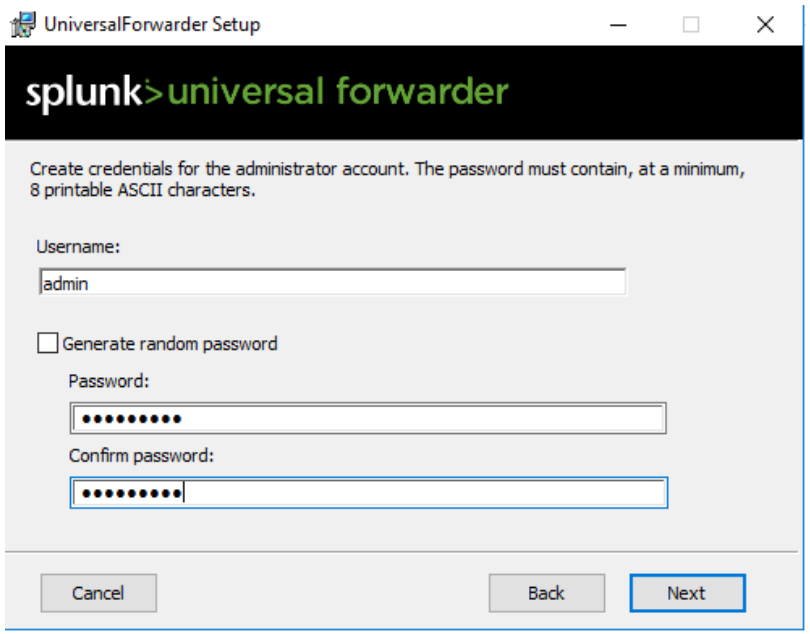
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Clique em “Next”



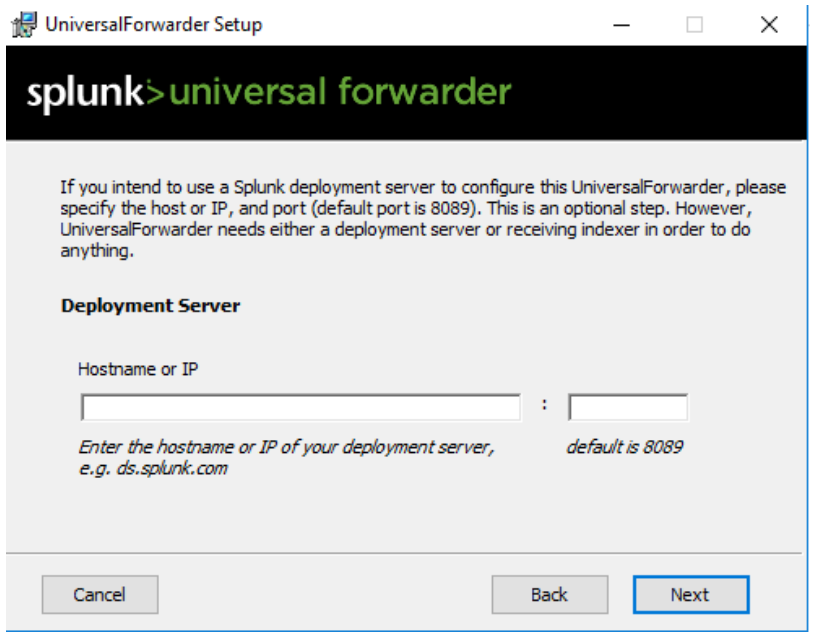
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Selecione “Security Log” e clique em “Next”



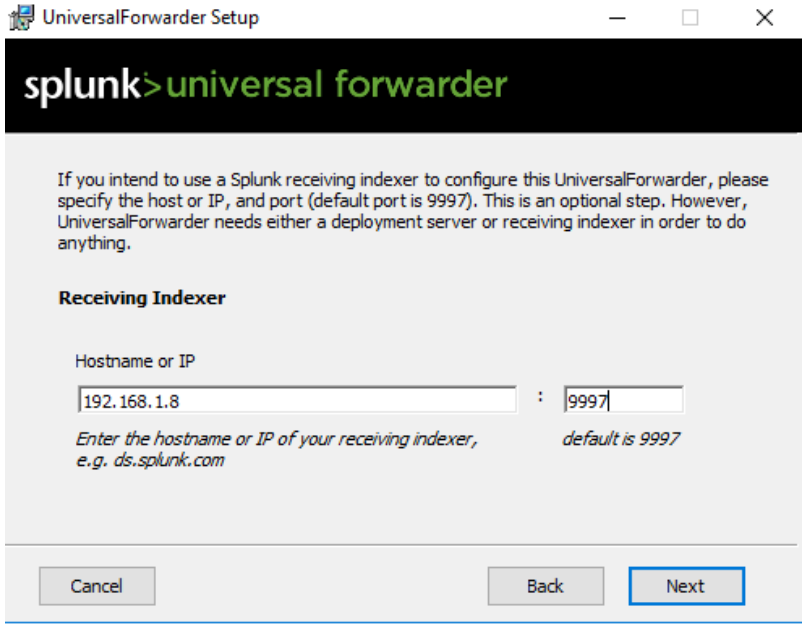
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Defina um nome de usuário e senha e clique em “Next”



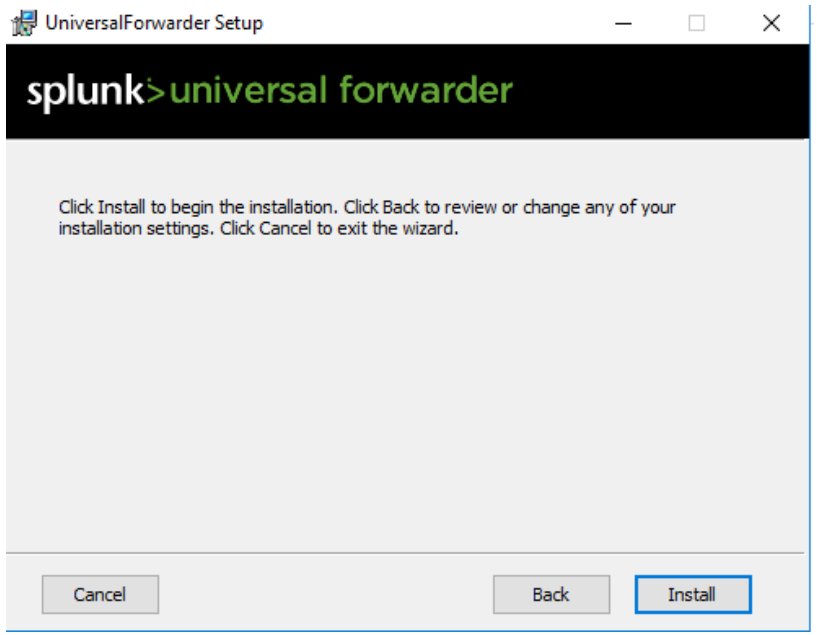
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Deixe em branco e clique em “Next”



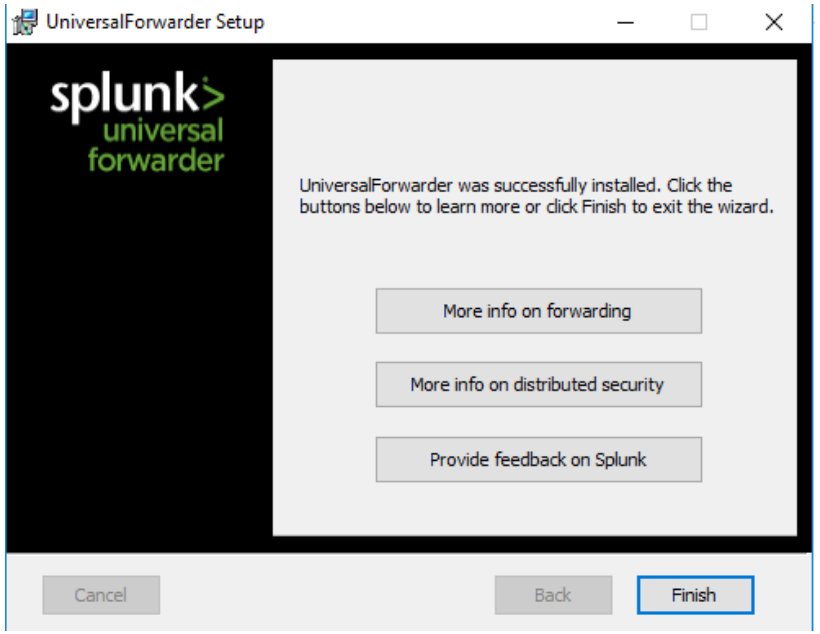
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Em “hostname or IP”, preencha com o **SEU IP** e porta 9997



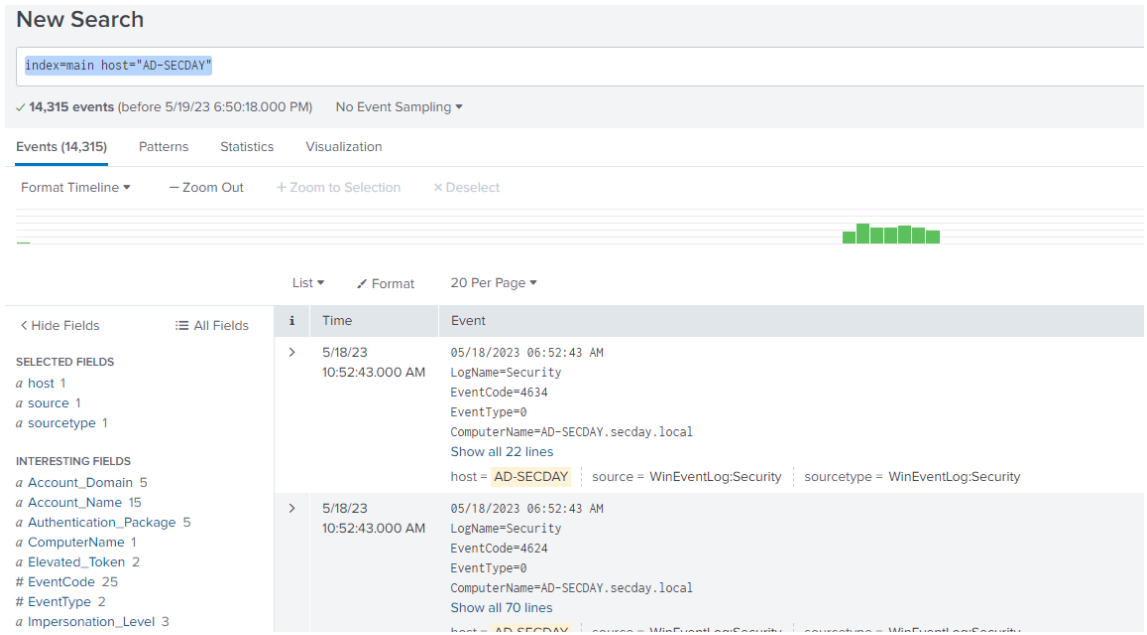
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Clique em “Install” e aguarde



INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

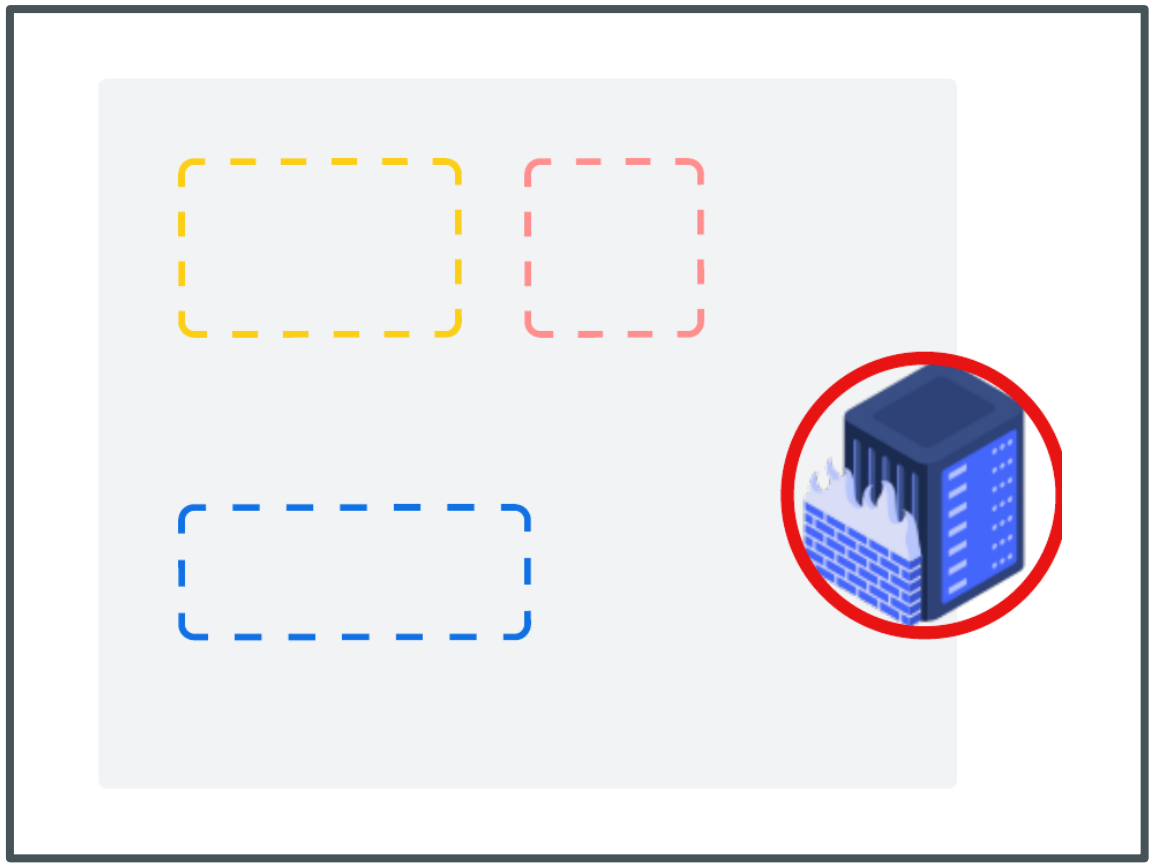
- Finalizada a instalação, clique em “Finish”



INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

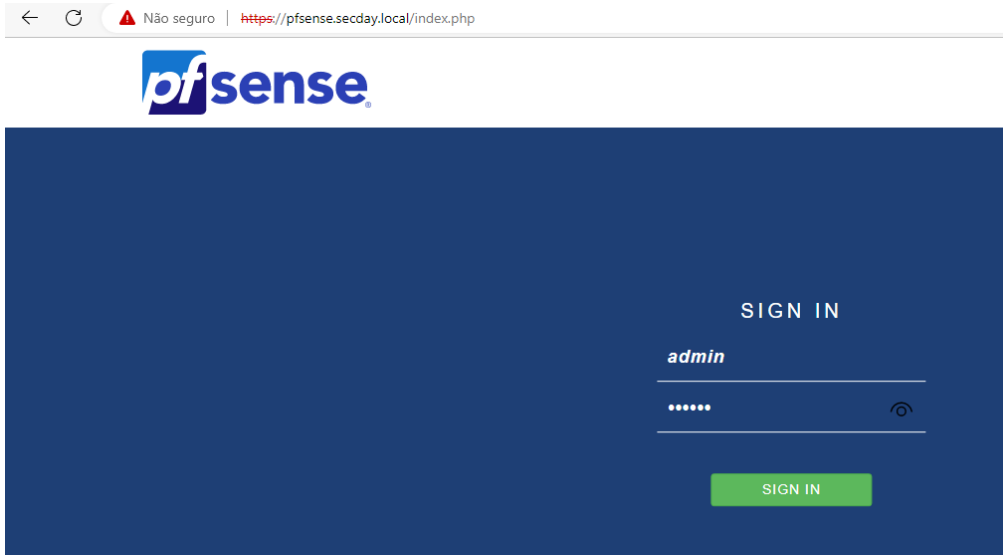
- Vá até o Splunk e faça a seguinte busca, os logs devem aparecer
  - index=main host="AD-SECDAY"

COLETA



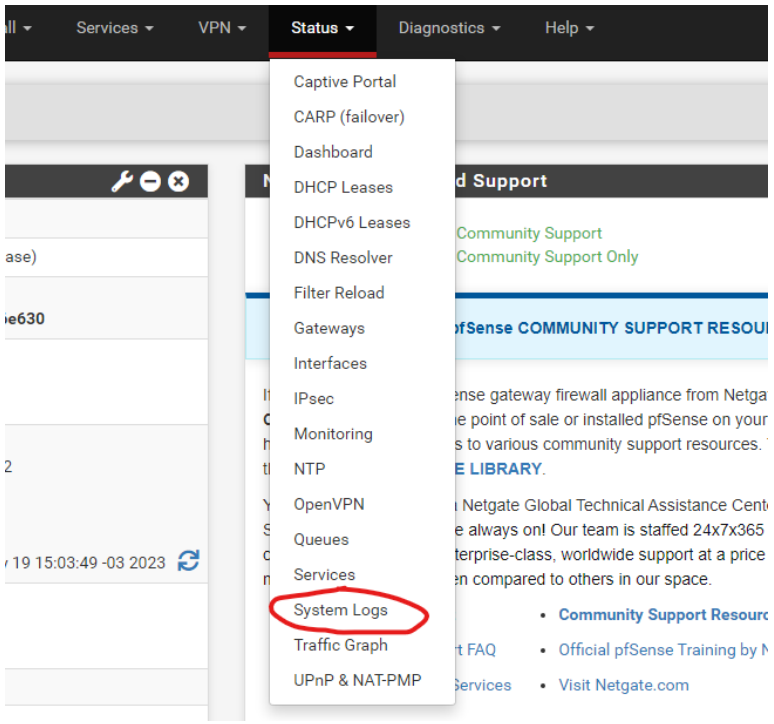
- Rede
- Firewall

CONFIGURAÇÃO – LOGS FIREWALL



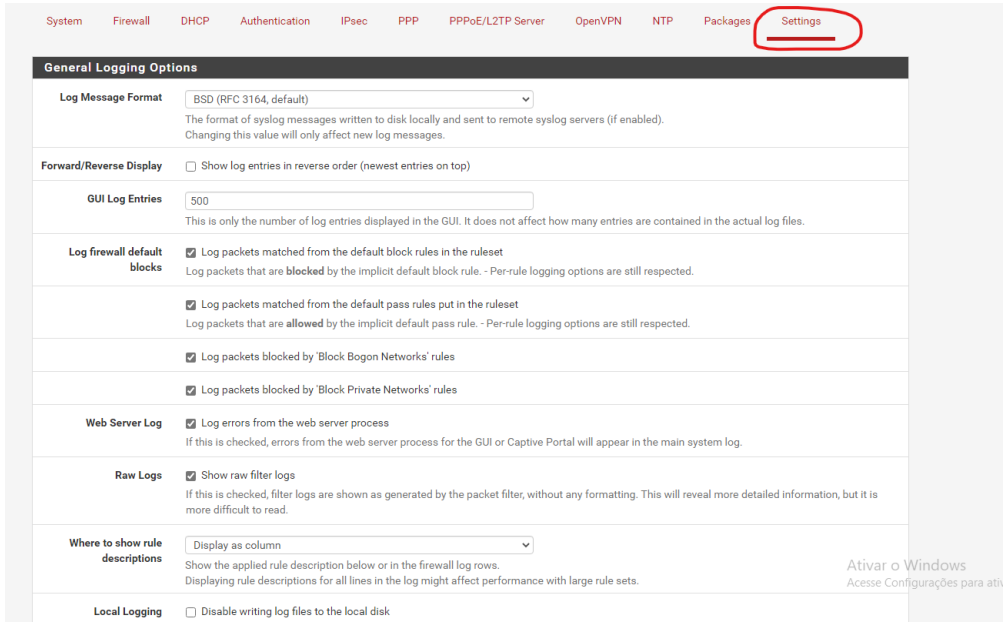
- Acesse a interface web do pfsense e logue com o usuario
  - User: admin
  - Pass: secday

CONFIGURAÇÃO – LOGS FIREWALL



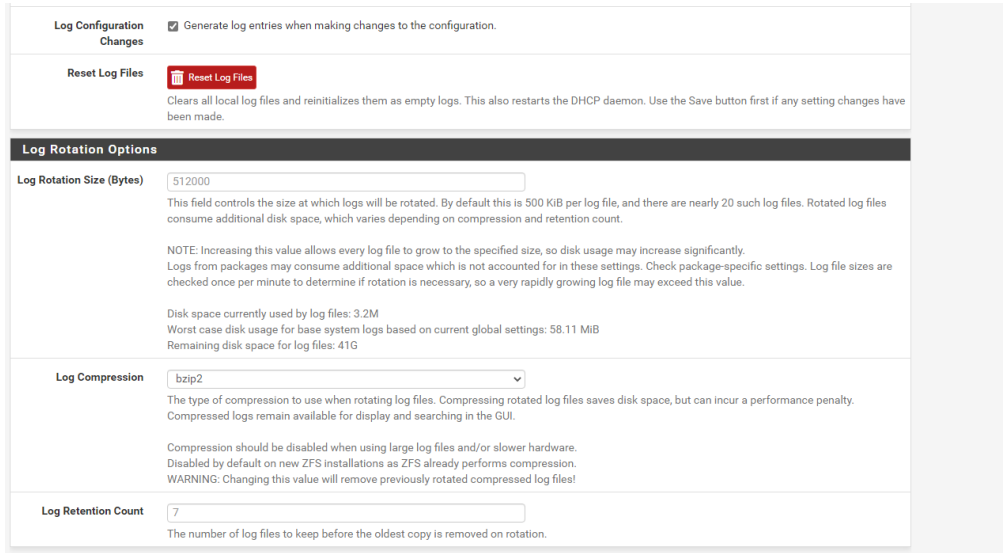
- Navegue até “Status → System Logs”

CONFIGURAÇÃO – LOGS FIREWALL



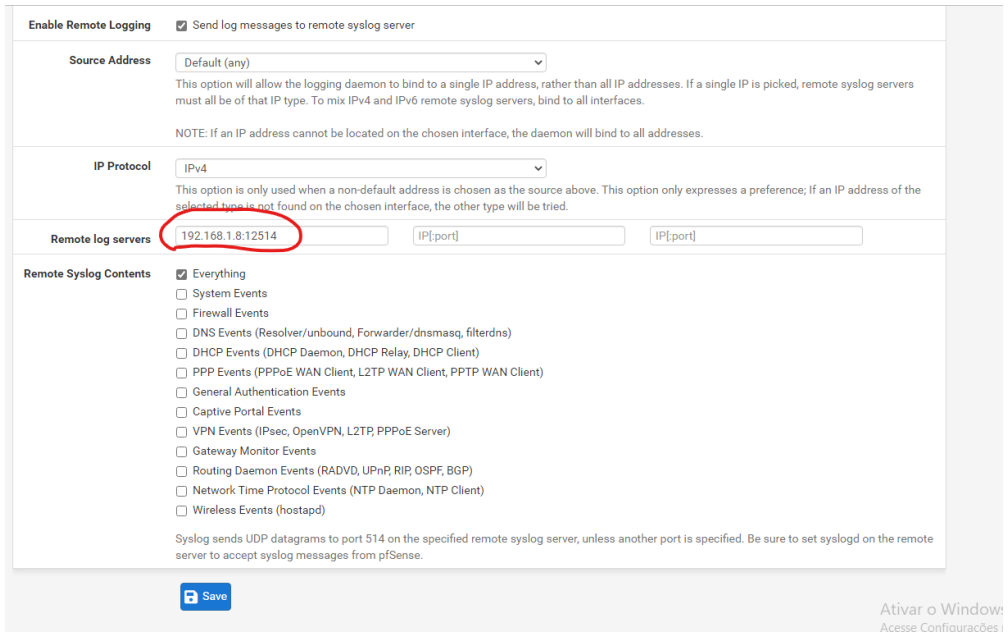
- Navegue até “Settings” e altere as configurações para ficarem iguais as configurações da imagem ao lado

CONFIGURAÇÃO – LOGS FIREWALL



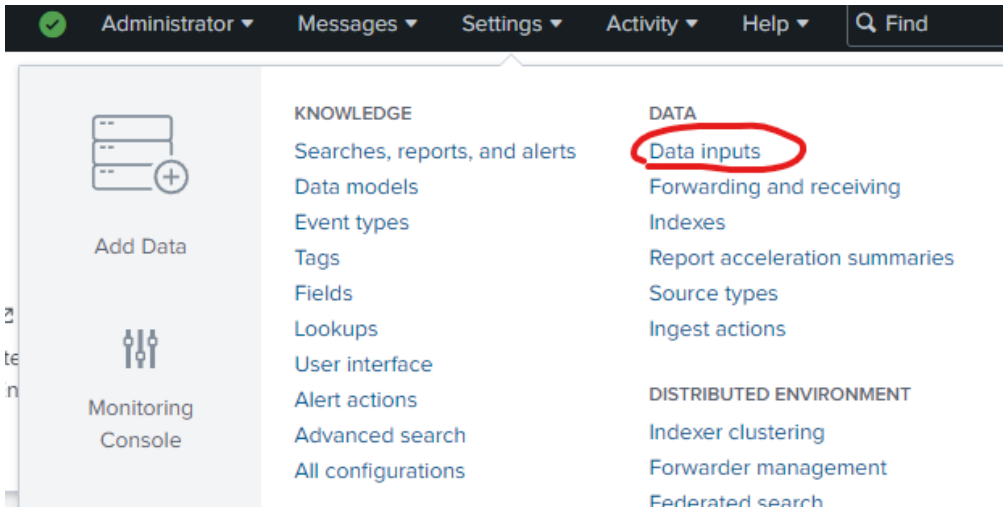
- Navegue até “Settings” e altere as configurações para ficarem iguais as configurações da imagem ao lado

CONFIGURAÇÃO – LOGS FIREWALL



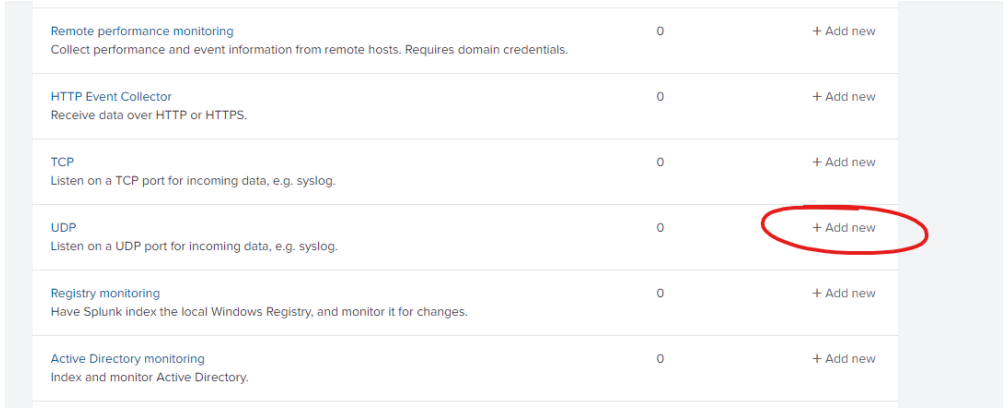
- No campo “Remote log servers” altere o IP para o **SEU IP**, na porta 12514, após isso, clique em “Save”

CONFIGURAÇÃO – LOGS FIREWALL



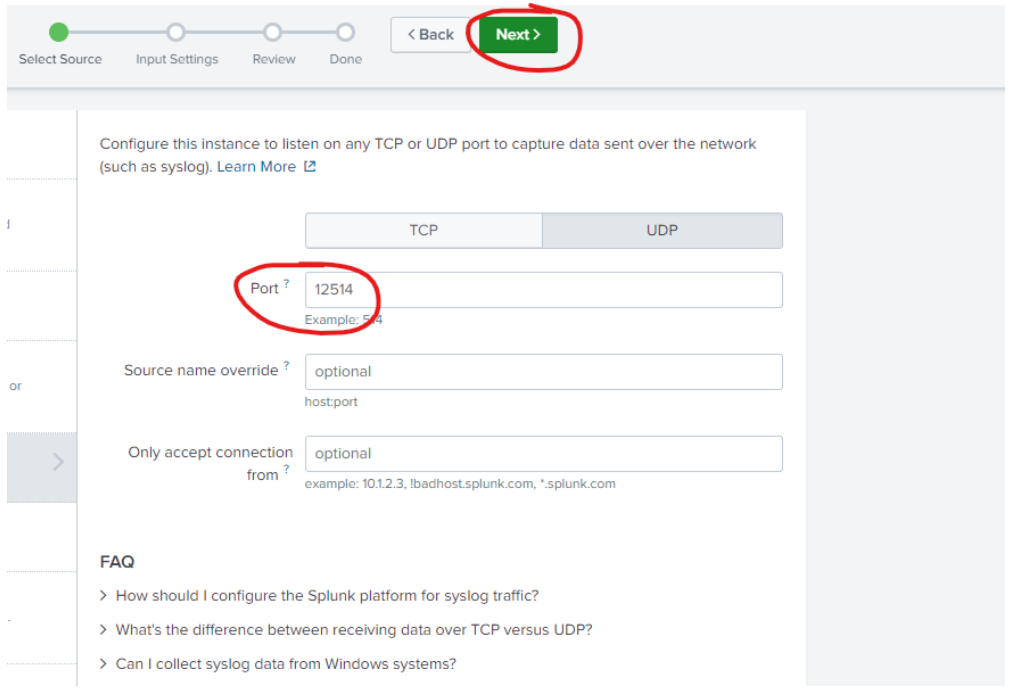
- Agora, no Splunk, vá em
  - Settings → Data Inputs

CONFIGURAÇÃO – LOGS FIREWALL



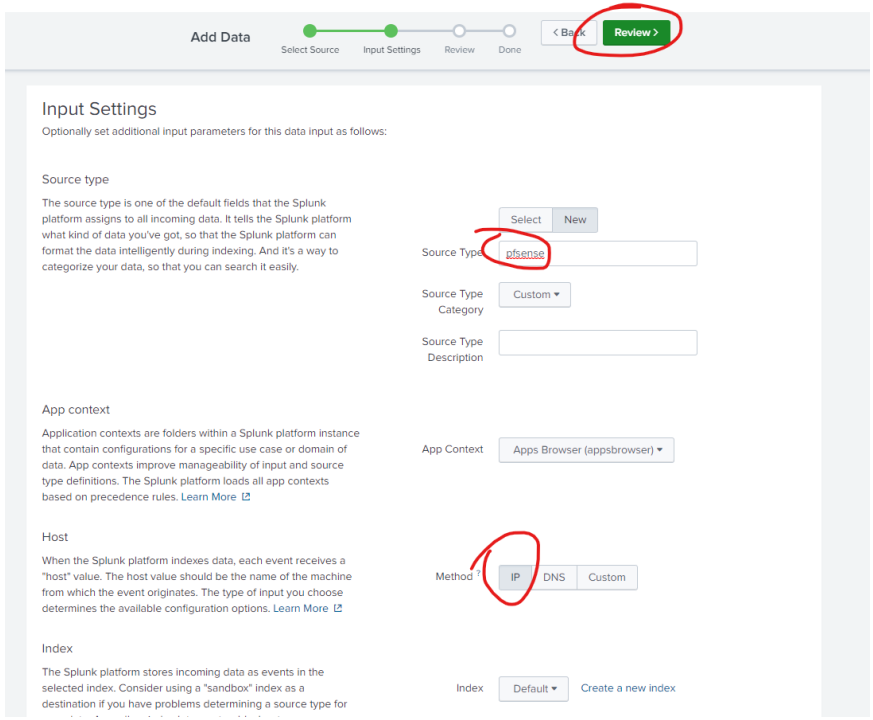
- Procure por ‘UDP” e clique em + “Add new”

CONFIGURAÇÃO – LOGS FIREWALL



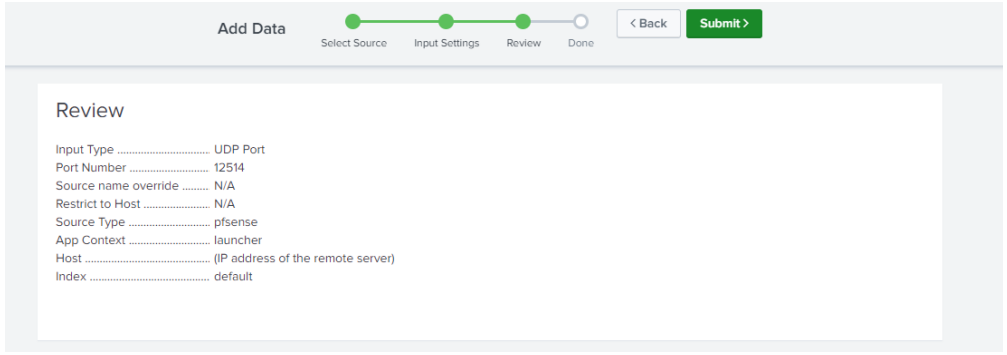
- Preencha conforme a imagem ao lado e clique em “Next”

CONFIGURAÇÃO – LOGS FIREWALL



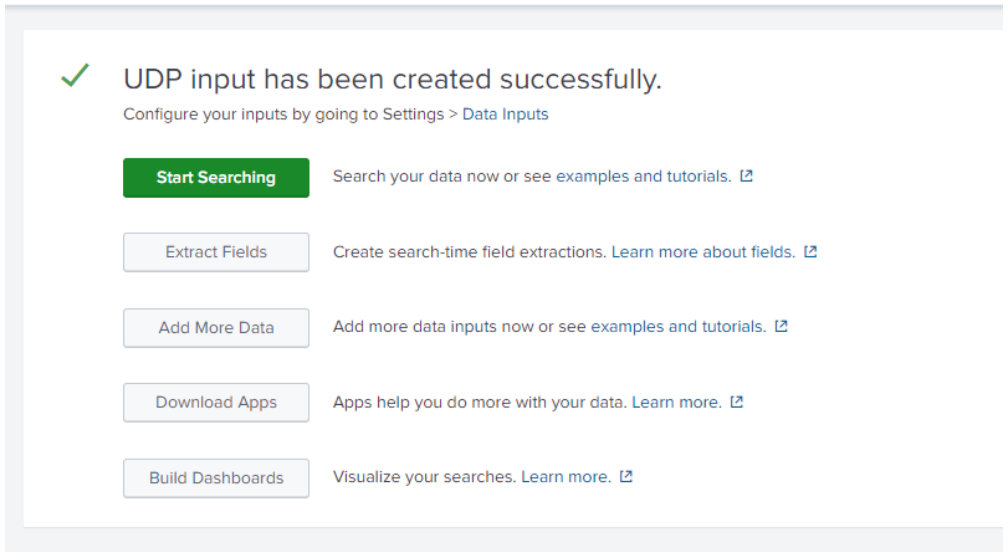
- No campo “Source Type”, preencha com “pfsense”
- Em “Method”, selecione “IP”
- Clique em “Review”

CONFIGURAÇÃO – LOGS FIREWALL



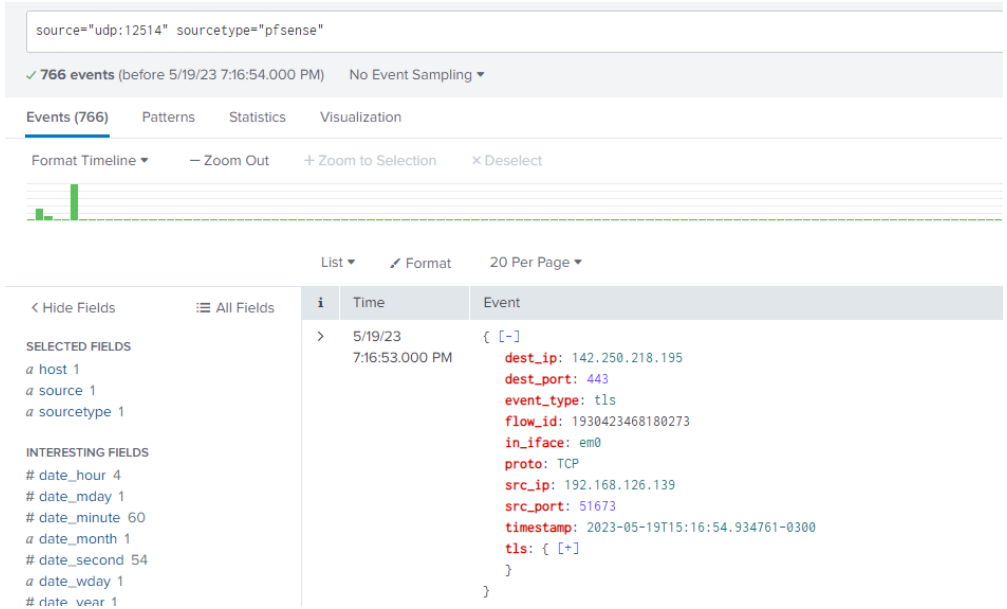
- Tudo certo! Clique em “Submit”

CONFIGURAÇÃO – LOGS FIREWALL



- Clique em “Start Searching”

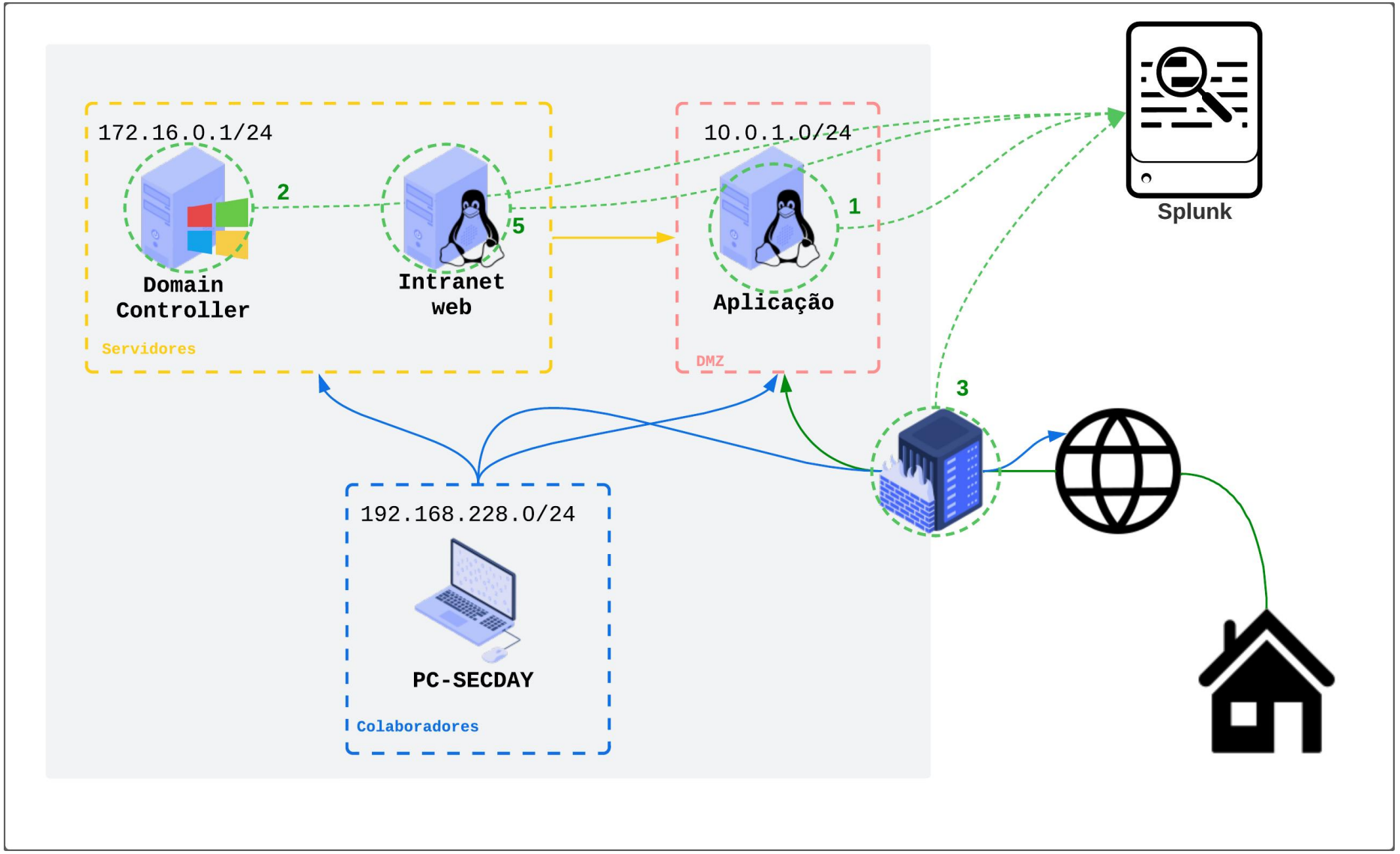
CONFIGURAÇÃO – LOGS FIREWALL



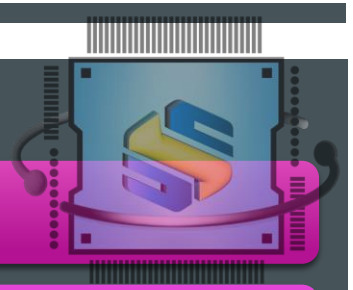
- Acesse “www.google.com” na maquina “Windows 10” e depois aperte “F5” na tela do Splunk, os logs devem começar aparecer

SECURITY
EVERY DAY

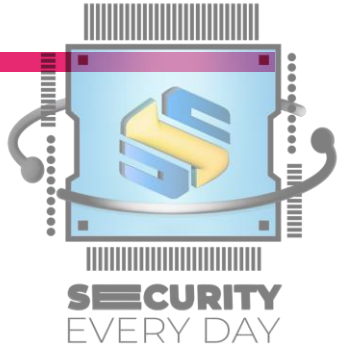
- Desenho atual da rede



ESTRATÉGIAS DE MONITORAMENTO

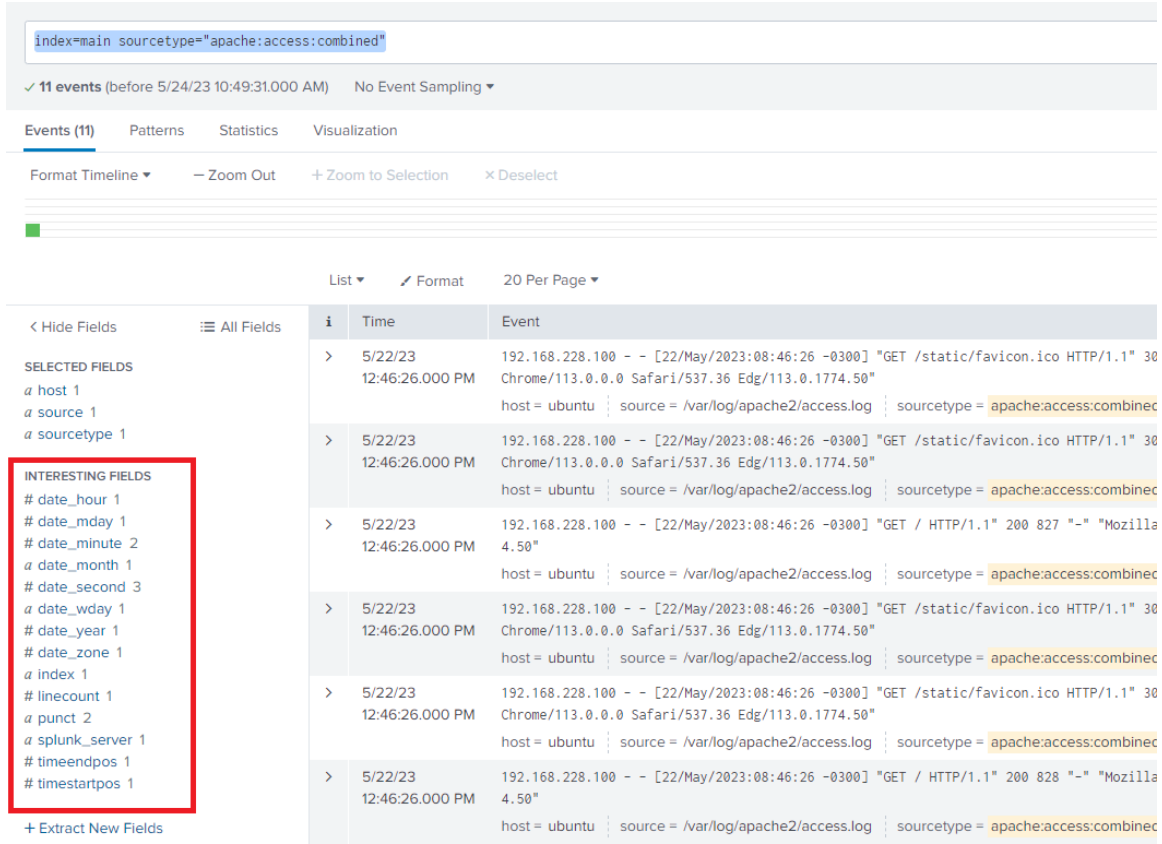


- ~~Identificação das Joias da Coroa~~
- ~~Instalação do SIEM~~
- Coleta dos logs
  - ~~Configuração do NTP~~
  - ~~Logs da aplicação exposta para internet~~
  - ~~Logs do Firewall~~
  - ~~Logs da aplicação da Web da intranet~~
  - ~~Controlador de Domínio~~
  - Logs de endpoints
- Exercício de Purple team
  - Realização de ataques
  - Criação de regras
  - Teste de efetividade



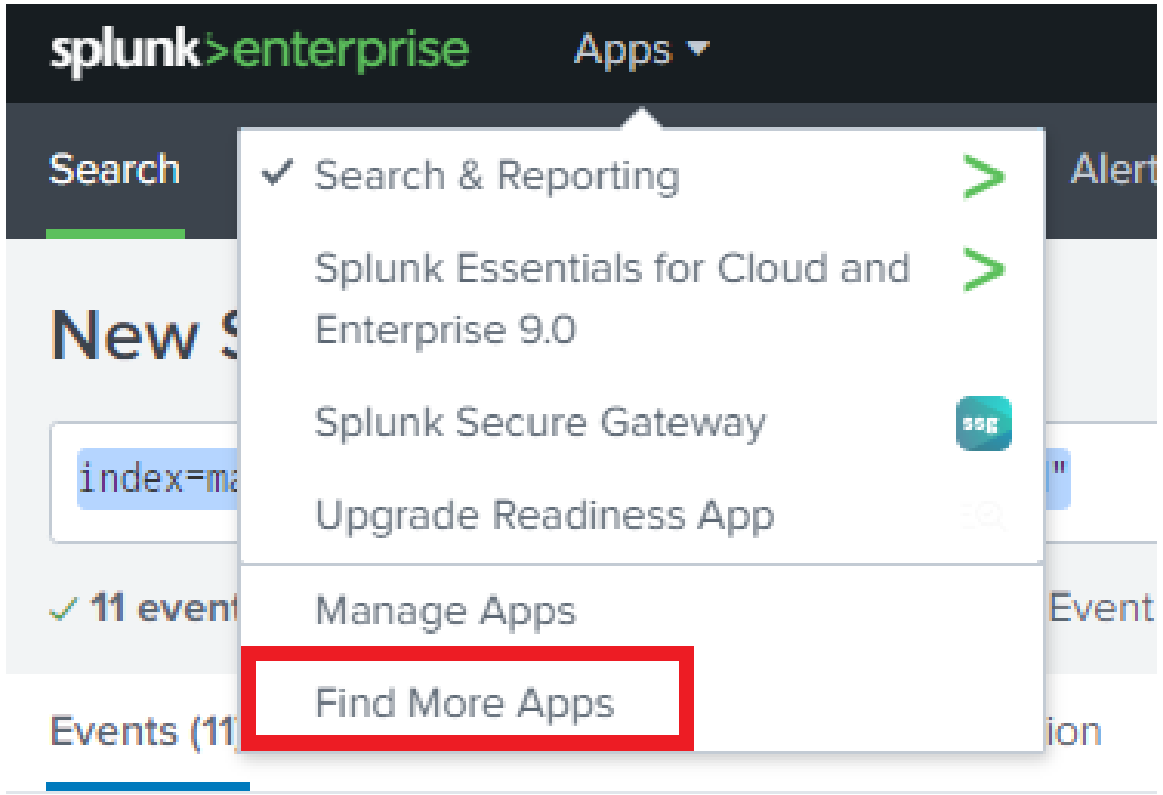
PARSING DE LOGS

- Parsing de logs é o processo de analisar e interpretar os registros ou "logs" produzidos por sistemas computacionais para extrair informações úteis.



CONFIGURAR OS PARSINGS - APACHE

- Se conduzirmos a pesquisa **index=main sourcetype="apache:access:combined"** no Splunk, observaremos que os logs ainda não passaram pelo processo de parsing. Para resolver essa isso, podemos instalar um add-on no Splunk que realiza automaticamente essa tarefa para nós.

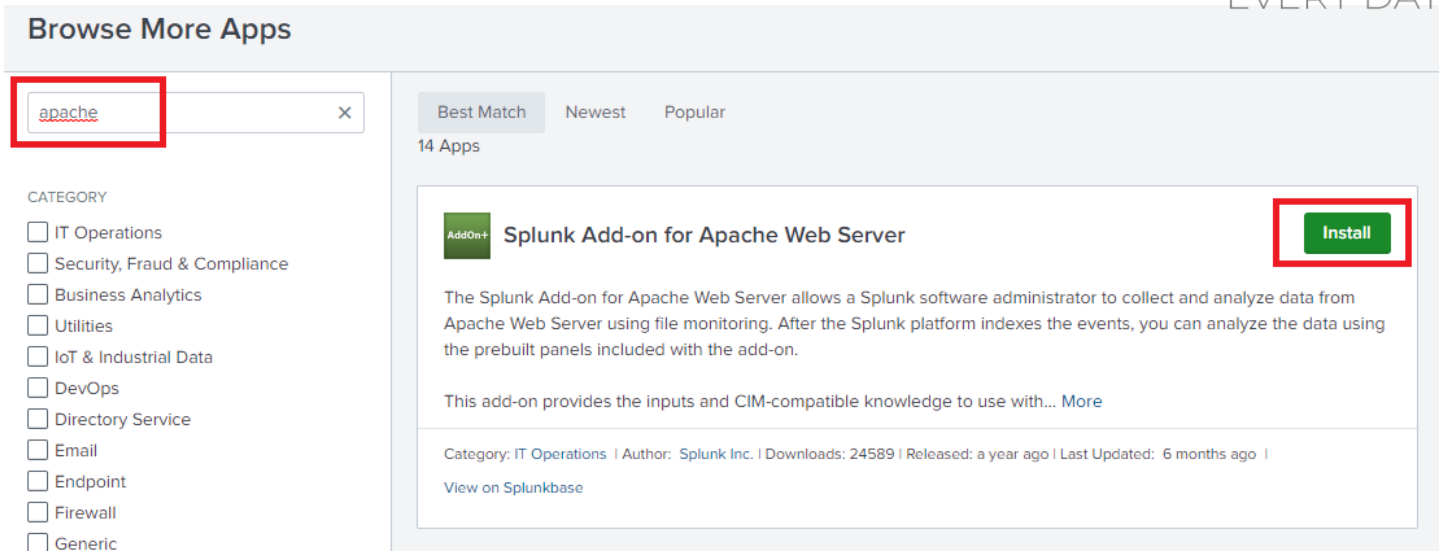


CONFIGURAR OS PARSINGS - APACHE

- Para fazer isso, acesse o Splunk e navegue até "Apps" e depois selecione "Find More Apps".

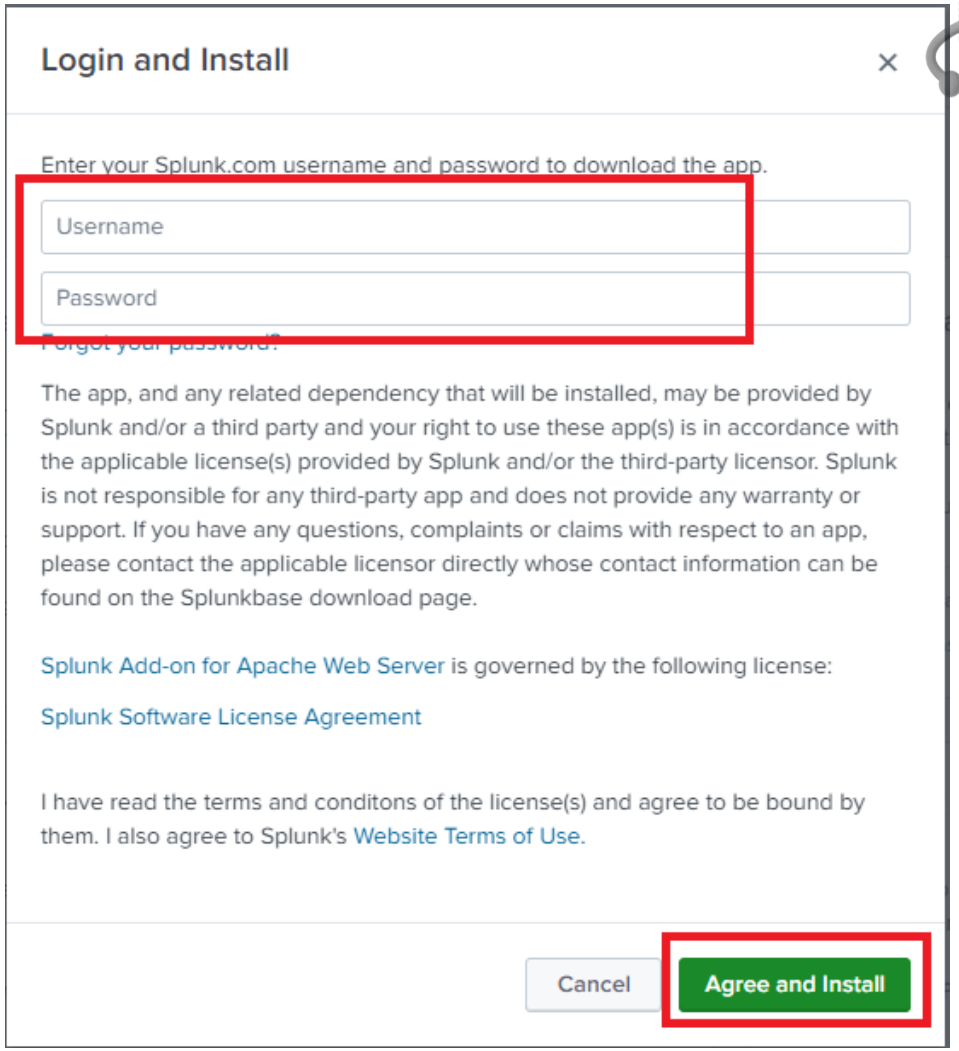
CONFIGURAR OS PARSINGS - APACHE

- Pesquisa por “apache” e clique em “Install” no “Splunk Add-on for Apache Web Server”



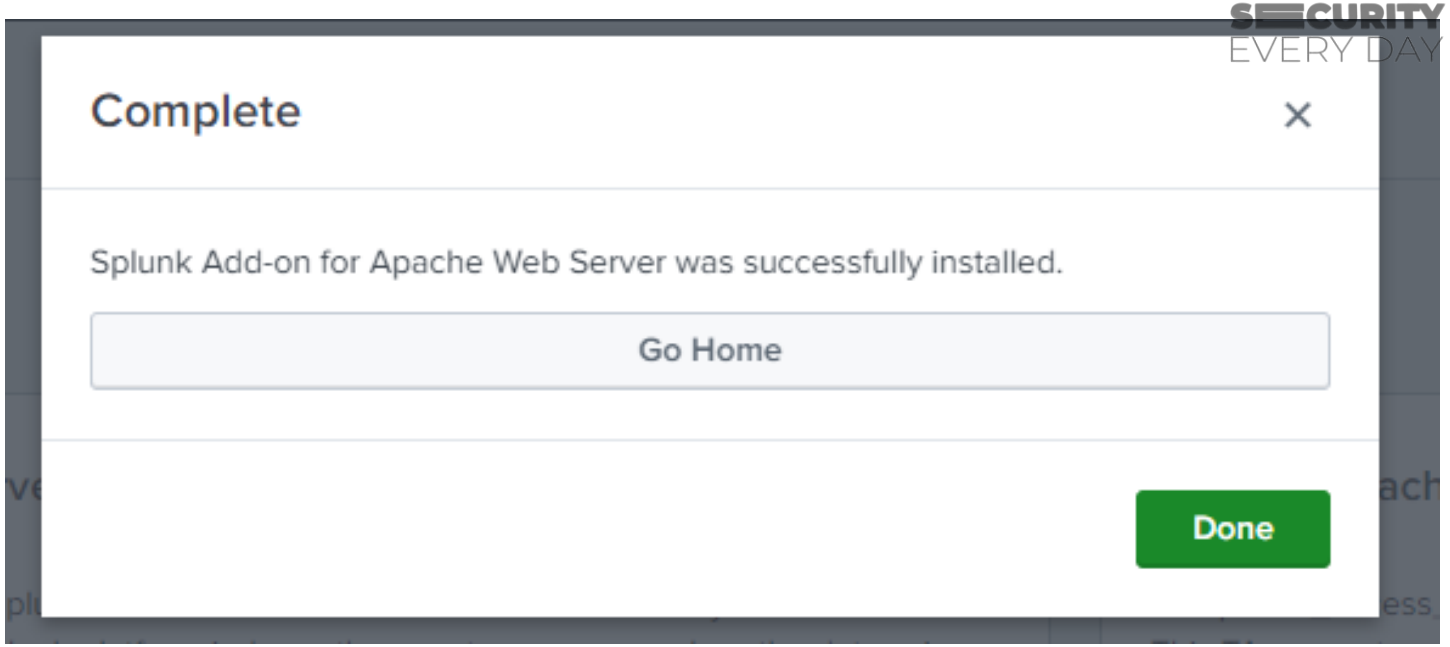
CONFIGURAR OS PARSINGS - APACHE

- Para instalar o add-on, é necessário possuir uma conta criada no site da Splunk. Depois de garantir que possui uma conta de usuário válida, você poderá prosseguir com a instalação. Basta clicar em "Agree and Install" para iniciar o processo de instalação do add-on no Splunk.
  - https://idp.login.splunk.com/signin/register



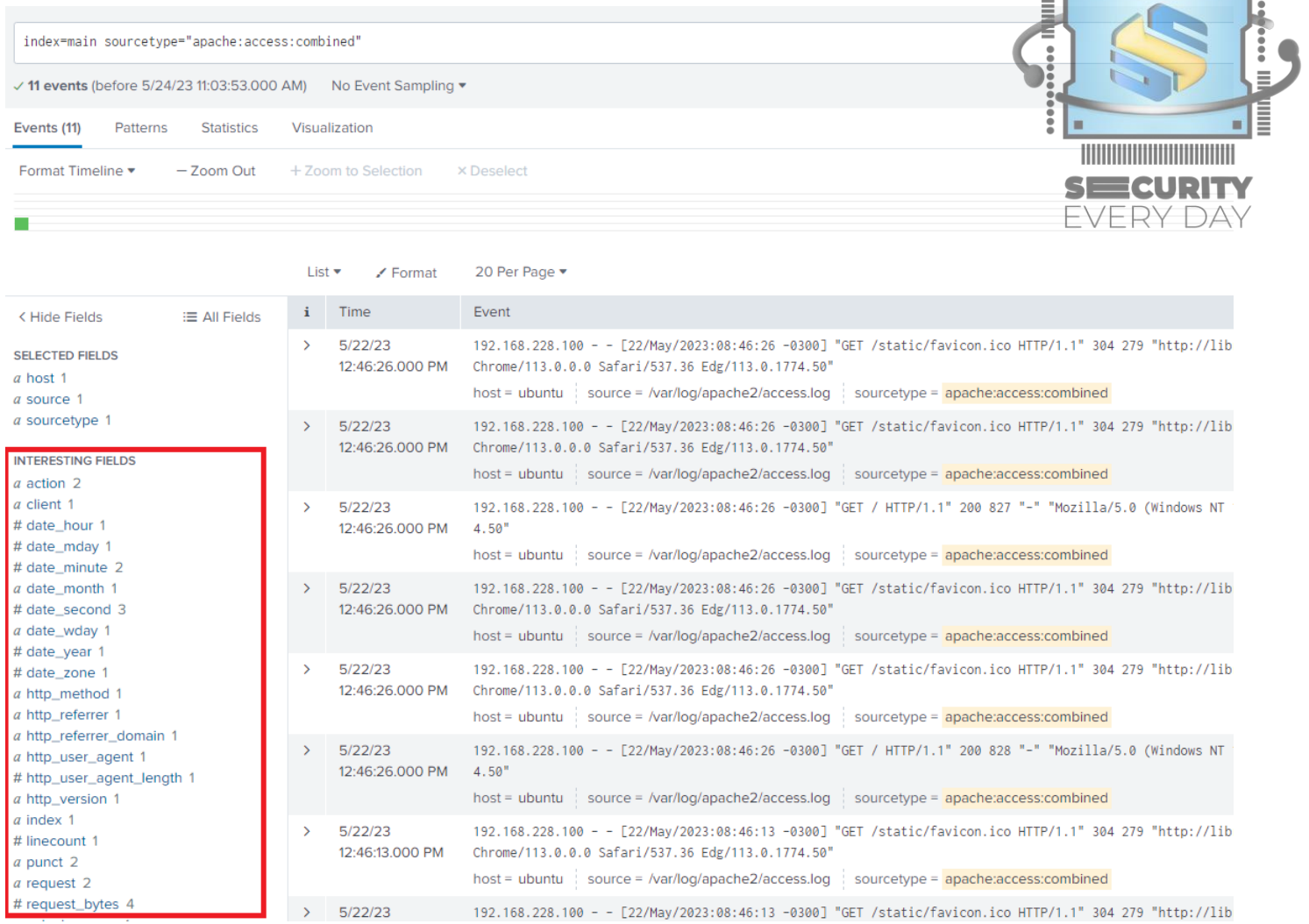
CONFIGURAR OS PARSINGS - APACHE

- Depois de instalado, basta clicar em “Done”



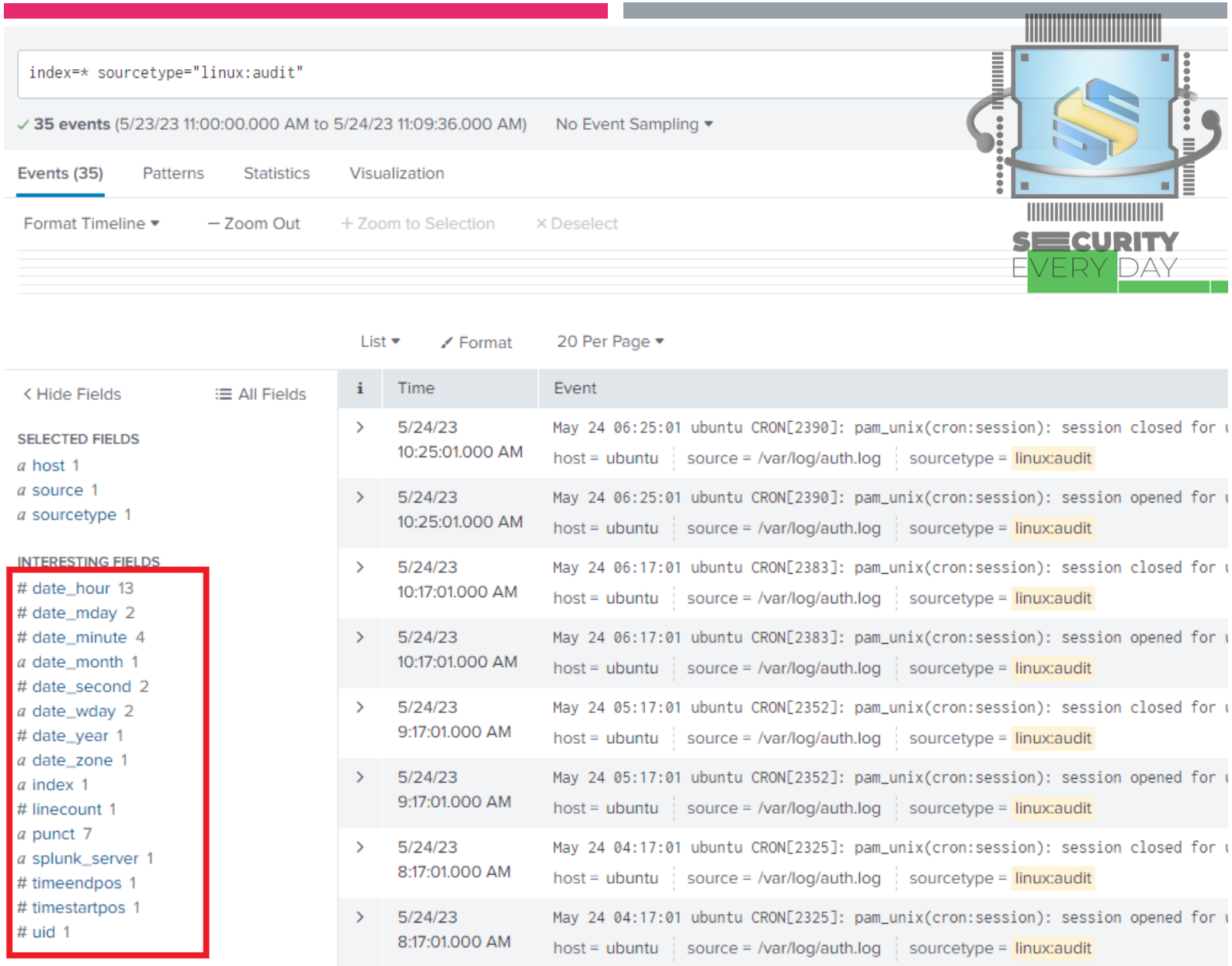
CONFIGURAR OS PARSINGS - APACHE

- Agora, ao executar a pesquisa **index=main sourcetype="apache:access:combined"** no Splunk, você notará que novos campos apareceram em "INTERESTING FIELDS". Esses campos foram gerados pelo add-on e correspondem aos valores presentes nos logs do Apache.



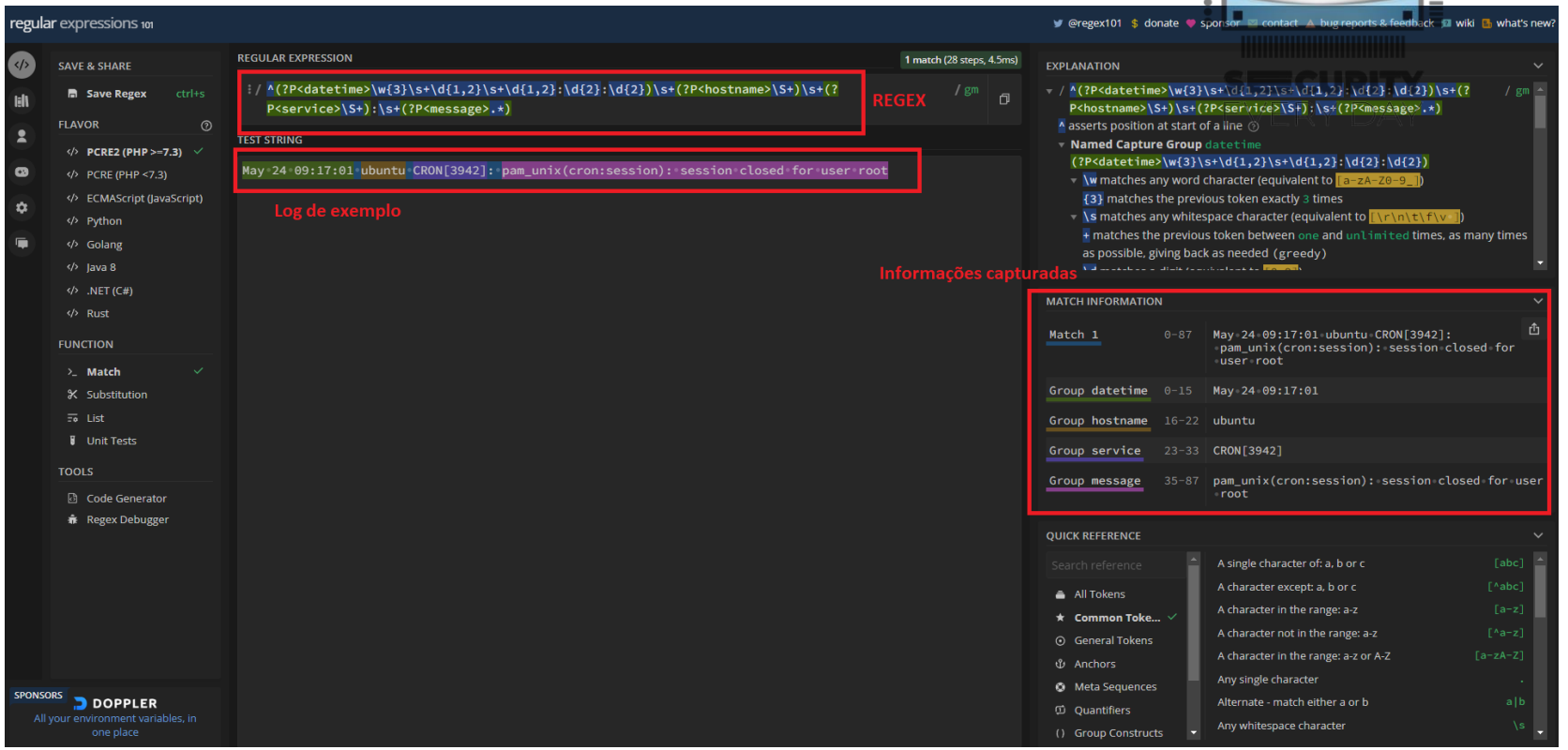
CONFIGURAR OS PARSINGS - LINUX

- Para os logs do /var/log/auth.log, vamos fazer algo diferente. Vamos criar nossos próprios regexs, para pegar as informações que queremos.



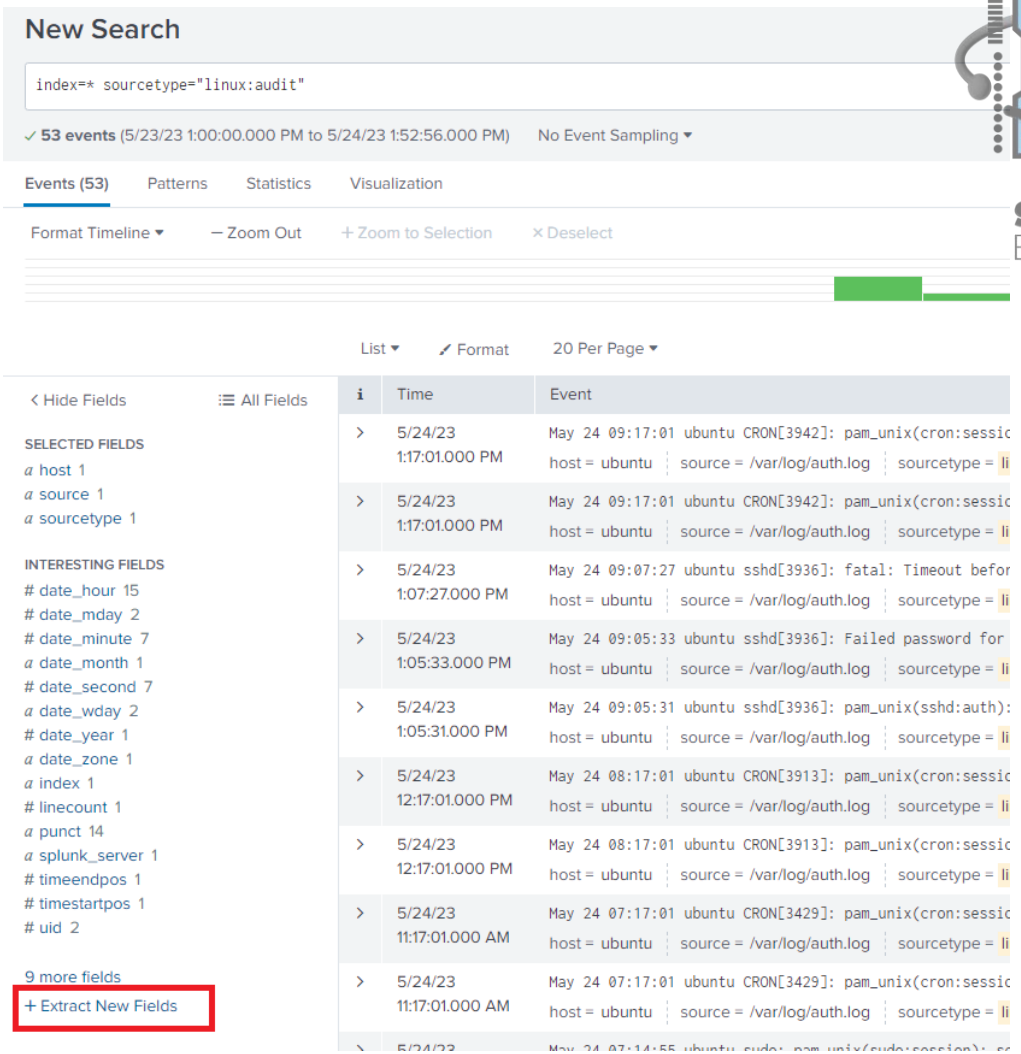
CONFIGURAR OS PARSINGS - LINUX

- Vamos desenvolver um regex básico para extrair as partes principais dos logs. Podemos pegar um exemplo de log e usar o site regex101.com para testar e ajustar nosso código regex.
  - REGEX
    - ^(?P<datetime>\w{3}\s+\d{1,2}\s+\d{1,2}:\d{2}:\d{2})\s+(?P<hostname>\S+)\s+(?P<service>\S+):\s+(?P<message>.*)



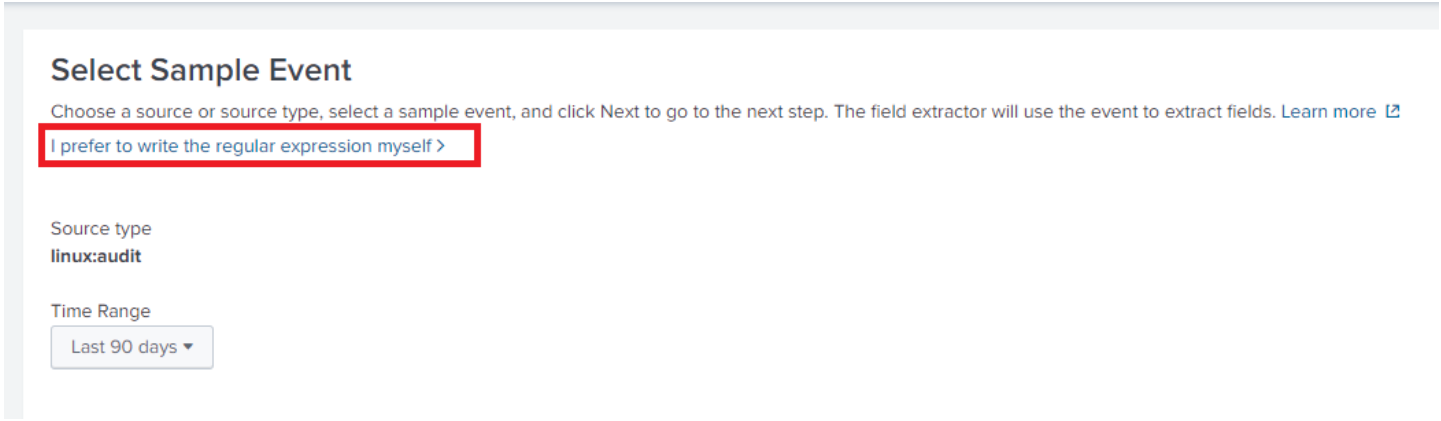
CONFIGURAR OS PARSINGS - LINUX

- Depois de criar o código regex, retorne ao Splunk e selecione a opção "Extract New Fields".



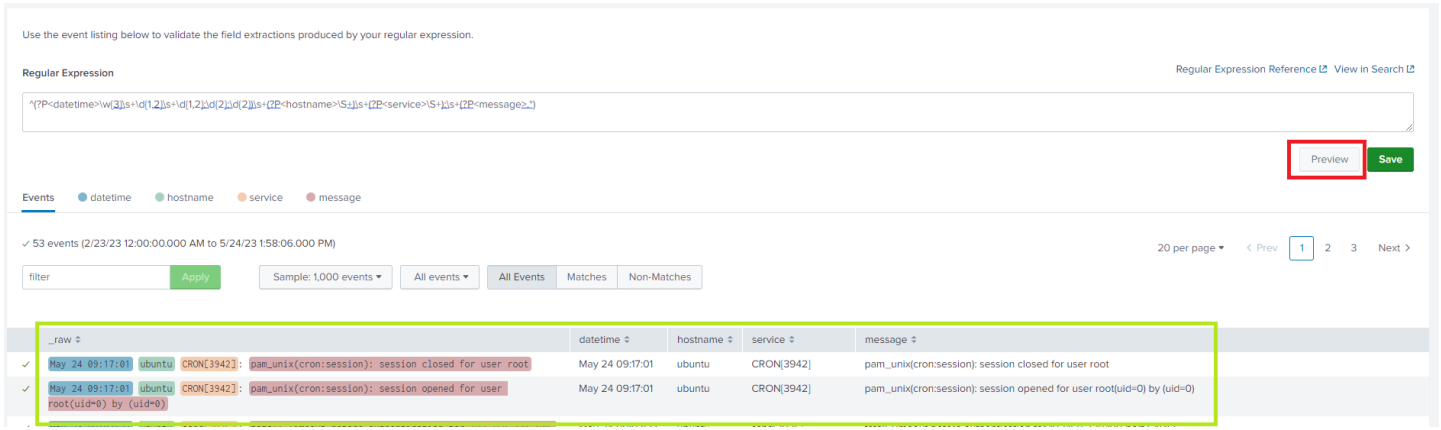
CONFIGURAR OS PARSINGS - LINUX

- Selecione a opção "I prefer to write the regular expression myself" e insira o código regex que criamos.



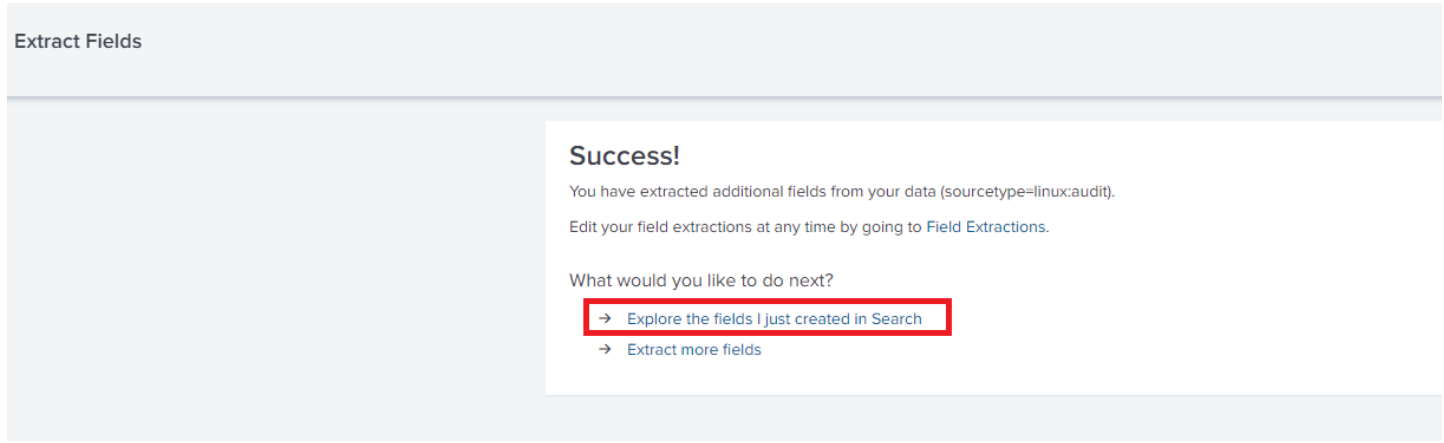
CONFIGURAR OS PARSINGS - LINUX

- Insira a expressão regular que criamos e clique em "Preview" para ter uma prévia de como os dados serão organizados depois do parsing.
- Depois, clique em “Save”



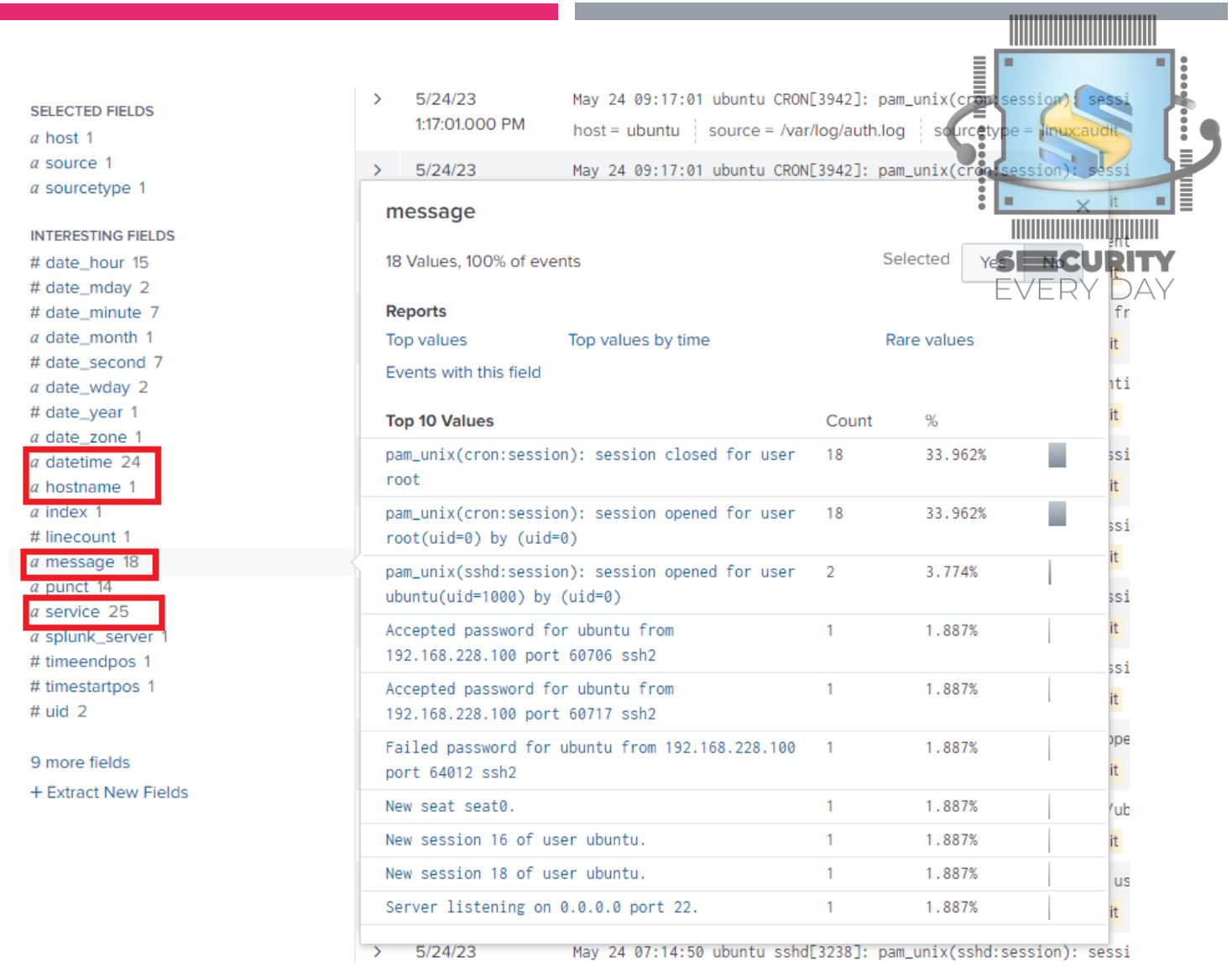
CONFIGURAR OS PARSINGS - LINUX

- clique em " Explore the fields I just created in Search".



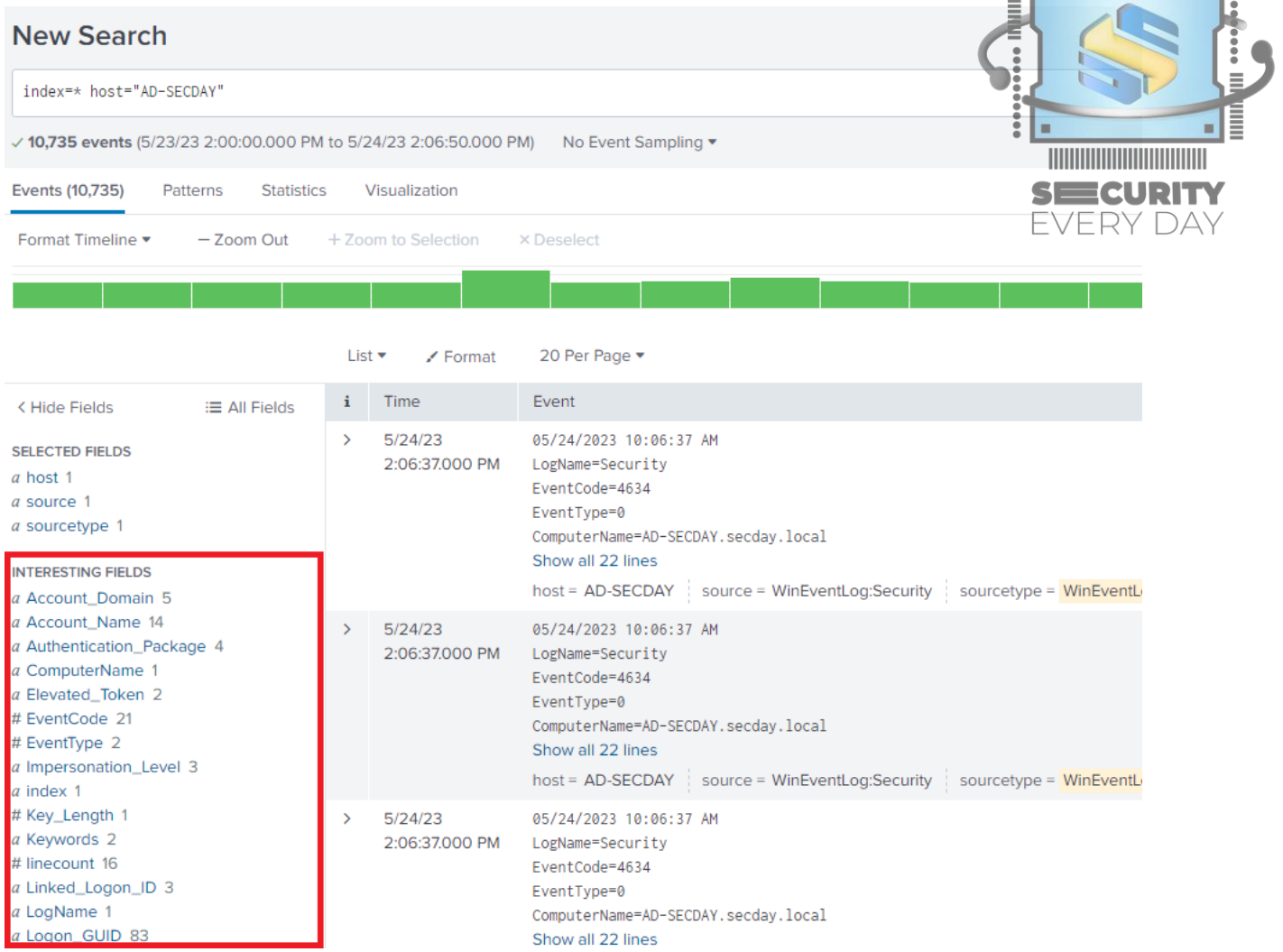
CONFIGURAR OS PARSINGS - LINUX

- Observe que agora os campos "datetime", "hostname", "service" e "message" estão preenchidos com as informações extraídas



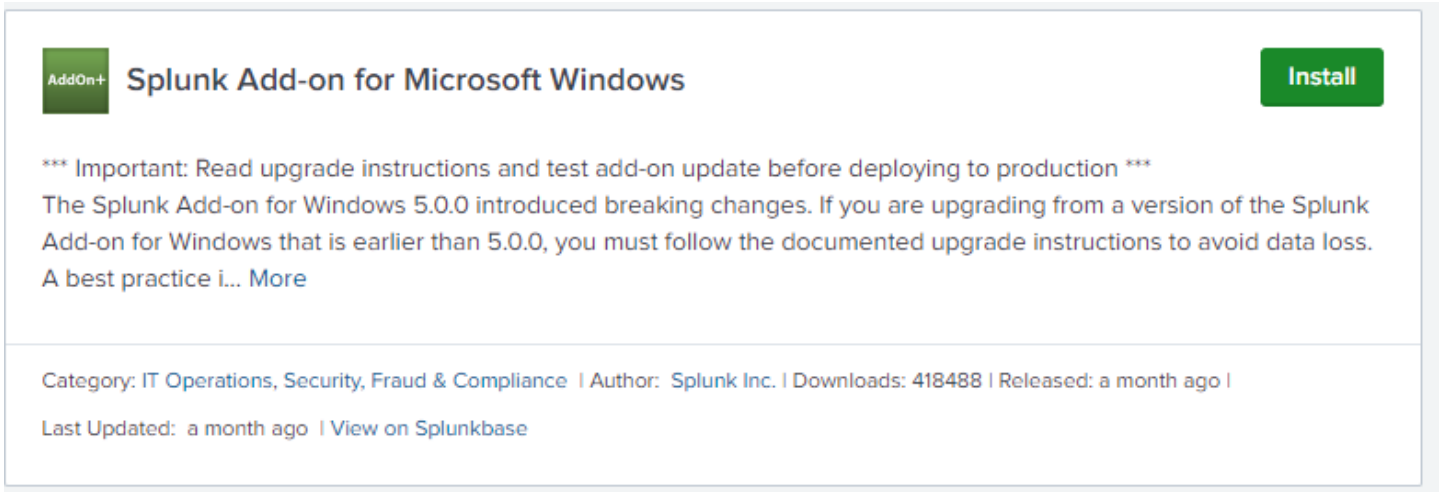
CONFIGURAR OS PARSINGS - WINDOWS

- O mesmo processo de instalação de add-on será realizado para os logs do Windows. Note que, por padrão, alguns campos já são extraídos automaticamente.



CONFIGURAR OS PARSINGS - WINDOWS

- Instale o add-on “Splunk Add-on for Microsoft Windows”

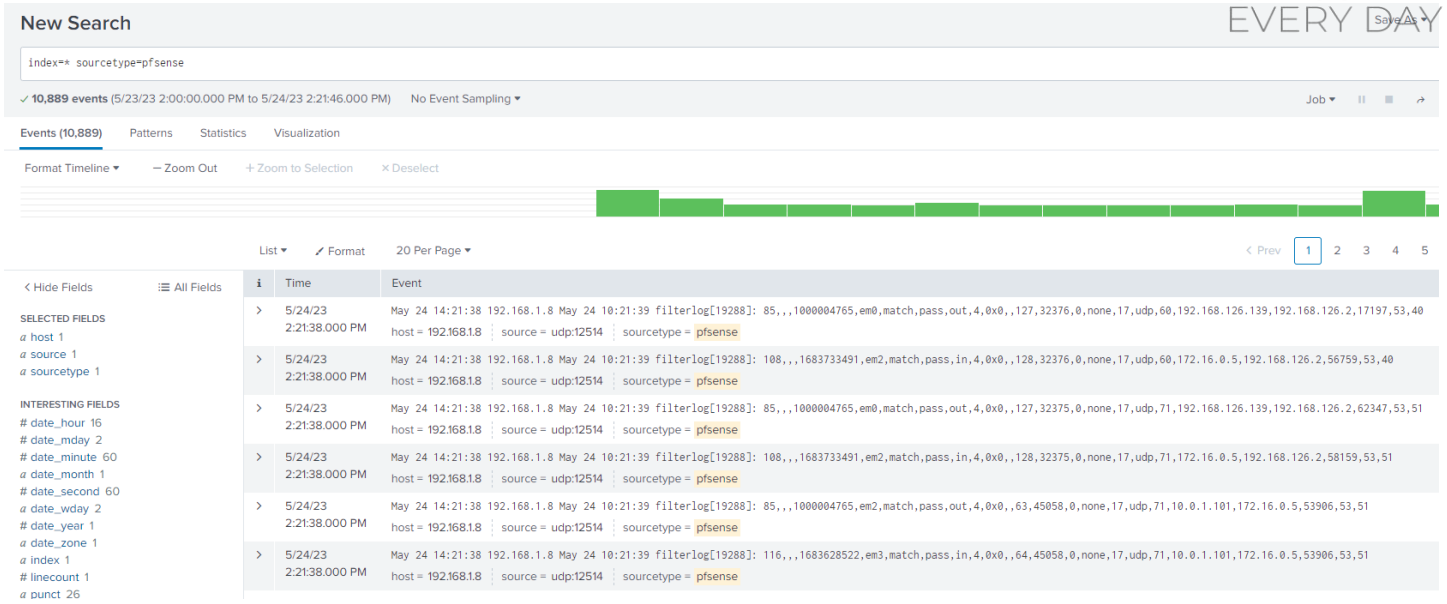


CONFIGURAR OS PARSINGS - WINDOWS

- Observe que, após a instalação do add-on, uma série de novos campos foram gerados no Splunk.

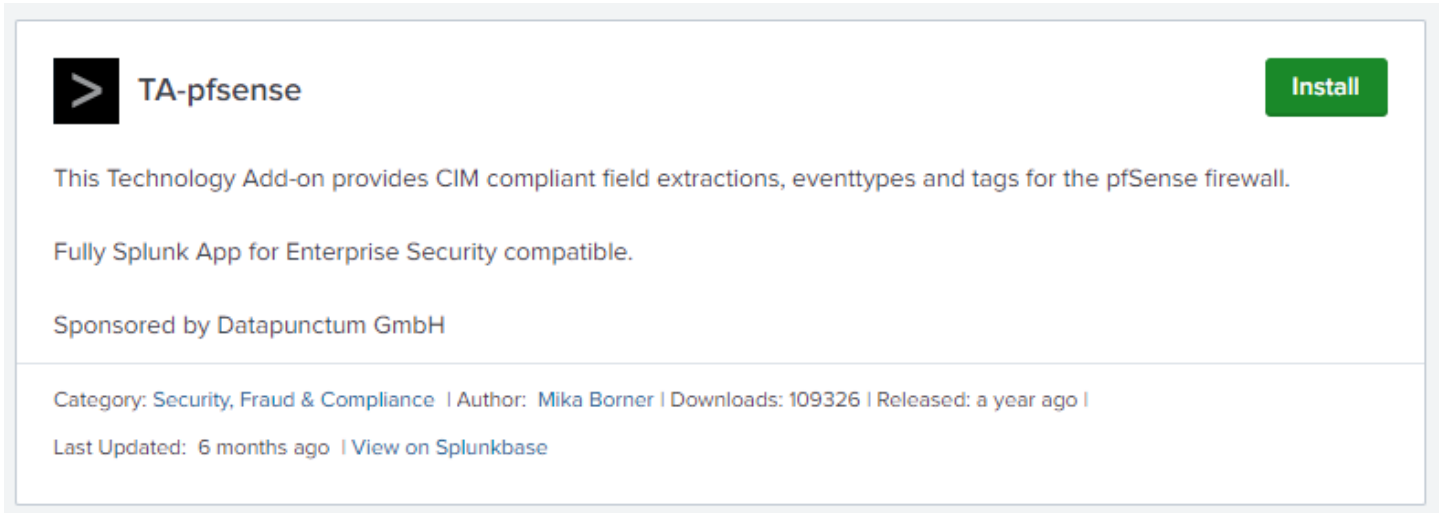
CONFIGURAR OS PARSINGS - PFSENSE

- O mesmo processo de instalação de add-on será realizado para os logs do Pfsense.



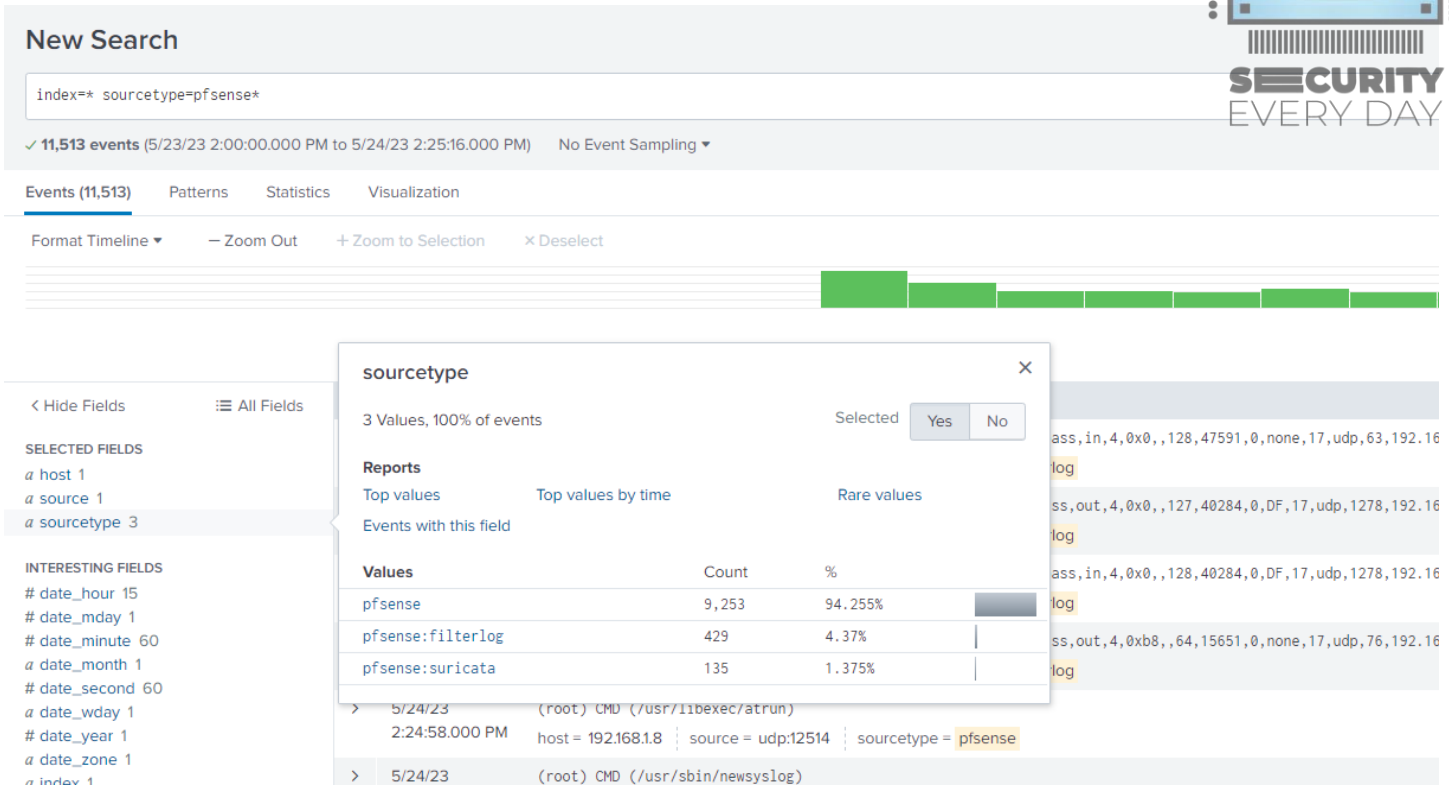
CONFIGURAR OS PARSINGS - PFSENSE

- Instale o add-on “TA-pfsense”



CONFIGURAR OS PARSINGS - PFSENSE

- Acesse o site google.com a partir de um computador na rede de colaboradores. Em seguida, realize uma nova pesquisa no Splunk, focando nos logs do pfsense. Você observará a geração de novos sourcetypes ao executar a **pesquisa index=* sourcetype=pfsense*.** Isso ocorre porque o add-on que instalamos categoriza e separa os diferentes tipos de logs provenientes do pfsense.



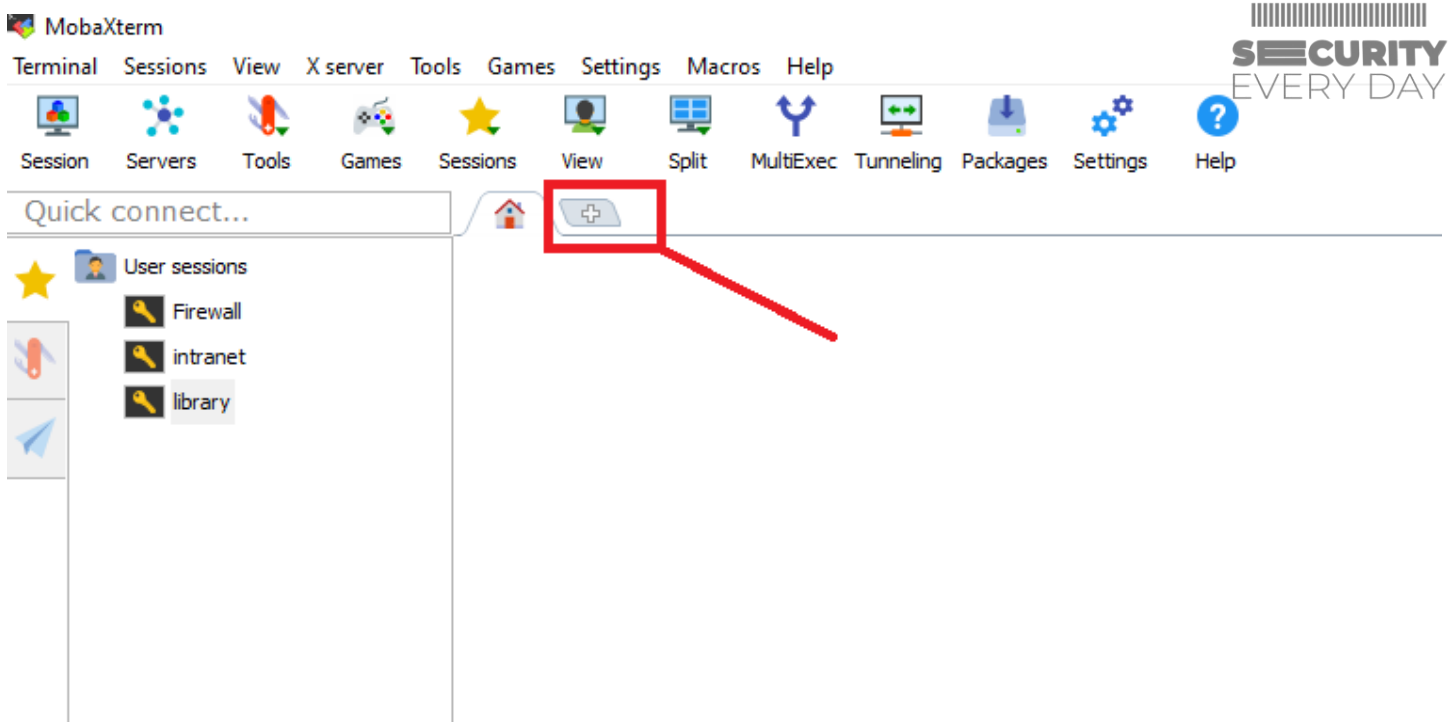
EXERCÍCIO DE PURPLE TEAM

SCAN DE PORTAS

- O comportamento básico de um scan de portas é quando um host estabelece várias conexões em diferentes portas de outro host. Isso é feito para identificar quais portas estão abertas, fechadas ou filtradas, é uma técnica comumente utilizada para enumeração de serviços.

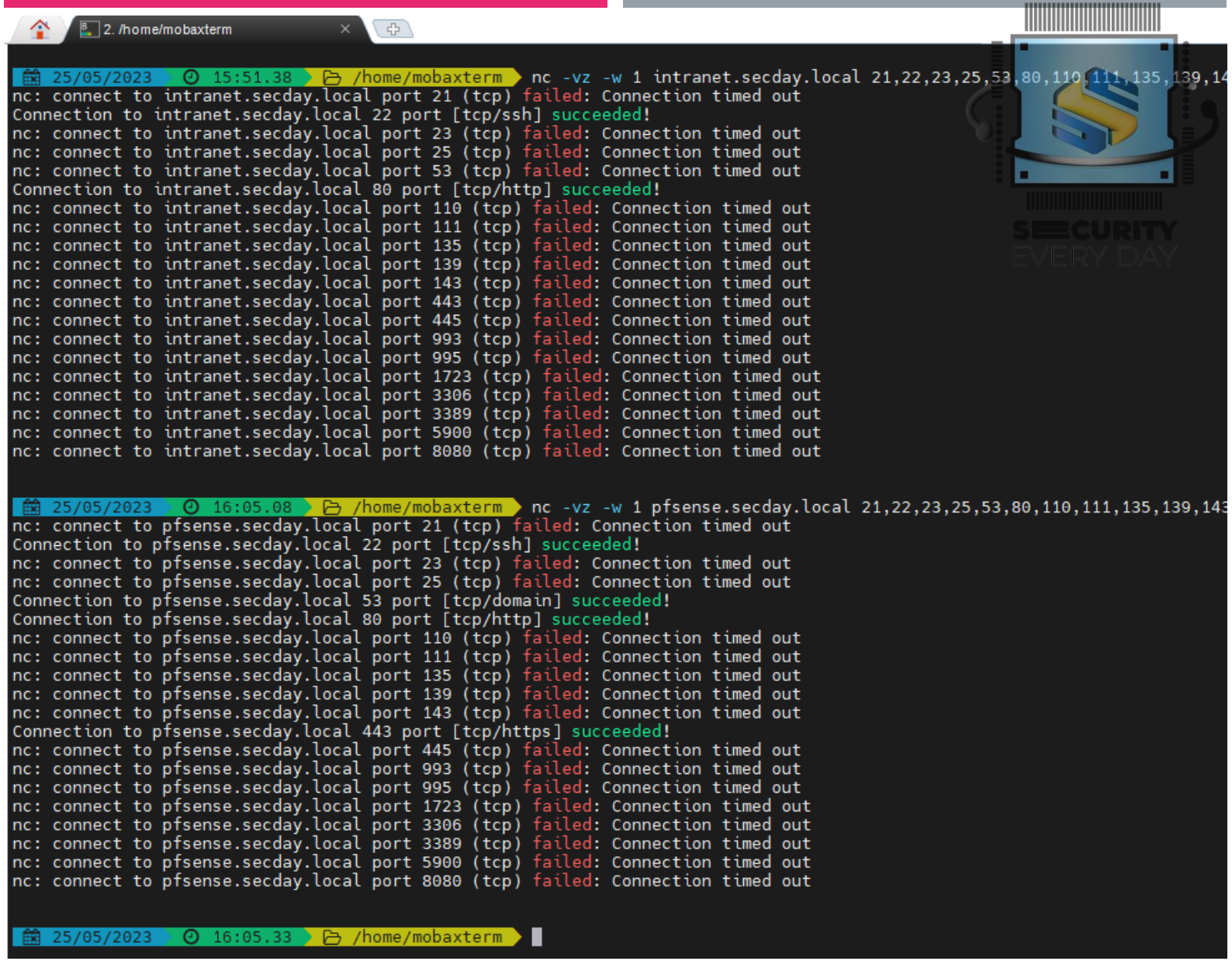
SCAN DE PORTAS - ATAQUE

- Vamos iniciar o primeiro teste com um scan de portas para verificar nossa capacidade de detectar enumerações de portas no ambiente. Para começar, acesse a máquina "Windows 10 - Colaboradores", abra o "MobaxTerm" e clique no botão "+" para abrir um novo terminal



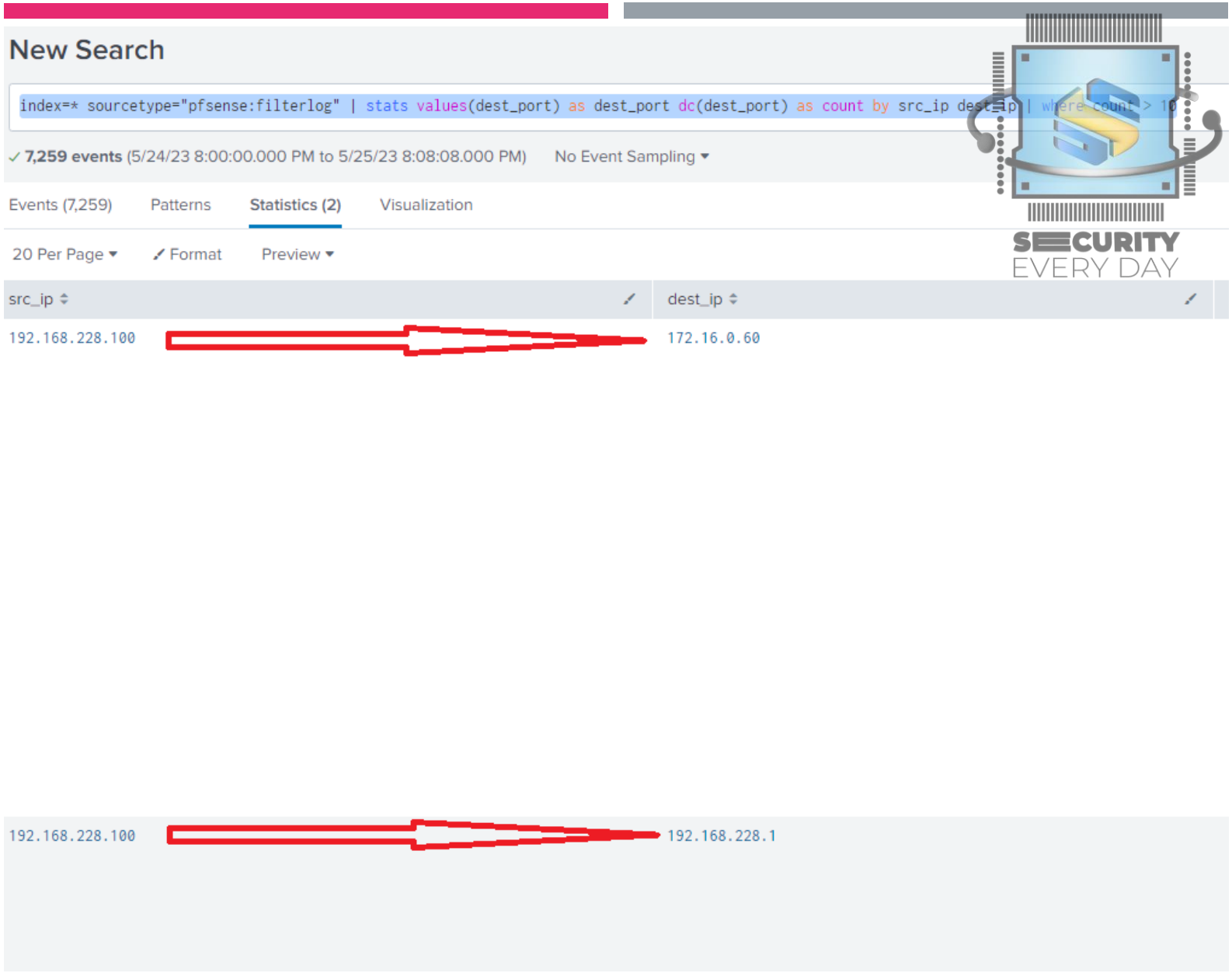
SCAN DE PORTAS - ATAQUE

- Execute os dois comandos abaixo para enumerar as 20 top portas
  - nc -vz -w 1 intranet.secday.local 21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080
  - nc -vz -w 1 pfsense.secday.local 21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080



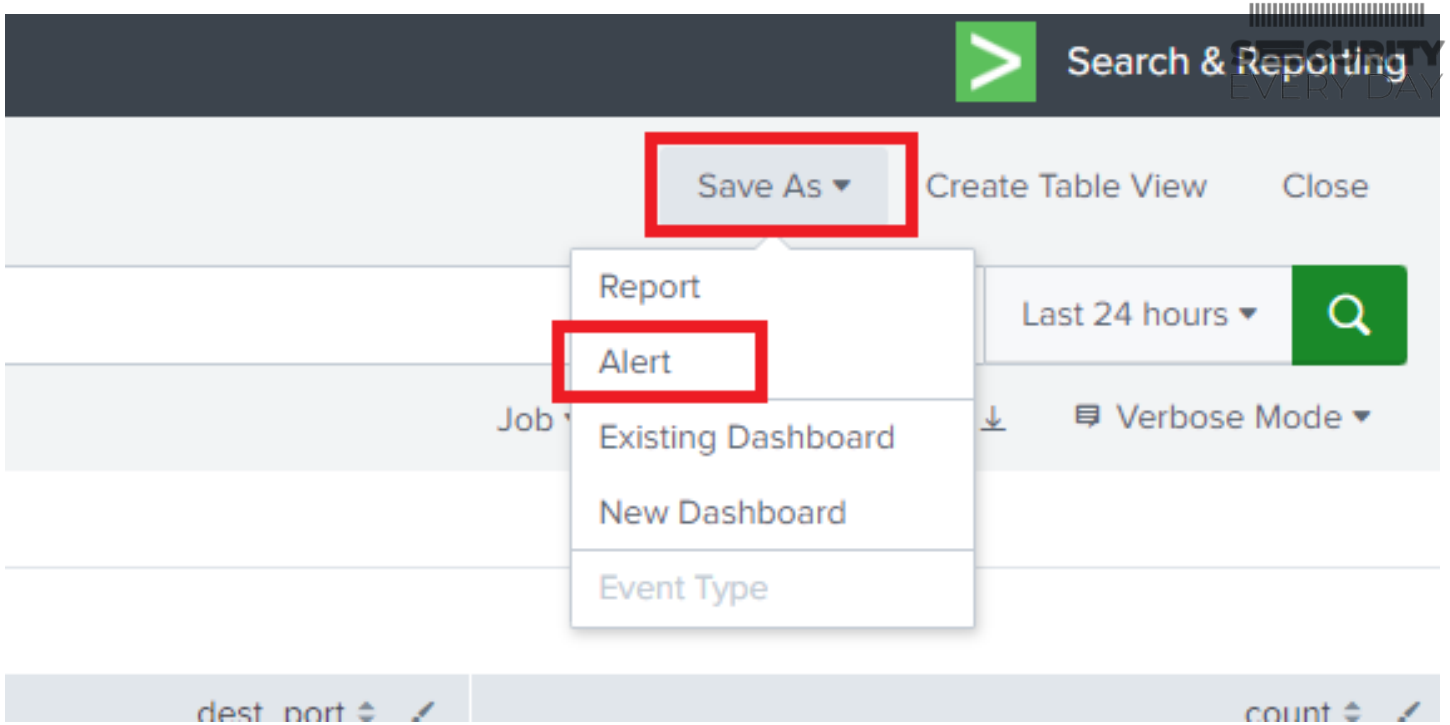
SCAN DE PORTAS – REGRA

- Para identificar os logs no Splunk e criar uma regra para detectar o comportamento desejado, você pode executar o seguinte código:
  - index=* sourcetype="pfsense:filterlog" | stats values(dest_port) as dest_port dc(dest_port) as count by src_ip dest_ip | where count > 10
- Dessa forma, será possível analisar os testes realizados e implementar a regra para detectar o comportamento.



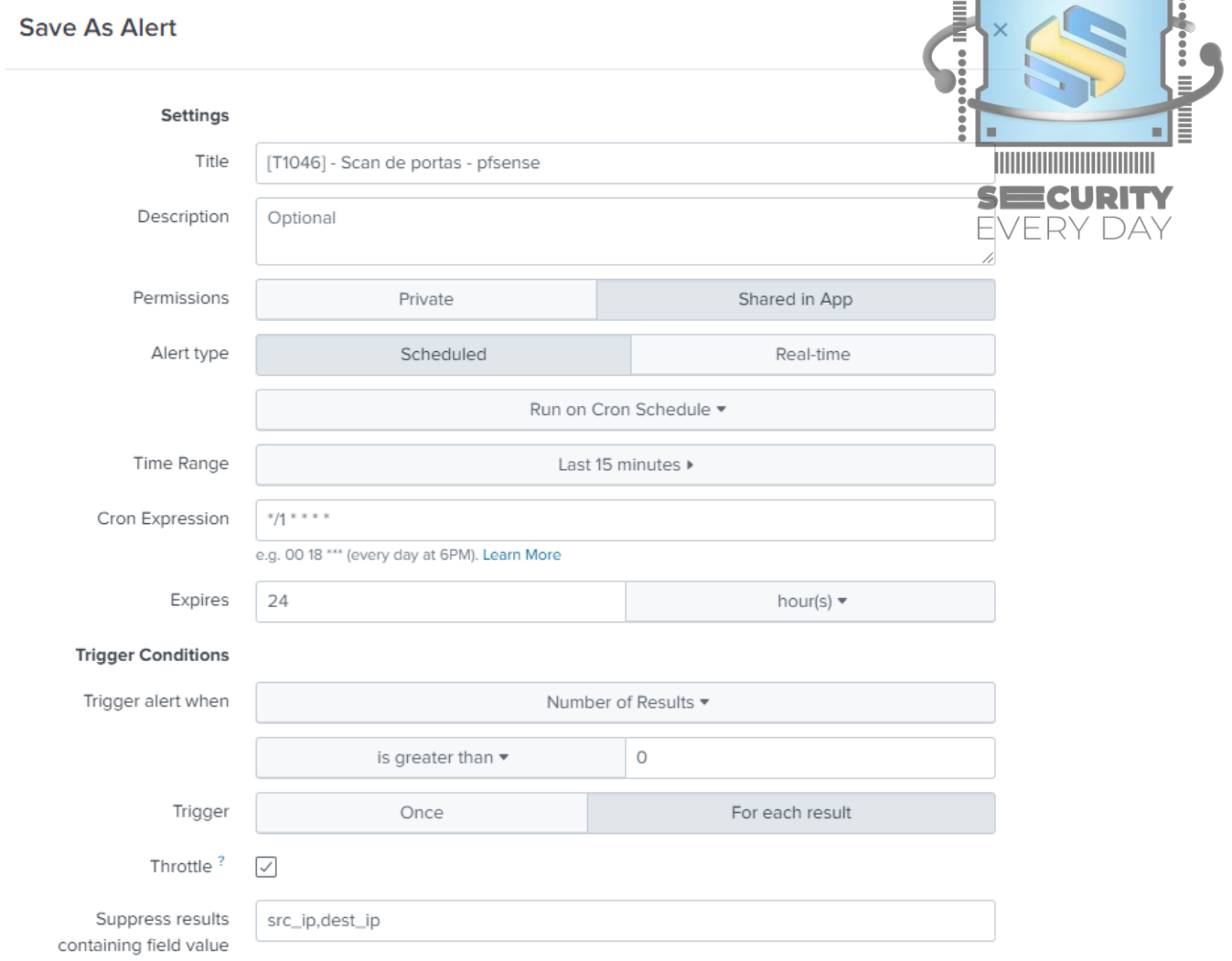
SCAN DE PORTAS - REGRA

- Após executar o código e identificar os testes realizados, clique em “Save As → Alert” para criar a regra



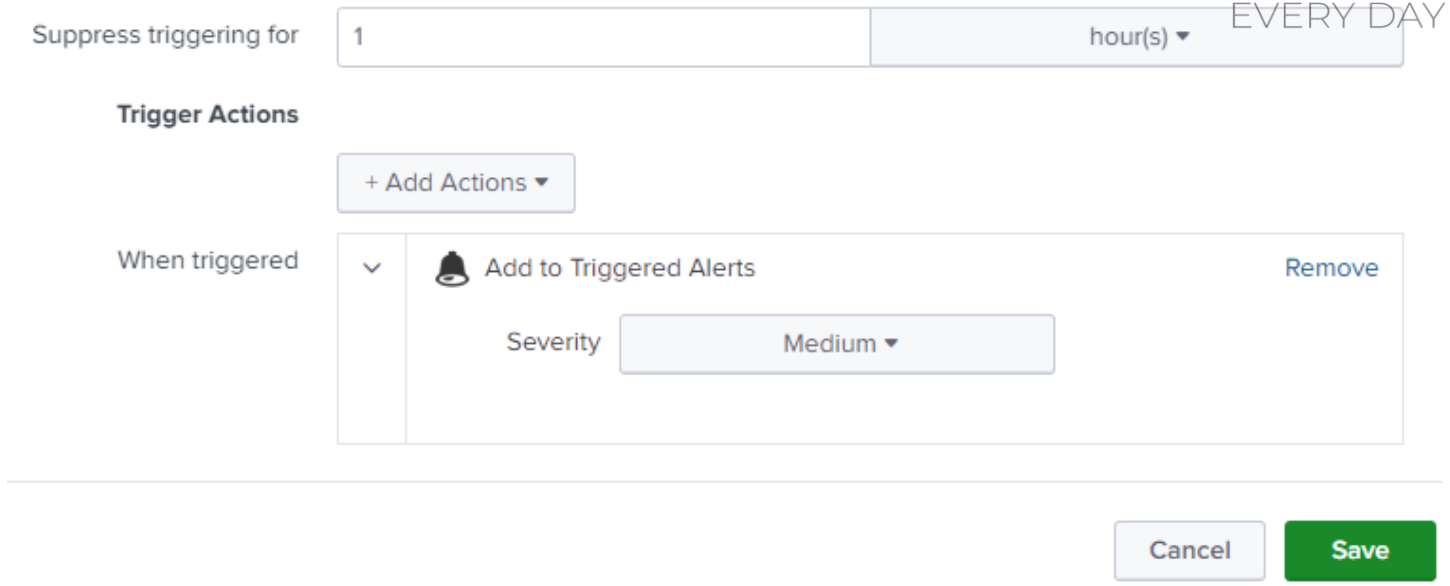
SCAN DE PORTAS - REGRA

- Preencha os campos conforme à imagem



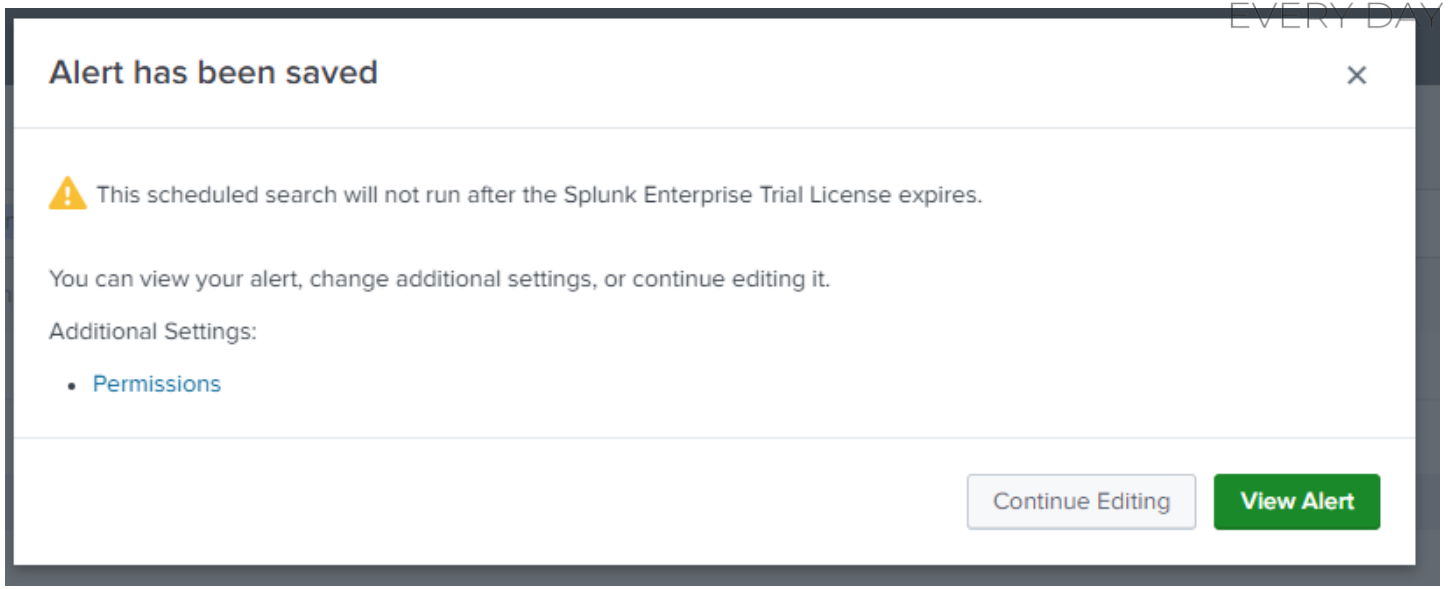
SCAN DE PORTAS - REGRA

- Finalize o preenchimento e clique em “Save”



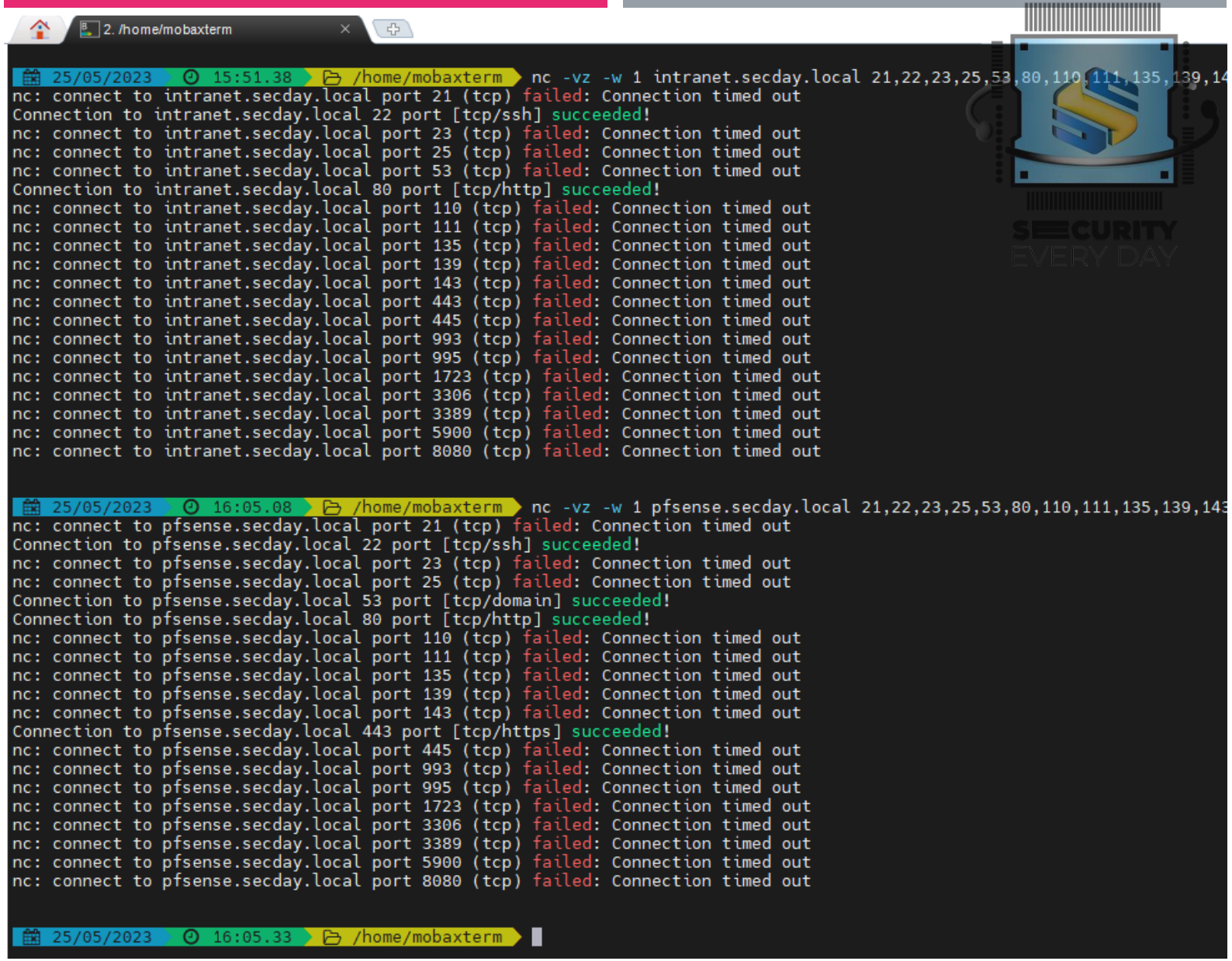
SCAN DE PORTAS - REGRA

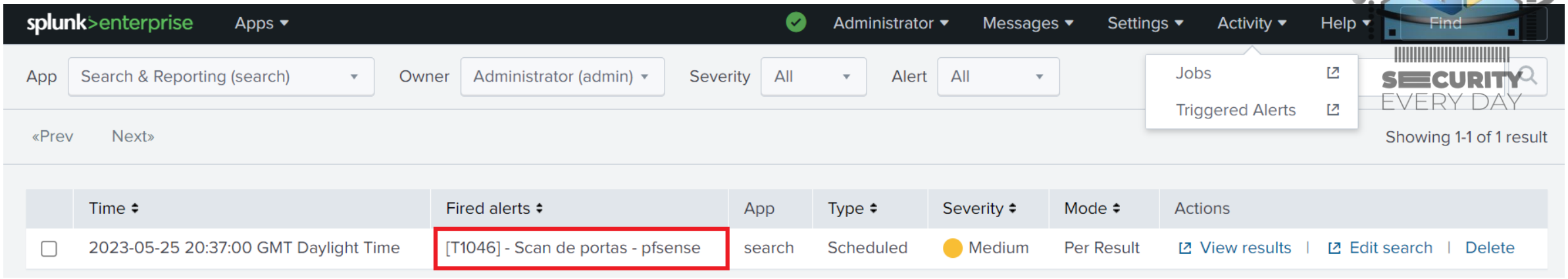
- Selecione a opção "View Alert" e, voilà, a regra será criada. vamos executar um novo "ataque" para verificar se a regra será devidamente acionada.



SCAN DE PORTAS - TESTE DE EFETIVIDADE

- Vamos executar novamente os comandos para enumerar as portas
  - nc -vz -w 1 intranet.secday.local 21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080
  - nc -vz -w 1 pfsense.secday.local 21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,5900,8080





SCAN DE PORTAS - TESTE DE EFETIVIDADE

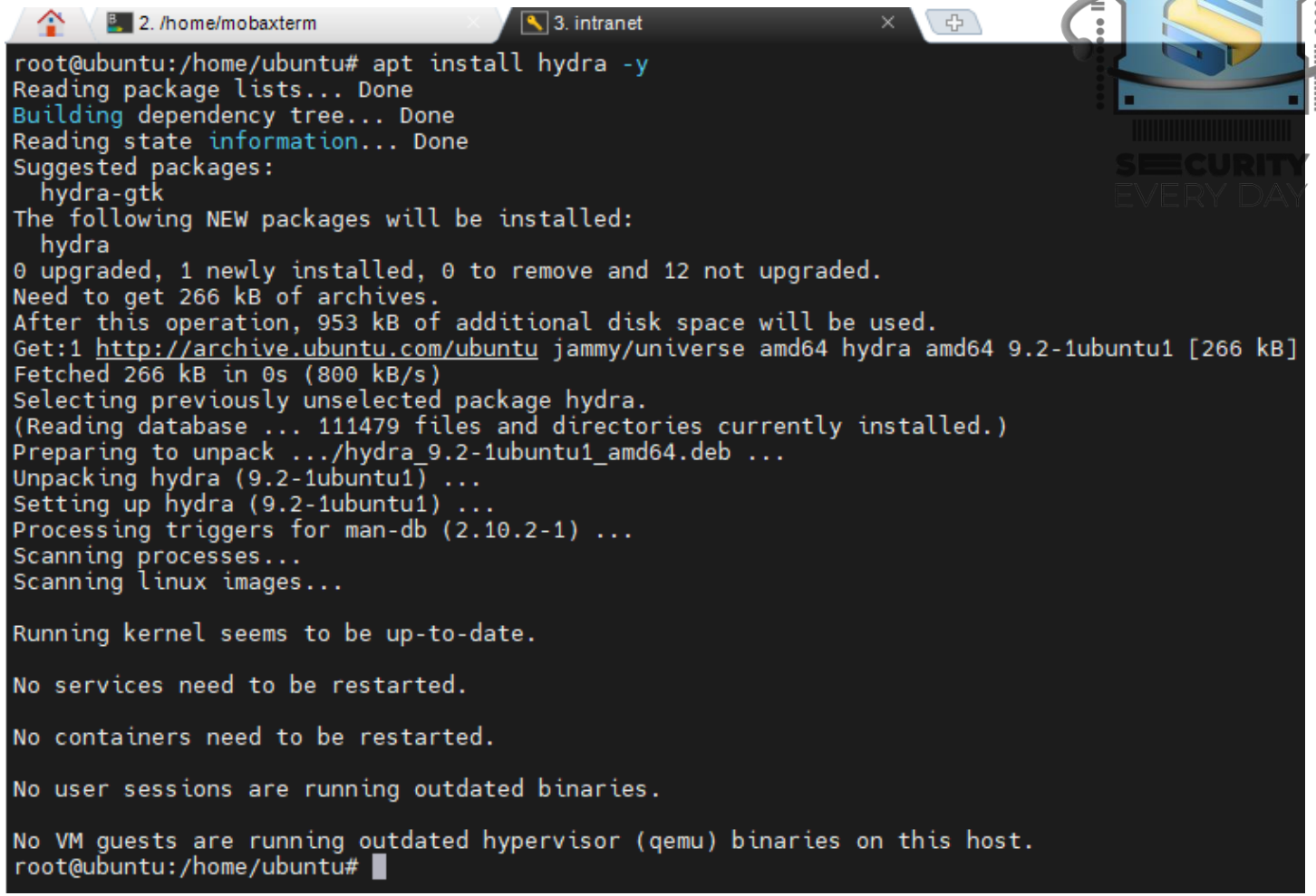
- Após executar os testes, acesse o Splunk e navegue até "Activity -> Triggered Alerts". Se a regra estiver funcionando corretamente, você deverá visualizar um alerta correspondente.
- **Obs**: Para confirmar se o resultado está alinhado com o esperado, simplesmente clique na opção "View results".

BRUTE FORCE

- O comportamento de um ataque de Brute Force se caracteriza por um grande número de tentativas de login mal-sucedidas. Esta ação é sistematicamente repetida, às vezes milhares de vezes por segundo, dependendo da capacidade do hardware utilizado pelo atacante.

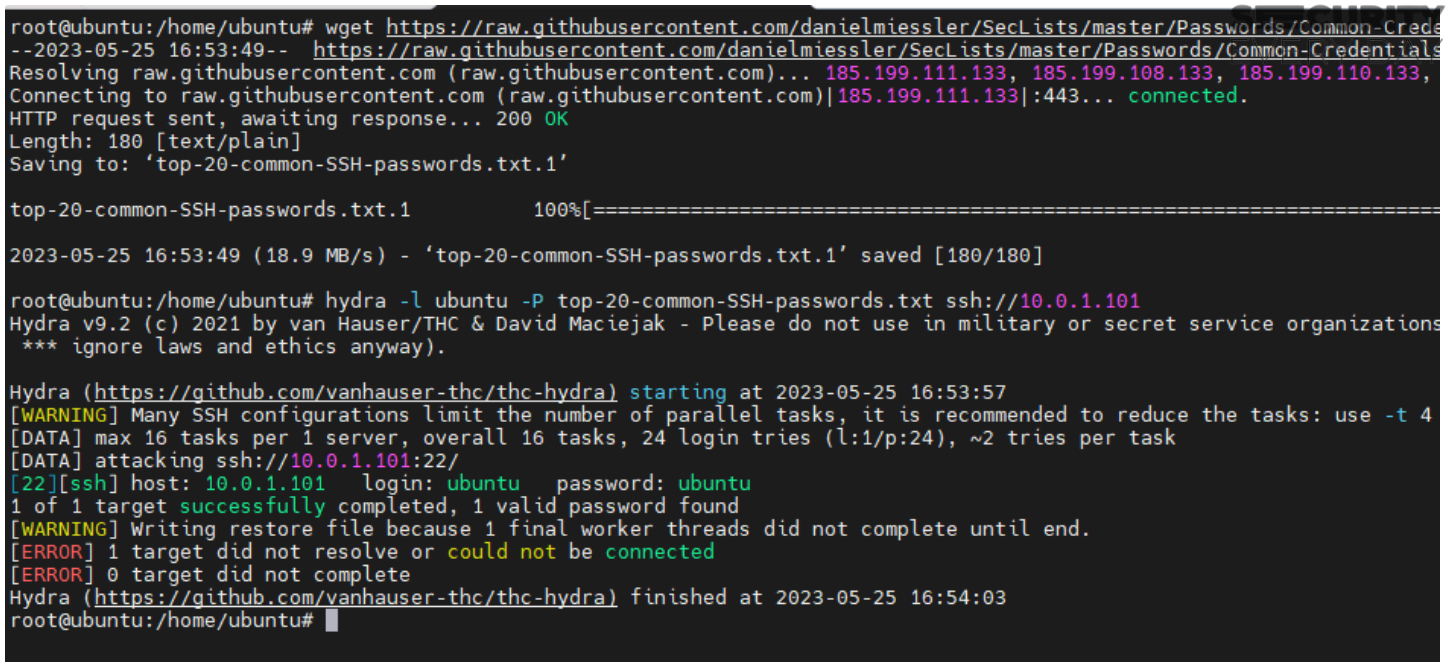
BRUTE FORCE - ATAQUE

- Acesse a maquina “intranet” via SSH e prossiga com a instalação do Hydra executando o seguinte comando
  - apt install hydra -y



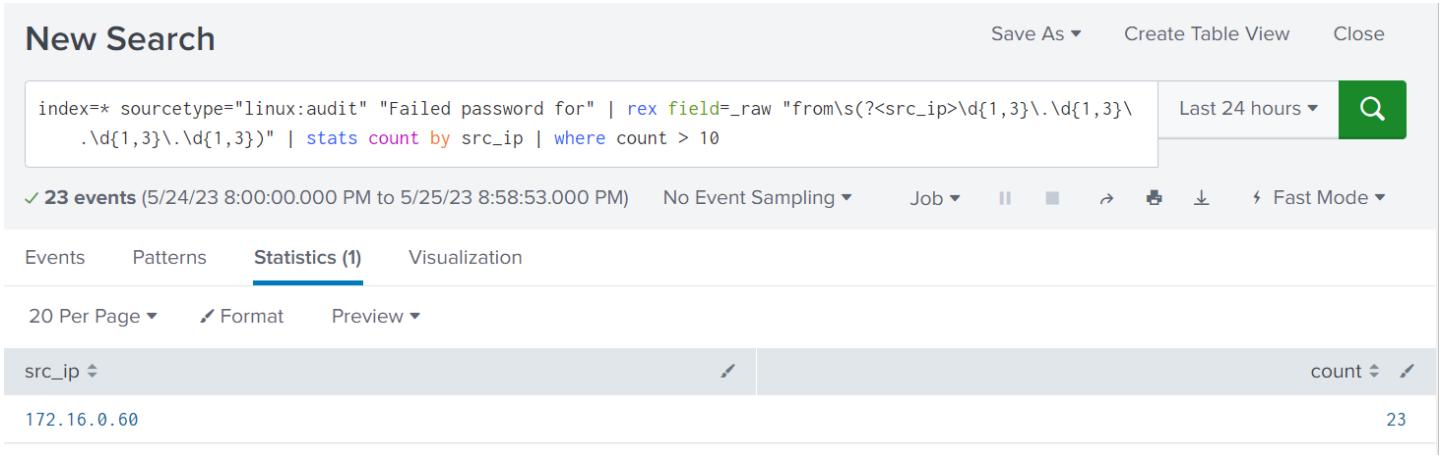
BRUTE FORCE - ATAQUE

- A seguir, execute os comandos abaixo para realizar um ataque de força bruta no SSH do servidor “library”
  - wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt
  - hydra -l ubuntu -P top-20-common-SSH-passwords.txt ssh://10.0.1.101
- **Obs**: adicione a senha ”ubuntu” no final do arquivo top-20-common-SSH-passwords.txt



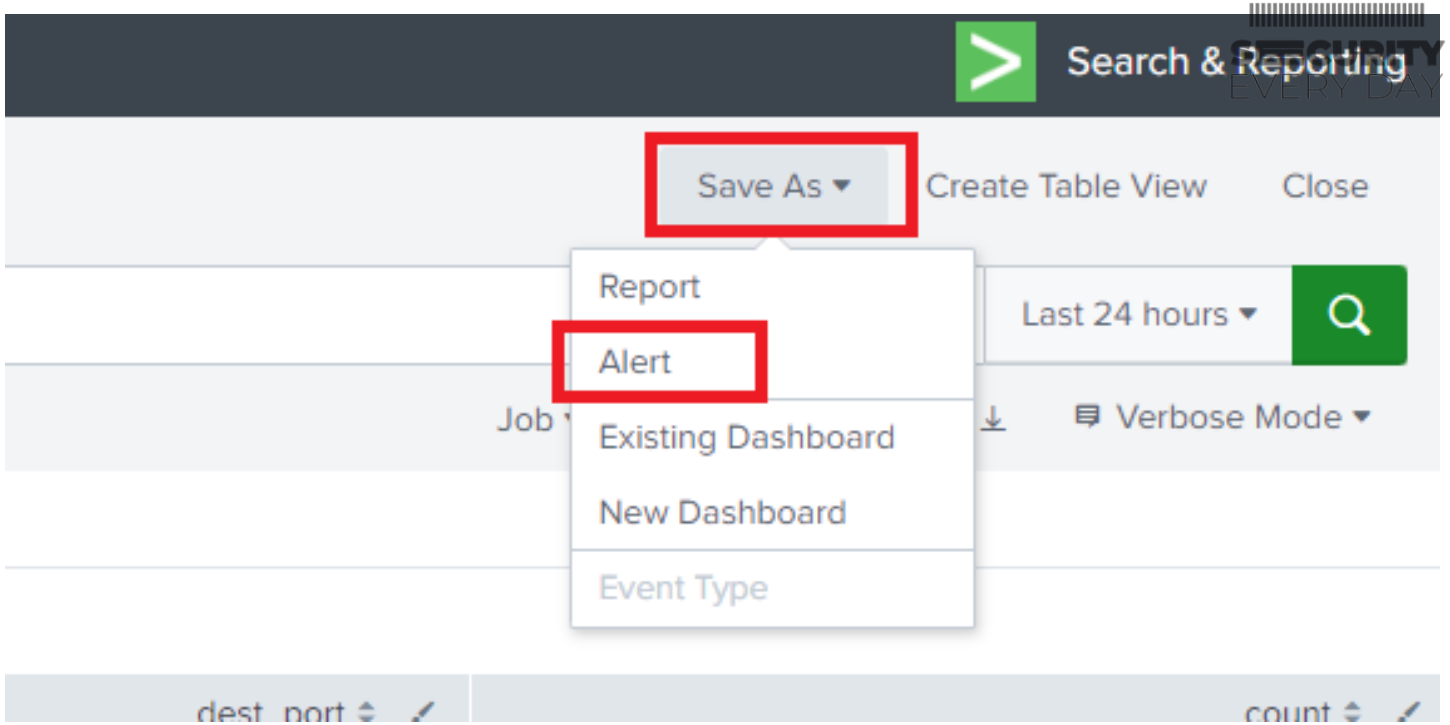
BRUTE FORCE – REGRA

- Novamente, para identificar os logs no Splunk e criar a regra, execute o seguinte código:
  - index=* sourcetype="linux:audit" "Failed password for" | rex field=_raw "from\s(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | stats count by src_ip | where count > 10



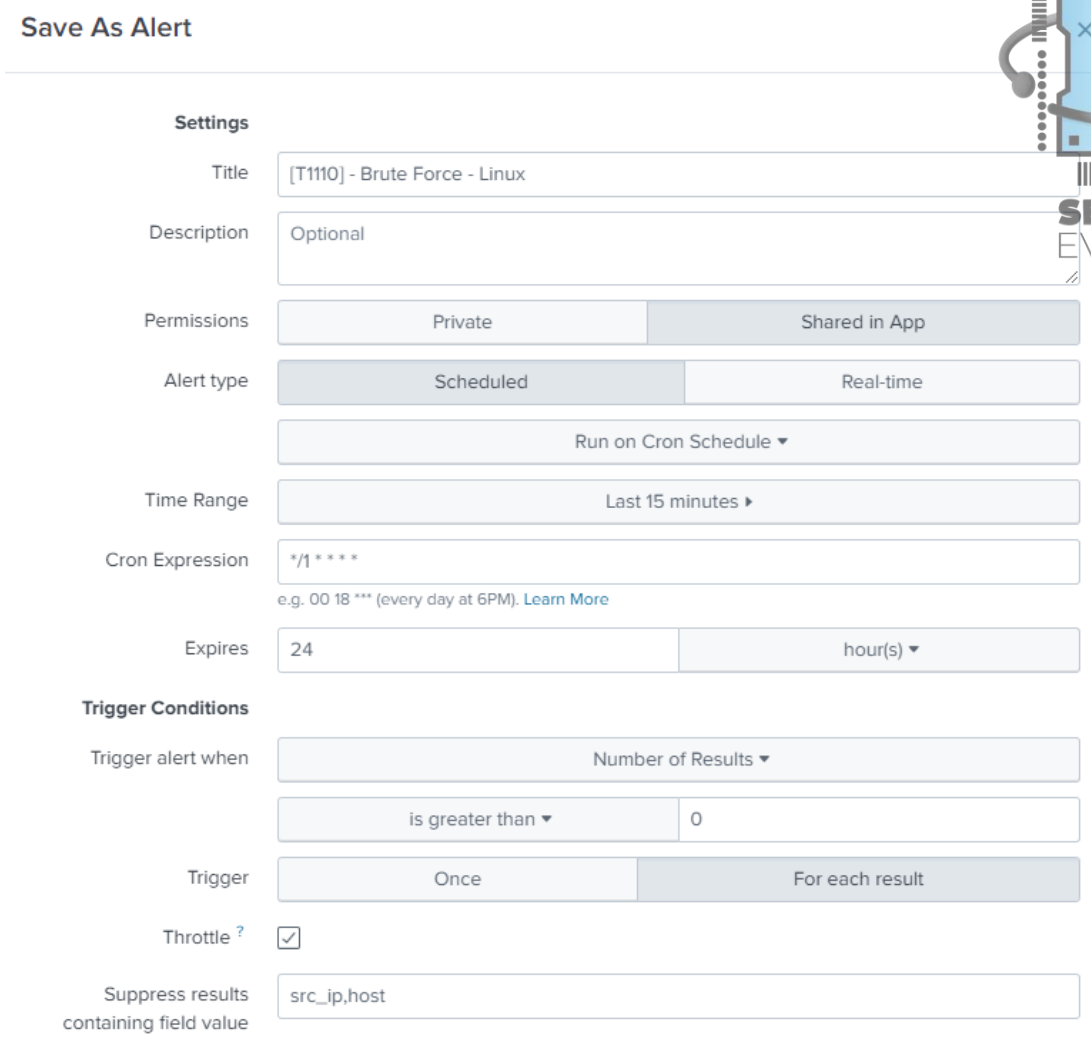
BRUTE FORCE - REGRA

- Após executar o código e identificar os testes realizados, clique em “Save As → Alert” para criar a regra



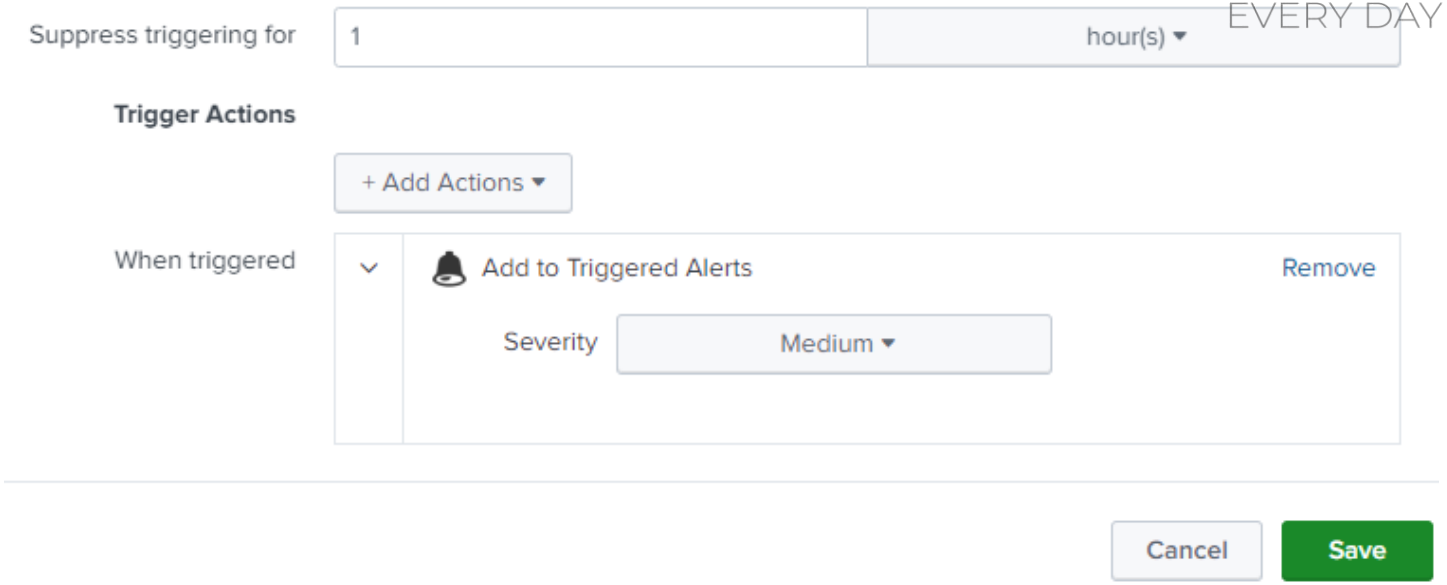
BRUTE FORCE - REGRA

- Preencha os campos conforme à imagem



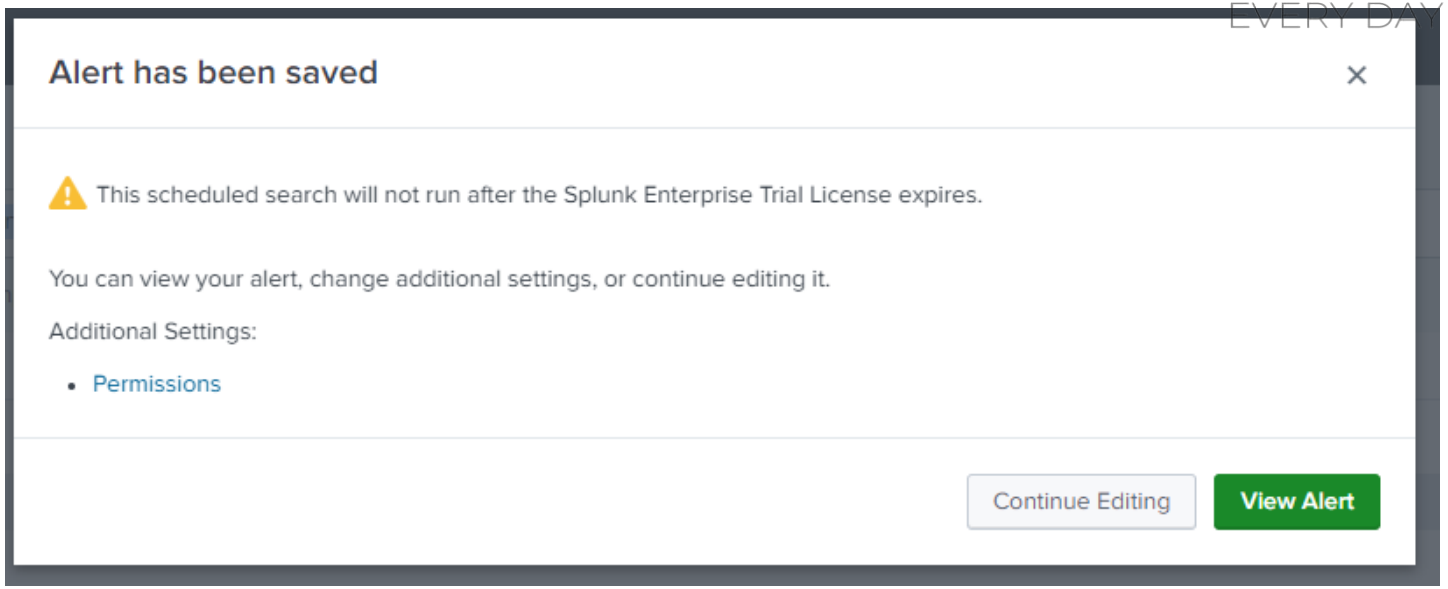
BRUTE FORCE - REGRA

- Finalize o preenchimento e clique em “Save”



BRUTE FORCE-REGRA

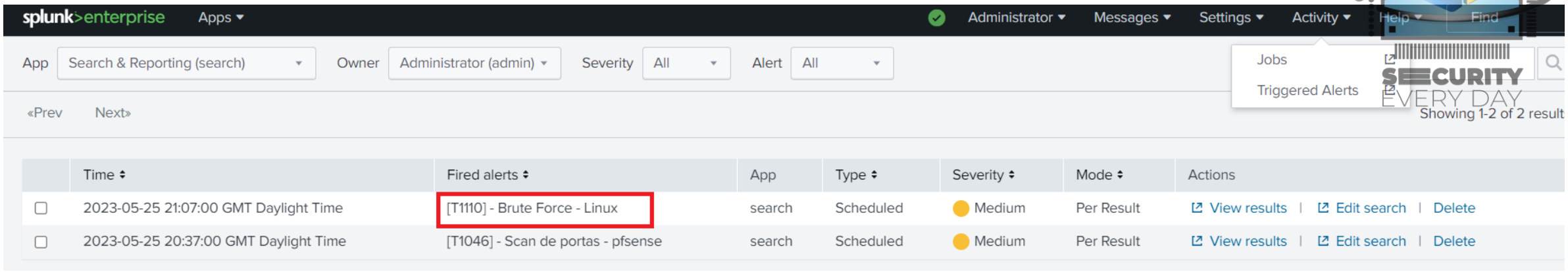
- Selecione a opção "View Alert" e, voilà, a regra será criada. vamos executar um novo "ataque" para verificar se a regra será devidamente acionada.



BRUTE FORCE - TESTE DE EFETIVIDADE

- Novamente, acesse a maquina “intranet” e execute o seguinte comando
  - hydra -l ubuntu -P top-20-common-SSH-passwords.txt ssh://10.0.1.101


```
root@ubuntu:/home/ubuntu# hydra -l ubuntu -P top-20-common-SSH-passwords.txt ssh://10.0.1.101
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
 *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-25 17:08:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:1/p:24), ~2 tries per task
[DATA] attacking ssh://10.0.1.101:22/
[22][ssh] host: 10.0.1.101   login: ubuntu   password: ubuntu
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-25 17:08:39
root@ubuntu:/home/ubuntu#
```

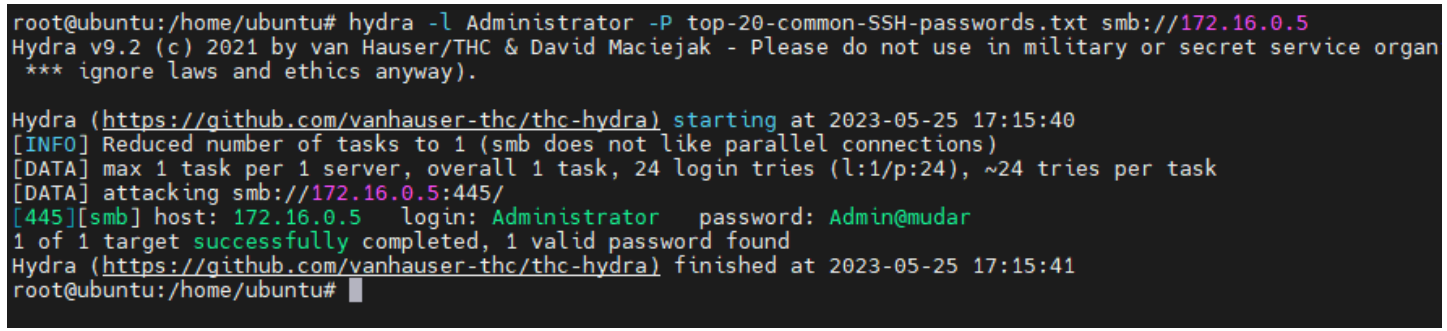


BRUTE FORCE- TESTE DE EFETIVIDADE

- Após executar os testes, acesse o Splunk e navegue até "Activity -> Triggered Alerts". Se a regra estiver funcionando corretamente, você deverá visualizar um alerta correspondente.
- **Obs**: Para confirmar se o resultado está alinhado com o esperado, simplesmente clique na opção "View results".

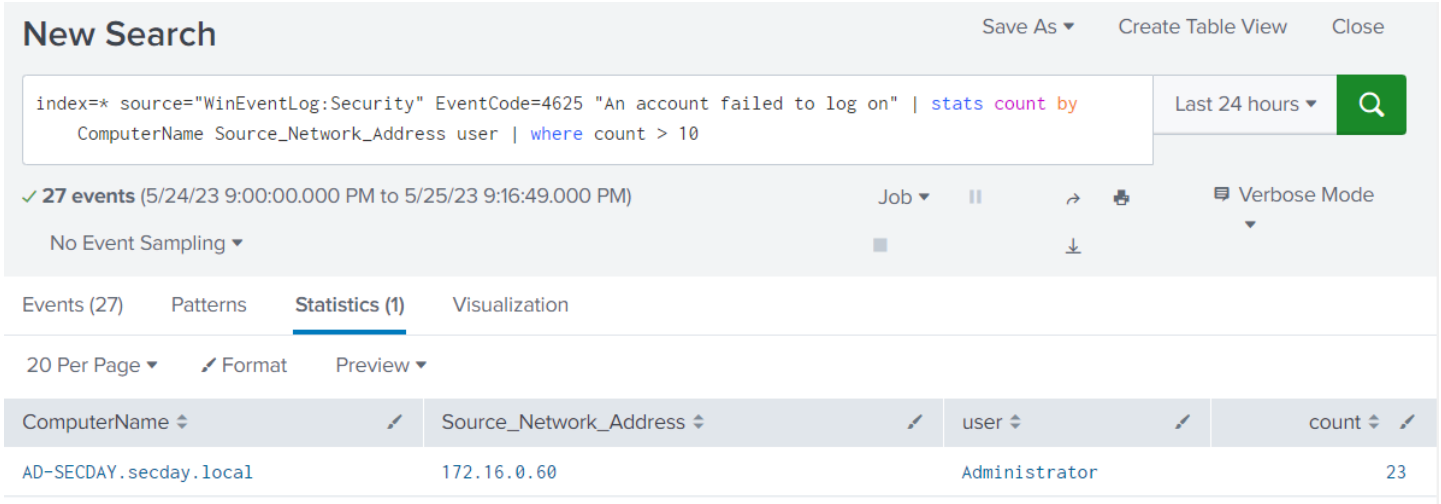
BRUTE FORCE – ATAQUE (WINDOWS)

- Para realizar o ataque de força bruta no sistema Windows, prosseguiremos utilizando o Hydra
  - hydra -l Administrator -P top-20-common-SSH-passwords.txt smb://172.16.0.5
- Obs: adicione a senha ”Admin@mudar” no final do arquivo top-20-common-SSH-passwords.txt



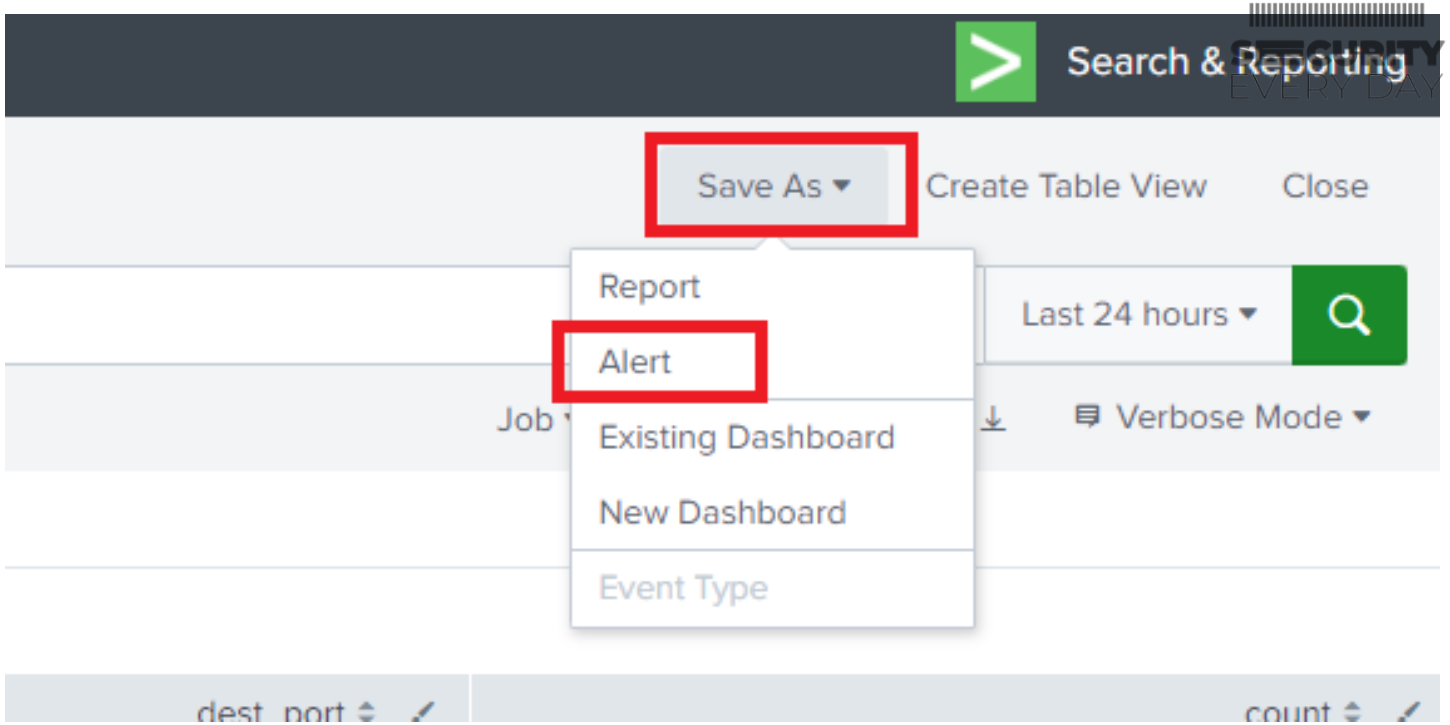
BRUTE FORCE – REGRA (WINDOWS)

- Novamente, para identificar os logs no Splunk e criar a regra, execute o seguinte código:
  - index=* source="WinEventLog:Security" EventCode=4625 "An account failed to log on" | stats count by ComputerName Source_Network_Address user | where count > 10



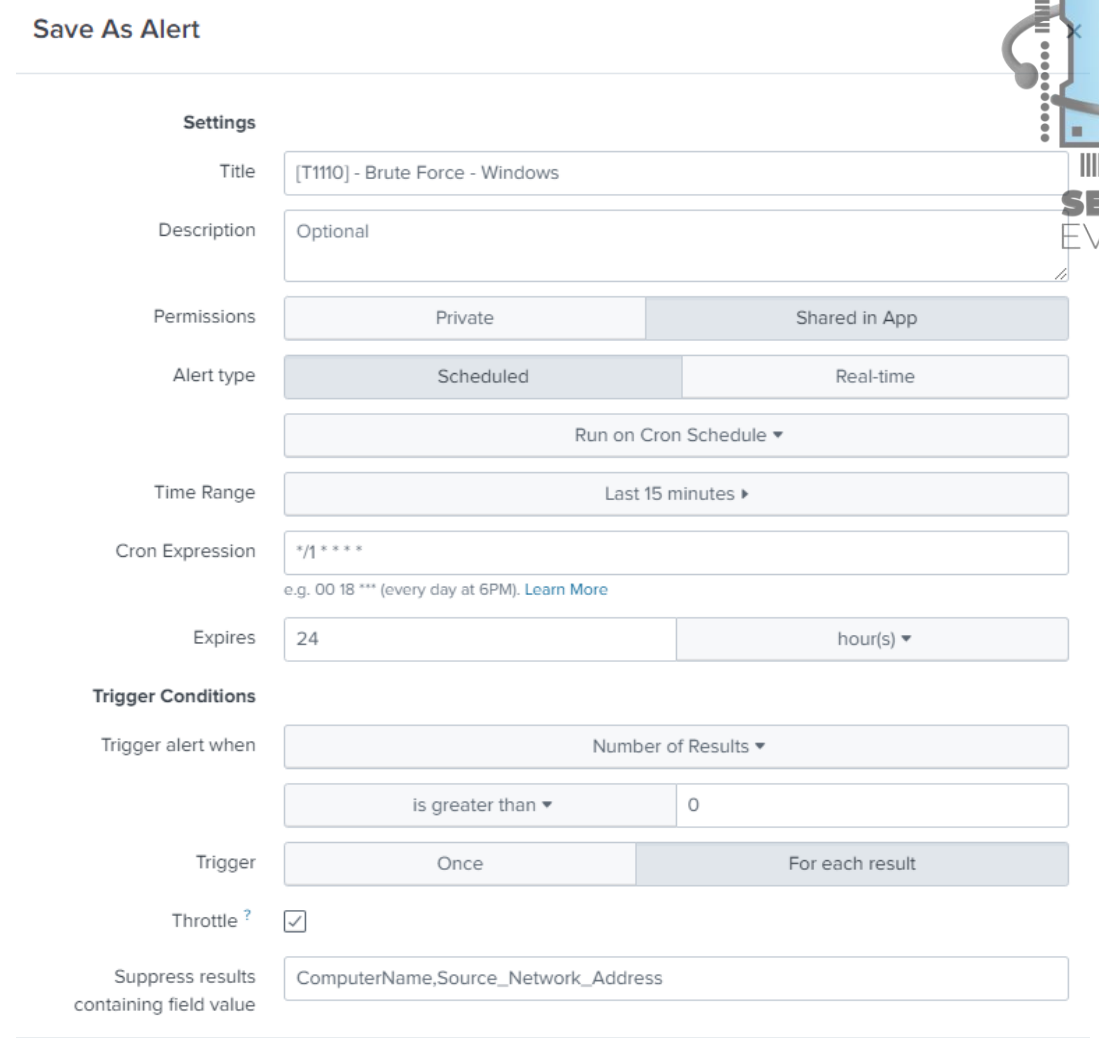
BRUTE FORCE - REGRA (WINDOWS)

- Após executar o código e identificar os testes realizados, clique em “Save As → Alert” para criar a regra



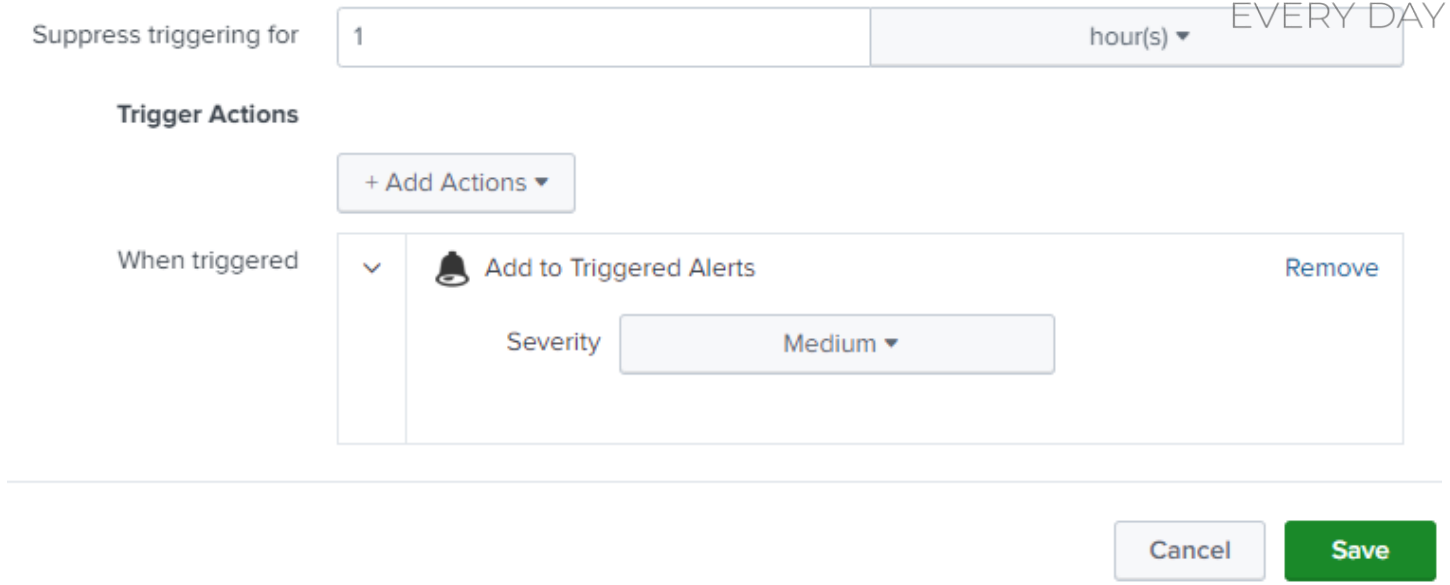
BRUTE FORCE – REGRA (WINDOWS)

- Preencha os campos conforme à imagem



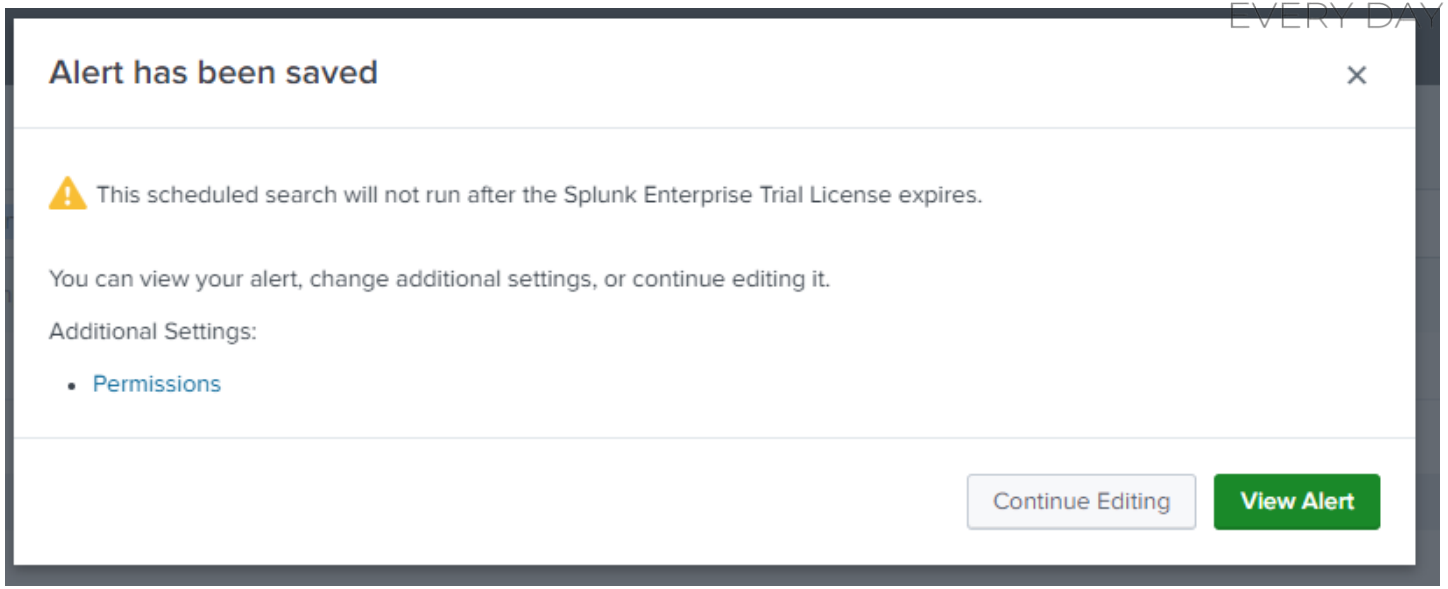
BRUTE FORCE – REGRA (WINDOWS)

- Finalize o preenchimento e clique em “Save”



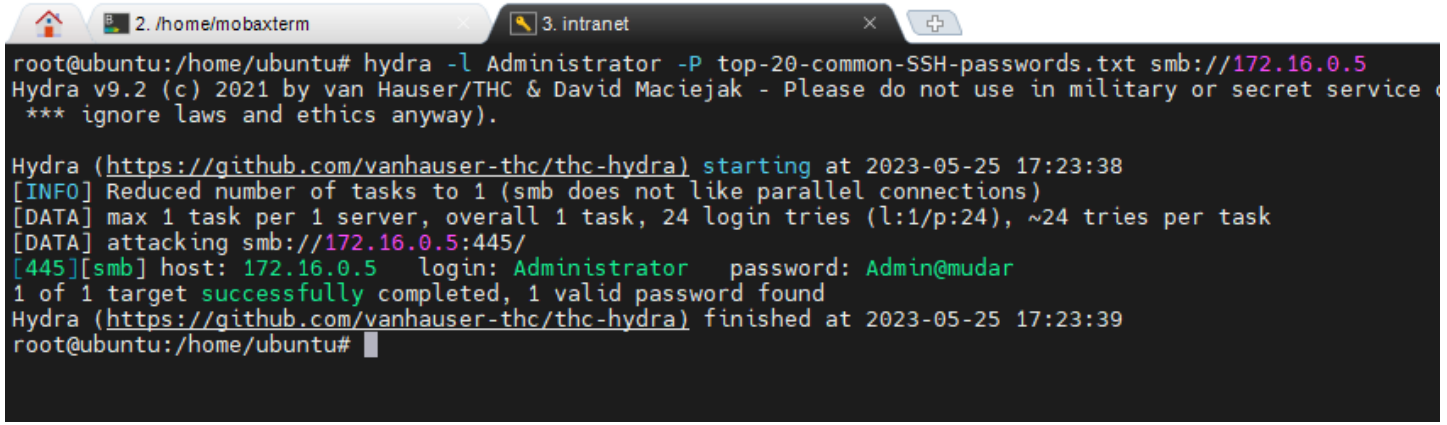
BRUTE FORCE- REGRA (WINDOWS)

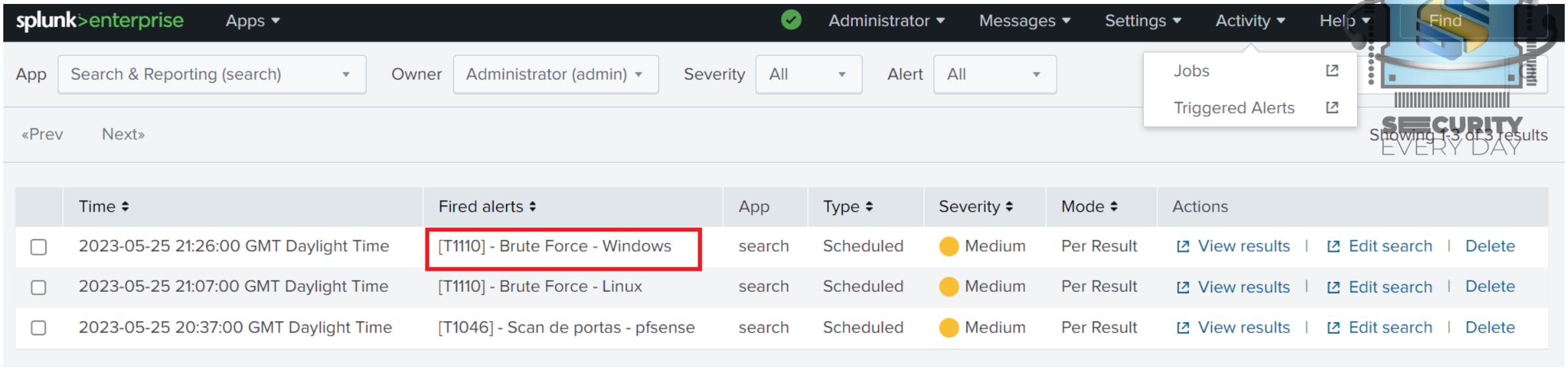
- Selecione a opção "View Alert" e, voilà, a regra será criada. vamos executar um novo "ataque" para verificar se a regra será devidamente acionada.



BRUTE FORCE - TESTE DE EFETIVIDADE (WINDOWS)

- Novamente, execute o seguinte comando
  - hydra -l Administrator -P top-20-common-SSH-passwords.txt smb://172.16.0.5

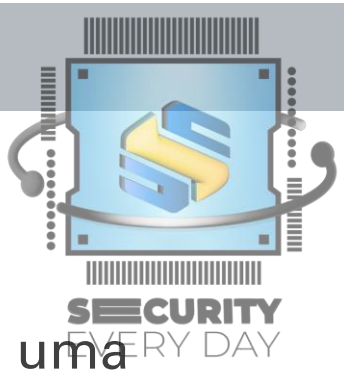




BRUTE FORCE- TESTE DE EFETIVIDADE (WINDOWS)

- Após executar os testes, acesse o Splunk e navegue até "Activity -> Triggered Alerts". Se a regra estiver funcionando corretamente, você deverá visualizar um alerta correspondente.
- **Obs**: Para confirmar se o resultado está alinhado com o esperado, simplesmente clique na opção "View results".

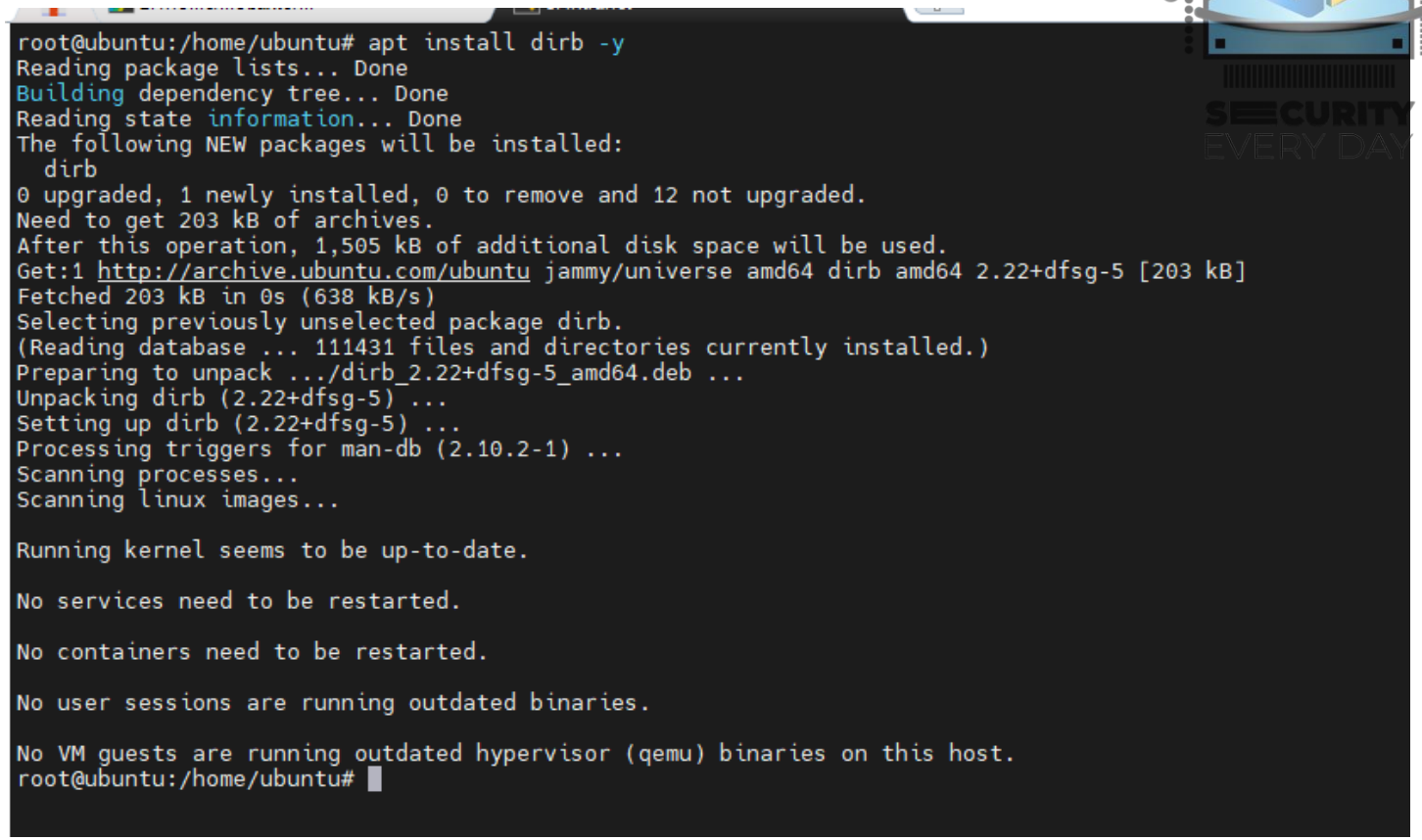
BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB



- O "Brute Force em Arquivos/Diretórios Web" é uma variante do ataque Brute Force que busca descobrir páginas, arquivos ou diretórios ocultos em um website. Os atacantes utilizam listas de palavras comuns com ferramentas automatizadas (ou não) para tentar identificar os diretórios e arquivos escondidos.

BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - ATAQUE

- Vamos realizar este ataque na aplicação “library”, para isso, acesse a maquina “intranet” via SSH e em seguida, instale o Dirb executando o seguinte comando:
  - apt install dirb -y



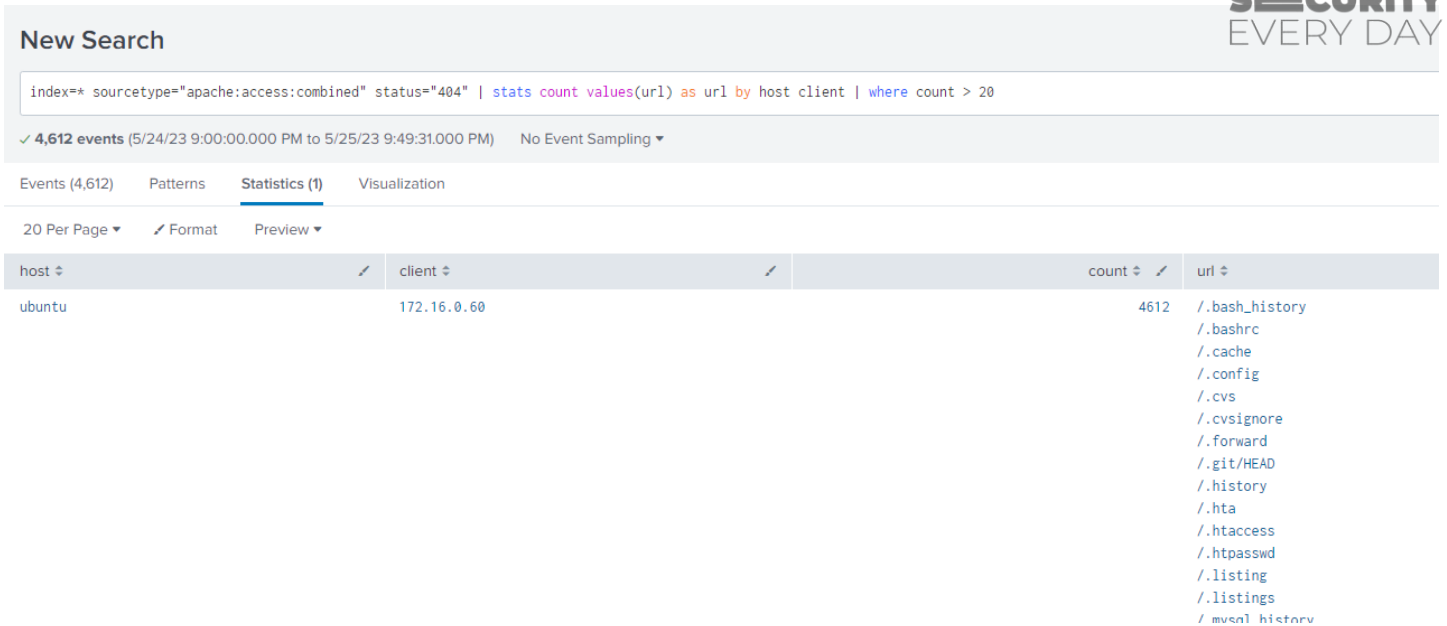
BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - ATAQUE

- Para realizar o ataque, execute o comando:
  - dirb http://10.0.1.101

```
root@ubuntu:/home/ubuntu# dirb http://10.0.1.101

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu May 25 17:47:52 2023
URL_BASE: http://10.0.1.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.1.101/ ----
+ http://10.0.1.101/books (CODE:302|SIZE:189)
+ http://10.0.1.101/logout (CODE:302|SIZE:189)
+ http://10.0.1.101/server-status (CODE:403|SIZE:275)

-----------------
END_TIME: Thu May 25 17:47:59 2023
DOWNLOADED: 4612 - FOUND: 3
```

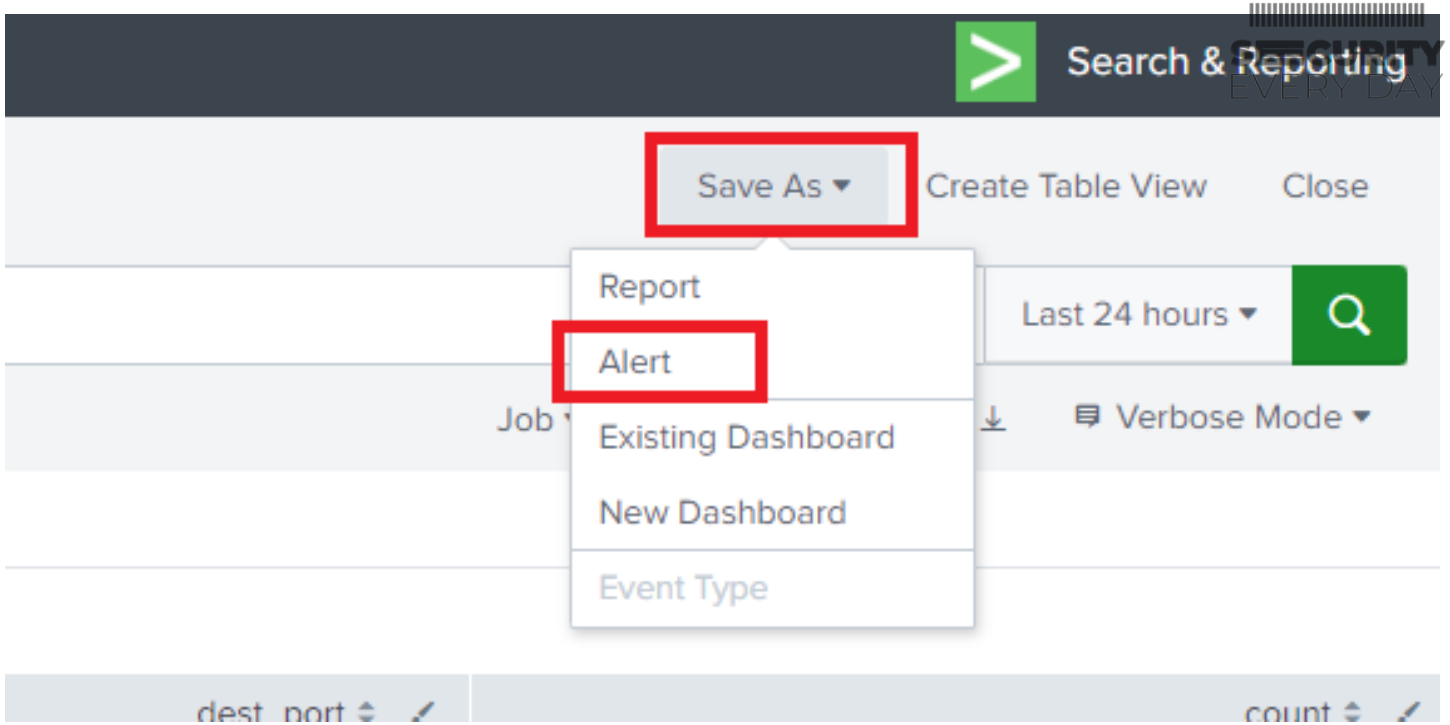
BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - REGRA

- Novamente, para identificar os logs no Splunk e criar a regra, execute o seguinte código:
  - index=* sourcetype="apache:access:combined" status="404" | stats count values(url) as url by host client | where count > 20



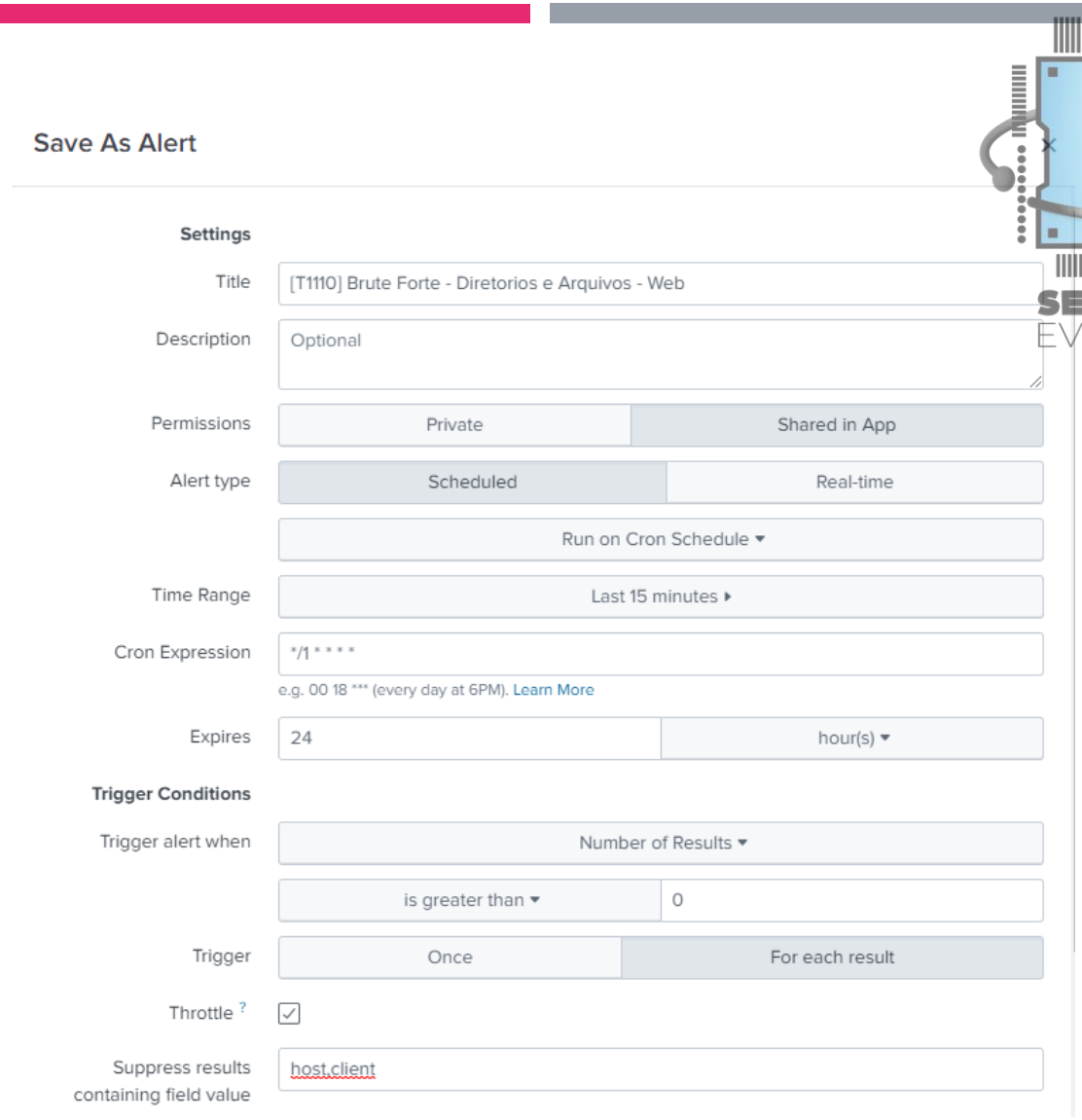
BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - REGRA

- Após executar o código e identificar os testes realizados, clique em “Save As → Alert” para criar a regra



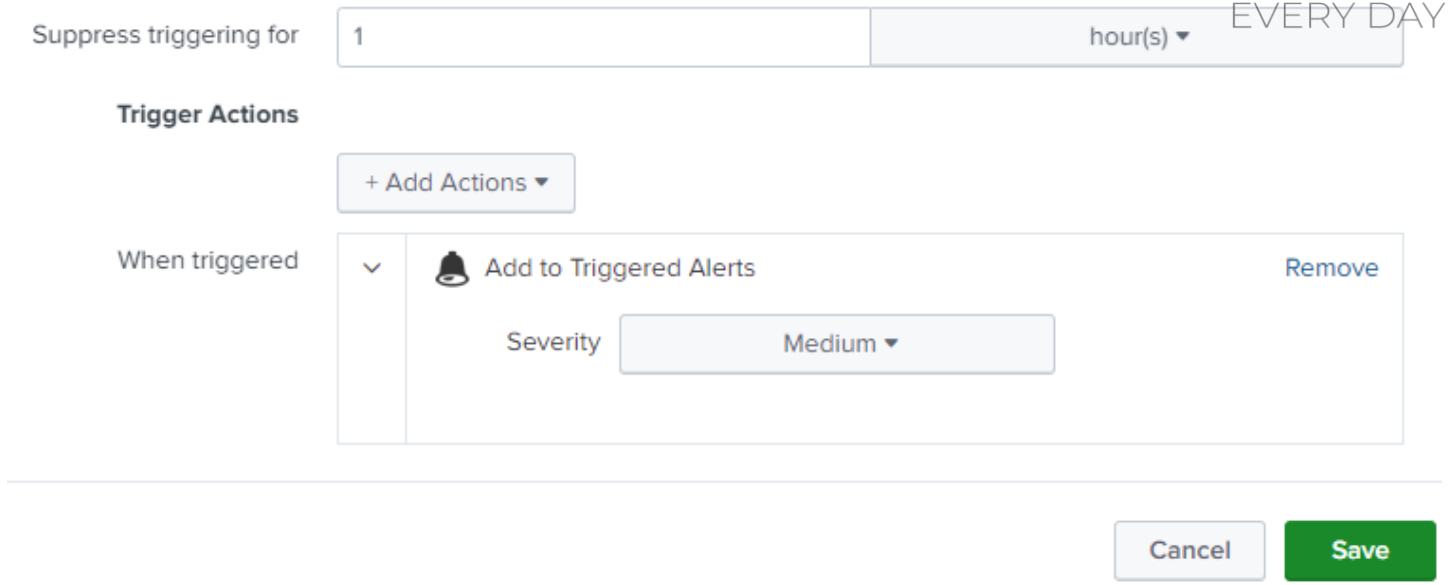
BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - REGRA

- Preencha os campos conforme à imagem



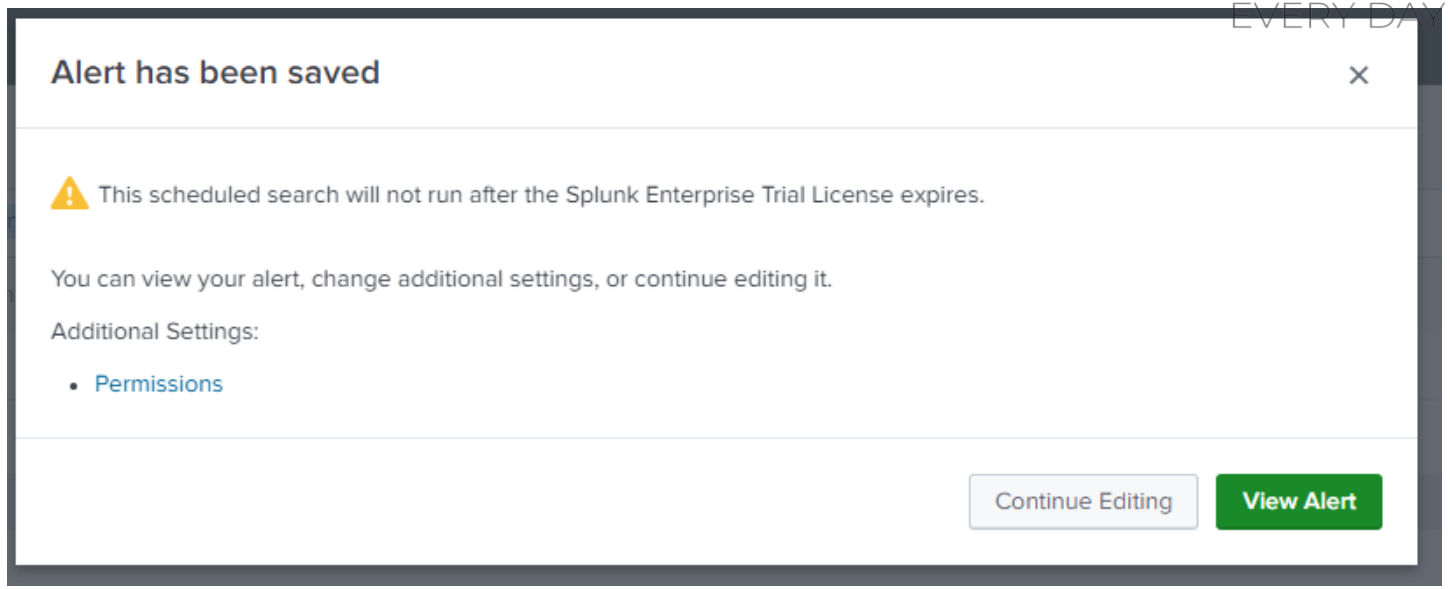
BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - REGRA

- Finalize o preenchimento e clique em “Save”



BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - REGRA

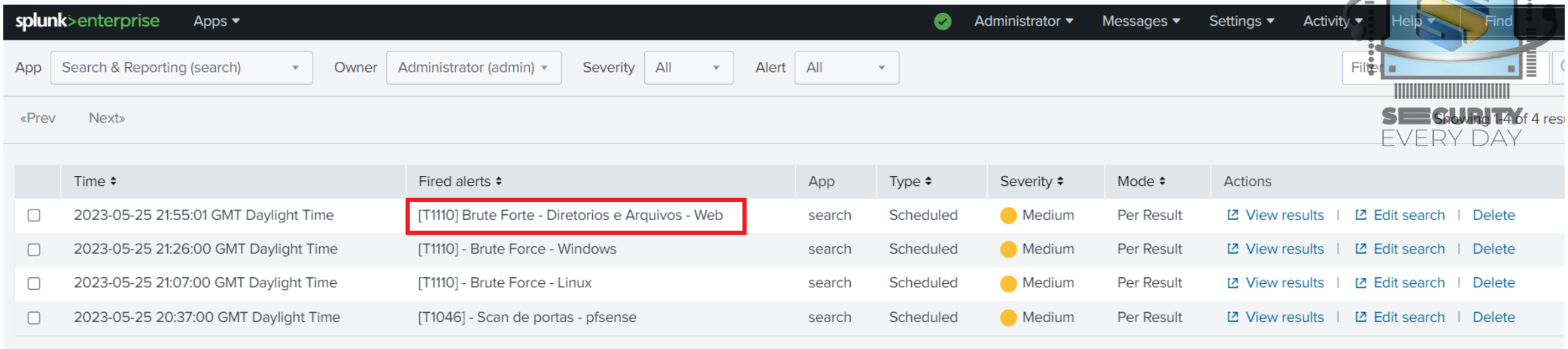
- Selecione a opção "View Alert" e, voilà, a regra será criada. vamos executar um novo "ataque" para verificar se a regra será devidamente acionada.



BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - TESTE DE EFETIVIDADE

- Novamente, execute o comando:
  - dirb http://10.0.1.101

```
root@ubuntu:/home/ubuntu# dirb http://10.0.1.101

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu May 25 17:47:52 2023
URL_BASE: http://10.0.1.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.1.101/ ----
+ http://10.0.1.101/books (CODE:302|SIZE:189)
+ http://10.0.1.101/logout (CODE:302|SIZE:189)
+ http://10.0.1.101/server-status (CODE:403|SIZE:275)

-----------------
END_TIME: Thu May 25 17:47:59 2023
DOWNLOADED: 4612 - FOUND: 3
```



BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - TESTE DE EFETIVIDADE

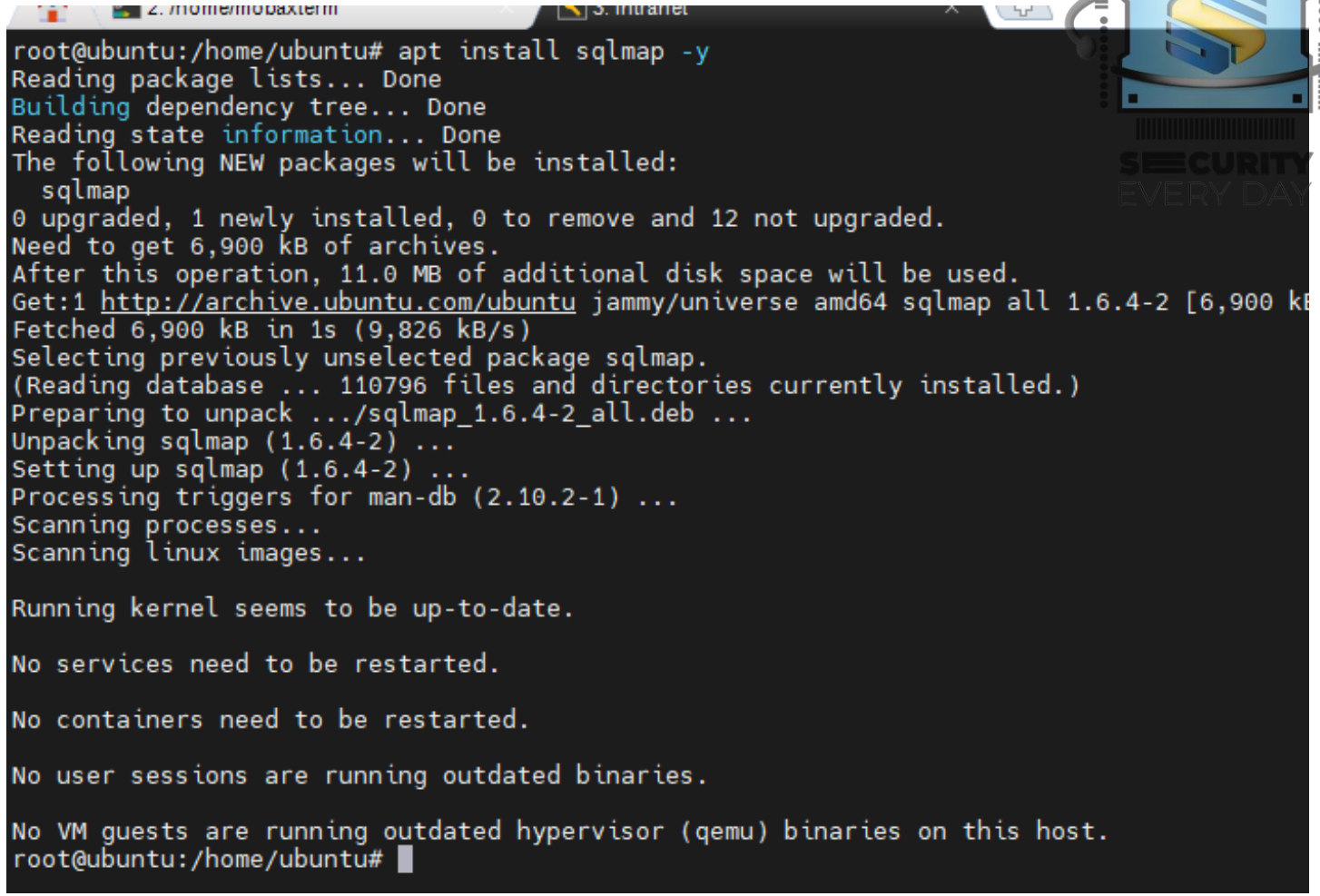
- Após executar os testes, acesse o Splunk e navegue até "Activity -> Triggered Alerts". Se a regra estiver funcionando corretamente, você deverá visualizar um alerta correspondente.
- **Obs**: Para confirmar se o resultado está alinhado com o esperado, simplesmente clique na opção "View results".

SQLINJECTION

- O ataque de "SQL Injection" é uma tecnica que tem como objetivo explorar vulnerabilidades em aplicações por meio da inserção de instruções SQL maliciosas.

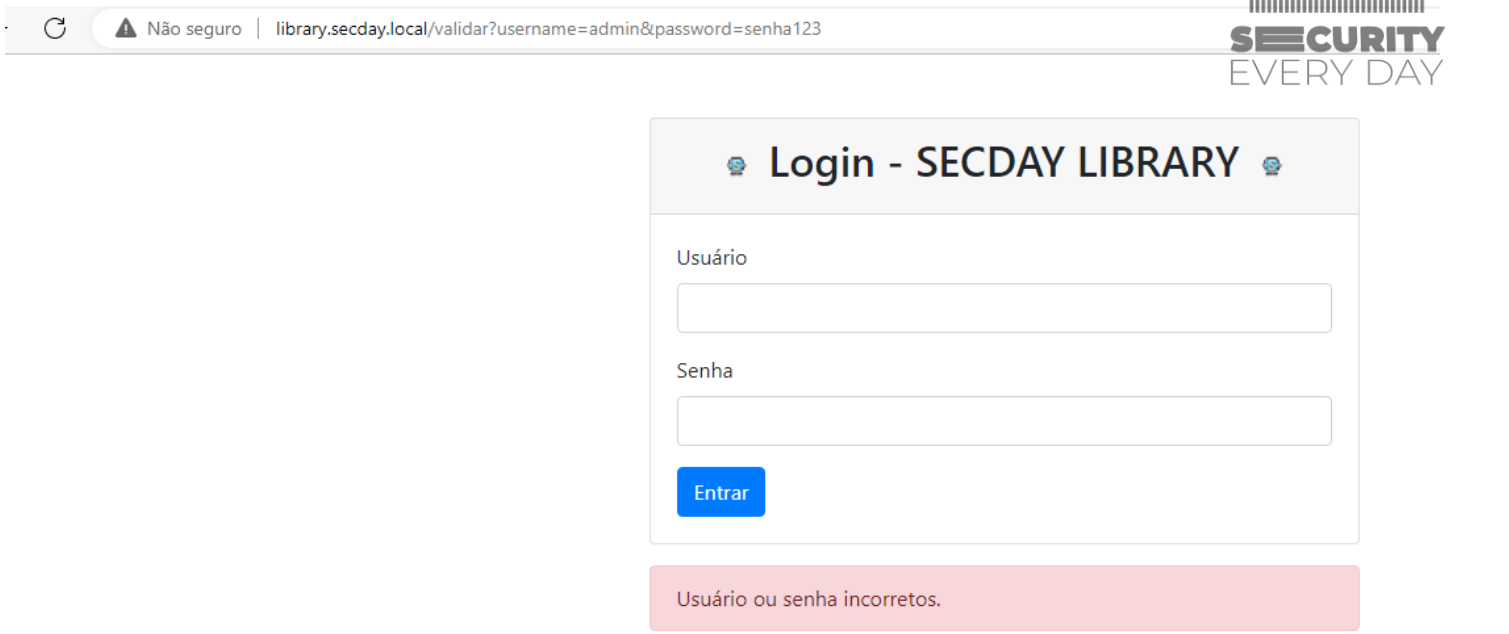
SQLINJECTION - ATAQUE

- Vamos realizar este ataque na aplicação “library”, para isso, acesse a maquina “intranet” via SSH e em seguida, instale o sqlmap executando o seguinte comando:
  - apt install sqlmap -y



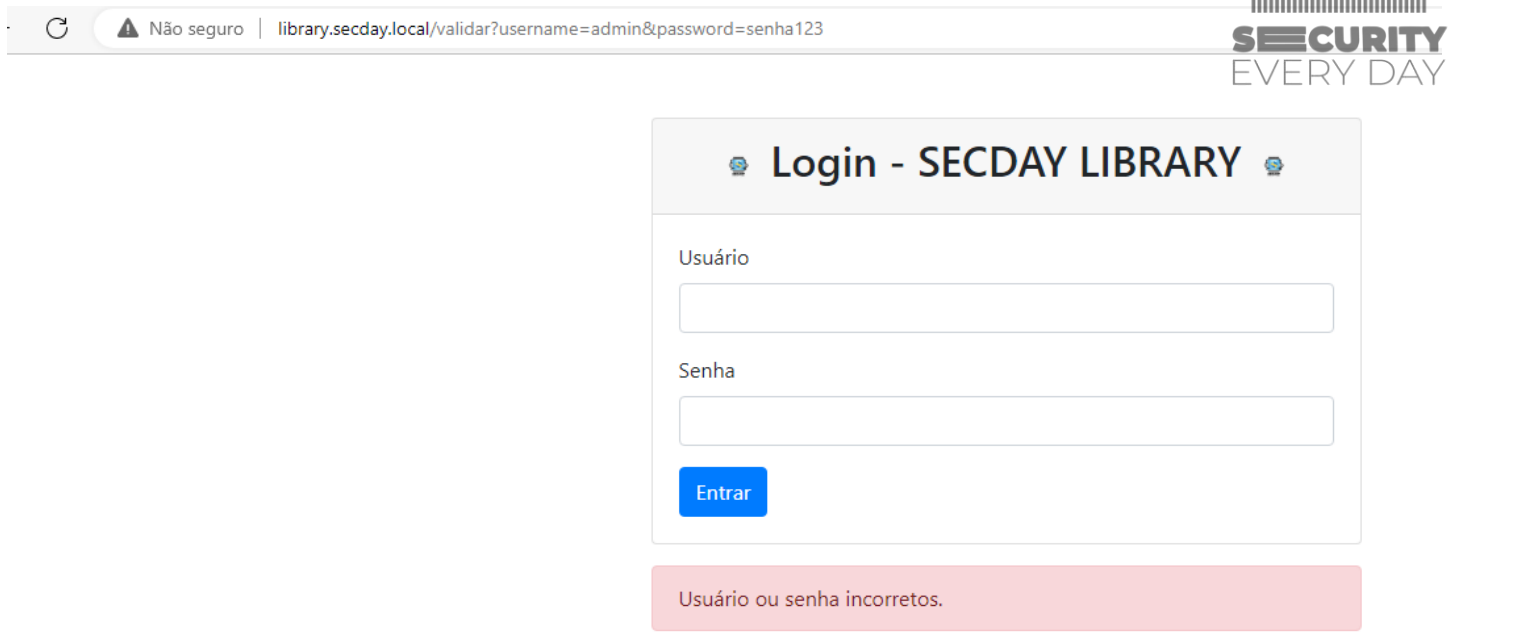
SQLINJECTION - ATAQUE

- Antes de realizar o “ataque”, vamos acessar a aplicação e tentar realizar um login com usuário e senha qualquer
  - http://library.secday.local



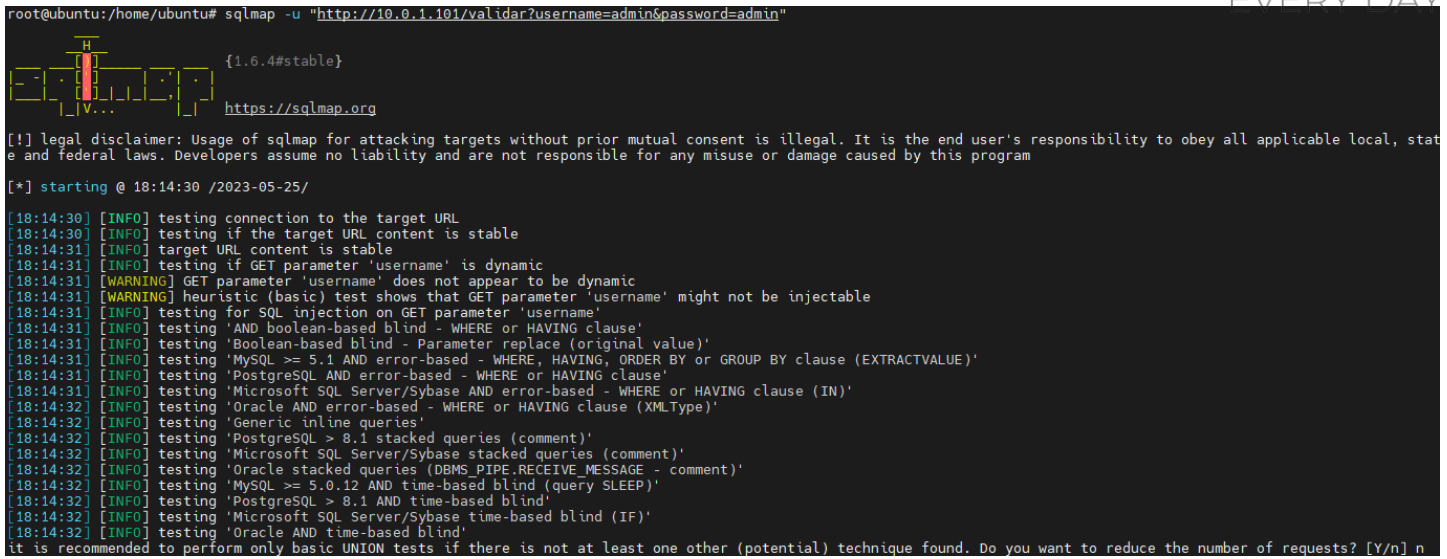
SQLINJECTION - ATAQUE

- Observe que o nome de usuário e a senha estão sendo transmitidos na URL, prática que não é recomendada em termos de segurança. Porém, vamos deixar essa questão de lado por enquanto. Nosso foco, neste momento, será tentar executar um ataque de SQL Injection e com base nos logs que temos à disposição, conseguiremos identificar esse ataque.



SQLINJECTION - ATAQUE

- Para realizar o “ataque” execute o commando
  - sqlmap -u http://10.0.1.101/validar?username=admin&password=admin



SQLINJECTION - REGRA

- Novamente, para identificar os logs no Splunk e criar a regra, execute o seguinte código:
  - index=* sourcetype="apache:access:combined" | regex url="(\%27)|(---)|(\%22)|(UNION)|(\%3D)|(\%3B)|(\%2F*)|(*/)|(\<\>)|(\<\=)|(AND)|(OR)|(NOT)|(SELECT)|(UPDATE)|(DELETE)|(DROP)|(INSERT)|(ALTER)|(--)|(\#\#)|(SLEEP)|(WAITFOR)" | eval url=urldecode(url) | stats count values(url) as url by host client

New Search

```
index=* sourcetype="apache:access:combined" | regex url="(\%27)|(---)|(\%22)|(UNION)|(\%3D)|(\%3B)|(\%2F\*)|(\*/)|(\<\>)|(\<\=)|(AND)|(OR)|(NOT)|(SELECT)|(UPDATE)|(
    )|(ALTER)|(--)|(\#\#)|(SLEEP)|(WAITFOR)" | eval url=urldecode(url) | stats count values(url) as url by host client
```

✓ **248 events** (5/24/23 10:00:00.000 PM to 5/25/23 10:52:06.000 PM) No Event Sampling ▾ Job ▾

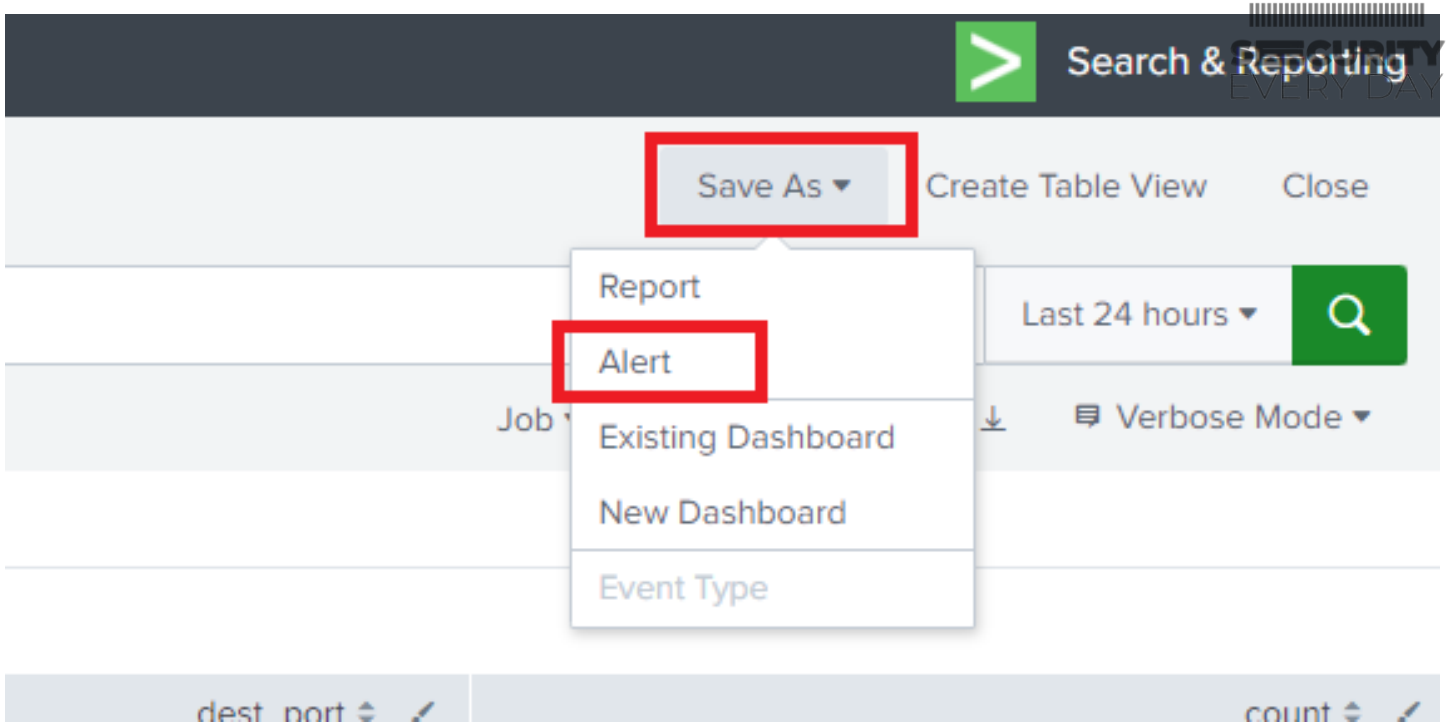
Events (248) Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

host	client	count	url
ubuntu	172.16.0.60	248	/validar?username=(SELECT (CASE WHEN (3800=2338) THEN 'admin' ELSE (SELECT 2338 UNION SELECT 8191) END))&password=admin /validar?username=(SELECT (CASE WHEN (9082=9082) THEN 'admin' ELSE (SELECT 3175 UNION SELECT 7753) END))&password=admin /validar?username=(SELECT CONCAT(CONCAT('qbkjq',(CASE WHEN (6148=6148) THEN '1' ELSE '0' END)),'qpvxq'))&password=admin /validar?username=admin AND (SELECT 7797 FROM (SELECT(SLEEP(5)))zRQZ)&password=admin /validar?username=admin AND (SELECT 7797 FROM (SELECT(SLEEP(5)))zRQZ)-- cYDq&password=admin /validar?username=admin AND 1785=7715-- RvmT&password=admin /validar?username=admin AND 2036=CAST((CHR(113)||CHR(98)||CHR(107)||CHR(106)||CHR(113))||(SELECT (CASE WHEN (2036=2036) THEN 1 EL (CHR(113)||CHR(112)||CHR(118)||CHR(120)||CHR(113)) AS NUMERIC)&password=admin /validar?username=admin AND 2036=CAST((CHR(113)||CHR(98)||CHR(107)||CHR(106)||CHR(113))||(SELECT (CASE WHEN (2036=2036) THEN 1 EL (CHR(113)||CHR(112)||CHR(118)||CHR(120)||CHR(113)) AS NUMERIC)-- fRYw&password=admin /validar?username=admin AND 2160=(SELECT UPPER(XMLType(CHR(60)||CHR(58)||CHR(113)||CHR(98)||CHR(107)||CHR(106)||CHR(113)||(SELECT FROM DUAL)||CHR(113)||CHR(112)||CHR(118)||CHR(120)||CHR(113)||CHR(62))) FROM DUAL)&password=admin

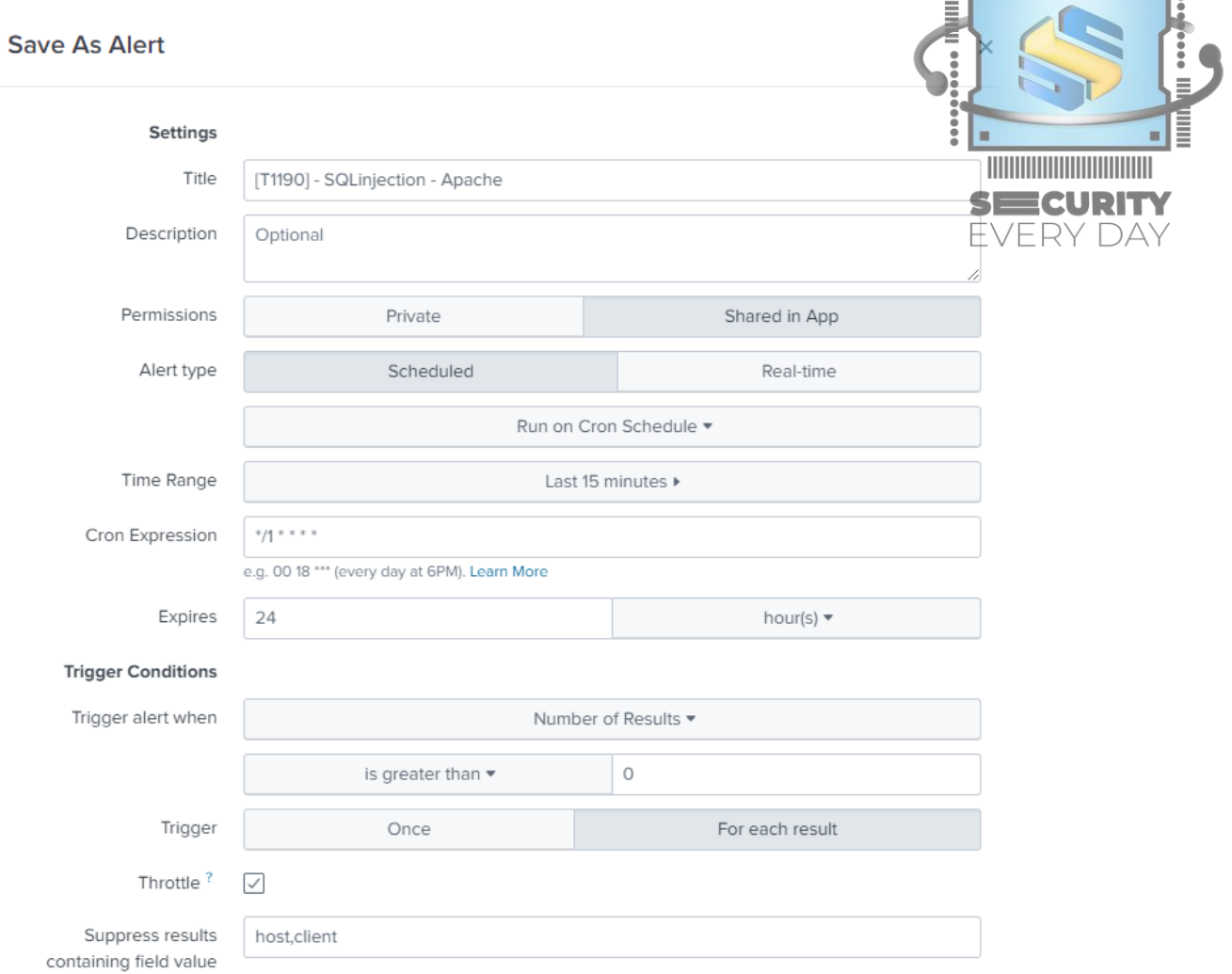
SQLINJECTION - REGRA

- Após executar o código e identificar os testes realizados, clique em “Save As → Alert” para criar a regra



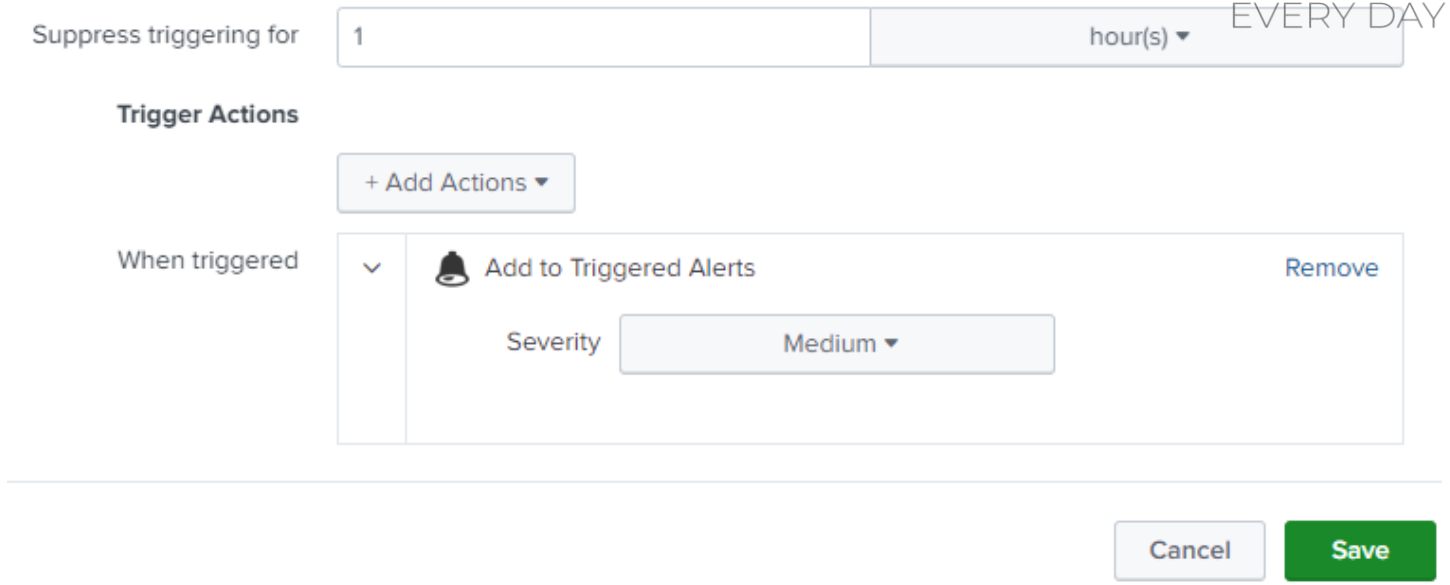
SQLINJECTION - REGRA

- Preencha os campos conforme à imagem



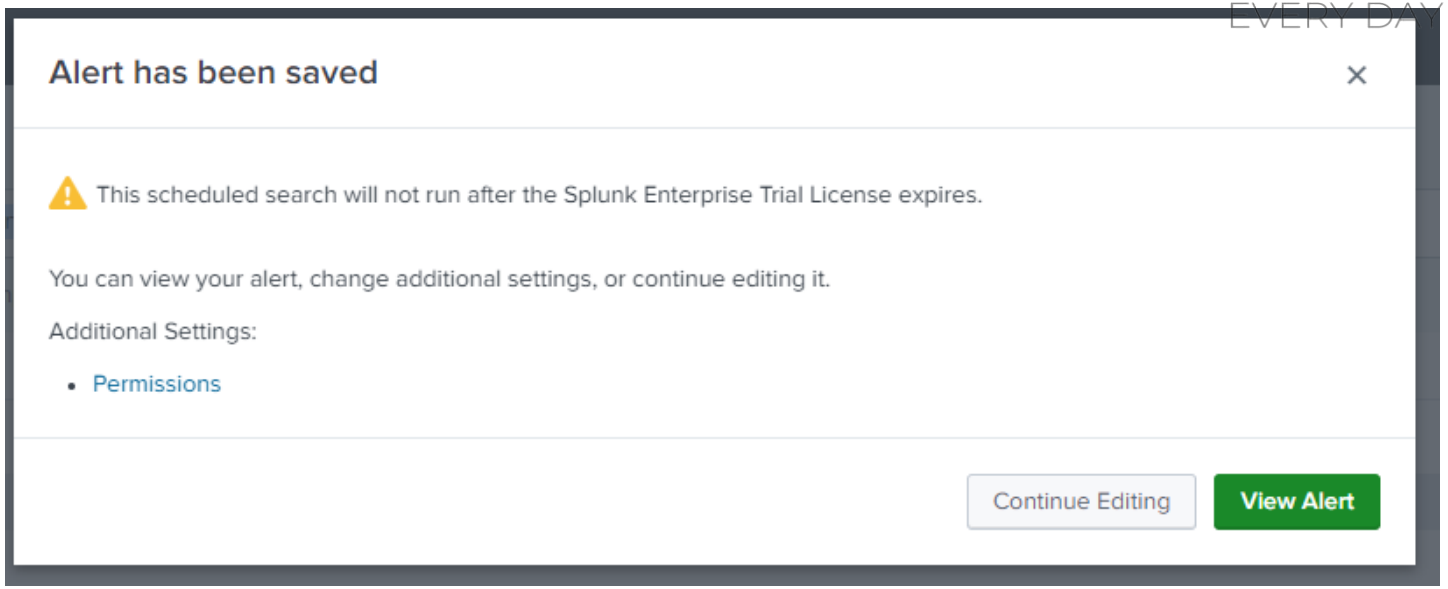
SQLINJECTION - REGRA

- Finalize o preenchimento e clique em “Save”



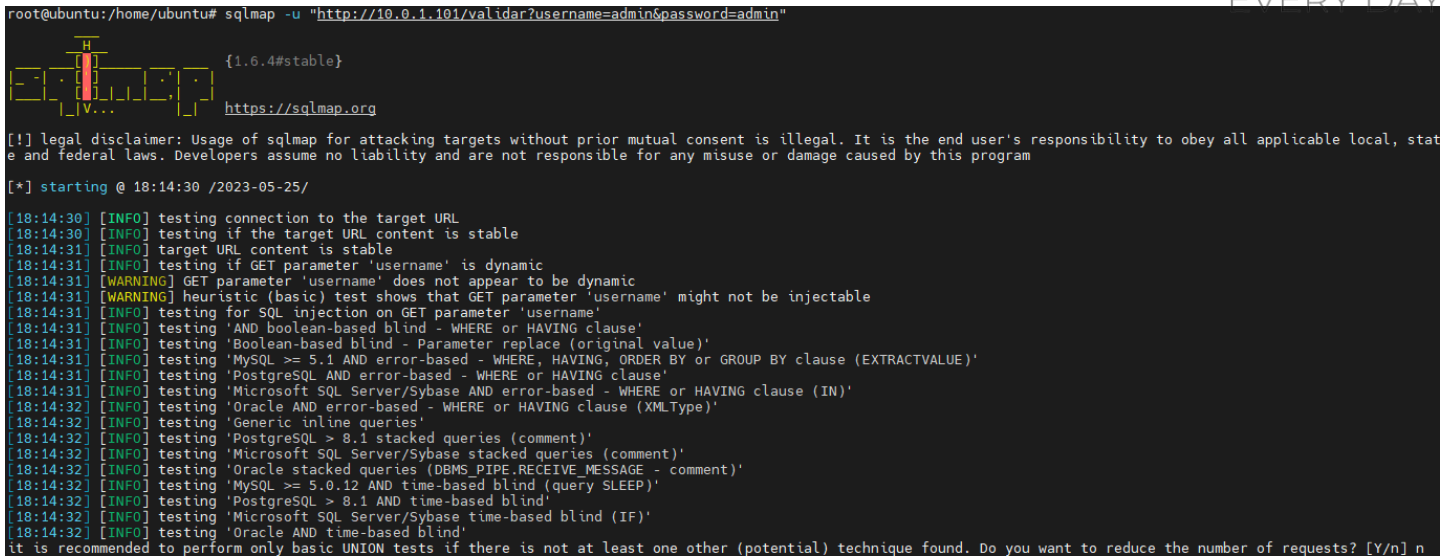
SQLINJECTION - REGRA

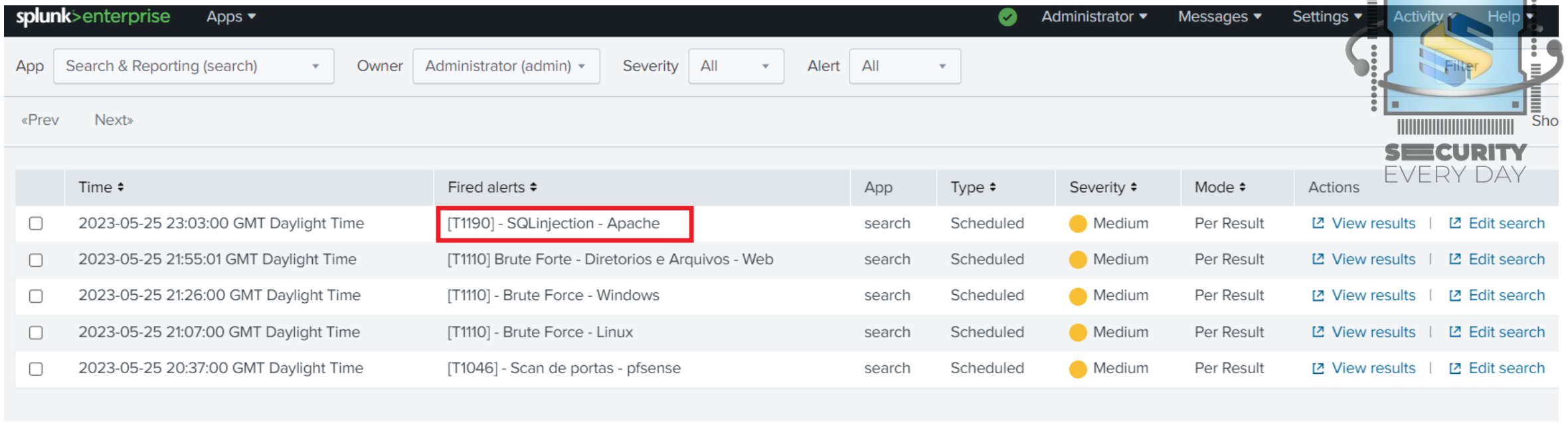
- Selecione a opção "View Alert" e, voilà, a regra será criada. vamos executar um novo "ataque" para verificar se a regra será devidamente acionada.



SQLINJECTION - TESTE DE EFETIVIDADE

- Novamente, execute o comando
  - sqlmap -u "http://10.0.1.101/validar?username=admin&password=admin"



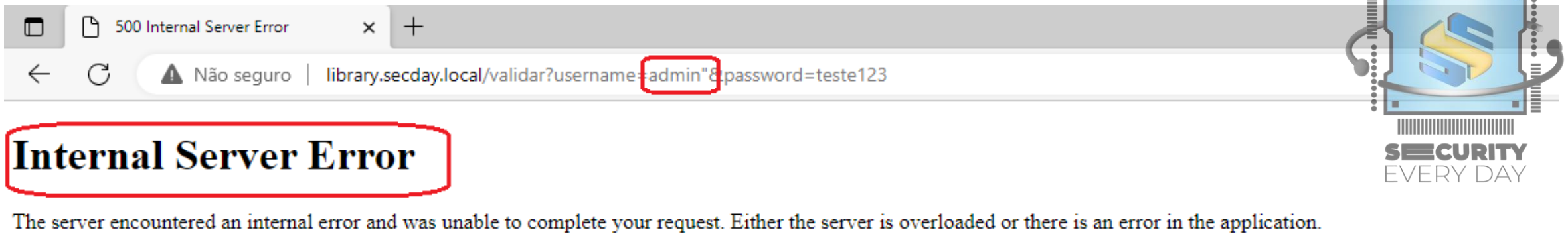


SQLINJECTION - TESTE DE EFETIVIDADE

- Após executar os testes, acesse o Splunk e navegue até "Activity -> Triggered Alerts". Se a regra estiver funcionando corretamente, você deverá visualizar um alerta correspondente.
- **Obs**: Para confirmar se o resultado está alinhado com o esperado, simplesmente clique na opção "View results".

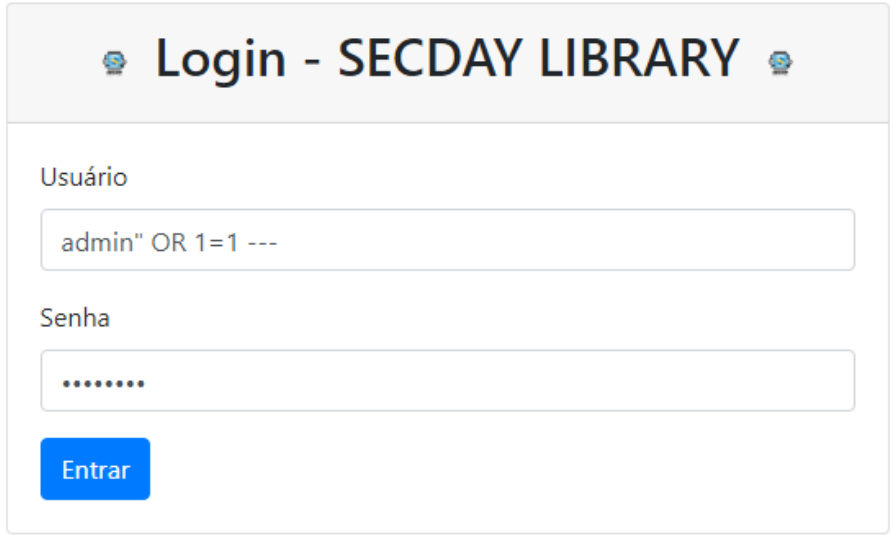
OBSERVAÇÕES

- Observe que, ao executar o sqlmap, ele não detectou a vulnerabilidade de injeção de SQL na página. No entanto, a vulnerabilidade existe. Vamos tentar uma abordagem manual.



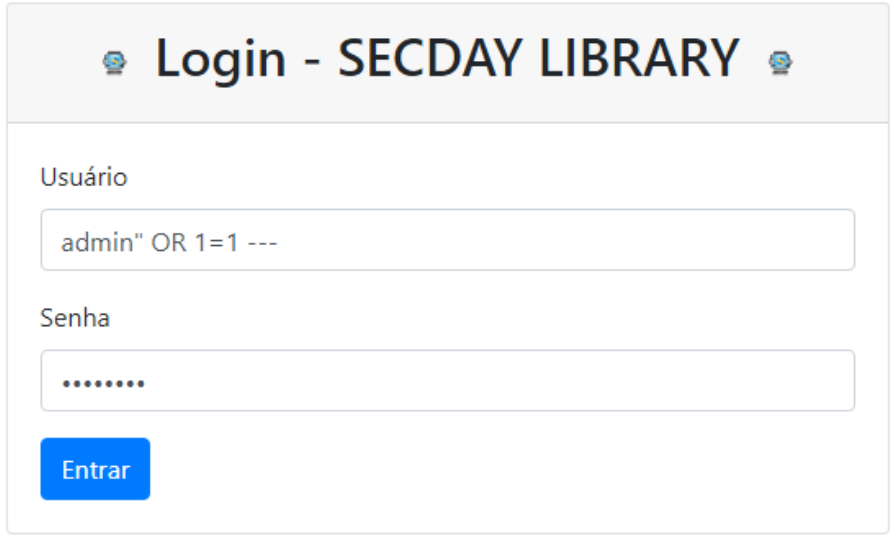
OBSERVAÇÕES

- Acesse a página pelo navegador e tente logar com o usuário
  - User: admin"
  - Pass: qualquer senha
- O servidor retornou um erro 500, o que indica fortemente a presença da vulnerabilidade de SQL injection na página. Vamos aprimorar nosso teste para realizar uma validação mais completa.



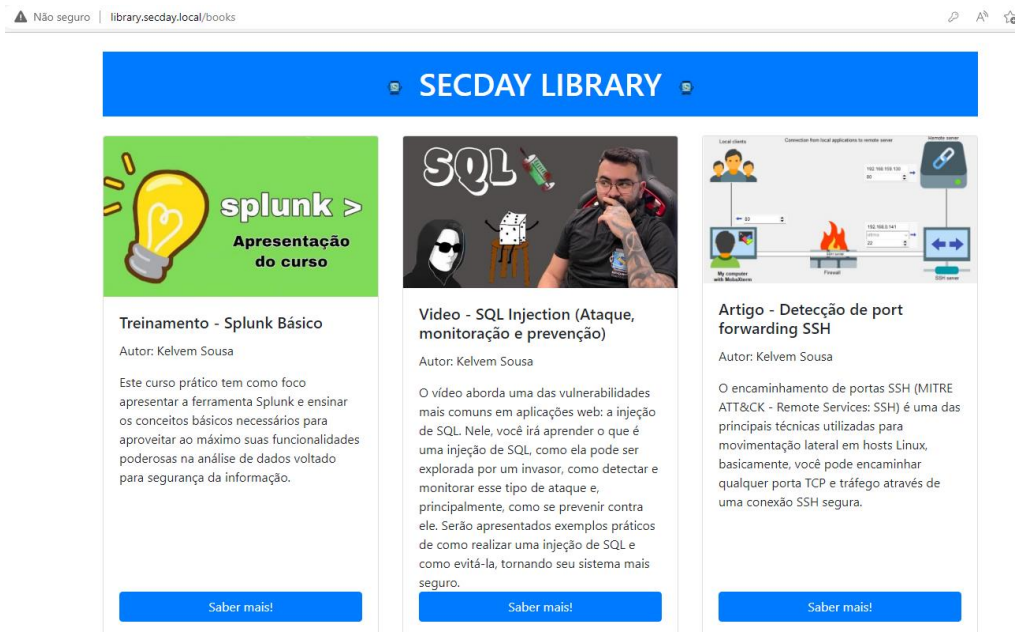
OBSERVAÇÕES

- Para esse teste, coloque no campo do usuário
  - User: admin" OR 1=1 ---
  - Pass: qualquer senha
- Aperte em “Entrar” e veja o bypass acontecer



OBSERVAÇÕES

- Para esse teste, coloque no campo do usuário
  - User: admin" OR 1=1 ---
  - Pass: qualquer senha
- Aperte em “Entrar” e veja o bypass acontecer



OBSERVAÇÕES

- Você conseguiu acessar a 'SECDAY LIBRARY' por meio de um SQL injection. Aproveite para assistir ao vídeo 'SQL Injection (Ataque, monitoramento e prevenção)' para entender melhor o que acabamos de fazer

```
index=* sourcetype="apache:access:combined" | regex url="(\%27)|(---)|(\%22)|(UNION)|(\%3D)|(\%3B)|(\%2F\*)|(\*/)|(\<\>)|(\<\=)|(AND)|(OR)|(NOT)|(SELECT)|(UPD
    )|(ALTER)|(--)|(\#\#)|(SLEEP)|(WAITFOR)" | eval url=urldecode(url) | stats count values(url) as url by host client
```

✓ **1 event** (5/26/23 2:37:17.000 PM to 5/26/23 2:52:17.000 PM) No Event Sampling

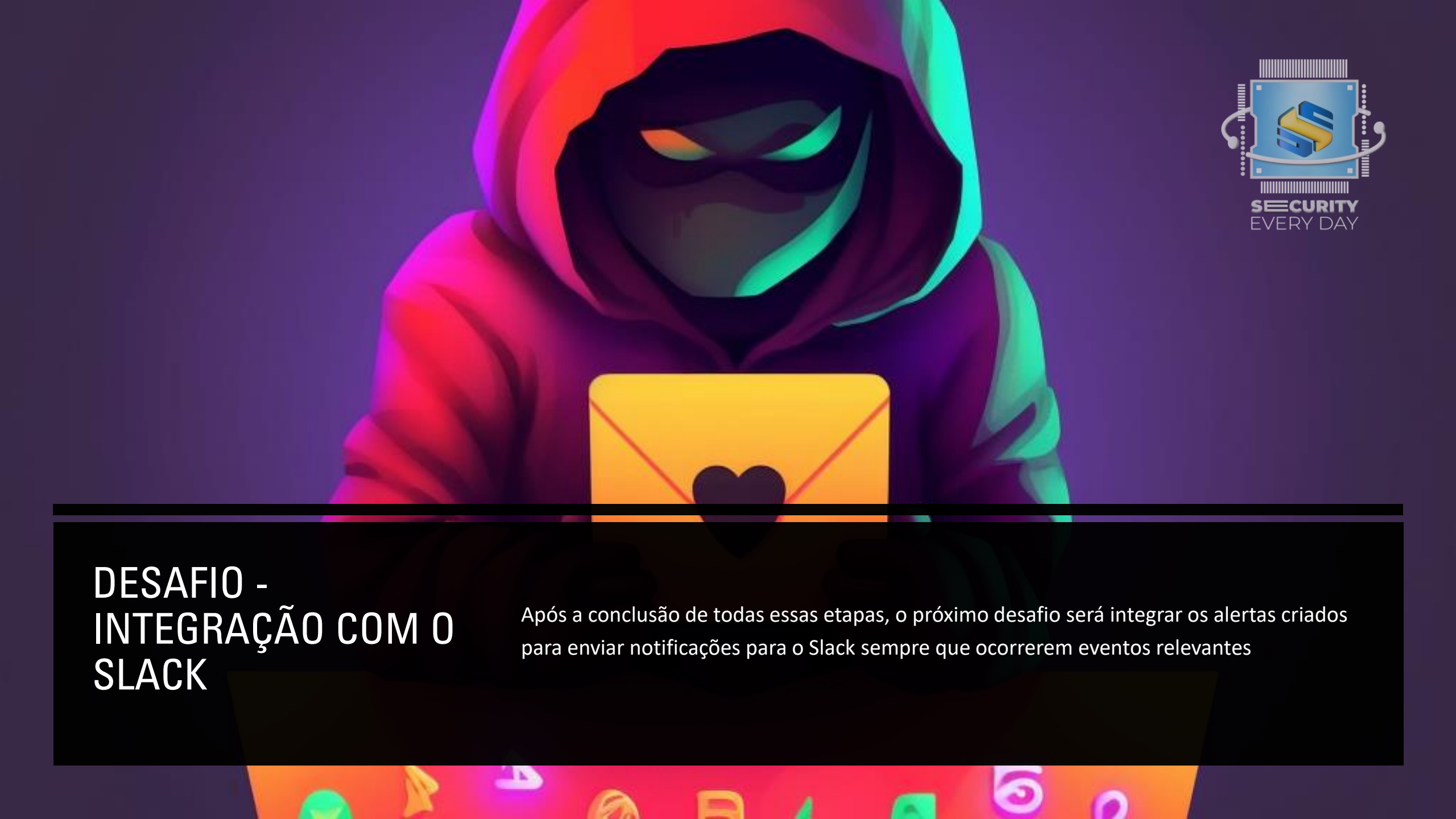
Events Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

host	client	count	url
ubuntu	192.168.228.100	1	/validar?username=admin" OR 1=1 --- &password=teste123

OBSERVAÇÕES

- Além disso, você deve observar um novo alerta relacionado à injeção SQL



DESAFIO - INTEGRAÇÃO COM O SLACK

Após a conclusão de todas essas etapas, o próximo desafio será integrar os alertas criados para enviar notificações para o Slack sempre que ocorrerem eventos relevantes

DESAFIO - INTEGRAÇÃO COM O SLACK

- Para completar o desafio, assista ao nosso vídeo sobre a criação de alertas e integração do Slack.
  - Splunk Fundamentos - Módulo 12 - Aula 01 Criando alerta e enviado para o Slack – YouTube

CHEGAMOS AO FIM?

- Este foi o nosso treinamento "BEGGINER MONITOR". Agora você possui as habilidades para:
  - Configurar máquinas virtuais e preparar o ambiente de laboratório;
  - Ter uma visão geral sobre segurança defensive;
  - Praticar e compreender brevemente a identificação das "Joias da Coroa“;
  - Praticar e compreender brevemente o funcionamento do SIEM (Security Information and Event Management);
  - Praticar e compreender brevemente as camadas de monitoramento;
  - Realizar a coleta simplificada de logs;
  - Identificar um ataque e criar regras de detecções simples;
  - Participar de um exercício simples de equipe “Purple team“;
- No entanto, isso é apenas a ponta do iceberg. Foi apenas uma visão geral do monitoramento e da segurança defensiva. Continue acompanhando nosso canal e nossos vídeos e não pare de estudar. Desejamos muito sucesso!