



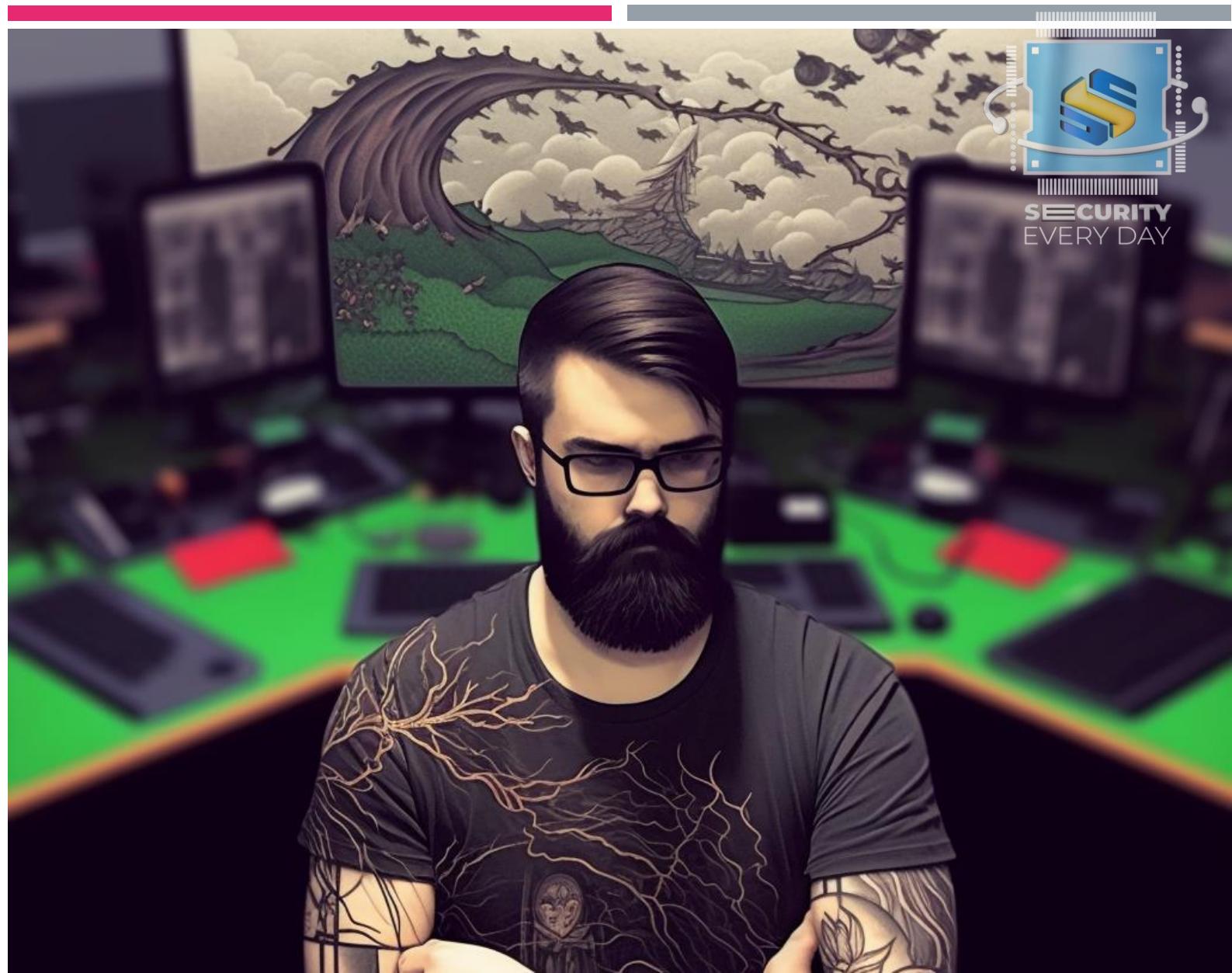
SECDAY - BEGINNER MONITOR

SDBM



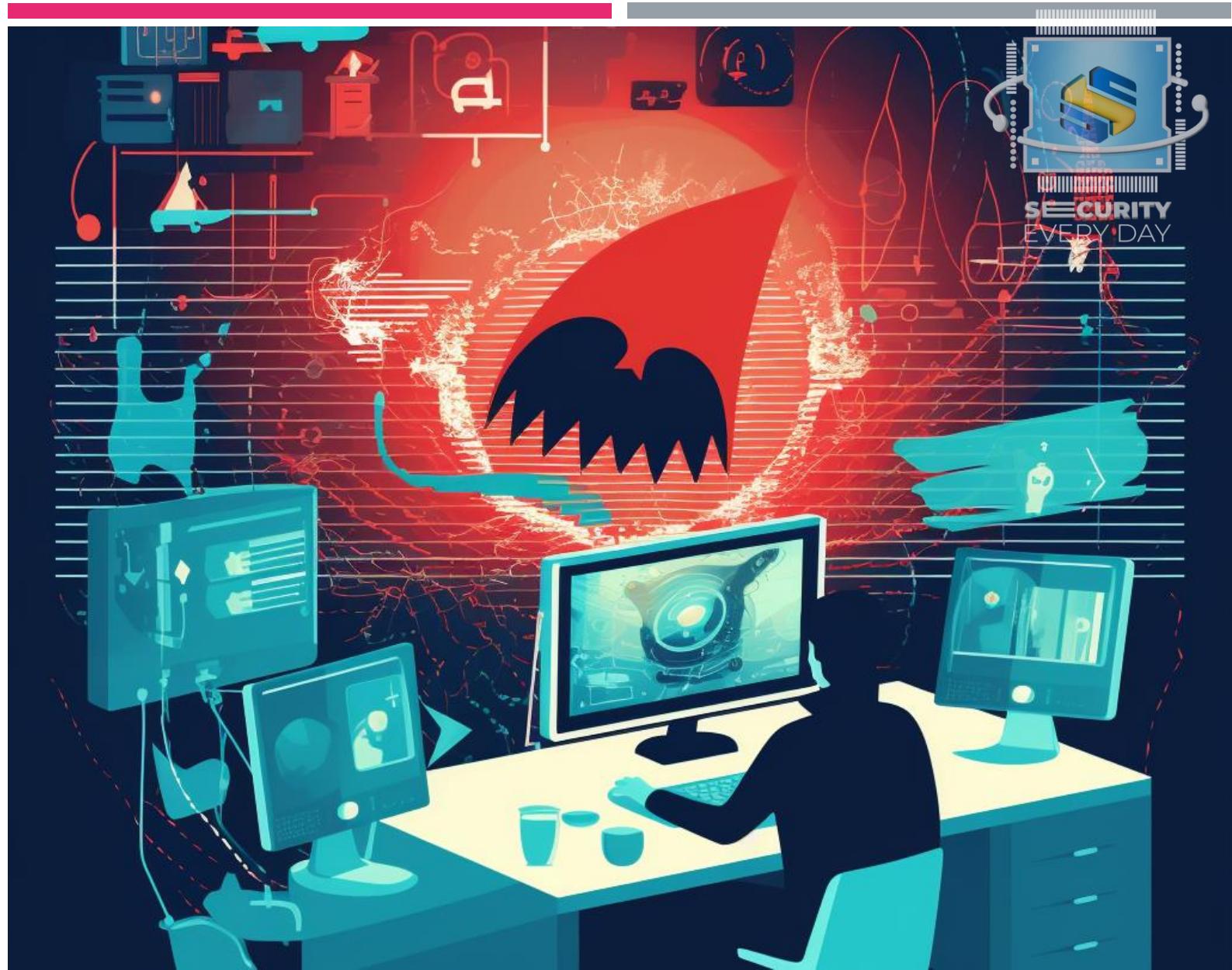
WHOAMI?

- 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

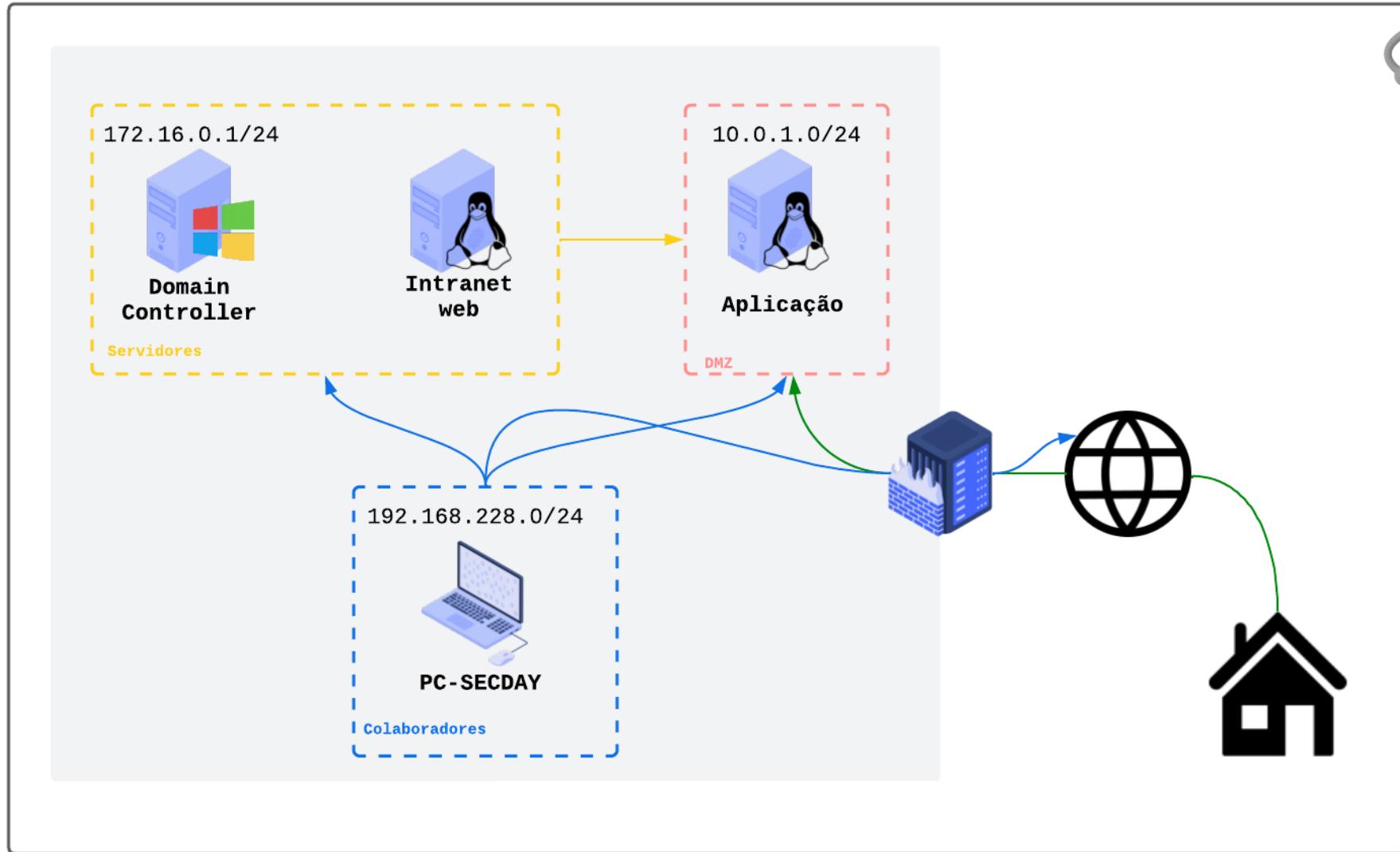
Noções básicas de implantação do SIEM

Visão geral do framework MITRE ATT&CK e sua utilidade

Desenvolvimento de casos de uso simples para detecção de ataques

Integração do Slack





PRÉ-REQUISITOS



8GB de RAM



100 GB espaço em
disco



Conexão com a
internet

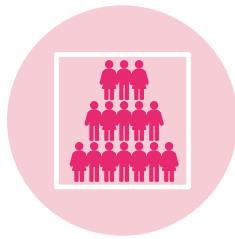


CPU Core I3 ou
equivalente

INTRODUÇÃO



O QUE É
SEGURANÇA
DEFENSIVA?



QUAIS SÃO AS
EQUIPES QUE
COMPÕEM?



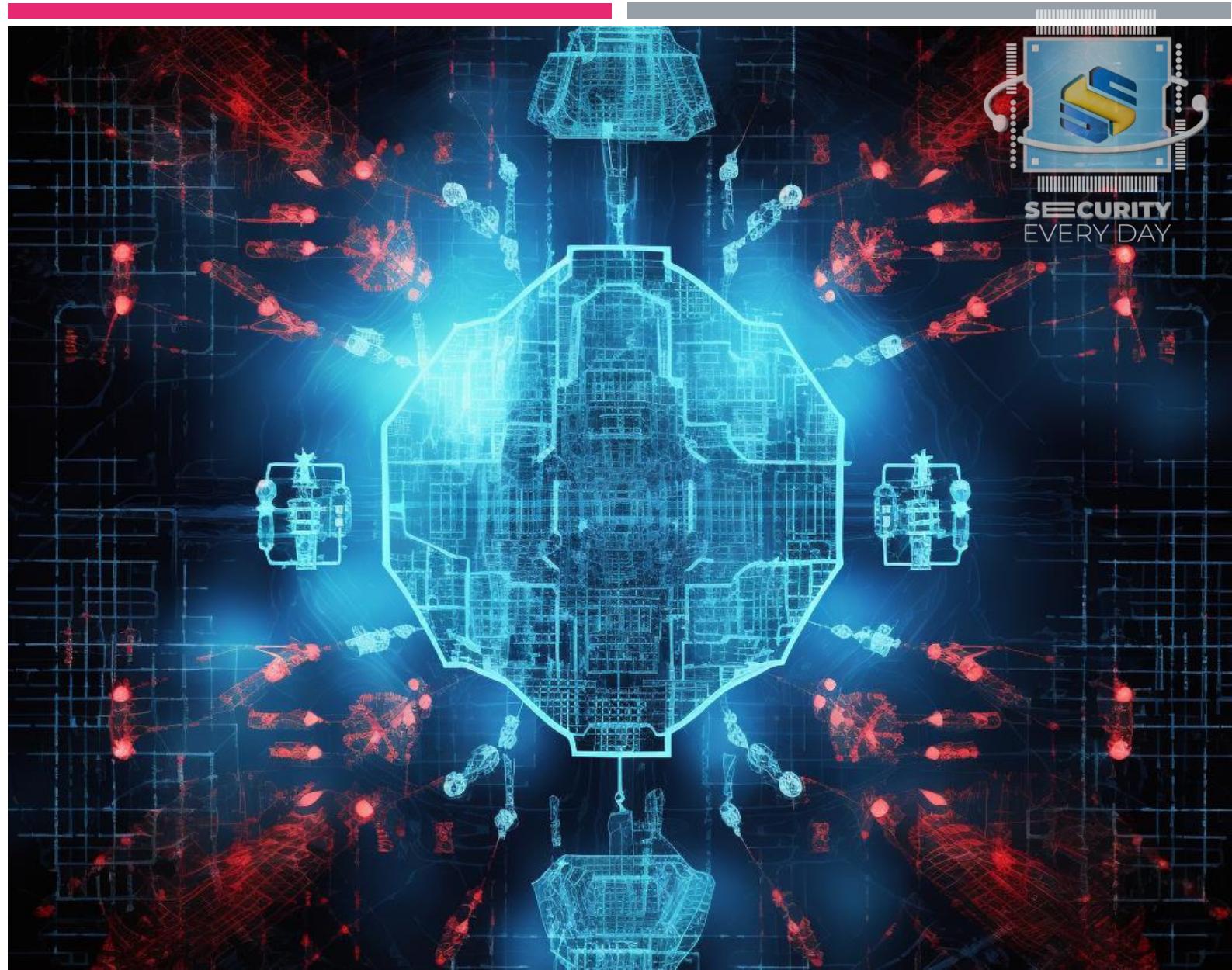
PREVENÇÃO X
DETECÇÃO



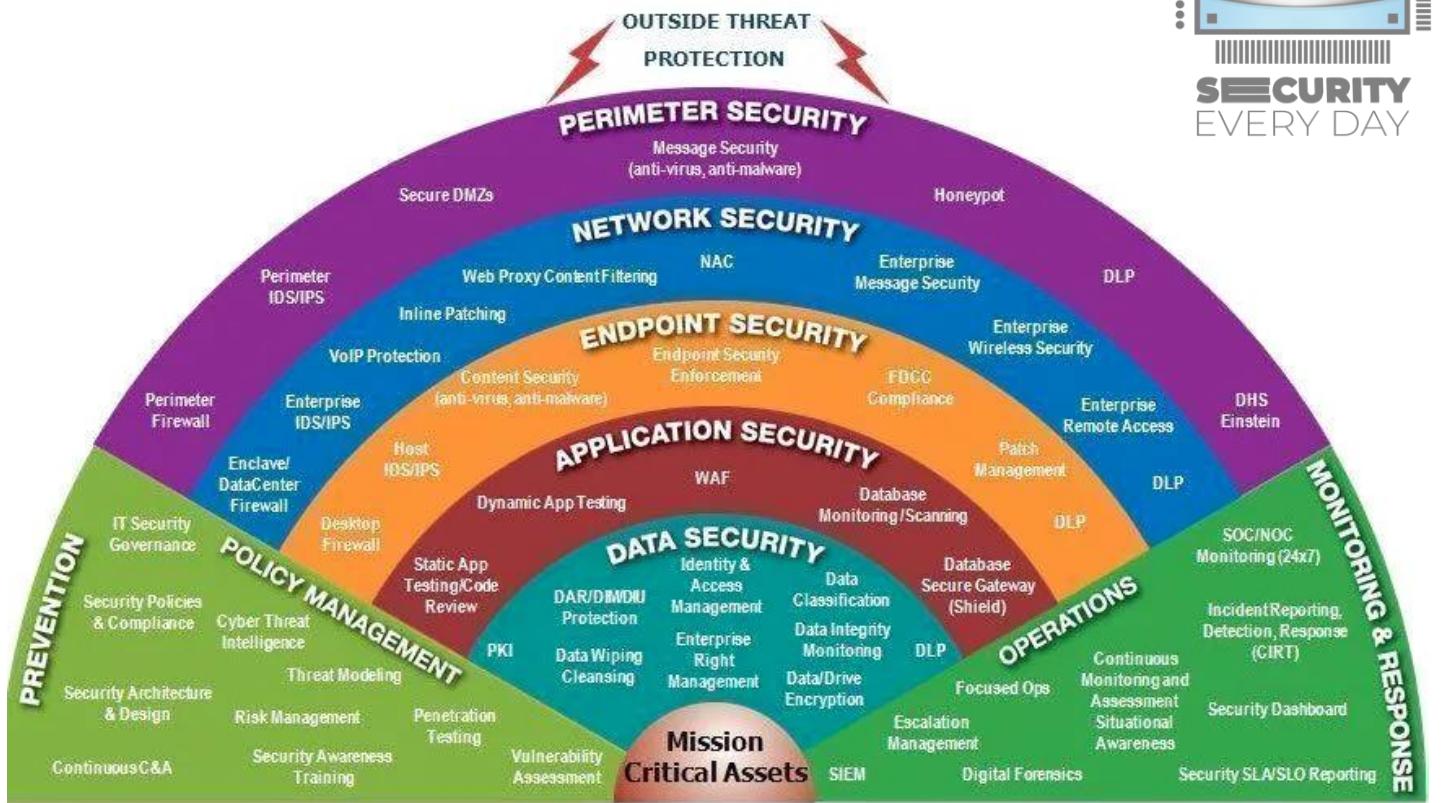
POR QUE
MONITORAR?

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



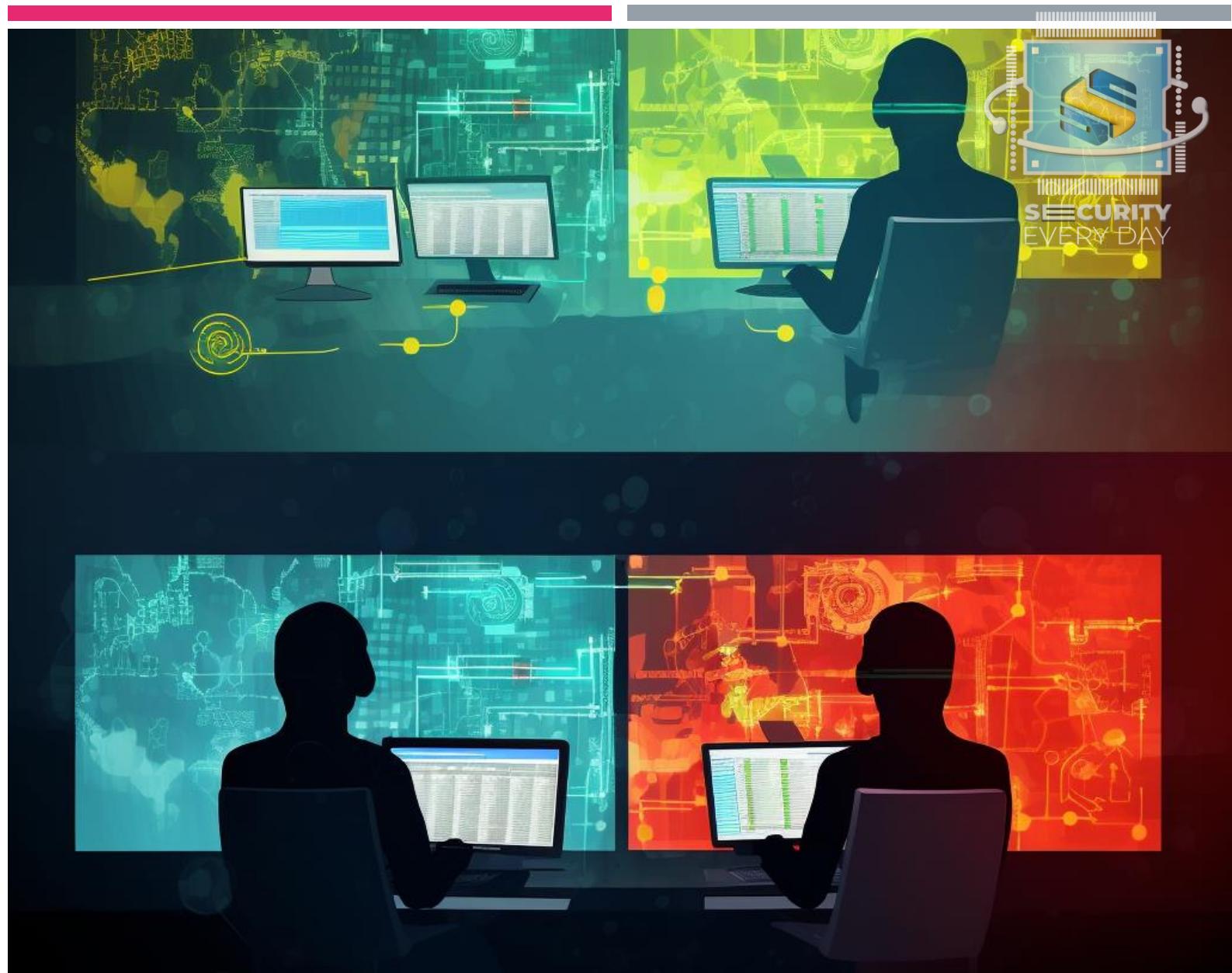
QUAIS SÃO AS EQUIPES QUE COMPÕEM?

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



PREVENÇÃO VS DETECÇÃO

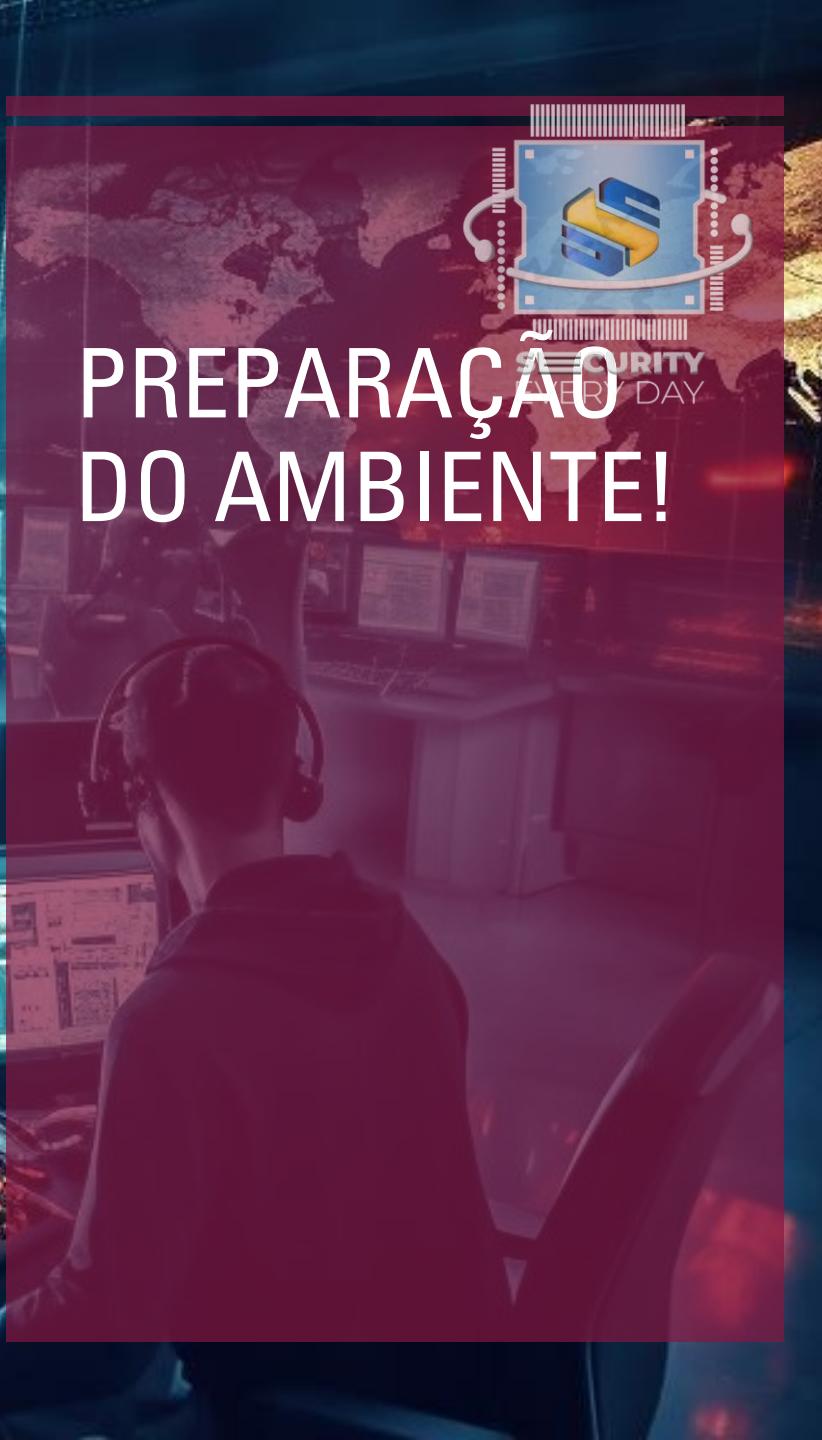
- Prevenção
 - Controle de acesso
 - Proteção de perimetro
 - Criptografia de dados
 - Gestão de vulnerabilidades
- Detecção
 - Monitoramento de eventos
 - Sistemas de detecção de intrusão
 - Ferramentas de SIEM
 - Análise de tráfego de rede



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>

VMware Workstation 17 Pro



VMWARE
WORKSTATION
PRO™
17

Workstation 17 Pro improves on the industry defining technology with DirectX 11 and OpenGL 4.3 3D Accelerated graphics support, a dark mode user interface, support for Windows 11, the vcli CLI for running and building containers and Kubernetes clusters, added support for the latest Windows and Linux operating systems, and more.

Use the links below to start your free, fully functional 30-day trial, no registration required.

Workstation 17 Pro for Windows

[DOWNLOAD NOW >](#)

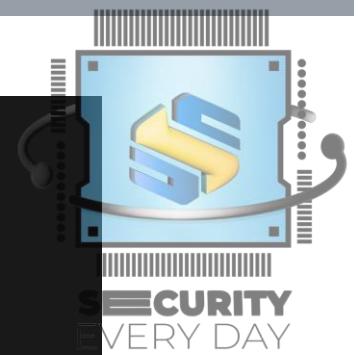
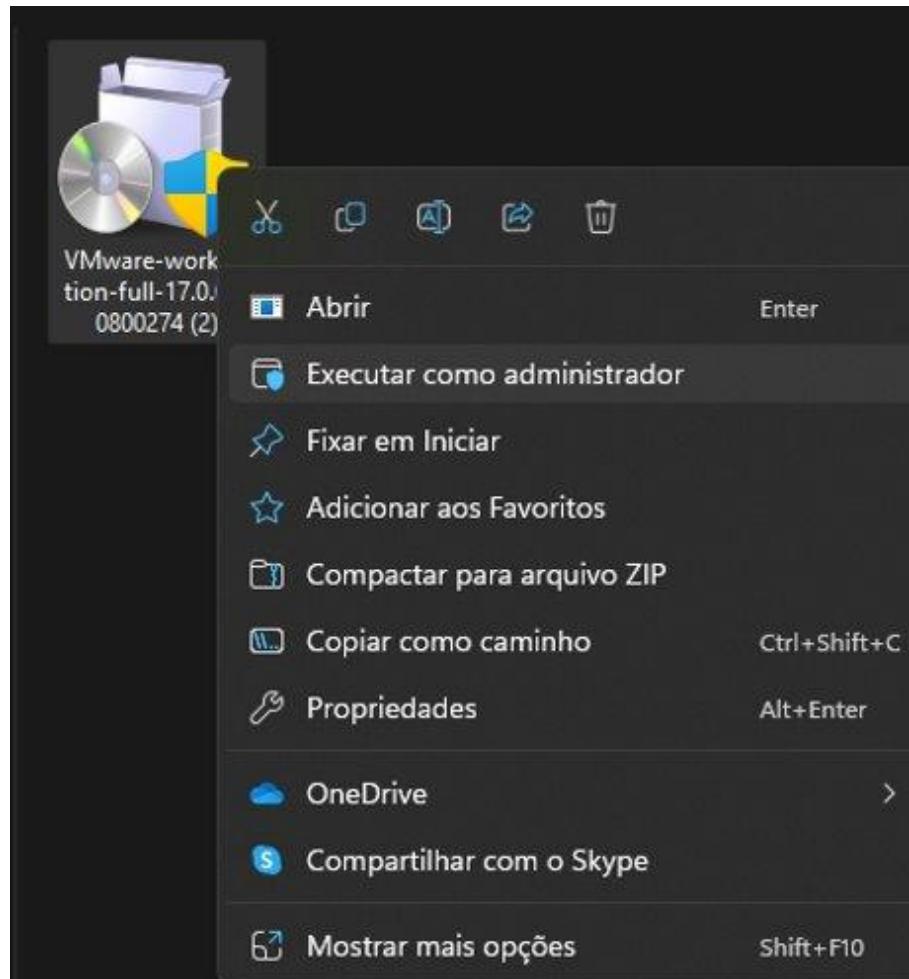
Workstation 17 Pro for Linux

[DOWNLOAD NOW >](#)



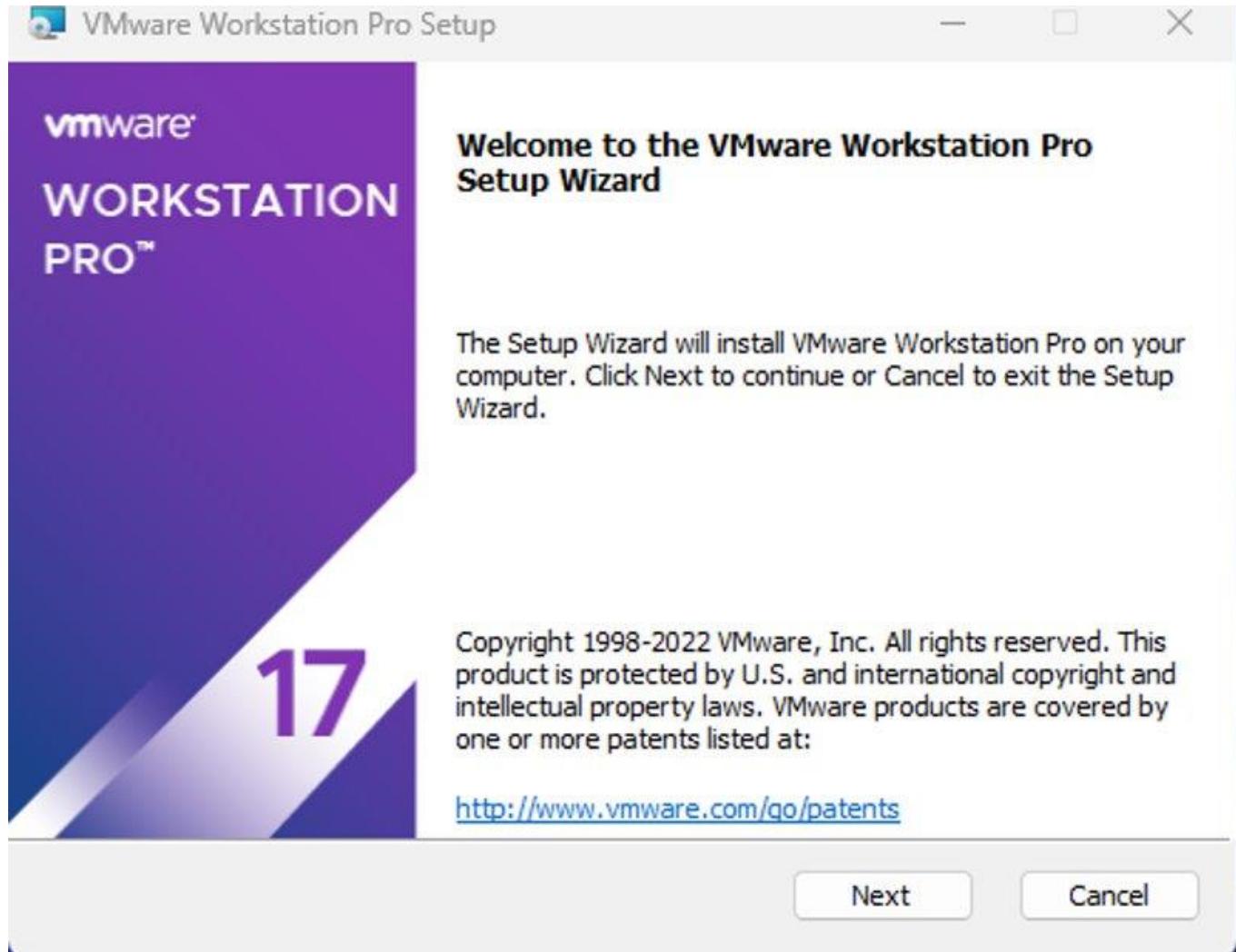
INSTALAÇÃO DO VMWARE WORKSTATION

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



INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



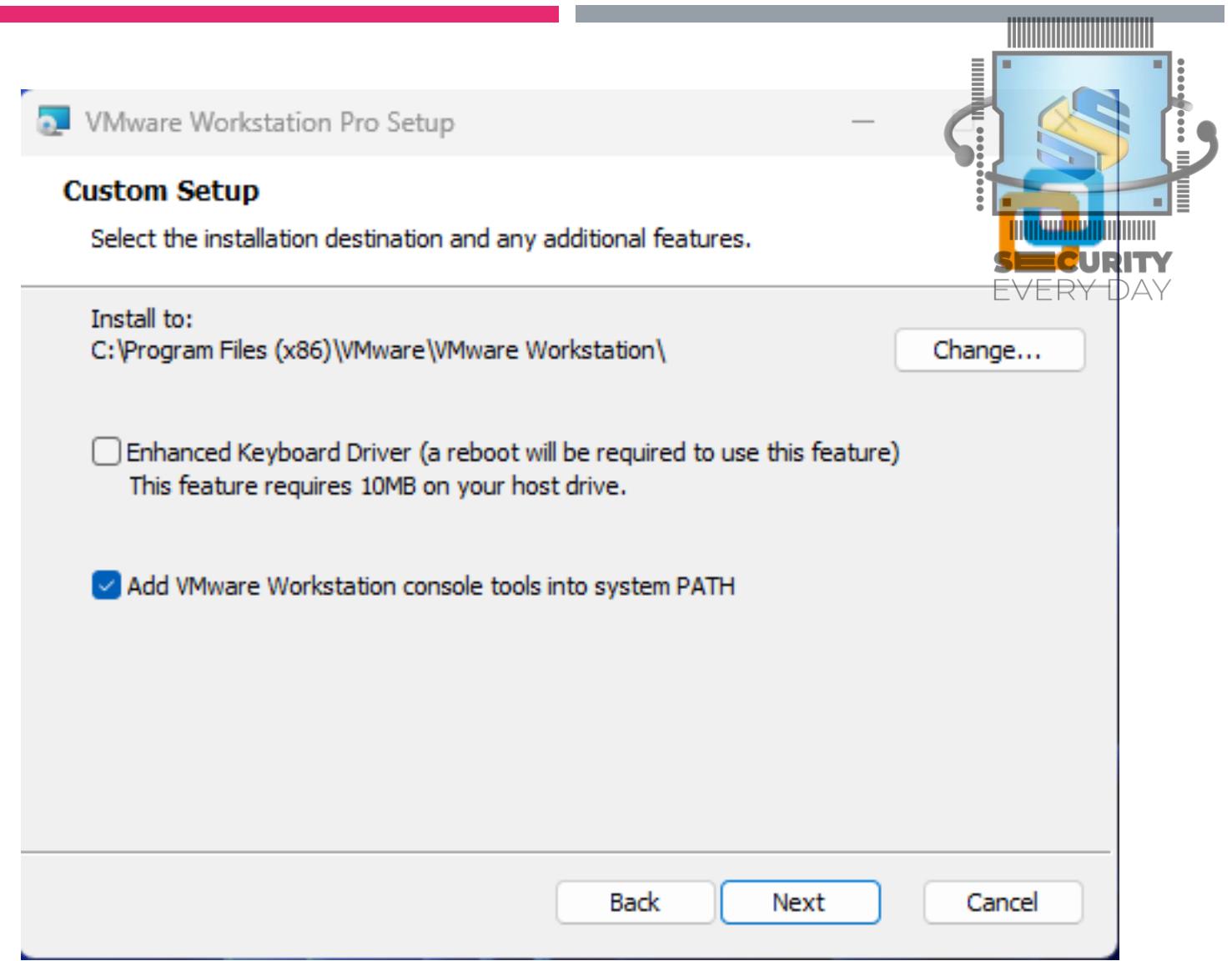
INSTALAÇÃO DO VMWARE WORKSTATION

- Aceite a licença e clique em "Next"



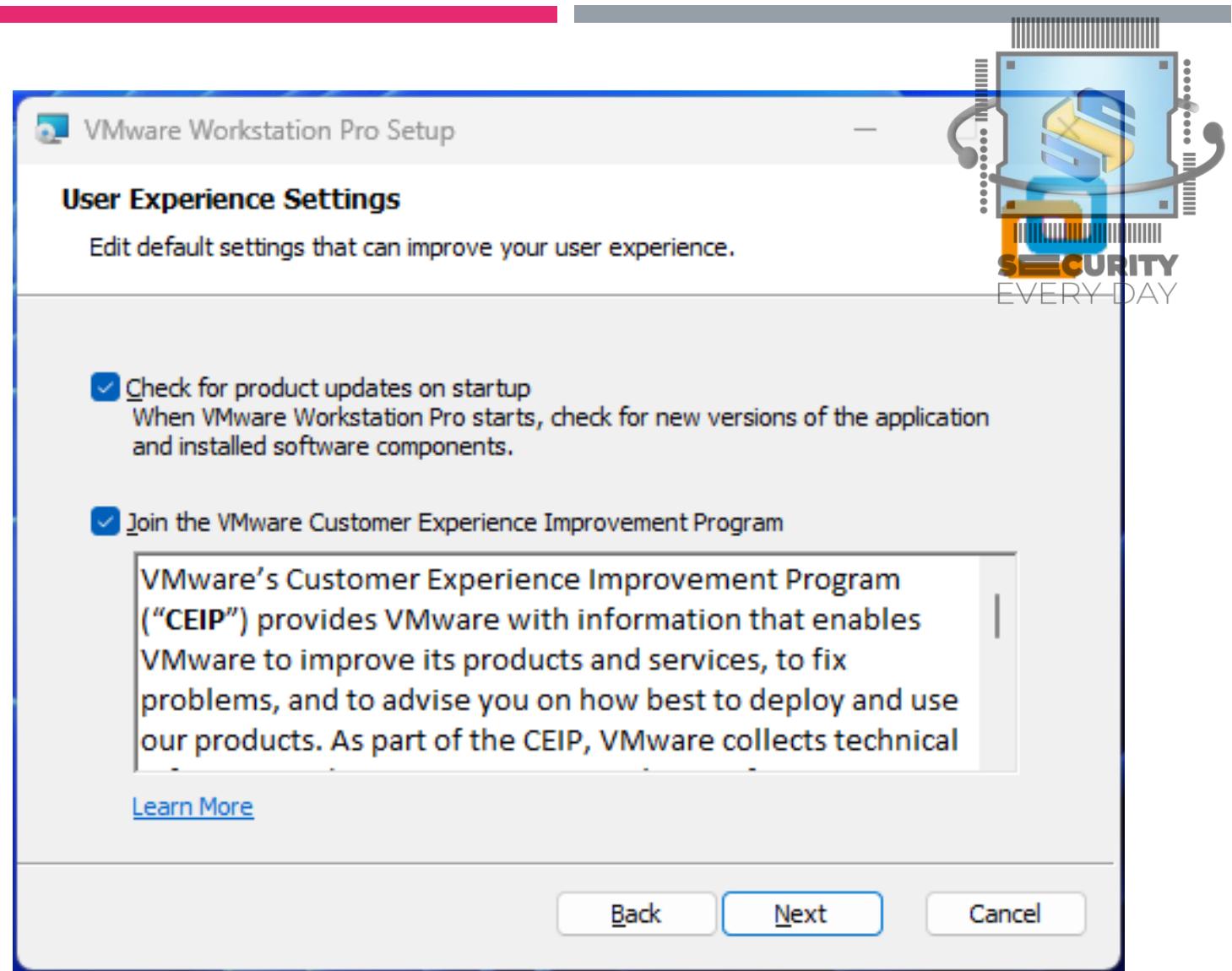
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



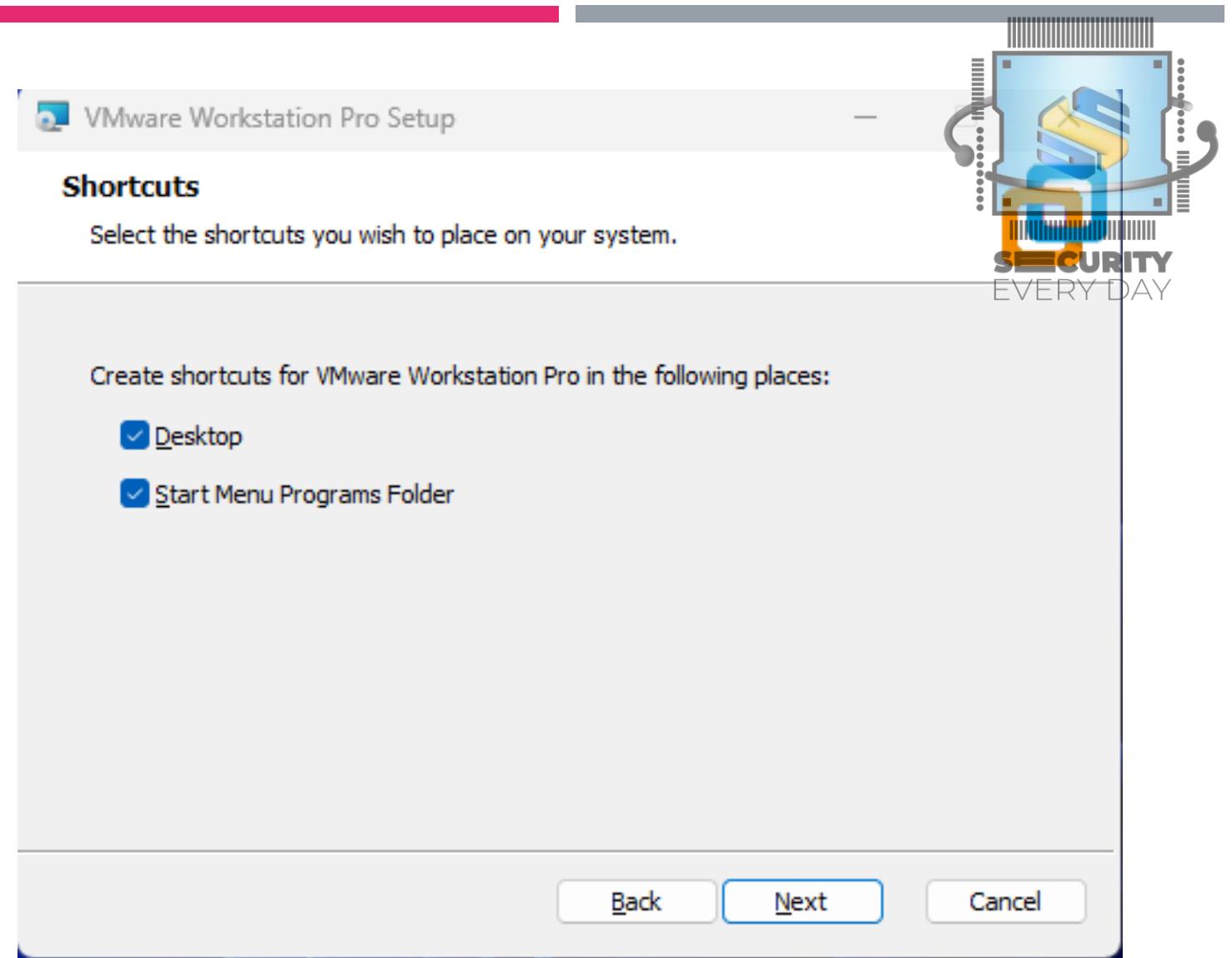
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



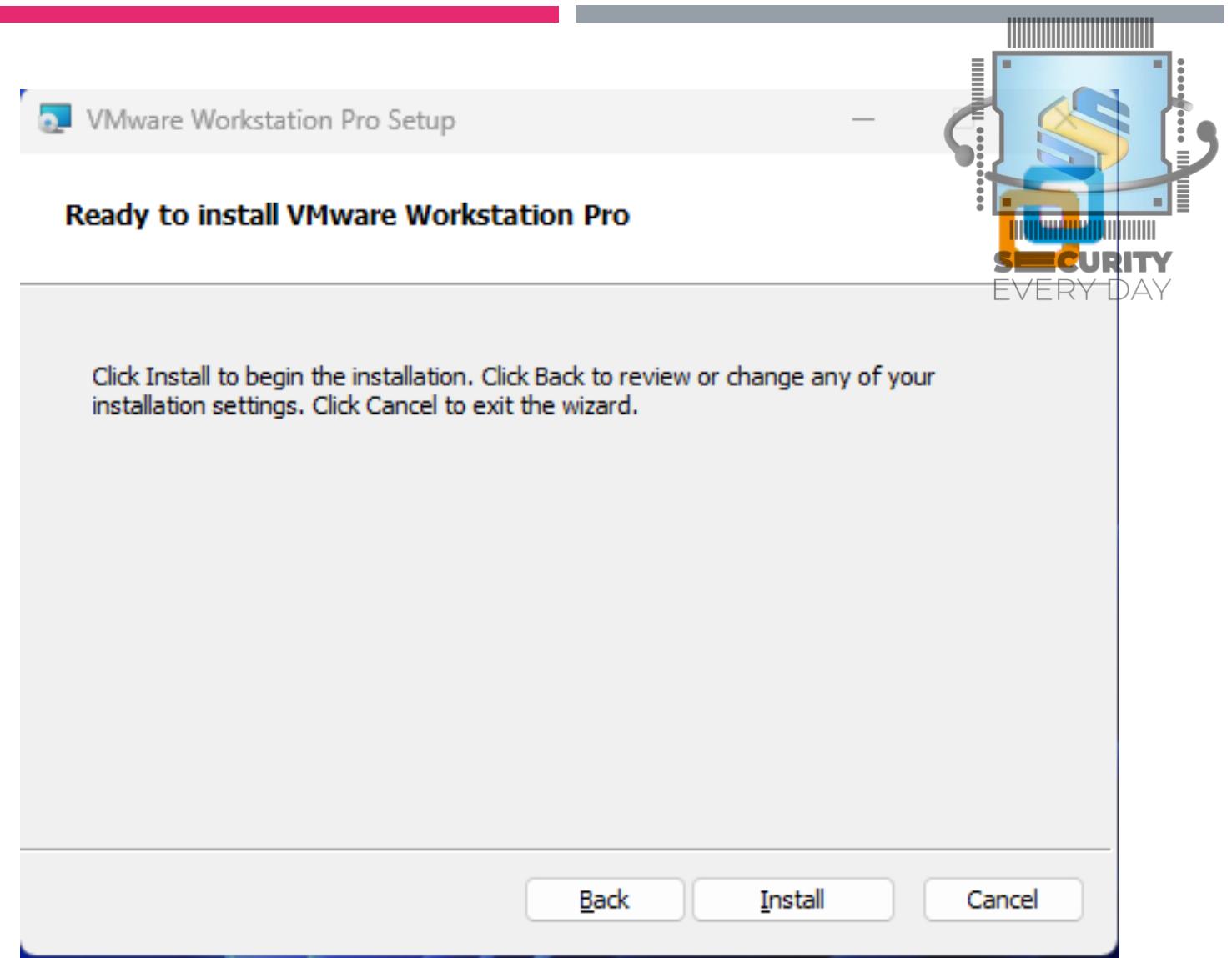
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Next"



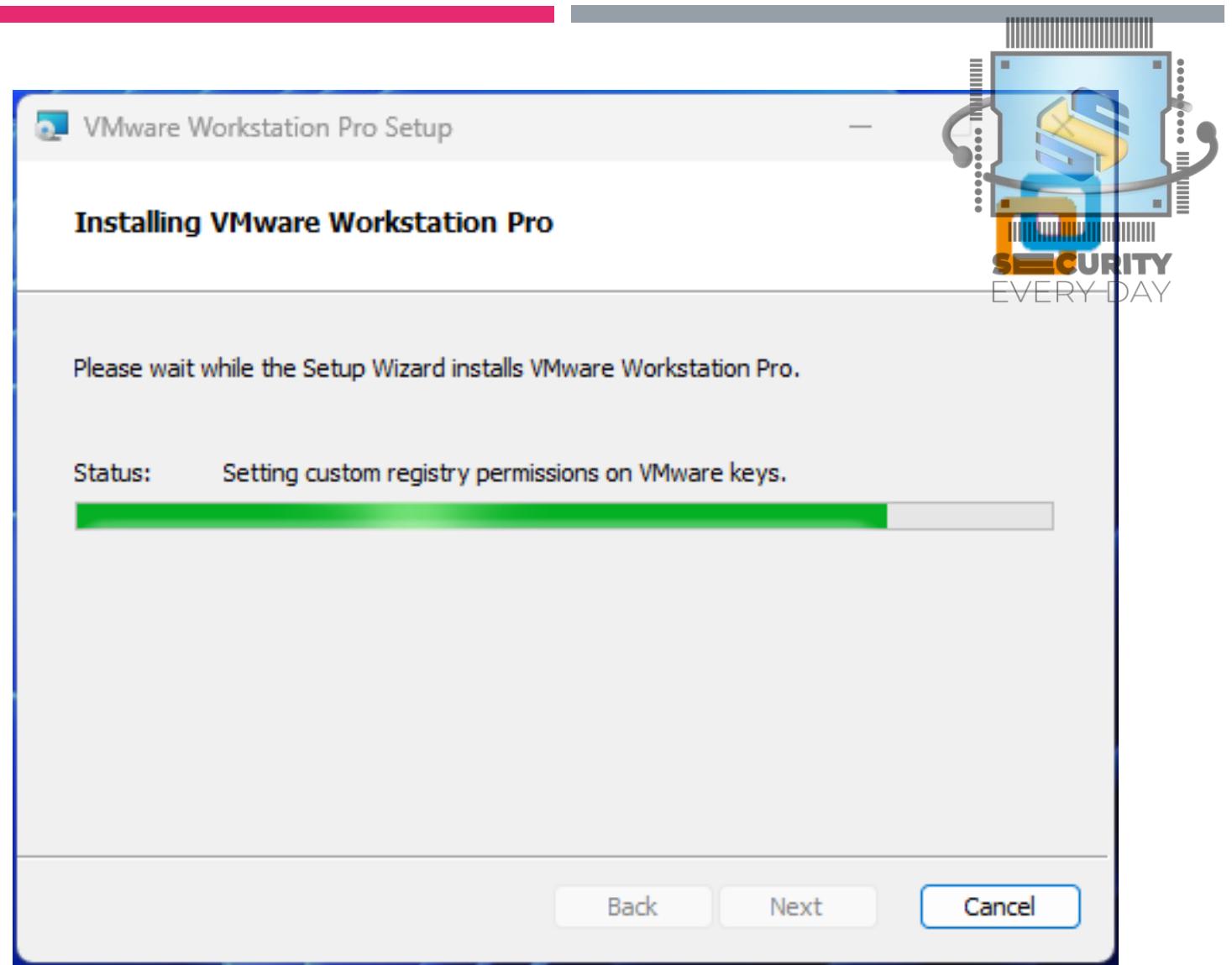
INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Install"



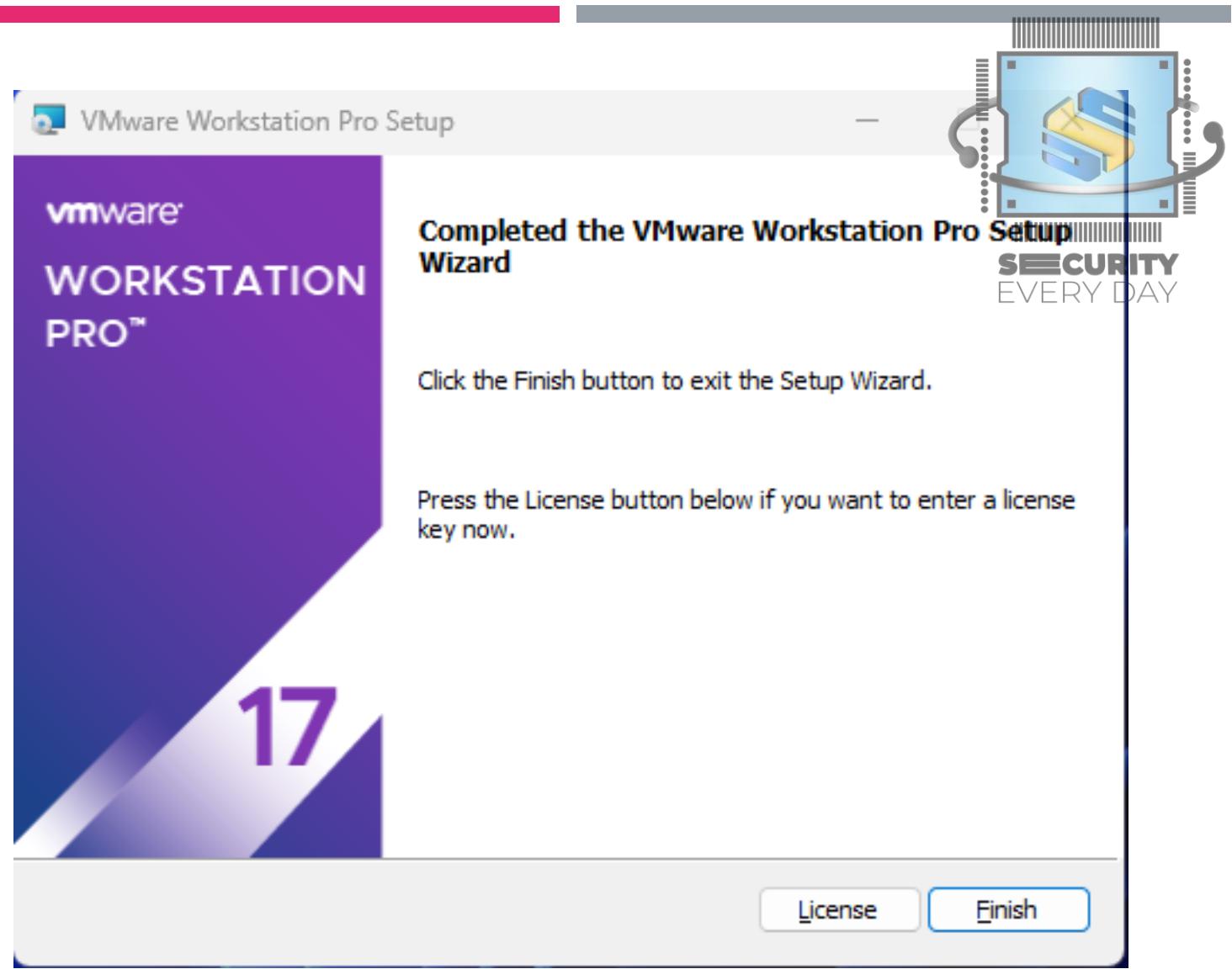
INSTALAÇÃO DO VMWARE WORKSTATION

- Aguarde a instalação ser finalizada



INSTALAÇÃO DO VMWARE WORKSTATION

- Clique em "Finish"



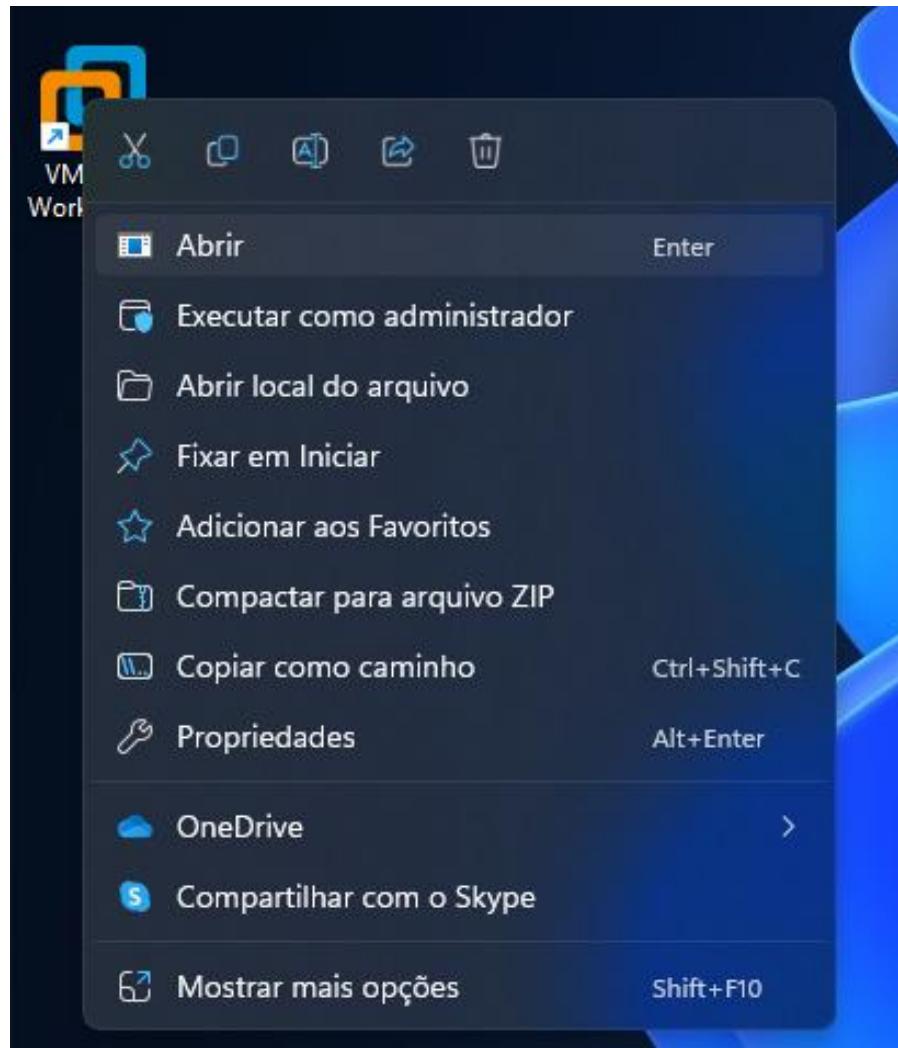
INSTALAÇÃO DO VMWARE WORKSTATION

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



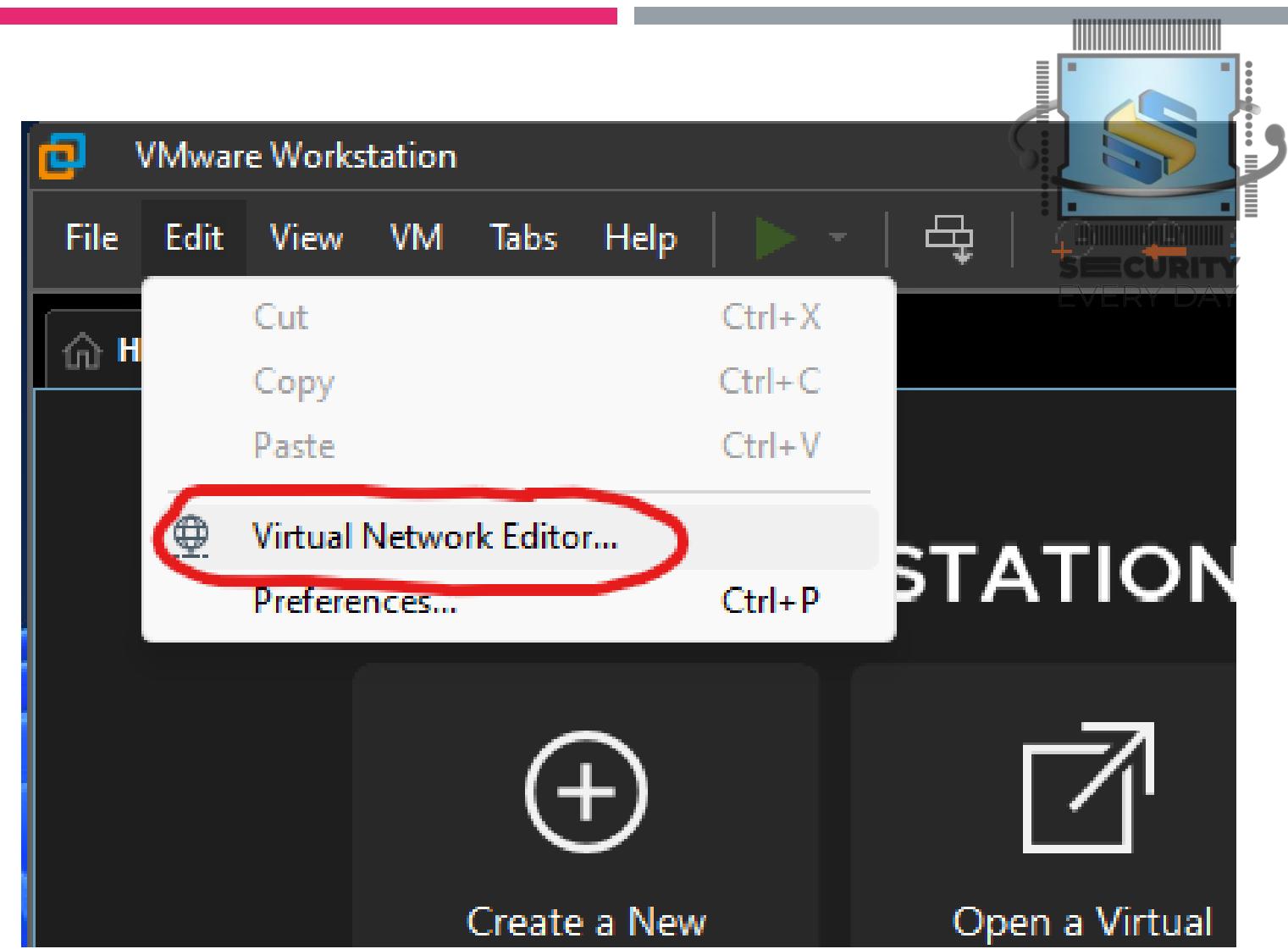
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



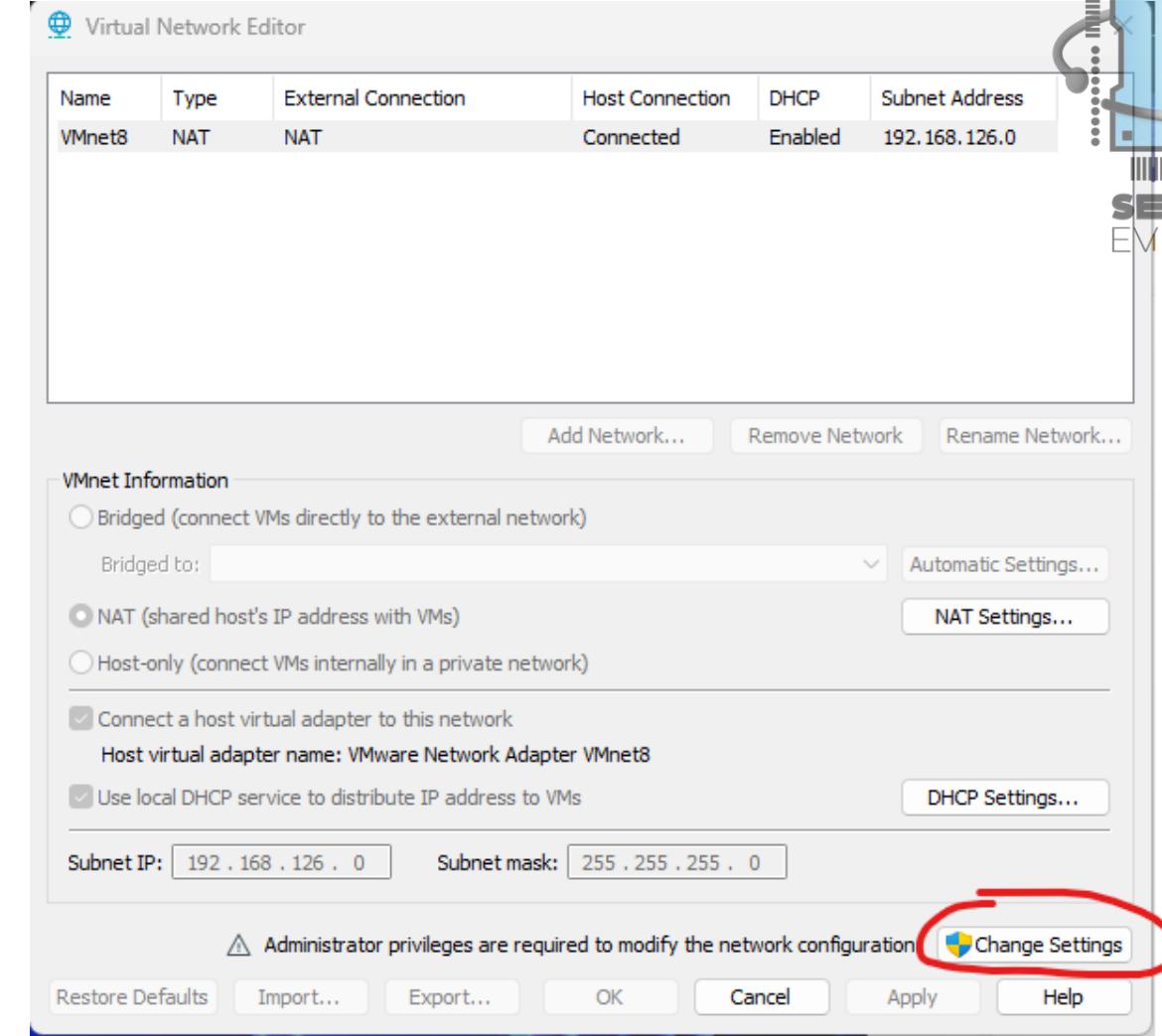
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



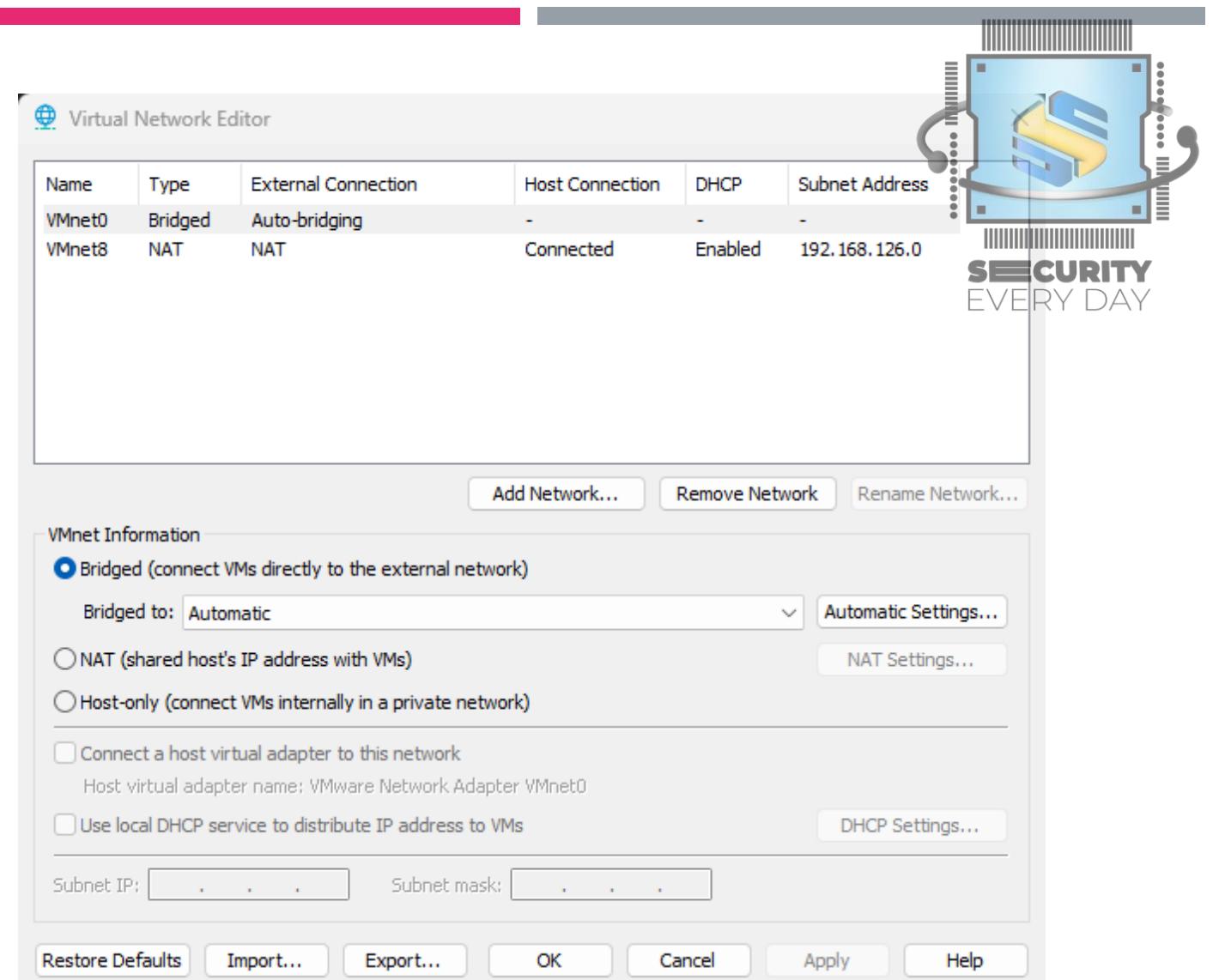
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



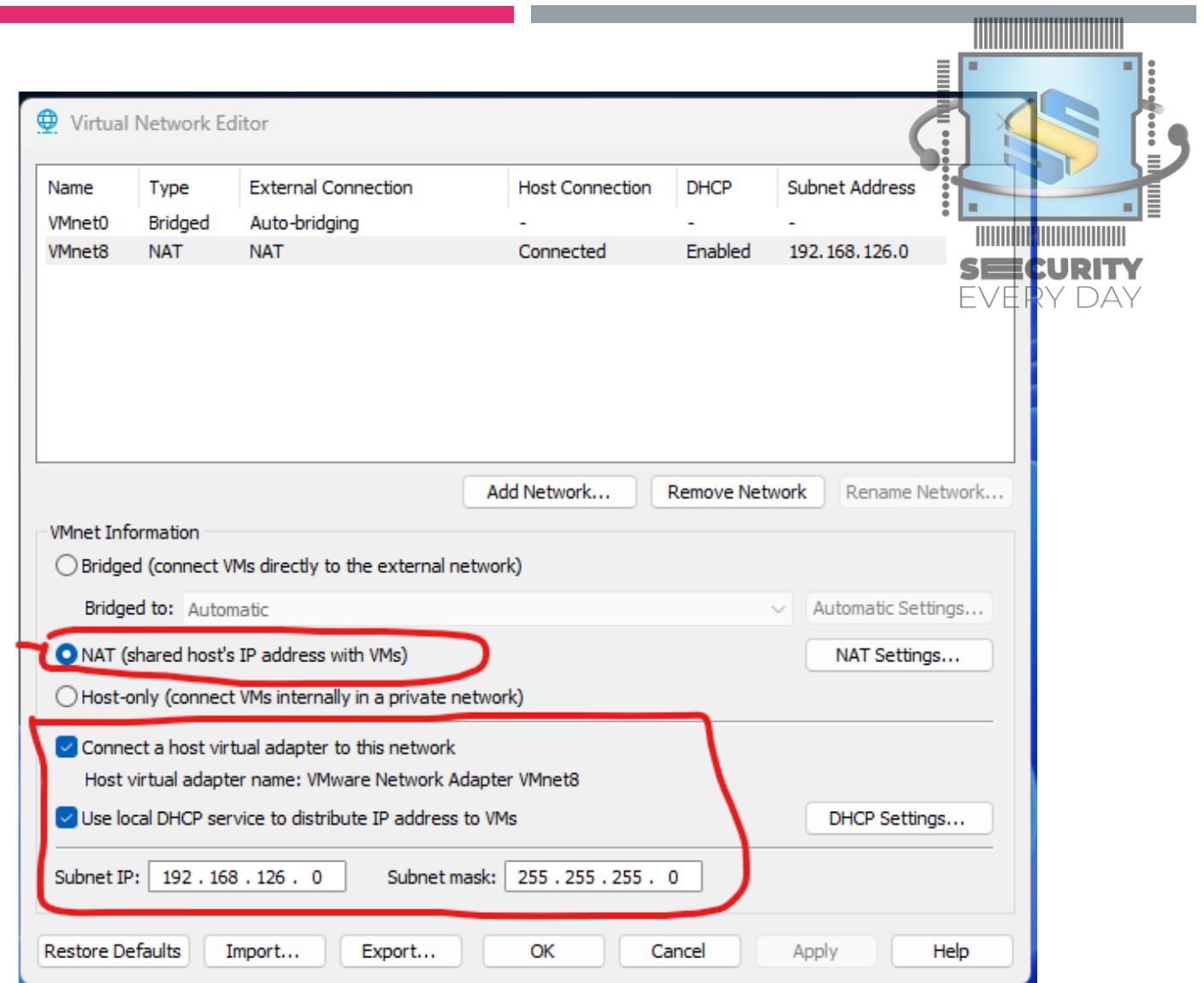
CONFIGURAÇÃO DO VMWARE WORKSTATION

- 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.



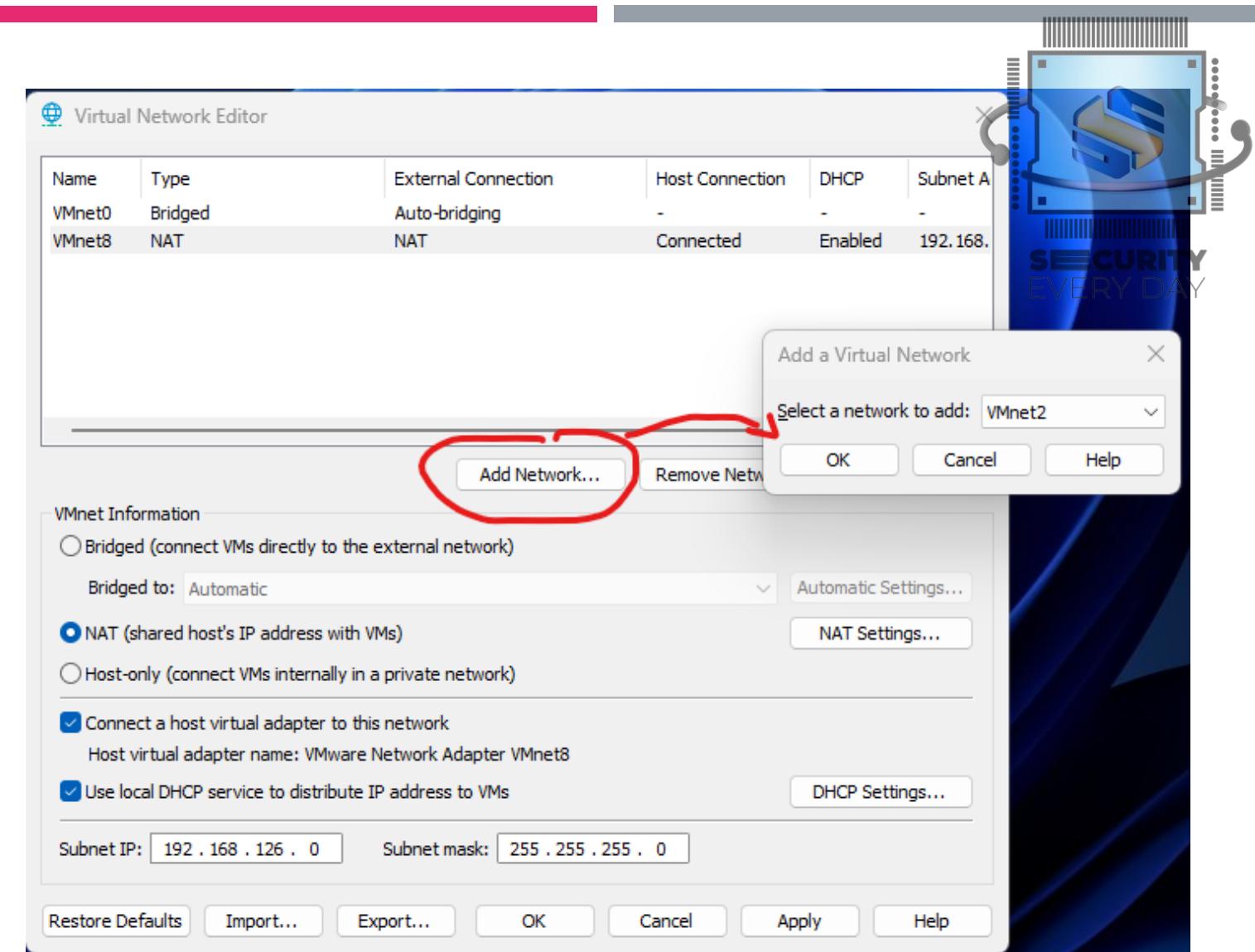
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



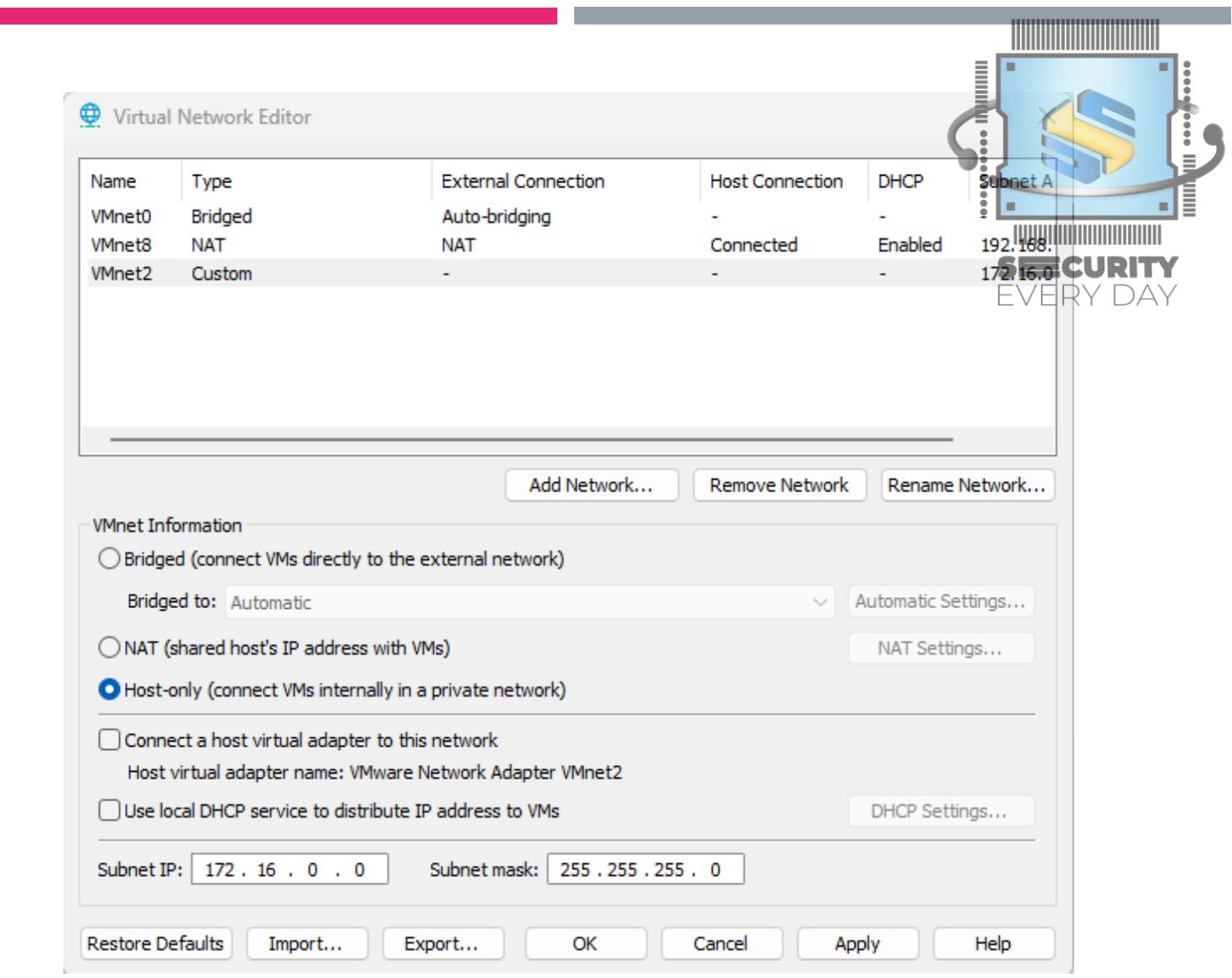
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



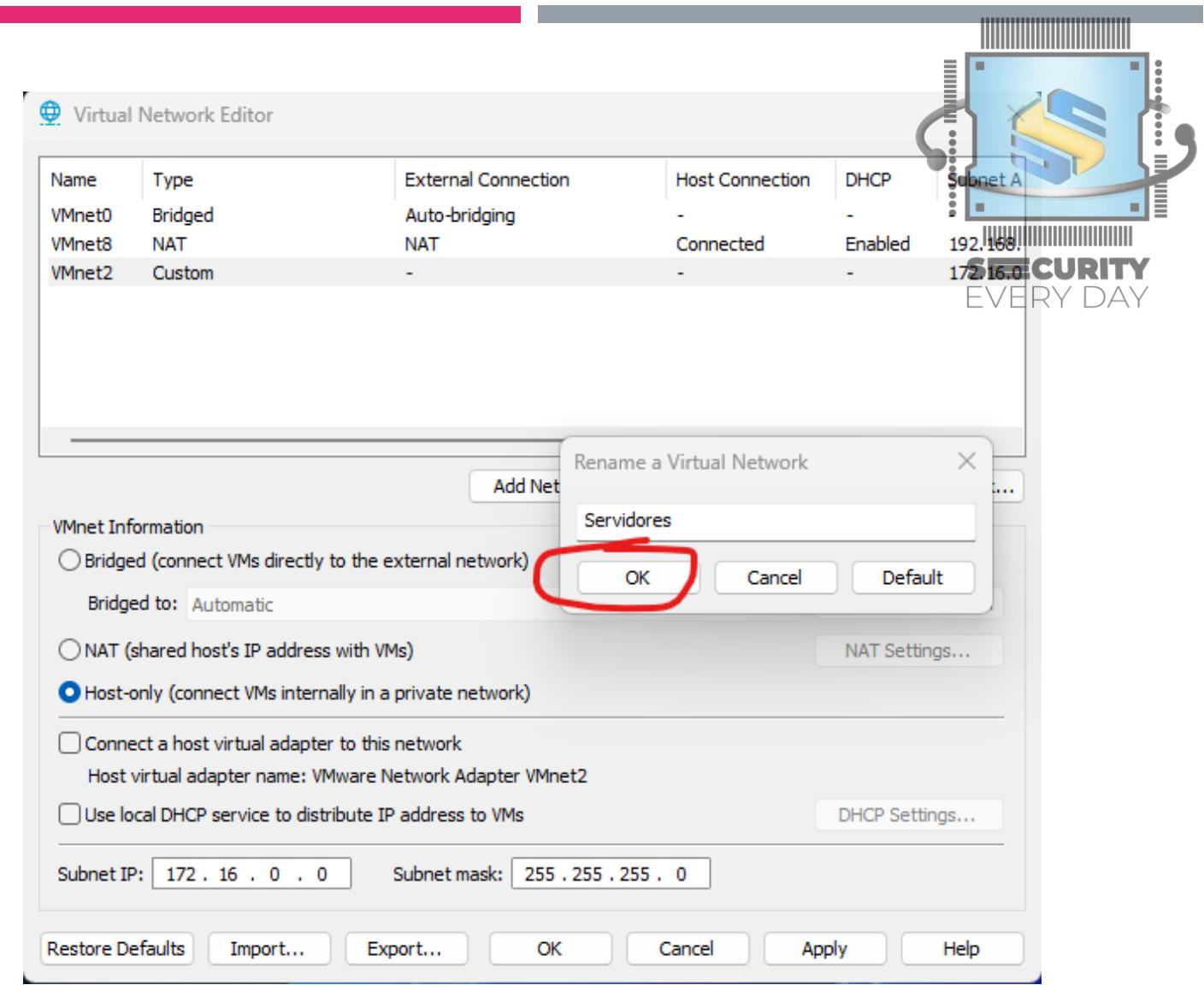
CONFIGURAÇÃO DO VMWARE WORKSTATION

- 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"



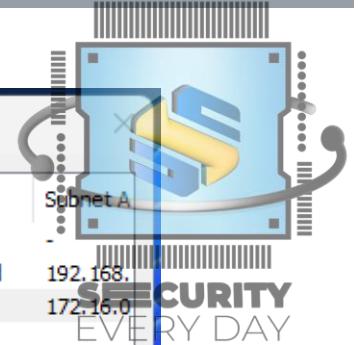
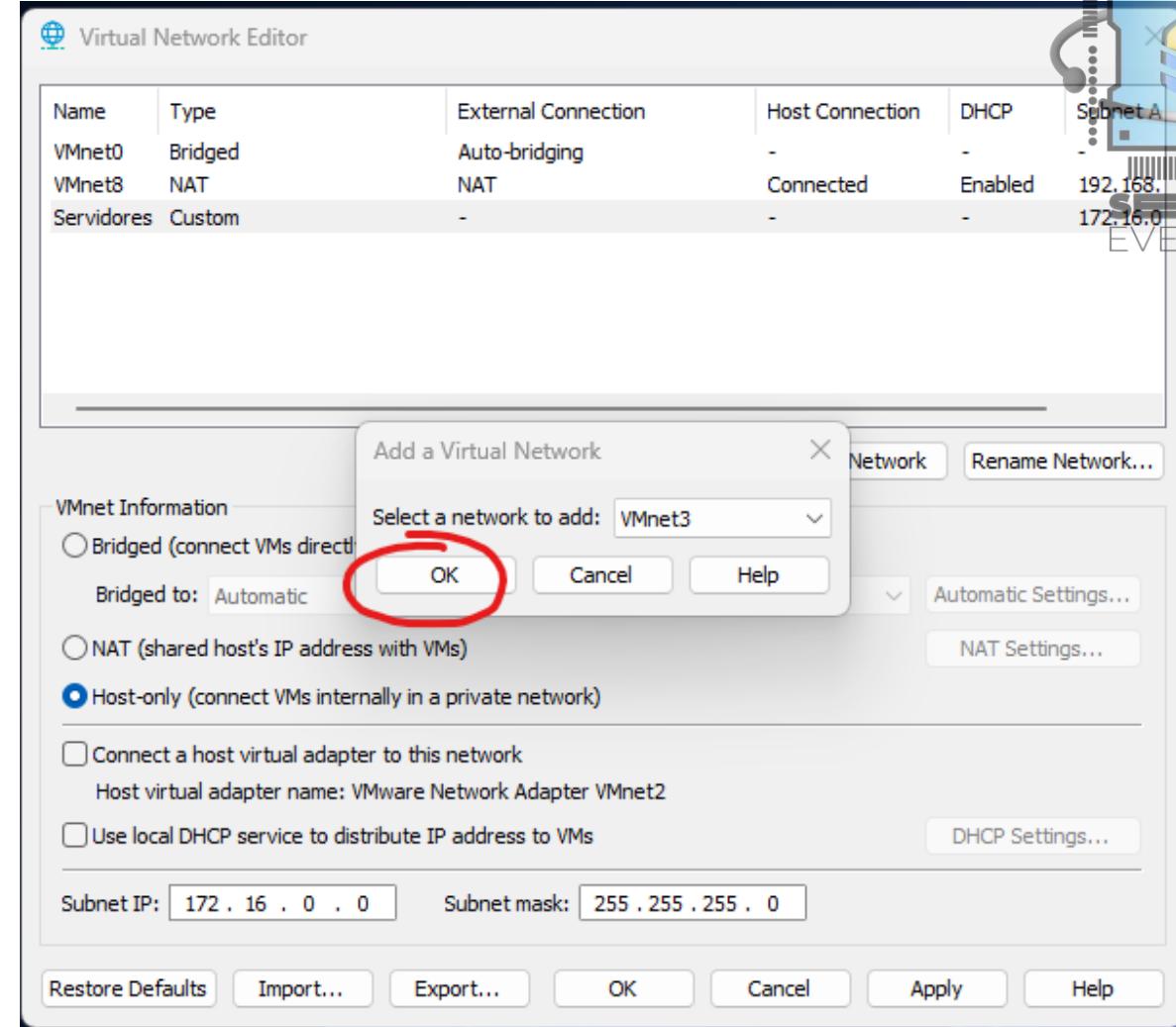
CONFIGURAÇÃO DO VMWARE WORKSTATION

- 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"



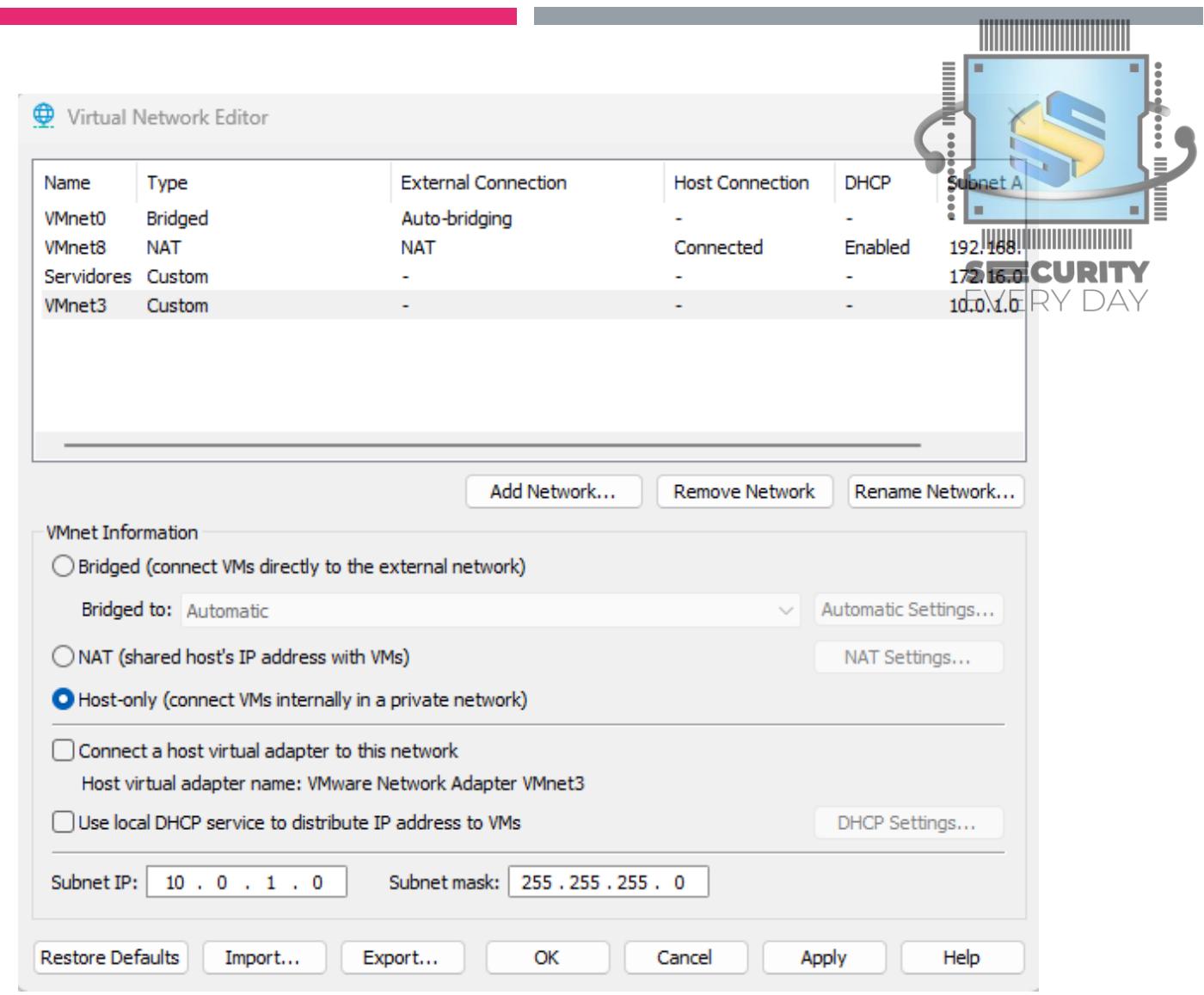
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



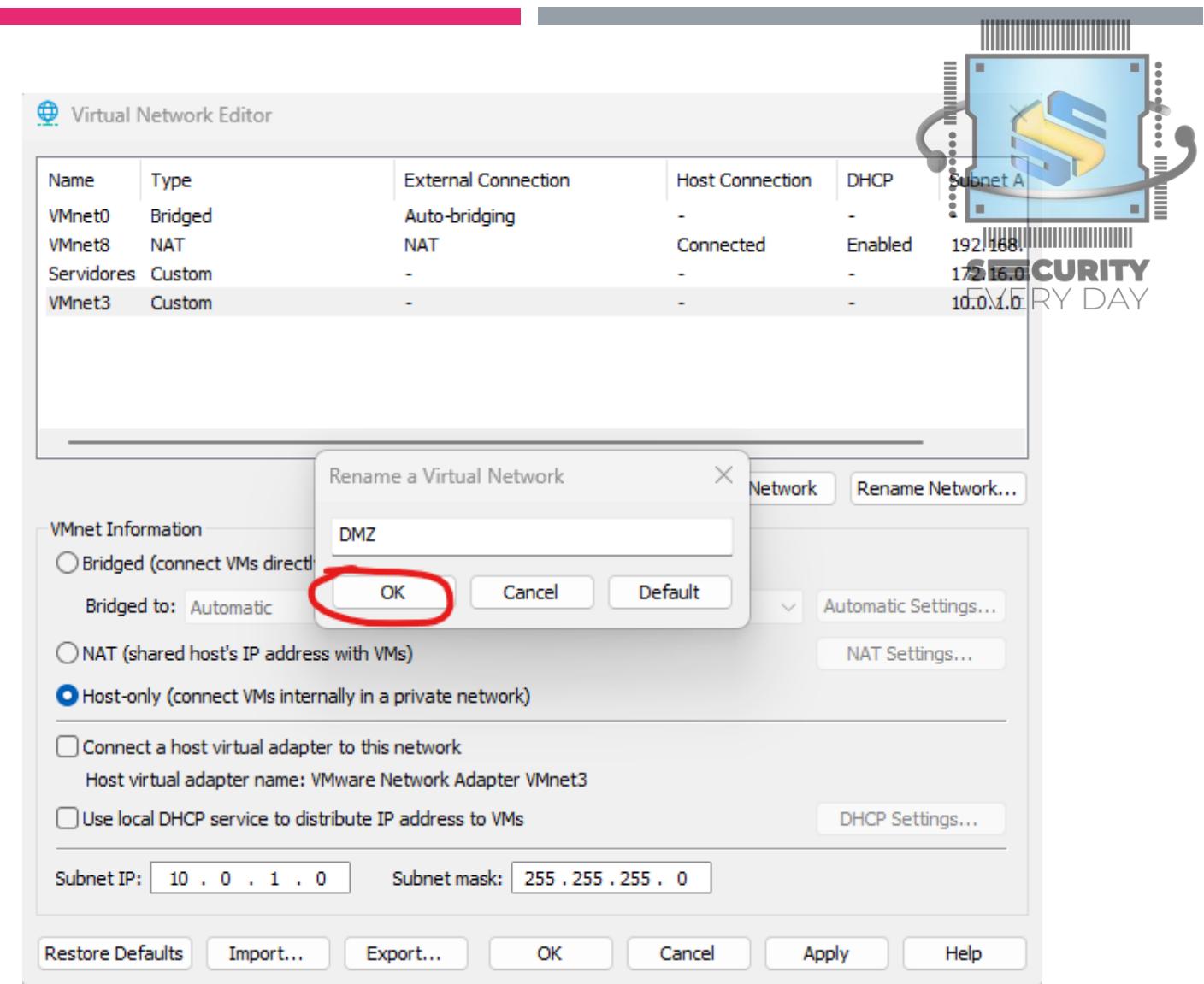
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



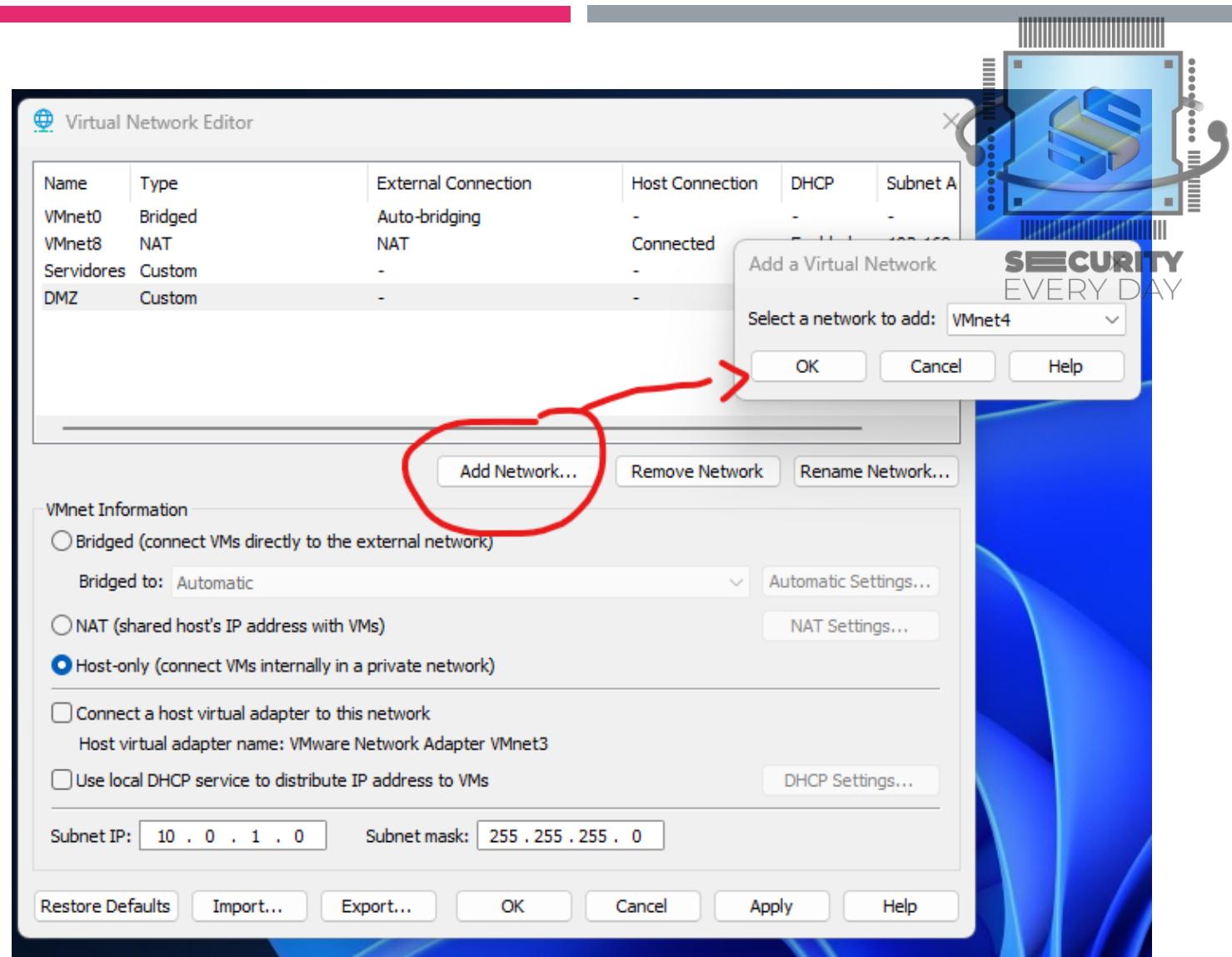
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



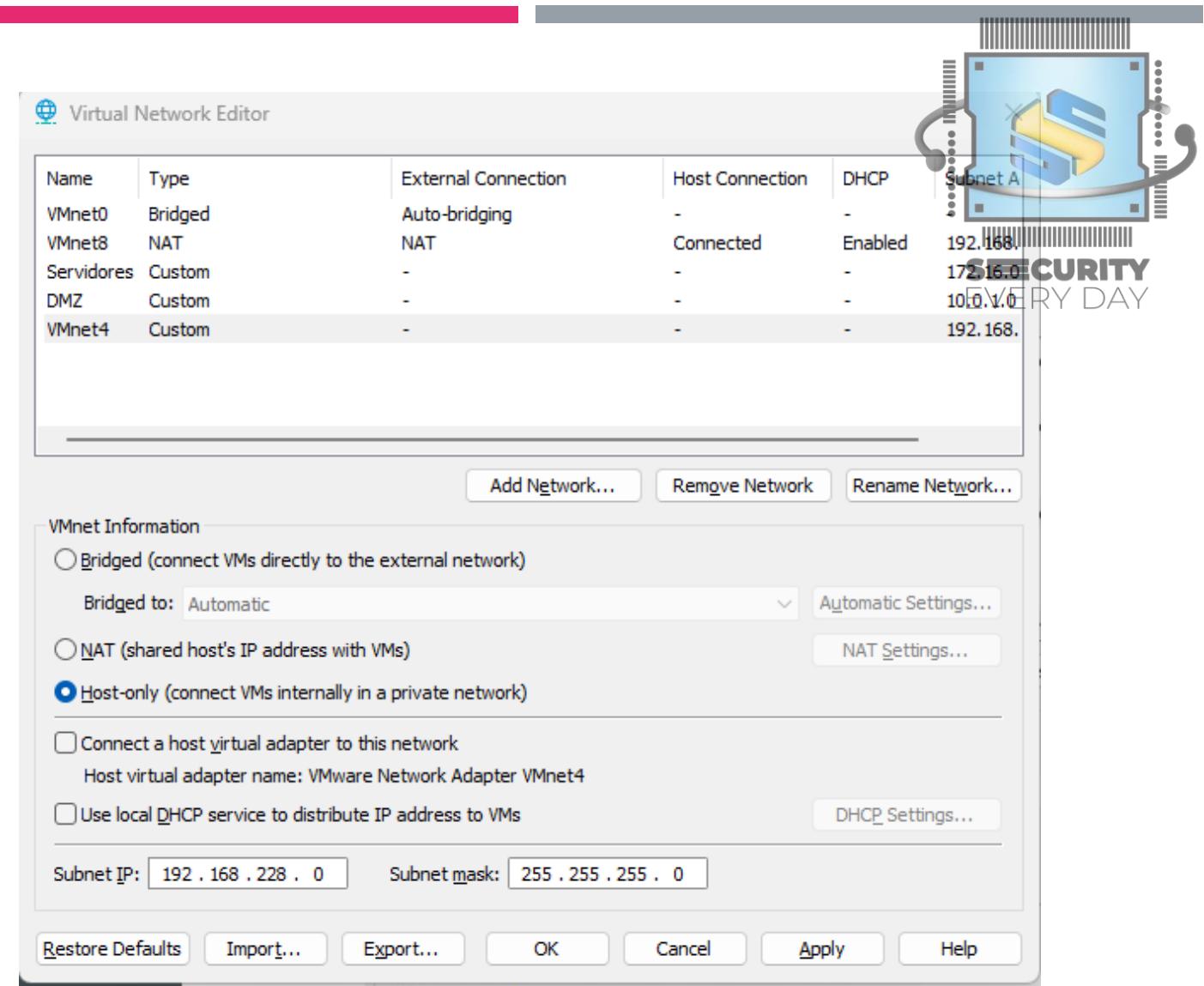
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



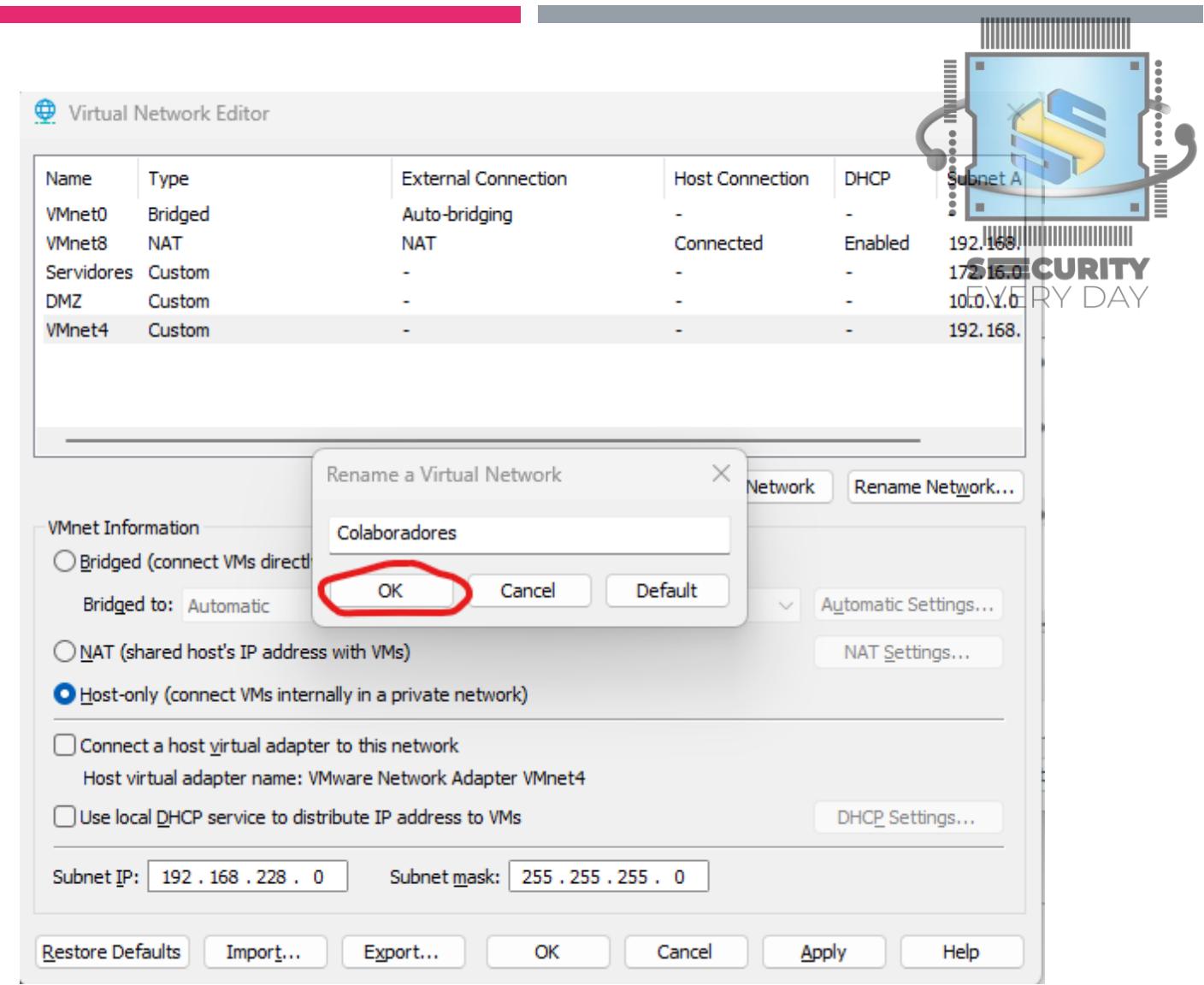
CONFIGURAÇÃO DO VMWARE WORKSTATION

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



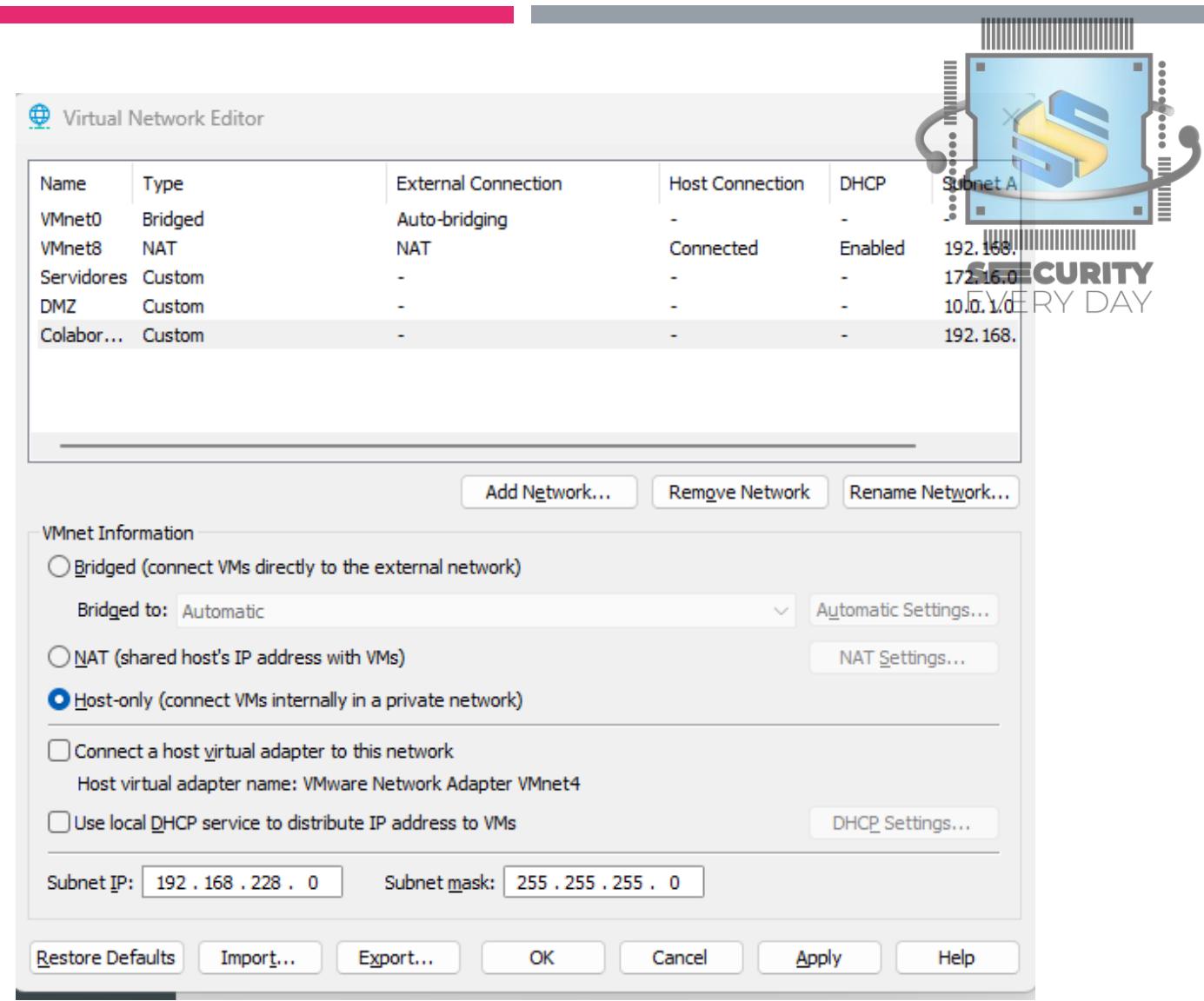
CONFIGURAÇÃO DO VMWARE WORKSTATION

- 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

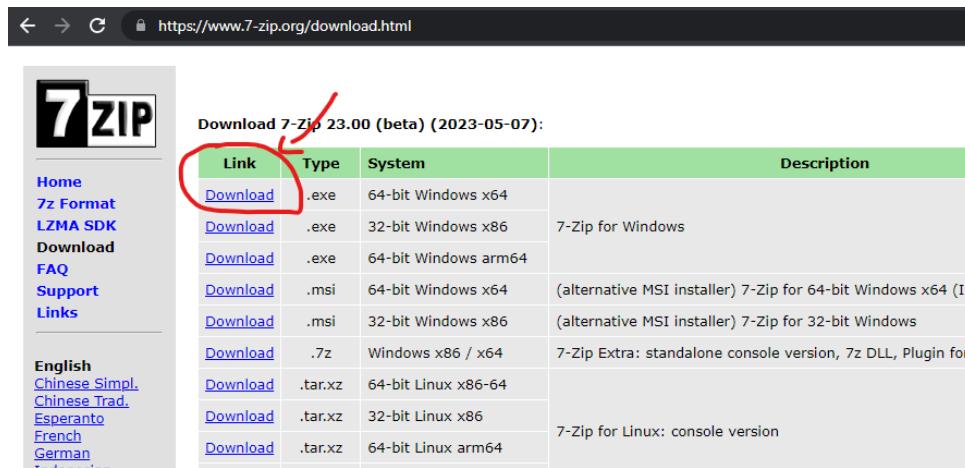
- Realize o download das maquinas no link
 - https://1drv.ms/f/s!Asw32WKX_XOWiPFuTs1_XoEsiC2bKw

VMs				
	Nome ↑ ▾	Modificado em	Tamanho do arq... ▾	Compartilhamento
1	Domain Controller - Servidores.7z	Ontem às 14:53:04	7.72 GB	Compartilhado
2	Firewall.7z	Ontem às 12:54:12	1.18 GB	Compartilhado
3	Library - DMZ.7z	Ontem às 13:27:57	2.72 GB	Compartilhado
4	Web interno - Servidores.7z	Ontem às 13:57:20	2.73 GB	Compartilhado
5	Windows 10 - Colaboradores.7z	Ontem às 19:40:10	23.6 GB	Compartilhado



INSTALAÇÃO DO 7-ZIP

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



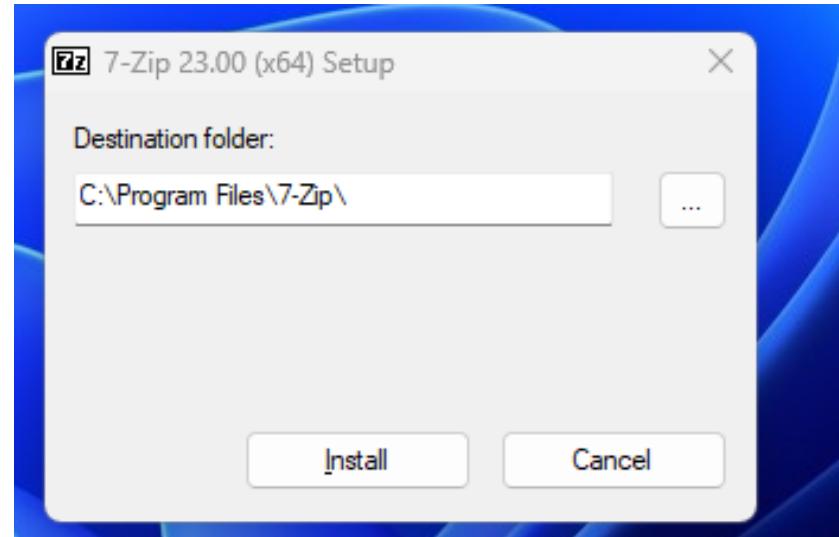
The screenshot shows the official 7-Zip download page at <https://www.7-zip.org/download.html>. The page features a sidebar with links like Home, 7z Format, LZMA SDK, Download, FAQ, Support, and Links. Below the sidebar is a language selection menu with English, Chinese Simpl., Chinese Trad., Esperanto, French, and German. The main content area is titled "Download 7-Zip 23.00 (beta) (2023-05-07)". A table lists download links for various platforms. The first row, which has a red circle around the "Link" column header, shows the Windows x64 MSI installer. A red arrow points from the text above the table to this header.

Link	Type	System	Description
Download	.exe	64-bit Windows x64	7-Zip for Windows
Download	.exe	32-bit Windows x86	(alternative MSI installer) 7-Zip for 32-bit Windows
Download	.exe	64-bit Windows arm64	
Download	.msi	64-bit Windows x64	(alternative MSI installer) 7-Zip for 64-bit Windows x64 (In
Download	.msi	32-bit Windows x86	(alternative MSI installer) 7-Zip for 32-bit Windows
Download	.7z	Windows x86 / x64	7-Zip Extra: standalone console version, 7z DLL, Plugin for
Download	.tar.xz	64-bit Linux x86-64	
Download	.tar.xz	32-bit Linux x86	
Download	.tar.xz	64-bit Linux arm64	7-Zip for Linux: console version



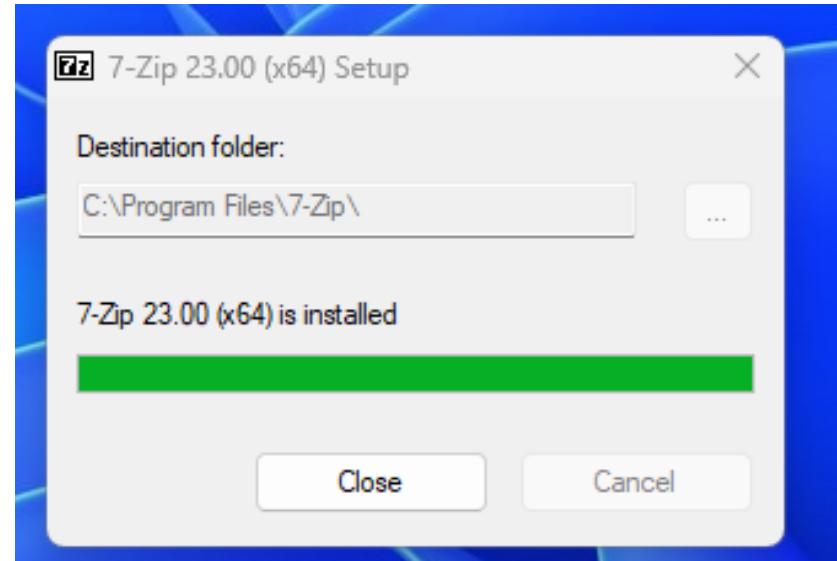
INSTALAÇÃO DO 7-ZIP

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



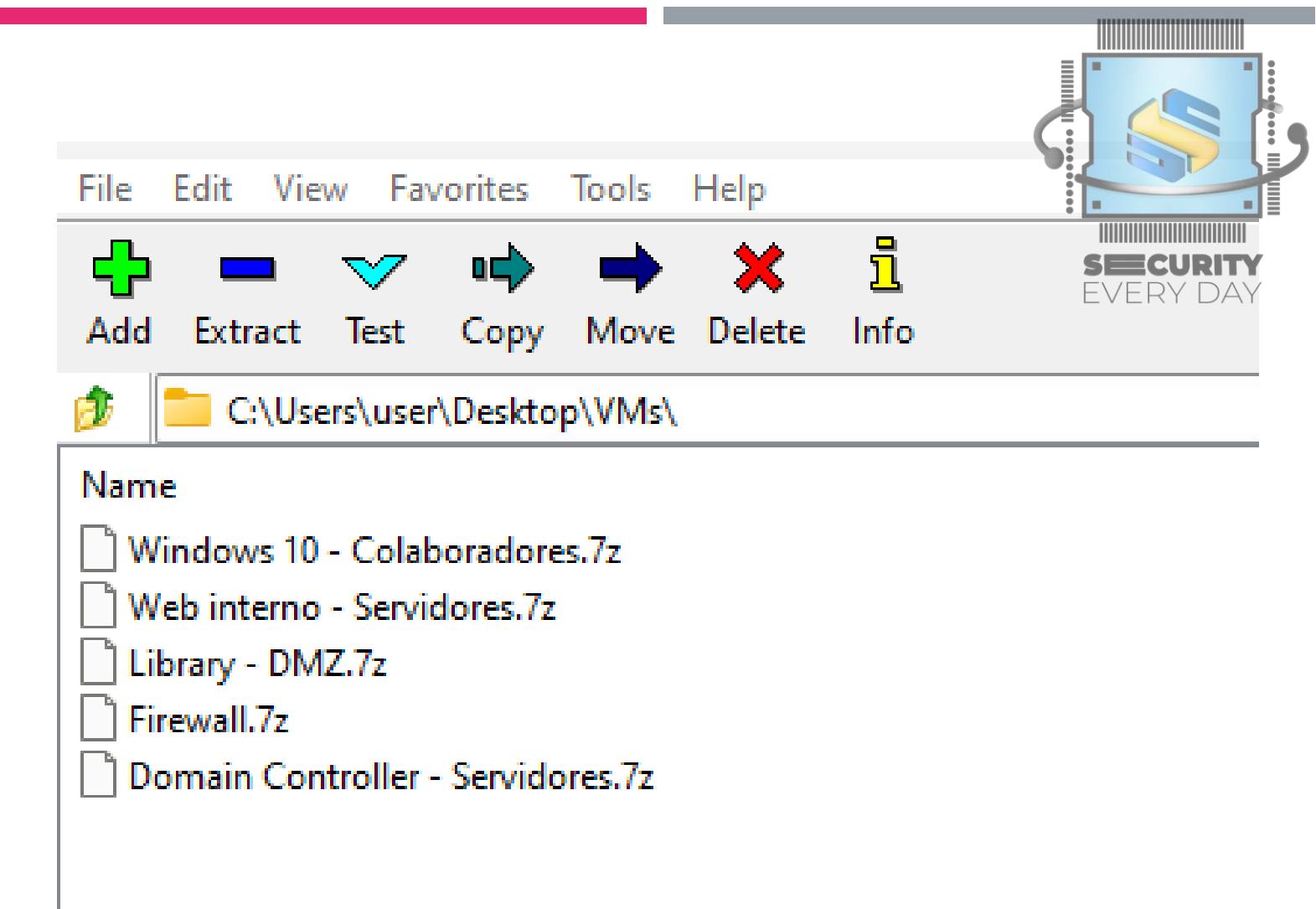
INSTALAÇÃO DO 7-ZIP

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



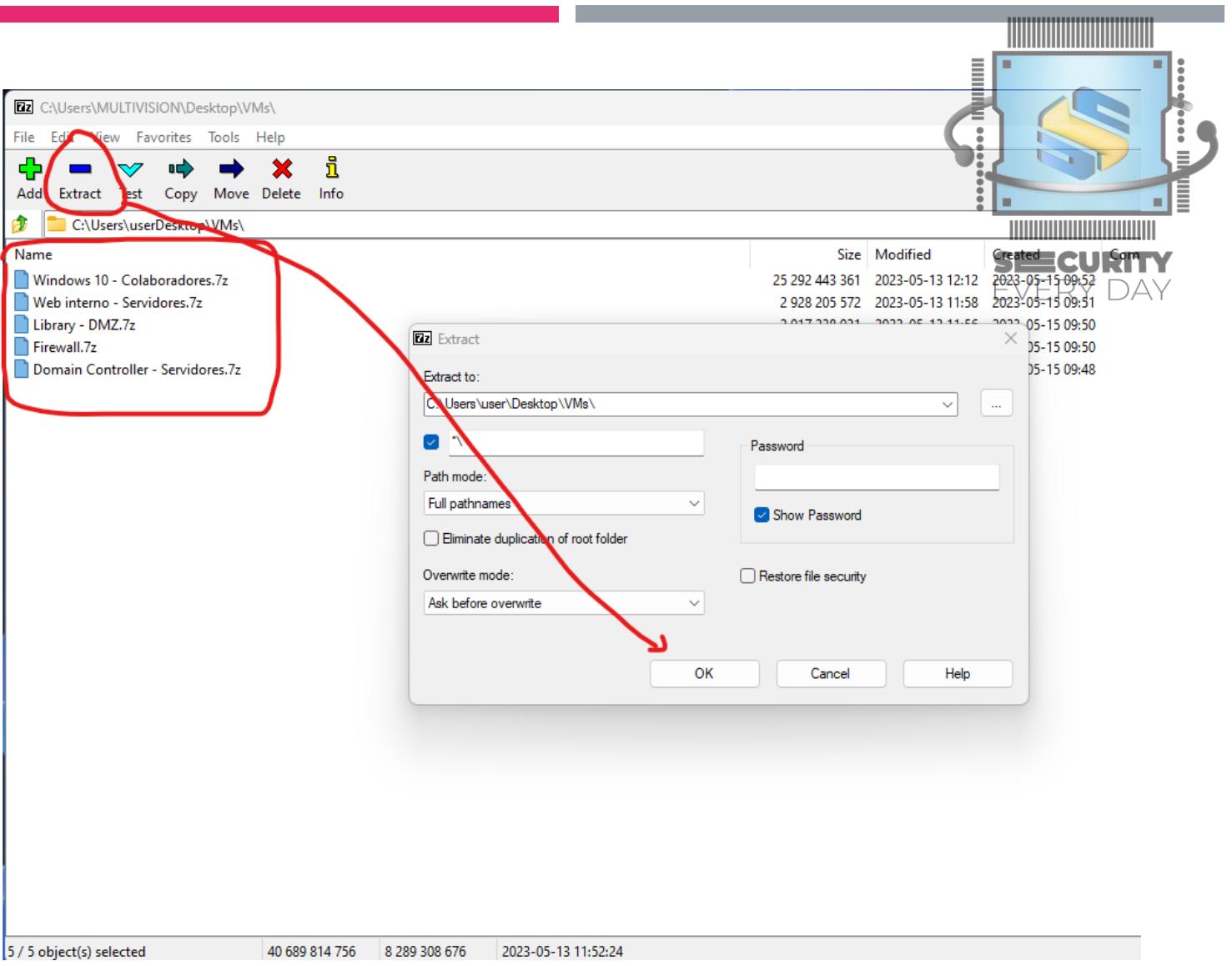
CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

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



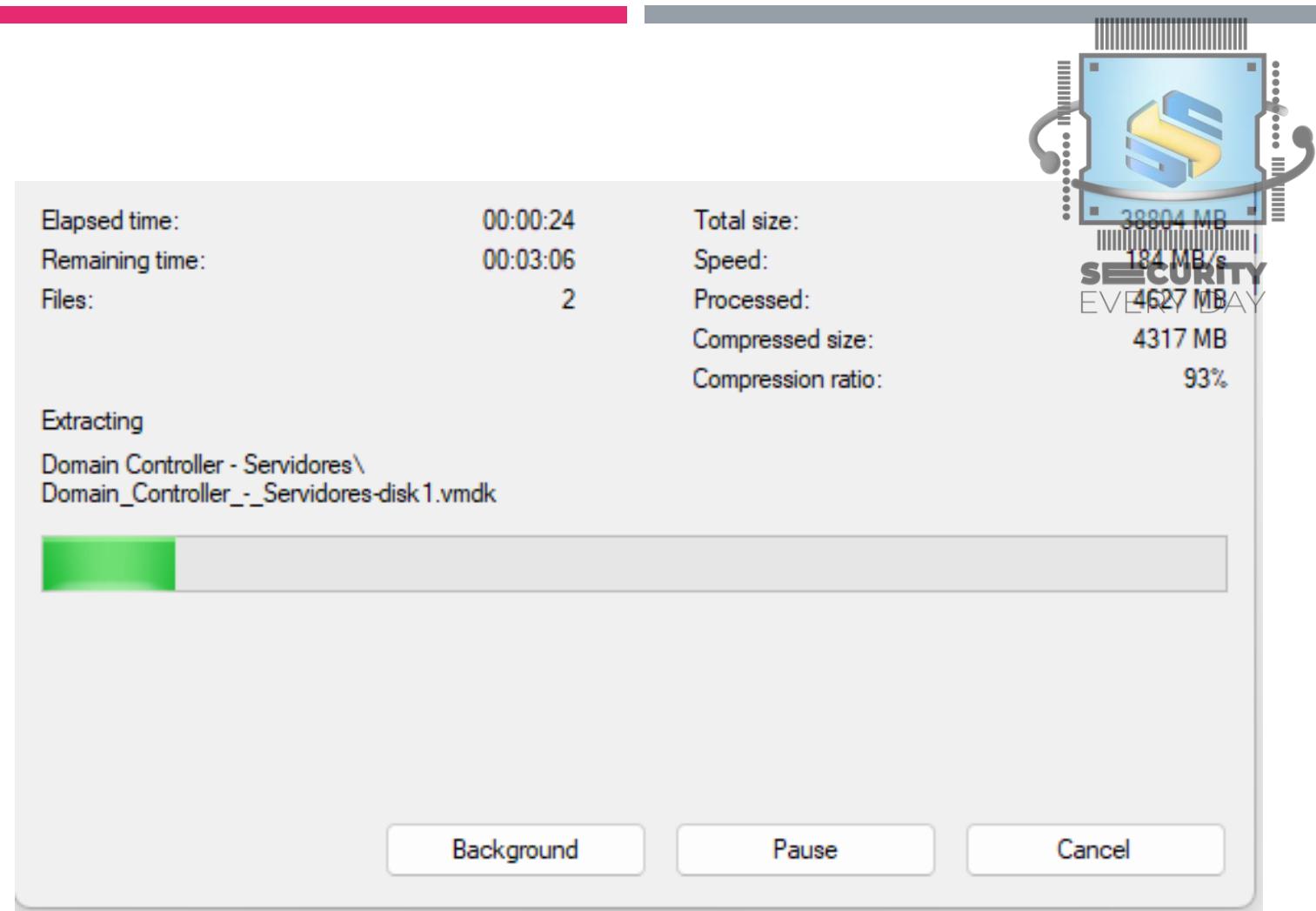
CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

- 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 extraídas



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.

Name
Windows 10 - Colaboradores
Web interno - Servidores
Library - DMZ
Firewall
Domain Controller - Servidores
Windows 10 - Colaboradores.7z
Web interno - Servidores.7z
Library - DMZ.7z
Firewall.7z
Domain Controller - Servidores.7z



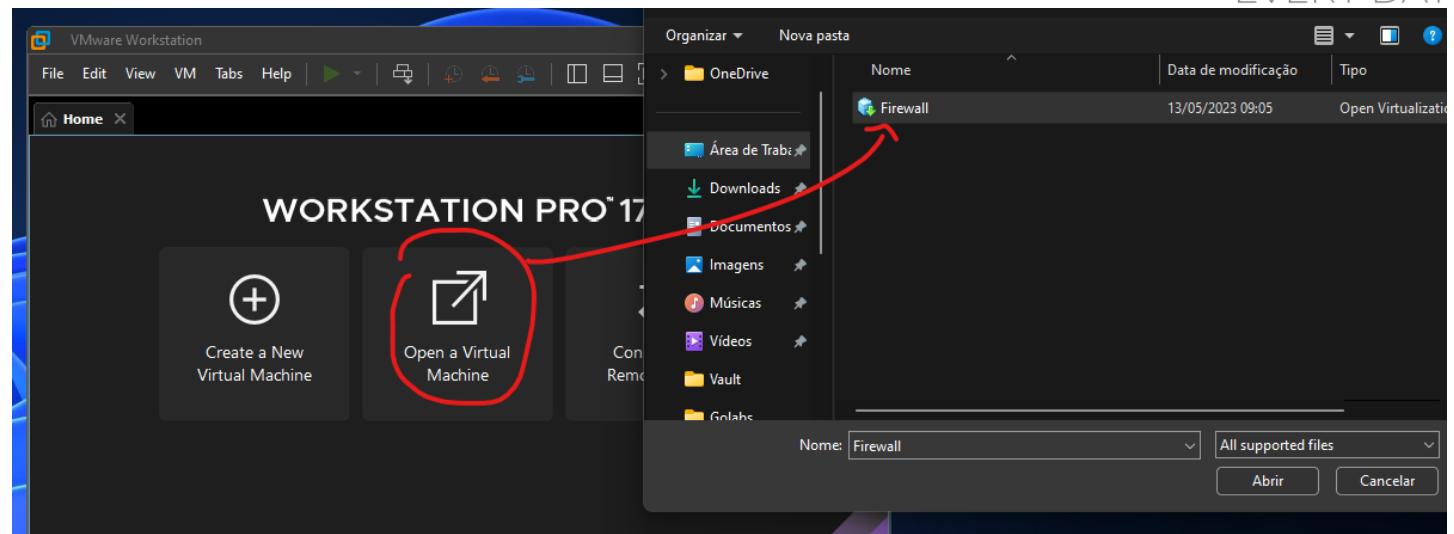
CONFIGURAÇÃO DAS MAQUINAS VIRTUAIS

TEMOS NOSSAS
MAQUINAS
AGORA, SÓ
FALTA SUBIR :)



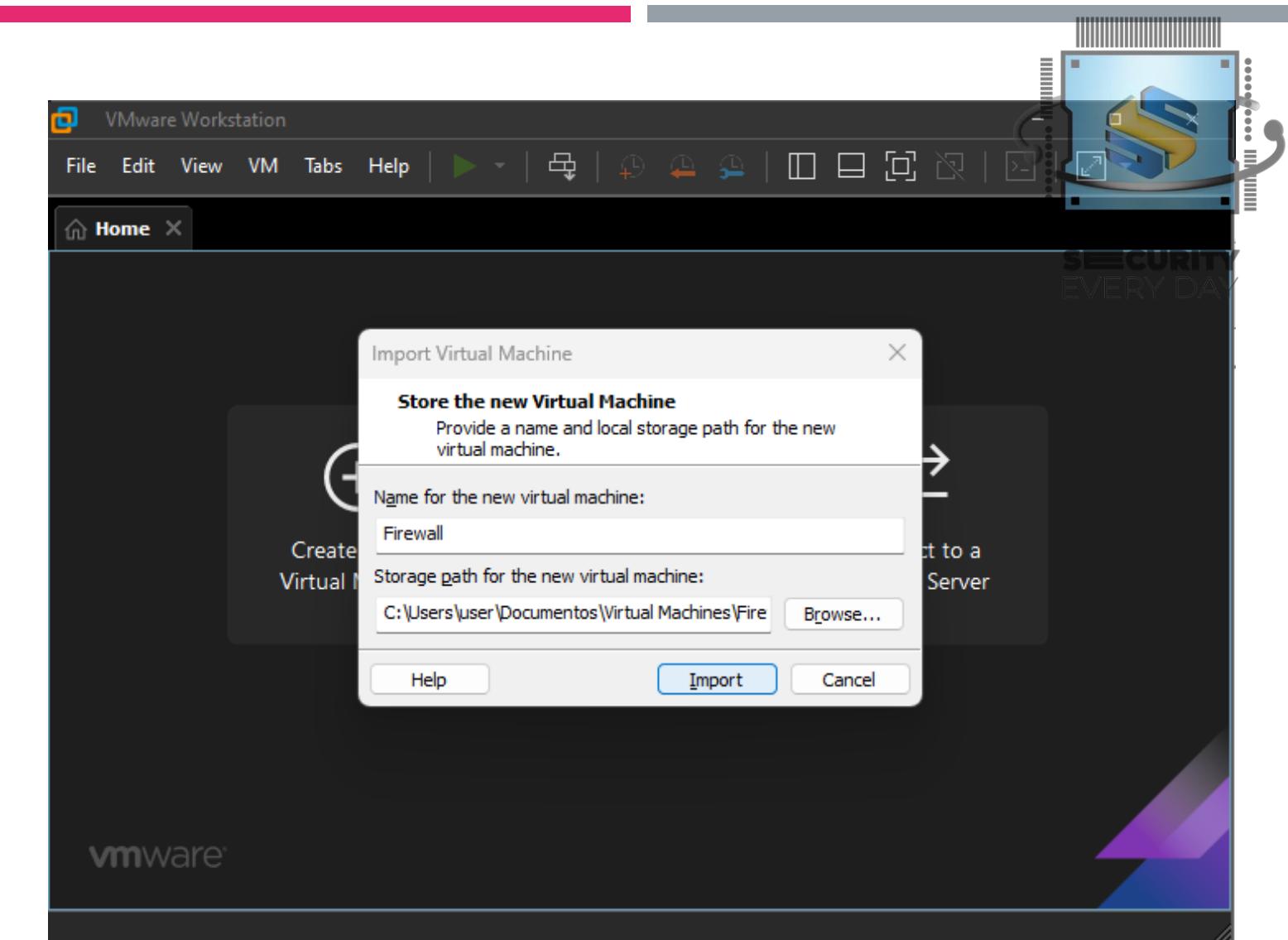
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- 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"



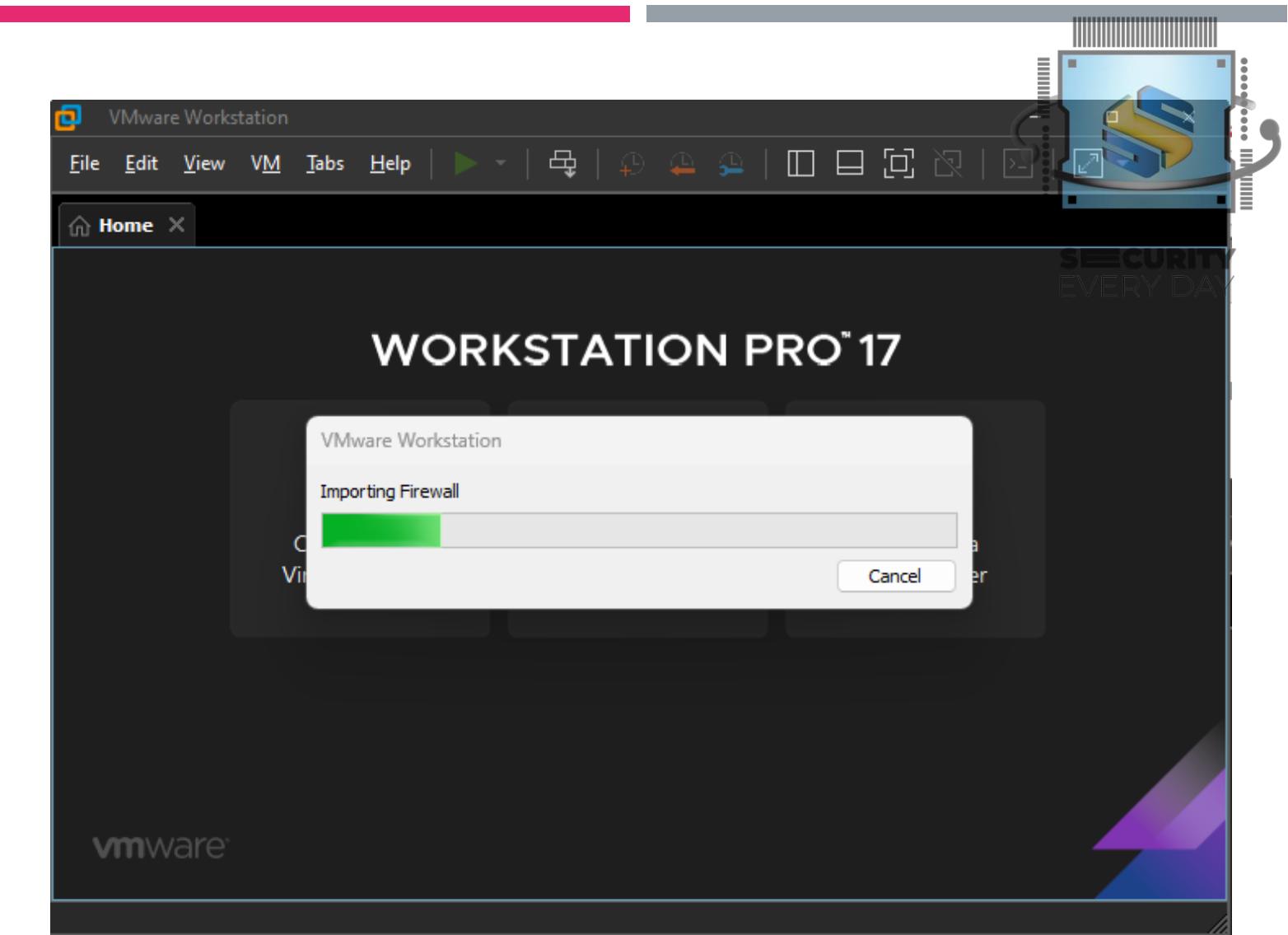
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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



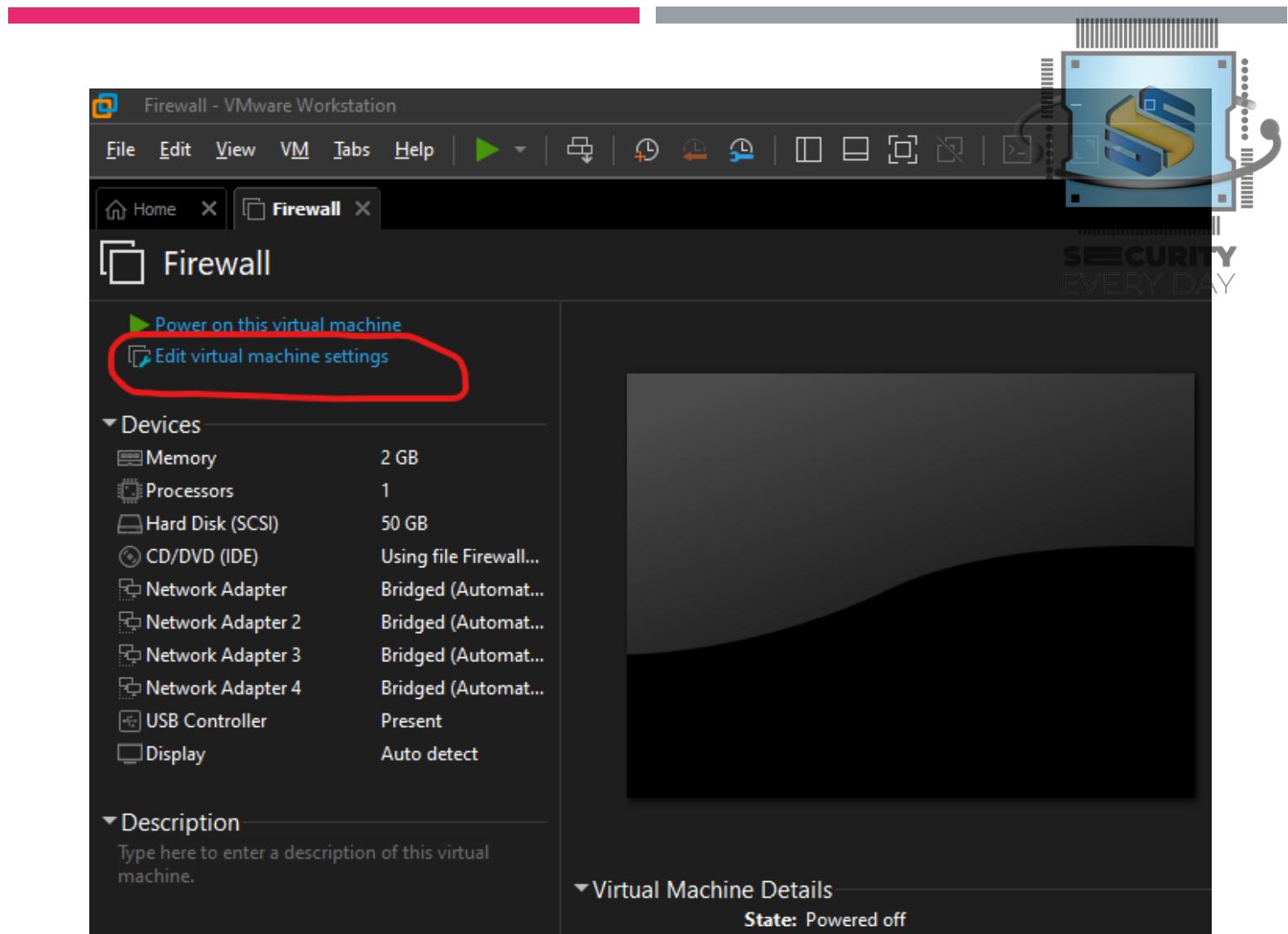
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Aguarde até que a VM seja importada



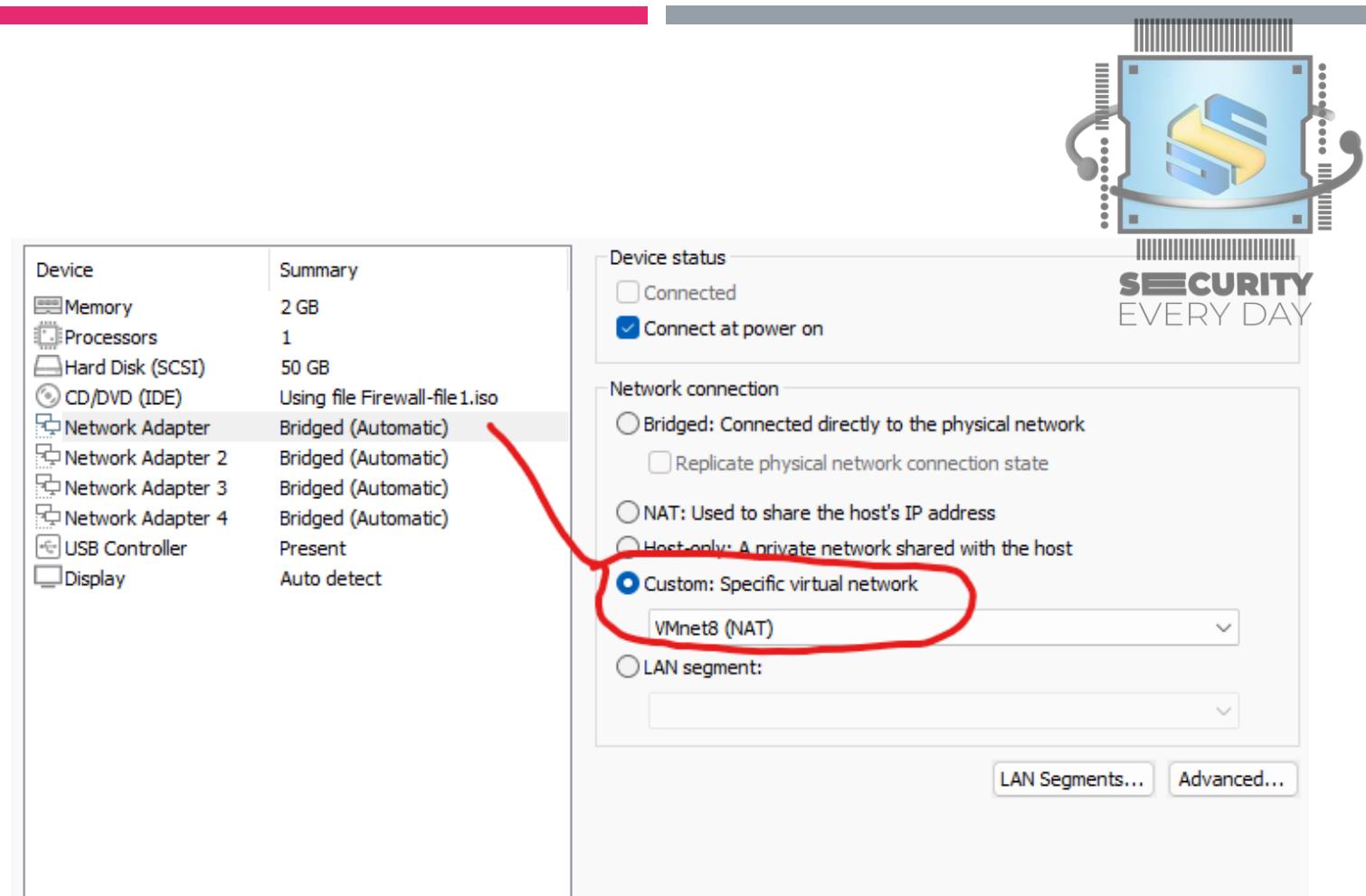
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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



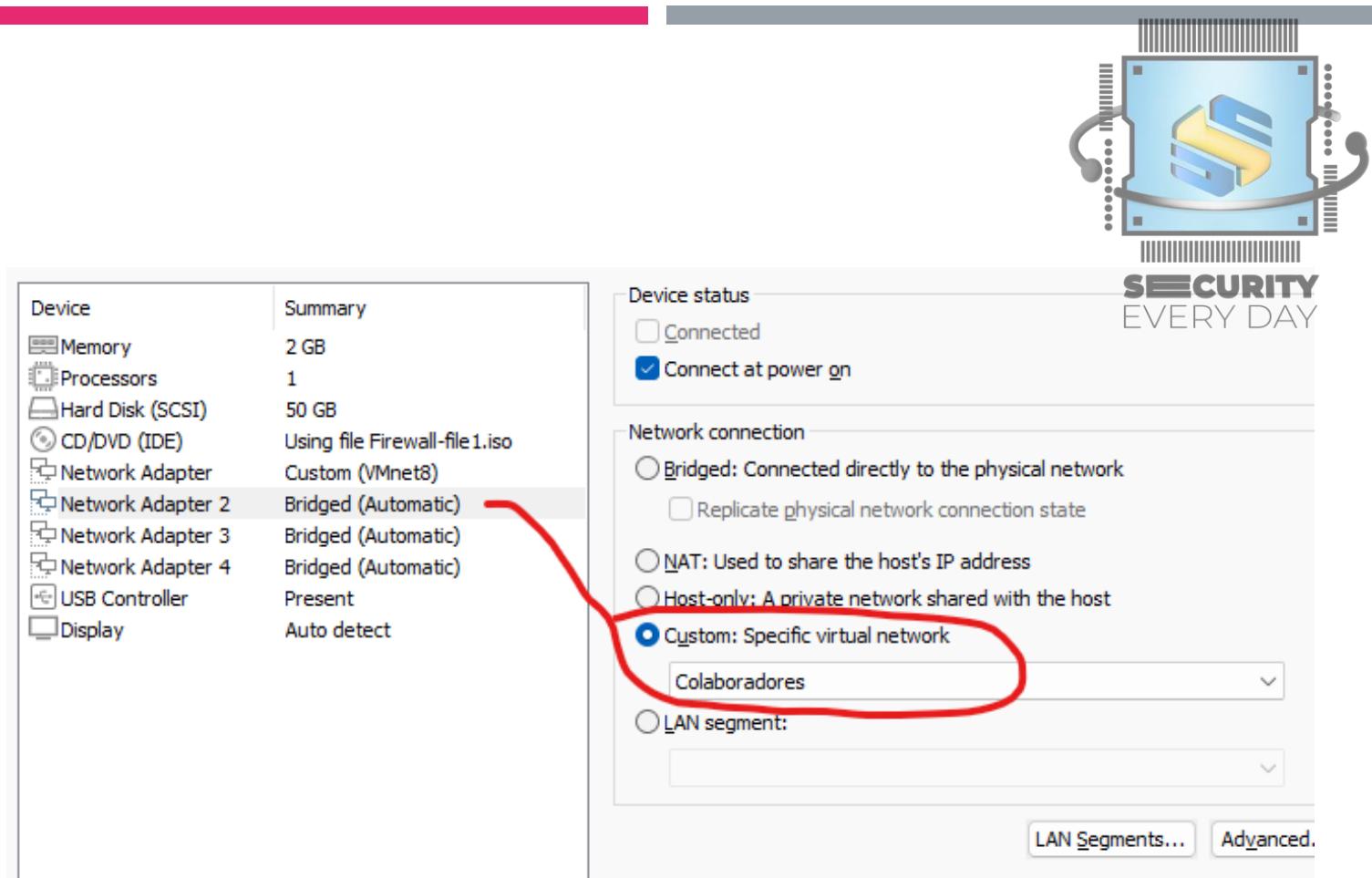
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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



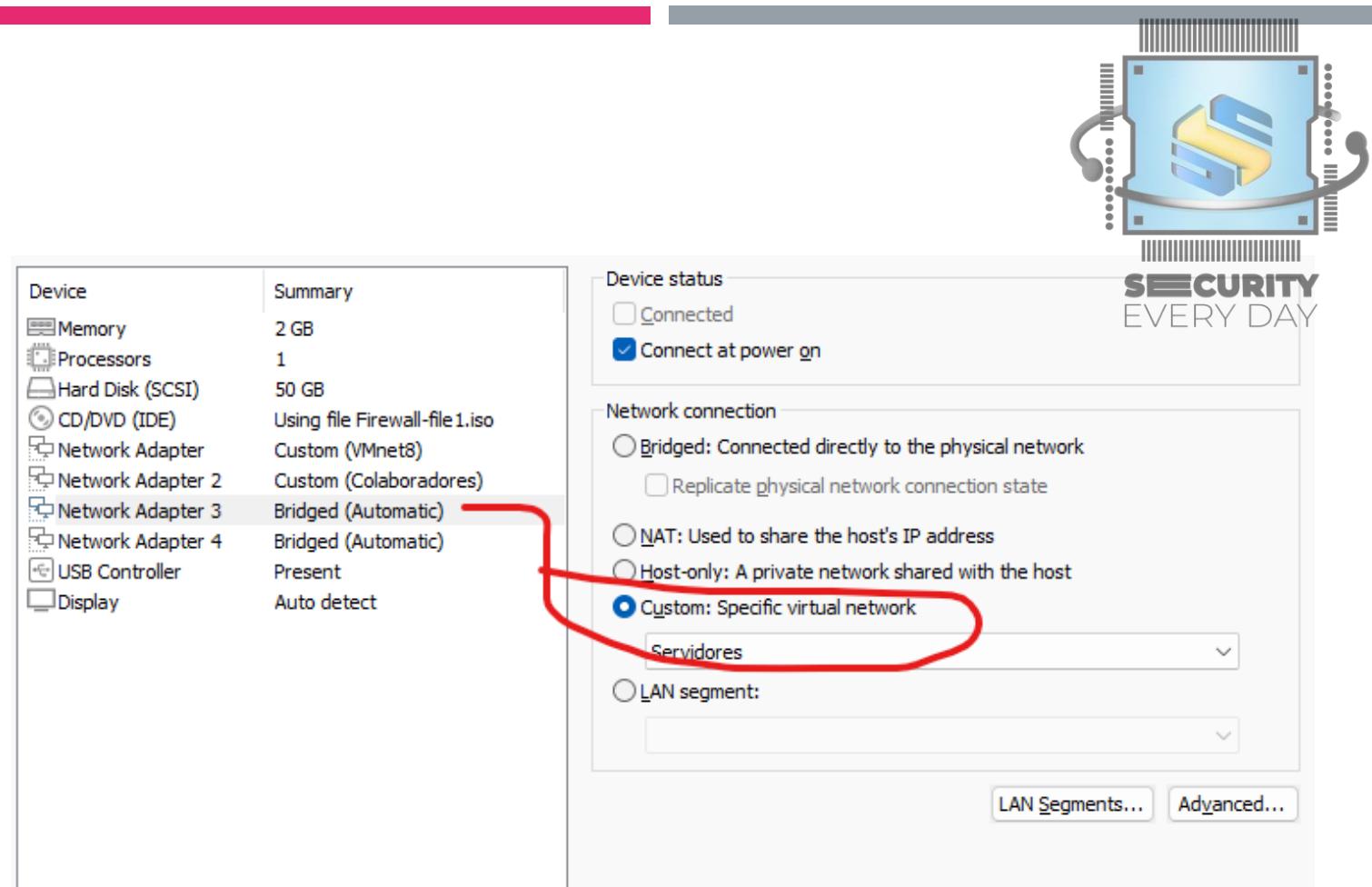
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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



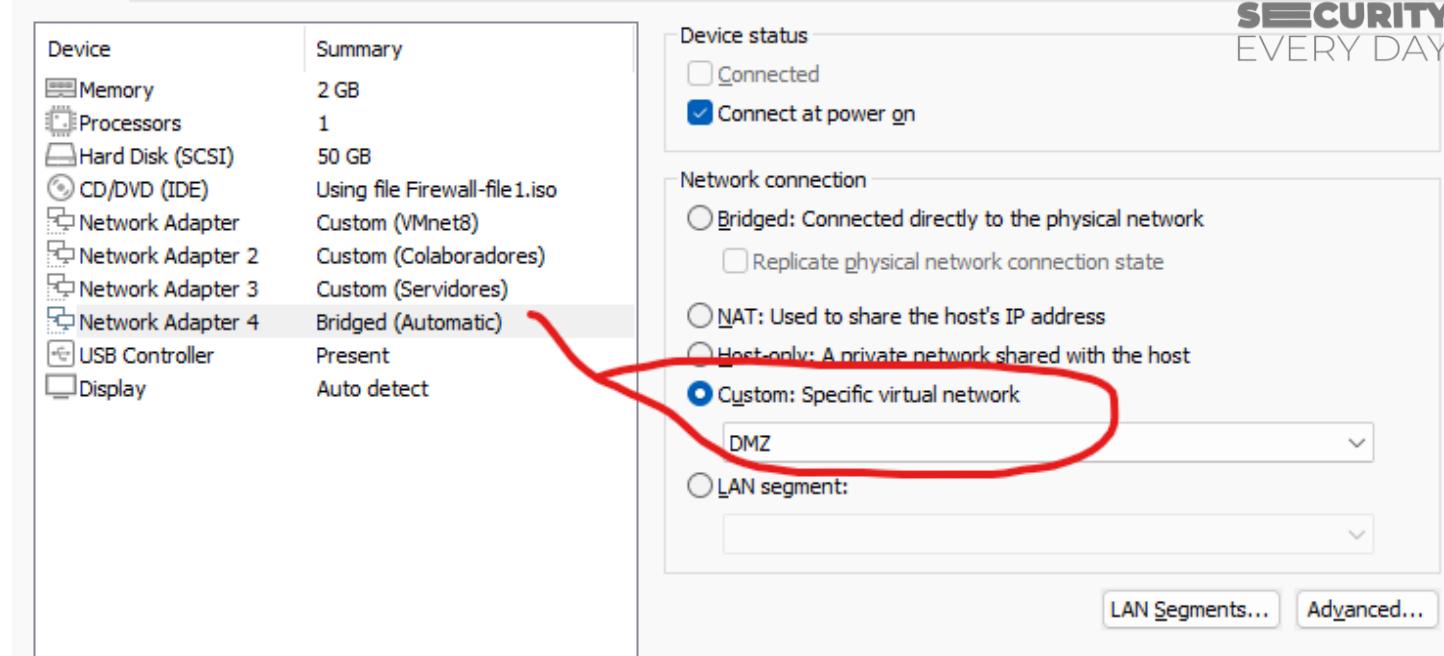
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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



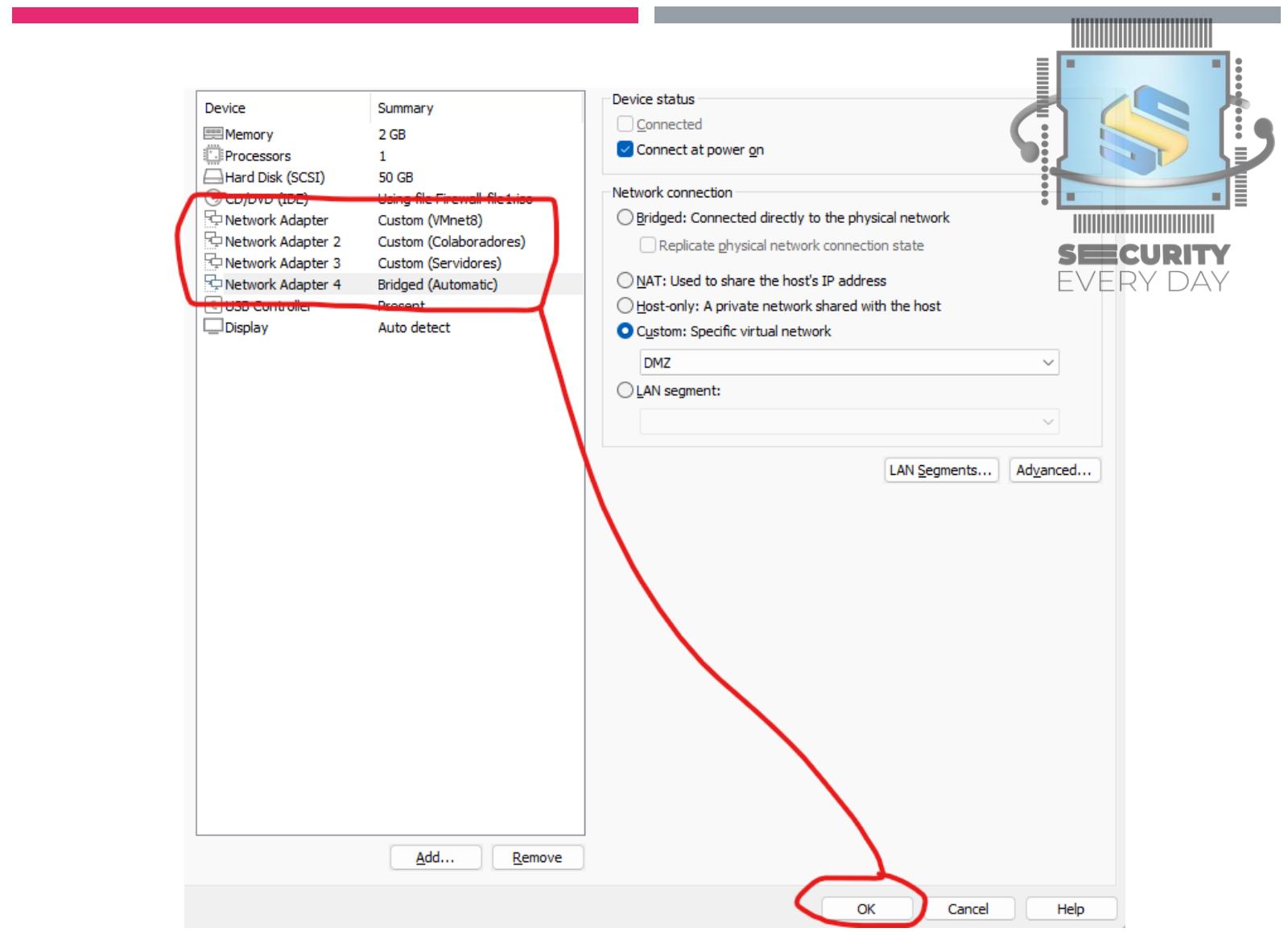
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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



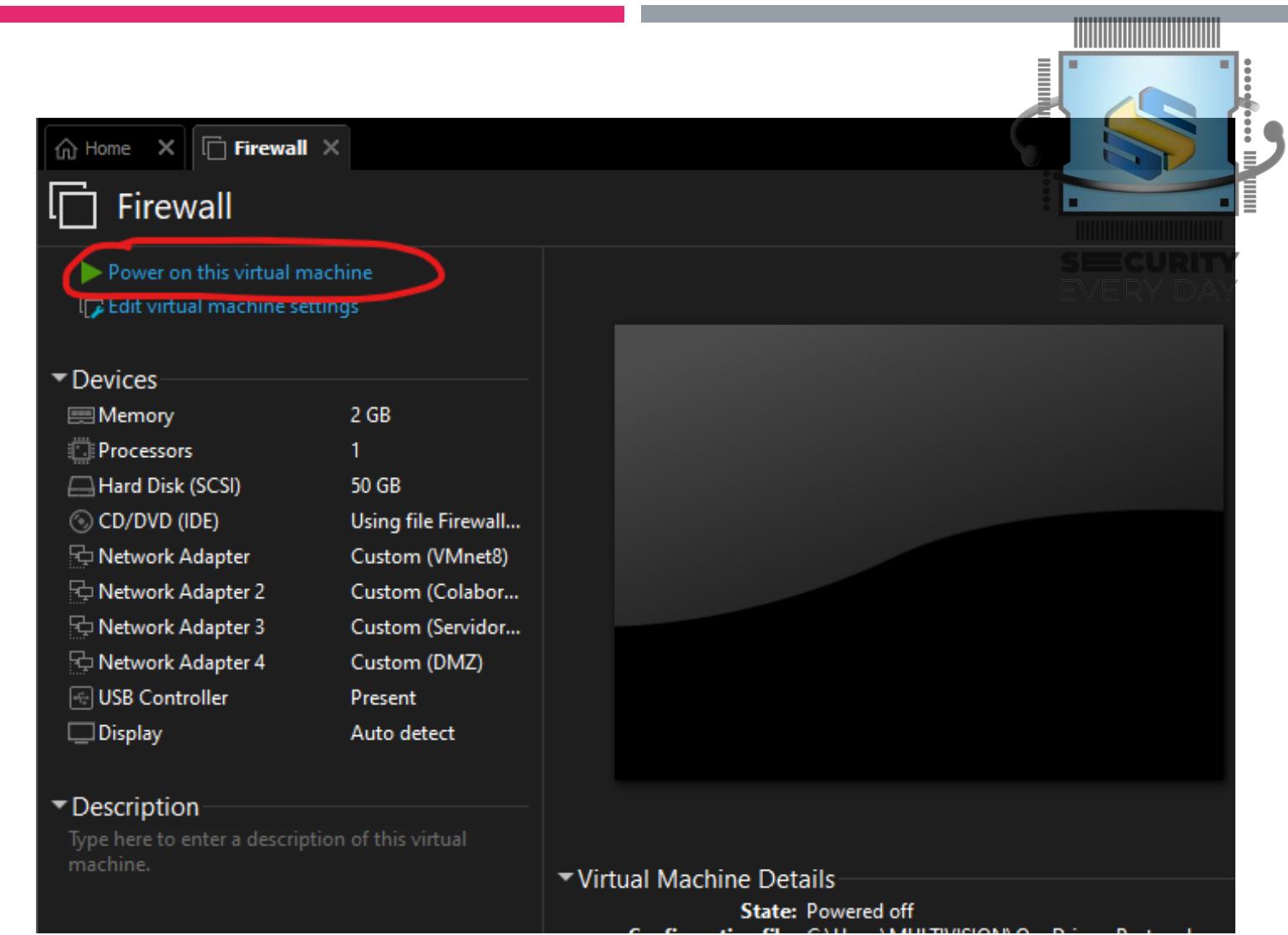
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

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

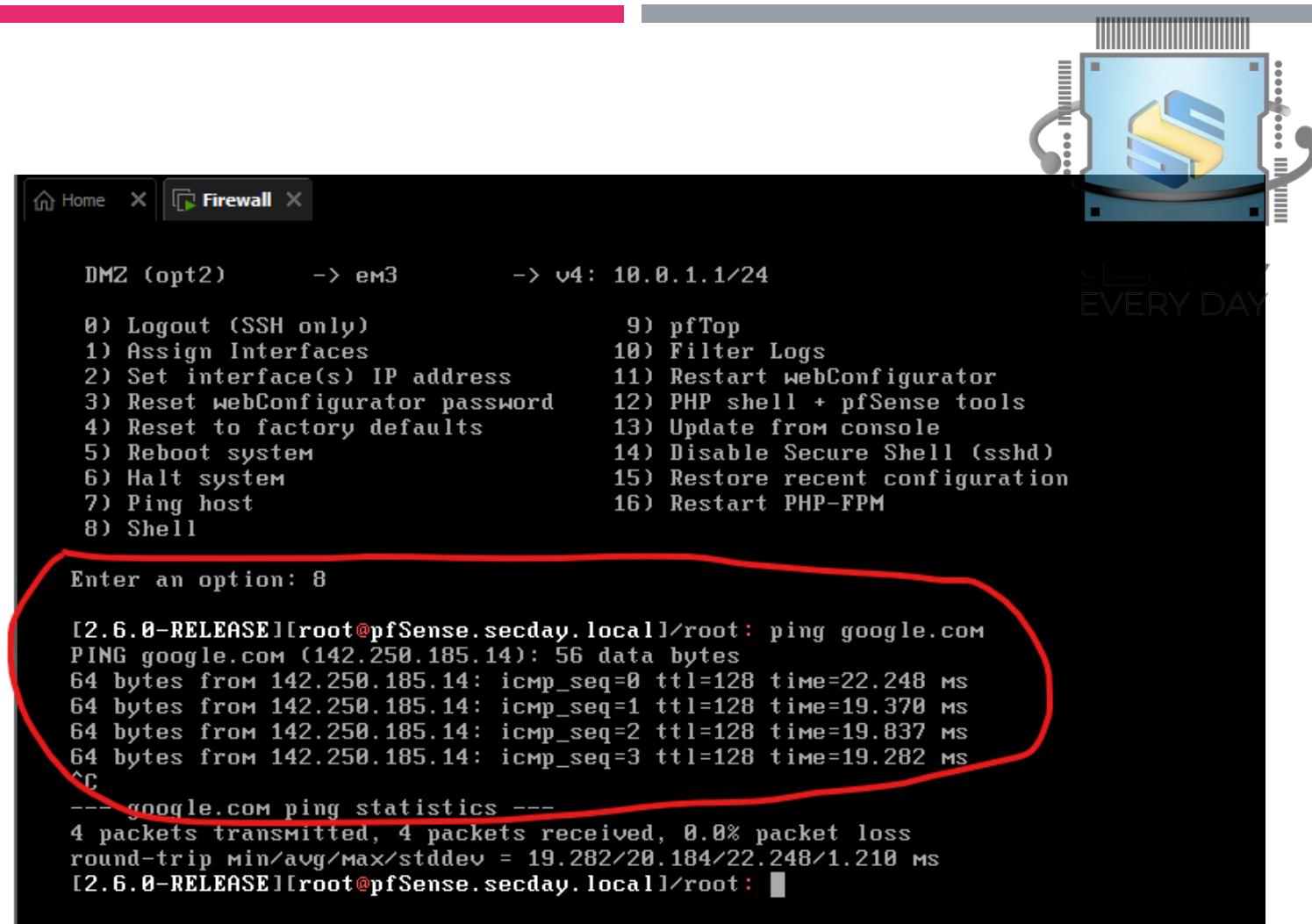


IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- 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.



The image shows a pfSense Firewall interface with a terminal window overlaid. The terminal window displays a menu of 16 options related to system management and monitoring, followed by a user input prompt and a ping command output.

```
Home X Firewall X

DMZ (opt2)      -> em3      -> v4: 10.0.1.1/24

0) Logout (SSH only)      9) pfTop
1) Assign Interfaces       10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system           14) Disable Secure Shell (sshd)
6) Halt system             15) Restore recent configuration
7) Ping host               16) Restart PHP-FPM
8) Shell

Enter an option: 8

[2.6.0-RELEASE][root@pfSense.secday.local]/root: ping google.com
PING google.com (142.250.185.14): 56 data bytes
64 bytes from 142.250.185.14: icmp_seq=0 ttl=128 time=22.248 ms
64 bytes from 142.250.185.14: icmp_seq=1 ttl=128 time=19.370 ms
64 bytes from 142.250.185.14: icmp_seq=2 ttl=128 time=19.837 ms
64 bytes from 142.250.185.14: icmp_seq=3 ttl=128 time=19.282 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 19.282/20.184/22.248/1.210 ms
[2.6.0-RELEASE][root@pfSense.secday.local]/root:
```

IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

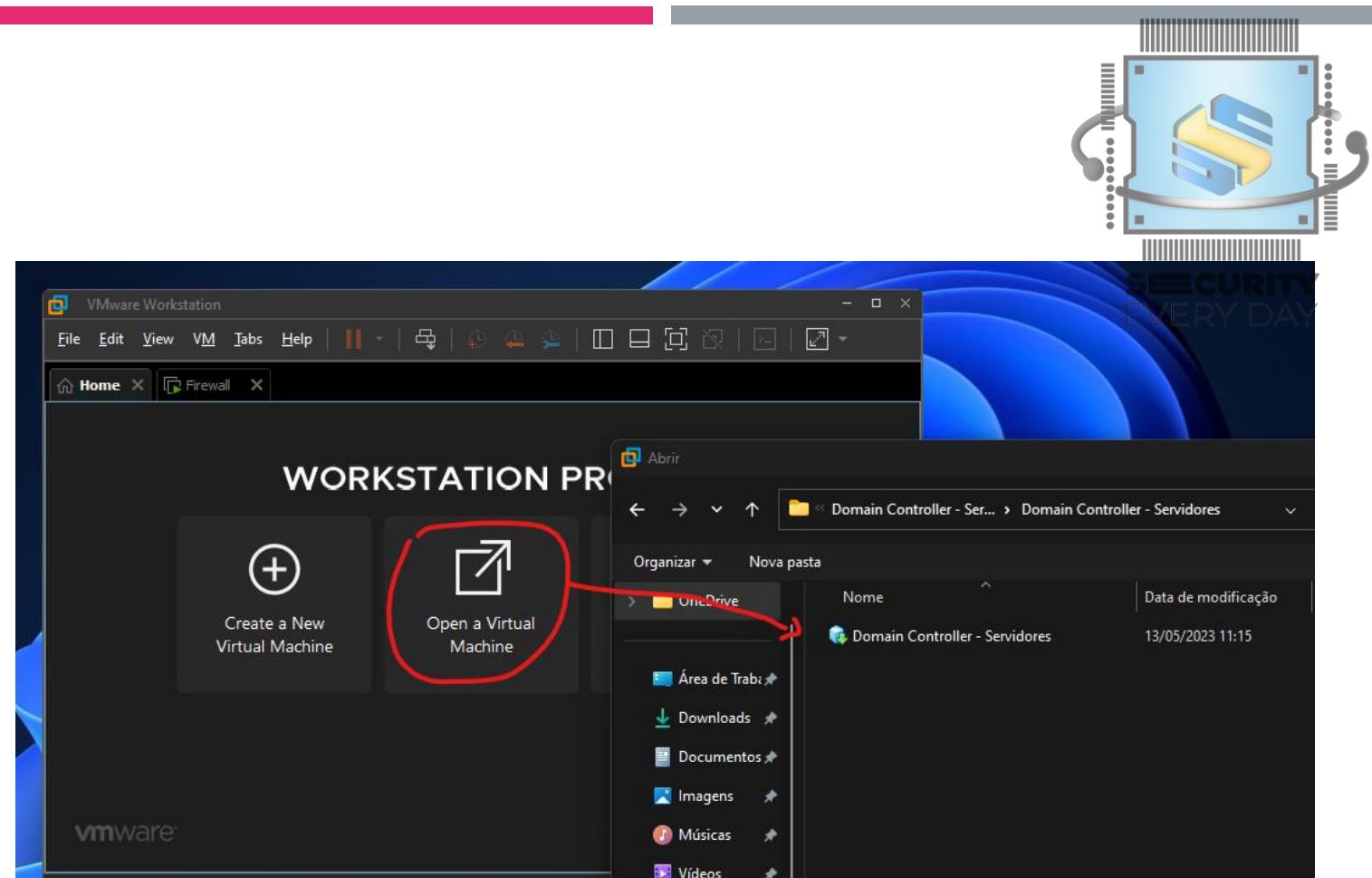
- Vamos fazer o mesmo para todas as maquinas
 - Atenção, altere o Network Adapter antes de iniciar a VM, a seguir vou adicionar os prints em sequencia da configuração de cada vm



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

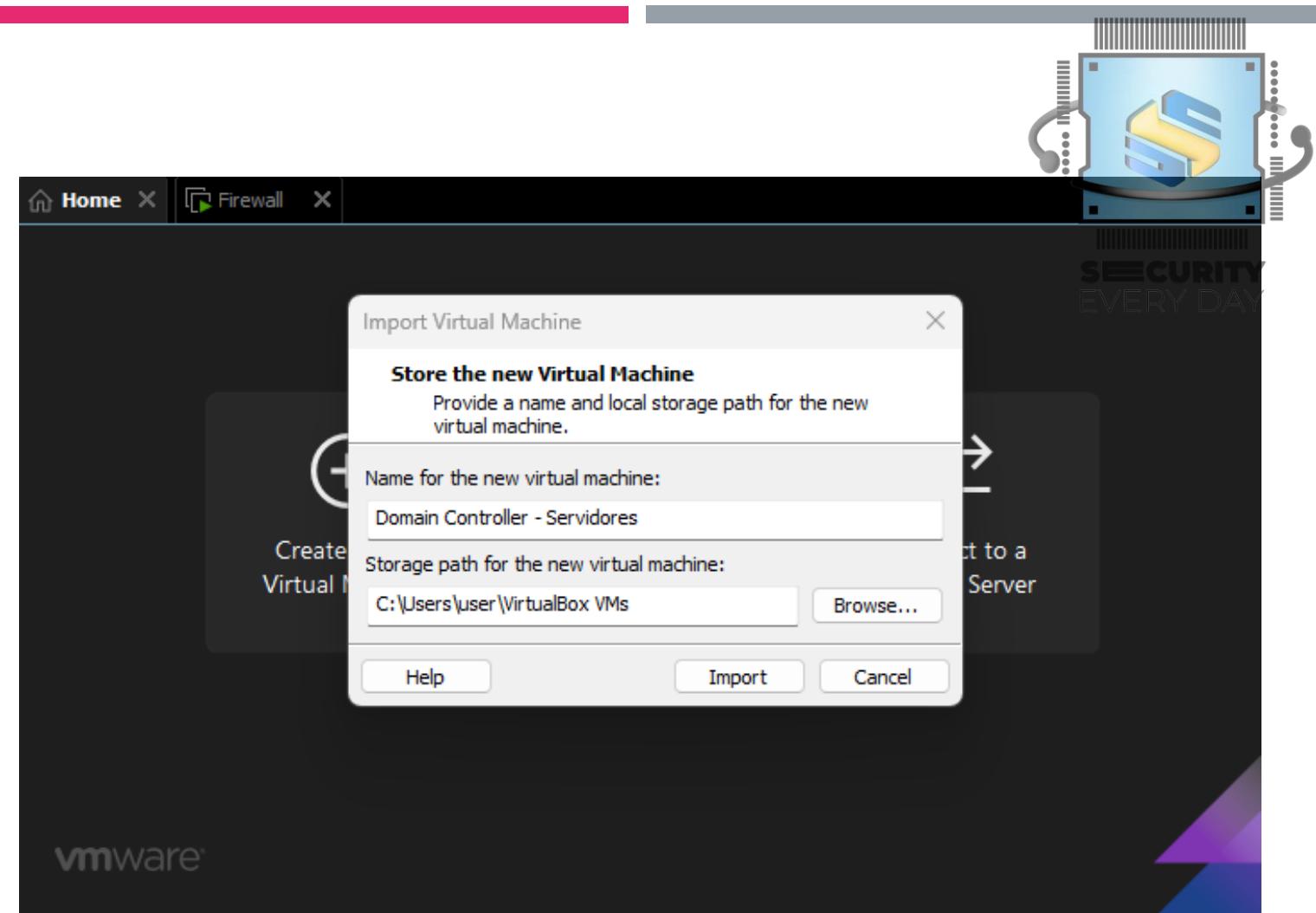
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



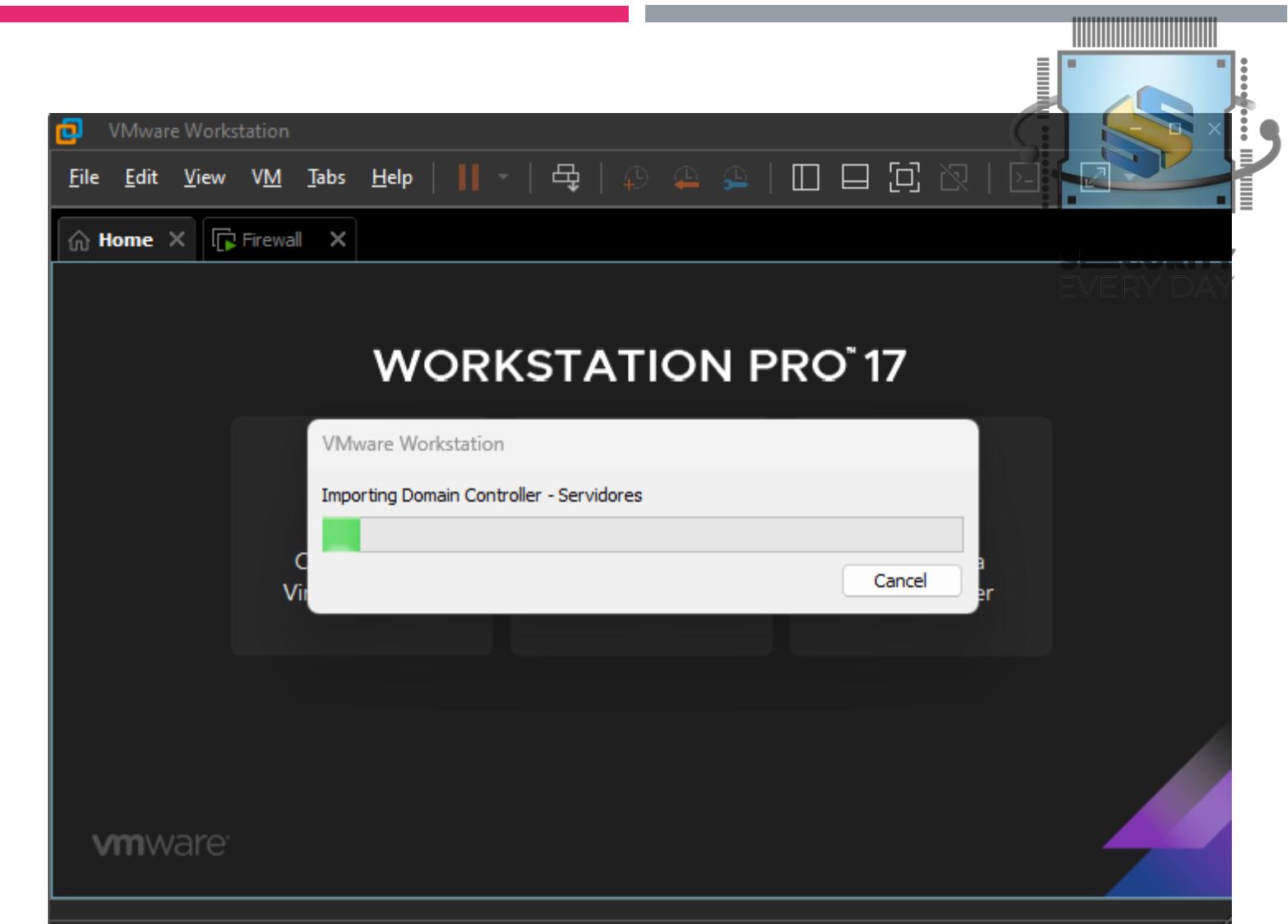
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



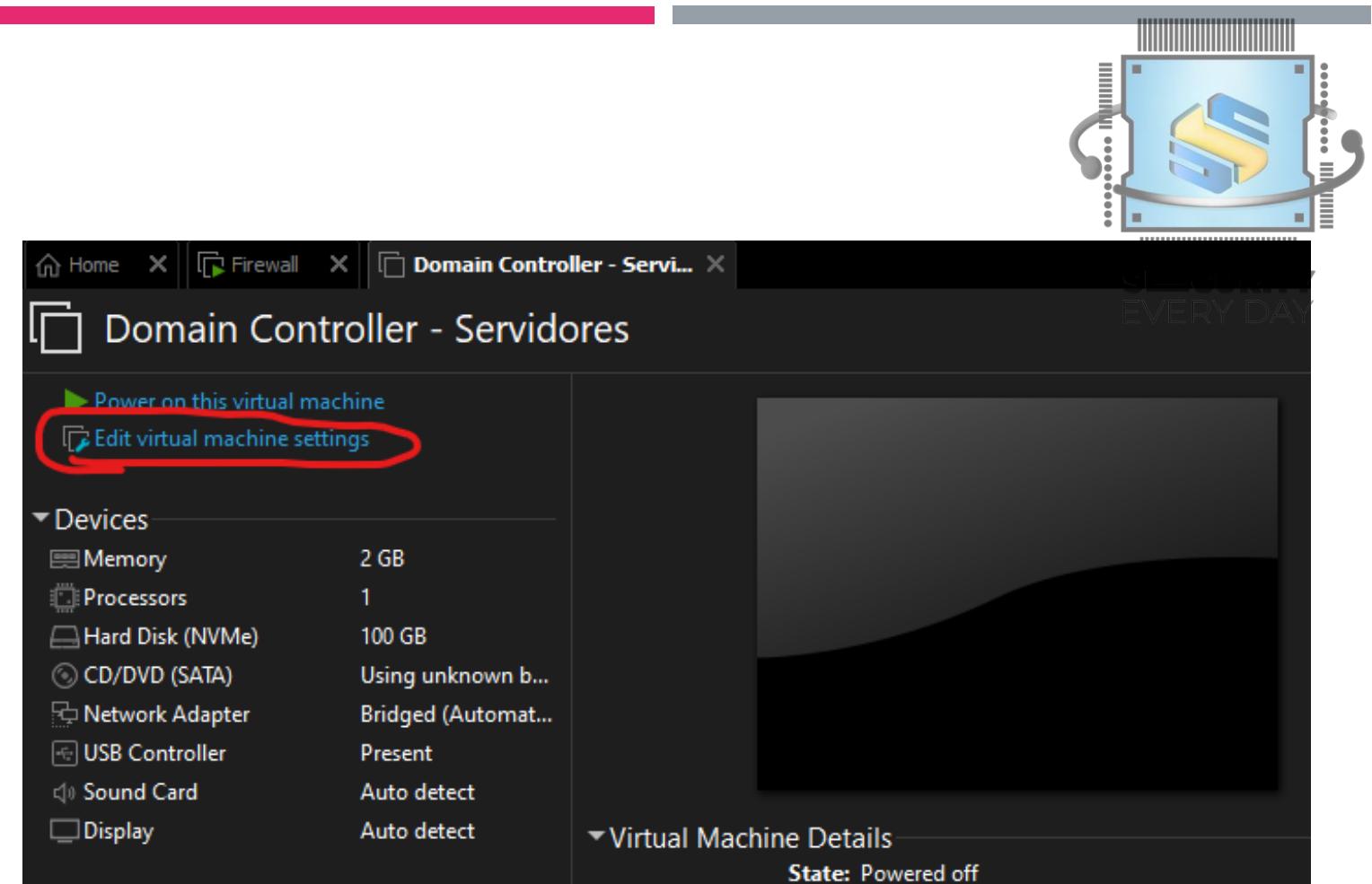
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



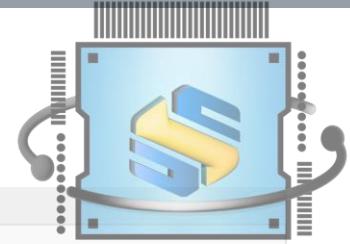
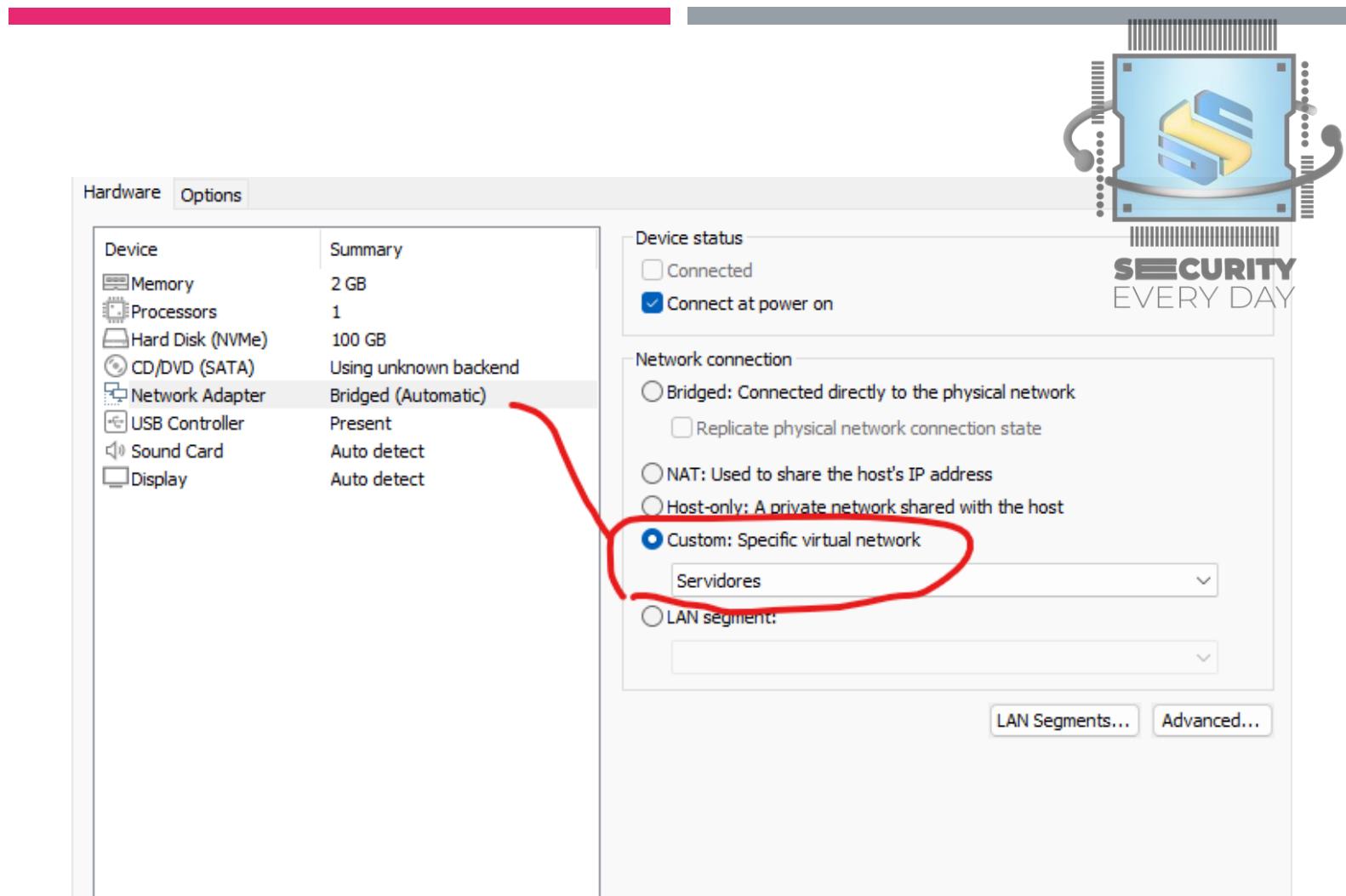
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



SECURITY
EVERY DAY

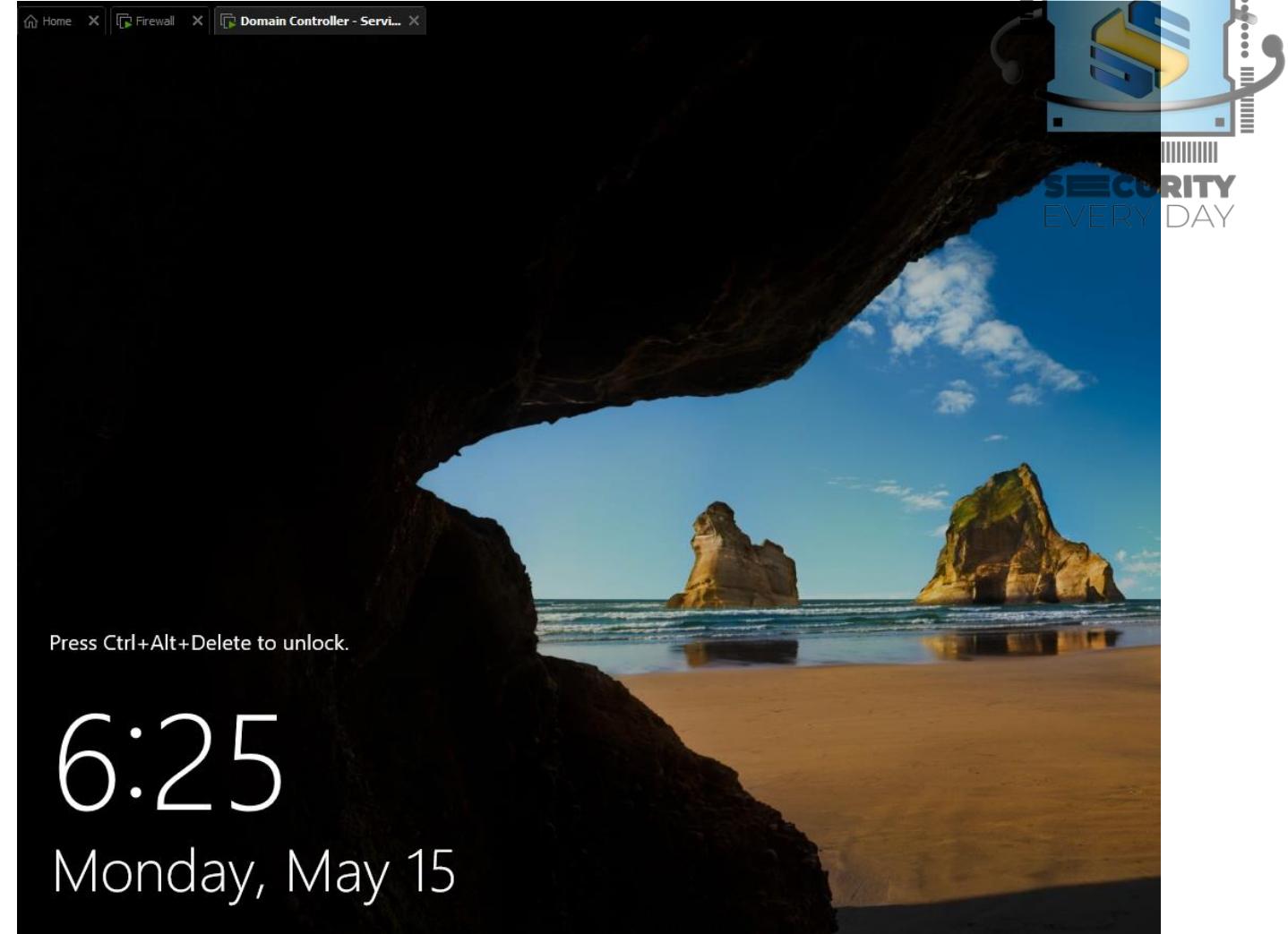
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



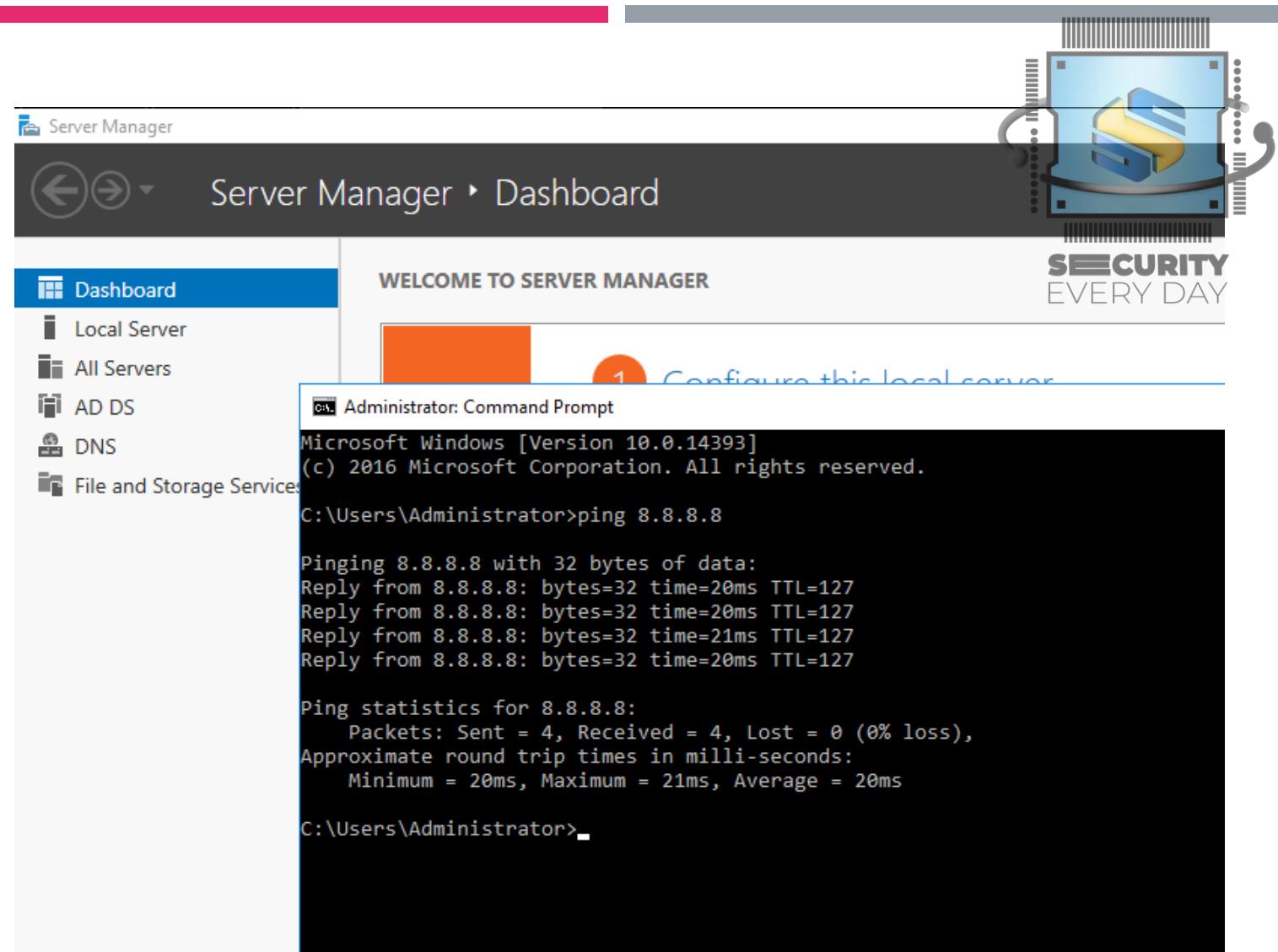
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Domain Controller - Servidores



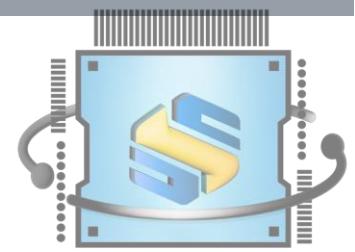
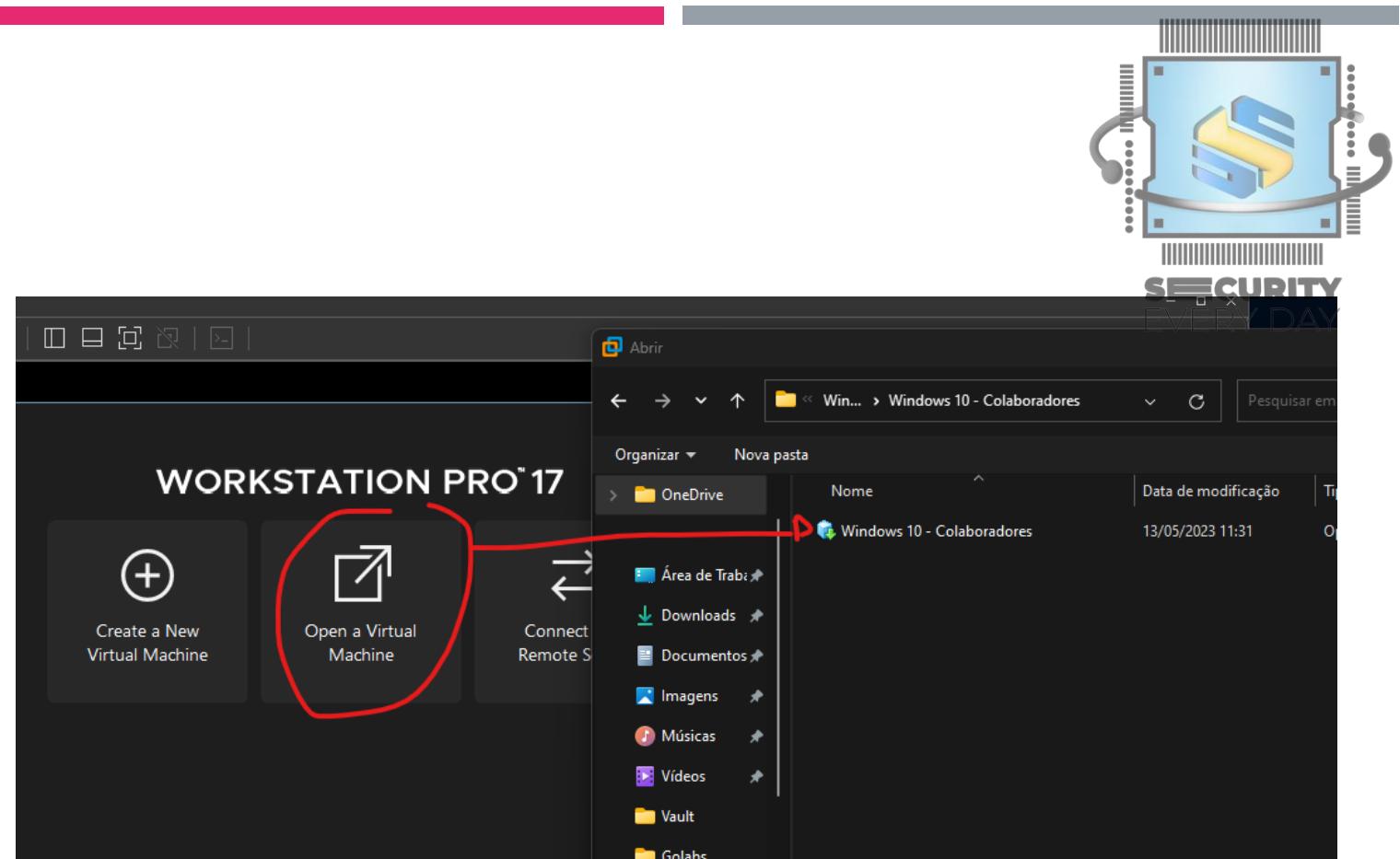
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- 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

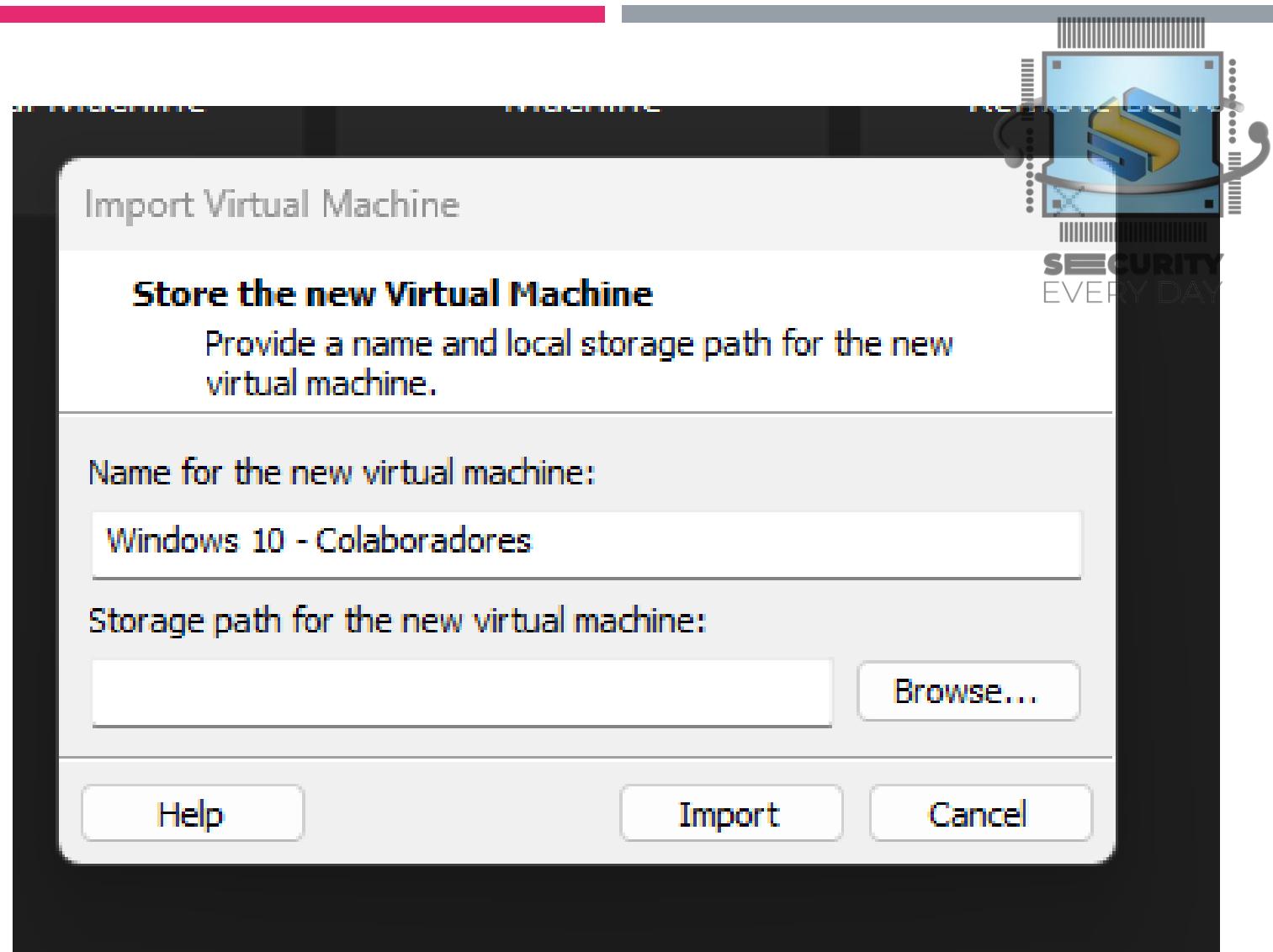
- Windows 10 - Colaboradores



SECURITY
EVERYDAY

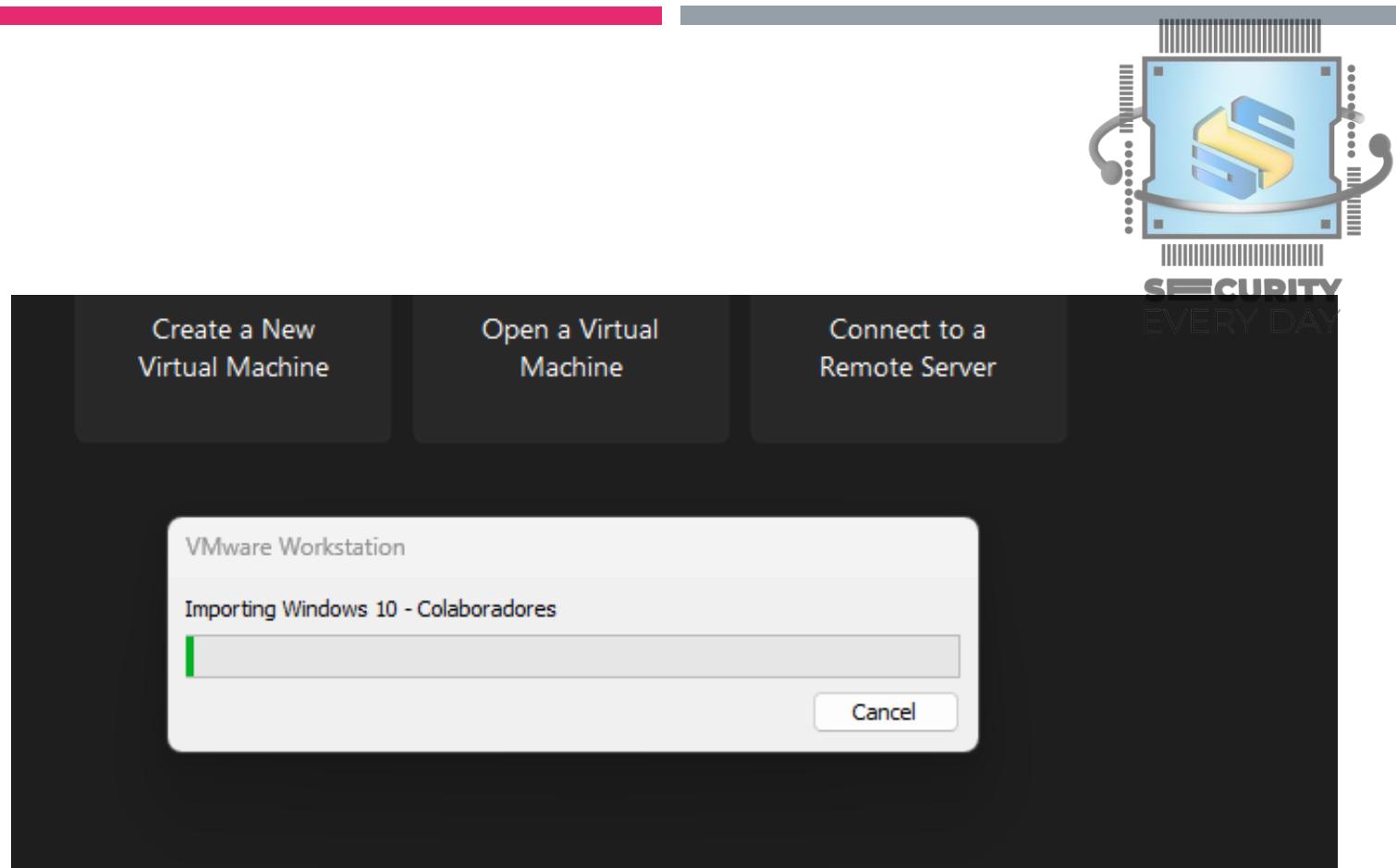
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



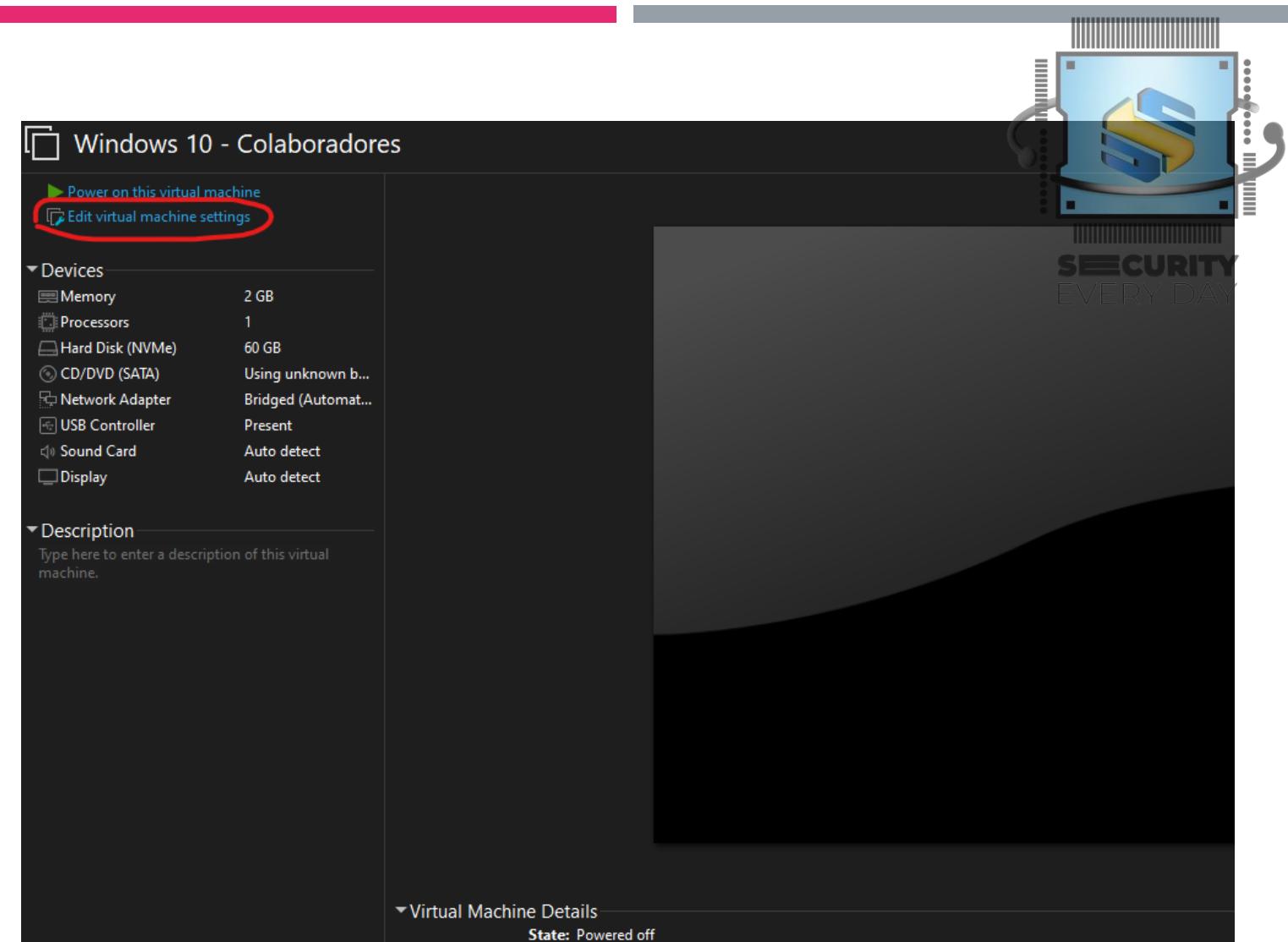
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



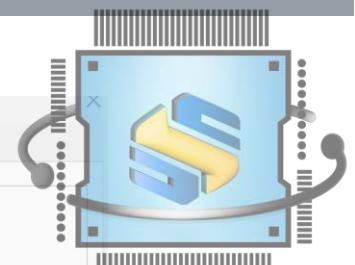
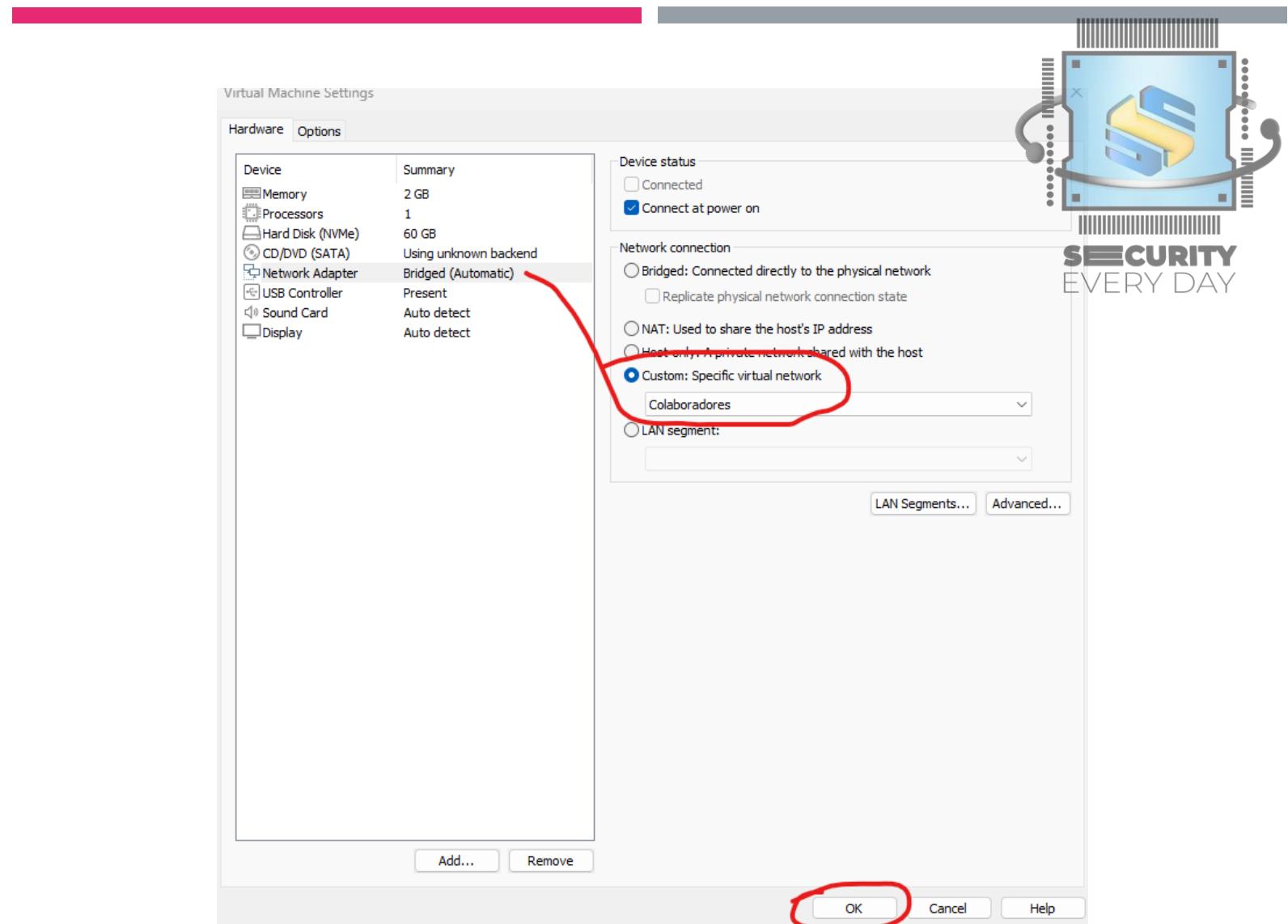
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

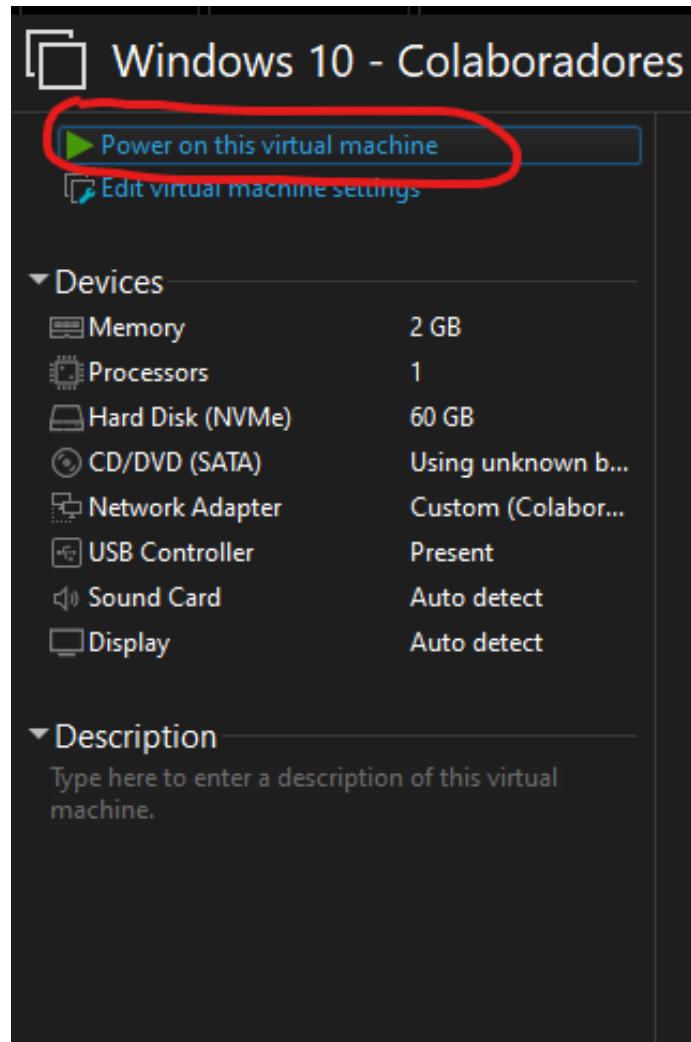
- Windows 10 - Colaboradores



SECURITY
EVERY DAY

IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



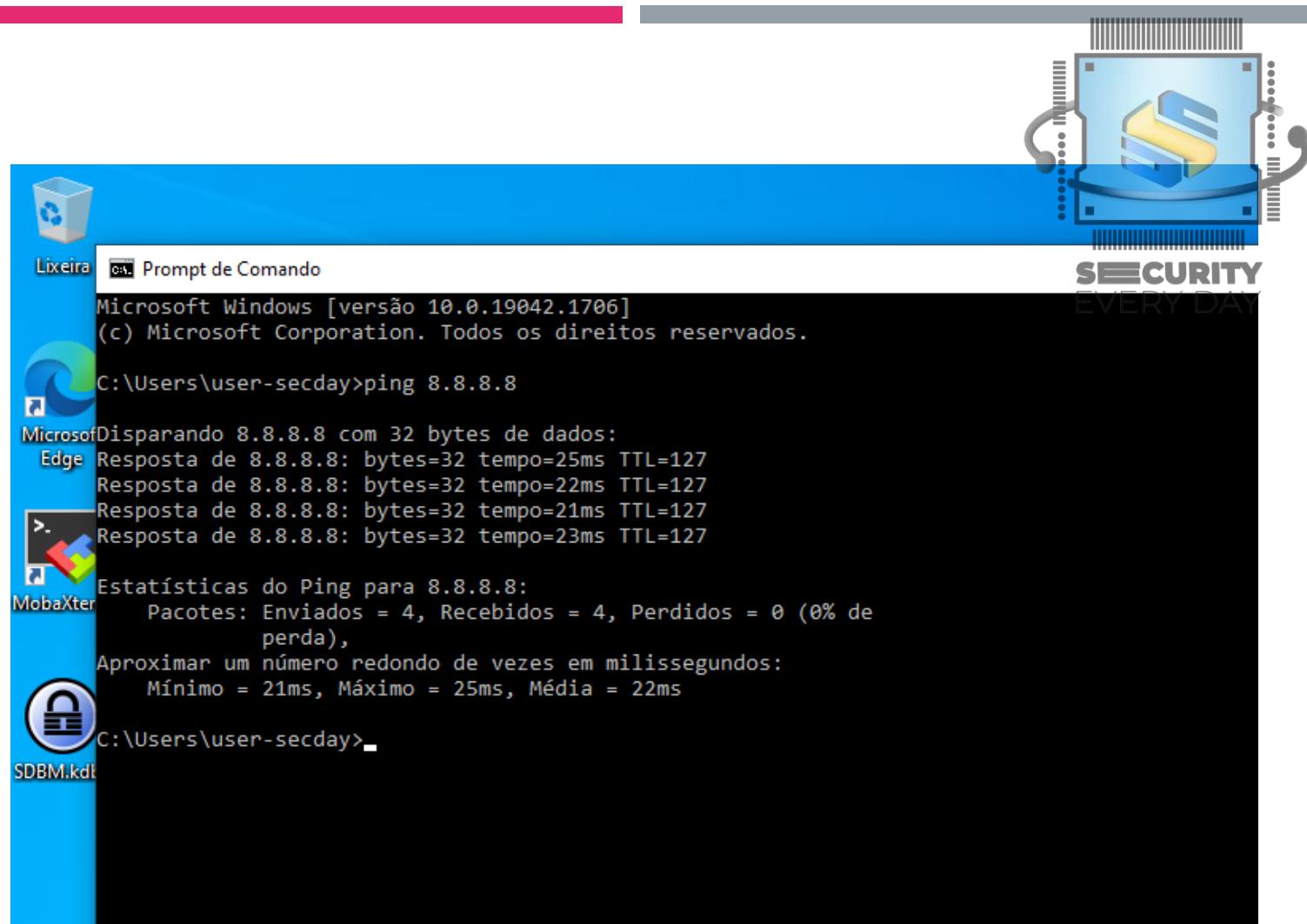
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Windows 10 - Colaboradores



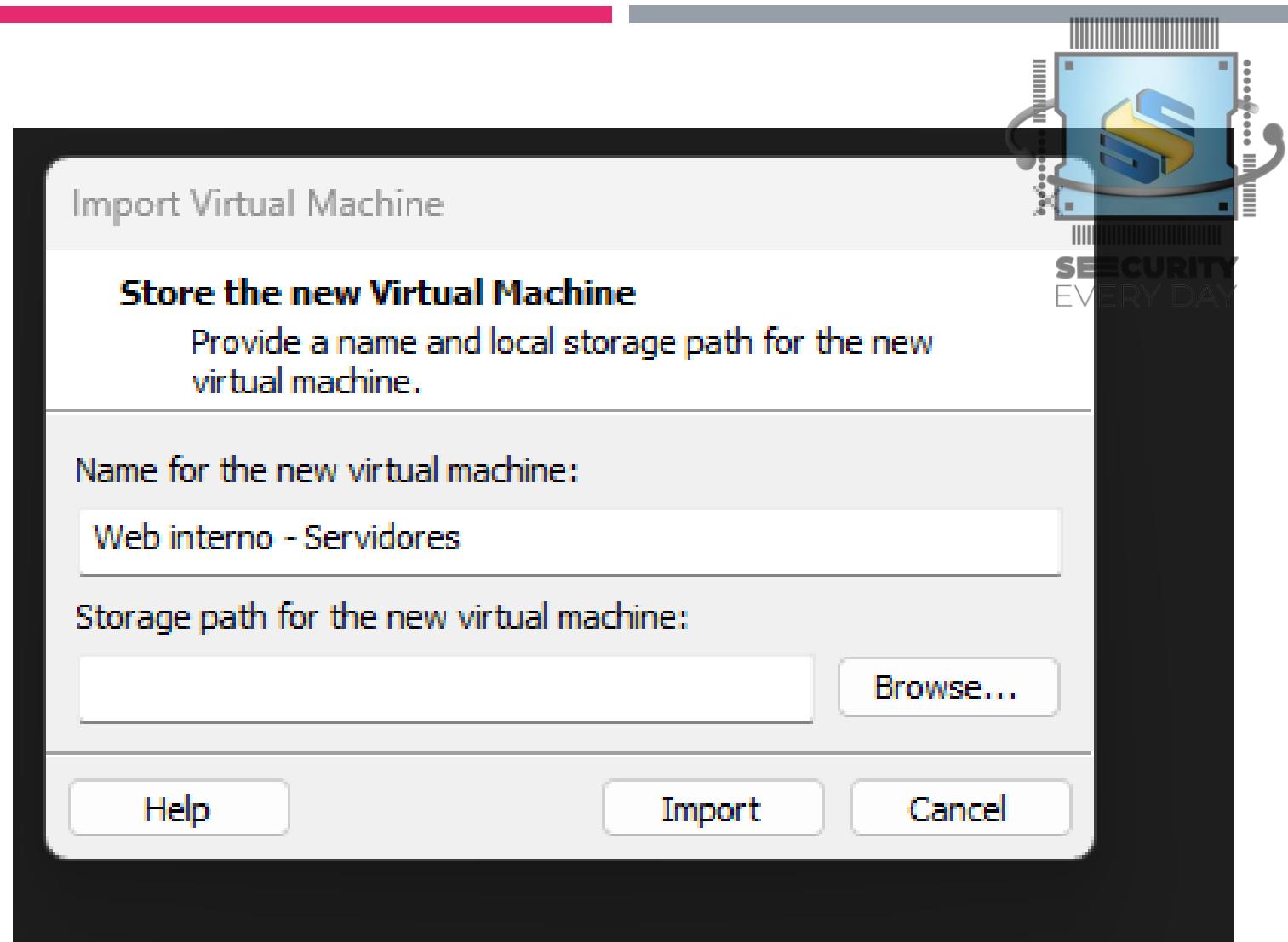
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- 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



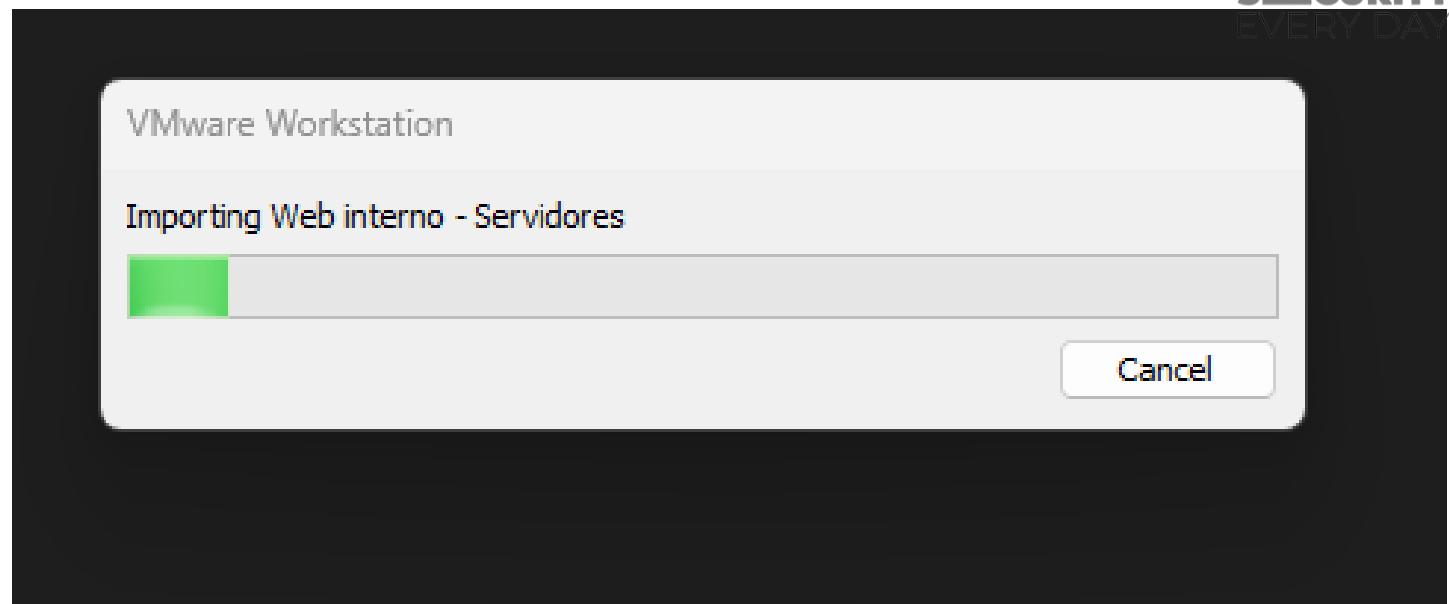
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores

Web interno - Servidores

[Power on this virtual machine](#)

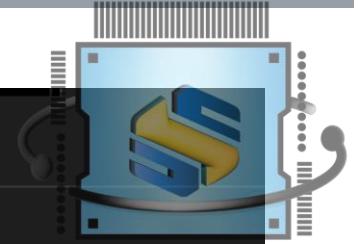
[Edit virtual machine settings](#)

Devices

	Memory	1 GB
	Processors	1
	Hard Disk (SCSI)	50 GB
	CD/DVD (SATA)	Using unknown b...
	Network Adapter	Bridged (Automat...
	USB Controller	Present
	Display	Auto detect

Description

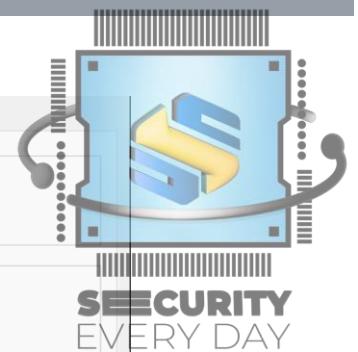
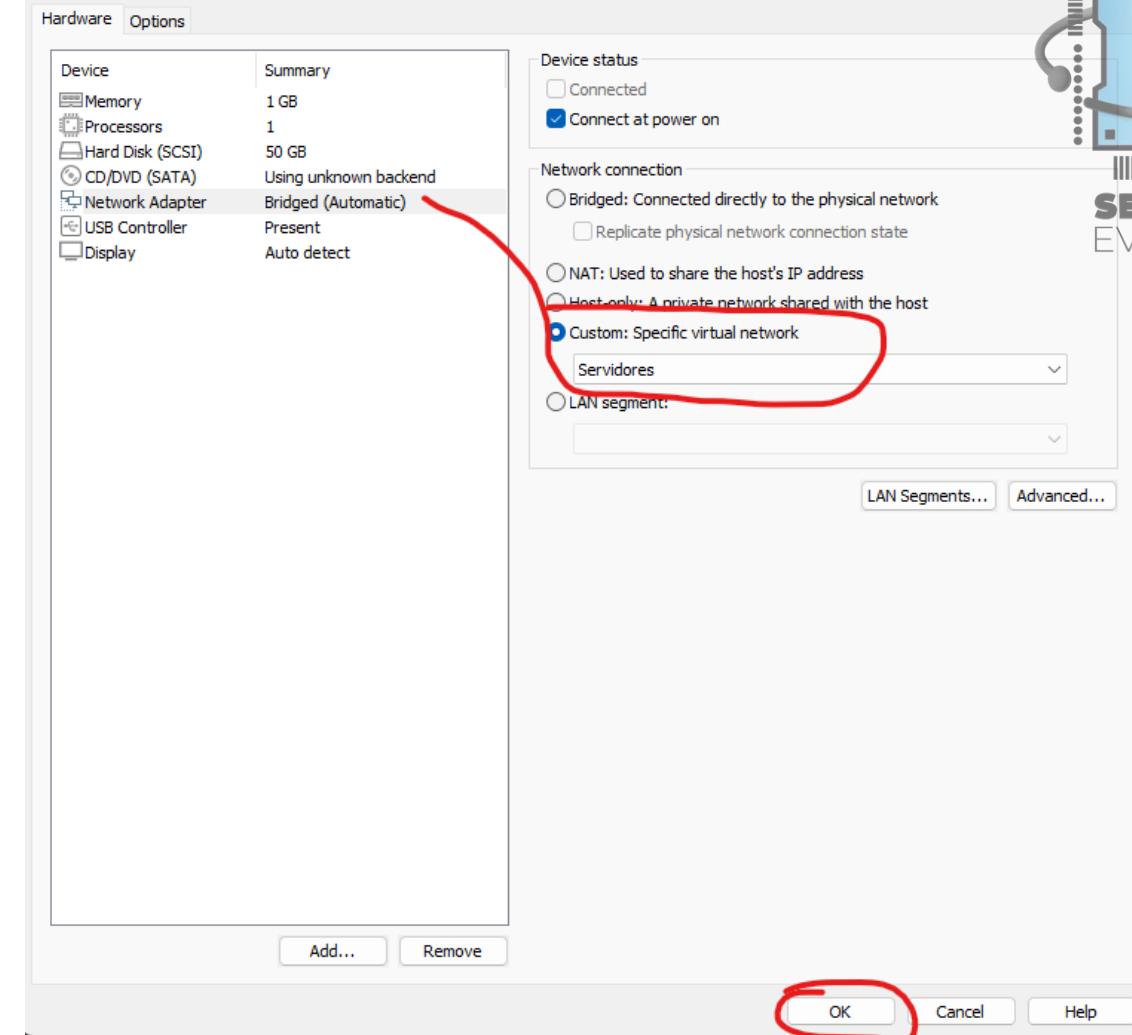
Type here to enter a description of this virtual machine.



SECURITY
EVERY DAY

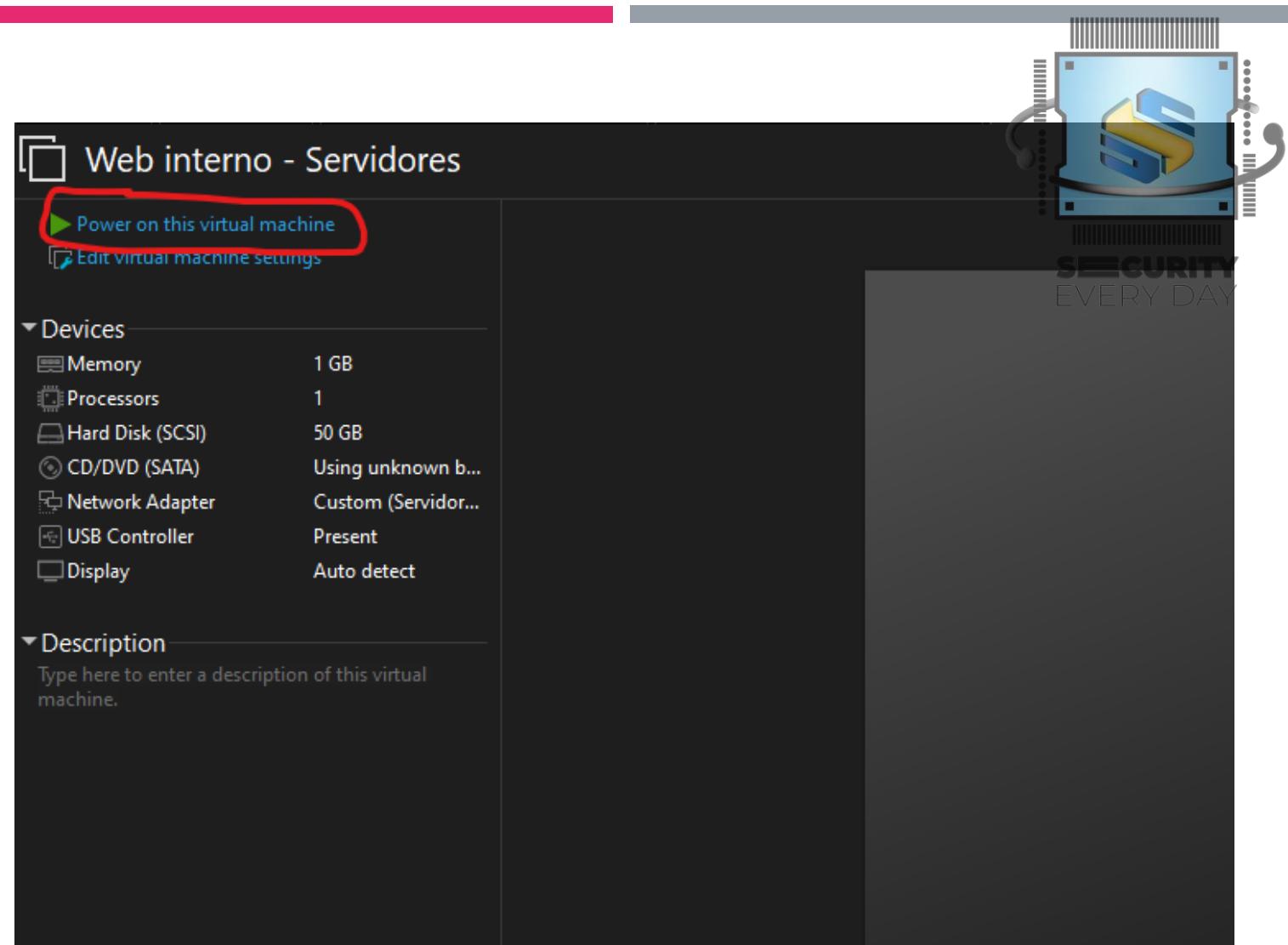
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Web interno - Servidores



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

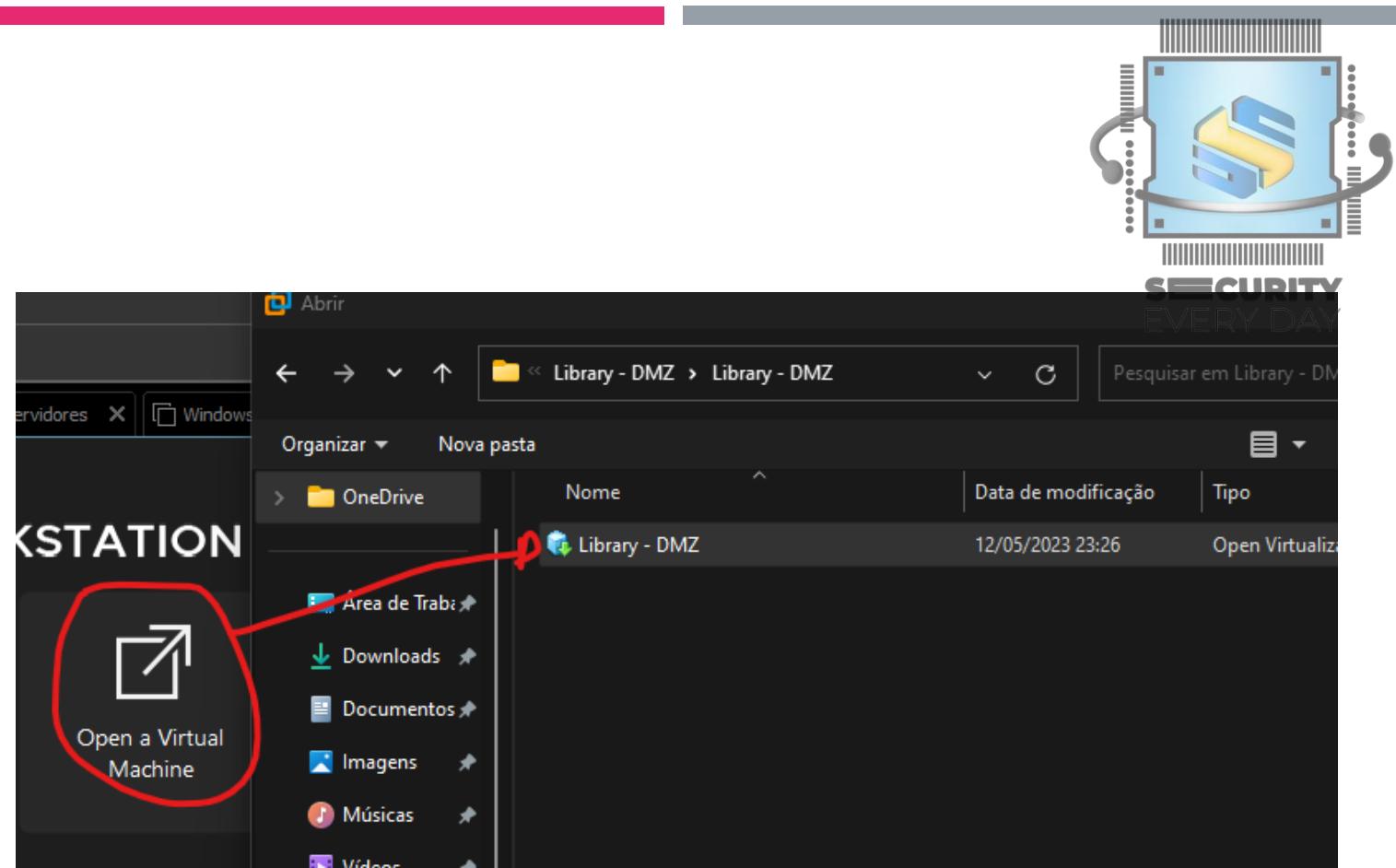
- Web interno – Servidores
- Entre com o usuário "ubuntu" senha "ubuntu" e execute um "ping google.com", se a conexão foi estabelecida com sucesso, significa que tudo deu certo



```
ubuntu@ubuntu:~$ ping google.com
PING google.com (142.250.201.78) 56(84) bytes of data.
64 bytes from mad07s25-in-f14.1e100.net (142.250.201.78): icmp_seq=1 ttl=127 time=26.8 ms
64 bytes from mad07s25-in-f14.1e100.net (142.250.201.78): icmp_seq=2 ttl=127 time=25.1 ms
64 bytes from mad07s25-in-f14.1e100.net (142.250.201.78): icmp_seq=3 ttl=127 time=26.5 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 25.078/26.138/26.833/0.761 ms
ubuntu@ubuntu:~$ _
```

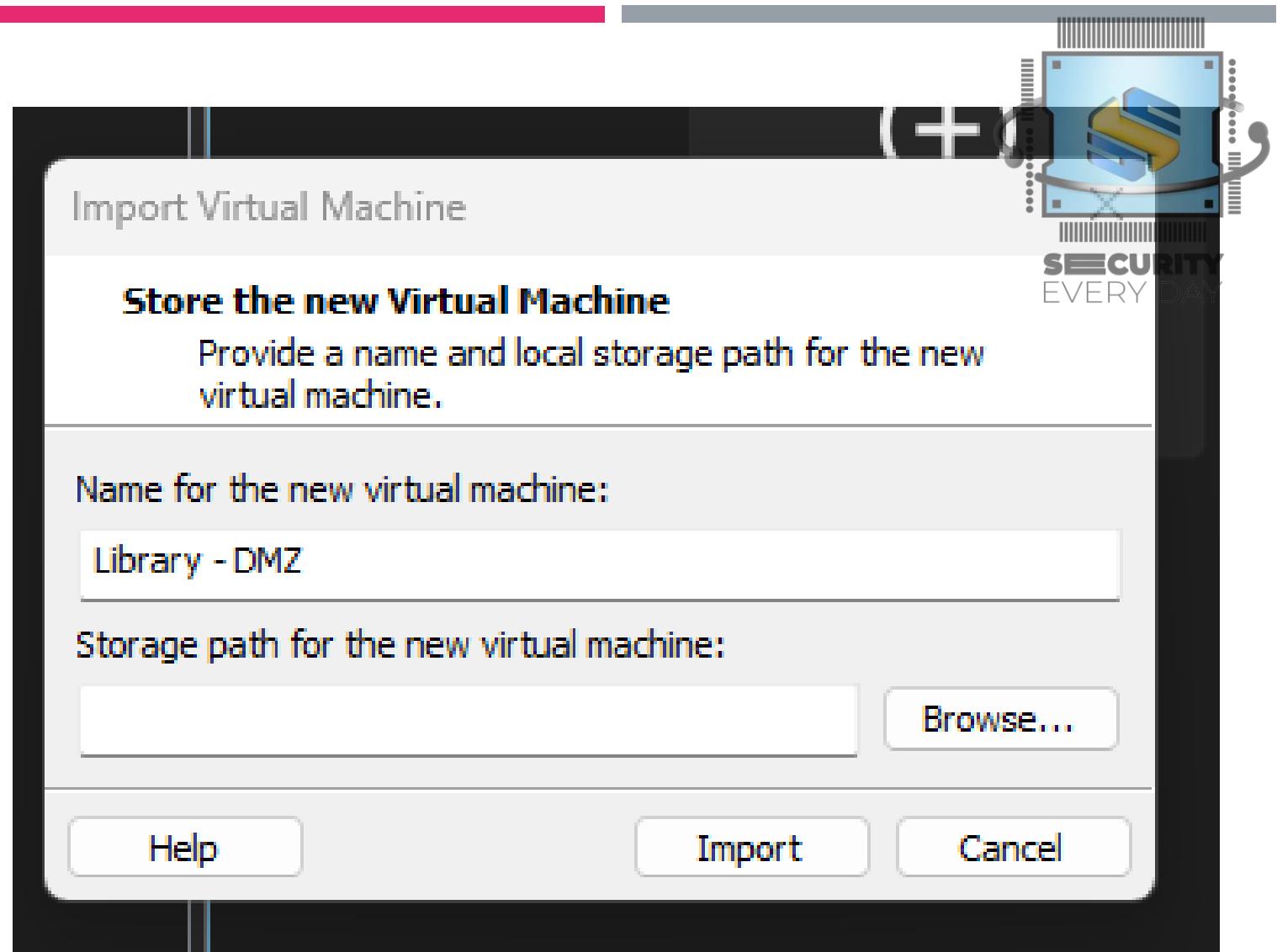
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



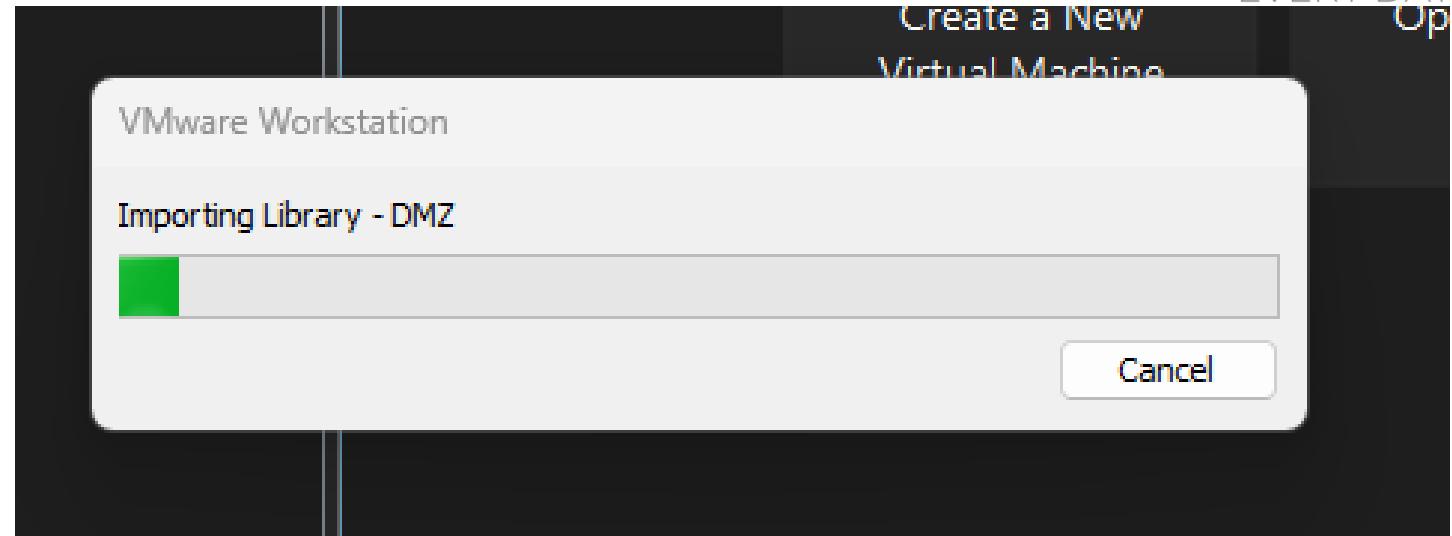
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



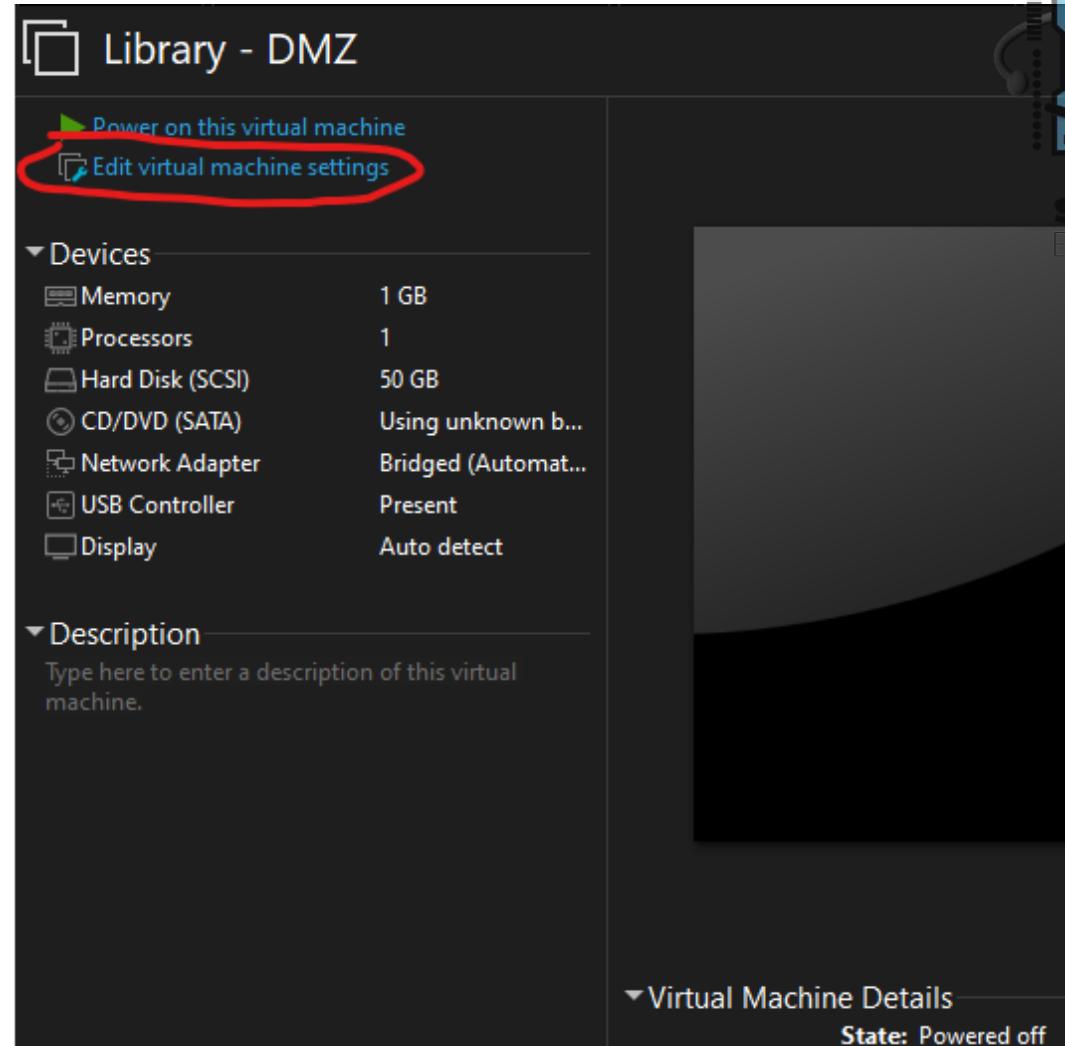
IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ

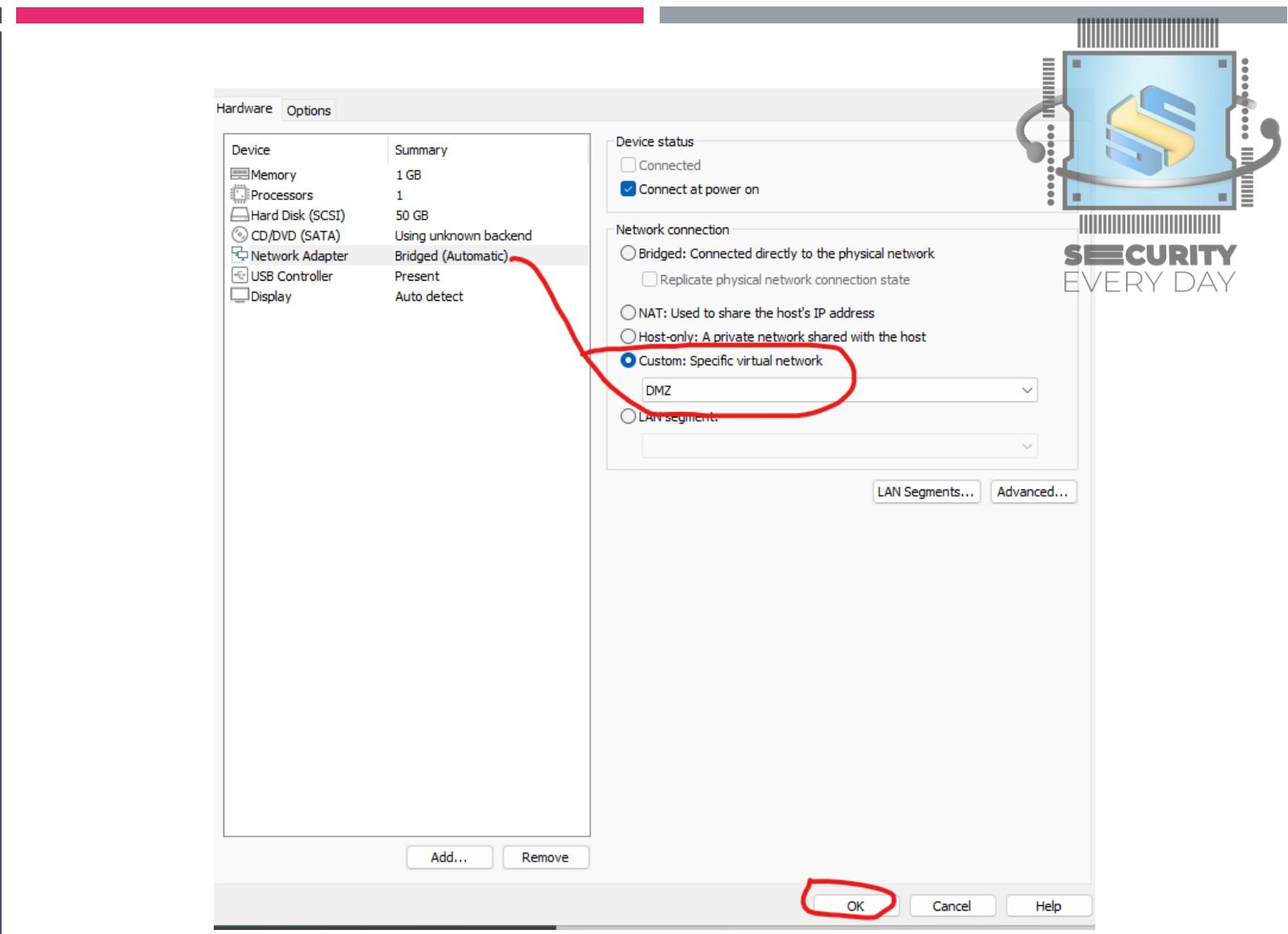


The screenshot shows the 'Library - DMZ' interface in VMware Workstation. At the top, there are two main options: 'Power on this virtual machine' and 'Edit virtual machine settings'. The 'Edit virtual machine settings' option is circled in red. Below these are sections for 'Devices' and 'Description'. The 'Devices' section lists memory (1 GB), processors (1), hard disk (50 GB, SCSI), CD/DVD (SATA, using unknown b...), network adapter (Bridged (Automat...)), USB controller (Present), and display (Auto detect). The 'Description' section has a placeholder 'Type here to enter a description of this virtual machine.' At the bottom, it says 'Virtual Machine Details' and 'State: Powered off'.



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ



IMPORTAR MAQUINAS PARA O VMWARE WORKSTATION

- Library - DMZ

Library - DMZ

[Power on this virtual machine](#) [Edit virtual machine settings](#)

▼ Devices

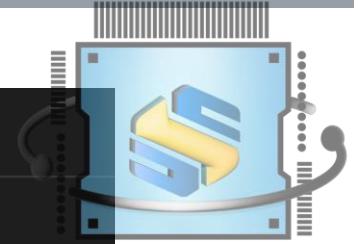
Memory	1 GB
Processors	1
Hard Disk (SCSI)	50 GB
CD/DVD (SATA)	Using unknown b...
Network Adapter	Custom (DMZ)
USB Controller	Present
Display	Auto detect

▼ Description

Type here to enter a description of this virtual machine.

▼ Virtual Machine Details

State: Powered off



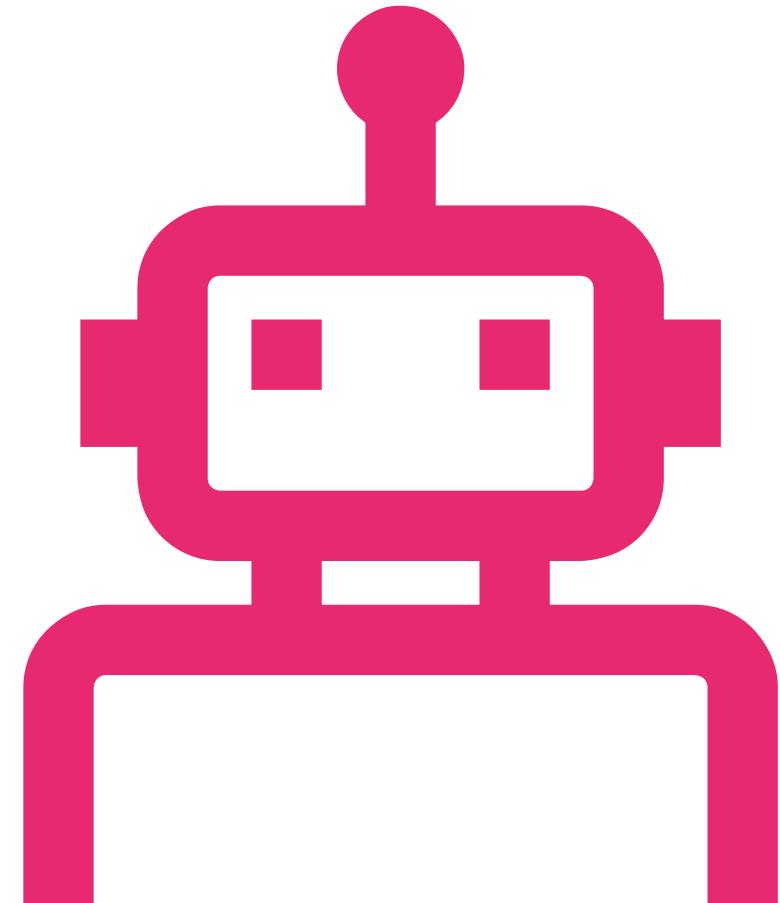
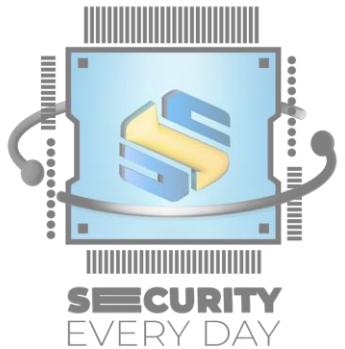
SECURITY
EVERY DAY

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



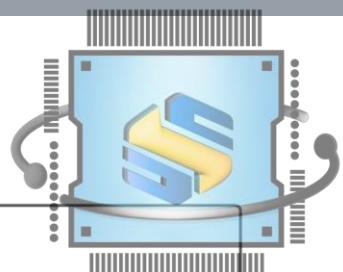
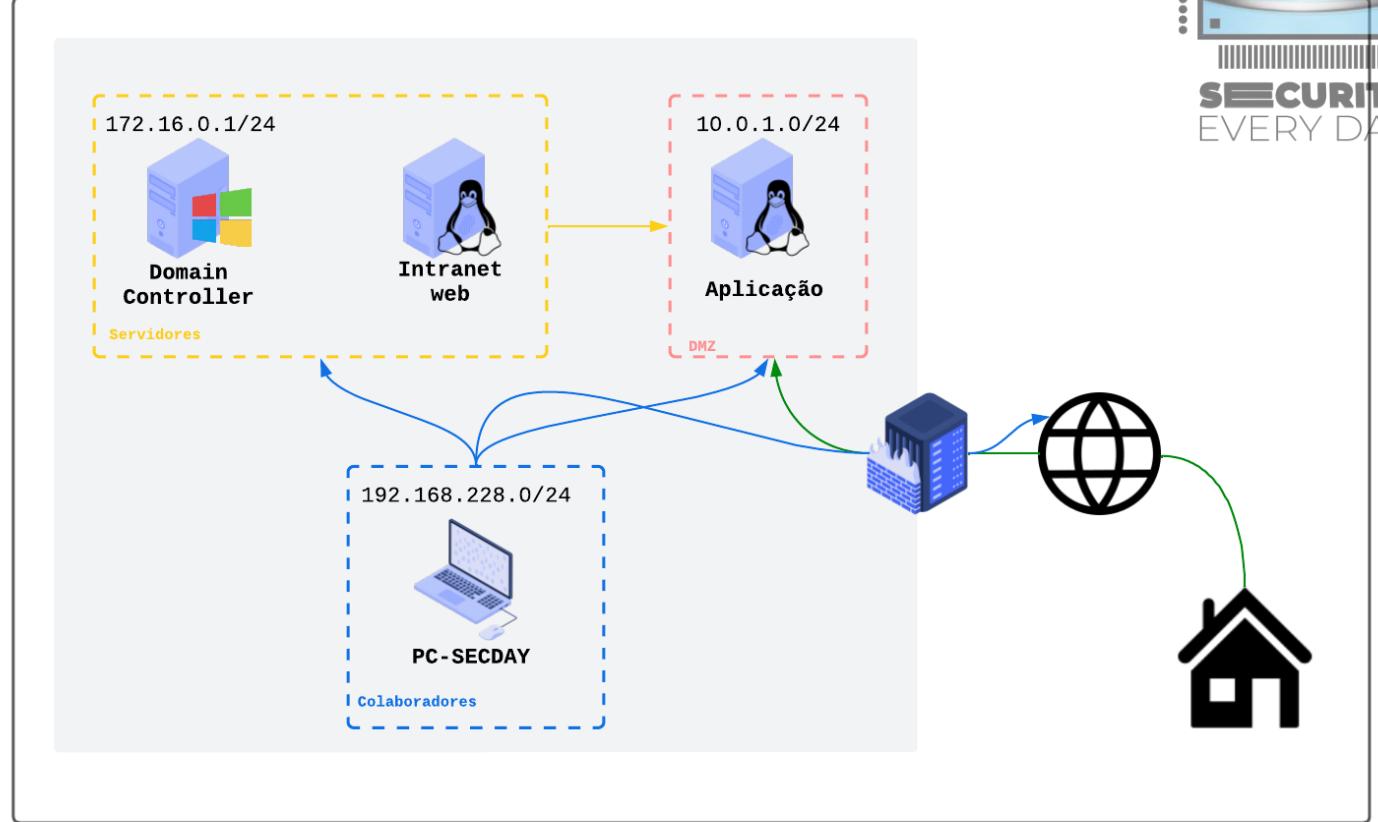
```
Last login: Mon May 15 16:18:13 UTC 2023 on ttys1
ubuntu@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=22.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=21.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=20.9 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 20.862/21.483/22.003/0.471 ms
ubuntu@ubuntu:~$
```



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

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



SECURITY
EVERY DAY

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

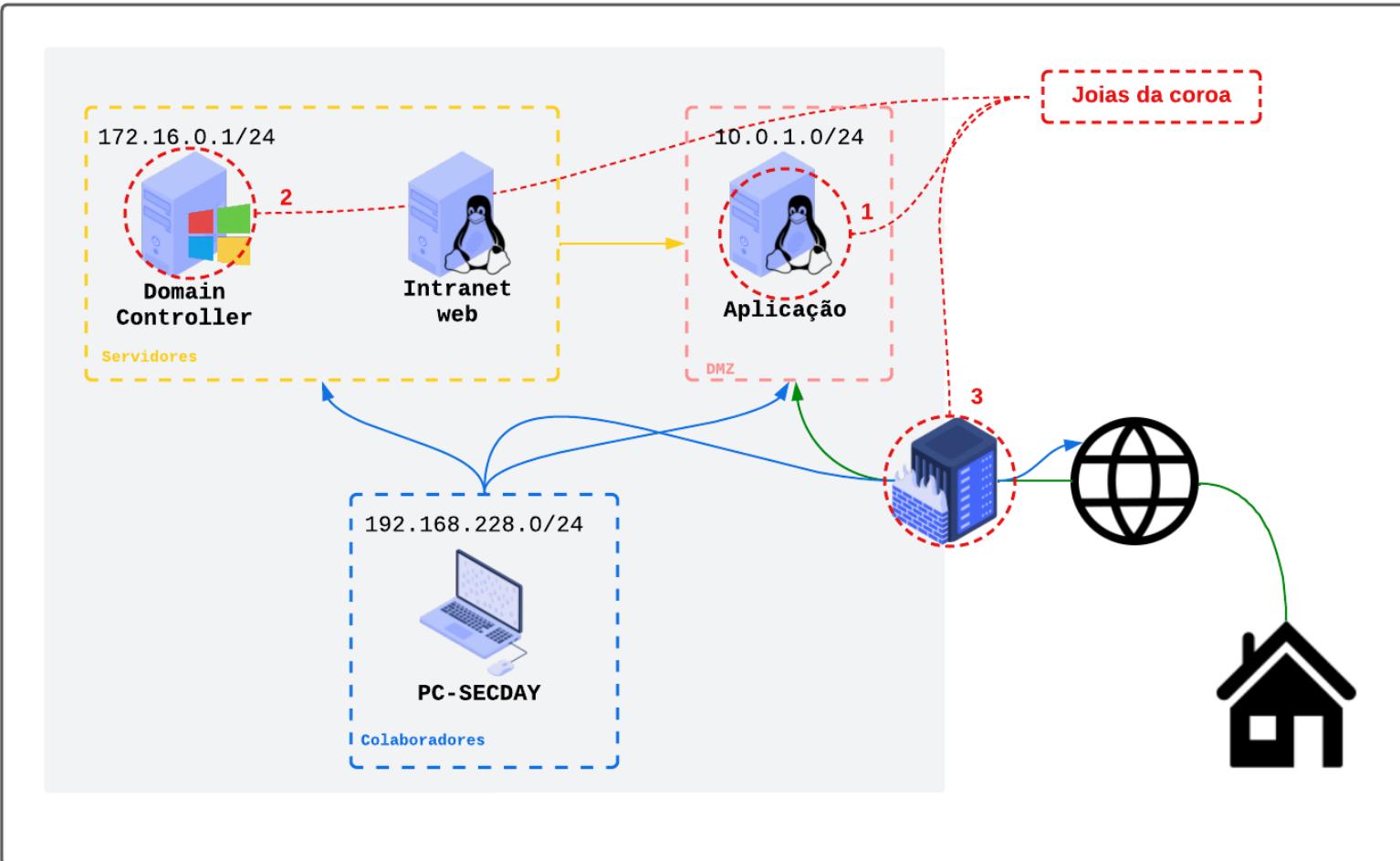
Propriedade intelectual

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



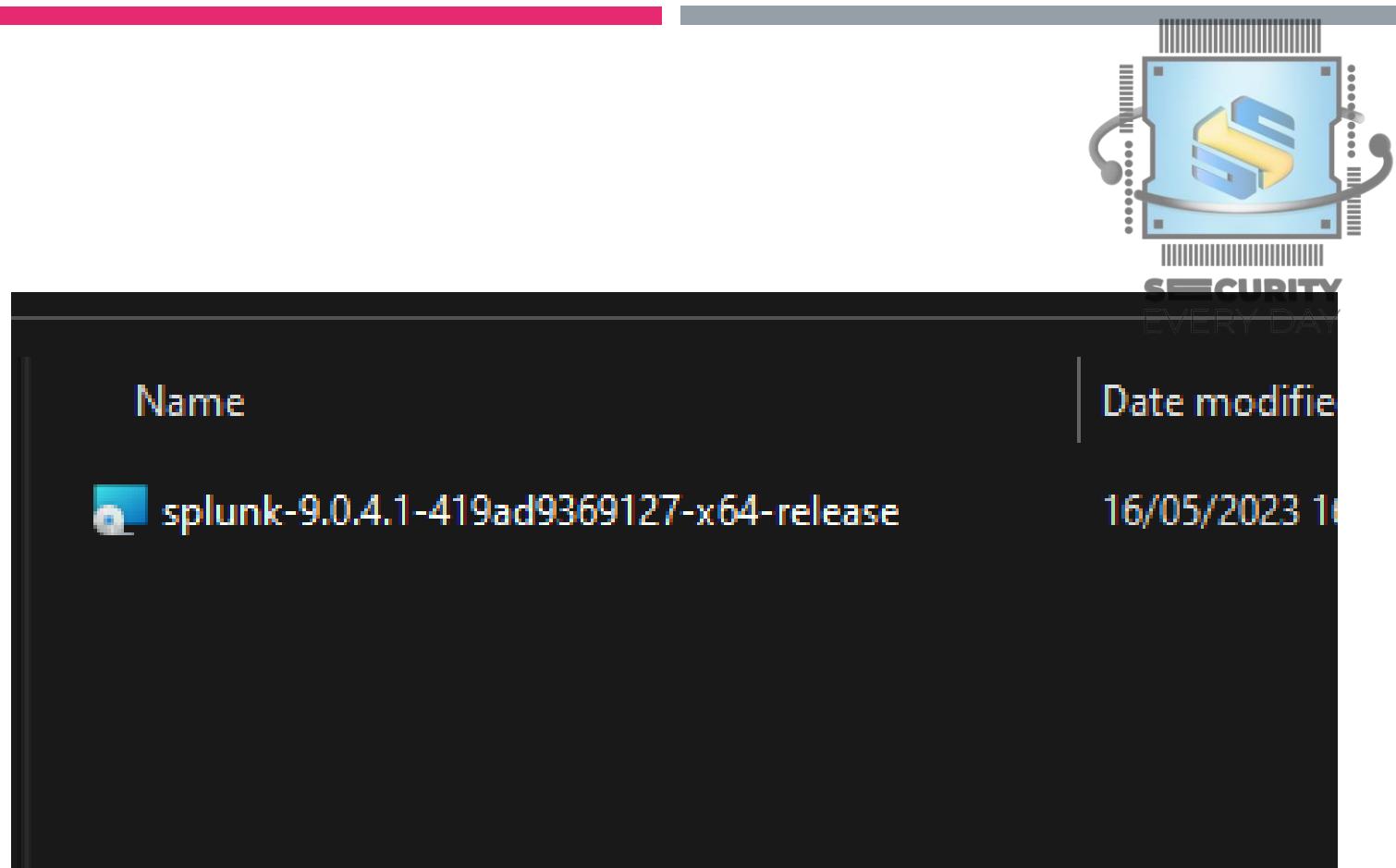
INSTALAÇÃO DO SIEM



- 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>

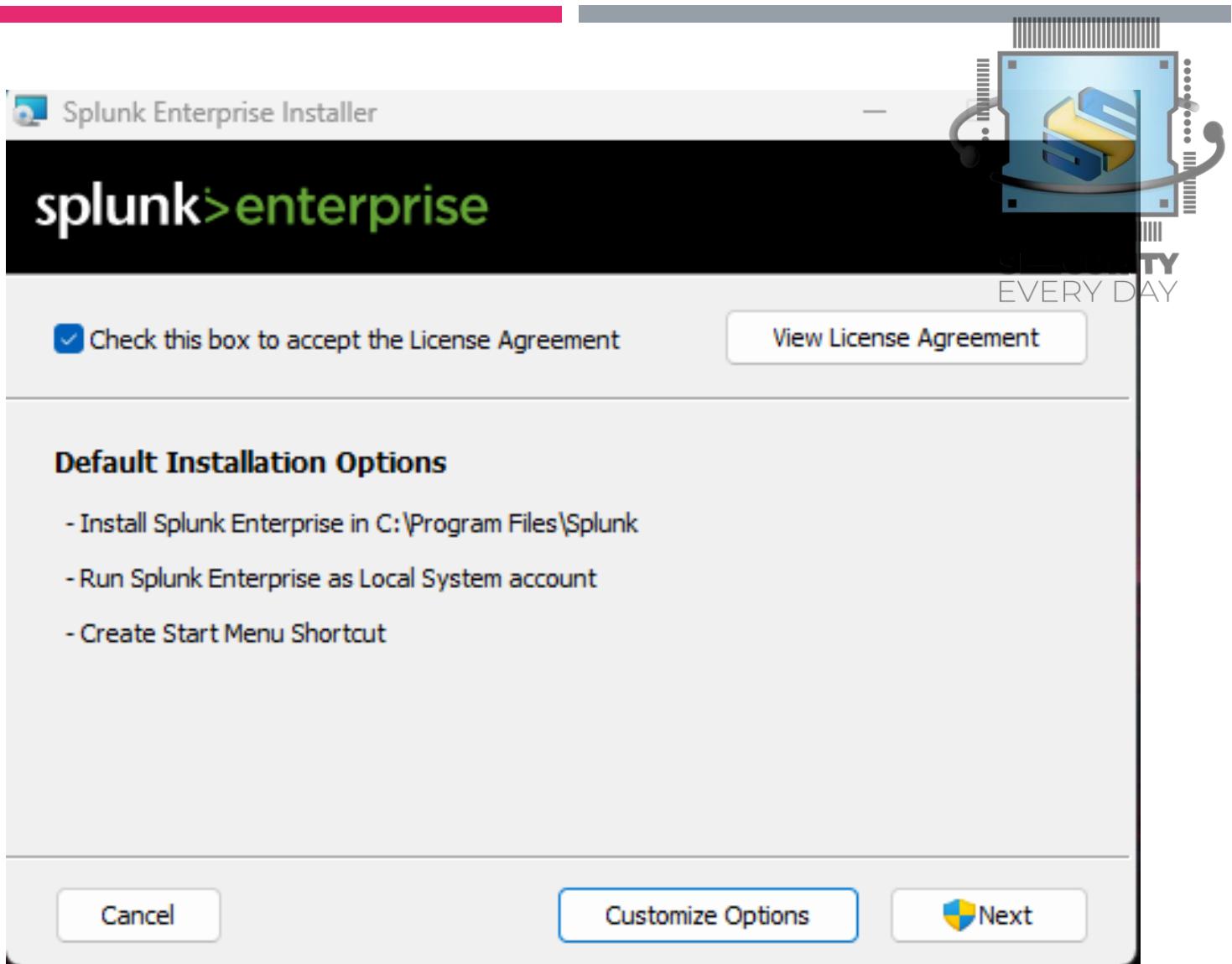
INSTALAÇÃO DO SIEM

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



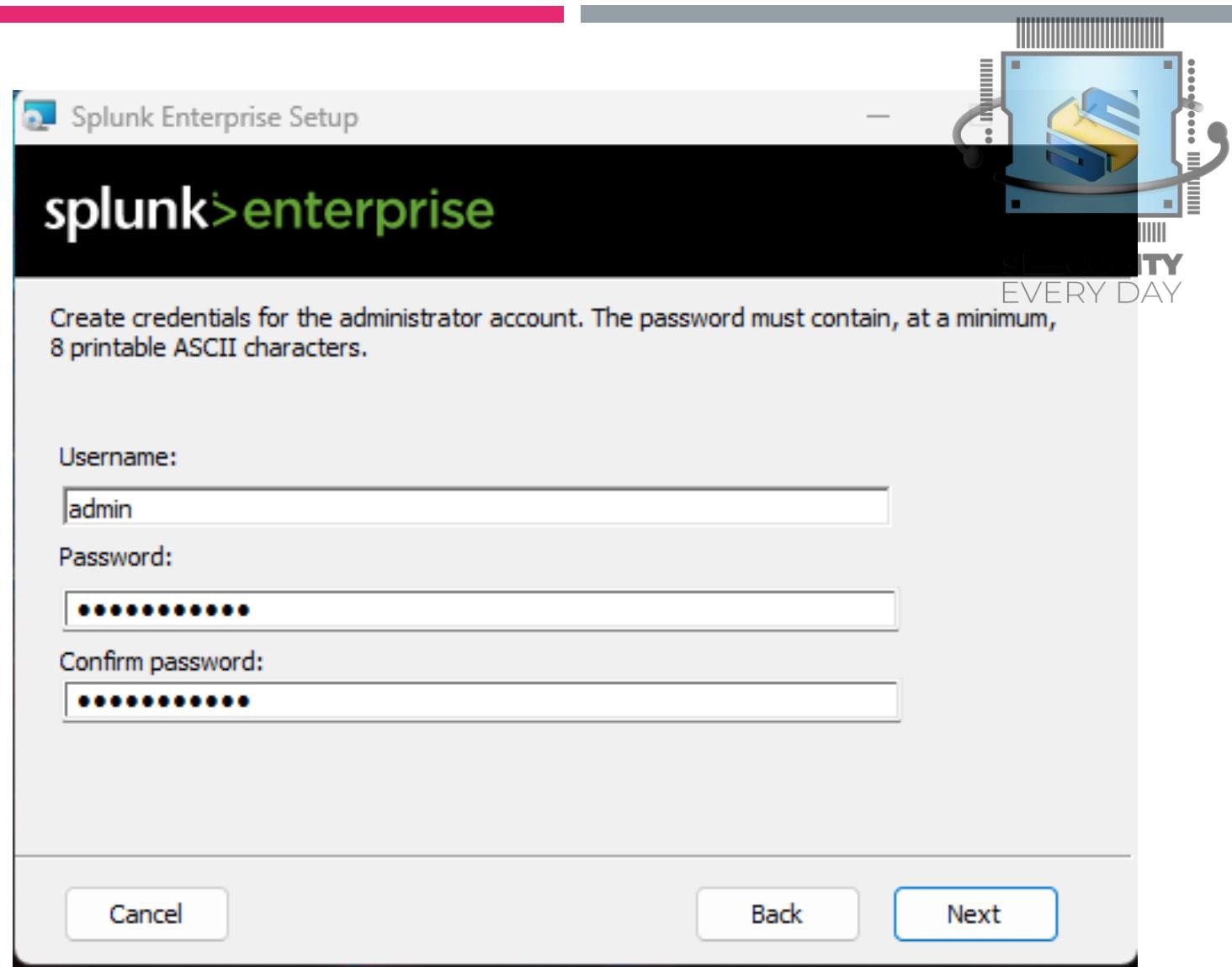
INSTALAÇÃO DO SIEM

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



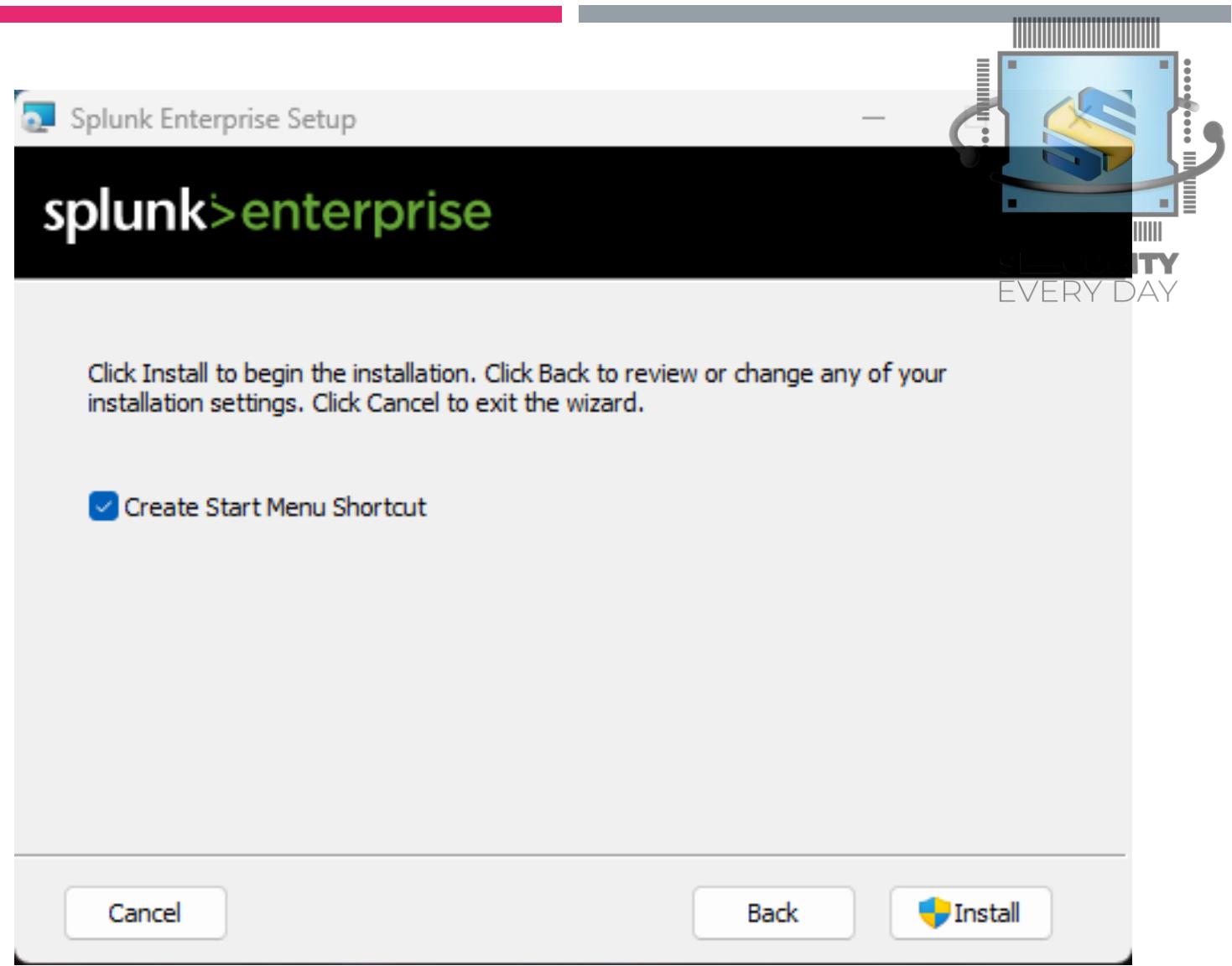
INSTALAÇÃO DO SIEM

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



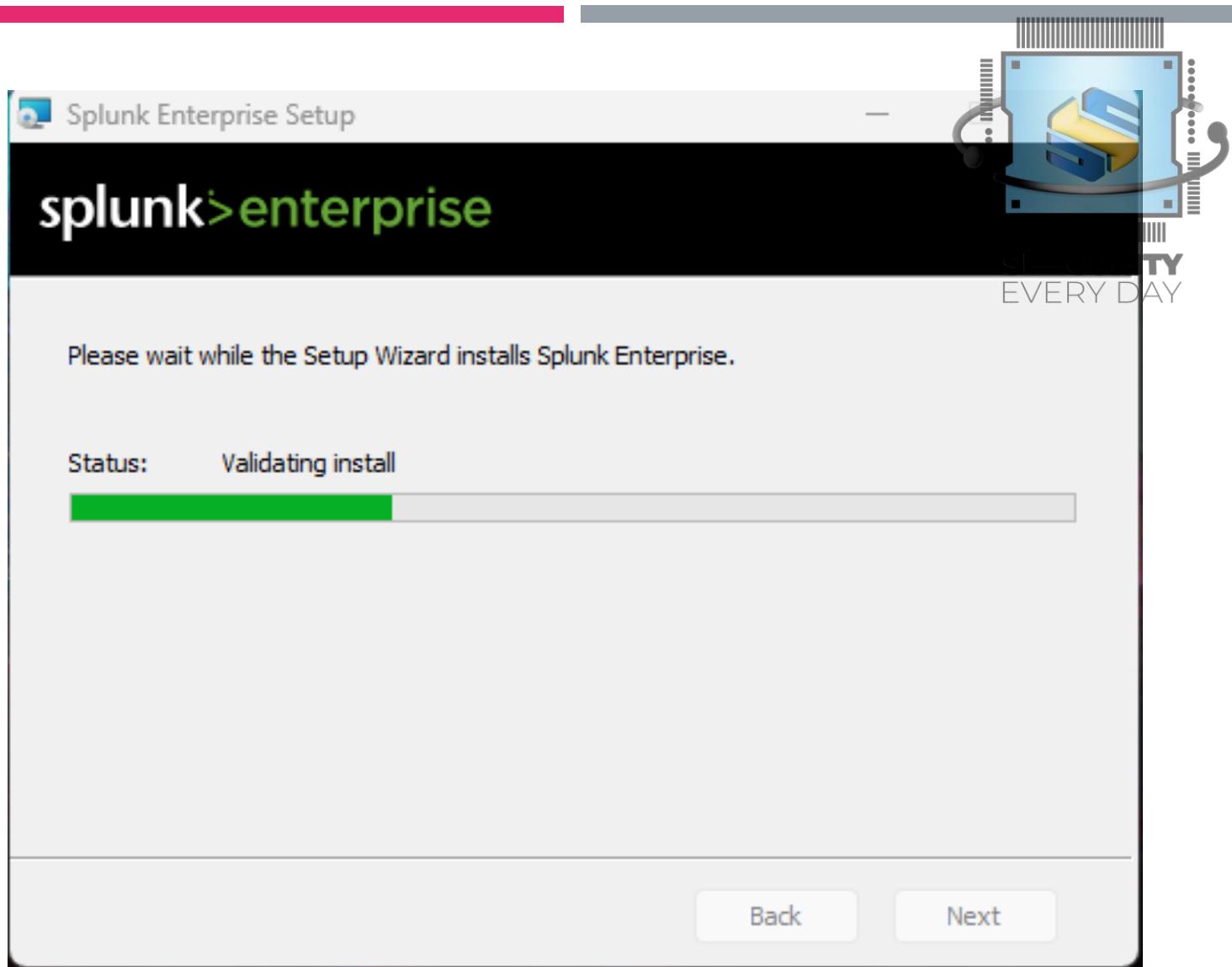
INSTALAÇÃO DO SIEM

- Clique em “Install”



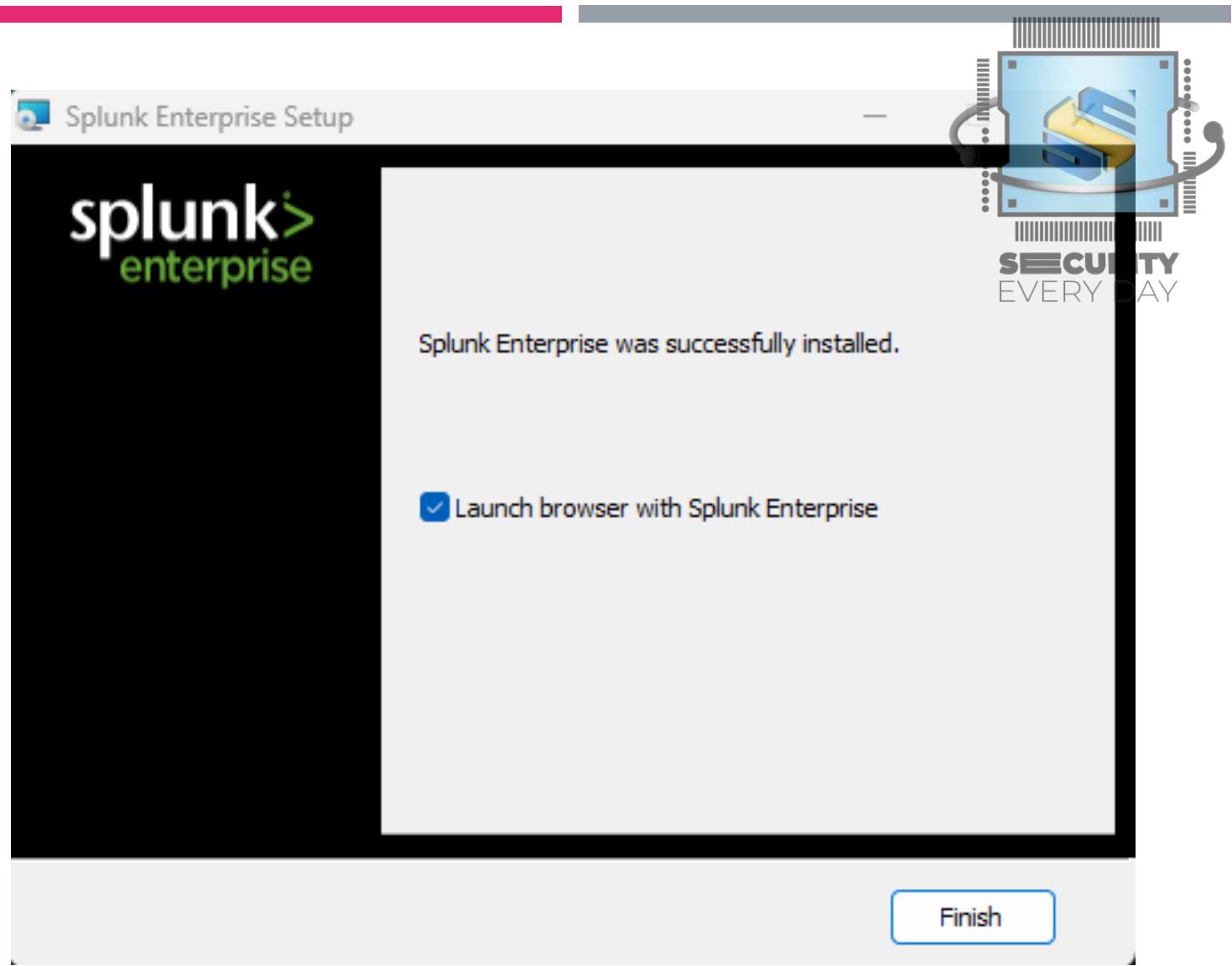
INSTALAÇÃO DO SIEM

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



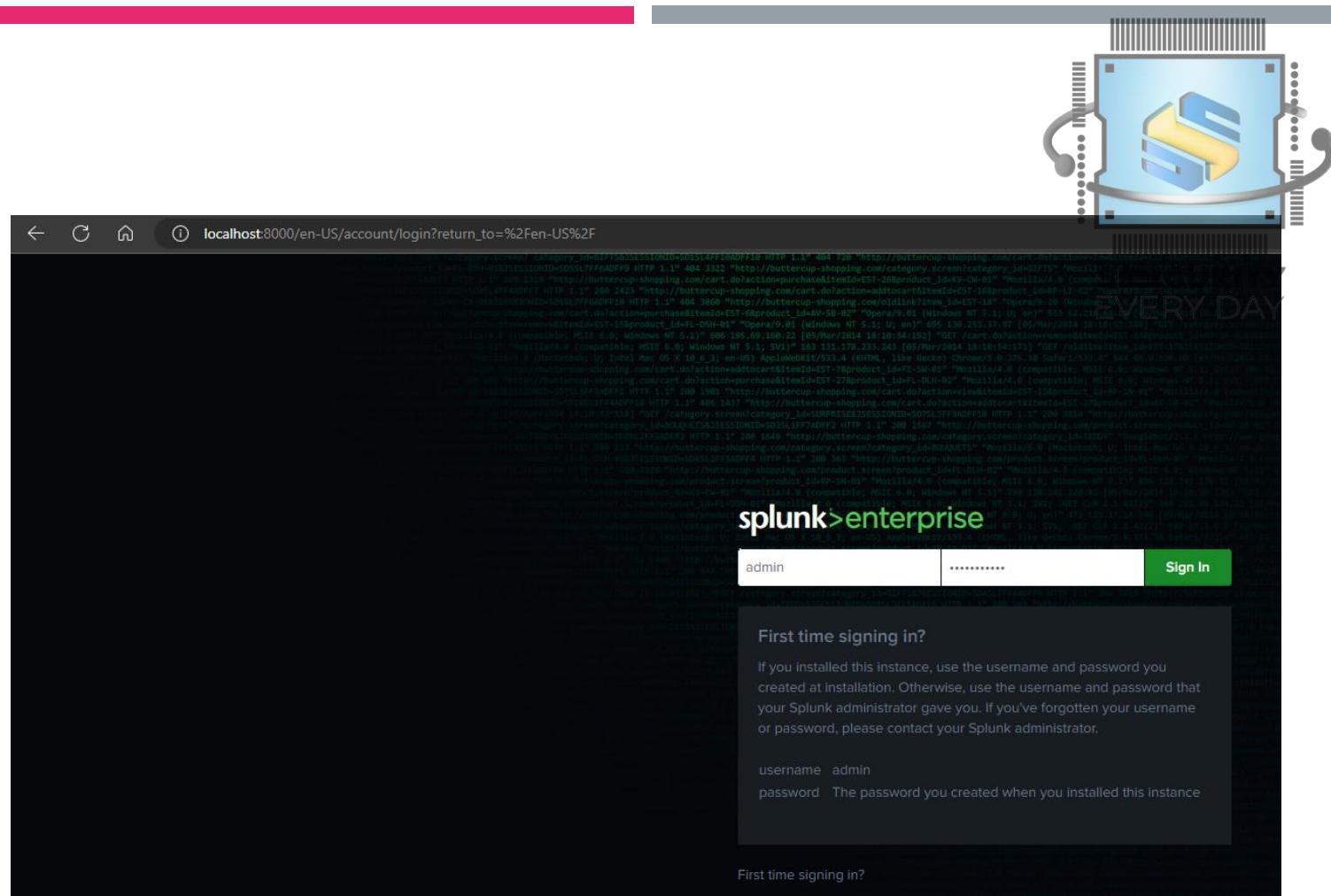
INSTALAÇÃO DO SIEM

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



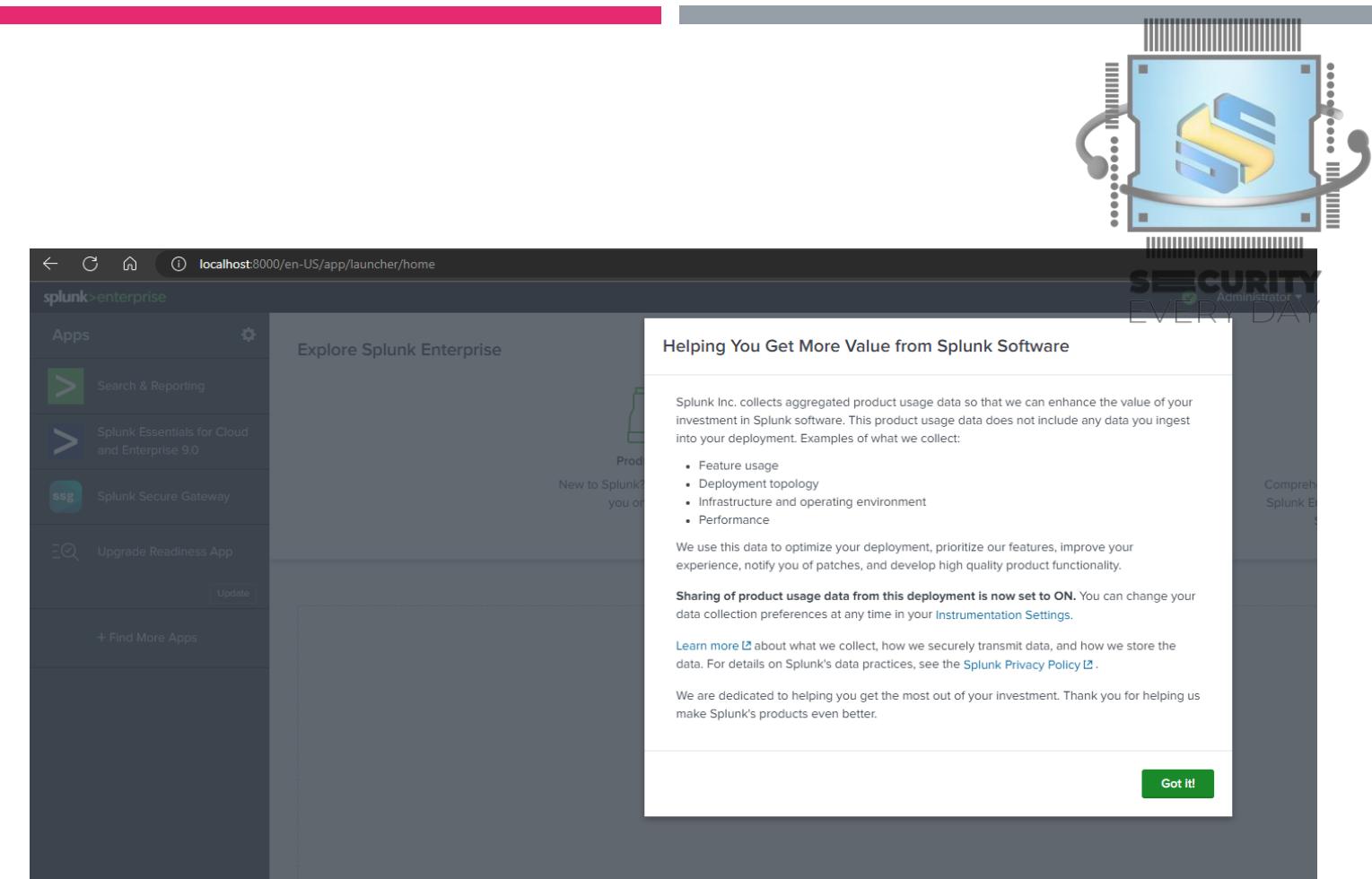
INSTALAÇÃO DO SIEM

- 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!”



The screenshot shows the Splunk Enterprise app launcher interface at `localhost:8000/en-US/app/launcher/home`. On the left, there's a sidebar titled "splunk>enterprise" with sections for "Apps" and "Search & Reporting". A central panel displays "Explore Splunk Enterprise" with a "New to Splunk? Get Started" button. Overlaid on the right is a white box containing the following text:

Helping You Get More Value from Splunk Software

Splunk Inc. collects aggregated product usage data so that we can enhance the value of your investment in Splunk software. This product usage data does not include any data you ingest into your deployment. Examples of what we collect:

- Feature usage
- Deployment topology
- Infrastructure and operating environment
- Performance

We use this data to optimize your deployment, prioritize our features, improve your experience, notify you of patches, and develop high quality product functionality.

Sharing of product usage data from this deployment is now set to ON. You can change your data collection preferences at any time in your [Instrumentation Settings](#).

[Learn more](#) about what we collect, how we securely transmit data, and how we store the data. For details on Splunk's data practices, see the [Splunk Privacy Policy](#).

We are dedicated to helping you get the most out of your investment. Thank you for helping us make Splunk's products even better.

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”

The screenshot shows the Splunk web interface. At the top, there is a navigation bar with links for Administrator, Messages, Settings (which is highlighted with a red oval), Activity, Help, and a search bar labeled "Find SECURITY EVERY DAY". To the right of the search bar is a cartoon character wearing headphones and holding a microphone. Below the navigation bar, there is a sidebar with icons for Add Data, Monitoring, and Console. The main content area is divided into several sections: KNOWLEDGE (Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations), DATA (Data inputs; Forwarding and receiving - which is also highlighted with a red oval; Indexes; Report acceleration summaries; Source types; Ingest actions), and DISTRIBUTED ENVIRONMENT (Indexer clustering; Forwarder management; Federated search). A red arrow points from the text in the list above to the "Forwarding and receiving" link in the DATA section.

INSTALAÇÃO DO SIEM

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

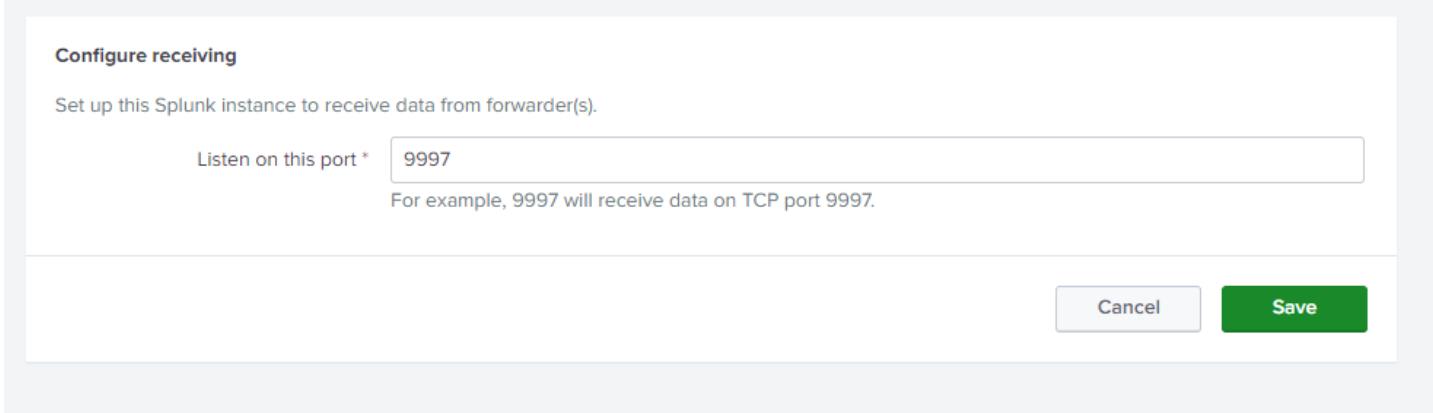
Receive data
Configure this instance to receive data forwarded from other instances.

[Configure receiving](#) + Add new



INSTALAÇÃO DO SIEM

- Clique em “Save”



Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

For example, 9997 will receive data on TCP port 9997.

Cancel Save



INSTALAÇÃO DO SIEM

- Pronto, porta configurada



Receive data
Forwarding and receiving > Receive data

Successfully saved "9997".

Showing 1-1 of 1 item

filter	Search icon	Status
9997		Enabled Disable

Listen on this port ▾

COLETA DE LOGS

CONFIGURAÇÃO
DO SERVIDOR
NTP



PORQUE O NTP É IMPORTANTE?



Correlação de logs



Análise forense



Integridade de transações

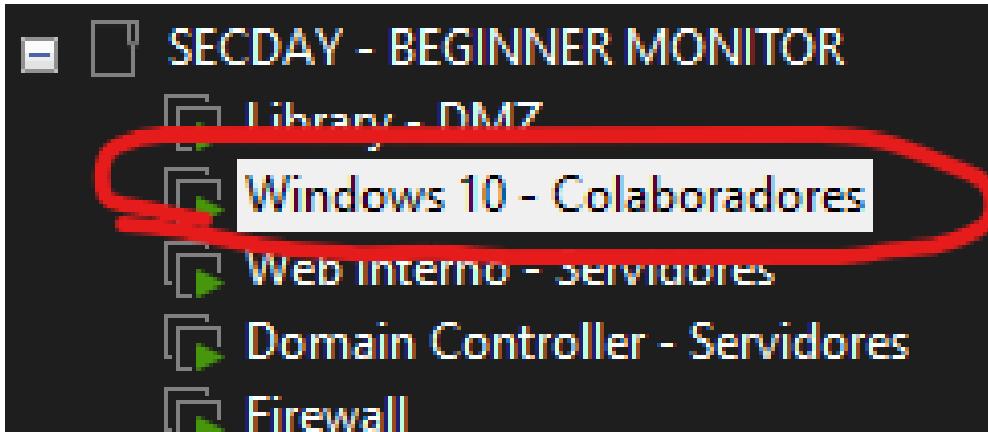


Etc...





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



A screenshot of a web browser displaying the pfSense Login interface. The address bar shows the URL <https://pfSense.secday.local/index.php>. The page title is "pfSense - Login". The pfSense logo is visible at the top left. The main area is a dark blue box containing a "SIGN IN" form. The "User" field is filled with "admin" and the "Pass" field contains ".....". A green "SIGN IN" button is at the bottom right of the form.

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

CONFIGURANDO O SERVIDOR NTP



⚠ Não seguro | <https://pfSense.secday.local>

pfSense COMMUNITY EDITION

Status / Dashboard

System Information

Name	pfSense.secday.local
User	admin@192.168.228.100 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 51c87d6f1ed81976e630
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	AMD Ryzen 7 5800X 8-Core Processor AES-NI CPU Crypto: Yes (inactive) OAT Crypto: No

Services ▾

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server & RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- NTP** (highlighted with a red circle)
- PPPoE Server
- SNMP
- Suricata
- UPnP & NAT-PMP
- Wake-on-LAN

If you purchased your pfSense, you have access to the **NETGATE RESOURCES**. You also may upgrade to a Support subscription. We're committed to delivering excellent support and more than competitive prices.

- [Upgrade Your Support](#)
- [Netgate Global Support](#)

- Vá até “Services → NTP”



CONFIGURANDO O SERVIDOR NTP

Services / NTP / Settings

Settings ACLs Serial GPS PPS

NTP Server Configuration

Enable Enable NTP Server
You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.

Interface WAN LAN SERVIDORES DMZ
Interfaces without an IP address will not be shown.
Selecting no interfaces will listen on all interfaces with a wildcard.
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers

Server	Prefer	Type
a.st1.ntp.br	<input checked="" type="checkbox"/>	Pool
b.st1.ntp.br	<input type="checkbox"/>	Pool
c.st1.ntp.br	<input type="checkbox"/>	Pool

Add + Add

- Em “Interface” selecione todas as interfaces
- Em “Time Servers”, vamos utilizar 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

The screenshot shows a configuration page for an NTP server. At the top, there are two 'Display Advanced' buttons. Below them is a warning about persistent log files. The 'Leap seconds' section contains detailed information about leap seconds and a note about IERS Bulletin C. The 'DNS Resolution' section has a dropdown set to 'Auto'. The 'Enable NTP Server Authentication' section has a checkbox for 'Enable NTPv3 authentication (RFC 1305)' which is unchecked. A 'Save' button is at the bottom.

- Em “Interface” selecione todas as interfaces
- Em “Time Servers”, vamos utilizar 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”

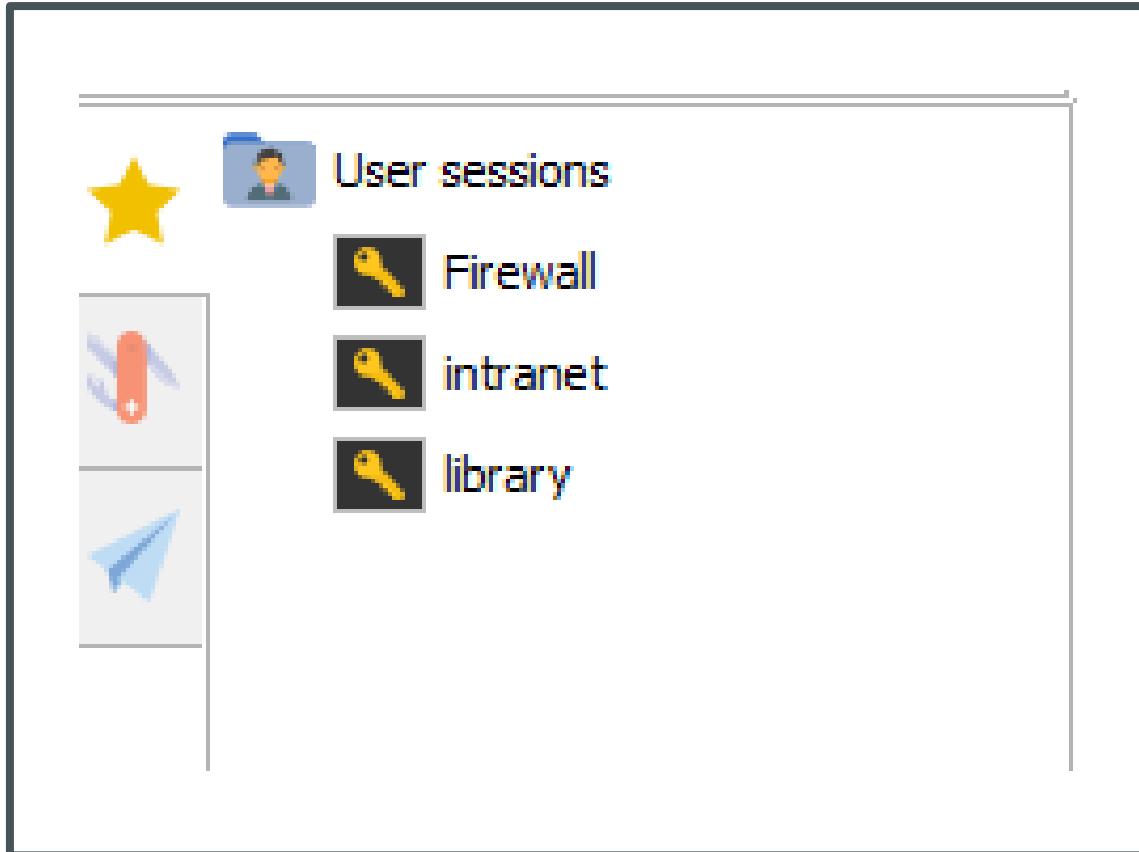
COLETA DE LOGS

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

```
• MobaXterm Personal Edition v23.1 •
(SSH client, X server and network tools)

SSH session to ubuntu@172.16.0.60
• Direct SSH : ✓
• SSH compression : ✓
• SSH-browser : ✓
• X11-forwarding : ✓ (remote display is forwarded through SSH)

For more info, ctrl+click on help or visit our website.

Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-71-generic x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Tue May 16 01:03:02 PM -03 2023

System load: 0.16015625 Processes: 209
Usage of /: 32.1% of 23.45GB Users logged in: 0
Memory usage: 46% IPv4 address for ens33: 172.16.0.60
Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

13 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue May 16 09:18:41 2023 from 192.168.228.100
ubuntu@ubuntu:~$
```

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



SINCRONIZAR NTP NOS SERVIDORES

```
ubuntu@ubuntu:~$ sudo apt-get install ntp -y
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ntp is already the newest version (1:4.2.8p15+dfsg-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
ubuntu@ubuntu:~$
```

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



SINCRONIZAR NTP NOS SERVIDORES

```
GNU nano 6.2
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
driftfile /var/lib/ntp/ntp.drift
# Leap seconds definition provided by tzdata
leapfile /usr/share/zoneinfo/leap-seconds.list
# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
# Specify one or more NTP servers.
server 172.16.0.1
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
#pool 0.ubuntu.pool.ntp.org iburst
#pool 1.ubuntu.pool.ntp.org iburst
#pool 2.ubuntu.pool.ntp.org iburst
#pool 3.ubuntu.pool.ntp.org iburst
# Use Ubuntu's ntp server as a fallback.
#pool ntp.ubuntu.com
# Access control configuration; see /usr/share/doc/ntp-doc/html/accept.html for
# details. The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.
#
# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery limited
restrict -6 default kod notrap nomodify nopeer noquery limited
```

- 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

```
ubuntu@ubuntu:~$ sudo service ntp restart
ubuntu@ubuntu:~$ sudo service ntp status
● ntp.service - Network Time Service
  Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
  Active: active (running) since Tue 2023-05-16 13:10:34 -03; 6s ago
    Docs: man:ntpd(8)
   Process: 2438 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
 Main PID: 2444 (ntpd)
   Tasks: 2 (limit: 907)
  Memory: 1.6M
     CPU: 9ms
    CGroup: /system.slice/ntp.service
           └─2444 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 114:120

May 16 13:10:34 ubuntu ntpd[2444]: Listen and drop on 0 v6wildcard [::]:123
May 16 13:10:34 ubuntu ntpd[2444]: Listen and drop on 1 v4wildcard 0.0.0.0:123
May 16 13:10:34 ubuntu ntpd[2444]: Listen normally on 2 lo 127.0.0.1:123
May 16 13:10:34 ubuntu ntpd[2444]: Listen normally on 3 ens33 172.16.0.60:123
May 16 13:10:34 ubuntu ntpd[2444]: Listen normally on 4 lo [::]:123
May 16 13:10:34 ubuntu ntpd[2444]: Listen normally on 5 ens33 [fe80::20c:29ff:fe61:fb50%2]:123
May 16 13:10:34 ubuntu ntpd[2444]: Listening on routing socket on fd #22 for interface updates
May 16 13:10:34 ubuntu ntpd[2444]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
May 16 13:10:34 ubuntu ntpd[2444]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
May 16 13:10:34 ubuntu systemd[1]: Started Network Time Service.
```

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



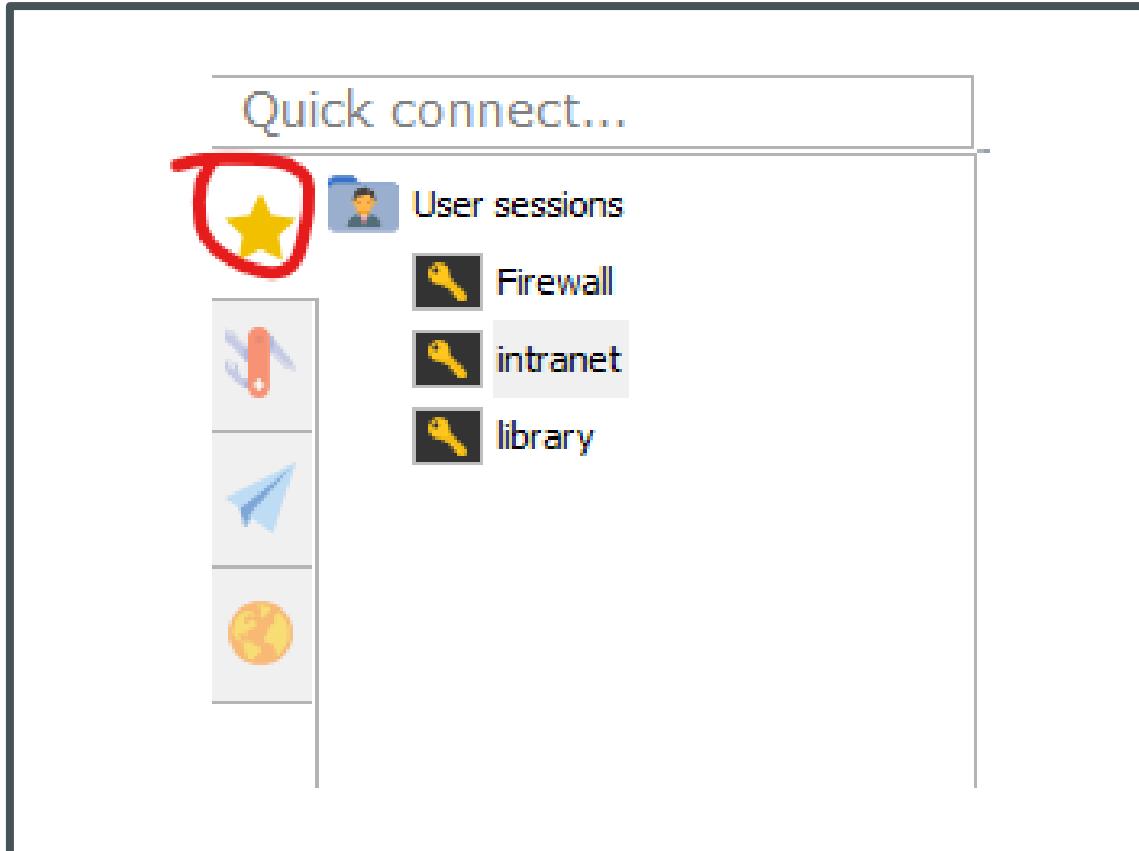
SINCRONIZAR NTP NOS SERVIDORES

```
ubuntu@ubuntu:~$ sudo timedatectl set-timezone America/Sao_Paulo
ubuntu@ubuntu:~$ timedatectl
      Local time: Tue 2023-05-16 13:14:21 -03
      Universal time: Tue 2023-05-16 16:14:21 UTC
            RTC time: Tue 2023-05-16 16:14:21
           Time zone: America/Sao_Paulo (-03, -0300)
System clock synchronized: no
    NTP service: n/a
      RTC in local TZ: no
ubuntu@ubuntu:~$ sudo ln -sf /usr/share/zoneinfo/America/Sao_Paulo /etc/localtime
ubuntu@ubuntu:~$ date
Tue May 16 01:20:03 PM -03 2023
ubuntu@ubuntu:~$ █
```

- 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



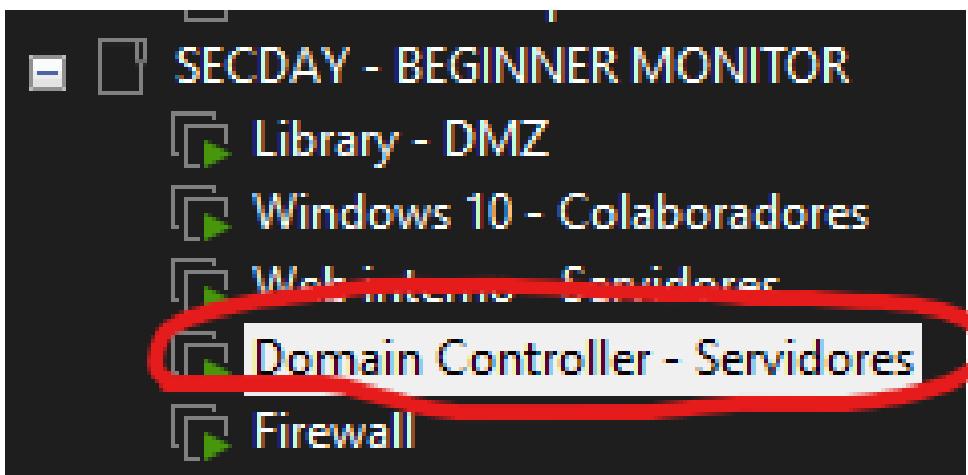
SINCRONIZAR NTP NOS SERVIDORES



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



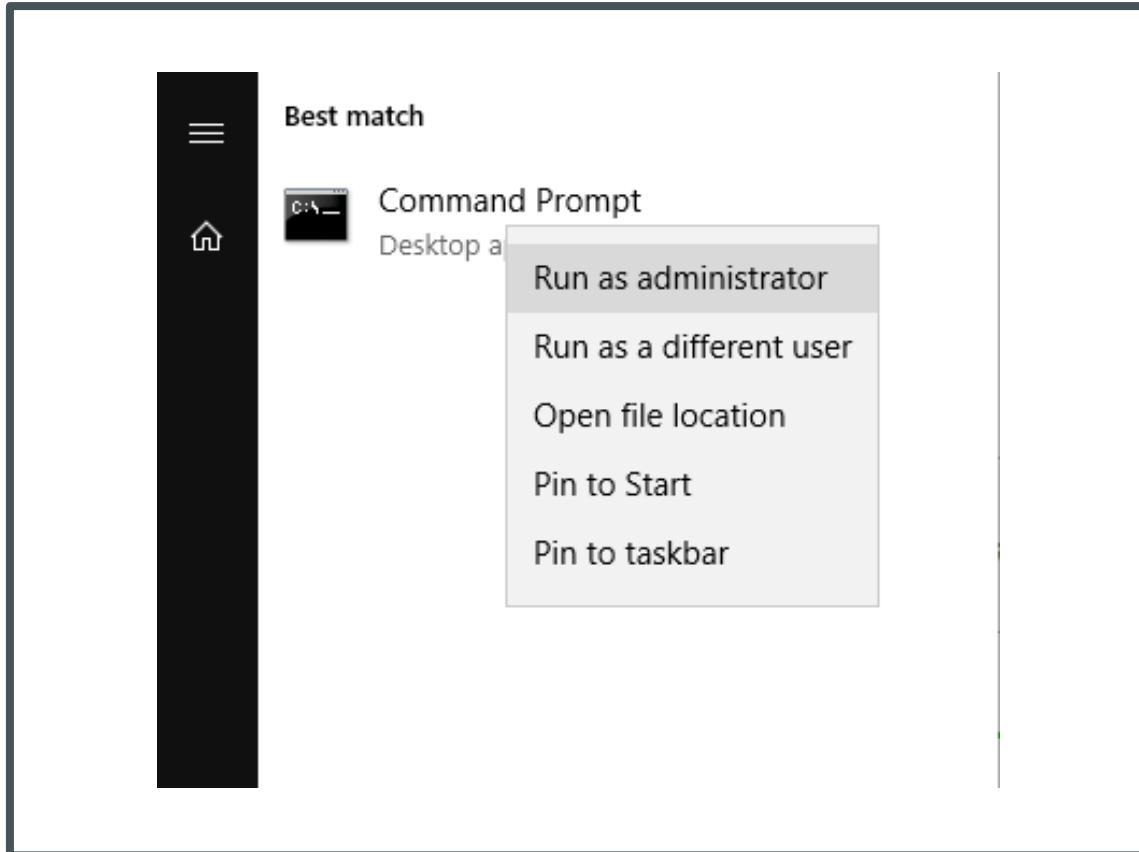
SINCRONIZAR NTP NOS SERVIDORES



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



SINCRONIZAR NTP NOS SERVIDORES



- Abra o prompt de comando como administrador



SINCRONIZAR NTP NOS SERVIDORES

```
C:\Users\Administrator>w32tm /config /manualpeerlist:"172.16.0.1" /syncfromflags:MANUAL
The command completed successfully.

C:\Users\Administrator>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

C:\Users\Administrator>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.

C:\Users\Administrator>w32tm /resync
Sending resync command to local computer
The command completed successfully.
```

- 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

```
C:\ Administrator: Command Prompt  
C:\Users\Administrator>tzutil /s "E. South America Standard Time"  
C:\Users\Administrator>
```

- Para configurar o time zone, execute o comando
 - 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



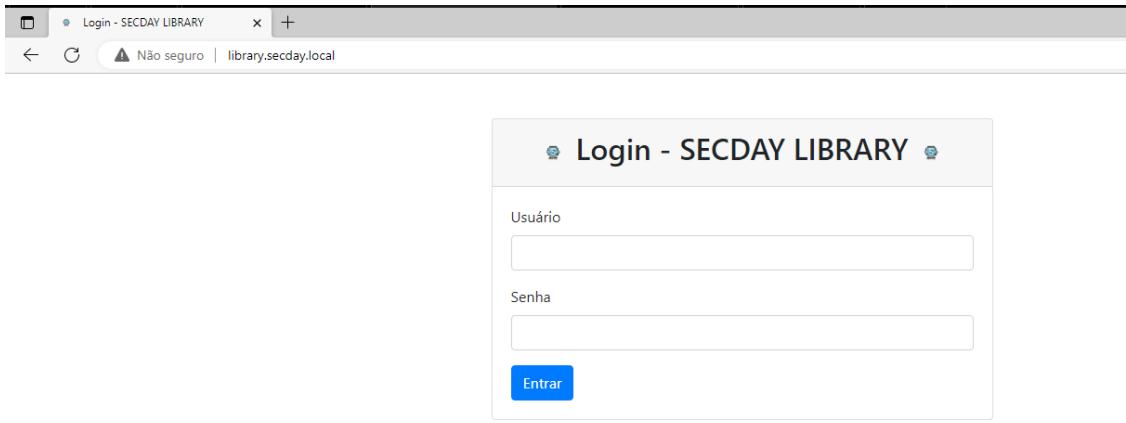
APLICAÇÃO



DADOS



SEGURANÇA



Login - SECDAY LIBRARY

Usuário

Senha

Entrar

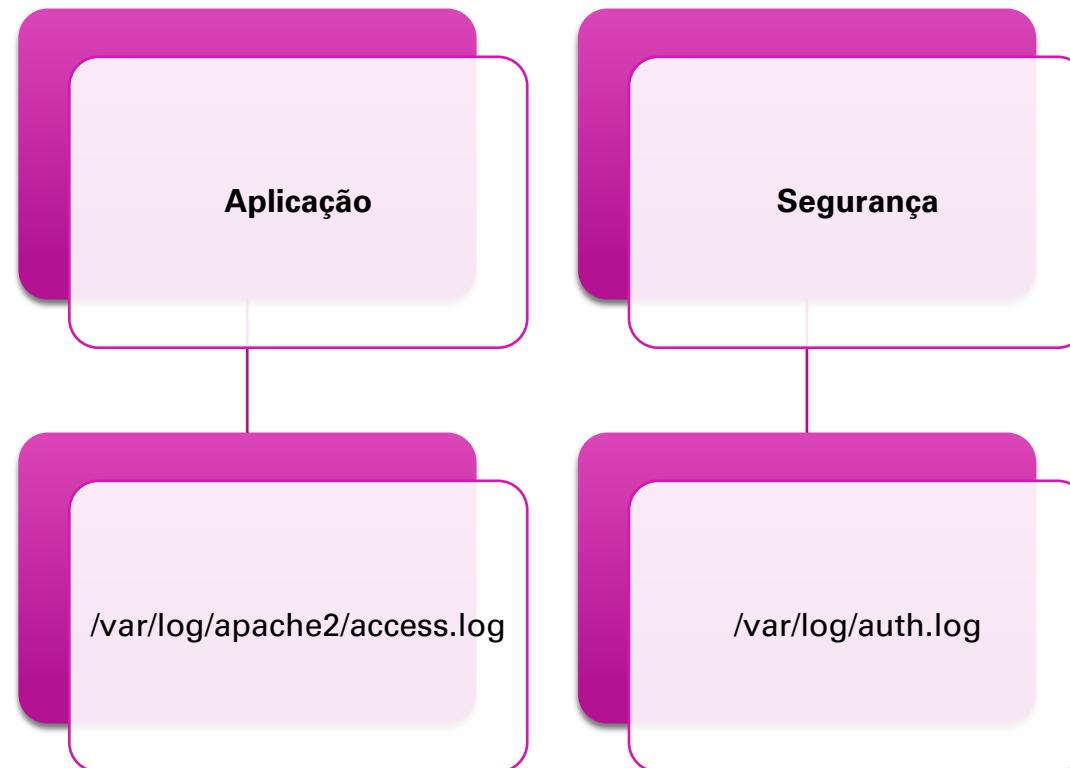


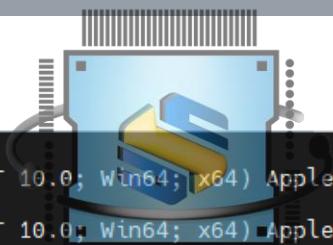
COLETA

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



COLETA

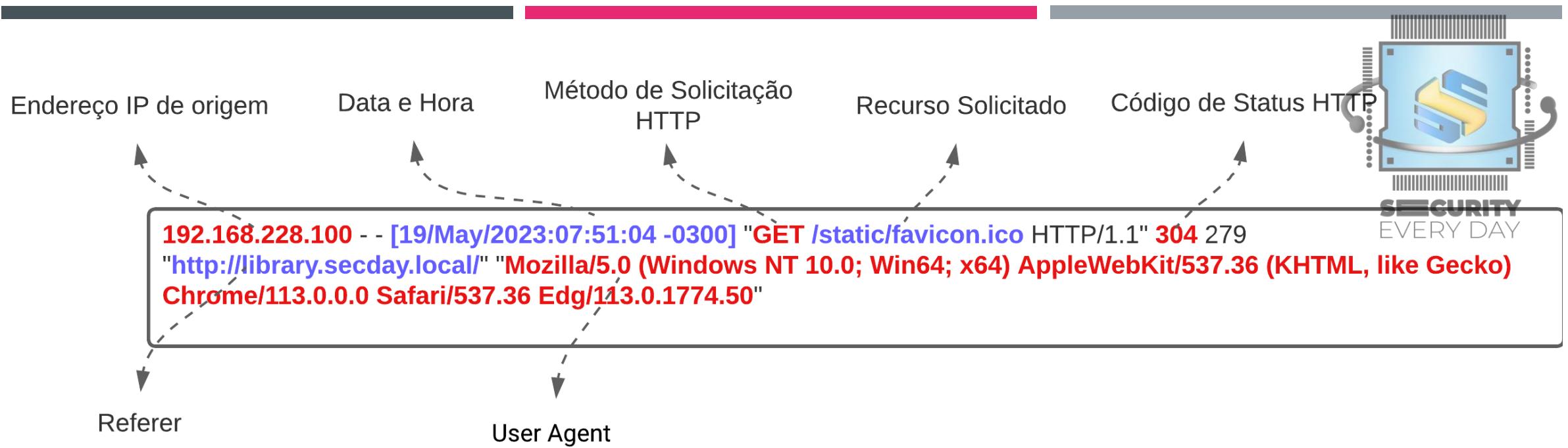




```
ubuntu@ubuntu:~$ sudo tail -f /var/log/apache2/access.log
192.168.228.100 - - [19/May/2023:07:51:04 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library.secday.local/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:04 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library.secday.local/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:04 -0300] "GET / HTTP/1.1" 200 827 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:05 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library.secday.local/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:05 -0300] "GET / HTTP/1.1" 200 827 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:05 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library.secday.local/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:06 -0300] "GET / HTTP/1.1" 200 827 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:06 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library.secday.local/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
192.168.228.100 - - [19/May/2023:07:51:06 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library.secday.local/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50"
```

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





SECURITY
EVERY DAY

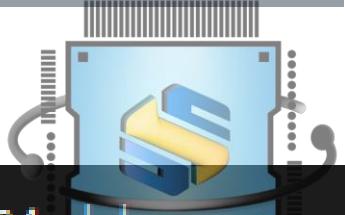
```
ubuntu@ubuntu:~$ wget -O splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.0.4/linux/splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb"
--2023-05-19 08:38:02-- https://download.splunk.com/products/universalforwarder/releases/9.0.4/linux/splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 13.225.244.115, 13.225.244.34, 13.225.244.5, ...
Connecting to download.splunk.com (download.splunk.com)|13.225.244.115|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32420798 (31M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb'

splunkforwarder-9.0.4-de405f4a7979-linux-2 100%[=====] 30.92M 19.5MB/s in 1.6s

2023-05-19 08:38:09 (19.5 MB/s) - 'splunkforwarder-9.0.4-de405f4a7979-linux-2.6-amd64.deb' saved [32420798/32420798]
```

INSTALAÇÃO SPLUNK UF - LIBRARY

- Para baixar e 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"

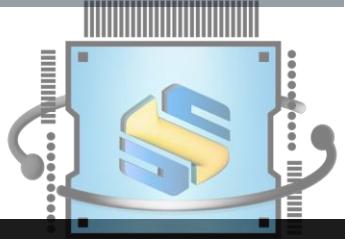


SECURITY
EVERY DAY

```
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`



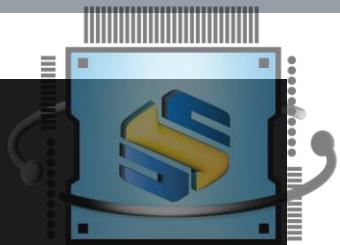
SECURITY
EVERY DAY

provided at no charge, and such 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



SECURITY
EVERY DAY

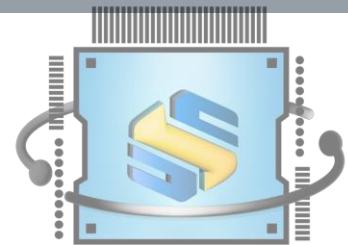
```
Please enter an administrator username: admin
Password must contain at least:
 * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunk
The unit file has been created.
```

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



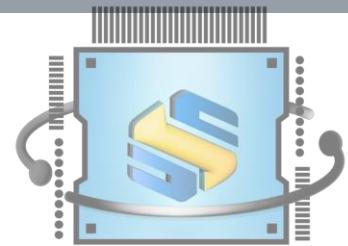
SECURITY
EVERY DAY

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

InterfaceAlias          IPv4Address
-----              -----
Ethernet 2             {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

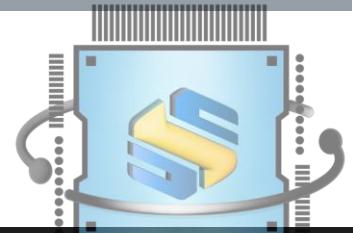


SECURITY
EVERY DAY

```
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



SECURITY
EVERY DAY

```
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`



New Search

```
index=main sourcetype="apache:access:combined"
```

✓ 4 events (5/18/23 1:00:00.000 PM to 5/19/23 1:25:25.000 PM) No Event Sampling ▾

Events (4) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ ✓ Format 20 Per Page ▾

Time	Event
5/19/23 1:15:04.000 PM	192.168.228.100 - - [19/May/2023:09:15:04 -0300] "-" 408 0 "-" "-" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/19/23 1:14:13:000 PM	192.168.228.100 - - [19/May/2023:09:14:13 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library/ome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/19/23 1:14:13:000 PM	192.168.228.100 - - [19/May/2023:09:14:13 -0300] "GET /static/favicon.ico HTTP/1.1" 304 279 "http://library/ome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/19/23 1:14:13:000 PM	192.168.228.100 - - [19/May/2023:09:14:13 -0300] "GET / HTTP/1.1" 200 828 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Edg/113.0.1774.50"

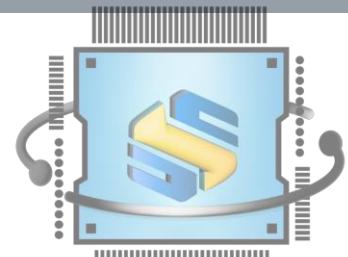
< Hide Fields | All Fields i

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 2
a date_month 1
date_second 2
a date_wday 1
date_year 1

COLETA - SPLUNK UF - LIBRARY

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



SECURITY
EVERY DAY

```
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`



New Search

```
index=main sourcetype="linux:audit"
```

✓ 4 events (5/18/23 1:00:00.000 PM to 5/19/23 1:40:29.000 PM) No Event Sampling ▾

Events (4) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

i	Time	Event
>	5/19/23 1:39:09.000 PM	May 19 09:39:08 ubuntu sudo: pam_unix(sudo:session): session closed for user root host = ubuntu source = /var/log/auth.log sourcetype = linux:audit
>	5/19/23 1:39:08.000 PM	May 19 09:39:08 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000) host = ubuntu source = /var/log/auth.log sourcetype = linux:audit
>	5/19/23 1:39:08.000 PM	May 19 09:39:08 ubuntu sudo: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/opt/splunkforwarder/bin/splunk host = ubuntu source = /var/log/auth.log sourcetype = linux:audit
>	5/19/23 1:39:08.000 PM	May 19 09:39:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root host = ubuntu source = /var/log/auth.log sourcetype = linux:audit

< Hide Fields ☰ All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

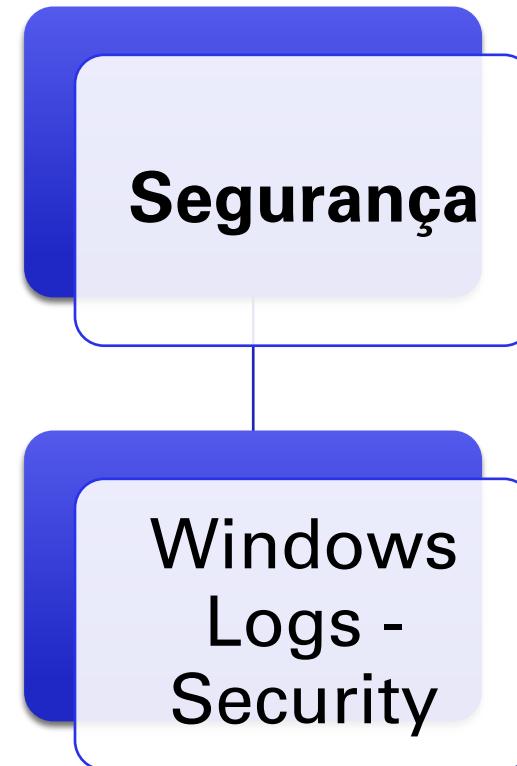
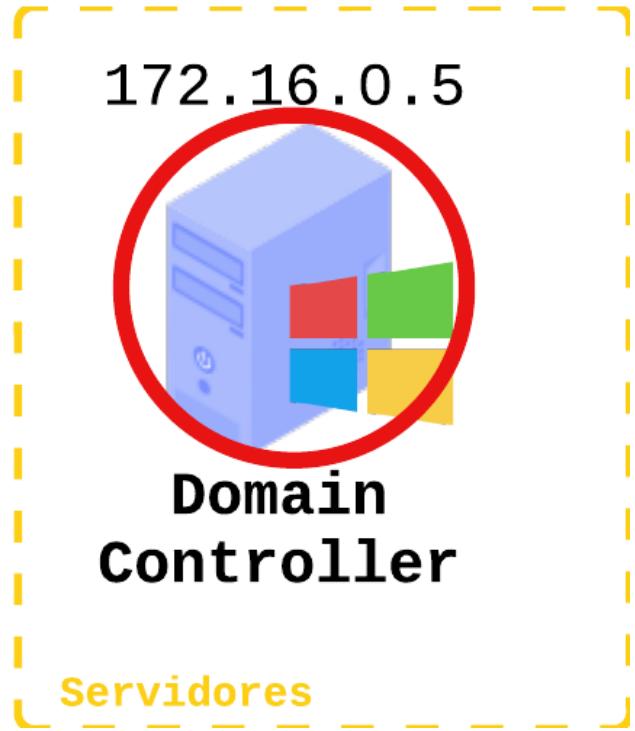
INTERESTING FIELDS
a COMMAND 1
a dest 1
a index 1
linecount 1
a punct 3

COLETA - SPLUNK UF - LIBRARY

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

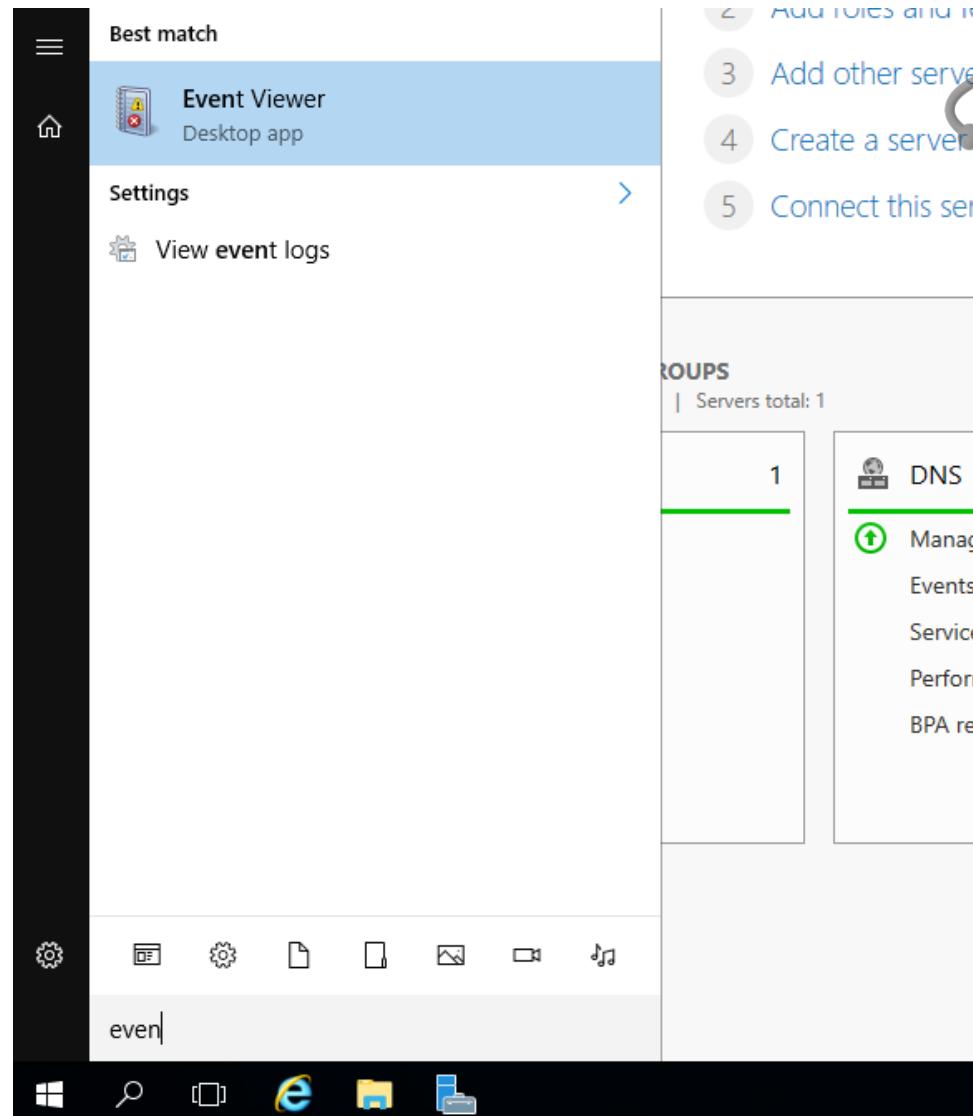


COLETA



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.

The image shows the Windows Event Viewer interface. The left pane displays a tree structure with 'Event Viewer (Local)', 'Custom Views', and 'Windows Logs' expanded, showing 'Application', 'Security', 'Setup', 'System', 'Forwarded Events', and 'Subscriptions'. The 'Security' node under 'Windows Logs' is selected. The right pane shows a table titled 'Security' with the message 'Number of events: 27,821 () New events available'. The table has columns for 'Keywords', 'Date and Time', 'Source', and 'Event ID / Task Category'. Below the table, a specific event is selected: 'Event 4634, Microsoft Windows security auditing.' The details pane shows the following information:
General tab:
Subject:
 Security ID: SYSTEM
 Account Name: AD-SECDAYS
 Account Domain: SECDAY
 Logon ID: 0x2C7904
Logon Type: 3
Details tab:
This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.





SECURITY
EVERY DAY

Administrator: Windows PowerShell

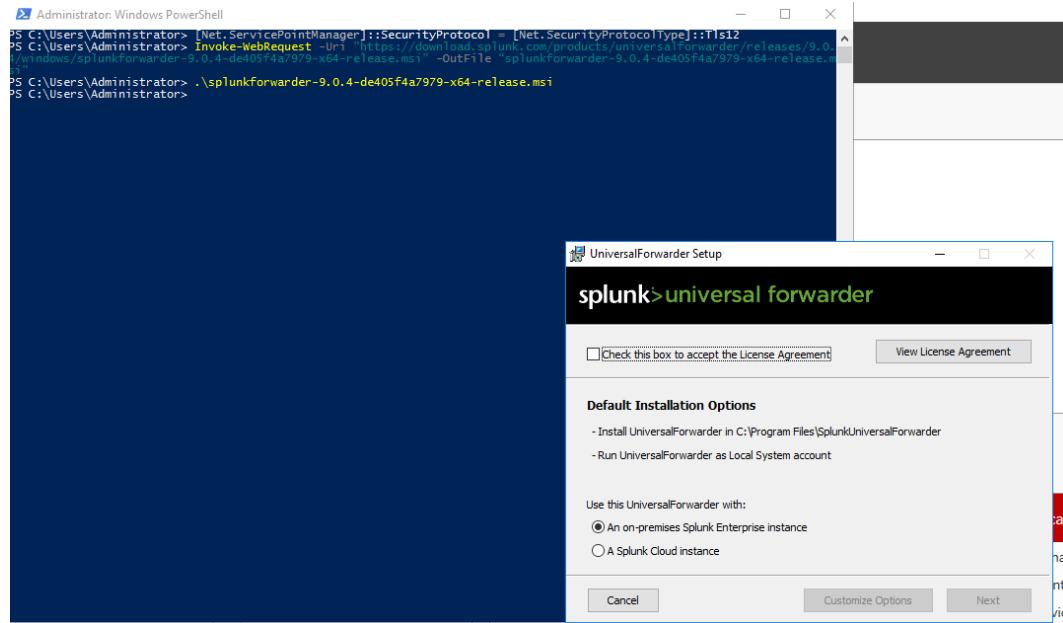
```
PS C:\Users\Administrator> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
PS C:\Users\Administrator> Invoke-WebRequest -Uri "https://download.splunk.com/products/universalforwarder/releases/9.0.4/windows/splunkforwarder-9.0.4-de405f4a7979-x64-release.msi" -OutFile "splunkforwarder-9.0.4-de405f4a7979-x64-release.msi"
Writing web request
Writing request stream... (Number of bytes written: 50886519)
```

INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

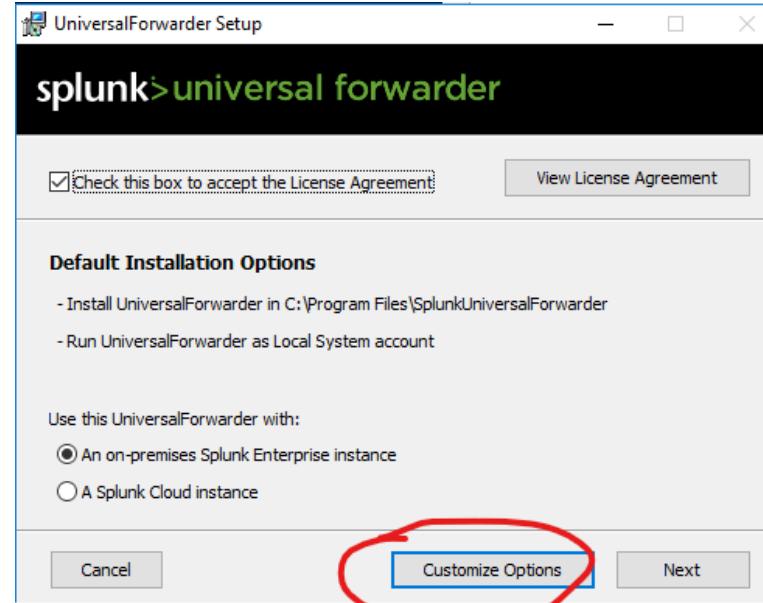
- Para baixar o instalar do Splunk UF, utilize os comando abaixo em sequencia via powershell:
 - [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
 - Invoke-WebRequest -Uri "https://download.splunk.com/products/universalforwarder/releases/9.0.4/windows/splunkforwarder-9.0.4-de405f4a7979-x64-release.msi"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



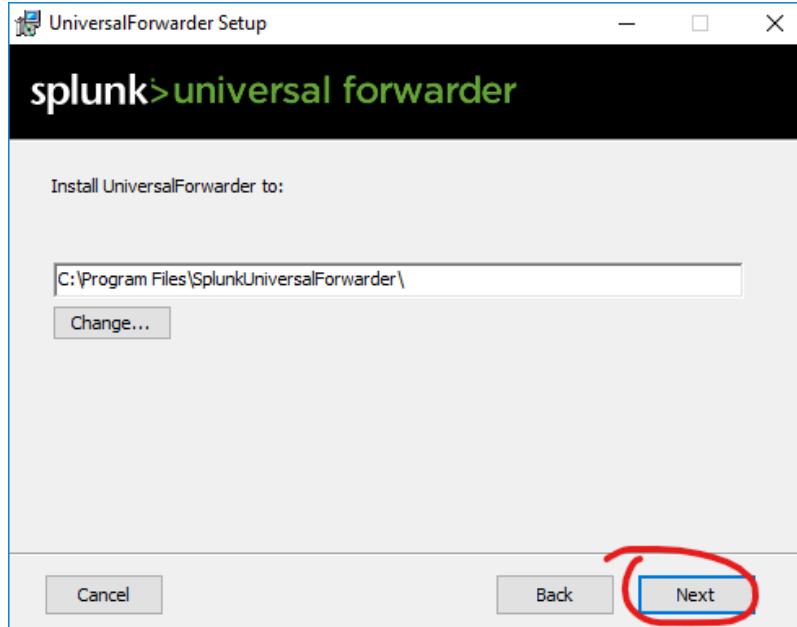
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER



- Aceite a licença e clique em “Customize Options”

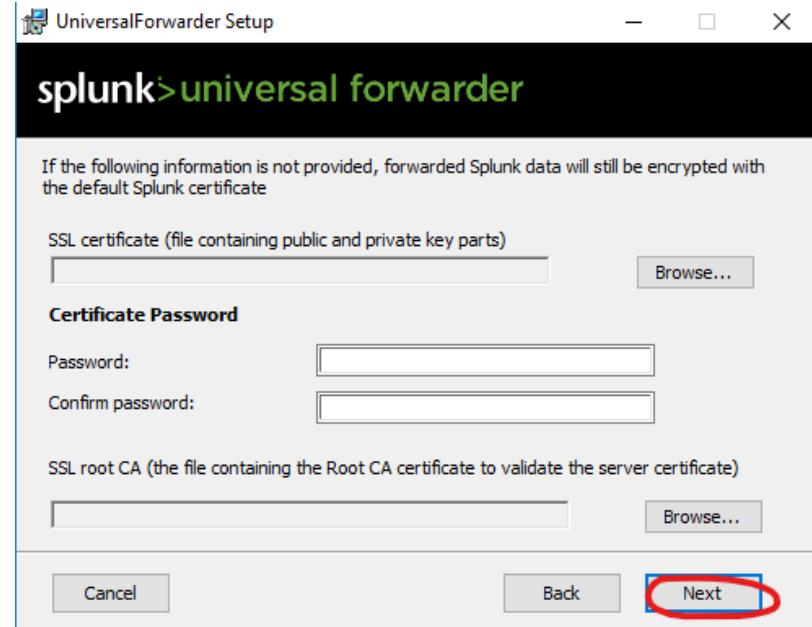


INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER



- Clique em “Next”

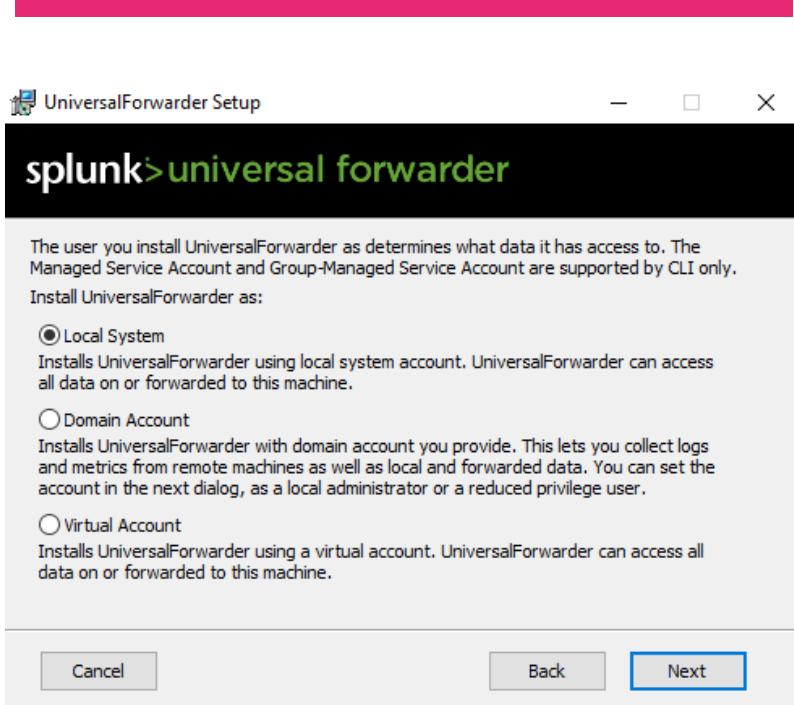




INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

- Clique em “Next”

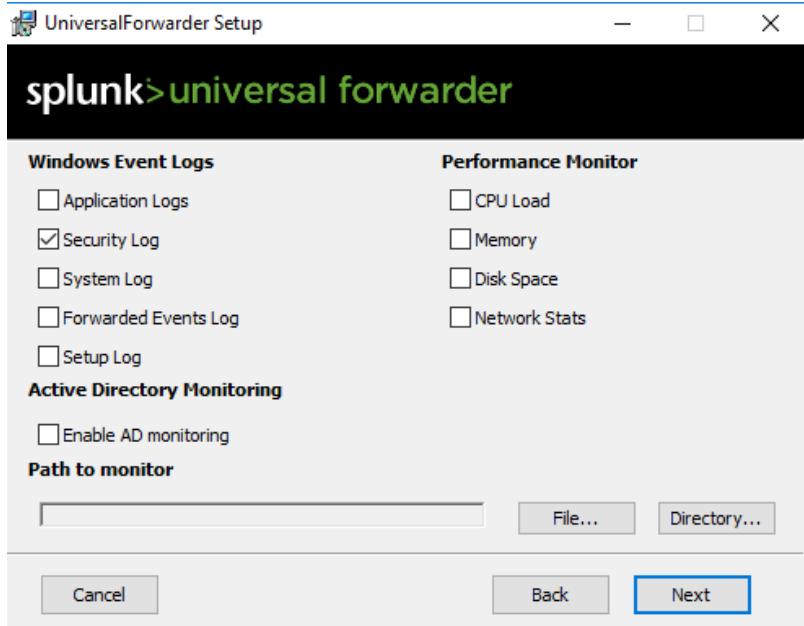
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER



- Clique em “Next”

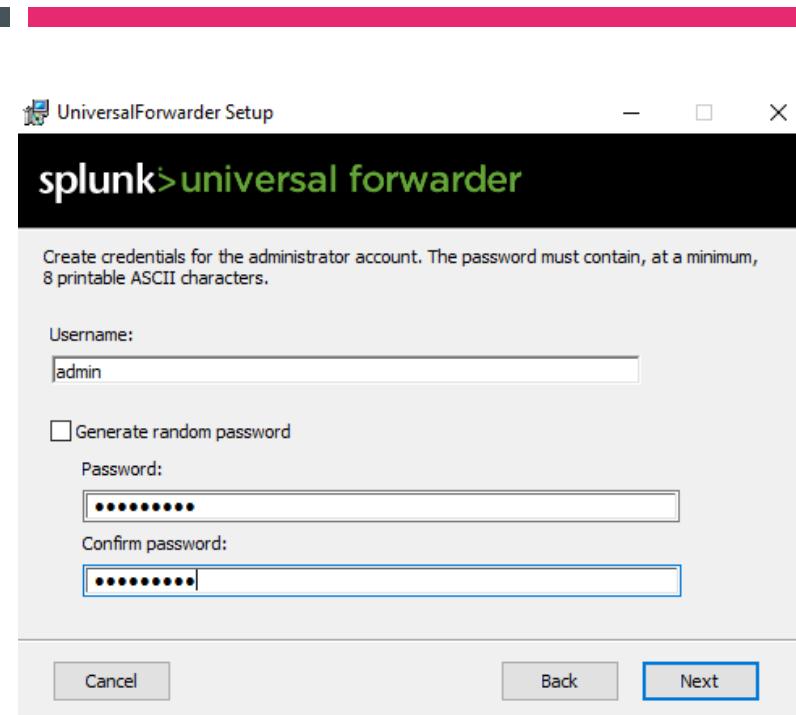


INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER



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

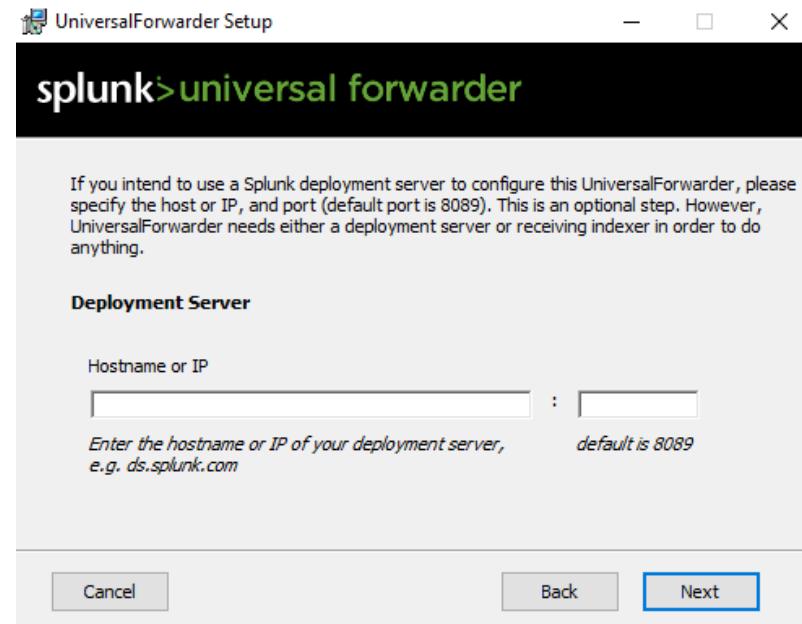




INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

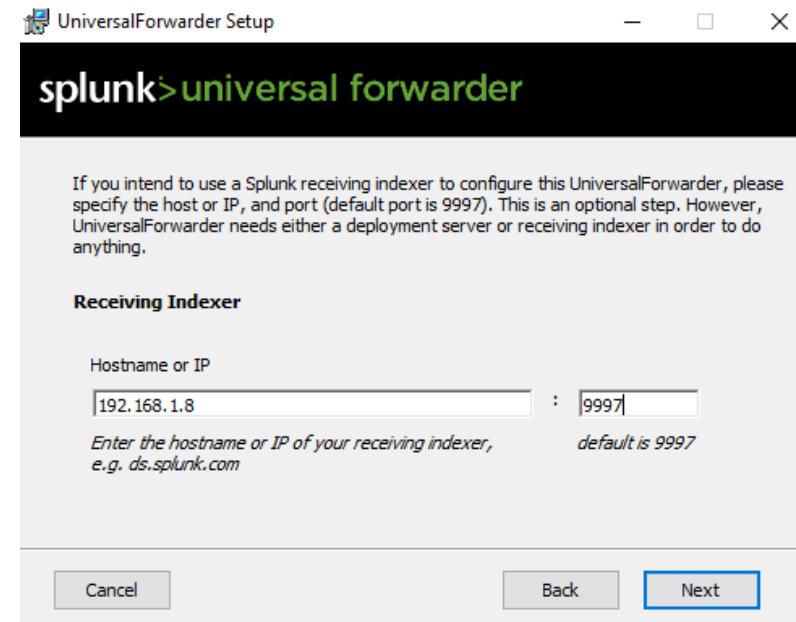
- Defina um nome de usuário e senha e clique em "Next"





INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

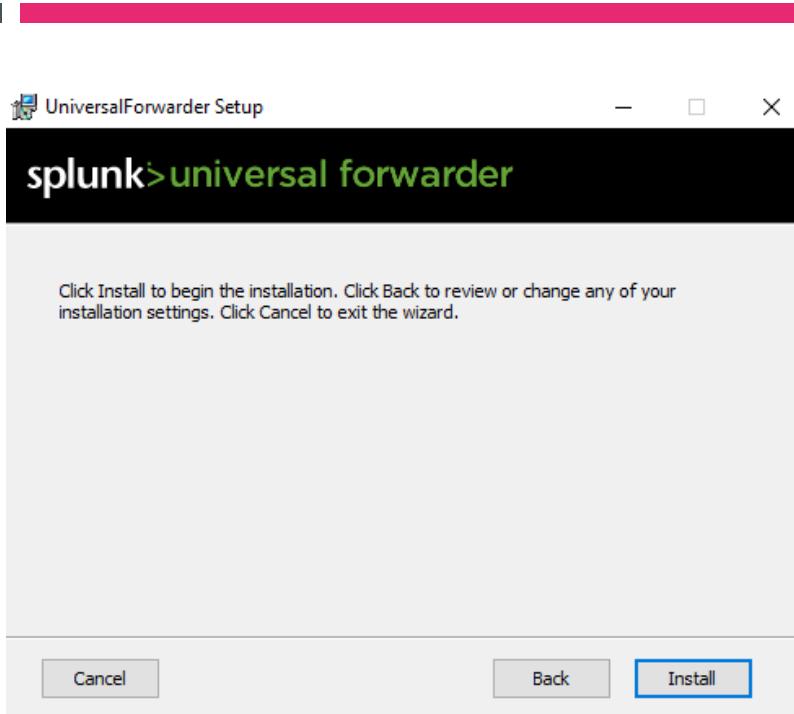
- Deixe em branco e clique em “Next”



INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER

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

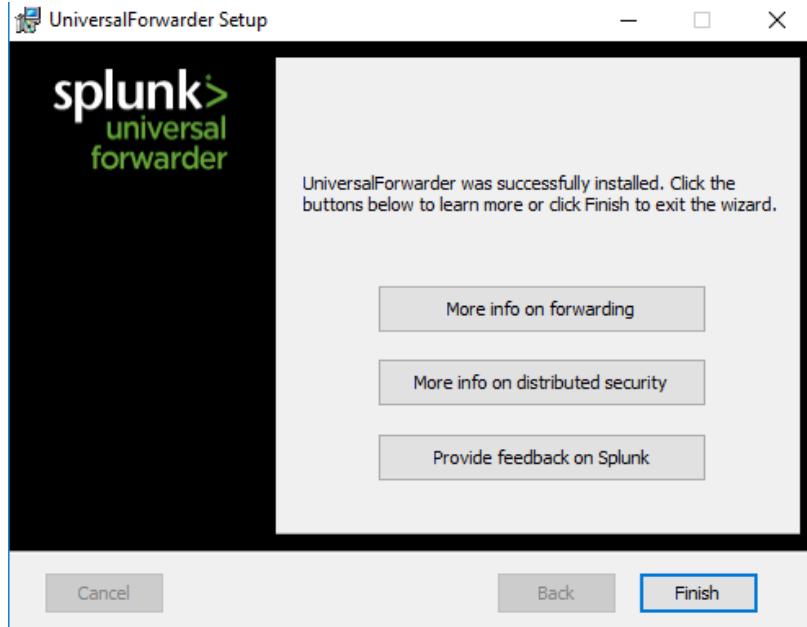
INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER



- Clique em “Install” e aguarde



INSTALAÇÃO SPLUNK UF – DOMAIN CONTROLLER



- Finalizada a instalação, clique em “Finish”





New Search

index=main host="AD-SECDAY"

✓ 14,315 events (before 5/19/23 6:50:18.000 PM) No Event Sampling ▾

Events (14,315) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

Time	Event
5/18/23 10:52:43.000 AM	05/18/2023 06:52:43 AM LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SECDAY, secday.local Show all 22 lines host = AD-SECDAY source = WinEventLog:Security sourcetype = WinEventLog:Security
5/18/23 10:52:43.000 AM	05/18/2023 06:52:43 AM LogName=Security EventCode=4624 EventType=0 ComputerName=AD-SECDAY, secday.local Show all 70 lines host = AD-SECDAY source = WinEventLog:Security sourcetype = WinEventLog:Security

< Hide Fields ≡ All Fields

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

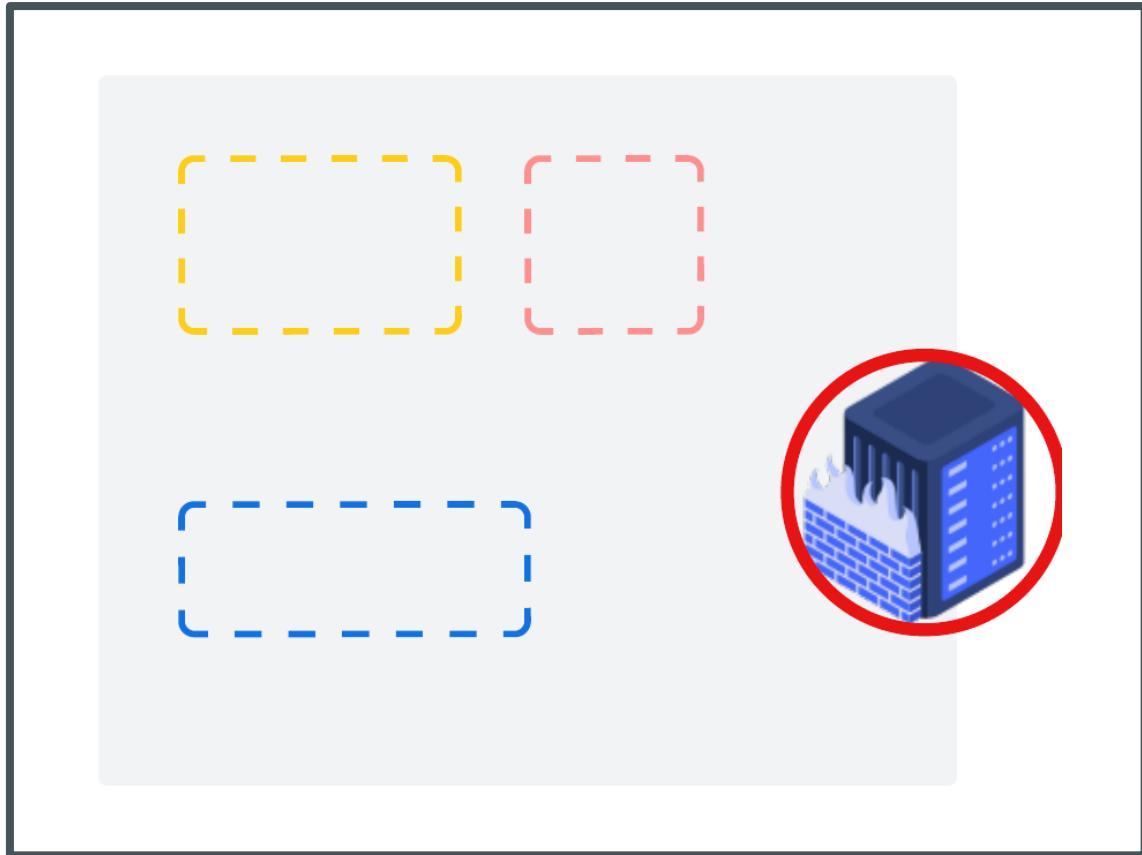
INTERESTING FIELDS

a Account_Domain 5
a Account_Name 15
a Authentication_Package 5
a ComputerName 1
a Elevated_Token 2
EventCode 25
EventType 2
a Impersonation_Level 3

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



Não seguro | <https://pfSense.secday.local/index.php>

pfSense

SIGN IN

admin

SIGN IN

- Acesse a interface web do pfSense e logue com o usuário
 - User: admin
 - Pass: secday



CONFIGURAÇÃO – LOGS FIREWALL

The screenshot shows the pfSense web interface with the 'Status' menu open. The 'System Logs' option is circled in red.

- Navegue até “Status → System Logs”

CONFIGURAÇÃO – LOGS FIREWALL



The screenshot shows a web-based configuration interface for a firewall. At the top, there is a navigation bar with tabs: System, Firewall, DHCP, Authentication, IPsec, PPP, PPPoE/L2TP Server, OpenVPN, NTP, Packages, and Settings. The 'Settings' tab is circled in red. Below the navigation bar, the page title is 'General Logging Options'. The configuration is divided into several sections:

- Log Message Format:** BSD (RFC 3164, default). A note says: "The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled). Changing this value will only affect new log messages."
- Forward/Reverse Display:** An unchecked checkbox for "Show log entries in reverse order (newest entries on top)".
- GUI Log Entries:** A text input field set to 500. A note says: "This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files."
- Log firewall default blocks:** A section with three checkboxes:
 - Log packets matched from the default block rules in the ruleset
 - Log packets that are blocked by the implicit default block rule. - Per-rule logging options are still respected.
 - Log packets matched from the default pass rules put in the rulesetA note says: "Log packets that are allowed by the implicit default pass rule. - Per-rule logging options are still respected."
- Web Server Log:** A section with a checked checkbox for "Log errors from the web server process". A note says: "If this is checked, errors from the web server process for the GUI or Captive Portal will appear in the main system log."
- Raw Logs:** A section with a checked checkbox for "Show raw filter logs". A note says: "If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information, but it is more difficult to read."
- Where to show rule descriptions:** A dropdown menu set to "Display as column". A note says: "Show the applied rule description below or in the firewall log rows. Displaying rule descriptions for all lines in the log might affect performance with large rule sets." A link "Ativar o Windows" and "Acesse Configurações para ativar" is visible.
- Local Logging:** An unchecked checkbox for "Disable writing log files to the local disk".

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

CONFIGURAÇÃO – LOGS FIREWALL



Log Configuration Changes Generate log entries when making changes to the configuration.

Reset Log Files

Clears all local log files and reinitializes them as empty logs. This also restarts the DHCP daemon. Use the Save button first if any setting changes have been made.

Log Rotation Options

Log Rotation Size (Bytes) This field controls the size at which logs will be rotated. By default this is 500 KiB per log file, and there are nearly 20 such log files. Rotated log files consume additional disk space, which varies depending on compression and retention count.

NOTE: Increasing this value allows every log file to grow to the specified size, so disk usage may increase significantly. Logs from packages may consume additional space which is not accounted for in these settings. Check package-specific settings. Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Disk space currently used by log files: 3.2M
Worst case disk usage for base system logs based on current global settings: 58.11 MiB
Remaining disk space for log files: 41G

Log Compression The type of compression to use when rotating log files. Compressing rotated log files saves disk space, but can incur a performance penalty. Compressed logs remain available for display and searching in the GUI.

Compression should be disabled when using large log files and/or slower hardware. Disabled by default on new ZFS installations as ZFS already performs compression.

WARNING: Changing this value will remove previously rotated compressed log files!

Log Retention Count The number of log files to keep before the oldest copy is removed on rotation.

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

CONFIGURAÇÃO – LOGS FIREWALL



Enable Remote Logging Send log messages to remote syslog server

Source Address

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; if an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers

Remote Syslog Contents Everything
 System Events
 Firewall Events
 DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
 DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
 PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
 General Authentication Events
 Captive Portal Events
 VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
 Gateway Monitor Events
 Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
 Network Time Protocol Events (NTP Daemon, NTP Client)
 Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Ativar o Window:
Acesse Configurações!

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



CONFIGURAÇÃO – LOGS FIREWALL

The screenshot shows the Splunk web interface. The top navigation bar includes links for Administrator, Messages, Settings, Activity, Help, and a search bar labeled 'Find'. On the left, there's a sidebar with icons for 'Add Data' (two servers) and 'Monitoring Console' (a gauge). The main content area is divided into sections: 'KNOWLEDGE' (Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations), 'DATA' (Data inputs, Forwarding and receiving, Indexes, Report acceleration summaries, Source types, Ingest actions), and 'DISTRIBUTED ENVIRONMENT' (Indexer clustering, Forwarder management, Federated search). The 'Data inputs' link under the DATA section is highlighted with a red oval.

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

CONFIGURAÇÃO – LOGS FIREWALL



Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Registry monitoring Have Splunk index the local Windows Registry, and monitor it for changes.	0	+ Add new
Active Directory monitoring Index and monitor Active Directory.	0	+ Add new

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



CONFIGURAÇÃO – LOGS FIREWALL

Screenshot of the Splunk interface for configuring a new log source. The steps are: Select Source, Input Settings, Review, Done. The 'Input Settings' step is shown.

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

or

TCP UDP

Port ? **12514** Example: 514

Source name override ? optional host:port

Only accept connection from ? optional example: 10.1.2.3, lbadhost.splunk.com, *.splunk.com

FAQ

- > How should I configure the Splunk platform for syslog traffic?
- > What's the difference between receiving data over TCP versus UDP?
- > Can I collect syslog data from Windows systems?

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



CONFIGURAÇÃO – LOGS FIREWALL

The screenshot shows the 'Input Settings' step of the 'Add Data' wizard. The top navigation bar includes 'Add Data', 'Select Source', 'Input Settings', 'Review', and 'Done'. A red circle highlights the 'Review' button. The main area contains sections for 'Source type', 'App context', 'Host', and 'Index'. In the 'Source type' section, a red circle highlights the 'Source Type' input field containing 'pfSense'. In the 'Host' section, a red circle highlights the 'Method' dropdown menu with 'IP' selected. The 'Index' section shows 'Default' selected.

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

CONFIGURAÇÃO – LOGS FIREWALL



Add Data

Select Source Input Settings Review Done

Submit < Back

Review

Input Type	UDP Port
Port Number	12514
Source name override	N/A
Restrict to Host	N/A
Source Type	pfSense
App Context	launcher
Host	(IP address of the remote server)
Index	default

- Tudo certo! Clique em “Submit”

CONFIGURAÇÃO – LOGS FIREWALL



✓ UDP input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Start Searching Search your data now or see examples and tutorials. [\[link\]](#)

Extract Fields Create search-time field extractions. Learn more about fields. [\[link\]](#)

Add More Data Add more data inputs now or see examples and tutorials. [\[link\]](#)

Download Apps Apps help you do more with your data. Learn more. [\[link\]](#)

Build Dashboards Visualize your searches. Learn more. [\[link\]](#)

- Clique em “Start Searching”

CONFIGURAÇÃO – LOGS FIREWALL



The screenshot shows a Splunk search results page. At the top, there is a search bar with the query "source=udp:12514 sourcetype=pfsense". Below the search bar, it says "766 events (before 5/19/23 7:16:54.000 PM) No Event Sampling". The main area displays a histogram and a table of log entries. The table has columns for "Time" and "Event". One visible event entry is:

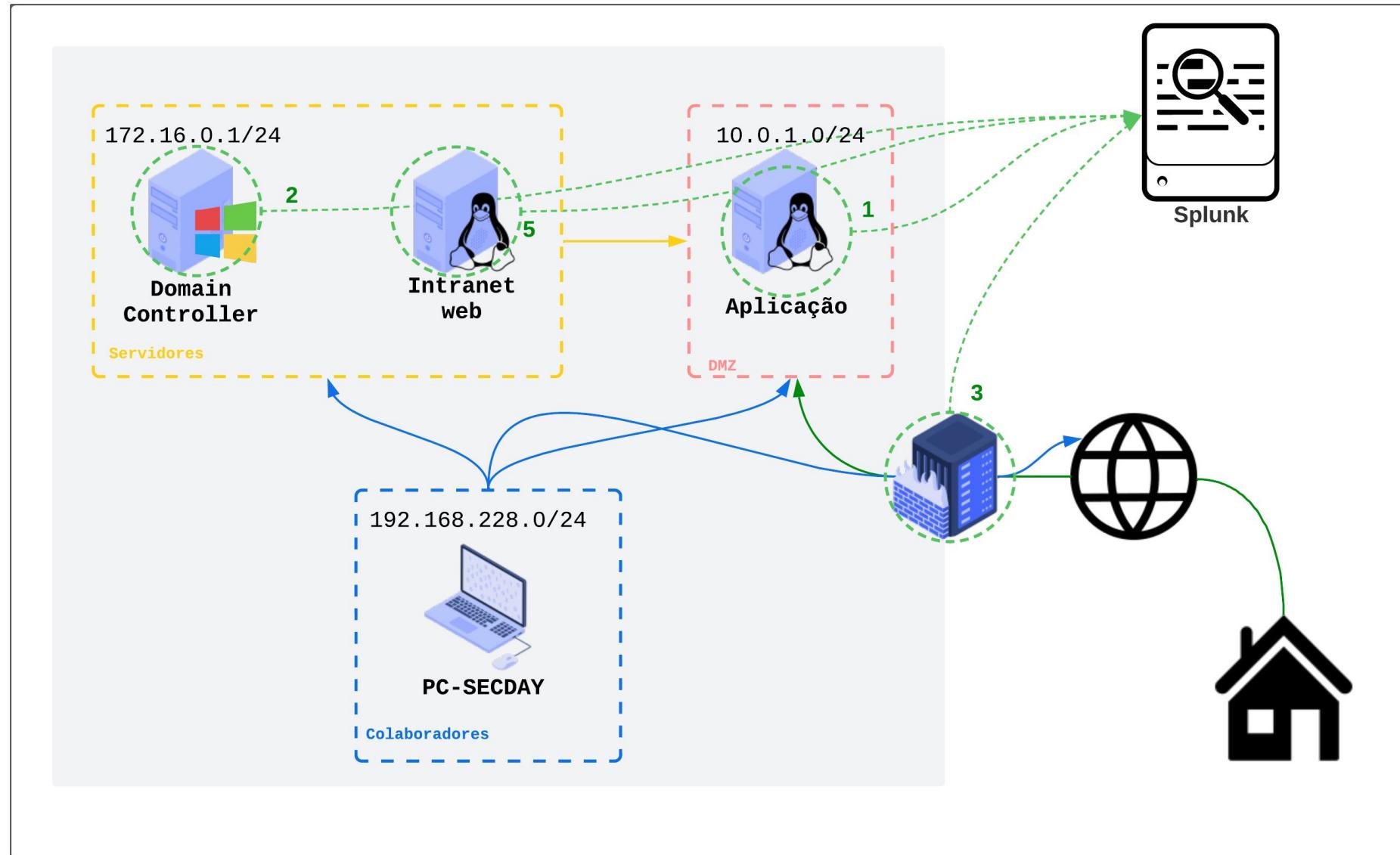
Time	Event
5/19/23 7:16:53.000 PM	{ [-] dest_ip: 142.250.218.195 dest_port: 443 event_type: tls flow_id: 1930423468180273 in_iface: em0 proto: TCP src_ip: 192.168.126.139 src_port: 51673 timestamp: 2023-05-19T15:16:54.934761-0300 tls: { [+] } }

On the left side, there are sections for "SELECTED FIELDS" (host, source, sourcetype) and "INTERESTING FIELDS" (date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year).

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



■ Desenho atual da rede



ESTRATÉGIAS DE MONITORAMENTO

Identificação das Joias da Coreia

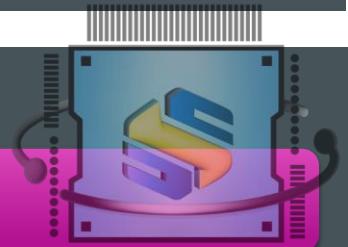
Instalação do SIEM

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



SECURITY
EVERY DAY



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.

index=main sourcetype="apache:access:combined"

✓ 11 events (before 5/24/23 10:49:31.000 AM) No Event Sampling ▾

Events (11) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

Time	Event
5/22/23 12:46:26.000 PM	192.168.228.100 - [22/May/2023:08:46:26 -0300] "GET /static/favicon.ico HTTP/1.1" 30 Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/22/23 12:46:26.000 PM	192.168.228.100 - [22/May/2023:08:46:26 -0300] "GET /static/favicon.ico HTTP/1.1" 30 Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/22/23 12:46:26.000 PM	192.168.228.100 - [22/May/2023:08:46:26 -0300] "GET / HTTP/1.1" 200 827 "-" "Mozilla/5.0" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/22/23 12:46:26.000 PM	192.168.228.100 - [22/May/2023:08:46:26 -0300] "GET /static/favicon.ico HTTP/1.1" 30 Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/22/23 12:46:26.000 PM	192.168.228.100 - [22/May/2023:08:46:26 -0300] "GET /static/favicon.ico HTTP/1.1" 30 Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/22/23 12:46:26.000 PM	192.168.228.100 - [22/May/2023:08:46:26 -0300] "GET / HTTP/1.1" 200 828 "-" "Mozilla/5.0" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined
5/22/23 12:46:26.000 PM	192.168.228.100 - [22/May/2023:08:46:26 -0300] "GET /static/favicon.ico HTTP/1.1" 30 Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50" host = ubuntu source = /var/log/apache2/access.log sourcetype = apache:access:combined

◀ Hide Fields ⌂ All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

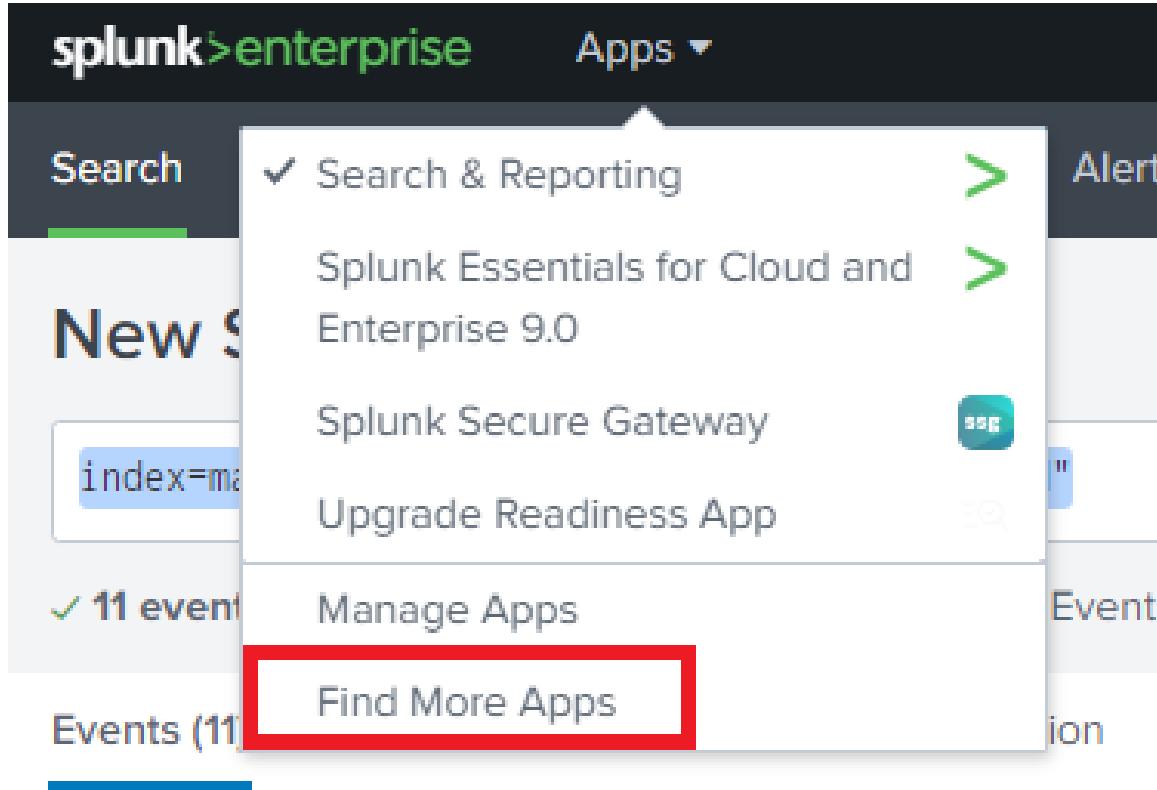
- # date_hour 1
- # date_mday 1
- # date_minute 2
- a date_month 1
- # date_second 3
- a date_wday 1
- # date_year 1
- # date_zone 1
- a index 1
- # linecount 1
- a punct 2
- a splunk_server 1
- # timeendpos 1
- # timestamppos 1

+ Extract New Fields



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”



Browse More Apps

apache X

Best Match Newest Popular

14 Apps

Splunk Add-on for Apache Web Server Install

The Splunk Add-on for Apache Web Server allows a Splunk software administrator to collect and analyze data from Apache Web Server using file monitoring. After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on.

This add-on provides the inputs and CIM-compatible knowledge to use with... [More](#)

Category: IT Operations | Author: Splunk Inc. | Downloads: 24589 | Released: a year ago | Last Updated: 6 months ago | [View on Splunkbase](#)

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>

Login and Install

Enter your Splunk.com username and password to download the app.

Username

Password

[Forgot your password?](#)

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app and does not provide any warranty or support. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

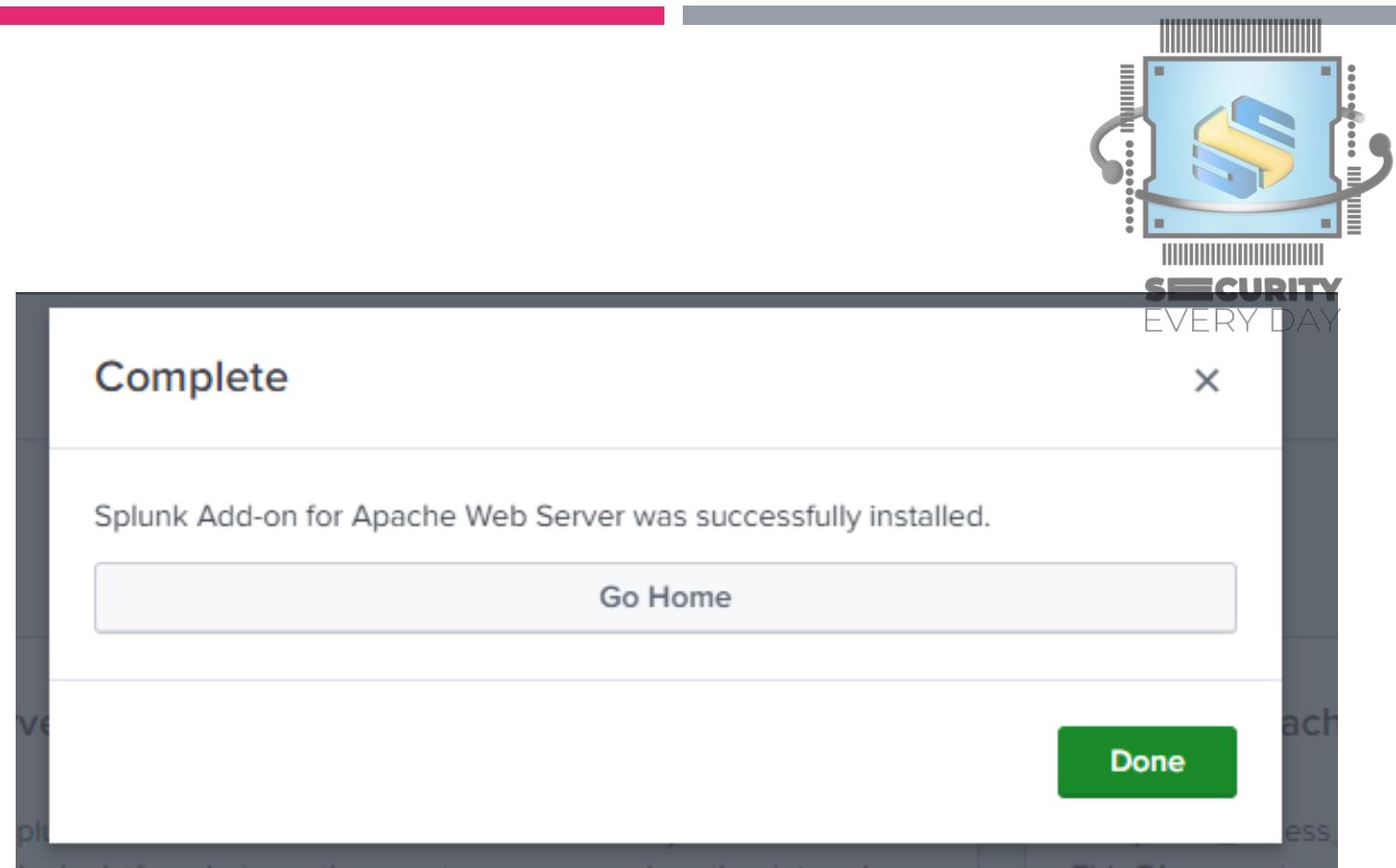
Splunk Add-on for Apache Web Server is governed by the following license:
[Splunk Software License Agreement](#)

I have read the terms and conditions of the license(s) and agree to be bound by them. I also agree to Splunk's [Website Terms of Use](#).



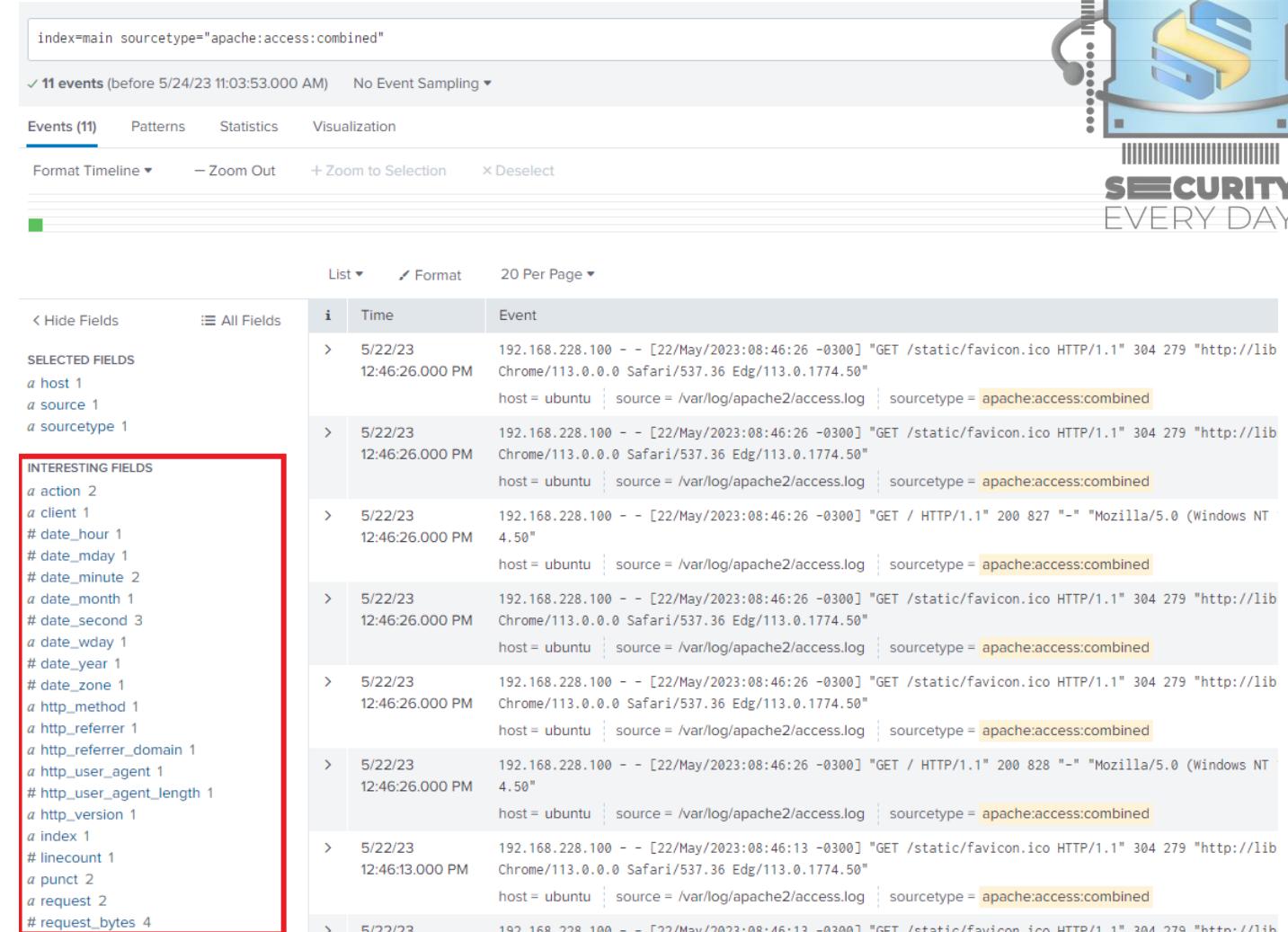
CONFIGURAR OS PARSINGS - APACHE

- 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.



The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index=main sourcetype="apache:access:combined"
- Results Summary:** ✓ 11 events (before 5/24/23 11:03:53.000 AM) No Event Sampling ▾
- Event List:** Events (11) Patterns Statistics Visualization
- Event Details:** Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect
- Event Headers:** List ▾ Format 20 Per Page ▾
- Selected Fields:** < Hide Fields i All Fields host source sourcetype
- Interesting Fields (highlighted by a red box):** action client date_hour date_mday date_minute date_month date_second date_wday date_year date_zone http_method http_referrer http_referrer_domain http_user_agent http_user_agent_length http_version index linecount punct request request_bytes
- Event Data:** The list displays 11 events from May 22, 2023, at 12:46:26.000 PM, showing log entries for Apache access requests from host 192.168.228.100 to /static/favicon.ico, with various browser and OS details.



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.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index=* sourcetype="linux:audit"
- Event Count:** 35 events (5/23/23 11:00:00.000 AM to 5/24/23 11:09:36.000 AM) | No Event Sampling
- Panel Tabs:** Events (35) (selected), Patterns, Statistics, Visualization
- Panel Buttons:** Format Timeline ▾, - Zoom Out, + Zoom to Selection, × Deselect
- Table Headers:** List ▾, Format, 20 Per Page ▾
- Selected Fields:** host 1, source 1, sourcetype 1
- Interesting Fields:** date_hour 13, date_mday 2, date_minute 4, date_month 1, date_second 2, date_wday 2, date_year 1, date_zone 1, index 1, linecount 1, punct 7, splunk_server 1, timeendpos 1, timestampstartpos 1, uid 1 (highlighted with a red box)
- Table Data:** A list of 35 events from May 24, 2023, at 06:25:01 to 04:17:01. Each event is a log entry from an Ubuntu CRON process (pam_unix) regarding session openings and closings. The host is ubuntu, the source is /var/log/auth.log, and the sourcetype is linux:audit.

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>.*)`

The screenshot shows the regex101.com website interface. On the left, there's a sidebar with options like 'SAVE & SHARE', 'FLAVOR' (set to PCRE2 (PHP >= 7.3)), 'FUNCTION' (set to Match), and 'TOOLS'. The main area has a 'REGULAR EXPRESSION' input field containing the regex pattern: `^(?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>.*)`. Below it is a 'TEST STRING' input field containing the log entry: `May 24 09:17:01 ubuntu CRON[3942]: pam_unix(cron:session): session closed for user root`. To the right, the 'EXPLANATION' section provides a detailed breakdown of the regex components. The 'MATCH INFORMATION' section shows the captured groups: Match 1 (0-87), Group datetime (0-15), Group hostname (16-22), Group service (23-33), and Group message (35-87). The 'QUICK REFERENCE' sidebar on the far right lists various regex symbols and their meanings.

CONFIGURAR OS PARSINGS - LINUX

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

New Search

index=* sourcetype="linux:audit"

✓ 53 events (5/23/23 1:00:00.000 PM to 5/24/23 1:52:56.000 PM) No Event Sampling ▾

Events (53) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ ✓ Format 20 Per Page ▾

Time	Event
> 5/24/23 1:17:01.000 PM	May 24 09:17:01 ubuntu CRON[3942]: pam_unix(cron:session): session opened for user root by (uid=0)
> 5/24/23 1:17:01.000 PM	May 24 09:17:01 ubuntu CRON[3942]: pam_unix(cron:session): session closed for user root
> 5/24/23 1:07:27.000 PM	May 24 09:07:27 ubuntu sshd[3936]: fatal: Timeout before authentication for user root from 127.0.0.1 port 53529 ssh2
> 5/24/23 1:05:33.000 PM	May 24 09:05:33 ubuntu sshd[3936]: Failed password for user root from 127.0.0.1 port 53529 ssh2
> 5/24/23 1:05:31.000 PM	May 24 09:05:31 ubuntu sshd[3936]: pam_unix(sshd:auth): authentication failure; logname=uid=0 name=root atty=pts/0 file=/var/run/sshd.pid method=pam_unix
> 5/24/23 12:17:01.000 PM	May 24 08:17:01 ubuntu CRON[3913]: pam_unix(cron:session): session opened for user root by (uid=0)
> 5/24/23 12:17:01.000 PM	May 24 08:17:01 ubuntu CRON[3913]: pam_unix(cron:session): session closed for user root
> 5/24/23 11:17:01.000 AM	May 24 07:17:01 ubuntu CRON[3429]: pam_unix(cron:session): session opened for user root by (uid=0)
> 5/24/23 11:17:01.000 AM	May 24 07:17:01 ubuntu CRON[3429]: pam_unix(cron:session): session closed for user root
> 5/24/23 11:17:14.550 AM	May 24 07:17:14.550 ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)

◀ Hide Fields : All Fields i

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # date_hour 15
- # date_mday 2
- # date_minute 7
- a date_month 1
- # date_second 7
- a date_wday 2
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 14
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1
- # uid 2

9 more fields

+ 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.

Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [Learn more ↗](#)

I prefer to write the regular expression myself >

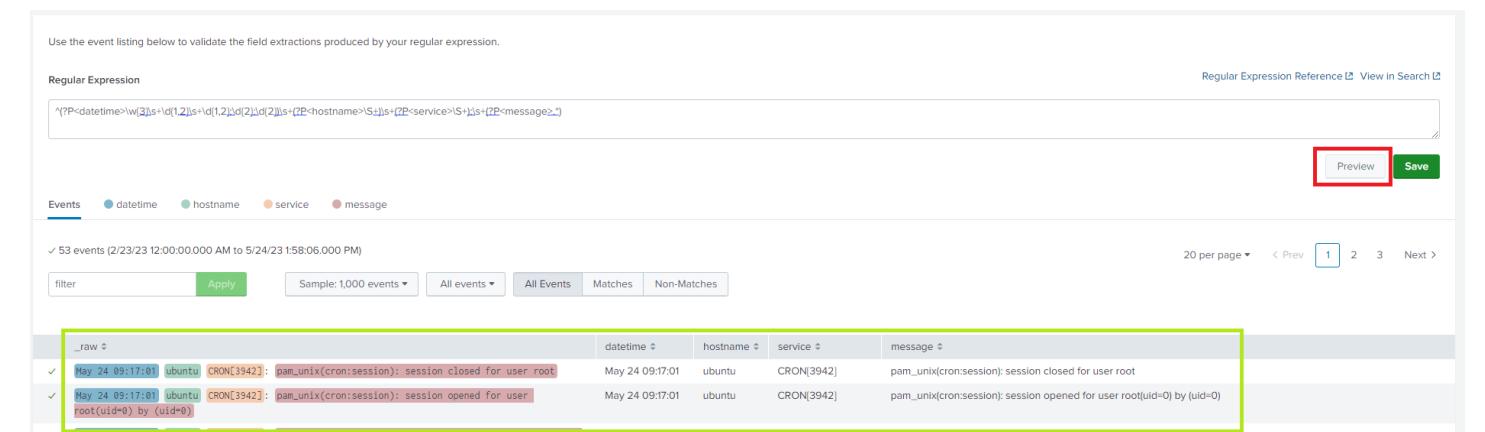
Source type
`linux:audit`

Time Range
`Last 90 days ▾`



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"



The screenshot shows a log parsing interface. At the top, there is a red bar. On the right side, there is a logo for "SECURITY EVERY DAY" featuring a stylized "S" and "E" inside a blue shield-like shape with a barcode pattern.

The main area contains the following elements:

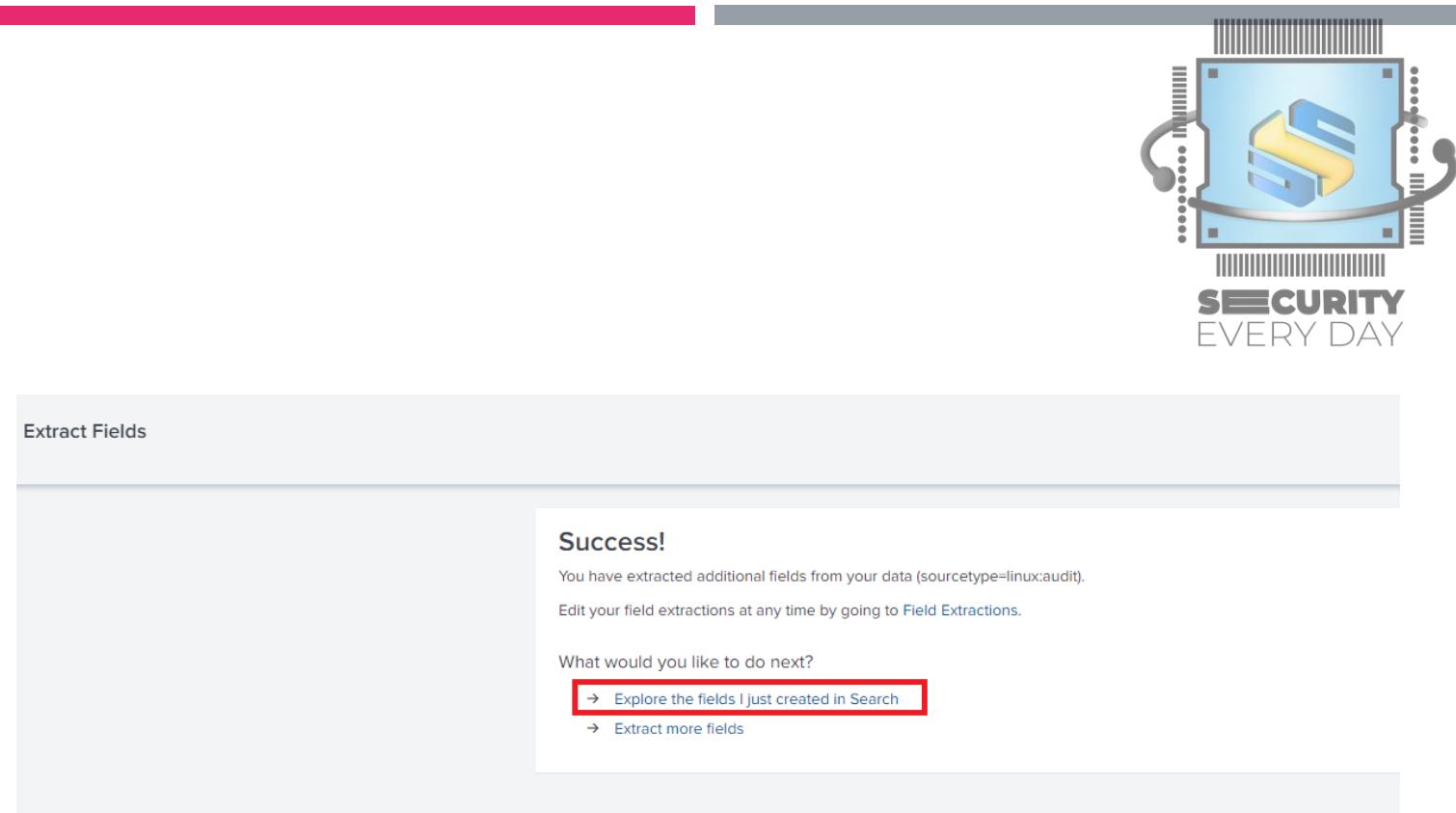
- Regular Expression:** A text input field containing the regular expression: `^(\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}) (\w{3}) (\d{1,2}.\d{1,2}.\d{1,2}.\d{1,2}) (\d{1,2}:\d{1,2}:\d{1,2}:\d{1,2}) (\w{3}.\w{3}.\w{3}.\w{3}) (\w{3}.\w{3}.\w{3}.\w{3}) (\w{3}.\w{3}.\w{3}.\w{3}) (\w{3}.\w{3}.\w{3}.\w{3})`.
- Events:** A section showing a preview of 53 events from May 24, 2023, at 09:17:01. The events are listed in a table with columns: raw, datetime, hostname, service, and message.
- Buttons:** A "Preview" button (highlighted with a red box) and a "Save" button.
- Toolbar:** Includes buttons for filter, Apply, Sample: 1,000 events, All events, All Events, Matches, Non-Matches, and a page navigation section (20 per page, 1, 2, 3, Next).

The "message" column for the first two events is highlighted with a green box:

raw	datetime	hostname	service	message
May 24 09:17:01 ubuntu CRON[3942]: pam_unix(cron:session): session closed for user root	May 24 09:17:01	ubuntu	CRON[3942]	pam_unix(cron:session): session closed for user root
May 24 09:17:01 ubuntu CRON[3942]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)	May 24 09:17:01	ubuntu	CRON[3942]	pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)

CONFIGURAR OS PARSINGS - LINUX

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



The screenshot shows a user interface for extracting fields from data. At the top, there's a header bar with a red bar on the left and a grey bar on the right. On the right side of the grey bar is a logo featuring a blue shield with a yellow 'S' and the text 'SECURITY EVERY DAY'. Below the header, the main content area has a light grey background. On the left, there's a section titled 'Extract Fields'. On the right, a white box contains a 'Success!' message with the following text:

Success!
You have extracted additional fields from your data (sourcetype=linux:audit).
Edit your field extractions at any time by going to [Field Extractions](#).

What would you like to do next?

→ [Explore the fields I just created in Search](#) (This link is highlighted with a red box.)
→ [Extract more fields](#)

CONFIGURAR OS PARSINGS - LINUX

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

The screenshot shows the Splunk interface with the following details:

- Selected Fields:** a host 1, a source 1, a sourcetype 1.
- Interesting Fields:** # date_hour 15, # date_mday 2, # date_minute 7, a date_month 1, # date_second 7, a date_wday 2, # date_year 1, a date_zone 1, a datetime 24, a hostname 1, a index 1, # linecount 1, a message 18, a punct 14, a service 25, a splunk_server 1, # timeendpos 1, # timestamppos 1, # uid 2, 9 more fields, + Extract New Fields.
- Log Entries:** Two entries are shown:
 - > 5/24/23 May 24 09:17:01 ubuntu CRON[3942]: pam_unix(cron:session): session closed for user root
 - > 5/24/23 May 24 09:17:01 ubuntu CRON[3942]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
- Message Panel:** Shows 18 Values, 100% of events. A red box highlights the "Selected" checkbox.
- Reports:** Top values, Top values by time, Rare values.
- Top 10 Values:** A table showing the most frequent log entries and their percentages:

Value	Count	%
pam_unix(cron:session): session closed for user root	18	33.962%
pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)	18	33.962%
pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by (uid=0)	2	3.774%
Accepted password for ubuntu from 192.168.228.100 port 60706 ssh2	1	1.887%
Accepted password for ubuntu from 192.168.228.100 port 60717 ssh2	1	1.887%
Failed password for ubuntu from 192.168.228.100 port 64012 ssh2	1	1.887%
New seat seat0.	1	1.887%
New session 16 of user ubuntu.	1	1.887%
New session 18 of user ubuntu.	1	1.887%
Server listening on 0.0.0.0 port 22.	1	1.887%
- Security Banner:** SECURITY EVERY DAY

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.

The screenshot shows the Splunk "New Search" interface. The search query is "index= host='AD-SECDAY'". The results show 10,735 events from May 24, 2023, between 10:06:37 AM and 2:06:37:000 PM. The "Events (10,735)" tab is selected. The interface includes filters for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". Below the search bar, there are buttons for "List", "Format", and "20 Per Page". The results table has columns for "Time" and "Event". The "SELECTED FIELDS" section on the left lists "host", "source", and "sourcetype". The "INTERESTING FIELDS" section, which is highlighted with a red box, lists various fields such as "Account_Domain", "Account_Name", "Authentication_Package", "ComputerName", "Elevated_Token", "EventCode", "EventType", "Impersonation_Level", "index", "Key_Length", "Keywords", "linecount", "Linked_Logon_ID", "LogName", and "Logon_GUID". The results table shows three event entries, each with detailed log information including LogName, EventCode, EventType, ComputerName, and a link to "Show all 22 lines".

Time	Event
5/24/23 2:06:37:000 PM	05/24/2023 10:06:37 AM LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SECDAY.secday.local Show all 22 lines host = AD-SECDAY source = WinEventLog:Security sourcetype = WinEventLog
5/24/23 2:06:37:000 PM	05/24/2023 10:06:37 AM LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SECDAY.secday.local Show all 22 lines host = AD-SECDAY source = WinEventLog:Security sourcetype = WinEventLog
5/24/23 2:06:37:000 PM	05/24/2023 10:06:37 AM LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SECDAY.secday.local Show all 22 lines host = AD-SECDAY source = WinEventLog:Security sourcetype = WinEventLog

CONFIGURAR OS PARSINGS - WINDOWS

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



AddOn+ **Splunk Add-on for Microsoft Windows** **Install**

*** Important: Read upgrade instructions and test add-on update before deploying to production ***
The Splunk Add-on for Windows 5.0.0 introduced breaking changes. If you are upgrading from a version of the Splunk Add-on for Windows that is earlier than 5.0.0, you must follow the documented upgrade instructions to avoid data loss.
[A best practice](#) [... More](#)

Category: IT Operations, Security, Fraud & Compliance | Author: Splunk Inc. | Downloads: 418488 | Released: a month ago | Last Updated: a month ago | [View on Splunkbase](#)

CONFIGURAR OS PARSINGS - WINDOWS

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

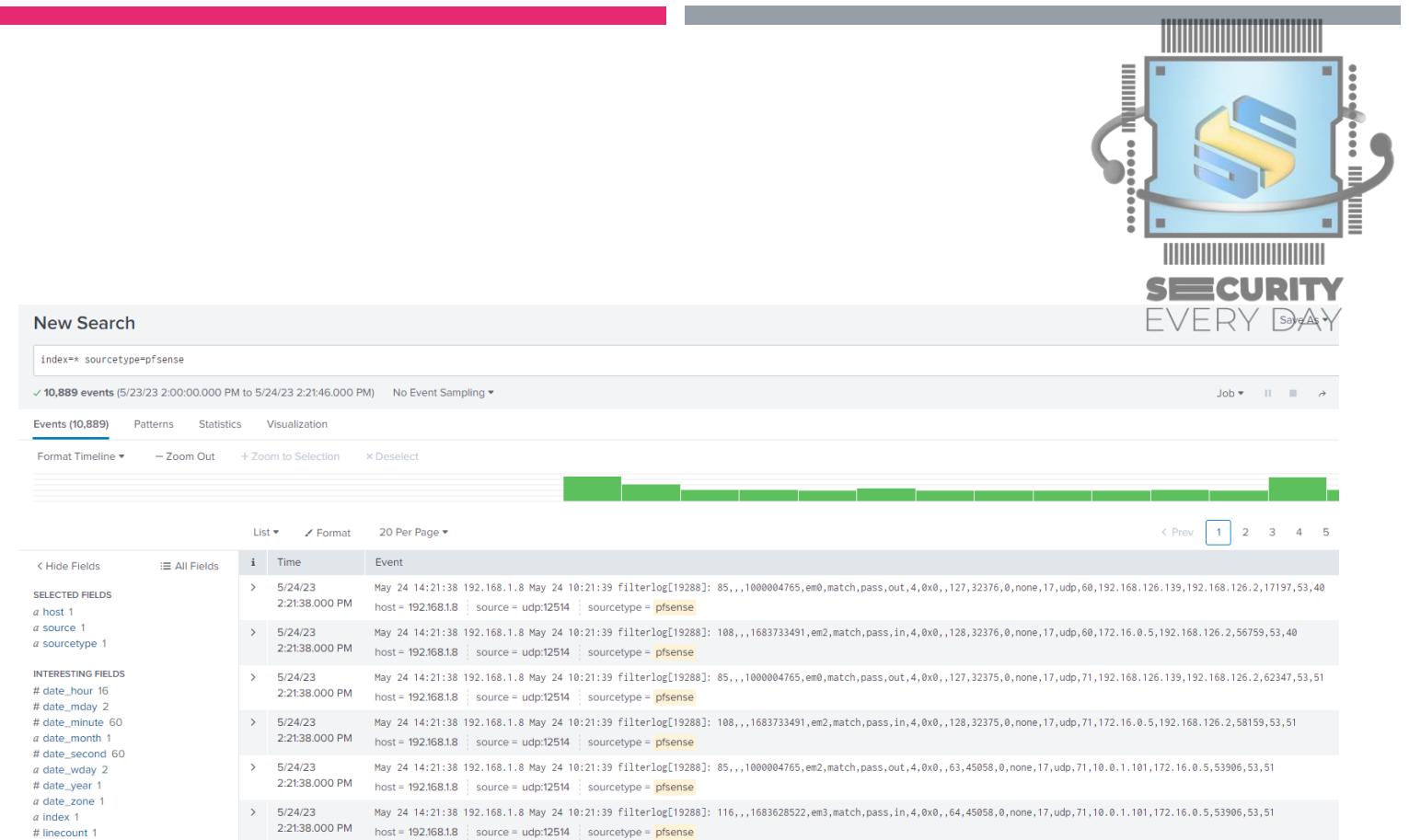
```
a Logon_ID 100+
a Logon_Process 5
# Logon_Type 4
a member_dn 26
a member_id 23
a Message 100+
a name 20
a Network_Account_Domain 1
a Network_Account_Name 1
a object 5
a objectAttrs 3
a objectCategory 3
a object_id 6
a OpCode 1
a Package_Name__NTLM_only_ 2
a privilege 12
a privilege_id 13
a Privileges 3
a process 12
a Process_ID 13
a process_id 17
a process_name 15
a Process_Name 8
a product 1
a punct 24
# RecordNumber 100+
a Restricted_Admin_Mode 1
a result 2
a Security_ID 12
a session_id 100+
a severity 1
# severity_id 2
a signature 20
# signature_id 21
a Source_Network_Address 7
# Source_Port 100+
a SourceName 2
a splunk_server 1
a src 8
a src_ip 7
a src_nt_domain 8
# src_port 100+
a src_user 3
a src_user_name 3
```

i	Time	Event
>	5/24/23 2:07:03.000 PM	HOST = AD-SECDAY 05/24/2023 10:07:03 LogName=Security EventCode=4672 EventType=0 ComputerName=AD-SEC Show all 29 lines host = AD-SECDAY
>	5/24/23 2:06:51.000 PM	05/24/2023 10:06:51 LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SEC Show all 22 lines host = AD-SECDAY
>	5/24/23 2:06:37.000 PM	05/24/2023 10:06:37 LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SEC Show all 22 lines host = AD-SECDAY
>	5/24/23 2:06:37.000 PM	05/24/2023 10:06:37 LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SEC Show all 22 lines host = AD-SECDAY
>	5/24/23 2:06:37.000 PM	05/24/2023 10:06:37 LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SEC Show all 22 lines host = AD-SECDAY
>	5/24/23 2:06:37.000 PM	05/24/2023 10:06:37 LogName=Security EventCode=4634 EventType=0 ComputerName=AD-SEC Show all 22 lines host = AD-SECDAY
>	5/24/23 2:06:37.000 PM	05/24/2023 10:06:37 LogName=Security



CONFIGURAR OS PARSINGS - PFSENSE

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



The screenshot shows a log analysis interface with the following details:

- Search Bar:** index=* sourcetype=pfsense
- Results Summary:** ✓ 10,889 events (5/23/23 2:00:00.000 PM to 5/24/23 2:21:46.000 PM) No Event Sampling ▾
- Event List:** Events (10,889) Patterns Statistics Visualization
- Event Fields:** List ▾ Format 20 Per Page ▾
- Selected Fields:** host 1 source 1 sourcetype 1
- Interesting Fields:** date_hour 16 date_mday 2 date_minute 60 date_month 1 date_second 60 date_wday 2 date_year 1 date_zone 1 index 1 linecount 1 punct 26
- Event Log Entries:** A list of log entries from May 24, 2023, at 14:21:38, showing various filterlog entries from host 192.168.1.8 and source udp:12514.



CONFIGURAR OS PARSINGS - PFSENSE

- Instale o add-on “TA-pfsense”



TA-pfsense Install

This Technology Add-on provides CIM compliant field extractions, eventtypes and tags for the pfSense firewall.

Fully Splunk App for Enterprise Security compatible.

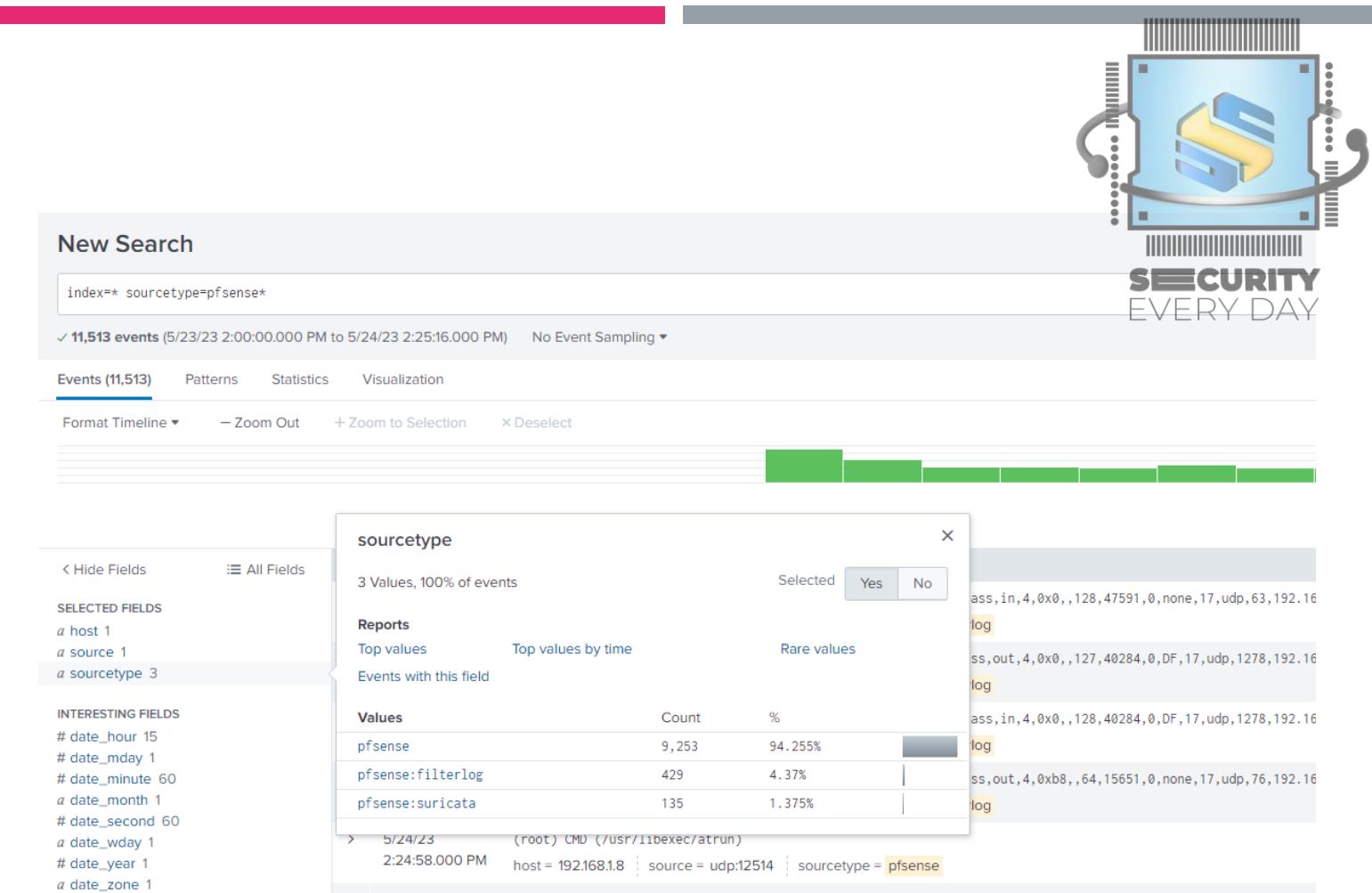
Sponsored by Datapunctum GmbH

Category: Security, Fraud & Compliance | Author: Mika Borner | Downloads: 109326 | Released: a year ago | Last Updated: 6 months ago | [View on Splunkbase](#)



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



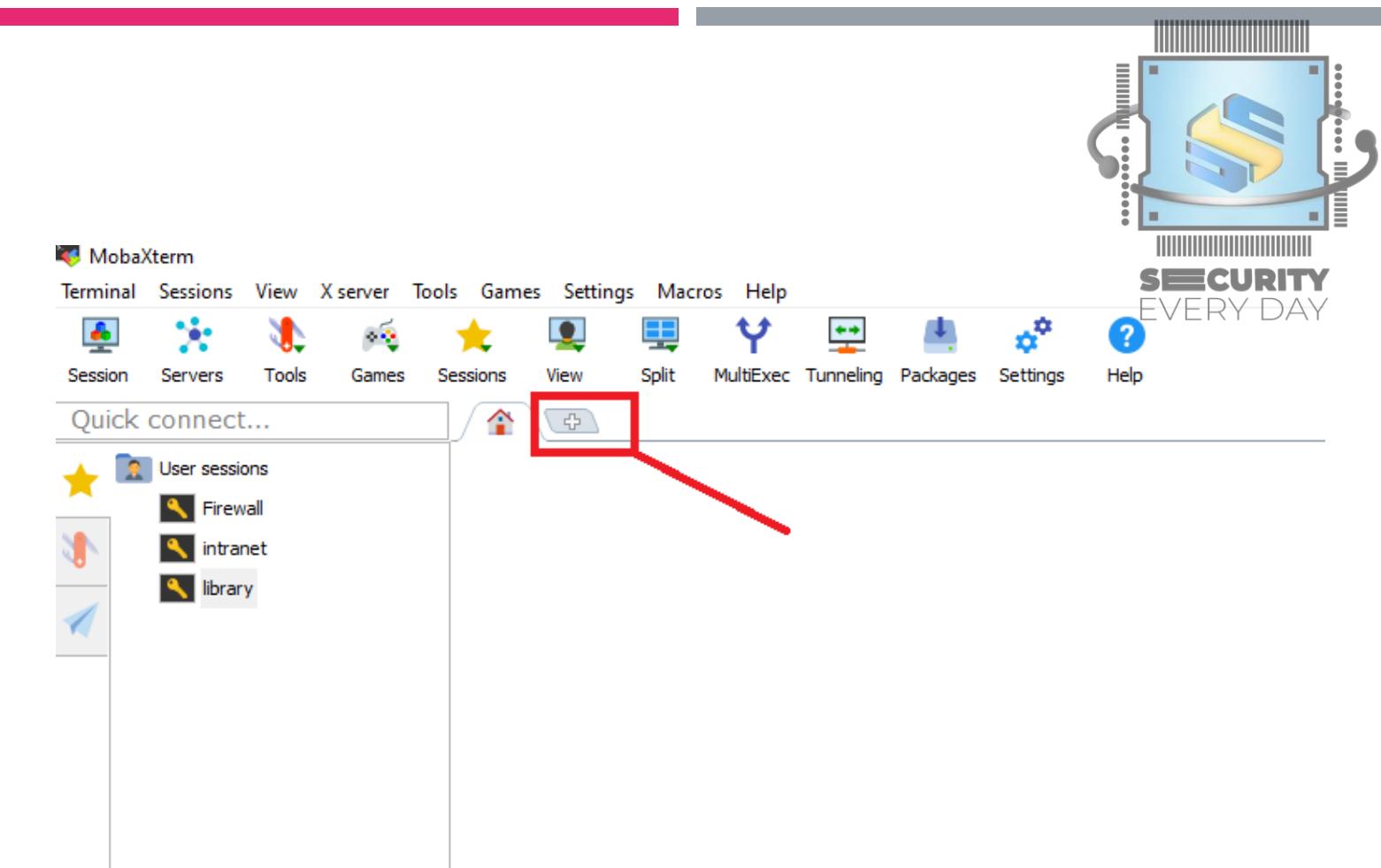
SCAN DE PORTAS

- 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.



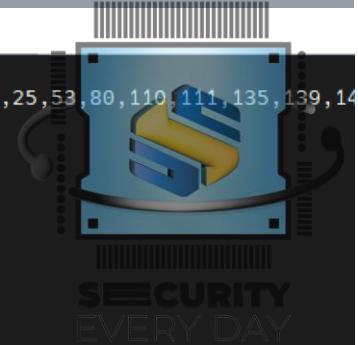
SCAN DE PORTAS - ATAQUE

- 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
,139,143,443,445,993,995,172
3,3306,3389,5900,8080
 - nc -vz -w 1
pfSense.secday.local
21,22,23,25,53,80,110,111,135
,139,143,443,445,993,995,172
3,3306,3389,5900,8080



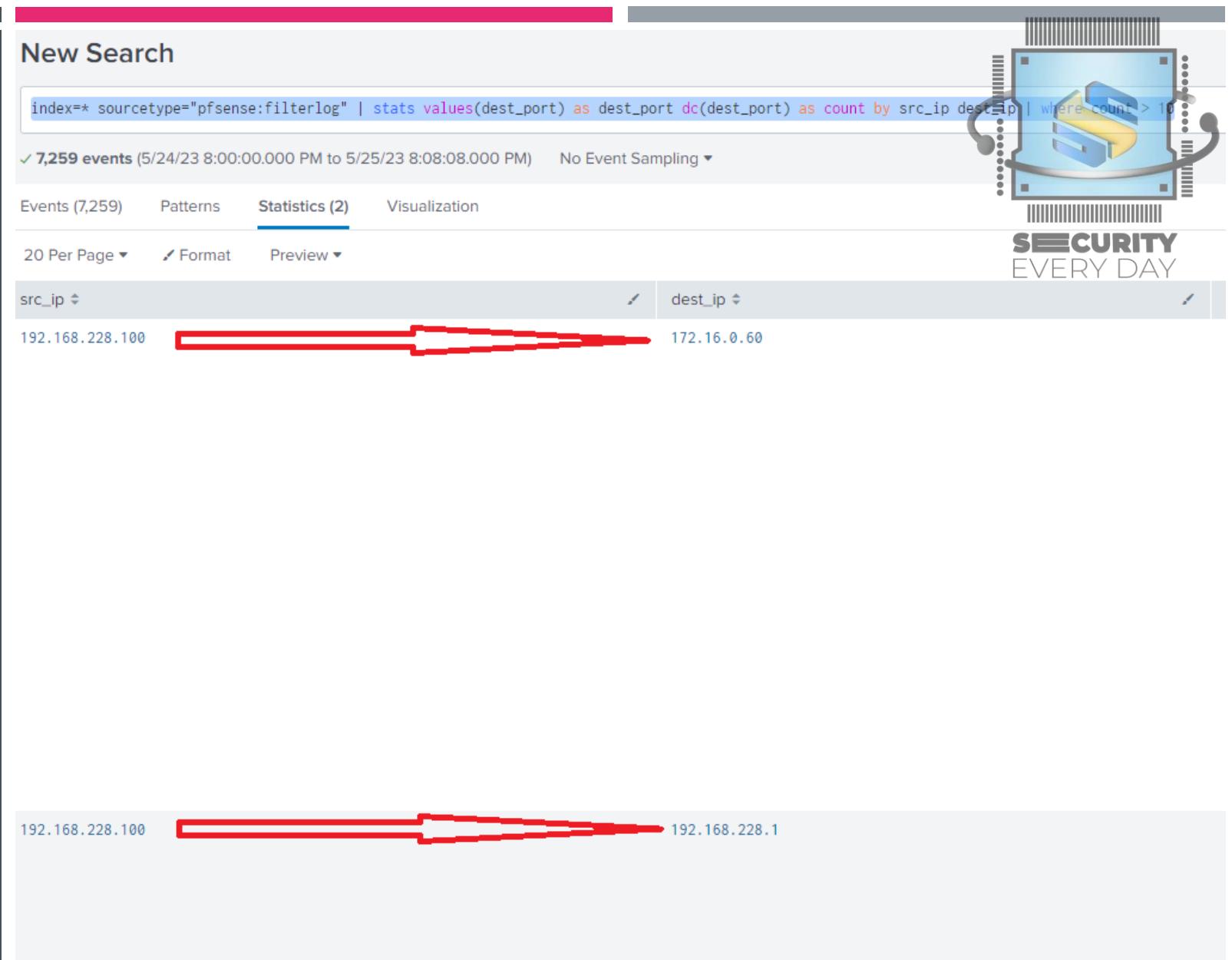
```
25/05/2023 15:51:38 /home/mobaxterm nc -vz -w 1 intranet.secday.local 21,22,23,25,53,80,110,111,135,139,143
nc: connect to intranet.secday.local port 21 (tcp) failed: Connection timed out
Connection to intranet.secday.local 22 port [tcp/ssh] succeeded!
nc: connect to intranet.secday.local port 23 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 25 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 53 (tcp) failed: Connection timed out
Connection to intranet.secday.local 80 port [tcp/http] succeeded!
nc: connect to intranet.secday.local port 110 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 111 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 135 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 139 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 143 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 443 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 445 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 993 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 995 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 1723 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 3306 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 3389 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 5900 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 8080 (tcp) failed: Connection timed out

25/05/2023 16:05:08 /home/mobaxterm nc -vz -w 1 pfSense.secday.local 21,22,23,25,53,80,110,111,135,139,143
nc: connect to pfSense.secday.local port 21 (tcp) failed: Connection timed out
Connection to pfSense.secday.local 22 port [tcp/ssh] succeeded!
nc: connect to pfSense.secday.local port 23 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 25 (tcp) failed: Connection timed out
Connection to pfSense.secday.local 53 port [tcp/domain] succeeded!
Connection to pfSense.secday.local 80 port [tcp/http] succeeded!
nc: connect to pfSense.secday.local port 110 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 111 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 135 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 139 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 143 (tcp) failed: Connection timed out
Connection to pfSense.secday.local 443 port [tcp/https] succeeded!
nc: connect to pfSense.secday.local port 445 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 993 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 995 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 1723 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 3306 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 3389 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 5900 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 8080 (tcp) failed: Connection timed out

25/05/2023 16:05:33 /home/mobaxterm
```

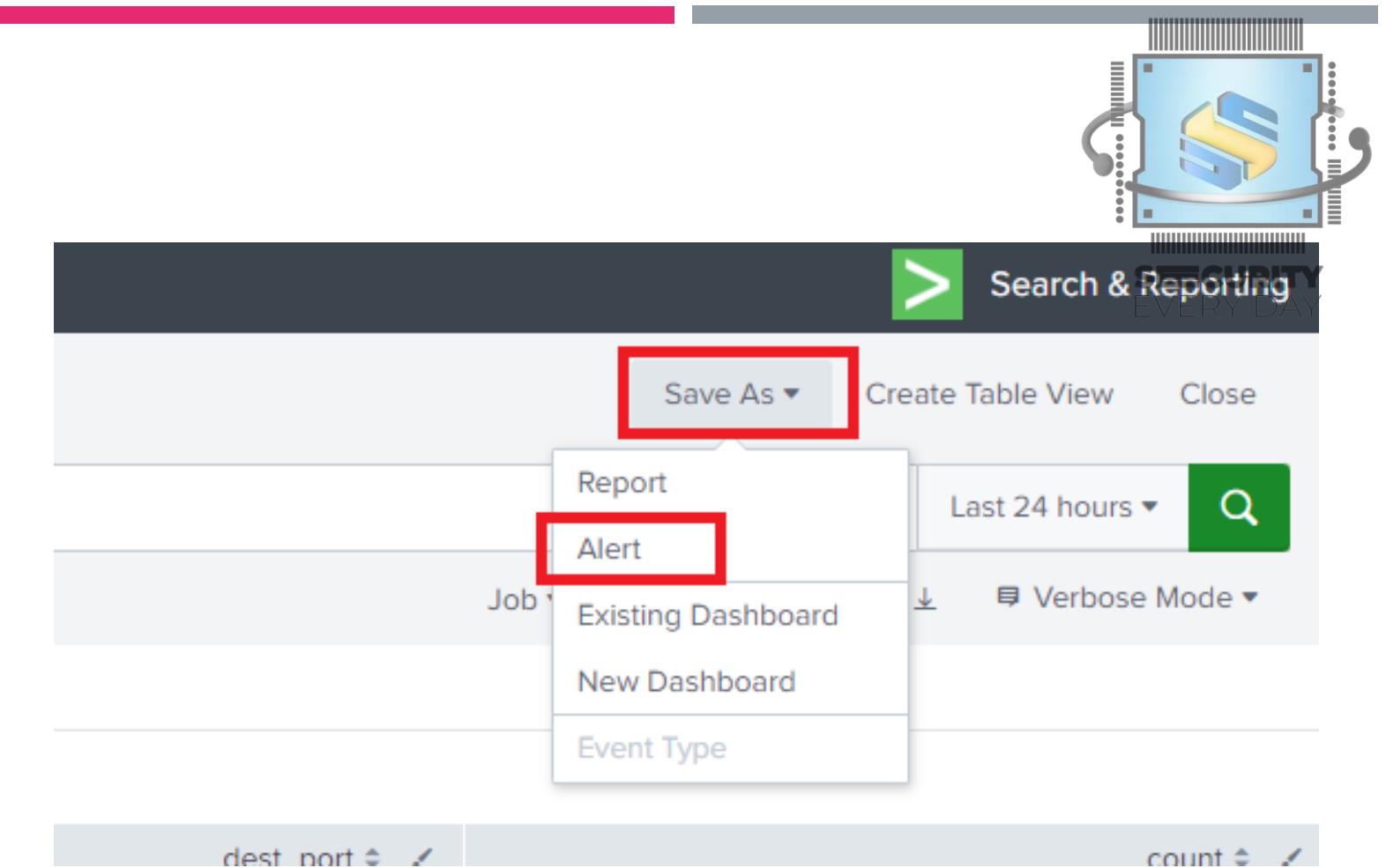
SCAN DE PORTAS – REGRA

- 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

## Save As Alert

### Settings

Title [T1046] - Scan de portas - pfSense

Description Optional

Permissions Private Shared in App

Alert type Scheduled Real-time

Run on Cron Schedule ▾

Time Range Last 15 minutes ▾

Cron Expression \*/1 \* \* \* \*

e.g. 00 18 \*\*\* (every day at 6PM). [Learn More](#)

Expires 24 hour(s) ▾

### Trigger Conditions

Trigger alert when Number of Results ▾

is greater than ▾ 0

Trigger Once For each result

Throttle ?

Suppress results containing field value  
src\_ip,dest\_ip



# SCAN DE PORTAS - REGRA

- Finalize o preenchimento e clique em “Save”



Suppress triggering for  hour(s) ▾

**Trigger Actions**

+ Add Actions ▾

When triggered

Add to Triggered Alerts

Severity

# 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.



Alert has been saved

⚠ This scheduled search will not run after the Splunk Enterprise Trial License expires.

You can view your alert, change additional settings, or continue editing it.

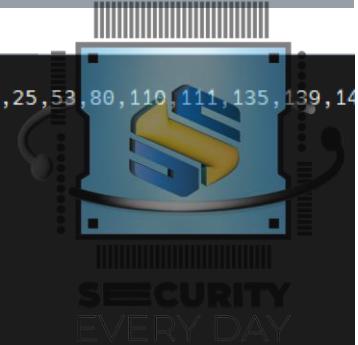
Additional Settings:

- [Permissions](#)

[Continue Editing](#) [View Alert](#)

# 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 ,139,143,443,445,993,995,172 3,3306,3389,5900,8080
  - nc -vz -w 1 pfSense.secday.local 21,22,23,25,53,80,110,111,135 ,139,143,443,445,993,995,172 3,3306,3389,5900,8080



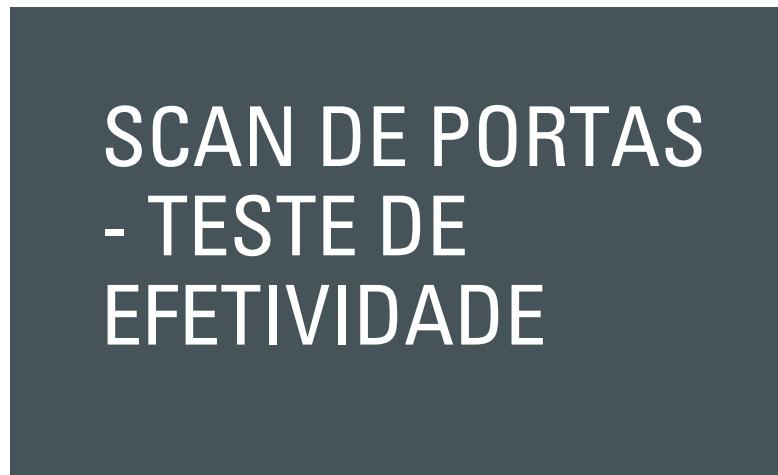
```
25/05/2023 15:51:38 /home/mobaxterm nc -vz -w 1 intranet.secday.local 21,22,23,25,53,80,110,111,135,139,143
nc: connect to intranet.secday.local port 21 (tcp) failed: Connection timed out
Connection to intranet.secday.local 22 port [tcp/ssh] succeeded!
nc: connect to intranet.secday.local port 23 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 25 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 53 (tcp) failed: Connection timed out
Connection to intranet.secday.local 80 port [tcp/http] succeeded!
nc: connect to intranet.secday.local port 110 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 111 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 135 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 139 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 143 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 443 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 445 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 993 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 995 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 1723 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 3306 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 3389 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 5900 (tcp) failed: Connection timed out
nc: connect to intranet.secday.local port 8080 (tcp) failed: Connection timed out

25/05/2023 16:05:08 /home/mobaxterm nc -vz -w 1 pfSense.secday.local 21,22,23,25,53,80,110,111,135,139,143
nc: connect to pfSense.secday.local port 21 (tcp) failed: Connection timed out
Connection to pfSense.secday.local 22 port [tcp/ssh] succeeded!
nc: connect to pfSense.secday.local port 23 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 25 (tcp) failed: Connection timed out
Connection to pfSense.secday.local 53 port [tcp/domain] succeeded!
Connection to pfSense.secday.local 80 port [tcp/http] succeeded!
nc: connect to pfSense.secday.local port 110 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 111 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 135 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 139 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 143 (tcp) failed: Connection timed out
Connection to pfSense.secday.local 443 port [tcp/https] succeeded!
nc: connect to pfSense.secday.local port 445 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 993 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 995 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 1723 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 3306 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 3389 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 5900 (tcp) failed: Connection timed out
nc: connect to pfSense.secday.local port 8080 (tcp) failed: Connection timed out

25/05/2023 16:05:33 /home/mobaxterm
```

The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes "splunk>enterprise", "Apps", "Administrator", "Messages", "Settings", "Activity", "Help", and a "Find" icon. On the right side of the header, there is a "SECURITY EVERY DAY" logo. The main search bar has "Search & Reporting (search)" selected. Below the search bar, filters are set for "Owner: Administrator (admin)", "Severity: All", "Alert: All", and "Jobs" and "Triggered Alerts" sections. The results table has columns: Time, Fired alerts, App, Type, Severity, Mode, and Actions. A single row is shown: "2023-05-25 20:37:00 GMT Daylight Time" under Time, "[T1046] - Scan de portas - pfsense" under Fired alerts (which is highlighted with a red box), "search" under App, "Scheduled" under Type, "Medium" under Severity (indicated by a yellow circle), "Per Result" under Mode, and "View results", "Edit search", and "Delete" under Actions.

| Time                                  | Fired alerts                       | App    | Type      | Severity | Mode       | Actions                                                                             |
|---------------------------------------|------------------------------------|--------|-----------|----------|------------|-------------------------------------------------------------------------------------|
| 2023-05-25 20:37:00 GMT Daylight Time | [T1046] - Scan de portas - pfsense | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |



- 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".

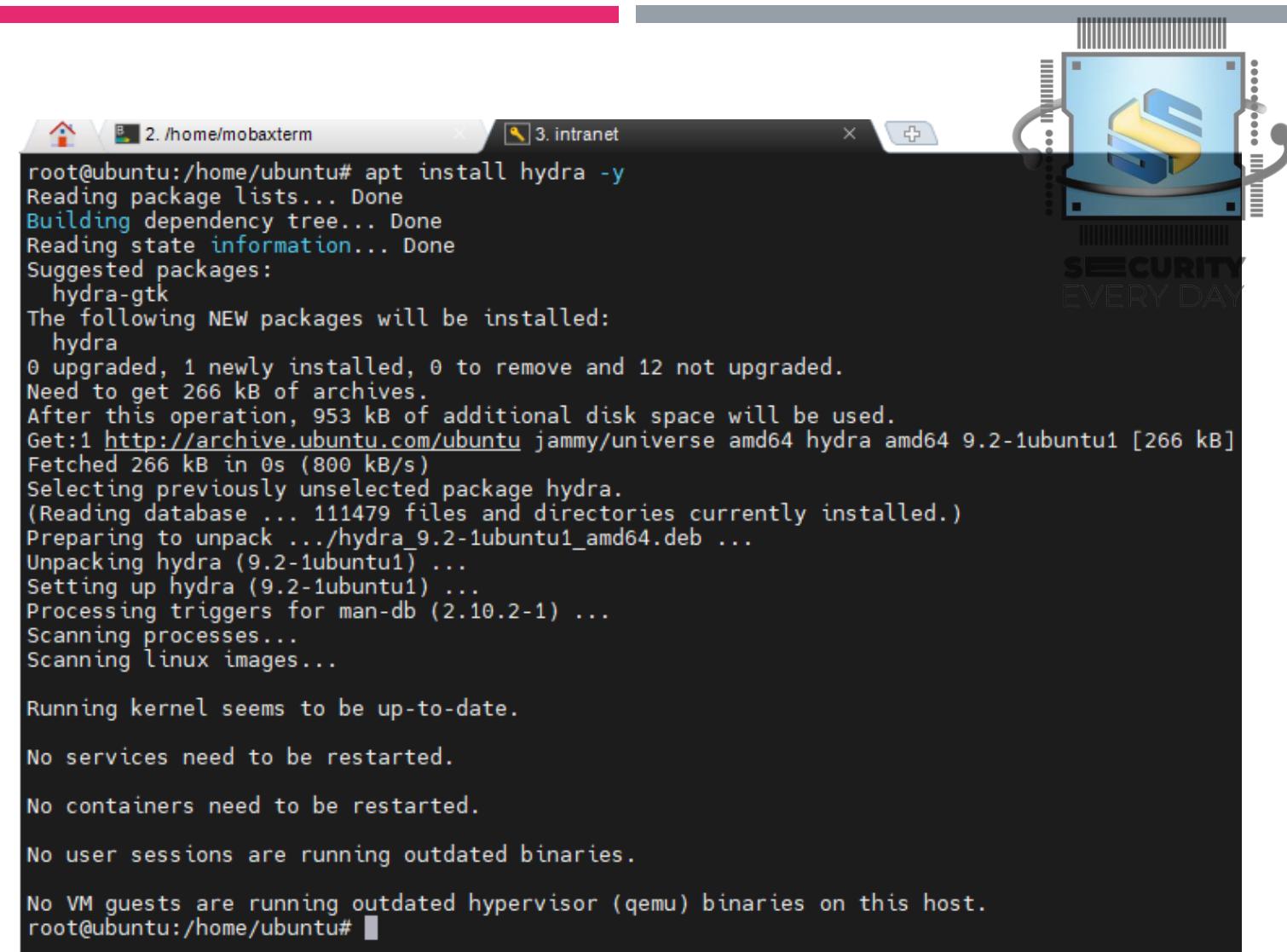
# BRUTE FORCE

- 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



```
root@ubuntu:/home/ubuntu# apt install hydra -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
 hydra-gtk
The following NEW packages will be installed:
 hydra
0 upgraded, 1 newly installed, 0 to remove and 12 not upgraded.
Need to get 266 kB of archives.
After this operation, 953 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 hydra amd64 9.2-1ubuntu1 [266 kB]
Fetched 266 kB in 0s (800 kB/s)
Selecting previously unselected package hydra.
(Reading database ... 111479 files and directories currently installed.)
Preparing to unpack .../hydra_9.2-1ubuntu1_amd64.deb ...
Unpacking hydra (9.2-1ubuntu1) ...
Setting up hydra (9.2-1ubuntu1) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

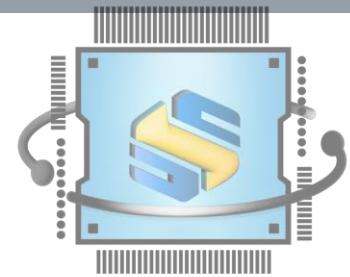
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ubuntu:/home/ubuntu#
```

# 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



```
root@ubuntu:/home/ubuntu# wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt
--2023-05-25 16:53:49-- https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.110.133,
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 180 [text/plain]
Saving to: 'top-20-common-SSH-passwords.txt.1'

top-20-common-SSH-passwords.txt.1 100%[=====] 20338 18.9 MB/s
2023-05-25 16:53:49 (18.9 MB/s) - 'top-20-common-SSH-passwords.txt.1' saved [180/180]

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 organizations
*** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-25 16:53:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[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 1 final worker threads did not complete until end.
[ERROR] 1 target 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 16:54:03
root@ubuntu:/home/ubuntu#
```

# 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`



New Search

Save As ▾ Create Table View Close

```
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
```

Last 24 hours ▾ 🔍

✓ 23 events (5/24/23 8:00:00.000 PM to 5/25/23 8:58:53.000 PM) No Event Sampling ▾ Job ▾ || ■ ↗ ✖ ↓ ⚡ Fast Mode ▾

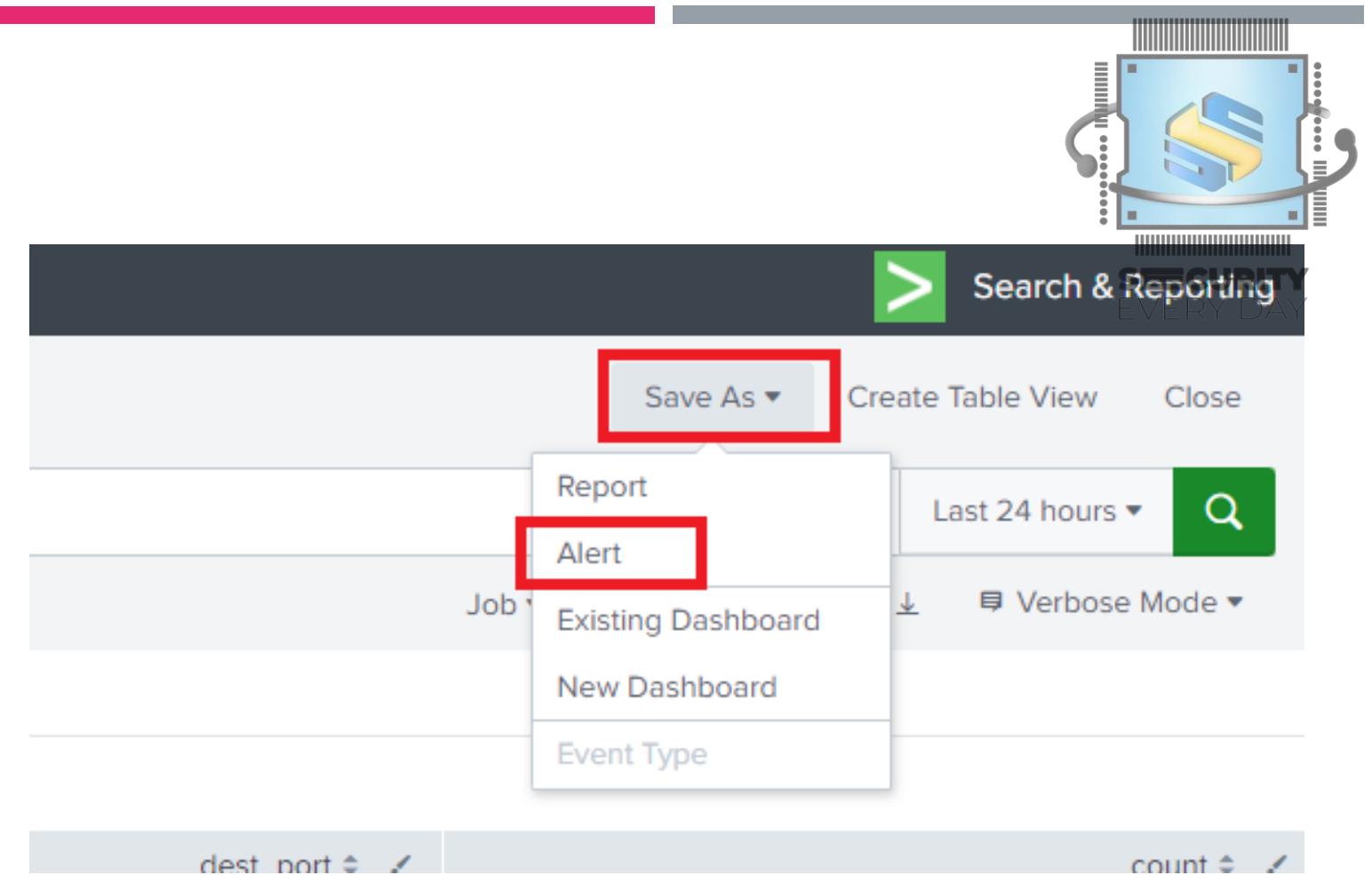
Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview ▾

| src_ip      | count |
|-------------|-------|
| 172.16.0.60 | 23    |

# 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

## Save As Alert

### Settings

Title [T1110] - Brute Force - Linux

Description Optional

Permissions Private Shared in App

Alert type Scheduled Real-time

Run on Cron Schedule ▾

Time Range Last 15 minutes ▾

Cron Expression \*/1 \* \* \* \*

e.g. 00 18 \*\*\* (every day at 6PM). [Learn More](#)

Expires 24 hour(s) ▾

### Trigger Conditions

Trigger alert when Number of Results ▾

is greater than ▾ 0

Trigger Once For each result

Throttle ?

Suppress results containing field value src\_ip,host



# BRUTE FORCE - REGRA

- Finalize o preenchimento e clique em “Save”



Suppress triggering for  hour(s) ▾

**Trigger Actions**

+ Add Actions ▾

When triggered

Add to Triggered Alerts

Severity

# 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.



A screenshot of a Splunk alert creation interface. A modal window titled "Alert has been saved" is displayed. It contains a warning message: "⚠ This scheduled search will not run after the Splunk Enterprise Trial License expires." Below the message, it says "You can view your alert, change additional settings, or continue editing it." Under "Additional Settings:", there is a link to "Permissions". At the bottom right of the modal are two buttons: "Continue Editing" (gray) and "View Alert" (green).

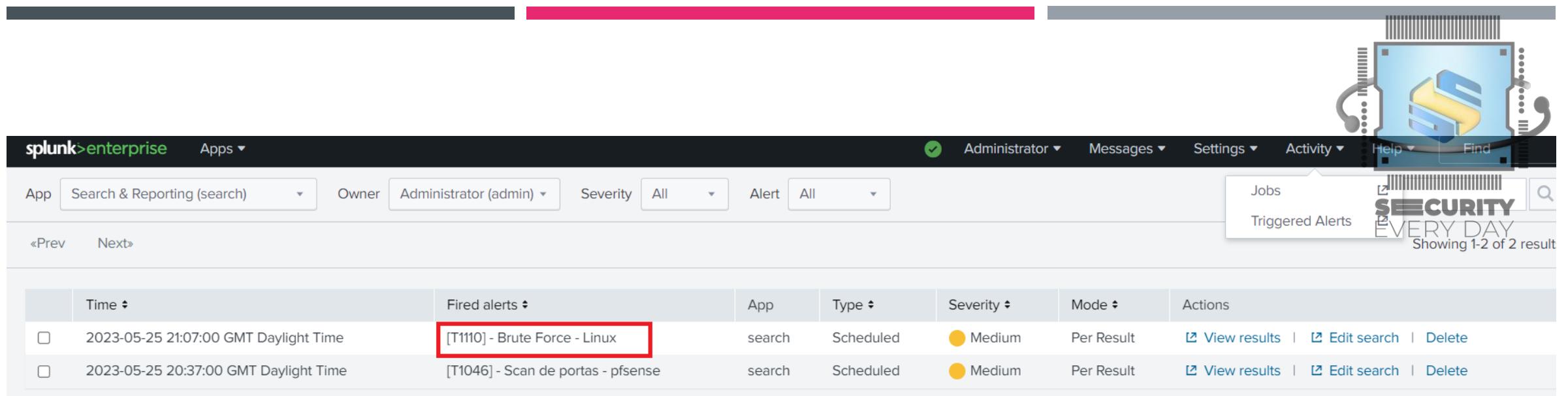
# BRUTE FORCE - TESTE DE EFETIVIDADE

- 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 contexts
*** 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 tasks per 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#
```



The screenshot shows the Splunk Enterprise interface. The top navigation bar includes 'splunk>enterprise' and 'Apps'. On the right, there's a user icon for 'Administrator', a 'Find' search bar, and a 'SECURITY EVERY DAY' banner. Below the navigation, there are filters for 'App' (Search & Reporting), 'Owner' (Administrator), 'Severity' (All), and 'Alert' (All). To the right of these filters are buttons for 'Jobs' and 'Triggered Alerts'. The main table lists two triggered alerts:

|                          | Time                                  | Fired alerts                       | App    | Type      | Severity | Mode       | Actions                                                                             |
|--------------------------|---------------------------------------|------------------------------------|--------|-----------|----------|------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 2023-05-25 21:07:00 GMT Daylight Time | [T1110] - Brute Force - Linux      | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| <input type="checkbox"/> | 2023-05-25 20:37:00 GMT Daylight Time | [T1046] - Scan de portas - pfSense | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |

# 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

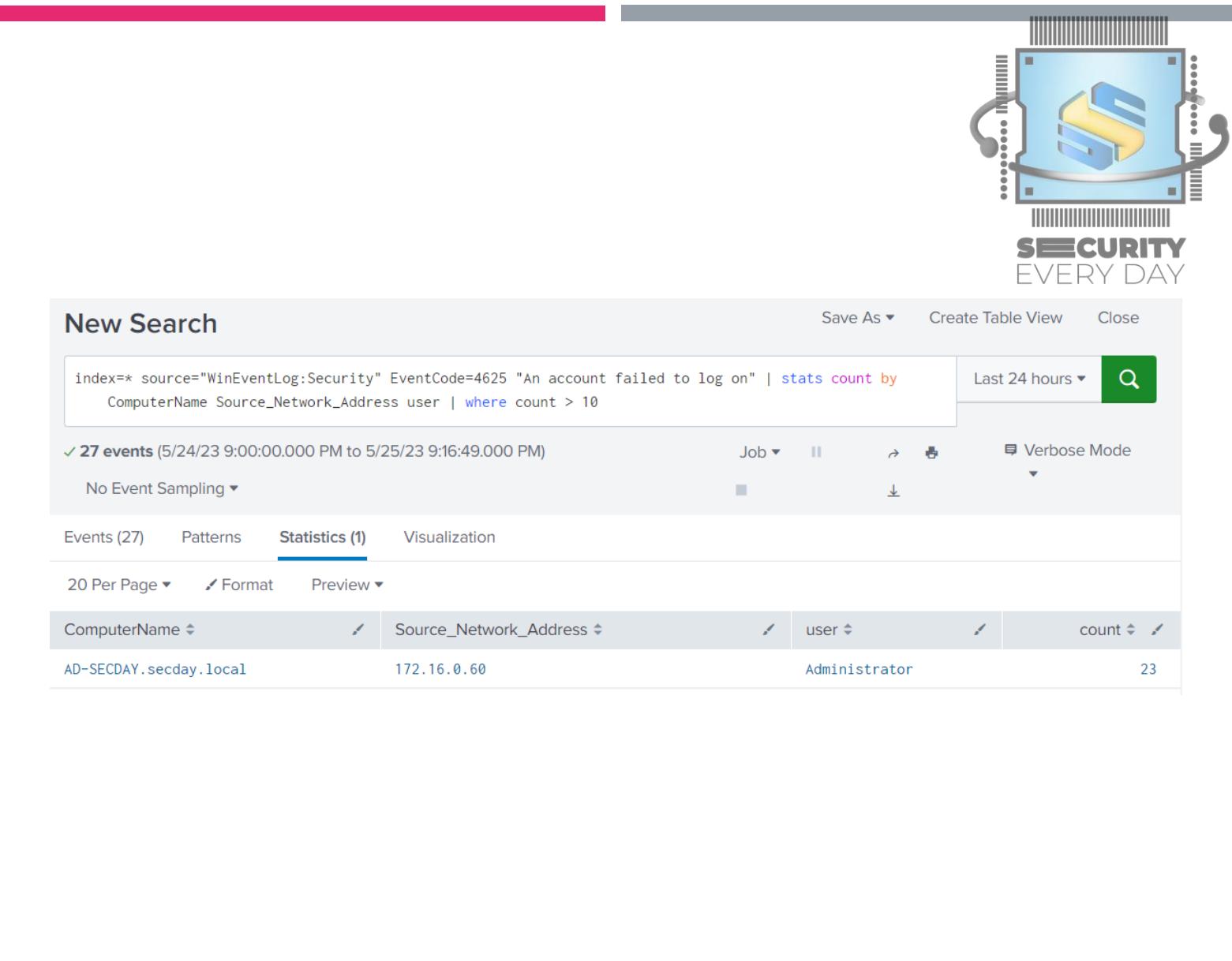
```
root@ubuntu:/home/ubuntu# hydra -l Administrator -P top-20-common-SSH-passwords.txt smb://172.16.0.5
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organ
*** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-25 17:15:40
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 24 login tries (l:1/p:24), ~24 tries per task
[DATA] attacking smb://172.16.0.5:445/
[445][smb] host: 172.16.0.5 login: Administrator password: Admin@mudar
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-25 17:15:41
root@ubuntu:/home/ubuntu#
```



# 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



The image shows a screenshot of the Splunk web interface. At the top, there is a search bar with the following query:

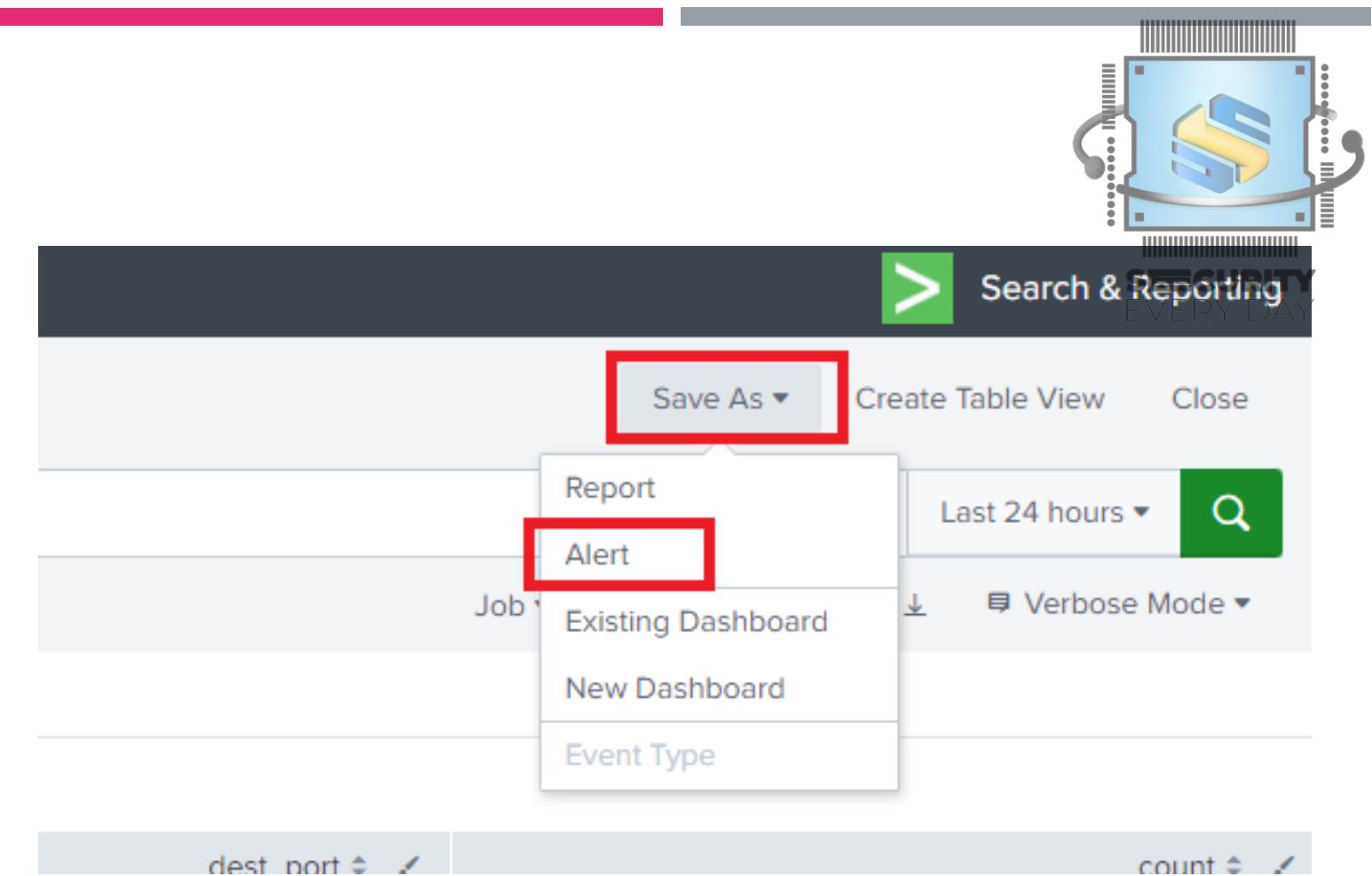
```
index=* source="WinEventLog:Security" EventCode=4625 "An account failed to log on" | stats count by ComputerName Source_Network_Address user | where count > 10
```

Below the search bar, it says "27 events (5/24/23 9:00:00.000 PM to 5/25/23 9:16:49.000 PM)". The "Statistics (1)" tab is selected. A table below shows the results:

| ComputerName           | Source_Network_Address | user          | count |
|------------------------|------------------------|---------------|-------|
| AD-SECDAY.secday.local | 172.16.0.60            | Administrator | 23    |

# 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

## Save As Alert

### Settings

|                 |                                                                              |               |
|-----------------|------------------------------------------------------------------------------|---------------|
| Title           | [T1110] - Brute Force - Windows                                              |               |
| Description     | Optional                                                                     |               |
| Permissions     | Private                                                                      | Shared in App |
| Alert type      | Scheduled                                                                    | Real-time     |
|                 | Run on Cron Schedule ▾                                                       |               |
| Time Range      | Last 15 minutes ▾                                                            |               |
| Cron Expression | */1 * * * *<br>e.g. 00 18 *** (every day at 6PM). <a href="#">Learn More</a> |               |
| Expires         | 24                                                                           | hour(s) ▾     |

### Trigger Conditions

|                                         |                                     |                 |
|-----------------------------------------|-------------------------------------|-----------------|
| Trigger alert when                      | Number of Results ▾                 |                 |
|                                         | is greater than ▾                   | 0               |
| Trigger                                 | Once                                | For each result |
| Throttle ?                              | <input checked="" type="checkbox"/> |                 |
| Suppress results containing field value | ComputerName,Source_Network_Address |                 |



# BRUTE FORCE – REGRA (WINDOWS)

- Finalize o preenchimento e clique em “Save”



Suppress triggering for  hour(s) ▾

**Trigger Actions**

+ Add Actions ▾

When triggered

Add to Triggered Alerts Remove

Severity  ▾

Cancel 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.



A screenshot of a Splunk alert success message. The message box has a black header bar with the text "Alert has been saved". Below the header, there is a yellow warning icon followed by the text: "⚠ This scheduled search will not run after the Splunk Enterprise Trial License expires." Underneath this, it says "You can view your alert, change additional settings, or continue editing it." A section titled "Additional Settings:" contains a single item: "• Permissions". At the bottom right of the message box are two buttons: "Continue Editing" (gray) and "View Alert" (green).

# 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



```
root@ubuntu:/home/ubuntu# hydra -l Administrator -P top-20-common-SSH-passwords.txt smb://172.16.0.5
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service operations
*** ignore laws and ethics anyway.

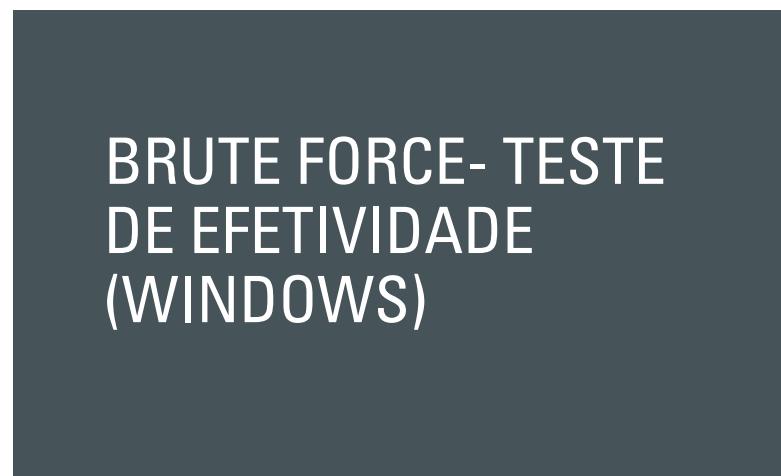
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-25 17:23:38
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 24 login tries (l:1/p:24), ~24 tries per task
[DATA] attacking smb://172.16.0.5:445/
[445][smb] host: 172.16.0.5 login: Administrator password: Admin@mudar
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-25 17:23:39
root@ubuntu:/home/ubuntu#
```

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' on the left, followed by 'Apps ▾', 'Administrator' (with a green checkmark), 'Messages ▾', 'Settings ▾', 'Activity ▾', 'Help ▾', and a search bar with a magnifying glass icon labeled 'Find'. To the right of the search bar is a graphic of a computer monitor displaying a blue 'S' logo, with the word 'SECURITY' and the tagline 'Showing 1-3 of 3 results' below it.

The main area has a toolbar at the top with 'App' set to 'Search & Reporting (search)', 'Owner' set to 'Administrator (admin)', and dropdowns for 'Severity' (All), 'Alert' (All), and 'Jobs' (with a link to 'Triggered Alerts'). Below the toolbar, there are links for '<Prev' and 'Next>'.

The main content area is a table titled 'Triggered Alerts' with the following columns: Time, Fired alerts, App, Type, Severity, Mode, and Actions. The table contains three rows:

|                          | Time                                  | Fired alerts                       | App    | Type      | Severity | Mode       | Actions                                                                             |
|--------------------------|---------------------------------------|------------------------------------|--------|-----------|----------|------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 2023-05-25 21:26:00 GMT Daylight Time | [T1110] - Brute Force - Windows    | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| <input type="checkbox"/> | 2023-05-25 21:07:00 GMT Daylight Time | [T1110] - Brute Force - Linux      | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| <input type="checkbox"/> | 2023-05-25 20:37:00 GMT Daylight Time | [T1046] - Scan de portas - pfSense | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |



- 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

```
root@ubuntu:/home/ubuntu# apt install dirb -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
 dirb
0 upgraded, 1 newly installed, 0 to remove and 12 not upgraded.
Need to get 203 kB of archives.
After this operation, 1,505 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 dirb amd64 2.22+dfsg-5 [203 kB]
Fetched 203 kB in 0s (638 kB/s)
Selecting previously unselected package dirb.
(Reading database ... 111431 files and directories currently installed.)
Preparing to unpack .../dirb_2.22+dfsg-5_amd64.deb ...
Unpacking dirb (2.22+dfsg-5) ...
Setting up dirb (2.22+dfsg-5) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ubuntu:/home/ubuntu# █
```



# 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

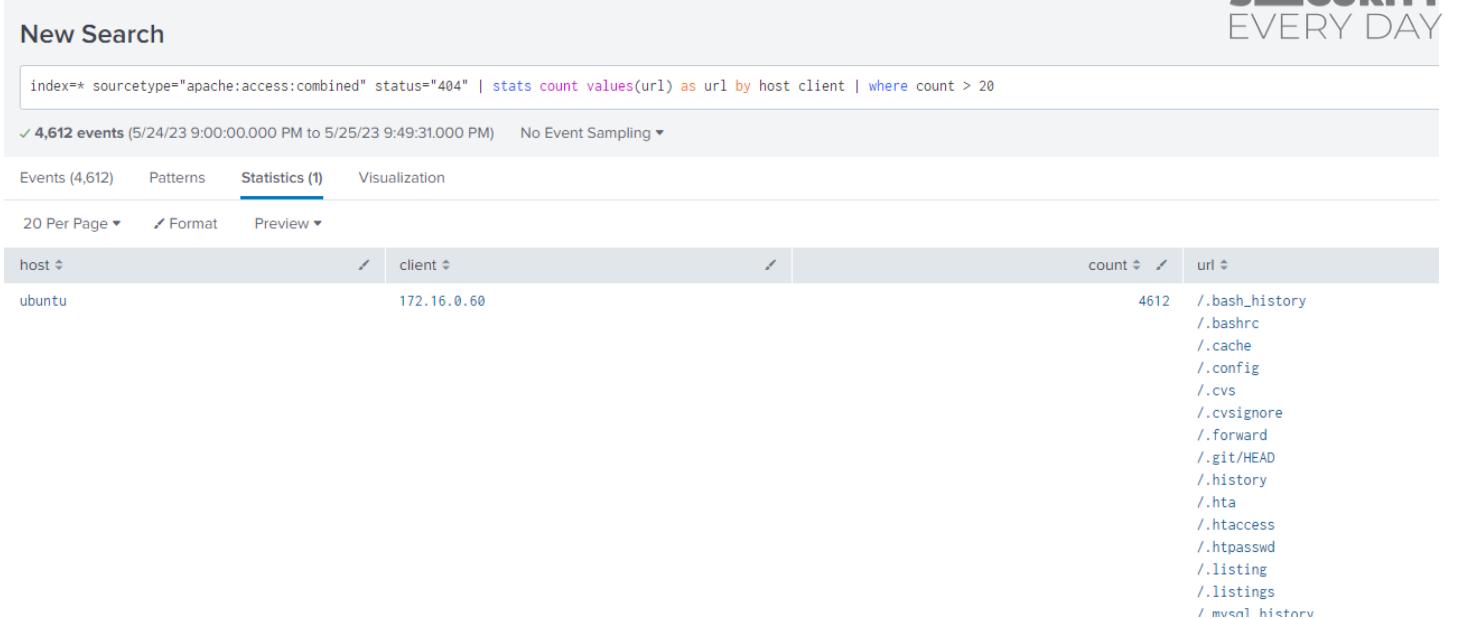
---- Scanning URL: http://10.0.1.101/ ----
+ http://10.0.1.101/books (CODE:302|SIZE:189)
+ http://10.0.1.101/logout (CODE:302|SIZE:189)
+ http://10.0.1.101/server-status (CODE:403|SIZE:275)

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=\*<br>sourcetype="apache:access:combined" status="404" | stats count values(url) as url by host client | where count > 20



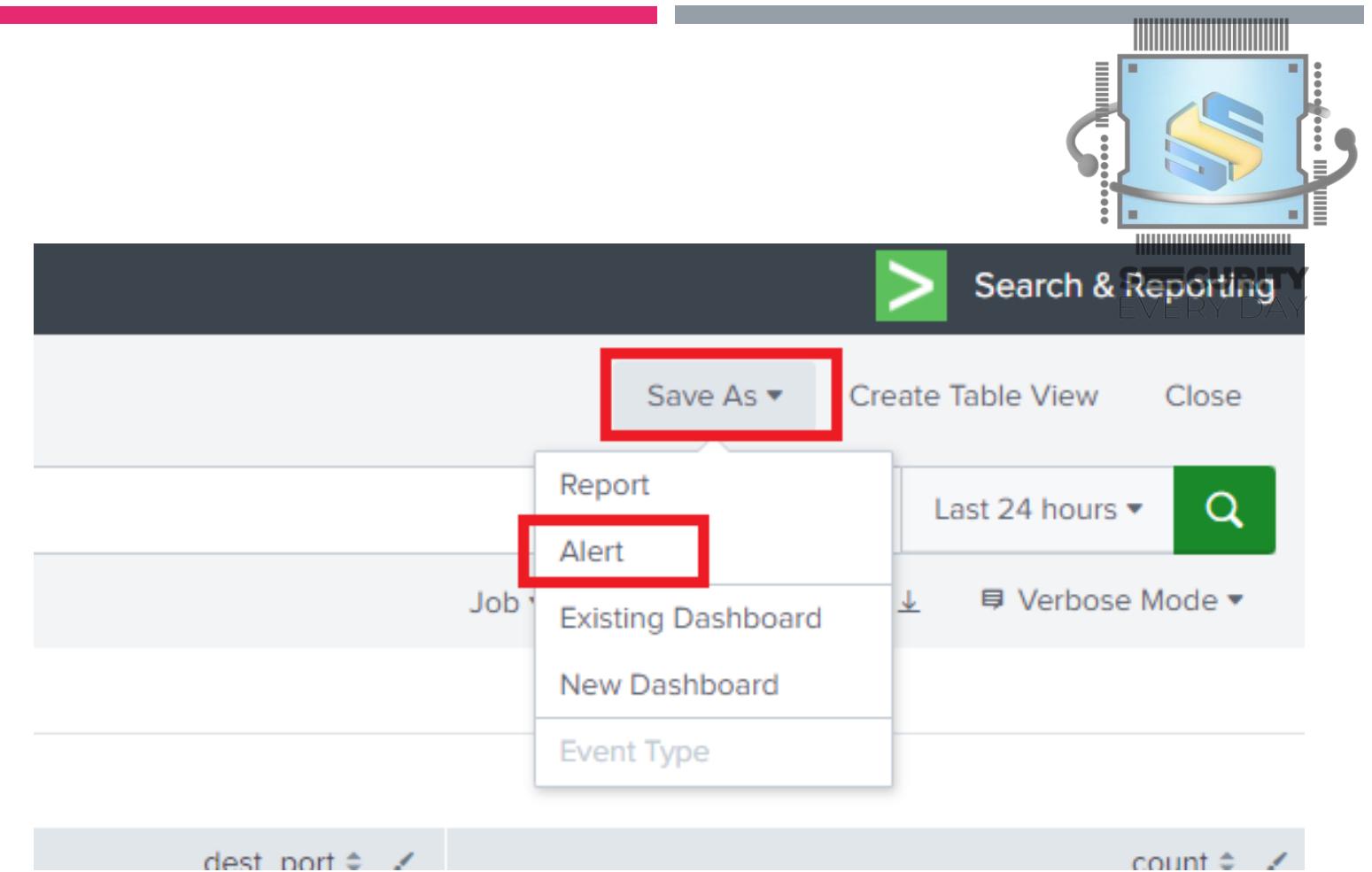
The screenshot shows a Splunk search interface with the following details:

- New Search:** The search bar contains the command: `index=* sourcetype="apache:access:combined" status="404" | stats count values(url) as url by host client | where count > 20`.
- Results:** 4,612 events were found between 5/24/23 9:00:00.000 PM and 5/25/23 9:49:31.000 PM. No Event Sampling was applied.
- Statistics View:** The Statistics tab is selected, showing the following table of results:

| host   | client      | count | url                                                                                                                                                                                     |
|--------|-------------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ubuntu | 172.16.0.60 | 4612  | /.bash_history<br>/.bashrc<br>.cache<br>.config<br>.cvs<br>.cvignore<br>.forward<br>.git/HEAD<br>.history<br>.hta<br>.htaccess<br>.htpasswd<br>.listing<br>.listings<br>/.mvenl history |

# 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

## Save As Alert

### Settings

Title [T1110] Brute Forte - Diretorios e Arquivos - Web

Description Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run on Cron Schedule ▾

Time Range

Last 15 minutes ▾

Cron Expression

\*/1 \* \* \* \*

e.g. 00 18 \*\*\* (every day at 6PM). [Learn More](#)

Expires

24

hour(s) ▾

### Trigger Conditions

Trigger alert when

Number of Results ▾

is greater than ▾

0

Trigger

Once

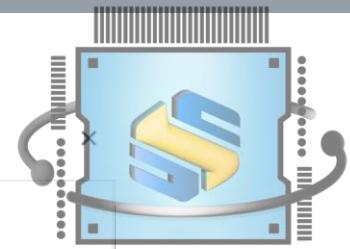
For each result

Throttle ?



Suppress results  
containing field value

host.client



SECURITY  
EVERY DAY

# BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - REGRA

- Finalize o preenchimento e clique em “Save”



Suppress triggering for  hour(s) ▾

**Trigger Actions**

+ Add Actions ▾

When triggered

Add to Triggered Alerts Remove

Severity  ▾

Cancel 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.



Alert has been saved

⚠ This scheduled search will not run after the Splunk Enterprise Trial License expires.

You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- [Permissions](#)

[Continue Editing](#) [View Alert](#)

## BRUTE FORCE EM ARQUIVOS/DIRETÓRIOS WEB - TESTE DE EFETIVIDADE

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

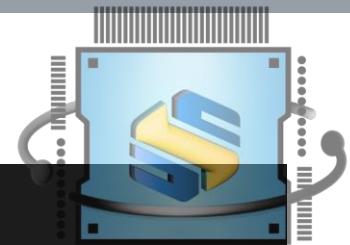
```
root@ubuntu:/home/ubuntu# dirb http://10.0.1.101

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
```



SECURITY  
EVERY DAY

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation bar, there are search filters: 'App' set to 'Search & Reporting (search)', 'Owner' set to 'Administrator (admin)', 'Severity' set to 'All', and 'Alert' set to 'All'. A 'Filtered' button is also present. On the right side of the header, there's a 'SECURITY EVERY DAY' logo and a message 'Showing 1 of 4 results'. The main content area displays a table of triggered alerts:

|                          | Time                                  | Fired alerts                                      | App    | Type      | Severity | Mode       | Actions                                                                             |
|--------------------------|---------------------------------------|---------------------------------------------------|--------|-----------|----------|------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 2023-05-25 21:55:01 GMT Daylight Time | [T1110] Brute Forte - Diretorios e Arquivos - Web | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| <input type="checkbox"/> | 2023-05-25 21:26:00 GMT Daylight Time | [T1110] - Brute Force - Windows                   | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| <input type="checkbox"/> | 2023-05-25 21:07:00 GMT Daylight Time | [T1110] - Brute Force - Linux                     | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |
| <input type="checkbox"/> | 2023-05-25 20:37:00 GMT Daylight Time | [T1046] - Scan de portas - pfsense                | search | Scheduled | Medium   | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a> |

## 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



```
root@ubuntu:/home/ubuntu# apt install sqlmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
 sqlmap
0 upgraded, 1 newly installed, 0 to remove and 12 not upgraded.
Need to get 6,900 kB of archives.
After this operation, 11.0 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 sqlmap all 1.6.4-2 [6,900 kB]
Fetched 6,900 kB in 1s (9,826 kB/s)
Selecting previously unselected package sqlmap.
(Reading database ... 110796 files and directories currently installed.)
Preparing to unpack .../sqlmap_1.6.4-2_all.deb ...
Unpacking sqlmap (1.6.4-2) ...
Setting up sqlmap (1.6.4-2) ...
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

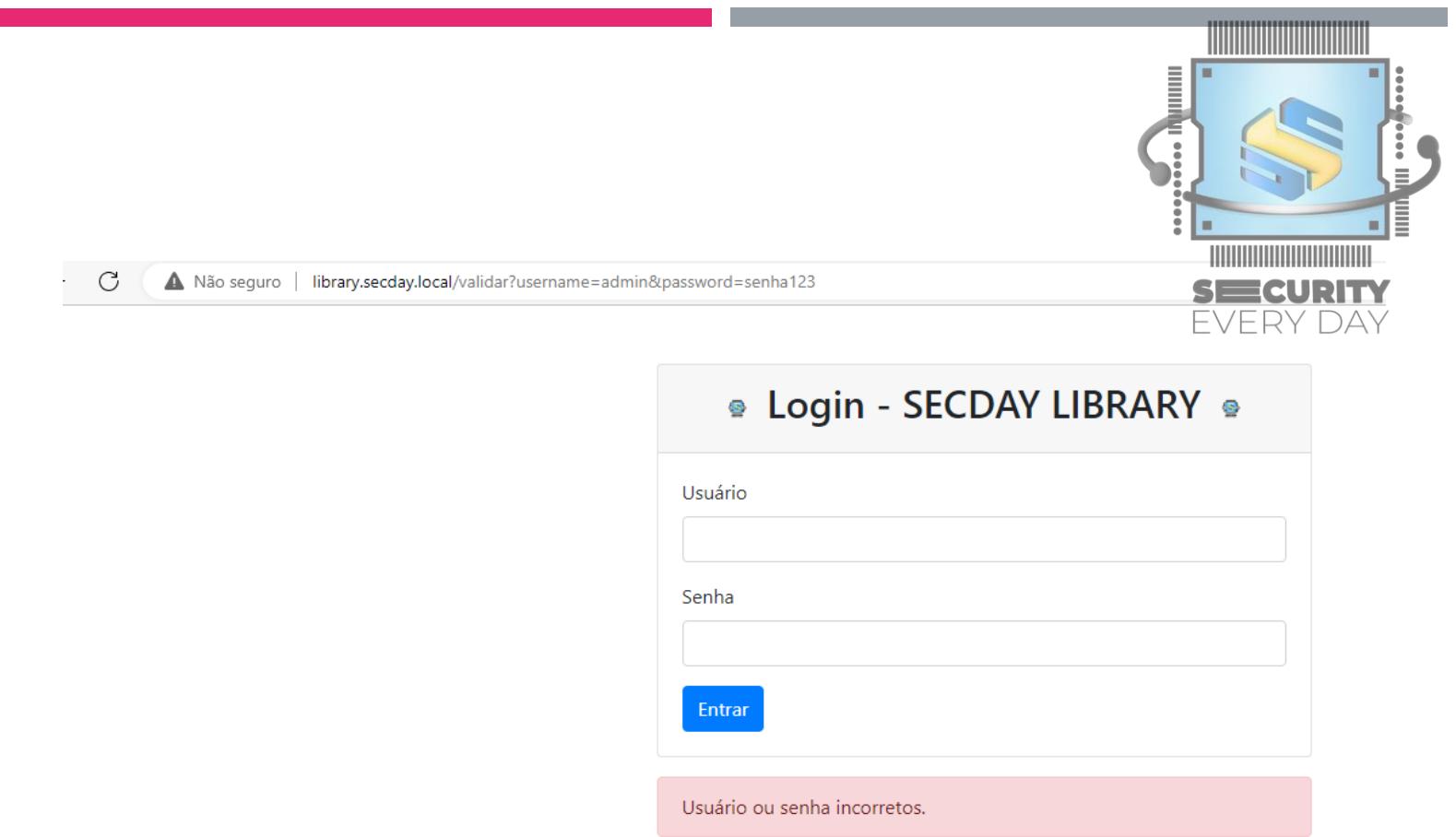
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@ubuntu:/home/ubuntu#
```

# 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>



Não seguro | library.secday.local/validar?username=admin&password=senha123

## Login - SECDAY LIBRARY

Usuário

Senha

Entrar

Usuário ou senha incorretos.

# 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. Nossa foco, neste momento, será tentar executar um ataque de SQL Injection e com base nos logs que temos à disposição, conseguiremos identificar esse ataque.

Não seguro | library.secday.local/validar?username=admin&password=senha123

### Login - SECDAY LIBRARY

Usuário

Senha

Entrar

Usuário ou senha incorretos.

# SQLINJECTION - ATAQUE

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

```
root@ubuntu:/home/ubuntu# sqlmap -u "http://10.0.1.101/validar?username=admin&password=admin"
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 18:14:30 /2023-05-25

[18:14:30] [INFO] testing connection to the target URL
[18:14:30] [INFO] testing if the target URL content is stable
[18:14:31] [INFO] target URL content is stable
[18:14:31] [INFO] testing if GET parameter 'username' is dynamic
[18:14:31] [WARNING] GET parameter 'username' does not appear to be dynamic
[18:14:31] [WARNING] heuristic (basic) test shows that GET parameter 'username' might not be injectable
[18:14:31] [INFO] testing for SQL injection on GET parameter 'username'
[18:14:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:14:31] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:14:31] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:14:31] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:14:31] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[18:14:32] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:14:32] [INFO] testing 'Generic inline queries'
[18:14:32] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:14:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:14:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:14:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:14:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:14:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:14:32] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] n
```



# 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)|(%)|(AND)|(OR)|(NOT)|(SELECT)|(UPDATE)|(DELETE)|(DROP)|(INSERT)|(ALTER)|(--)|(\#\#)|(SLEEP)|(WAITFOR)" | eval url=urldecode(url) | stats count values(url) as url by host client

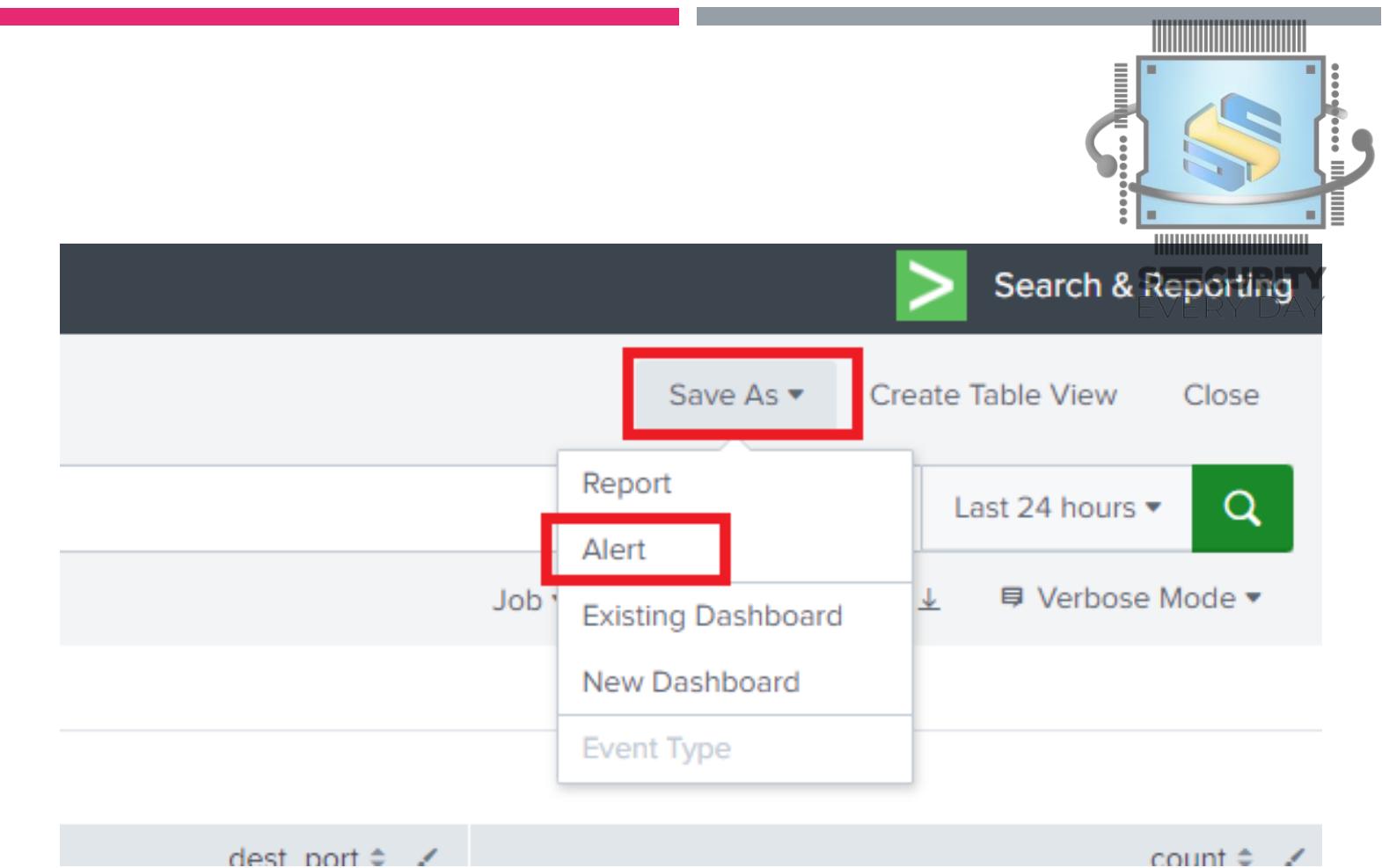
The screenshot shows a Splunk search interface with the following details:

- New Search:** The search bar contains the command: `index=* sourcetype="apache:access:combined" | regex url="(\%27)|(--)|(\%22)|(UNION)|(%)|(AND)|(OR)|(NOT)|(SELECT)|(UPDATE)|(DELETE)|(DROP)|(INSERT)|(ALTER)|(--)|(\#\#)|(SLEEP)|(WAITFOR)" | eval url=urldecode(url) | stats count values(url) as url by host client`.
- Results:** 248 events were found between 5/24/23 10:00:00.000 PM and 5/25/23 10:52:06.000 PM. No Event Sampling was used.
- Statistics:** The Statistics tab is selected, showing 248 events. The table includes columns: host, client, count, and url.
- Data:** One row from the table is shown: host: ubuntu, client: 172.16.0.60, count: 248, url: /validar?username=(SELECT (CASE WHEN (3800=2338) THEN 'admin' ELSE (SELECT 2338 UNION SELECT 8191) END))&password=admin. The URL contains numerous encoded SQL injection patterns.



# 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

## Save As Alert

### Settings

Title [T1190] - SQLinjection - Apache

Description Optional

Permissions Private Shared in App

Alert type Scheduled Real-time

Run on Cron Schedule ▾

Time Range Last 15 minutes ▾

Cron Expression \*/1 \* \* \* \*  
e.g. 00 08 \*\*\* (every day at 8PM). [Learn More](#)

Expires 24 hour(s) ▾

### Trigger Conditions

Trigger alert when Number of Results ▾

is greater than ▾ 0

Trigger Once For each result

Throttle ?

Suppress results  
containing field value  
host,client



# SQLINJECTION - REGRA

- Finalize o preenchimento e clique em “Save”



Suppress triggering for  hour(s) ▾

**Trigger Actions**

+ Add Actions ▾

When triggered

Severity

# 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.



A screenshot of a Splunk alert creation interface. A modal window titled "Alert has been saved" is displayed. It contains a warning message: "⚠ This scheduled search will not run after the Splunk Enterprise Trial License expires." Below the message, it says "You can view your alert, change additional settings, or continue editing it." Under "Additional Settings:", there is a link to "Permissions". At the bottom right of the modal are two buttons: "Continue Editing" and "View Alert".

# SQLINJECTION - TESTE DE EFETIVIDADE

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

```
root@ubuntu:/home/ubuntu# sqlmap -u "http://10.0.1.101/validar?username=admin&password=admin"
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 18:14:30 /2023-05-25

[18:14:30] [INFO] testing connection to the target URL
[18:14:30] [INFO] testing if the target URL content is stable
[18:14:31] [INFO] target URL content is stable
[18:14:31] [INFO] testing if GET parameter 'username' is dynamic
[18:14:31] [WARNING] GET parameter 'username' does not appear to be dynamic
[18:14:31] [WARNING] heuristic (basic) test shows that GET parameter 'username' might not be injectable
[18:14:31] [INFO] testing for SQL injection on GET parameter 'username'
[18:14:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:14:31] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:14:31] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:14:31] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:14:31] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[18:14:32] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:14:32] [INFO] testing 'Generic inline queries'
[18:14:32] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:14:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:14:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:14:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:14:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:14:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:14:32] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] n
```



splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity Help Filter Show

App Search & Reporting (search) ▾ Owner Administrator (admin) ▾ Severity All ▾ Alert All ▾

«Prev Next»

|                          | Time ▾                                | Fired alerts ▾                                    | App    | Type ▾    | Severity ▾ | Mode ▾     | Actions                                                    |
|--------------------------|---------------------------------------|---------------------------------------------------|--------|-----------|------------|------------|------------------------------------------------------------|
| <input type="checkbox"/> | 2023-05-25 23:03:00 GMT Daylight Time | [T1190] - SQLinjection - Apache                   | search | Scheduled | Medium     | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a> |
| <input type="checkbox"/> | 2023-05-25 21:55:01 GMT Daylight Time | [T1110] Brute Forte - Diretorios e Arquivos - Web | search | Scheduled | Medium     | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a> |
| <input type="checkbox"/> | 2023-05-25 21:26:00 GMT Daylight Time | [T1110] - Brute Force - Windows                   | search | Scheduled | Medium     | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a> |
| <input type="checkbox"/> | 2023-05-25 21:07:00 GMT Daylight Time | [T1110] - Brute Force - Linux                     | search | Scheduled | Medium     | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a> |
| <input type="checkbox"/> | 2023-05-25 20:37:00 GMT Daylight Time | [T1046] - Scan de portas - pfsense                | search | Scheduled | Medium     | Per Result | <a href="#">View results</a>   <a href="#">Edit search</a> |

SECURITY  
EVERY DAY

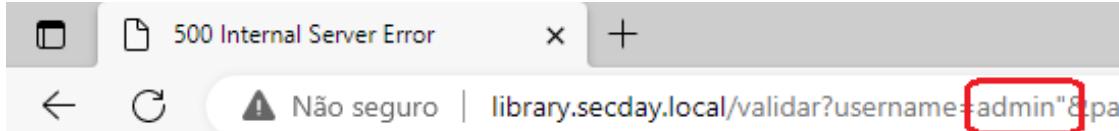
# SQLINJECTION - TESTE DE EFETIVIDADE

- 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.





## Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

## 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

>Login - SECDAY LIBRARY

Usuário  
admin" OR 1=1 ---

Senha  
.....

Entrar



- 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

>Login - SECDAY LIBRARY

Usuário  
admin" OR 1=1 ---

Senha  
.....

Entrar



- 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

Não seguro | library.secday.local/books

## SECDAY LIBRARY

**Treinamento - Splunk Básico**  
Autor: Kelvem Sousa  
Este curso prático tem como foco apresentar a ferramenta Splunk e ensinar os conceitos básicos necessários para aproveitar ao máximo suas funcionalidades poderosas na análise de dados voltado para segurança da informação.

**Video - SQL Injection (Ataque, monitoração e prevenção)**  
Autor: Kelvem Sousa  
O vídeo aborda uma das vulnerabilidades mais comuns em aplicações web: a injeção de SQL. Nele, você irá aprender o que é uma injeção de SQL, como ela pode ser explorada por um invasor, como detectar e monitorar esse tipo de ataque e, principalmente, como se prevenir contra ele. Serão apresentados exemplos práticos de como realizar uma injeção de SQL e como evitá-la, tornando seu sistema mais seguro.

**Artigo - Detecção de port forwarding SSH**  
Autor: Kelvem Sousa  
O encaminhamento de portas SSH (MITRE ATT&CK - Remote Services: SSH) é uma das principais técnicas utilizadas para movimentação lateral em hosts Linux, basicamente, você pode encaminhar qualquer porta TCP e tráfego através de uma conexão SSH segura.

- 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



The screenshot shows a Splunk search results page. At the top, there is a search bar containing a complex regex query for identifying SQL injection attempts. Below the search bar, a message indicates 1 event found between May 26, 2023, at 2:37:17 PM and 2:52:17 PM. The event details are as follows:

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

The page also features a "SECURITY EVERY DAY" logo in the top right corner.

```
index=* sourcetype="apache:access:combined" | regex url="(\%27)|(--)|(\%22)|(UNION)|(\%3D)|(%)|(\%2F*)|(*/)|(\<\>)|(\<\!=\>)|(AND)|(OR)|(NOT)|(SELECT)|(UPC)|(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 defensiva;
  - 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!