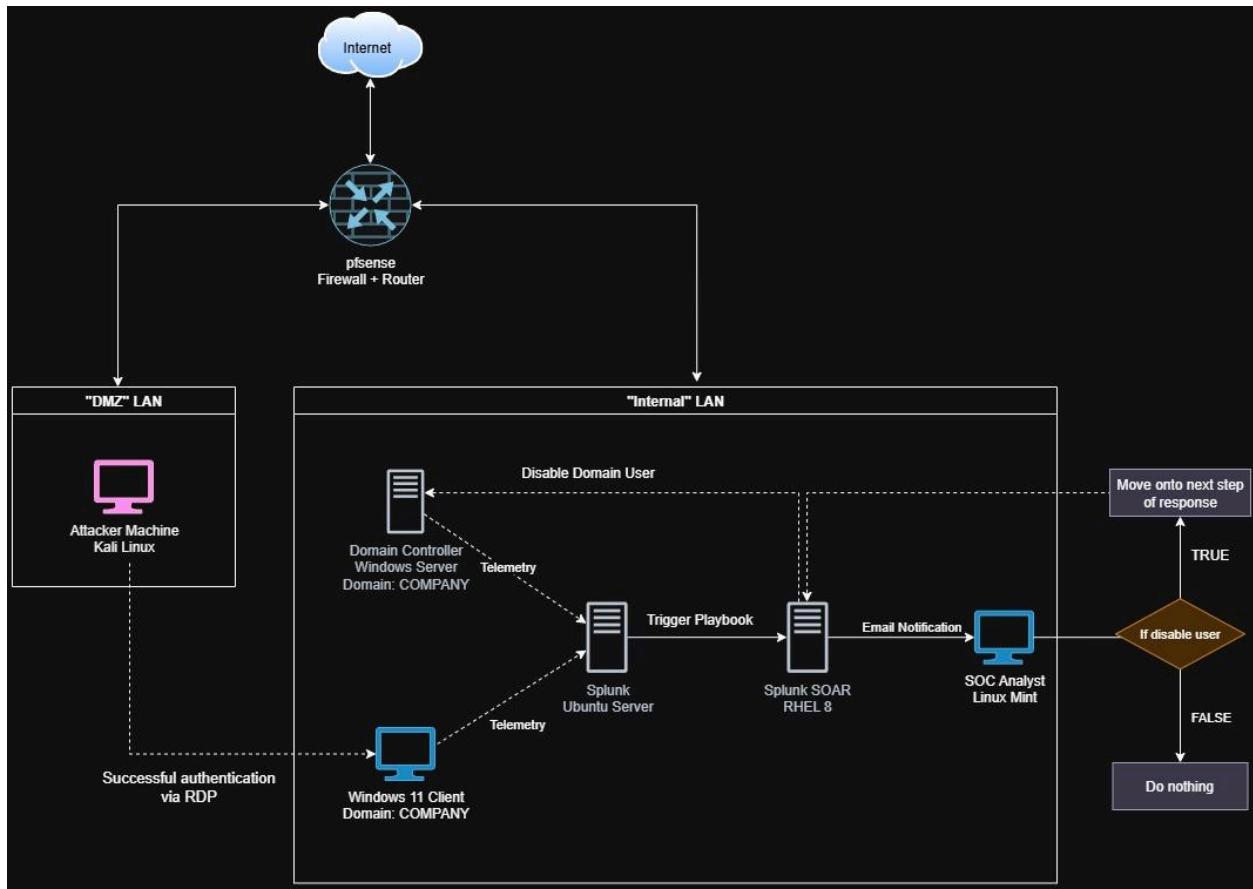


Active Directory + Splunk + SOAR

Diagram:



Playbook:

- The SOC Analyst will receive an email notification with information about the alert that was gathered from Splunk
- The Analyst can choose to either say YES, which will then move onto disabling the domain user account in Active Directory, or say NO, which will disregard the alert

Setup:

- Splunk Ubuntu Server
- Windows Server 2022 Domain Controller
- Attacker Kali Linux Machine (overkill)
- Windows 11 Client (overkill)
- RHEL 8 Server to host Splunk SOAR [Splunk SOAR Free Trial | Splunk](#)
- Linux Mint machine to access Splunk Logs. This will be the SOC Analyst computer
- pfSense for FW

kyle-splunk	kyle-kalilinux
Guest OS	Ubuntu Linux (64-bit)
Compatibility	ESXi 7.0 U2 virtual machine
VMware Tools	Yes
CPU	4
Memory	8 GB
Host name	ubuntu-server
kyle-winserver	kyle-win11client
Guest OS	Microsoft Windows Server 2022...
Compatibility	ESXi 7.0 U2 virtual machine
VMware Tools	No
CPU	2
Memory	8 GB
kyle-splunkSOAR	kyle-soc
Guest OS	Red Hat Enterprise Linux 8 (64-bit)
Compatibility	ESXi 7.0 U2 virtual machine
VMware Tools	No
CPU	2
Memory	8 GB
kyle-fw	
Guest OS	Other (64-bit)
Compatibility	ESXi 7.0 U2 virtual machine
VMware Tools	No
CPU	2
Memory	2 GB

IP Addresses: Setting up all in Private network

192.168.15.1 & 10.10.10.1 - pfSense

192.168.15.8 - Splunk SOAR

192.168.15.9 - splunk-server

192.168.15.10 - AD01 (Windows DC)

192.168.15.11 - Win11Client

192.168.15.12 - SOC Analyst

10.10.10.10 - Kali Linux

Weird issue with Ubuntu setup:

Wasn't showing my IPv4 nor IPv6 address

Fix: Turn the NICs on and Create and set the network config file

```
sudo ip link set ens192 up
```

```
sudo nano /etc/netplan/01-netcfg.yaml
```

```
network:
```

```
  version: 2
```

```
  renderer: networkd
```

```
  ethernets:
```

```
    ens192: # External Line
```

```
      dhcp4: true
```

```
    ens224: # LAN w/ AD01 and Win11Client
```

```
      dhcp4: false
```

```
      addresses:
```

```
        - 192.168.15.9/24 # Static IP for the Splunk Server
```

```
  nameservers:
```

```
    addresses:
```

```
      - 192.168.15.10 # DNS server, which would be the DC since it's able to resolve names
```

```
sudo netplan apply
```

- then try pinging 8.8.8.8

- Now we can do sudo apt-get update && sudo apt-get upgrade -y

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens192: # External line
      dhcp4: true

    ens224: # LAN
      dhcp4: false
      addresses:
        - 192.168.15.9/24
    nameservers:
      addresses:
        - 192.168.15.10
```

Another weird issue:

Splunk-Server and AD01 are unable to ping Win11Client, but win11Client can ping both the Splunk-Server and AD01

Culprit: probably a firewall issue, it's blocking ICMPv4 inbound traffic so outside devices can't reach this one

Type the following in powershell:

```
netsh advfirewall firewall add rule name="Allow ICMPv4 In" protocol=icmpv4:8,any dir=in action=allow
```

Finally Splunk-Server is able to communicate to Win11Client (192.168.15.11) and AD01 (192.168.15.10), and the other two devices can communicate to each other and the splunk-server now.

```
splunk@splunk-server:~$ ping 192.168.15.11
PING 192.168.15.11 (192.168.15.11) 56(84) bytes of data.
64 bytes from 192.168.15.11: icmp_seq=1 ttl=128 time=0.711 ms
64 bytes from 192.168.15.11: icmp_seq=2 ttl=128 time=0.548 ms
64 bytes from 192.168.15.11: icmp_seq=3 ttl=128 time=0.665 ms
^C
--- 192.168.15.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.548/0.641/0.711/0.068 ms
splunk@splunk-server:~$ ping 192.168.15.10
PING 192.168.15.10 (192.168.15.10) 56(84) bytes of data.
64 bytes from 192.168.15.10: icmp_seq=1 ttl=128 time=0.513 ms
64 bytes from 192.168.15.10: icmp_seq=2 ttl=128 time=0.618 ms
64 bytes from 192.168.15.10: icmp_seq=3 ttl=128 time=0.648 ms
64 bytes from 192.168.15.10: icmp_seq=4 ttl=128 time=0.551 ms
^C
--- 192.168.15.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.513/0.582/0.648/0.053 ms
splunk@splunk-server:~$
```

Next step: Create a domain, create an account that is going to be compromised, and join Win11client to the domain so that you can login with the compromised account

Setup of Windows Server:

- Add “Active Directory Domain Services” role and complete the flagged items
- Created a domain called company.local w/ the NetBIOS of COMPANY

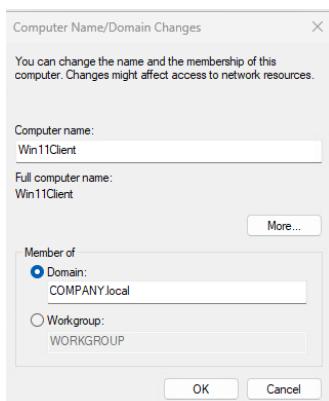
PROPERTIES For AD01			
Computer name	AD01	Last installed updates	Never
Domain	company.local	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Never
Microsoft Defender Firewall	Public: On	Microsoft Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet0	192.168.15.10, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2022 Standard	Processors	Intel(R) Xeon(R) Silver 4210R CPU @ 2.40GHz, Intel(R)
Hardware information	VMware, Inc. VMware7.1	Installed memory (RAM)	8 GB
		Total disk space	49.32 GB

Create a new user “John Doe” in ADUC under Users

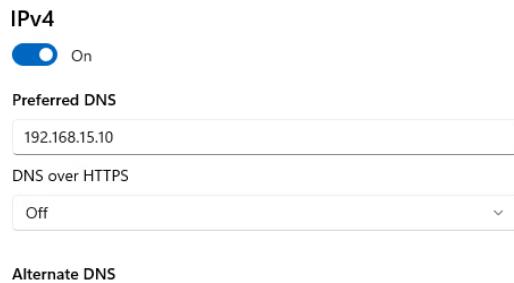
The screenshot shows the Active Directory Users and Computers (ADUC) interface. On the left, the navigation pane shows the tree structure: Active Directory Users and Computers [A] > company.local > Users. A 'New Object - User' dialog box is open over the main list. The dialog has fields for First name (John), Last name (Doe), and Full name (John Doe). Under User logon name, 'john.doe' is entered in the text box, with '@company.local' selected in the dropdown. Below that, the User logon name (pre-Windows 2000) field contains 'COMPANY\john.doe'. At the bottom right of the dialog are buttons for < Back, Next >, and Cancel.

The screenshot shows the list of users in the Active Directory. The user 'John Doe' is highlighted in blue. Other users listed include Guest, Key Admins, Protected Users, RAS and IAS Servers, Read-only Domain..., and Schema Admins. The 'John Doe' entry shows it is a User account from the company.local domain.

On the Win11Client, go to Advanced System Settings, then join to the COMPANY domain

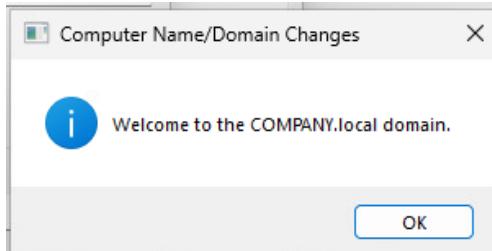


- You will run into an issue when trying to join to a domain and it can't resolve the name. This is a DNS issue
 - the fix for it is to make sure that in your IPv4 Network properties, you set AD01's IP address as your DNS since AD01 has the DNS role configured

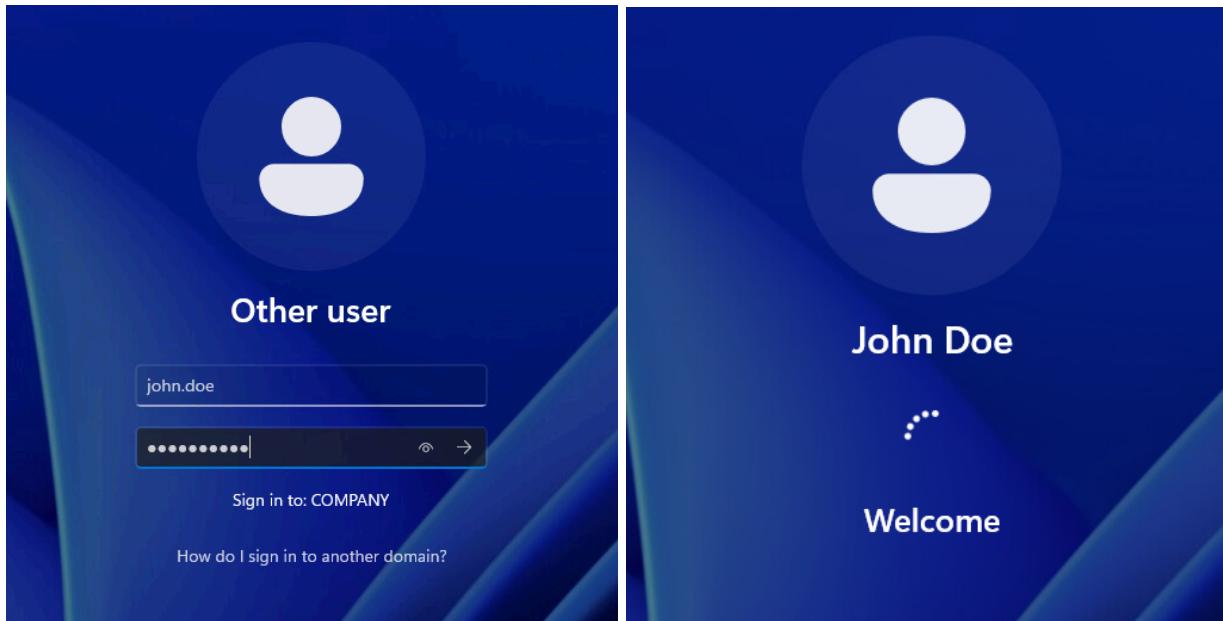


- If you want to be able to use the internet, set the DNS as 8.8.8.8 and as an alternate, set the AD01 DNS server

Win11Client has now been joined to the domain



You should now be able to sign into the computer with the “John Doe” credentials



Next step: Install & Configure Splunk, send Telemetry from Windows to Splunk and Create Splunk Alerts

- We will be using Splunk Universal Forwarder on anything sending telemetry to Splunk server
 - Why we need it:
You need UF when you're **collecting logs from remote systems**
Event logs, syslogs, application logs
You want lightweight, secure, and efficient forwarding
UF uses minimal CPU/memory and it's secure (encrypted via SSL)
Source machine doesn't allow Splunk Enterprise installation

To download Splunk Server: Go to [Splunk Enterprise Free Trial | Splunk](#) and copy the wget link for .deb (since Ubuntu is a debian based linux distro)

Also download the [Download Universal Forwarder for Remote Data Collection | Splunk](#) to download the Universal Forwarder to forward (collect and send machine data) to the Splunk server

Splunk Enterprise 9.4.3

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Platform	File Type	Size	Action			
Windows						
Linux						
Mac OS						
64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.tgz	1181.57 MB	Download Now	Copy wget link	More ▾
		.deb	894.53 MB	Download Now	Copy wget link	More ▾
		.rpm	1193.12 MB	Download Now		More ▾

Run the wget command. Then run the following:

```
splunk@splunk-server:~$ sudo dpkg -i splunk-9.4.3-237ebbd22314-linux-amd64.deb
[sudo] password for splunk:
Selecting previously unselected package splunk.
(Reading database ... 124908 files and directories currently installed.)
Preparing to unpack splunk-9.4.3-237ebbd22314-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.3) ...
Setting up splunk (9.4.3) ...
complete
splunk@splunk-server:~$
```

Change directory to /opt/splunk/bin and start splunk by doing ./splunk start:

```

splunk@splunk-server:~$ cd /opt/splunk
splunk@splunk-server:/opt/splunk$ ls
bin      etc      include  license-eula.txt  openssl  quarantined_files  share          swidtag
copyright.txt  ftr    lib     LICENSE.txt    opt      README-splunk.txt  splunk-9.4.3-237ebbd22314-linux-amd64-manifest
splunk@splunk-server:/opt/splunk$ cd bin
splunk@splunk-server:/opt/splunk/bin$ ls
2to3-3.7           fill_summary_index.py  mongod-4.4          prichunkpng  rapidDiag
2to3-3.9           genAuditKeys.py       mongod-5.0          priforgepng  recover-metadata
bloom              gemRootCA.sh        mongod-6.0          prigeypng   rest_handler.py
bottle.py          gensignedServerCert.py mongod-7.0          pripalpng   rsync
bttool             genSignedServerCert.sh mongodump          pripaintopng  rsync-ssl
btprobe            genKebCert.py       mongod_upgrade      pripongtopan runScript.py
bzip2              genKebCert.sh       mongorestore      pripongtopan S3benchmark
classify           idle3              noah_self_storage_archiver.py priueavepng  safe_restart_cluster_master.py
ColdStorageArchiver_GCP.py  idle3.7        node              pydoc3       scripts
ColdStorageArchiver.py   idle3.9        openssl          pydoc3.7    scrubber.py
coldToFrozenExample.py importtool       parse_xml_buckets.py pydoc3.9    searchtest
comsup              installit.py       pcre2-config      python       setsplunkEnv
copyright.txt       jars              pcregtest        python3     shc_upgrade_template.py
dbmanipulator.py    jsmn             pid_check.sh      python3.7   signtool
etc                locktest         pip               python3.7m  slim
etcctl             locktool         pip3             python3.9   spl2-orchestrator
etcutil            mongod          pip3.7           pyenv       spl-lang-server-sockets
exporttool          mongod-4.2       pip3.9           pyenv-3.7  splunk
splunk@splunk-server:/opt/splunk/bin$ ./splunk start

```

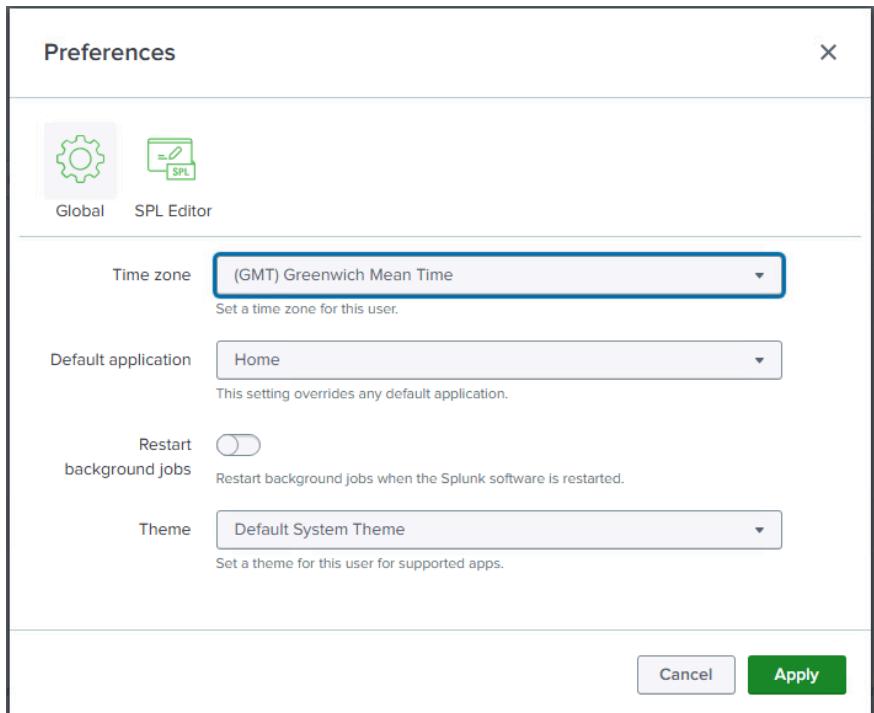
Agree with the terms and assign a username and password:

- Now I am able to access the private IP 192.168.15.9:8000 in my web browser (within the LAN and see the splunk interface)

Splunk Server configuration:

The screenshot shows the Splunk Enterprise home page for an administrator. At the top, there's a navigation bar with links for Home page settings, Find more apps, Manage, and a search bar. Below the navigation, there are several sections:

- Bookmarks:** A list of bookmarks categorized under "My bookmarks" (0), "Shared with my organization" (0), and "Shared by me".
- Shared with my organization:** A section showing items shared by other administrators.
- Splunk recommended (13):** A grid of common tasks:
 - Add data: Add data from a variety of common sources.
 - Search your data: Turn data into doing with Splunk search.
 - Visualize your data: Create dashboards that work for your data.
 - Add team members: Add your team members to Splunk platform.
 - Manage permissions: Control who has access with roles.
 - Configure mobile devices: Login or manage mobile devices using Splunk Secure Gateway.
- Learning & resources:** Links to Product tours, Learn more with Splunk Docs, Get help from Splunk experts, and Extend your capabilities.



The screenshot shows the Splunk App Store interface. A red arrow points to the search bar, which contains the text 'Windows'. Below the search bar is a 'CATEGORY' sidebar with various options like IT Operations, Security, Fraud & Compliance, etc. The main area displays search results for 'Windows', showing 73 apps. One result is highlighted with a red box: 'Splunk Add-on for Microsoft Windows'. The listing includes a green 'Install' button, a note about upgrade instructions, and details about the app's category, author, and release date.

Why do we need this add-on?

- **It's pretty much necessary** since it'll parse raw Windows Event logs and provide us with field extractions and tagging for event logs like
 - Security, System, Application, Setup, Forwarded Events
 - (basically makes Windows logs readable to Splunk and easier to manage)
- The add-on normalizes Windows data to something standard to Splunk and gives you useful fields off the rip
- If installed on Universal Forwarders, it can configure
 - WinEventLog collection
 - Windows performance counters
 - Registry monitoring

- WMI data collection

Create a new index:

- Why?
 - An index is a data repository where events are stored and is the first layer of separation for managing, searching, and securing data
 - Helps separate data within an org and improve security via access controls, apply data retention policies for individual indexes, and improve search performance, and aid in troubleshooting
- How?
 - Settings -> Indexes -> New Index

New Index

General Settings

Index Name: company-ad
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events Metrics

Home Path: optional
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable Disable

Max Size of Entire Index: 500 GB

Max Size of Hot/Warm/Cold Bucket: auto GB

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting

Storage Optimization

Tsidx Retention Policy: Enable Reduction Disable Reduction

Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More](#)

Save Cancel

Configure Forwarding and receiving

- You will need to configure the splunk server to receive data (basically identify the port that it listens from)
- Settings -> Forwarding and receiving -> Receive data (Configure receiving + Add new)

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

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.

- This is done on the Splunk side, **however** if the Splunk-server (ubuntu) itself has the firewall turned off, you'll need to turn it on to allow for traffic to come through that port

- `sudo ufw allow 9997`

```
splunk@splunk-server:/opt/splunk/bin$ ufw allow 9997
ERROR: You need to be root to run this script
splunk@splunk-server:/opt/splunk/bin$ sudo allow 9997
[sudo] password for splunk:
sudo: allow: command not found
splunk@splunk-server:/opt/splunk/bin$ sudo ufw allow 9997
Rules updated
Rules updated (v6)
splunk@splunk-server:/opt/splunk/bin$
```

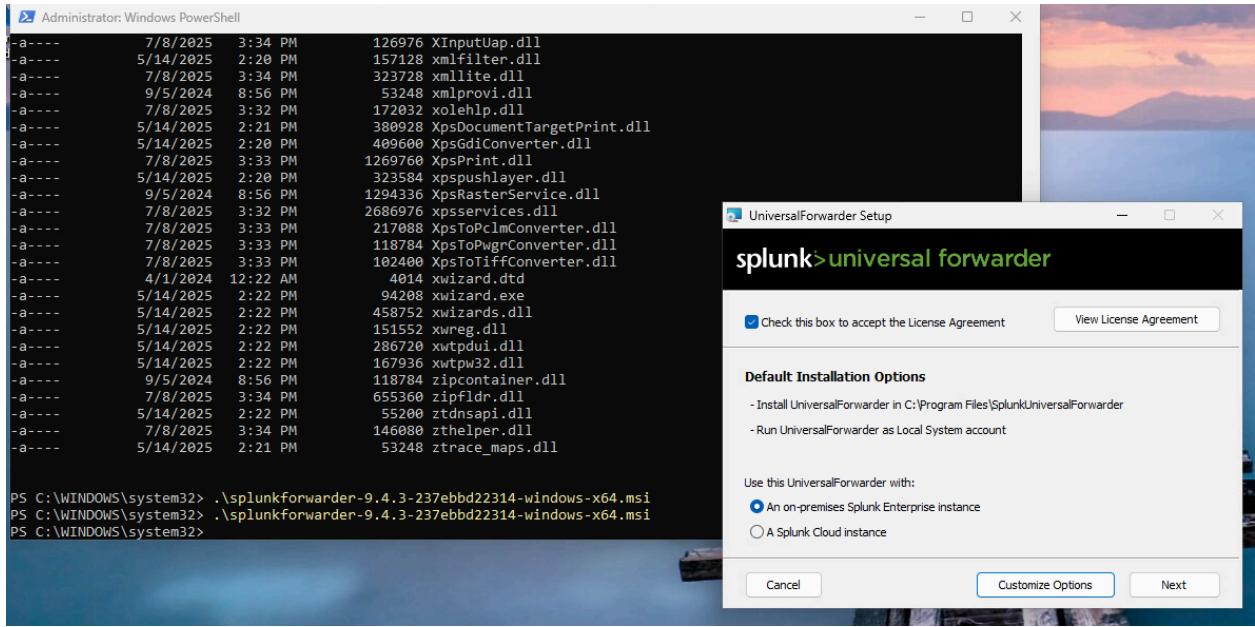
Splunk Universal Forwarder 9.4.3

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

Windows	Linux	Mac OS	FreeBSD	Solaris	AIX
32-bit	Windows 10	.msi	64.86 MB	Download Now	Copy wget link
64-bit	Windows 10, 11 Windows Server 2019, 2022, 2025	.msi	185.02 MB	Download Now	Copy wget link

- For some reason, Splunk UF is considered a “malicious download” to I will be installing using the wget link on the endpoints
 - `wget -O splunkforwarder-9.4.3-237ebbd22314-windows-x64.msi "https://download.splunk.com/products/universalforwarder/releases/9.4.3/windows/splunkforwarder-9.4.3-237ebbd22314-windows-x64.msi"`

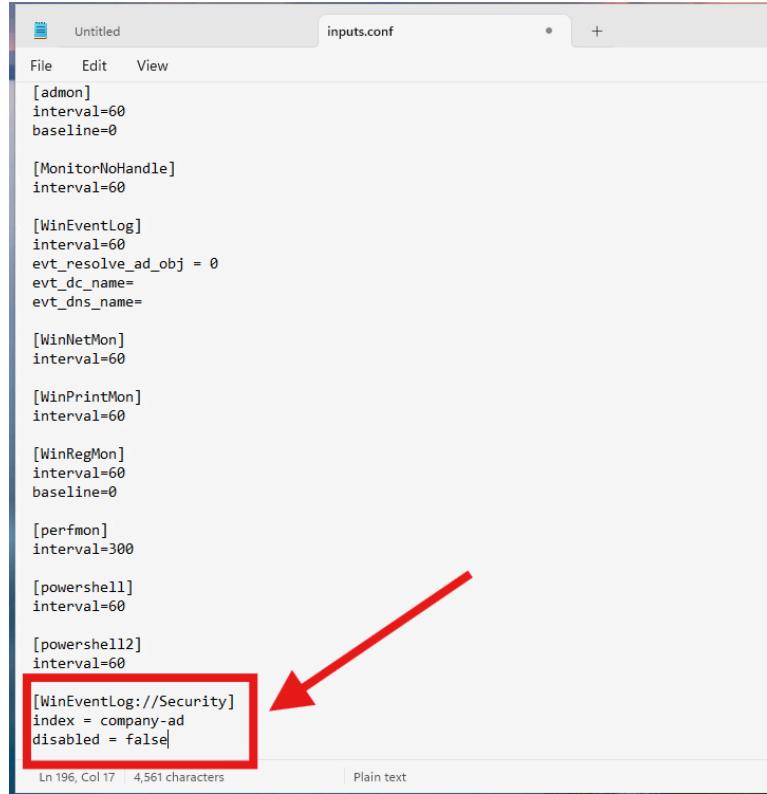


No Deployment Server so no need to fill out. But we DO have a Receiving Indexer, which is our Splunk server (it receives the info and indexes em)

- 192.168.15.9:9997

Once we finish downloading Universal Forwarder, we'll need to edit the **inputs.conf** file in the path: **C:\Program Files\SplunkUniversalForwarder\etc\system\local**.

- It may not be there by default, so you can go to **C:\Program Files\SplunkUniversalForwarder\etc\system\default** and copy the **inputs.conf** file from there and paste it into local (**You must do it as an administrator**)
- **Why do we need inputs.conf?**
 - This file tells the Universal Forwarder what data to collect (e.g. Windows Event Logs, file paths, perf counters)
 - Where it's coming from
 - How often to poll or monitor
 - Which index and sourcetype to tag the data with
 - In this case we want the one that we created earlier which is: **index=company-ad**
- After pasting **inputs.conf** into local, open notepad as **Administrator** and open the **inputs.conf** file (Change the extension search to All files to find **inputs.conf**)
 - You will need to do this since you won't have sufficient permissions with a standard account if you want to edit the conf file



```

Untitled           inputs.conf
File   Edit   View
[admon]
interval=60
baseline=0

[MonitorNoHandle]
interval=60

[WinEventLog]
interval=60
evt_resolve_ad_obj = 0
evt_dc_name=
evt_dns_name=

[WinNetMon]
interval=60

[WinPrintMon]
interval=60

[WinRegMon]
interval=60
baseline=0

[perfmon]
interval=300

[powershell]
interval=60

[powershell12]
interval=60

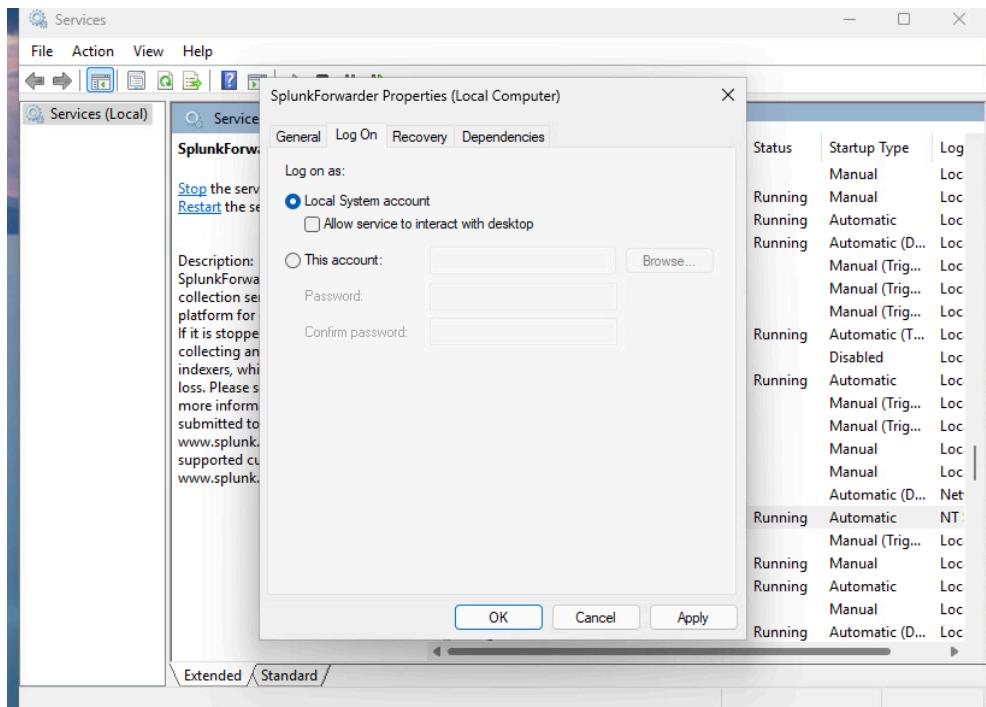
[WinEventLog://Security]
index = company-ad
disabled = false

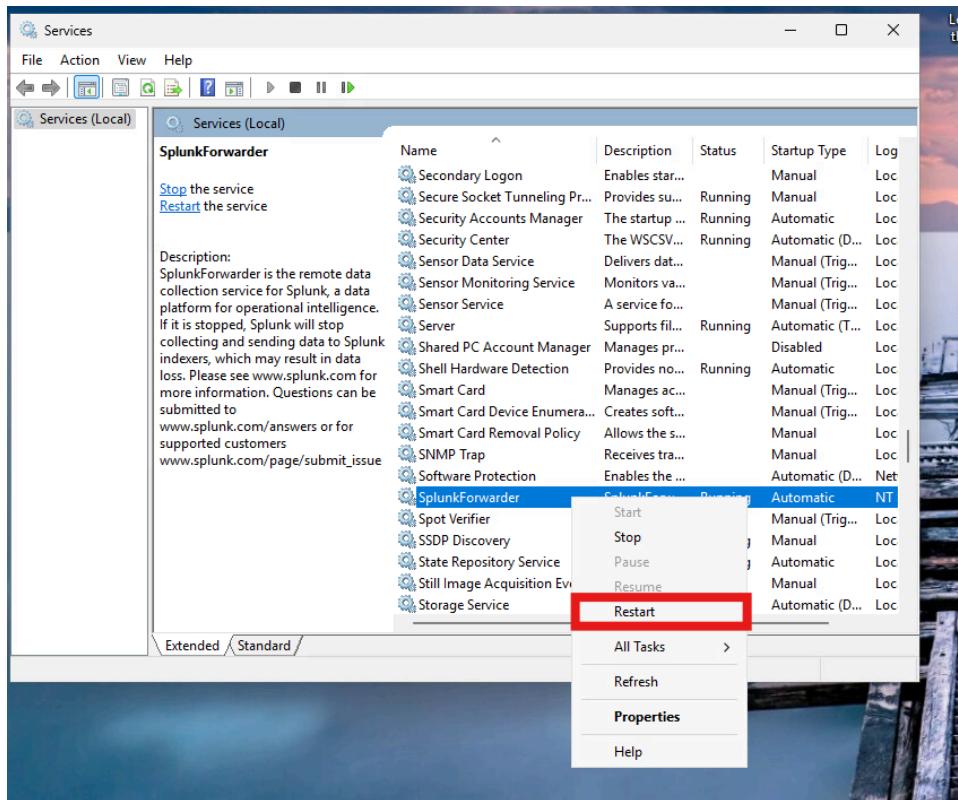
```

Ln 196, Col 17 | 4,561 characters Plain text

Now that the input.conf file is configured to send Windows Security Events to the index company-ad, we can now restart the Splunk UF service:

- First, change the SplunkForwarder properties to log on as the Local System Account:
 - This is because local accounts have full access to Event logs, Registry
 - And **doesn't require domain credentials to run the service**





Repeat steps for the Domain Controller.

The screenshot shows a Windows PowerShell window and the Windows Services snap-in. The PowerShell window displays the following commands:

```

PS C:\Users\Administrator> wget -O splunkforwarder-9.4.3-237ebbd22314-windows-x64.msi https://aka.ms/cnts/universalforwarder/releases/9.4.3/windows/splunkforwarder-9.4.3-237ebbd22314
PS C:\Users\Administrator> is

Directory: C:\Users\Administrator

Mode LastWriteTime      Length Name
---- -----          ---- 
d-r-- 5/1/2025 9:41 PM    30 Objects
d-r-- 5/1/2025 9:41 PM   Contacts
d-r-- 5/1/2025 9:41 PM   Desktop
d-r-- 5/1/2025 9:41 PM  Documents
d-r-- 5/1/2025 9:41 PM  Downloads
d-r-- 5/1/2025 9:41 PM Favorites
d-r-- 5/1/2025 9:41 PM  Links
d-r-- 5/1/2025 9:41 PM  Music
d-r-- 5/1/2025 9:41 PM  Pictures
d-r-- 5/1/2025 9:41 PM  Saved Games
d-r-- 5/1/2025 9:41 PM  Searches
d-r-- 5/1/2025 9:41 PM  Videos
-a--- 7/10/2025 7:57 PM 194002944 splunkforwarder-9.4.3-237ebbd22314

PS C:\Users\Administrator> .\splunkforwarder-9.4.3-237ebbd22314-windows-x64.msi
PS C:\Users\Administrator>

```

The Services snap-in shows the 'SplunkForwarder' service is running. The context menu for the service is open, and the 'Restart' option is highlighted with a red box. The menu also includes options like Stop, Pause, Resume, and a separator line followed by All Tasks, Refresh, Properties, and Help.

Now that the Splunk Receiving Indexer is set up (Splunk-server) and the Universal Forwarder is set up on the Windows machines, we can see telemetry being sent over to the Splunk server.

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

- Search Bar:** index=company-ad
- Time Range:** 7/09/25 8:00:00.000 AM to 7/10/25 3:23:08.000 AM
- Event Count:** 3,861
- Selected Fields:** host, source, sourcetype
- Interesting Fields:** Account_Domain, Account_Name, action, app, body, category, ComputerName, dest, dest_nt_domain, dest_nt_host, dvc, dvc_nt_host, Error_Code
- Events List:** The list shows three events from different hosts:
 - host = WIN11CLIENT | source = WinEventLog:Security | sourcetype = WinEventLog
 - host = WIN11CLIENT | source = WinEventLog:Security | sourcetype = WinEventLog
 - host = WIN11CLIENT | source = WinEventLog:Security | sourcetype = WinEventLog

You can see that logs are being forwarded from both devices (AD01 & Win11Client) since there are logs from 2 hosts in Splunk:

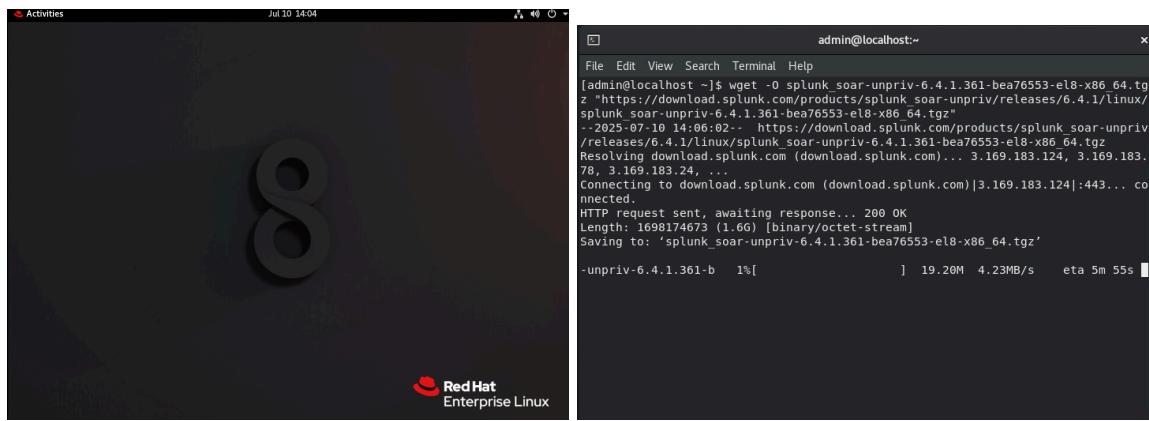
- If not, make sure that the service is running and outputs.conf has the right configurations. Also make sure that it is on the same LAN as the Splunk server

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

- Search Bar:** index=company-ad
- Event Count:** 5,177 events (7/9/25 8:00:00.000 PM to 7/10/25 8:57:10.000 PM)
- Selected Fields:** host, source, sourcetype
- Interesting Fields:** Account_Domain, Account_Name, action, app, body, category, ComputerName, dest, dest_nt_domain, dest_nt_host, dvc, dvc_nt_host, Error_Code
- Events List:** A summary bar indicates 2 Values, 100% of events.
- Host Distribution Modal:** A modal window titled "host" shows the distribution of events by host:

host	Count	%
AD01	3,104	59.958%
WIN11CLIENT	2,073	40.042%

RHEL 8 environment:



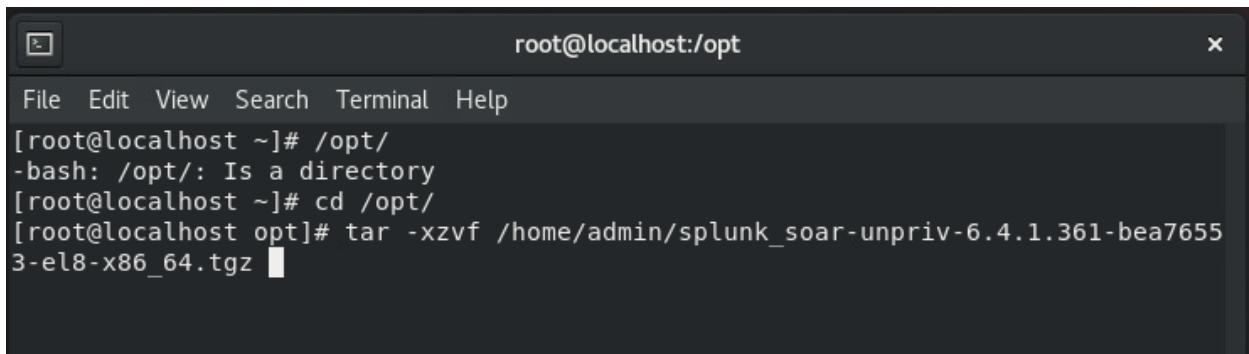
- You will need to do a yum update and yum upgrade **AND you will need to register the system with your RedHat account** <https://www.redhat.com/>

Mint Environment:

A screenshot of a Linux Mint desktop environment. On the left is a dark desktop background with a white 'LM' logo. On the right is a password dialog box titled 'SOC Analyst' with the text 'Please enter your password...'. Below the desktop is a network configuration window titled 'Wired' for 'IPv4'. The 'IPv4' tab is selected. Under 'Addresses', the 'Manual' dropdown is chosen. The 'Address' field contains '192.168.15.12', 'Netmask' contains '255.255.255.0', and 'Gateway' is empty. There is a '+' button to add more entries. Under 'DNS', the 'Automatic' radio button is selected, and the 'Server' field contains '192.168.15.10'. At the bottom of the window are 'Cancel' and 'Apply' buttons.

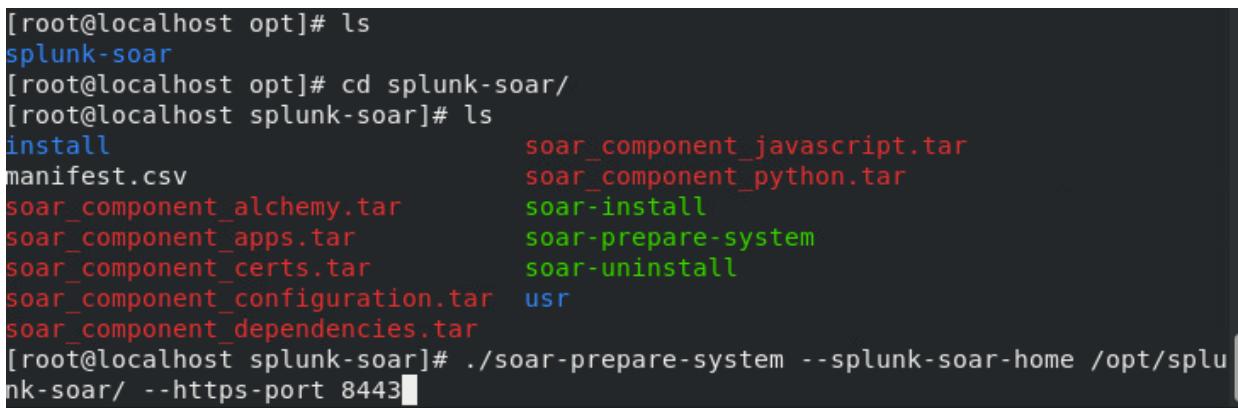
SOAR Setup: [Tutorial: Zero to Splunk SOAR \(in UNDER 10 Minutes\)](#)

can do sudo -i to stay in root



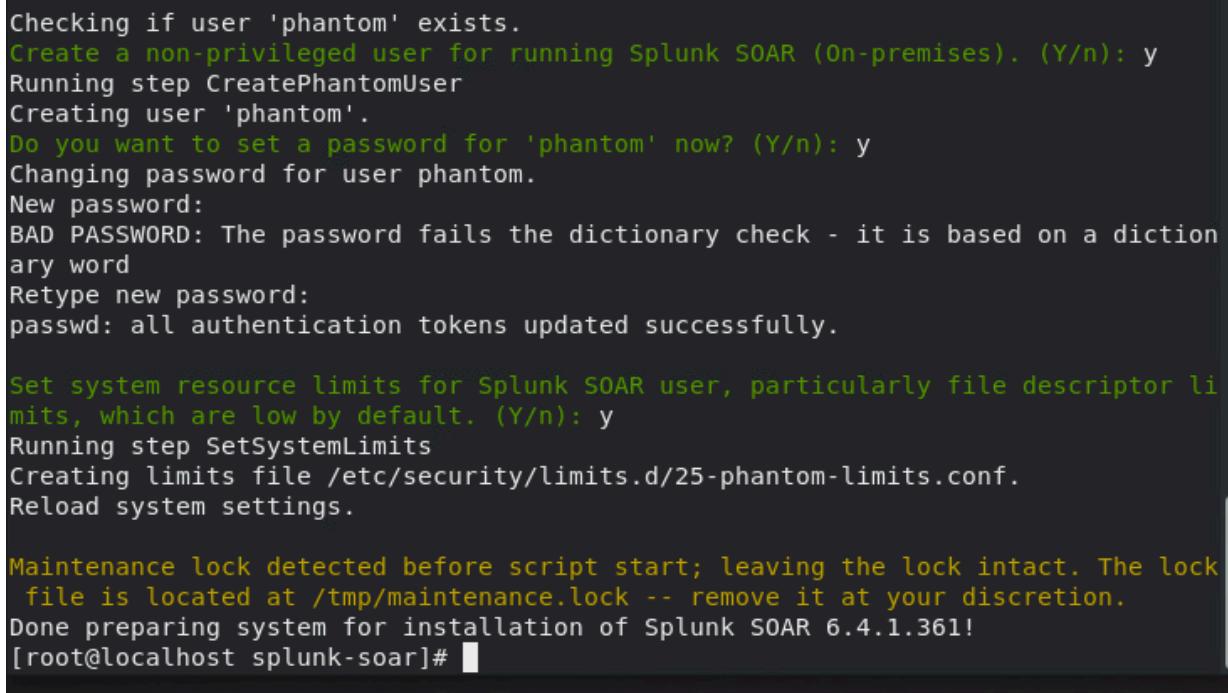
```
root@localhost:/opt
File Edit View Search Terminal Help
[root@localhost ~]# /opt/
-bash: /opt/: Is a directory
[root@localhost ~]# cd /opt/
[root@localhost opt]# tar -xzvf /home/admin/splunk_soar-unpriv-6.4.1.361-bea7655
3-el8-x86_64.tgz
```

Prepare the system:



```
[root@localhost opt]# ls
splunk-soar
[root@localhost opt]# cd splunk-soar/
[root@localhost splunk-soar]# ls
install                         soar_component_javascript.tar
manifest.csv                     soar_component_python.tar
soar_component_alchemy.tar      soar-install
soar_component_apps.tar         soar-prepare-system
soar_component_certs.tar        soar-uninstall
soar_component_configuration.tar usr
soar_component_dependencies.tar
[root@localhost splunk-soar]# ./soar-prepare-system --splunk-soar-home /opt/splunk-soar/ --https-port 8443
```

- This runs the system preparation script, sets the installation path of where SOAR will live on RHEL, and optionally setting the HTTPS port used to connect to SOAR



```
Checking if user 'phantom' exists.
Create a non-privileged user for running Splunk SOAR (On-premises). (Y/n): y
Running step CreatePhantomUser
Creating user 'phantom'.
Do you want to set a password for 'phantom' now? (Y/n): y
Changing password for user phantom.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.

Set system resource limits for Splunk SOAR user, particularly file descriptor limits, which are low by default. (Y/n): y
Running step SetSystemLimits
Creating limits file /etc/security/limits.d/25-phantom-limits.conf.
Reload system settings.

Maintenance lock detected before script start; leaving the lock intact. The lock file is located at /tmp/maintenance.lock -- remove it at your discretion.
Done preparing system for installation of Splunk SOAR 6.4.1.361!
[root@localhost splunk-soar]#
```

- As part of the preparation script, it will also create the user “**phantom**” . This is important.

Now that the initial preparation for Splunk SOAR is setup, you will need to change the ownership of `splunk-soar` to the **phantom** user that was created.

Why?

- **phantom** service (Splunk SOAR) runs under the **phantom** user
- If the install directory is owned by root, the SOAR won’t be able to write logs, configurations, or data
 - You’ll also get permissions denied errors during runtime
- Changing ownership to **phantom** helps the SOAR service start and run as expected and have proper file permissions

```
Done preparing system for installation of Splunk SOAR 6.4.1.361!
[root@localhost splunk-soar]# cd /opt
[root@localhost opt]# ls
splunk-soar
[root@localhost opt]# chown phantom: splunk-soar/
[root@localhost opt]# ls -lah
total 4.0K
drwx----- 3 1337 1337 25 Jun 6 17:17 .
dr-xr-xr-x. 17 root root 224 Jul 10 13:51 ..
drwxr-xr-x. 5 phantom phantom 4.0K Jul 10 14:25 splunk-soar
[root@localhost opt]#
```

Now cd into `splunk-soar` and then switch user:

Switch user (su) from root to phantom by doing:

su phantom

- You won’t be able to traverse through the directory as phantom within /opt/ so you should add these permissions to the /opt directory
 - `chmod +x /opt`

```
[root@localhost ~]# cd /opt
[root@localhost opt]# chmod +x /opt
[root@localhost opt]# ls -lah
total 4.0K
drwx--x--x. 3 1337 1337 25 Jun 6 17:17 .
dr-xr-xr-x. 17 root root 224 Jul 10 13:51 ..
drwxr-xr-x. 5 phantom phantom 4.0K Jul 10 14:25 splunk-soar
[root@localhost opt]# su phantom
[phantom@localhost opt]$ cd splunk-soar/
[phantom@localhost splunk-soar]$ ls
install                      soar_component_javascript.tar
manifest.csv                  soar_component_python.tar
soar_component_alchemy.tar    soar-install
soar_component_apps.tar       soar-prepare-system
soar_component_certs.tar      soar-uninstall
soar_component_configuration.tar  usr
soar_component_dependencies.tar var
```

Now you can run the `soar-install`

- `./soar-install –splunk-soar-home /opt/splunk-soar/ –https-port 8443`

Now that the installation for SOAR is complete, you can switch over to the LAN and change the static IP for both the SOAR machine and the SOC machine

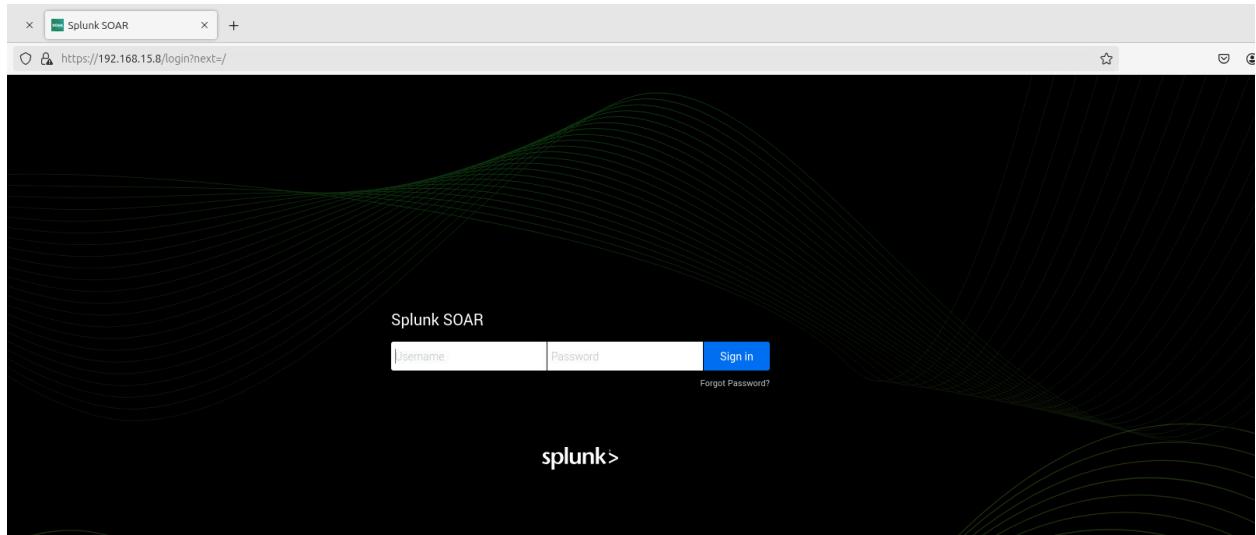
IP Addresses:

- Splunk SOAR: 192.168.15.8, Linux Mint: 192.168.15.12
- Make sure to set the DNS to the AD01
- Also make sure to change VMWare network adapter settings to “Lab-only” so that all devices are within the same lab and they are able to ping each other

Change directories into /opt/splunk-soar/bin and start up Splunk SOAR:

```
[phantom@localhost splunk-soar]$ cd bin
[phantom@localhost bin]$ ls
2to3                                phantom_decided
backup.pyc                            phantom_ingestd
clean_restart_scheduled.sh           phantom_supervisor
consul.sh                            phantom_watchdogd
create_output.pyc                     phantom_workflowd
create_tj.pyc                         phenv
enable_rabbitmq_management.pyc      phsev
engine_commands.py3                  prepare_db.pyc
extdb_backup_bootstrap.py          phantom.sh
ibackup.pyc                          recreate_local_db.pyc
import_cert.py                       repair_520_indicators.sh
initialize.py                        restore.pyc
init_watchdog                         run_daemon.sh
instsvcwini7                         setup_warm_standby.pyc
instsvcxp                           spawn3
is_clustering_enabled.pyc            spawn313
make_cluster_node.pyc                start_phantom.sh
make_server_node.pyc                 stop_daemon.sh
nginx                                stop_phantom.sh
pgbouncer                            uwsgi
phantom_actiond                      win
phantom_cluster                      wmic
[phantom@localhost bin]$ ./start_phantom.sh
grep -q /opt/phantom/etc/phantom.install.conf: No such file or directory
Starting all Splunk SOAR services
Starting Database server (PostgreSQL): [ OK ]
Starting Connection pooler (PgBouncer): [ OK ]
Checking daemon connectivity: [ OK ]
Checking component versions: [ OK ]
Starting Supervisord: [ OK ]
Starting Splunk SOAR daemons: [ OK ]
Checking Supervisord processes: [ OK ]
Starting Web application server (uwsgi): [ OK ]
Starting Web server (nginx): [ OK ]
Starting Embedded Universal Forwarder: [ OK ]
Starting Watchdog daemon: [ OK ]
Splunk SOAR startup successful
[phantom@localhost bin]$
```

Now in the SOC Analyst computer, you should be able to see the Splunk SOAR platform on the IP of the RHEL server (192.168.15.8):



Default login: `soar_local_admin`

Dashboard page:

The screenshot shows the Splunk SOAR Dashboard page. At the top, there are navigation tabs for 'Search | Splunk 9.4.3' and 'Splunk SOAR | Dashboard'. The main title is 'Automation ROI Summary' with a date range of '2025-07-04 - 2025-07-10'. Below this, there are six summary cards:

- Resolved events: 0
- Mean dwell time: 0m
- Mean time to resolve: 0m
- FTE Gained: 0.0
- Time saved: 0m
- Dollars saved: \$0

Below these cards are four status panels:

- Open**: Shows 'No Events are open'.
- Workload**: Shows 'Total Workload' of 0.
- Events by Status**: Shows 'No Data'.
- Top Playbooks and Actions**: Shows 'Top Playbooks' and 'Top Actions' with a link to 'All Categories'. It also lists 'Top Playbooks', 'Actions', 'Execute Time', and 'Executed'.

We will now set up the attacking method and circle back to Splunk and make sure that the attack is properly logged within Splunk.

Attacker Setup

For generating telemetry:

We want to have the Kali VM to be in a different VLAN/subnet than the “company” network (e.g. 10.10.10.0/24) and have an RDP connection from Linux to Windows.

- This will generate telemetry with the source IP 10.10.10.10, simulating that of an external attacker
- The use of private IP's simulates that of a corporate environment since attackers tend to sit on the DMZ systems (since firewalls/routers typically have NAT and translate public IP to private IP within the subnet)

To do this, I setup pfSense to route traffic between them but restrict/allow specific ports (in this case RDP);

- **This emulates an environment with weak firewall configurations / poorly segmented enterprise network that is allowing attackers to easily RDP.**
 - FW should restrict east-west and north-south traffic across VLANs
- Have a NIC in both subnets and route between them; allow RDP (TCP 3389) inbound In VMWare, you can add a port group

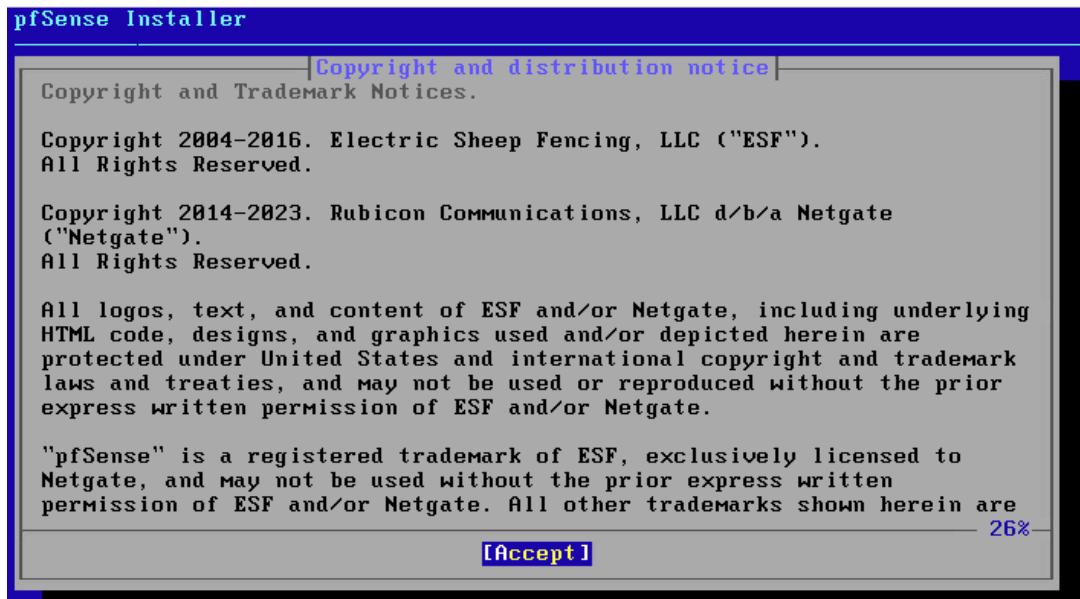
+ @ Add port group - Ports-DMZ

Name	Ports-DMZ
VLAN ID	0
Virtual switch	vSwitch-Lab-Only
> Security Click to expand	
CANCEL ADD	

pfSense setup:

- We want both subnets to route through the firewall to gain access to the internet
- We also want the firewall to control traffic between the Lab-Only and DMZ

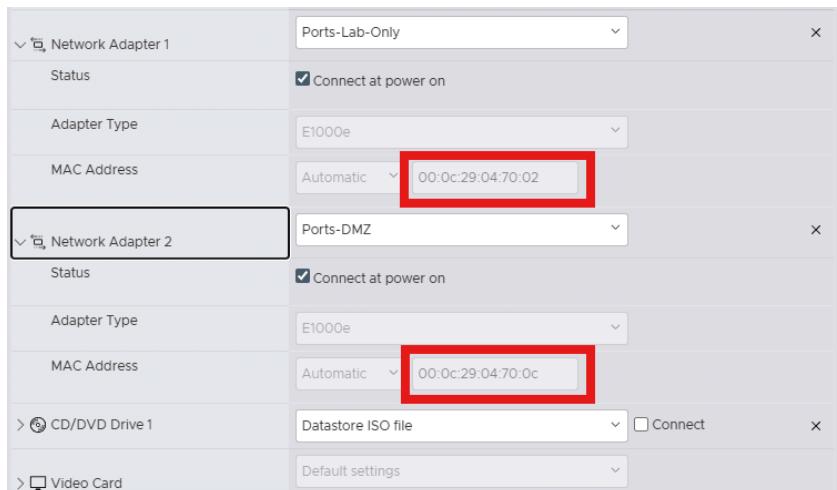
> Network Adapter 1	Ports-Lab-Only	<input checked="" type="checkbox"/> Connect	x
> Network Adapter 2	Ports-DMZ	<input checked="" type="checkbox"/> Connect	x
> Network Adapter 3	Ports-External	<input checked="" type="checkbox"/> Connect	x



There should be two adapters; em0 and em1. Hit “Shell” (Option 8) and do an ifconfig to see the MAC address:

```
[2.7.2-RELEASE][root@pfSense.home.apra]# ifconfig em0
em0: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu
1500
        options=4e100bb<RXCSUM,TXCSUM,ULAN_MTU,ULAN_HWTAGGING,JUMBO_MTU,ULAN_HWC
SUM,ULAN_HWFILTER,RXCSUM_IPV6,TXCSUM_IPV6,HWSTATS,MEXTPG>
        ether 00:0c:29:04:70:02
        inet 10.10.10.1 netmask 0xffffffff broadcast 10.10.10.255
        inet6 fe00::20c:29ff:fe04:7002%em0 prefixlen 64 scopeid 0x1
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
[2.7.2-RELEASE][root@pfSense.home.apra]# ifconfig em1
em1: flags=1008c02<BROADCAST,DRIVE_ACTIVE,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mt
1500
        options=4e120bb<RXCSUM,TXCSUM,ULAN_MTU,ULAN_HWTAGGING,JUMBO_MTU,ULAN_HWC
SUM,WOL_MAGIC,ULAN_HWFILTER,RXCSUM_IPV6,TXCSUM_IPV6,HWSTATS,MEXTPG>
        ether 00:0c:29:04:70:0c
        inet6 fe00::20c:29ff:fe04:700c%em1 prefixlen 64 tentative scopeid 0x2
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
[2.7.2-RELEASE][root@pfSense.home.apra]#
```

Then go to VMWare and look at the MAC Addresses:



Type exit to get back to the main menu, then Assign Interfaces to each NIC (Option 1). First set the external line to be the WAN:

```
kyle-fw
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em2

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em0 em1 a or nothing if finished): em0

Enter the Optional 1 interface name or 'a' for auto-detection
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN -> em2
LAN -> em0
OPT1 -> em1

Do you want to proceed [y\!n]?
```

From there, set the interface IP addresses and set it as static so that each subnet has a gateway (x.x.x.1) (Option 2): **You don't need to configure VLANs within pfSense because you already separated them within VMWare.**

- You only need to configure VLANs if everything is within the same physical switch and isn't managed by anything else other than pfSense.
- This is for the Lab-only VLAN/Port group:

```
The IPv4 LAN address has been set to 192.168.15.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://192.168.15.1/
```

- This is the full setup for the DMZ Port group:

```
The IPv4 OPT1 address has been set to 10.10.10.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.10.10.1/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: bb5efbc7e3ea4ba8b2c3

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em2      ->
LAN (lan)      -> em0      -> v4: 192.168.15.1/24
OPT1 (opt1)    -> em1      -> v4: 10.10.10.1/24
```

Now we test to see if we can access the pfSense web portal on a device in the main VLAN:

The screenshot shows the 'General Information' step of the pfSense Setup Wizard. The URL in the address bar is https://192.168.15.1/wizard.php?xml=setup_wizard.xml. The page title is 'Wizard / pfSense Setup / General Information'. A progress bar at the top indicates 'Step 2 of 9'. The 'General Information' section contains fields for Hostname ('firewall') and Domain ('company.firewall'), both with examples provided. It also includes a note about DNS resolution and manually configured DNS servers, with fields for Primary DNS Server ('192.168.15.10') and Secondary DNS Server. An 'Override DNS' checkbox is checked, with a note explaining it allows DNS servers to be overridden by DHCP/PPP on WAN. A blue 'Next' button is at the bottom.

To setup internet (WAN) for LAN devices: Set the gateways for the devices to the firewall IP (192.168.15.1) and set DHCP in pfsense on the WAN Interface:

The screenshot shows the 'General Configuration' screen for the WAN interface. The 'Enable' checkbox is checked. The 'Description' field is set to 'WAN'. The 'IPv4 Configuration Type' dropdown is set to 'DHCP'. The 'IPv6 Configuration Type' dropdown is set to 'None'. The 'MAC Address' field contains 'XXXX:XX:XXXX:XX' with a note about spoofing MAC addresses. The 'MTU' and 'MSS' fields have dropdown menus. The 'Speed and Duplex' dropdown is set to 'Default (no preference, typically autoselect)'. Below this, the 'DHCP Client Configuration' section has an 'Options' row with checkboxes for 'Advanced Configuration' and 'Configuration Override'. The 'Hostname' field is empty. A note at the bottom states: 'The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISDs may require this for client'.

Check the status of the interface (make sure that it is up):

WAN Interface (wan, em2)	
Status	up
DHCP	up Release WAN <input type="checkbox"/>
MAC Address	00:0c:29:04:70:16
IPv4 Address	192.148.1.172
Subnet mask IPv4	255.255.255.0
Gateway IPv4	192.148.1.1
IPv6 Link Local	fe80::20c:29ff:fe04:7016%em2
DNS servers	192.148.1.1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	393/444 (56 Kib/22 Kib)
In/out packets (pass)	393/444 (56 Kib/22 Kib)
In/out packets (block)	92/0 (11 Kib/0 B)
In/out errors	0/0
Collisions	0
Interrupts	1346 (1/s)

Then check Outbound NAT, since that is what will turn private IP's in public IP's:

The screenshot shows the pfSense interface under Firewall / NAT / Outbound. The "Outbound" tab is selected. Under "Outbound NAT Mode", the "Automatic outbound NAT rule generation" option is selected. In the "Mappings" section, there are two automatic rules listed:

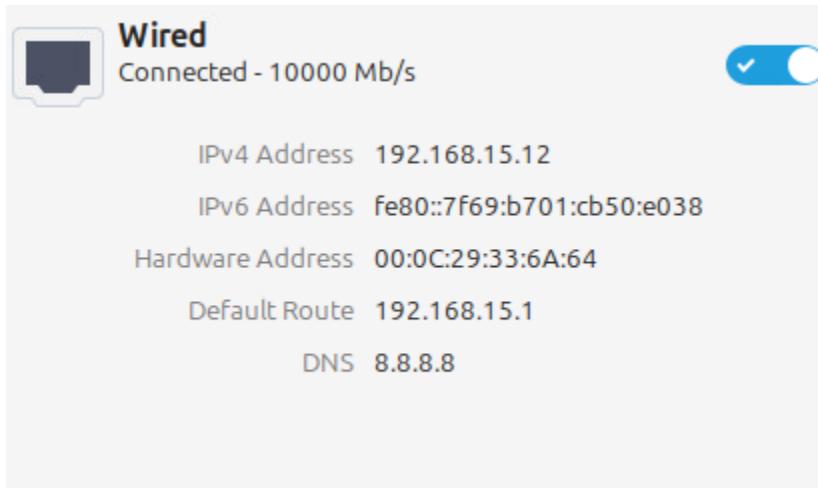
Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
WAN	127.0.0.0/8 :1/128	192.168.15.0/24 10.10.10.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
WAN	127.0.0.0/8 :1/128	192.168.15.0/24 10.10.10.0/24	*	*	*	WAN address	*	✗	Auto created rule

Then, make sure you have a firewall rule that lets you route traffic outbound:

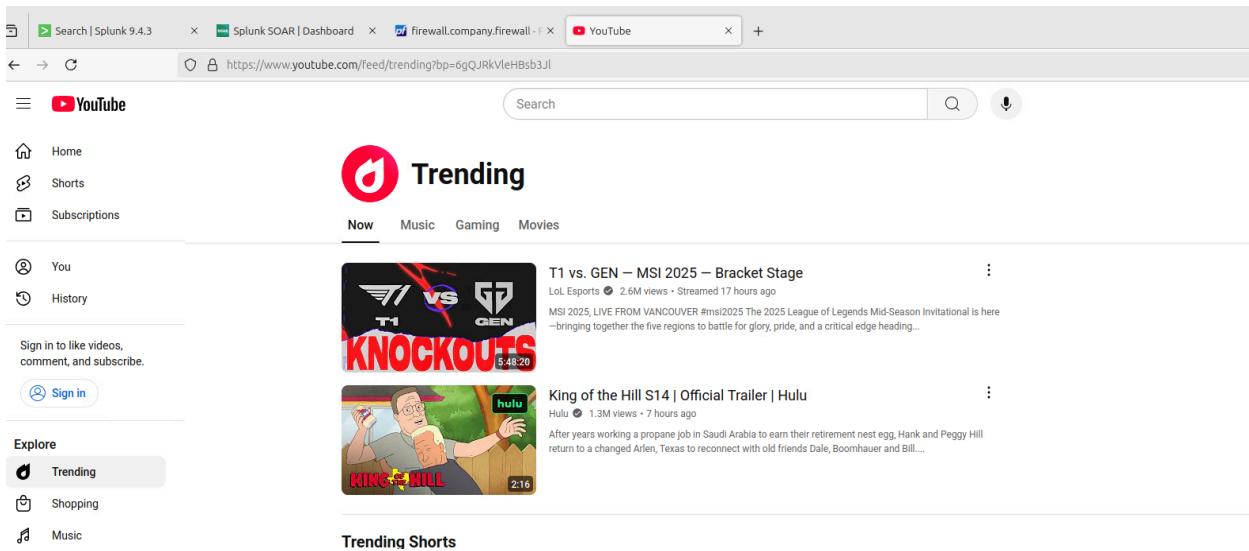
The screenshot shows the pfSense interface under Firewall / Rules / LAN. The "LAN" tab is selected. A table lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/1.47 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓ 0/7 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Test on a machine within the LAN (this is the SOC computer):



- Make sure that you change the Default Route (Gateway) to the Firewall: 192.168.15.1
- Also make sure that you change the DNS to an external DNS server like 8.8.8.8 so that you can resolve a name like [youtube.com](https://www.youtube.com) to an IP address



(The only reason why I added this was because the console pfsense made me force one of the LAN's to be a WAN, so I just decided to add an external internet to cover the WAN, and make OPTIONAL1 (OPT1) the DMZ LAN)

As of right now, we are not able to ping 10.10.10.1 (firewall) from the Kali machine in the subnet 10.10.10.0/24. Why?

```
(red@redteam01)~]$ ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
^C
--- 10.10.10.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2055ms
```

Fix: It may be a firewall rule thing within pfsense, you need to allow inbound traffic

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/213 KB	IPv4 *	OPT1 subnets	*	OPT1 address	*	none			

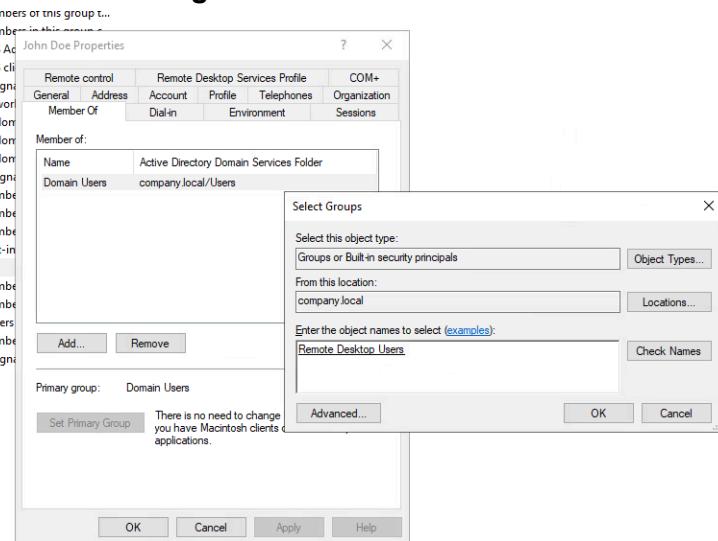
Add Add Delete Toggle Copy Save Separator

- You must allow ANY protocol (I put TCP, which still causes the machine to not be able to ping since ping uses protocol ICMP) from the OPT1 subnet to be able to communicate with the OPT1 address (10.10.10.1)
- **IMPORTANT TO NOTE:**
 - FW RULES ONLY APPLY TO TRAFFIC **ENTERING ON THAT SPECIFIC INTERFACE** (e.g. OPT1, LAN)
 - So if you want two interfaces to interact with each other, you need to specify an inbound rule on one interface, and an outbound rule on the other interface
 - e.g. Allow inbound traffic from src:OPT1 to dest:LAN within the LAN interface
 - You will also have to Allow **outbound** traffic from src:OPT1 subnets to dest:ANYTHING within the OPT1 interface
 - If you want to be able to ping across LANs, you need to make sure that all of the devices have the firewall IP address set as the default gateway.

```
(red㉿redteam01)-[~]
$ ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.502 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.571 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.329 ms
^C
--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2040ms
rtt min/avg/max/mdev = 0.329/0.467/0.571/0.101 ms
```

- Now it works

Troubleshooting RDP:



Make sure to do a gpupdate /force using the AD01 DNS (192.168.15.10) so that you don't get a Name Resolution Failure:

```

Windows PowerShell
Computer policy could not be updated successfully. The following errors were encountered:
The processing of Group Policy failed. Windows could not resolve the computer name. This could be caused by the following:
a) Name Resolution failure on the current domain controller.
b) Active Directory Replication Latency (an account created on another domain controller has not replicated to the current domain controller).
User Policy could not be updated successfully. The following errors were encountered:
The processing of Group Policy failed. Windows could not resolve the user name. This could be caused by the following:
a) Name Resolution failure on the current domain controller.
b) Active Directory Replication Latency (an account created on another domain controller has not replicated to the current domain controller).
To diagnose the failure, review the event log or run GPRESULT /H GPReport.html from the command line to see about Group Policy results.
PS C:\Users\john.doe> ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
PS C:\Users\john.doe> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
PS C:\Users\john.doe> |

```

Do this on the client side:

Make sure NLA is turned off; this allows for a less safe connection to happen which is good for the Kali attacker

Ignore that; just trying to generate some telemetry so we will just do RDP group policy locally:

- net localgroup "Remote Desktop Users" "company\john.doe" /add
- net localgroup "Remote Desktop Users"
 - this is to check that john.doe is in
- secpol.msc
 - Local Policies > User Rights Assignment > Allow log on through Remote Desktop Services
 - Make sure "Remote Desktop Users" is listed
- gpupdate /force
- Restart-Service TermService -Force

HERE IS THE WEAK VULNERABILITY SCENARIO:

Let's say there's are devices in the DMZ subnet and you need them to connect to devices via RDP on the LAN subnet, so you decide to create the following firewall rule:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
✓ 0/0 B	IPv4 *	OPT1 subnets	*	*	*	*	none				
✓ 0/168 B	IPv4 *	OPT1 subnets	*	OPT1 address	*	*	none				

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
✓ 0/1.85 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule		
✓ 0/0 B	IPv4 *	OPT1 subnets	*	LAN subnets	*	*	none				
✓ 0/10.79 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule		
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule		

There's now an issue:

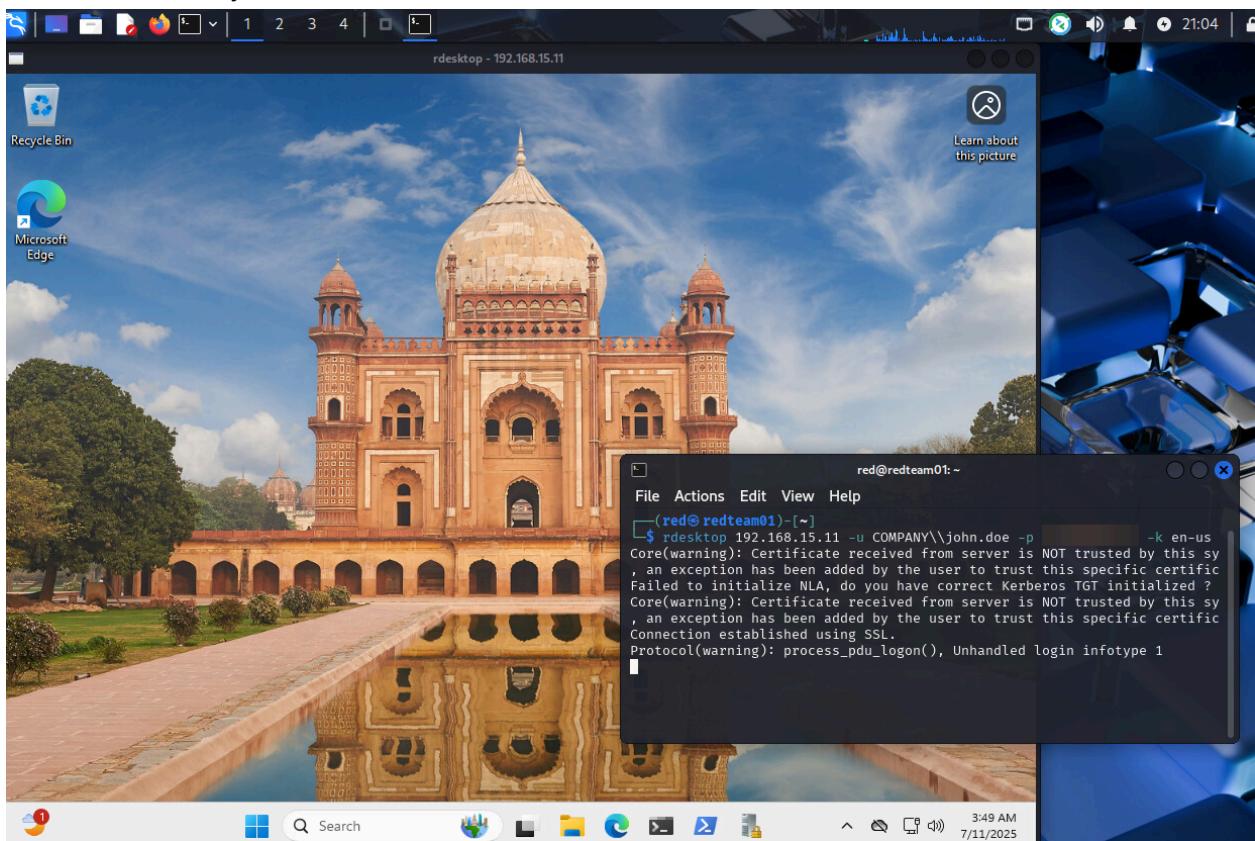
An attacker is in the DMZ and is able to ping a user's computer within the COMPANY VLAN:

```
(red@redteam01)~$ ping 192.168.15.11
PING 192.168.15.11 (192.168.15.11) 56(84) bytes of data.
64 bytes from 192.168.15.11: icmp_seq=1 ttl=127 time=0.917 ms
64 bytes from 192.168.15.11: icmp_seq=2 ttl=127 time=1.23 ms
64 bytes from 192.168.15.11: icmp_seq=3 ttl=127 time=0.860 ms
64 bytes from 192.168.15.11: icmp_seq=4 ttl=127 time=0.766 ms
^C
--- 192.168.15.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.766/0.943/1.229/0.173 ms
```

The attacker already knows the a domain user's username and password, and can now RDP into Win11Client using **rdesktop**:

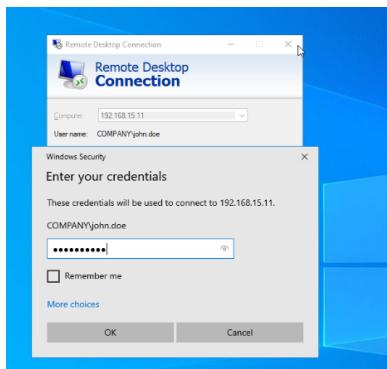
(it wasn't working because I didn't have RDP turned on for both the user and the computer)

Now we can finally RDP from the Kali VM:



- You have to put single quotes around the double quotes if you have any in your password
 - “example”

This should generate some telemetry on Splunk, but it doesn't. Troubleshooting...:



Also Disabled Legacy (Basic) Audit Policy:

- gpedit.msc
- Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options
- Enable: Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
- then gpupdate /force

Event 4624, Microsoft Windows security auditing.

General Details			
Virtual Account:	No	Elevated Token:	No
Impersonation Level:	Impersonation		
New Logon:	Security ID: COMPANY\john.doe Account Name: john.doe Account Domain: COMPANY Logon ID: 0x7FBE18A Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {9a0bb8de-f17a-2a6d-293b-869f9ed25d54}		
Process Information:	Process ID: 0x6a0 Process Name: C:\Windows\System32\svchost.exe		
Network Information:	Workstation Name: WIN11CLIENT Source Network Address: 10.10.10.10 Source Port: 0		
Detailed Authentication Information:	Logon Process: User32 Authentication Package: Negotiate Transited Services: -		

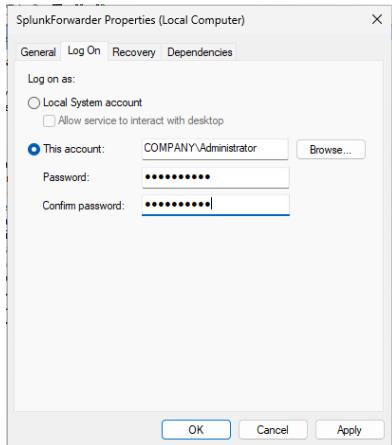
Event 4624, Microsoft Windows security auditing.

General Details			
<input checked="" type="radio"/> Friendly View	<input type="radio"/> XML View		
SubjectUserId	S-1-5-18		
SubjectUserName	WIN11CLIENT\$		
SubjectDomainName	COMPANY		
SubjectLogonId	0x3e7		
TargetUserId	S-1-5-21-3058509360-1065960445-970009866-1103		
TargetUserName	john.doe		
TargetDomainName	COMPANY		
TargetLogonId	0x854b622		
LogonType	10		
LogonProcessName	User32		
AuthenticationPackageName	Negotiate		
WorkstationName	WIN11CLIENT		
LogonGuid	{73d52ef1-2644-5cb3-5ea6-ff1f29e15615}		
TransmittedServices	-		
LmPackageName	-		
KeyLength	0		
ProcessId	0x6a0		
ProcessName	C:\Windows\System32\svchost.exe		
IpAddress	10.10.10.10		

It has the Logon Type: 10

It is still not forwarding to Splunk. I think it's lacking permissions to even see it

- You can create a splunk specific service account with specific permissions
 - we will just run the service as the administrator account



Time	Event
7/17/25 11:30:31:000 AM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/eventschemas-system"><System>Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-a5ba-3e3bd0328c30d}'><EventID>4624</EventID><Version>3</Version><Level>0</Level><Task>12544</Task><Opcode>0</Opcode><Keywords>0x802000</Keywords><TimeCreated SystemTime='2025-07-17T11:30:31.5771076Z' /><EventRecordID>59417</EventRecordID><Correlation ActivityID='ca7e52ca-f24e-0000-b053-7eca4ef2db01' /><Execution ProcessID='772' ThreadID='912' /><Channel>Security</Channel><Computer>Win11Client.company.local</Computer><Security/><System><EventData><Data Name='SubjectUserSid'>S-1-5-18</Data><Data Name='SubjectUserName'>WIN11CLIENT\$</Data><Data Name='SubjectDomainName'>COMPANY</Data><Data Name='SubjectLogonId'>0x37c00000000000000000000000000000</Data><Data Name='TargetUserSid'>S-1-5-21-3058509360-1065960445-970009866-1103</Data><Data Name='TargetUserName'>john.doe</Data><Data Name='TargetDomainName'>COMPANY</Data><Data Name='TargetLogonId'>0x8546622</Data><Data Name='LogonType'>10</Data><Data Name='LogonProcessName'>User32</Data><Data Name='AuthenticationPackageName'>Negotiate</Data><Data Name='WorkstationName'>WIN11CLIENT</Data><Data Name='LogonGuid'>(73d52ef1-2644-5cb3-5ea6-ff1f29e15615)</Data><Data Name='TransmittedServices'></Data><Data Name='LmPackageName'></Data><Data Name='KeyLength'>0</Data><Data Name='ProcessId'>0x60</Data><Data Name='ProcessName'>C:\Windows\System32\svchost.exe</Data><Data Name='IpAddress'>10.10.10.10</Data><Data Name='IpPort'>0</Data><Data Name='ImpersonationLevel'>%1833</Data><Data Name='RestrictedAdminMode'>%1843</Data><Data Name='RemoteCredentialGuard'>%1843</Data><Data Name='TargetOutboundUserName'></Data><Data Name='TargetOutboundDomainName'></Data><Data Name='VirtualAccount'>%1843</Data><Data Name='TargetLinkedLogonId'>0x0</Data><Data Name='ElevatedToken'>%1843</Data></Event>

We finally got it to forward to Splunk!

- We can see:
 - Event ID: 4624
 - Target User Name: john.doe
 - Logon Type: 10
 - IPAddress: 10.10.10.10 (the attacker's IP address)
- I tinkered around with so many settings that I forgot which one allowed this to be fixed.
Here is the input.conf file from Win11Client's forwarder:

```
[WinEventLog://Security]
index = company-ad
disabled = false
renderXml = true
checkpointInterval = 5
start_from = oldest
```

i found these extra things online

Now I can clean up with XML output, generate this alert as a cron job in Splunk for me to test my automation response.

Cleaning up Splunk query

We can clean up the Splunk query using Regular Expressions (though I do not know how to):

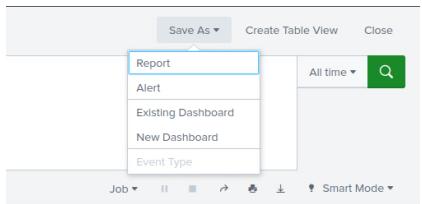
```
index=company-ad host=WIN11CLIENT EventCode=4624
| rex "<Data Name=\"TargetUserName\">(?<TargetUserName>[^<+])</Data>"
| rex "<Data Name=\"IpAddress\">(?<IpAddress>[^<+])</Data>"
| rex "<Data Name=\"LogonType\">(?<LogonType>[^<+])</Data>"
| search LogonType=10
| table _time, EventCode, TargetUserName, IpAddress, LogonType
| head 1
```

- head 1 will grab the top most / most recent event

Line by line:

- rex "<Data Name=\"TargetUserName\">(?<TargetUserName>[^<+])</Data>"
 - rex: Splunk command that applies a regex to each event
 - Data Name="TargetUserName": Matches this literal part of the XML: "Data Name=TargetUserName"
 - <: Matches a literal opening angle bracket
 - Data Name= Matches the literal text *Data Name=* in the XML
 - \" : Escaped quote character; just like powershell
 - TargetUserName: Actual field name we want to target
 - \": Closing quote
 - >: Matches the end of the opening tag
 - (?<TargetUserName>[^<+])
 - (and): Defines the capture group (the thing we want to extract)
 - ?<TargetUserName>: This names the group "TargetUserName";**THIS BECOMES YOUR SPLUNK FIELD**
 - [^<+]
 - [] : Defines a character set
 - ^: Inside a character set, it means "NOT"
 - <: We want to stop when we hit this (because it's the next XML tag), basically the **delimiter**
 - [^<]: Match **any character except <**
 - +: Match one or more of those characters
 - </Data> : Matches the literal closing tag that ends the XML value

Save as alert:



Save As Alert

Settings

- Title: Attacker RDP Login
- Description: Optional
- Permissions: Private
- Alert type: Scheduled
- Run on Cron Schedule: Run on Cron Schedule ▾
- Time Range: Last 60 minutes ▾
- Cron Expression: * * * * * (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

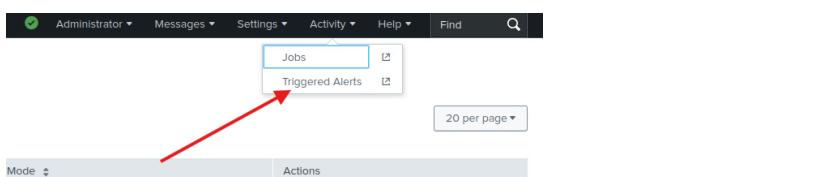
Trigger Actions

- + Add Actions ▾
- When triggered: Add to Triggered Alerts Remove
- Severity: Medium

Buttons: Cancel Save

Run a cron job, scheduled to run every minute.

Can view it in:



Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Jobs Triggered Alerts

20 per page ▾

Mode ▾ Actions

Successfully triggered an Alert!!

Triggered Alerts

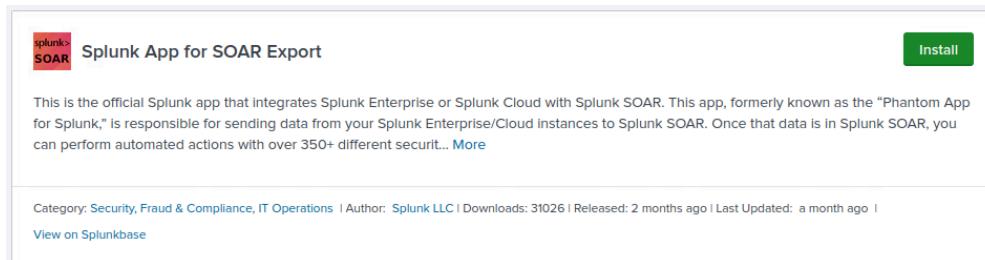
Filter <input type="text"/> <input type="button"/>	App <input type="text"/> Search & Report... <input type="button"/>	Owner <input type="text"/> All owners <input type="button"/>	Severity <input type="text"/> All severity <input type="button"/>	Alert name <input type="text"/> All alerts <input type="button"/>	Showing 1- 1 of 1 results		20 per... <input type="button"/>	1 of 1 pages <input type="button"/>	< >
<input type="checkbox"/> Time <input type="button"/>	2025-07-18 02:57:00 GMT	Attacker RDP Login	search	Scheduled	Medium	Digest	View Results <input type="button"/>	Edit Search <input type="button"/>	Delete

SPLUNK SOAR AUTOMATION

Plan for automation:

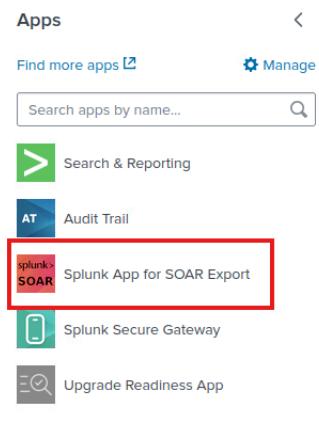
- Once an alert is triggered in Splunk, it should send an email with the Computer name/host, Username used to log in (TargetUserName), IPAddress (IP address of the remote computer), Event ID, Event code
- Once the email is sent, it will ask:
"Would you like to disable the account: TargetUserName?"
- in which the SOC analyst can pick Yes or No in SOAR
- This will then get sent back to the SOAR playbook and then disable the Active Directory account for that user.

Apps -> Find more apps -> **Splunk App for SOAR Export**



The screenshot shows the product page for the "Splunk App for SOAR Export". At the top, there's a "Install" button. Below it, a brief description states: "This is the official Splunk app that integrates Splunk Enterprise or Splunk Cloud with Splunk SOAR. This app, formerly known as the 'Phantom App for Splunk,' is responsible for sending data from your Splunk Enterprise/Cloud Instances to Splunk SOAR. Once that data is in Splunk SOAR, you can perform automated actions with over 350+ different securit... [More](#)". Below the description, it says "Category: Security, Fraud & Compliance, IT Operations | Author: Splunk LLC | Downloads: 31026 | Released: 2 months ago | Last Updated: a month ago | [View on Splunkbase](#)".

- Need this one because it **sends alerts and results** from **Splunk Enterprise TO Splunk SOAR**



The screenshot shows the Splunk Apps search interface. It has a search bar at the top with placeholder text "Search apps by name...". Below the search bar, there's a list of apps. One app, "Splunk App for SOAR Export", is highlighted with a red box around its icon and name. Other visible apps include "Search & Reporting", "Audit Trail", "Splunk Secure Gateway", and "Upgrade Readiness App".

Follow the

<https://docs.splunk.com/Documentation/SOARExport/latest/UserGuide/ConfigureSOARserver>
to connect SOAR App for SOAR Export to Splunk SOAR with the appropriate users. Just listing a few steps here:

Setting inheritance for **admin** to include **phantom** capabilities:

Edit Role admin

Name *

Inheritance Capabilities Indexes Restrictions Resources

Select roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be deselected. If you select multiple roles, this role inherits capabilities and indexes from all of them.

Role name
<input type="checkbox"/> can_delete
<input checked="" type="checkbox"/> phantom
<input checked="" type="checkbox"/> power
<input type="checkbox"/> sc_admin
<input type="checkbox"/> splunk_system_role
<input type="checkbox"/> splunk_system_upgrader
<input checked="" type="checkbox"/> user

Creating a new automation user in Splunk SOAR w/ the IP address of the Splunk instance, and grabbing the REST API key:

Edit User

User Type Automation

Username kt-automation

Default Label (Search or add new) events

Allowed IPs 192.168.15.9

Authorization Configuration for REST API

```
{"ph-auth-token": "*****", "server": "https://192.168.15.8"}
```

Re-Generate Auth Token

ASSETS ASSOCIATED WITH THIS USER

Roles Automation

Disabled

Cancel Save

Kept getting an error about IP address not being correct on the SOAR side.

[Intro to Splunk SOAR Phantom | Sending Splunk Alerts To SOAR Phantom](#)

Followed this video; **TLDR: go to**

- cd /opt/splunk/etc/apps/phantom/local/phantom.conf AND
- cd /opt/splunk/etc/apps/splunk_app_soar/local/soar.conf
 - Type in the following:
[verify_certs]
value = false
- After restarting Splunk server, it should result in this:

SOAR Server Configuration

 HTTPS certificate verification is disabled.

In Splunk App for SOAR Export, create a new server:

New Server X

To add a new server you must use an authorization token from SOAR.
See [Connect the Splunk App for SOAR Export and the Splunk Platform to a Splunk SOAR server](#) in the Splunk SOAR documentation.

Authorization Configuration

```
{ "ph-auth-token": "REDACTED", "server": "https://192.168.15.8" }
```

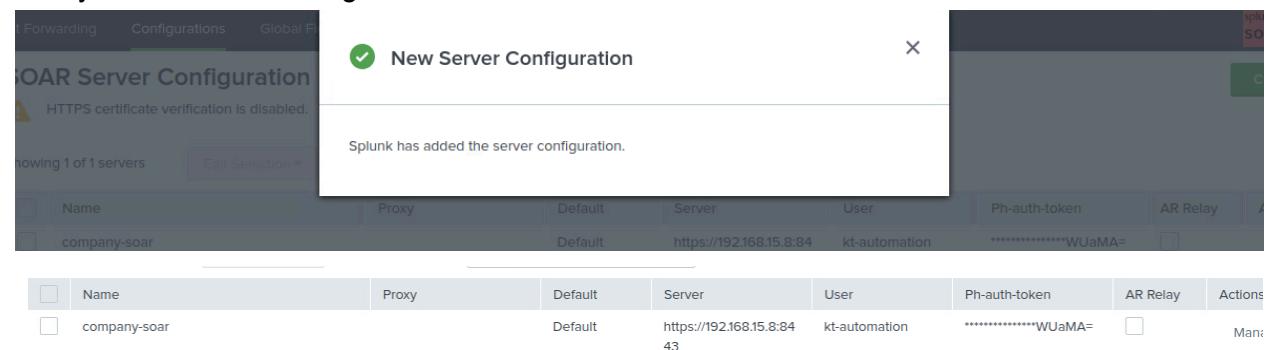
Name

Proxy

Optional: Mark server as [Adaptive Response Relay](#) forwarding target

Cancel Save

Now you can add the thing:


New Server Configuration
Splunk has added the server configuration.

Name	Proxy	Default	Server	User	Ph-auth-token	AR Relay	Actions
company-soar	Default	https://192.168.15.8:84	kt-automation	*****WUaMA=			Manage

I'm setting up the alert to send to SOAR:

Edit Alert

+ ADD ACTIONS ▾

When triggered > Add to Triggered Alerts Remove

▼ SOAR Send to SOAR Remove

Note: If your Splunk SOAR connection is not successful, the system saves events to send to Splunk SOAR later. Events with key names containing periods will not be saved or sent after the connection is reestablished.

SOAR company-soar Instance *Forward results to this Server/Asset.

Sensitivity Select... *Sensitivity level for these events.

Severity company-soar: Medium *Severity of these events.

Label events Label for these events.

Container Name Source Container name in SOAR.

Cancel Save

This is what shows up in my SOAR: (I left it running overnight)

The screenshot shows the SOAR interface with the following details:

- Top Events:** 423 events
- Severity:** 0 High, 423 Medium, 0 Low
- Status:** 423 New, 0 Open, 0 Closed
- Top Owners:** (Listed below)

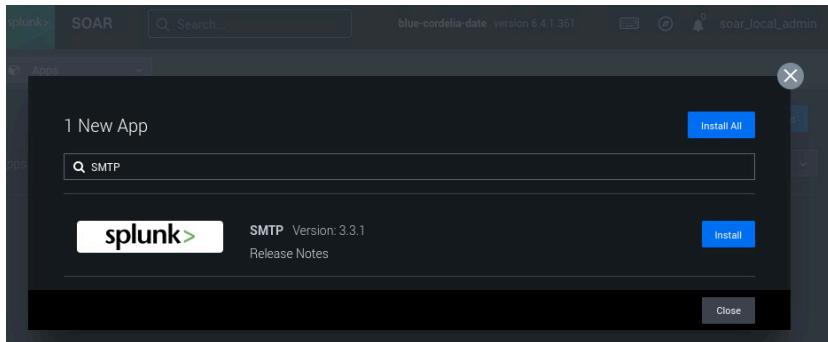
ID	NAME	LABEL	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED	OPENED	UPDATED	DUE	RE
423	Ad hoc search result	events		New	MEDIUM	TLP AMBER	1	Today at 11:59 am			Today at 11:59 pm	
422	Ad hoc search result	events		New	MEDIUM	TLP AMBER	1	Today at 11:58 am			Today at 11:58 pm	

Now to create a playbook:

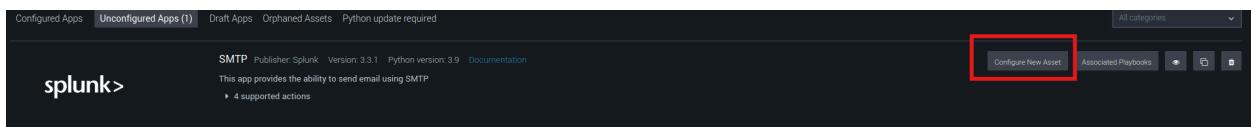
We want it to:

- Receive an alert
- Have user asking submit a YES/NO response on SOAR
- Disable the specified user account in AD based on that response

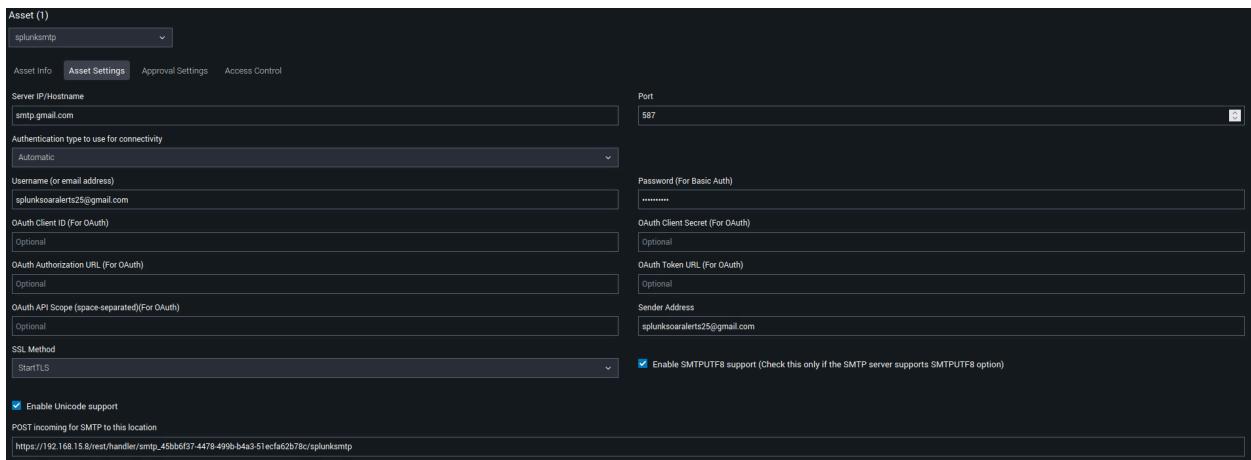
First: We need to set up an email connector (SMTP) **Make sure DNS on RHEL 8 is set to 8.8.8.8 or something that can reach external sites**



Go to Apps -> New App -> Search up “SMTP” and install it



Now you can configure the asset and include all of the things it needs



Use google voice for 2 Factor and set up a new app password using

<https://myaccount.google.com/apppasswords>

and use the key/password that is created in your SMTP Asset settings where it says “Password (For Basic Auth)

Your app passwords

splunksoar

Created on 12:25 PM



Create a gmail account and use Gmail's SMTP server to send the email

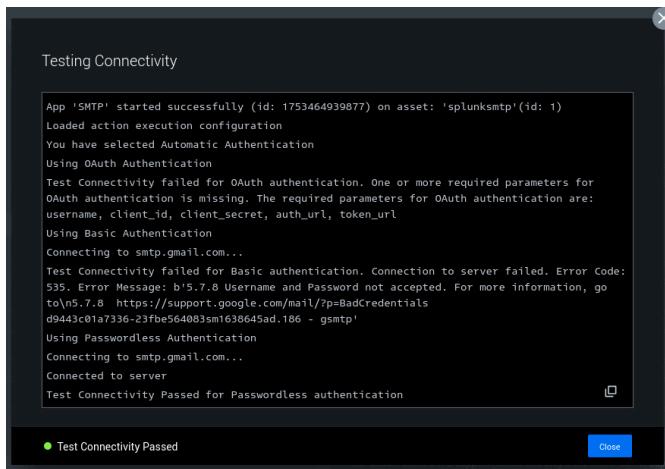
When using the Gmail SMTP server:

- The sending limit is 2,000 messages per day. Learn more about [email sending limits](#).
- Spam filters might reject or filter suspicious messages.
- The fully qualified domain name of the SMTP service is `smtp.gmail.com`.
- Configuration options include:
 - Port 25, 465, or 587
 - [SSL and TLS protocols](#)
 - Dynamic IP addresses
- Using port 587 and hostname [smtp.gmail.com](#)

Splunk SOAR Alert email address:



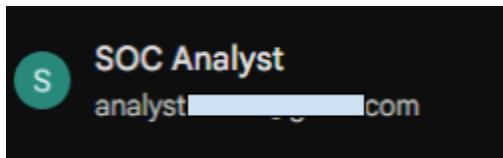
Test the connectivity to the SMTP server:



Now we need to build the playbook

- Extracting username from alert
- Send an email to analyst
- Wait for YES/NO response
 - If YES, it disables the account using AD

SOC Analyst email address:



Email has finally been received on the analyst-side:

Alert: RDP from Unknown IP

splunksoaralerts25@gmail.com
to me

An RDP logon was detected.

Event Code: {__cef.EventCode}
IP Address: {__cef.ipAddress}
Logon Type: {__cef.LogonType}
Target User: {__cef.TargetUserName}

Do you want to disable this account?

Please respond to the prompt with one of the following:
- YES
- NO

Reply Forward

Email Approval - Disable AD Acc...

send_email_1

SMTP

to = analyst

body = An RDP logon was detected. Event Code: {__cef.EventCode}

from = splunksoaralerts25@gmail.com

subject = Alert: RDP from Unknown IP

Email sent

Now to fix the actual contents of the email.

body* ⓘ

An RDP logon was detected.

Event Code: {0}

IP Address:

Logon Type:

Target User:

artifact:*.cef.EventCode

An RDP logon was detected.

Event Code: 4624

IP Address:

Logon Type:

Target User:

Do you want to disable this account?

Please respond to the prompt with:
- YES
- NO

What works: **artifact:*.cef.EventCode**

- You can just type in the name of the variable, even if it doesn't exist within the list of .cef

Alert: RDP from Unknown IP

splunksoaralerts25@gmail.com
to me

An RDP logon was detected.

Event Code: 4624

IP Address: 10.10.10.10

Logon Type: 10

Target User: john.doe

Do you want to disable this account?

Please respond to the prompt with:
- YES
- NO

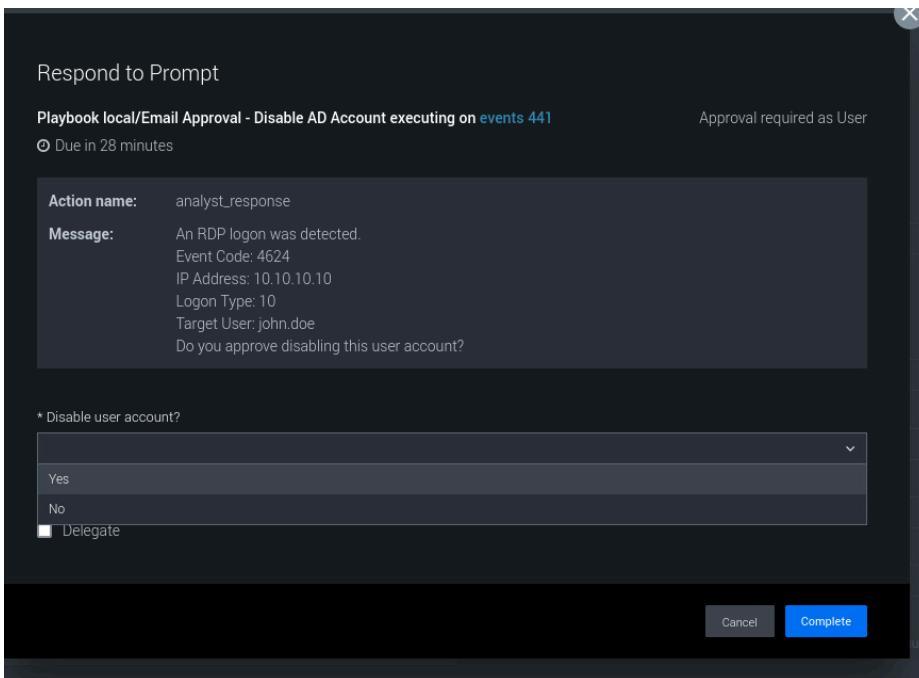
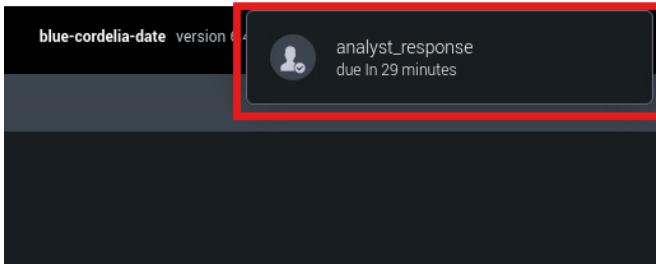
Now we need to create a prompt for the analyst to respond to (Yes/No) and then push the output into a Decision Block:

The screenshot shows the configuration of a PROMPT block named "analyst_response". The "User or role*" dropdown is set to "soar_local_admin". The "CONTENT" section contains an introductory message: "An RDP logon was detected." followed by artifact placeholders: "Event Code: {0}", "IP Address: {1}", "Logon Type: {2}", and "Target User: {3}". Below this, there are four artifact selection boxes: "0 artifact:*.cef.EventCode", "1 artifact:*.cefIpAddress", "2 artifact:*.cef.LogonType", and "3 artifact:*.cef.TargetUserName". A "Question 1" field contains the question "Disable user account?", a "Response Type" dropdown set to "Yes/No", and a checked "Required" checkbox. To the right, a flowchart shows the connection from the PROMPT block to a Decision Diamond, which then connects to an ACTION block labeled "send_email". The ACTION block has a status of 100%. The final step is an "End Unconfigured" block.

Decision Block: we choose `analyst_response:action_result.summary.responses.0` because it is the first index in which the response is saved in. (look at the logs)

The screenshot shows the configuration of a DECISION block named "decision_1". The "CONDITIONS" section includes a condition "If analyst_response:action_result.summary.responses.0 == Yes". Below this, there are "Else If" and "Else" buttons, with a red arrow pointing to the "Else" button. A "Data preview" panel is open, showing a dropdown menu with various Splunk SOAR variables. The variable "analyst_response:action_result.summary.responses.0" is selected, and its value is displayed in the preview area: "Action 'analyst_response'(prompt)
Status:success
Responses:[
"Yes"
]

When running, this will show up in Splunk SOAR:

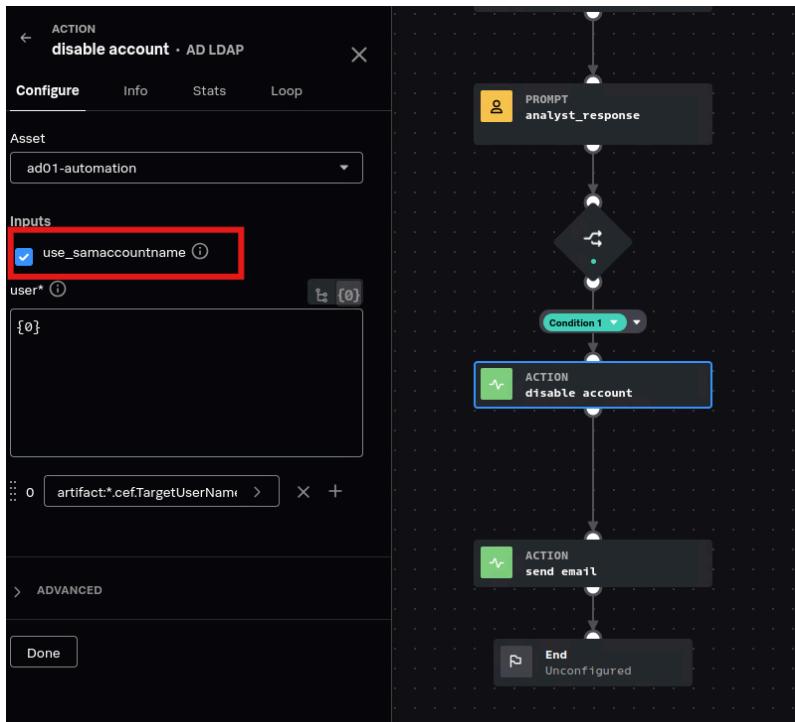


Now we want to take the TargetUserName and disable it in AD
Get the AD LDAP App in SOAR



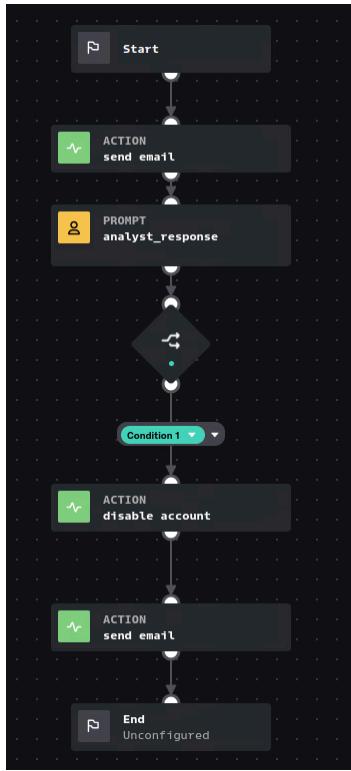
Connect to AD01 using Administrator (ideally you'd have a separate account for this that handles modifying of users but since this is a homelab environment, we'll just use Administrator since it has all the permissions required)

Now we add a new AD Action Block where we “disable account” using **artifact:*.cef.TargetUserName:**



You can either use the sAMAccountName (john.doe) or the more production-ready way would be to use the DistinguishedName (CN=John Doe,CN=Users,DC=company,DC=local)

- You can get this by putting in a “get user” block and pass it into the disable account block



Now when we look in AD01, we should see that account John Doe has been disabled

Group Policy Creator Owners	Security Group... N
John Doe	User B
Kali Linux	User
Protected Users	Security Group... N
RAS and IAS Servers	Security Group... N
Read-only Domain Controllers	Security Group... S
Schema Admins	Security Group... D

An email should be sent to the user like this:

User john.doe has been disabled ➔ [Inbox](#)

[splunksoaralerts25@gmail.com](#)
to me ▾

User john.doe has been disabled.

You may re-enable the account once you have remediated the vulnerability.

[Reply](#) [Forward](#) [Smile](#)

Misc. Troubleshooting:

New Search

Save As ▾

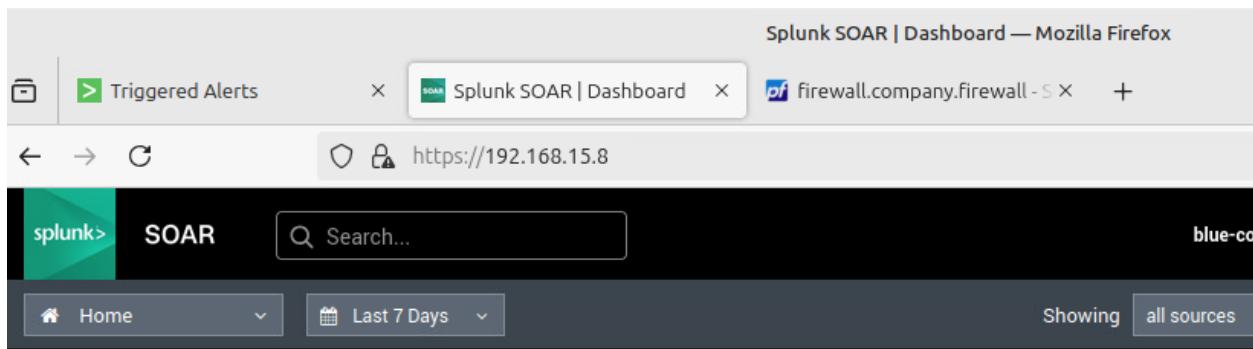
index=company-ad

⚠️ Search not executed: The minimum free disk space (5000MB) reached for /opt/splunk/var/run/splunk/dispatch. user=admin., concurrency_category="historical", concurrency_context="user_instance-wide", current_concurrency=0, concurrency_limit=5000

No Event Samplings ▾

Getting this error when trying to query in Splunk

- Go to settings -> Server Settings -> General Settings -> Change the “Pause indexing if free disk space (in MB) falls below” to something low
- Restart splunk: /opt/splunk/bin sudo ./splunk restart



I'm viewing the Splunk logs, Splunk SOAR and pfSense within my SOC Analyst Mint VM