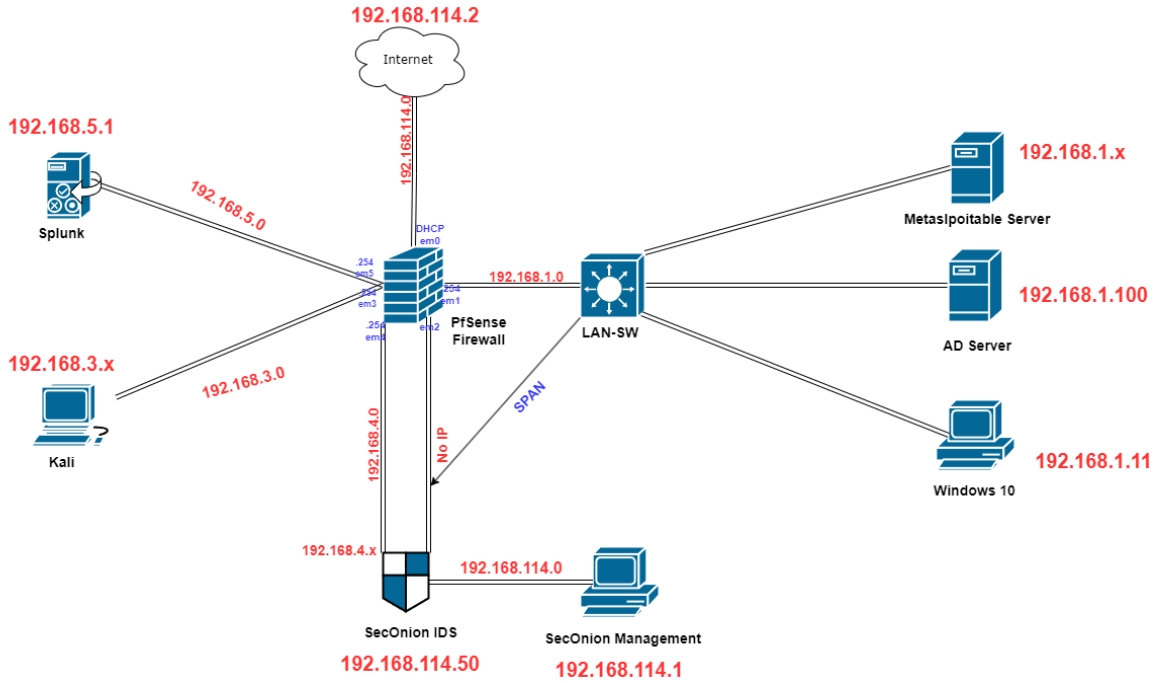
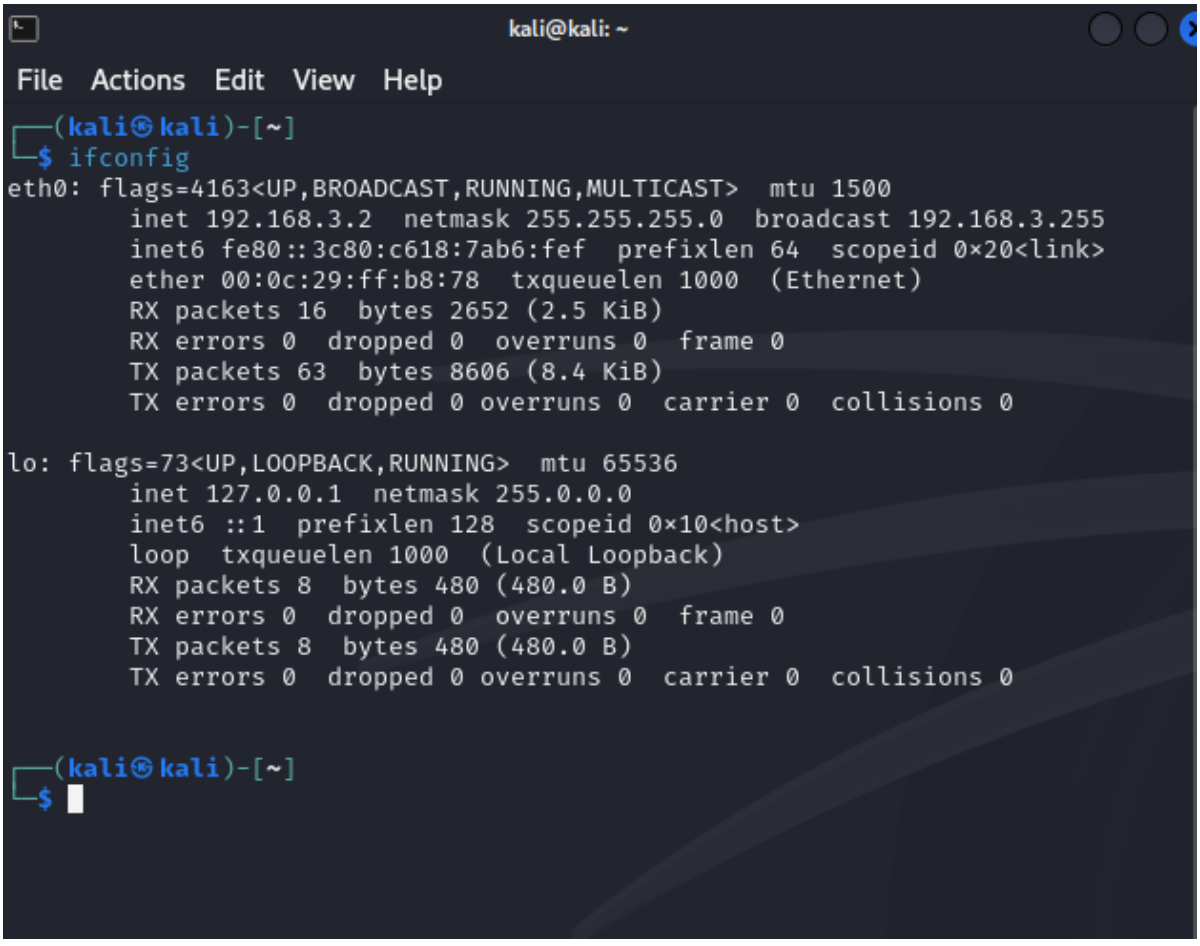
Security Onion Monitoring & Detection

I will be performing attacks on the Active Directory (AD) server. Since the Splunk Forwarder is installed on the AD server, and the SPAN port is configured to mirror network traffic to Security Onion, these malicious activities can be monitored and analyzed in both Splunk and Security Onion simultaneously.



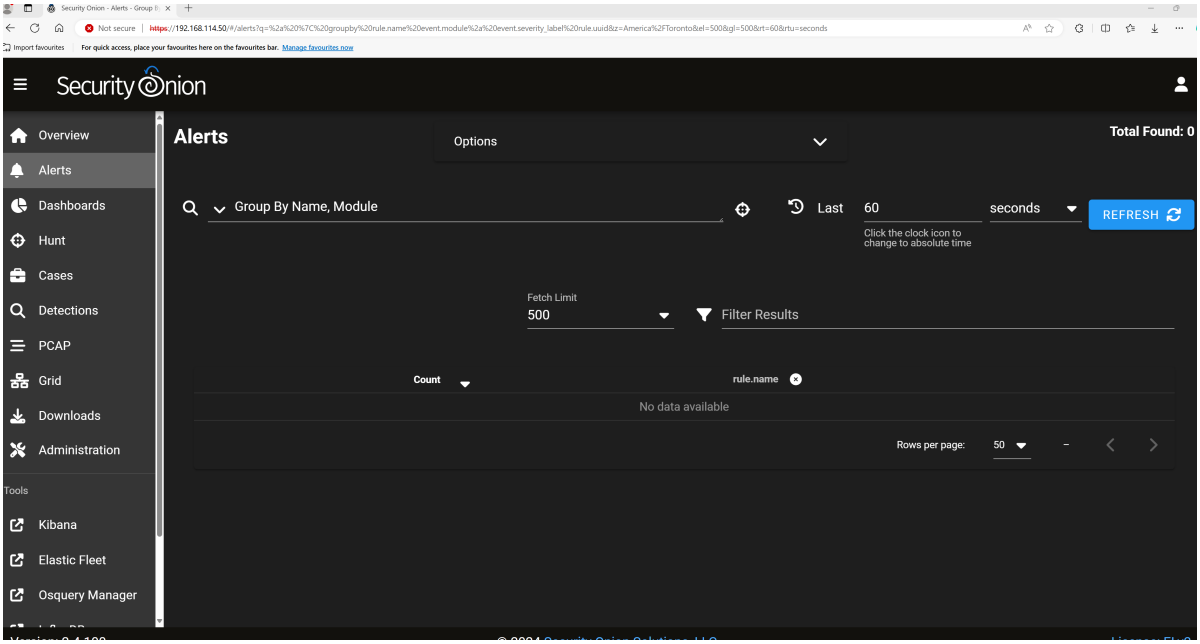
Kali IP **192.168.3.2**



AD Server IP **192.168.1.100**

```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

Security Onion is accessed in my host via https://192.168.114.50



1. Before conducting the attack, I will use the script from https://github.com/safebuffer/vulnerable-AD to create a vulnerable Active Directory environment on the AD server. This script will make the environment susceptible to attacks such as Kerberoasting. This setup will be used in the lab to simulate real-world vulnerabilities.
2. ping AD server 192.168.1.100 from Kali

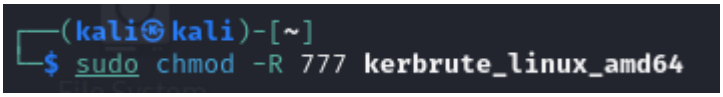
```
└─$ nmap 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 18:09 EDT
Nmap scan report for 192.168.1.100
Host is up (0.00095s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds
```

Attacks captured by Security Onion

t	192.168.3.2	47248	192.168.1.100	5432	ET SCAN Suspicious inbound to Postgre
t	192.168.3.2	46160	192.168.1.100	5800	ET SCAN Potential VNC Scan 5800-582(
t	192.168.3.2	42858	192.168.1.100	1433	ET SCAN Suspicious inbound to MSSQL
t	192.168.3.2	40788	192.168.1.100	1521	ET SCAN Suspicious inbound to Oracle
t	192.168.3.2	58762	192.168.1.100	5903	ET SCAN Potential VNC Scan 5900-592(
t	192.168.3.2	56056	192.168.1.100	3306	ET SCAN Suspicious inbound to mySQL

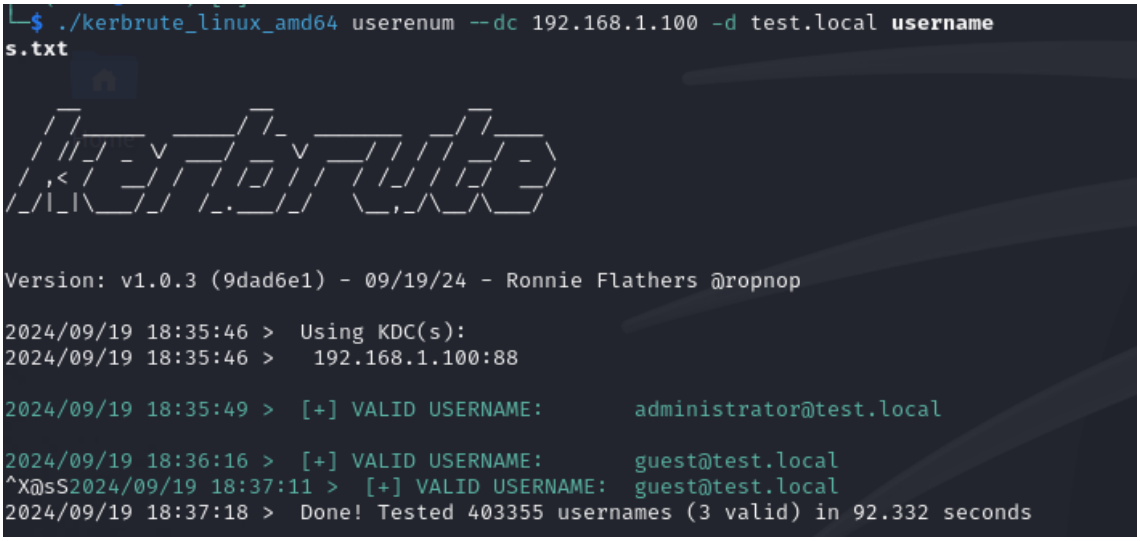
3. Perform Kerberoasting Attack from Linux to AD server, download tool from https://github.com/ropnop/kerbrute/releases.userenum, and download usename list from https://github.com/duyet/bruteforce-database/blob/master/usernames.txt

   Assign executable permission to kerbrut_linux_amd64

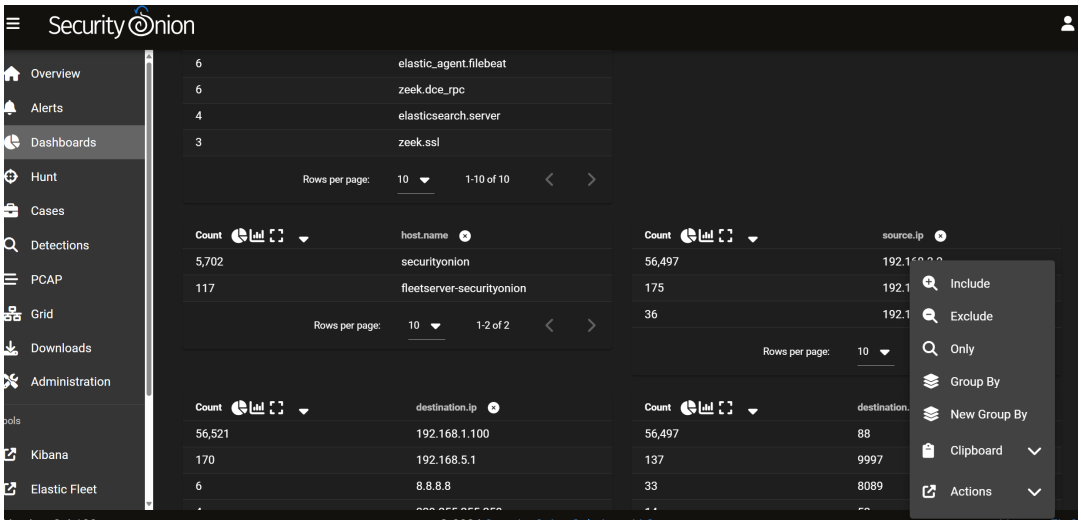


   Then execute command below, this command is to enumerate valid domain usernames via Kerberos

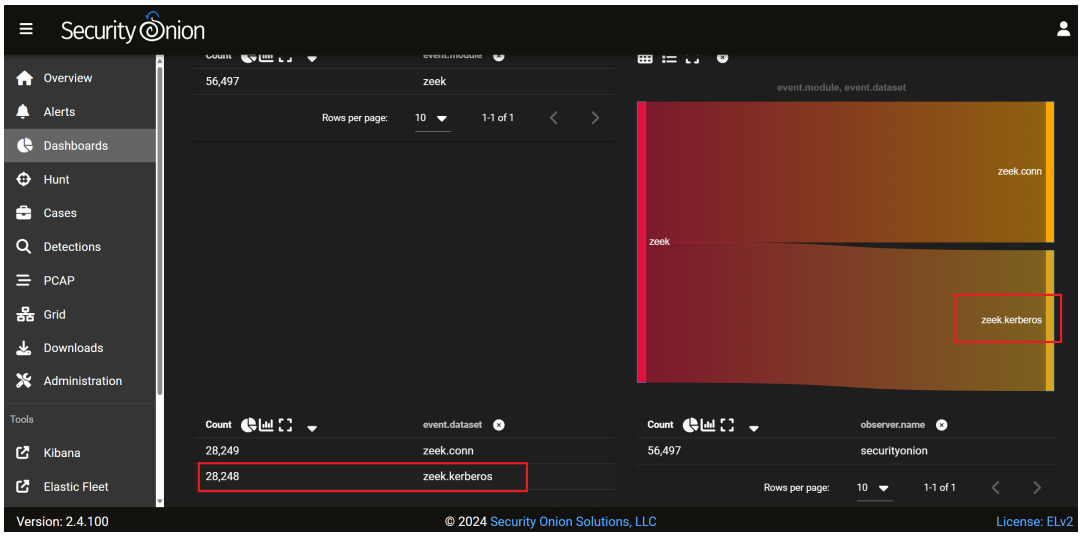
```
./kerbrute_linux_amd64 userenum --dc 192.168.1.100 -d test.local
usernames.txt
```



4. Go to Security Onion-> Dashboards, scroll down, and include 192.168.3.2



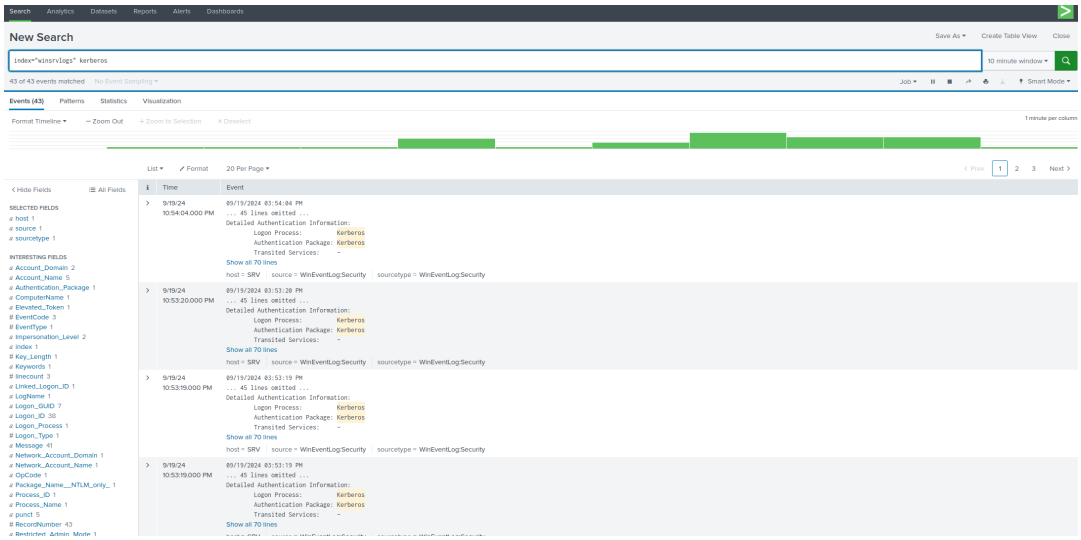
And kerberos attack with usernames was overserved by zeek



Timestamp	event.dataset	source.ip	source.port	destination.ip	destination.port	kerberos.client	kerberos.service
2024-09-19 18:52:25.778 -04:00	zeek.kerberos	192.168.1.11	50353	192.168.1.100	88	DESKTOP-S5PIQ9E$/TEST.LOCAL	desktop-s5piq9e$
2024-09-19 18:52:16.113 -04:00	zeek.kerberos	192.168.1.11	50347	192.168.1.100	445		
2024-09-19 18:48:10.303 -04:00	zeek.kerberos	192.168.3.2	48041	192.168.1.100	88	zirconium/TEST.LOCAL	krbtgt/TEST.LOCAL
2024-09-19 18:48:08.395 -04:00	zeek.kerberos	192.168.3.2	45588	192.168.1.100	88		krbtgt/TEST.LOCAL
2024-09-19 18:48:02.660 -04:00	zeek.kerberos	192.168.3.2	51861	192.168.1.100	88	orchestia/TEST.LOCAL	krbtgt/TEST.LOCAL
2024-09-19 18:48:02.166 -04:00	zeek.kerberos	192.168.3.2	50207	192.168.1.100	88	unmoralizing/TEST.LOCAL	krbtgt/TEST.LOCAL
2024-09-19 18:48:02.100 -04:00	zeek.kerberos	192.168.3.2	40107	192.168.1.100	88	unmailable/TEST.LOCAL	krbtgt/TEST.LOCAL
2024-09-19 18:47:56.336 -04:00	zeek.kerberos	192.168.3.2	36421	192.168.1.100	88	specifiability/TEST.LOCAL	krbtgt/TEST.LOCAL
2024-09-19 18:47:47.043 -04:00	zeek.kerberos	192.168.3.2	43249	192.168.1.100	88	pedicularia/TEST.LOCAL	krbtgt/TEST.LOCAL
2024-09-19 18:47:46.872 -04:00	zeek.kerberos	192.168.3.2	33381	192.168.1.100	88	paunchily/TEST.LOCAL	krbtgt/TEST.LOCAL

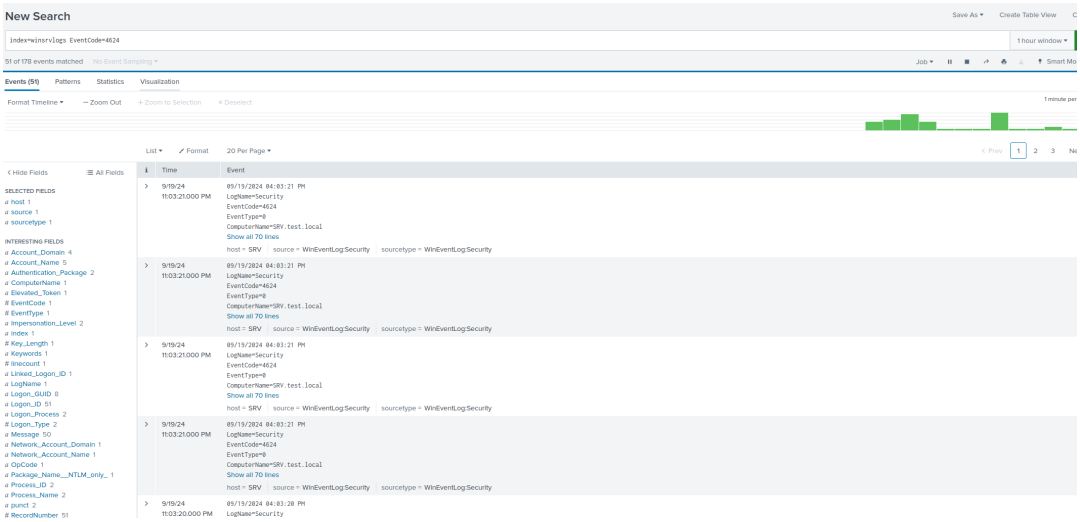
5. Go to Splunk server
    - logs associated with Kerberos attacks

```
index="winsrvlogs" kerberos
```



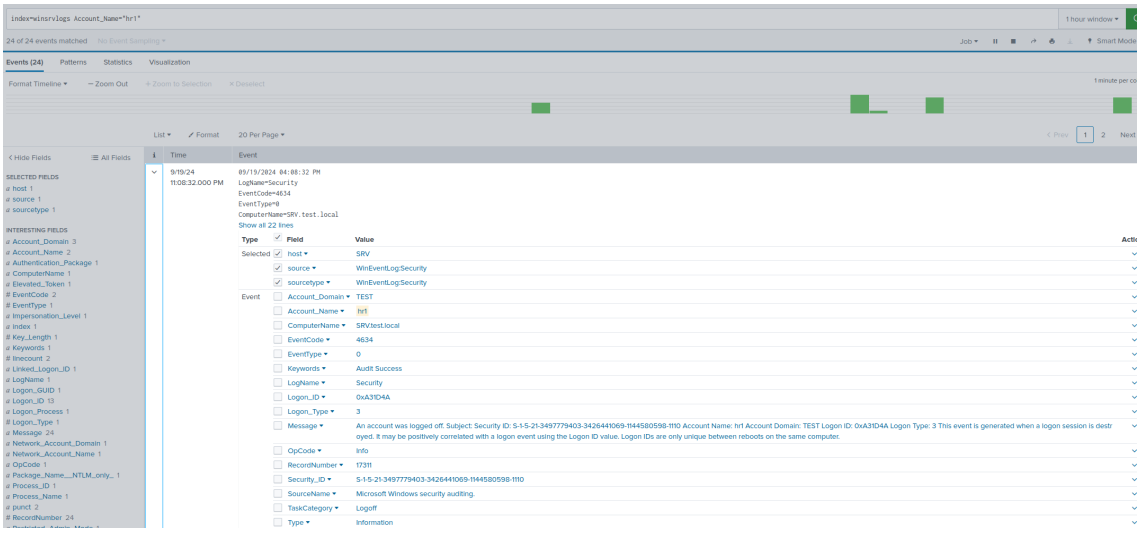
    - logs associated with logon session

```
index="winsrvlogs" EventCode=4624
```



- logs associated with my Windows 10 "hr1"

```
index="winsrvlogs" Account_Name="hr1"
```



login associated with EventCode 4624 and summarizes them by the host

```
index="winsrvlogs" EventCode=4624 | stats count by host
```