Security Monitoring in the telecommunication industry is important to keep daily operations running smooth, quickly detect bottlenecks, protect end users/customers.

Some days ago I had a session with 5 fellow cyber security analyst intern where we looked at multiple ways to keep a telecom environment and end users secure.

The logs used are still dummy logs, but are gotten from real world samples. After 2 days of intensive research, we found some critical security use cases, wrote some SPL queries to monitor suspicious activities, wrote correlation searches, and discover new information.

**What is IMSI(International Mobile Subscriber Identity)?**

This is a unique 15 digit number assigned to every mobile subscriber. It has the following format, MCC (3 digits) + MNC (2-3 digits) + MSIN (9-10 digits). For example, Nigeria has a country code of 272. The IMSI is stored on the SIM card. It is critical for network authentication and roaming. It is not known to end users. It is used for subscribers identification.

**What is MSISDN (Mobile Station International Subscriber Directory Number) ?**

This is the actual end user mobile number. The format is Country Code + Network Code + Subscriber Number.

This number is known to end users. It is used for voice calls, SMS, billing.

In summary, MSISDN is used for communication.

**What is Jitter, MOS\_score, latency?**

Jitter refers to the variation in packet arrival time. It is measured in milliseconds. When there is high jitter, it causes choppy voice calls, video call stutters. You know that moment when you are on a call and you cant properly hear the other person clearly, it’s caused by high jitter.

Latency refers to the time it takes for data to travel from source to destination. It is measured in milliseconds. A latency of <50ms is excellent. A high latency causes delays in video conferencing, affect call response time.

MOS(Mean Opinion Score) measures the quality of voice. A scoring of 5 is the best quality. Jitters and latency affect the MOS.

A typical telecommunication company, or a network service provider typically targets:

Jitter of <30ms

Latency of <100ms

Packet Loss of <1%

MOS score of > 4

**Critical Security Use Cases in Telecommunication**

*This is not an exhaustive list of security use cases in Telecommunication.*

* **SIM Swap Fraud :** In this scenario, a fraudster controls the victim’s phone number by transferring the number to a new SIM card without authorization.

For example,

John(fraudster) learns about Susan’s personal details (Address, Age, last bill amount, DOB)

John calls the network service provider to request new SIM on Susan’s behalf.

John provides all the stolen information gotten to NSP

Gets new SIM activated which John controls

Receives Susan’s SMS/calls, OTPs etc

John can use ussd to make payments from Susan’s bank account.

How to prevent this from happening to you is :

* Never share personal information online.
* Use strong passwords
* Use multiple 2FAs
* Never share OTPs
* Verify unexpected requests
* **SIM Boxing Fraud:** This refers to illegally terminating International call as local call.
* **SIM spoofing:** This refers to impersonating caller ID to display different number than actual number.
* **Porting Fraud:** This refers to the unauthorized transfer of phone number from one network service provider to another.

This techniques are used by fraudsters to perform more complex frauds.

1. SIM Swap is used to take over number
2. SIM porting is used to port to different carrier of NSP to avoid detection
3. SIM spoofing is used to social engineer more information from victim.
4. The compromised number is used for further fraud. Eg, perform transactions on victim’s behalf, clear victim bank account etc

Without further ado, read through the comprehensive project (link) to see how we monitored the different logs for suspicious activities.

**Project :** Telecom Network Performance Monitoring and Security Analytics using Splunk

**Objective:** Design and implement a Splunk – based monitoring system to analyze network performance and security threats in a telecommunication environment.

**Environment:**

* Telecom provider with 10million subscribers
* Network Infrastructure comprising 1000+ cell towers, 500+ routers, 200+ switches
* Data Sources: Network devices, Call Detail Records, SIM data

**Project Requirements:**

1. Monitor network performance metrics
2. Analyze CDR, SIM data, Network devices logs for fraud detection
3. Provide real-time dashboard and alerting.

**Project Benefits:**

1. Improved network performance monitoring
2. Enhanced security threat detection
3. Reduced fraud detection time
4. Real time visibility into network operations.

**Project Metrics:**

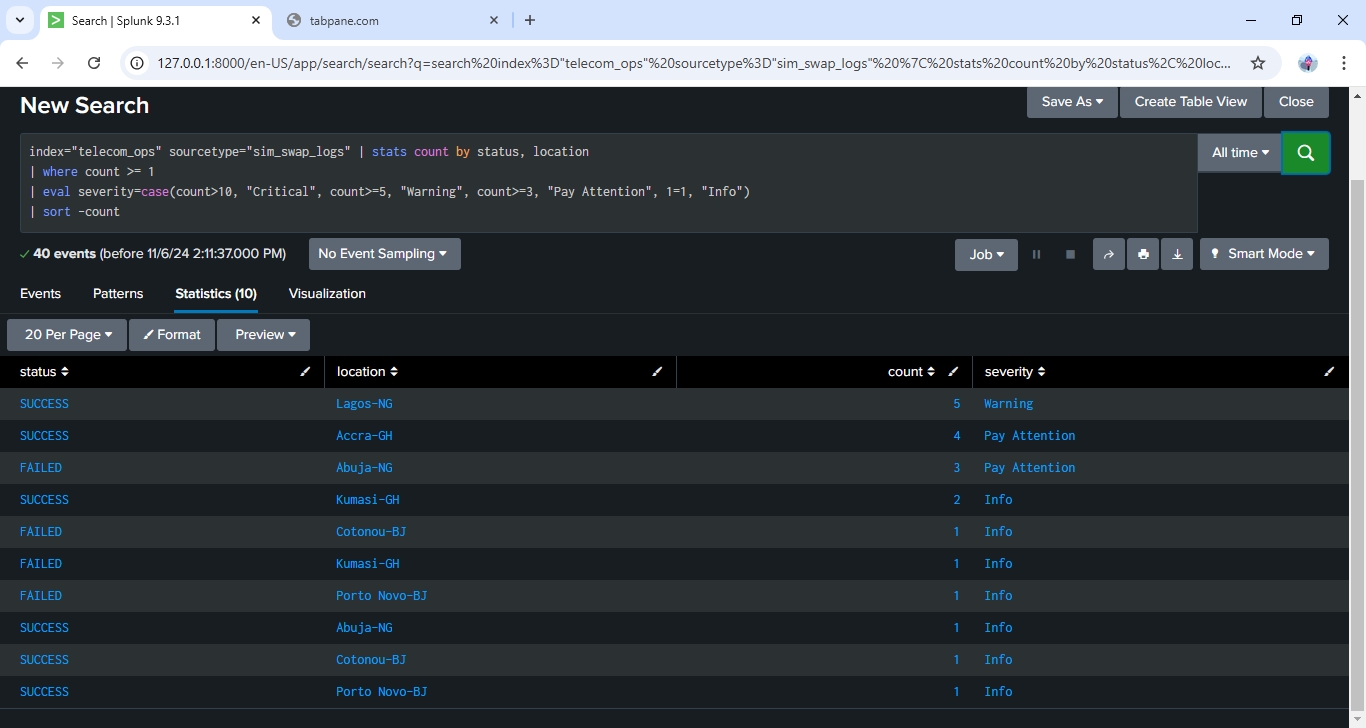
1. 99.9% network uptime
2. 90% reduction in security threats
3. 95% reduction in mean time to detect
4. 90% reduction in mean time to resolve

**Project Team:**

In as much as this was done by cyber security analyst interns as a side project, in a production environment it will comprise ***2 Splunk Administrators, 1 – 2 network engineers, 2-3 security engineers, 1 ITMS specialist.***

Monitoring SIM Swap Activities

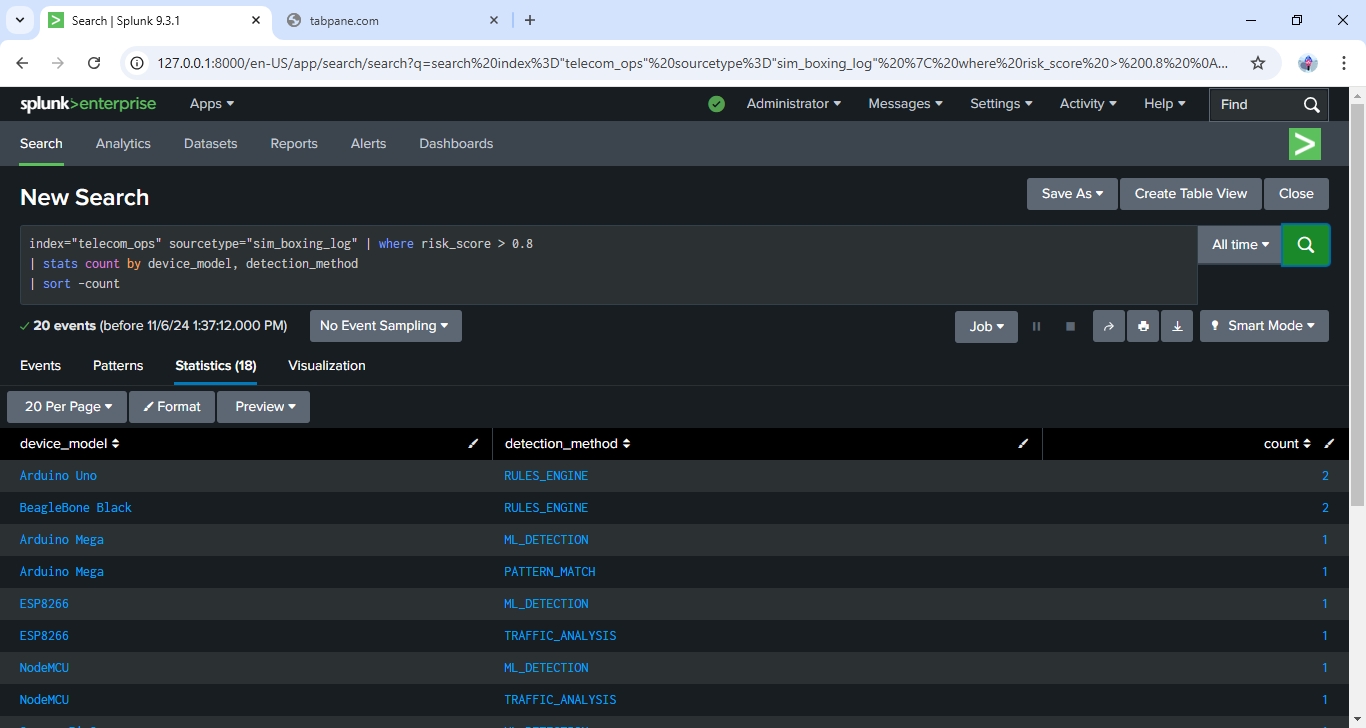
We start first by monitoring SIM Swap activities. If there are 5 and above SIM Swap request, it will be flagged as a warning, 4 and above is flagged as Pay Attention, 1 and above is Informational.



*Monitoring SIM Swap*

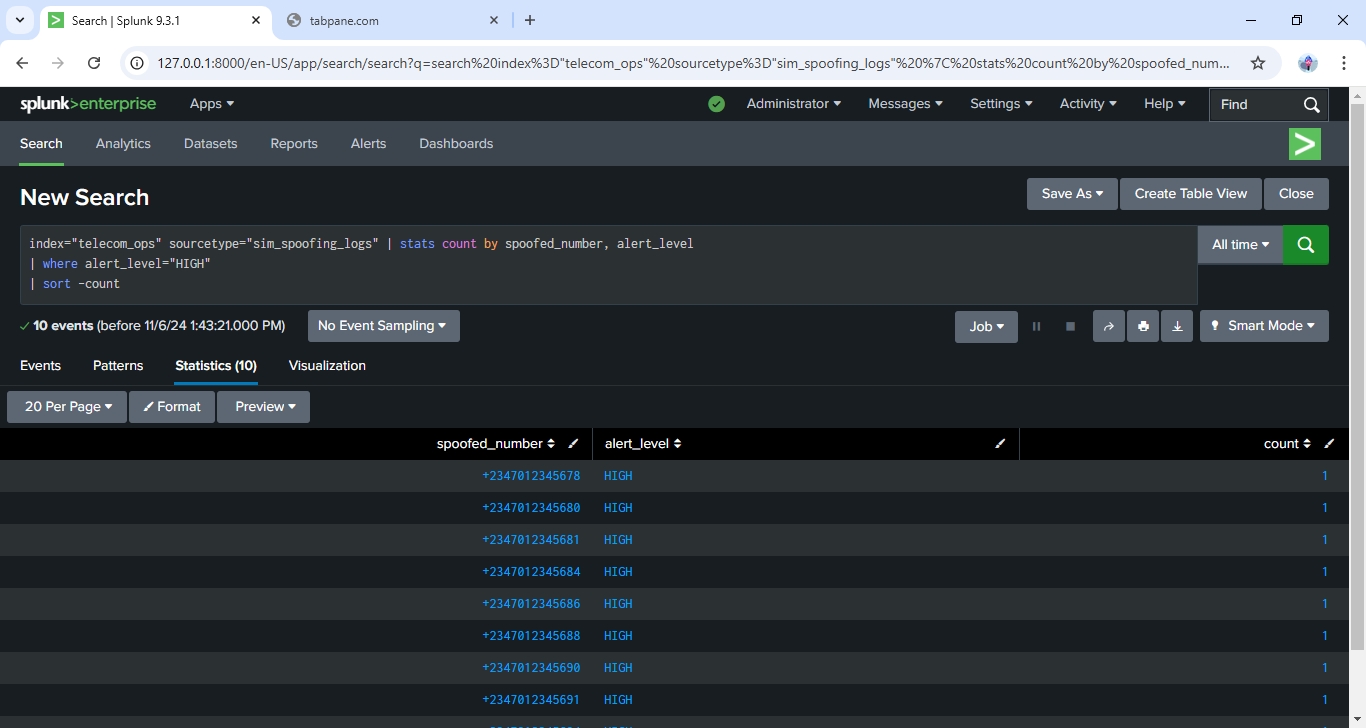
Monitoring SIM Boxing Fraud

Next we monitor SIM boxing fraud and detect the device used as the box. If the location field was added, then the location where the boxing fraud took place will be monitored



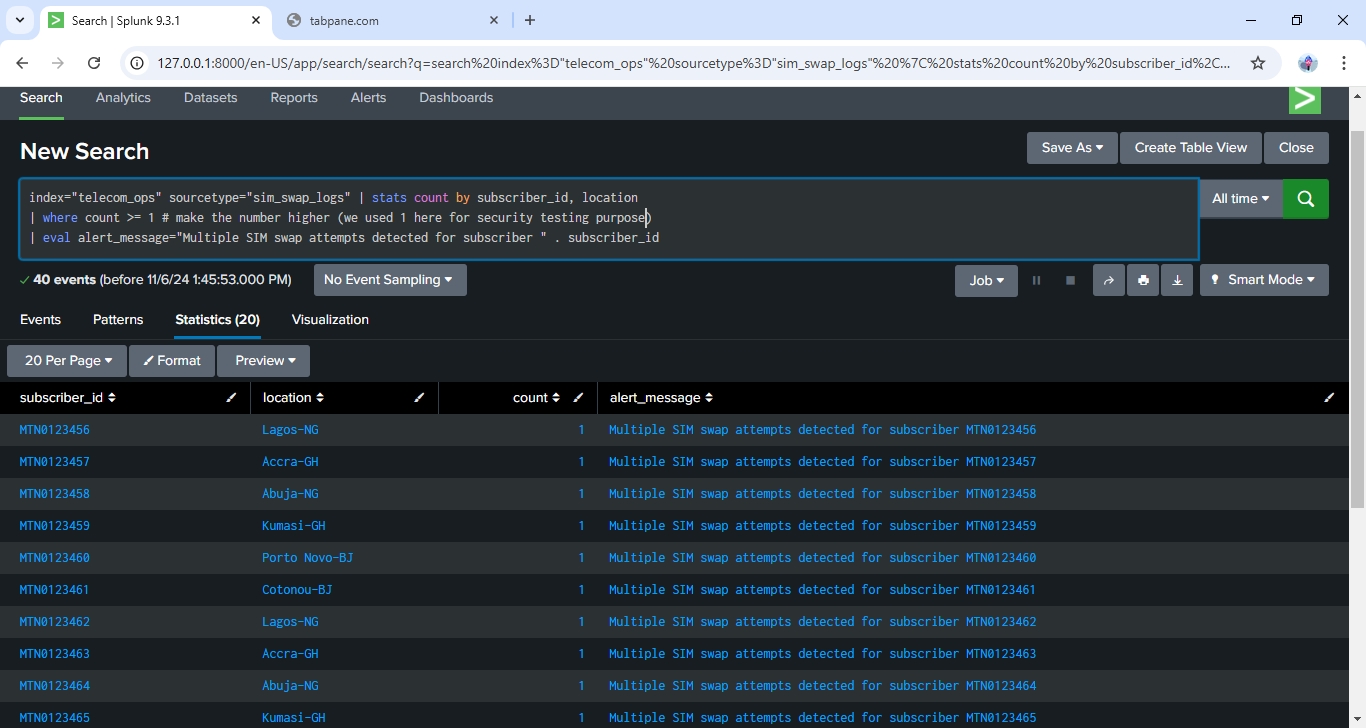
*Monitoring SIM boxing fraud*

Monitoring SIM spoofing attempts

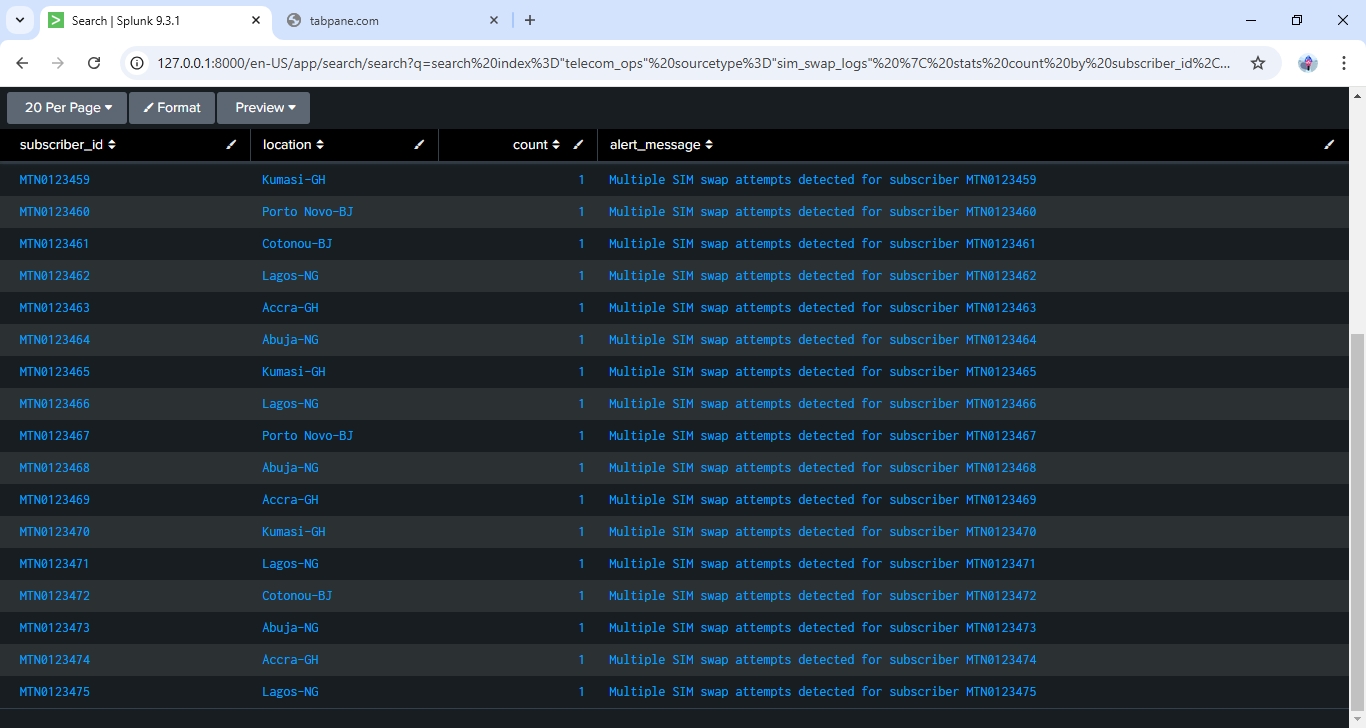
We detected the spoofed numbers. The alert level was set as ***HIGH,*** but fortunately from the logs, there were no successful spoofing attempts. 

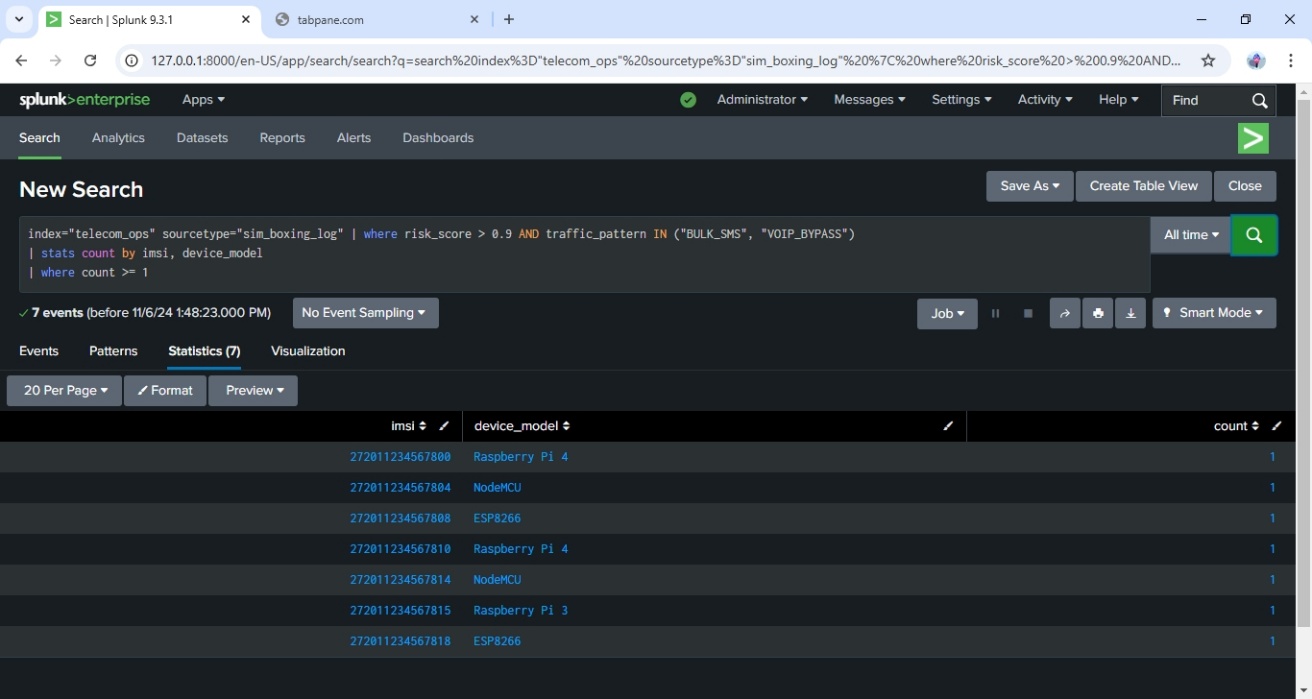
Generating Alerts for SIM Swap attempts

In this instance a fraudster might want to request a SIM Swap for a compromised user. In other to mitigate this from happening, once an unauthorized SIM Swap is detected an alert is generated. ***The alert is sent as mail to a recipient and also added to the Triggered List, although it isn’t shown in this project, you can refer to the previous project to see how to create alerts in Splunk.***



*Alert for SIM Swap attempt*

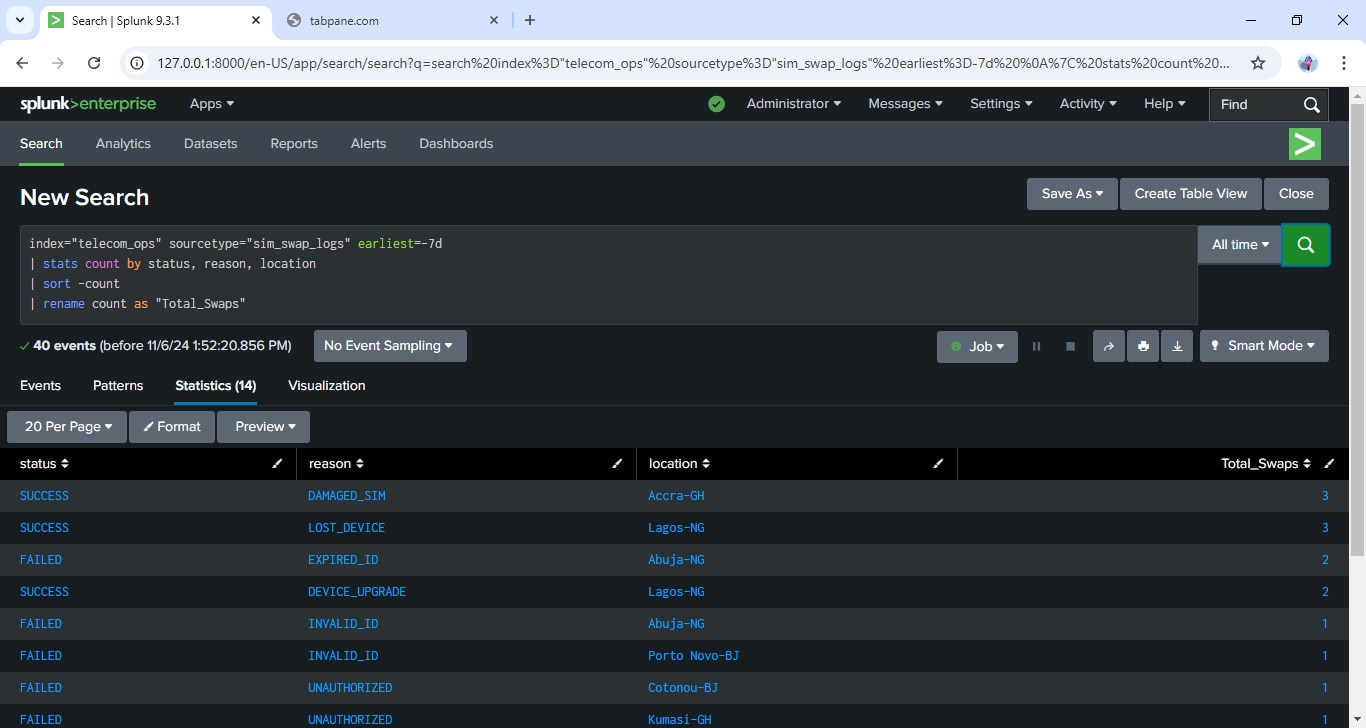


Generating Alerts for suspicious SIM Boxing Fraud

In this case we want to know the IMSI and the device model used for the SIM Boxing fraud. Once the IMSI is found, actions can then be taken to either ban that number or remove it out rightly.

Report for Total SIM Swap Request

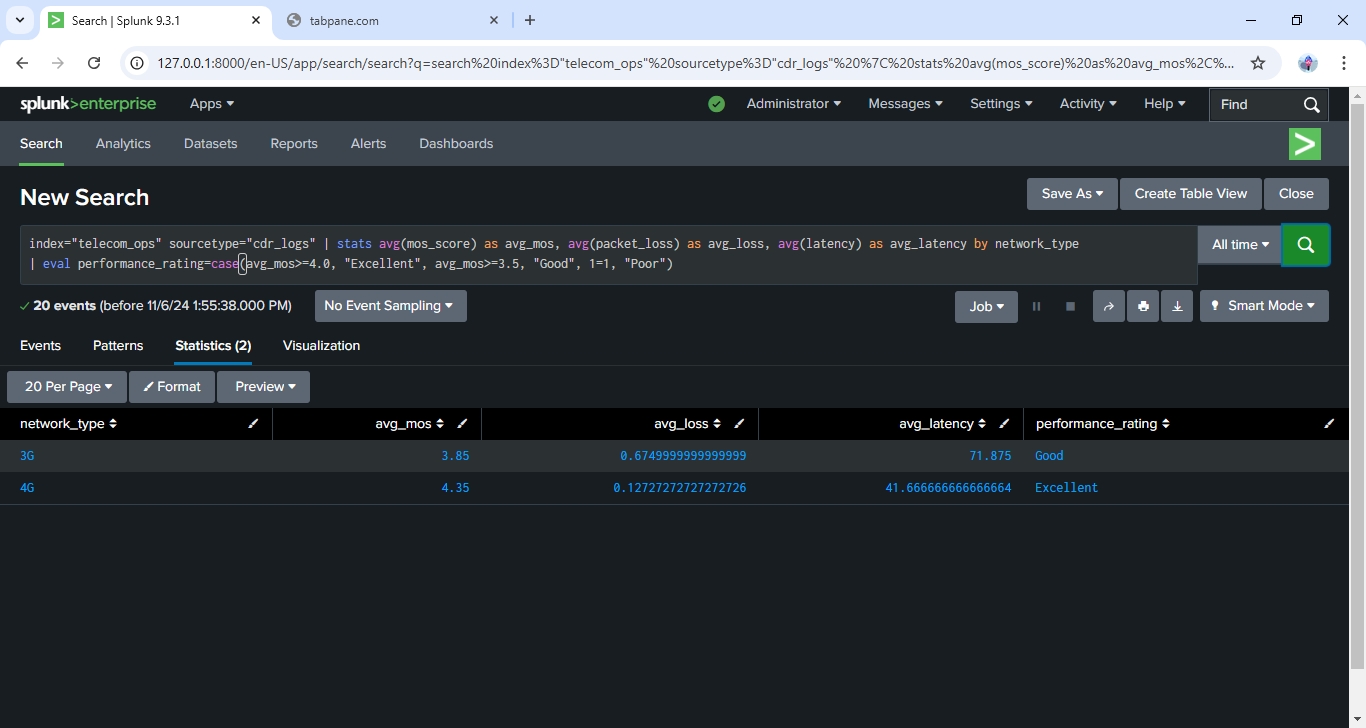
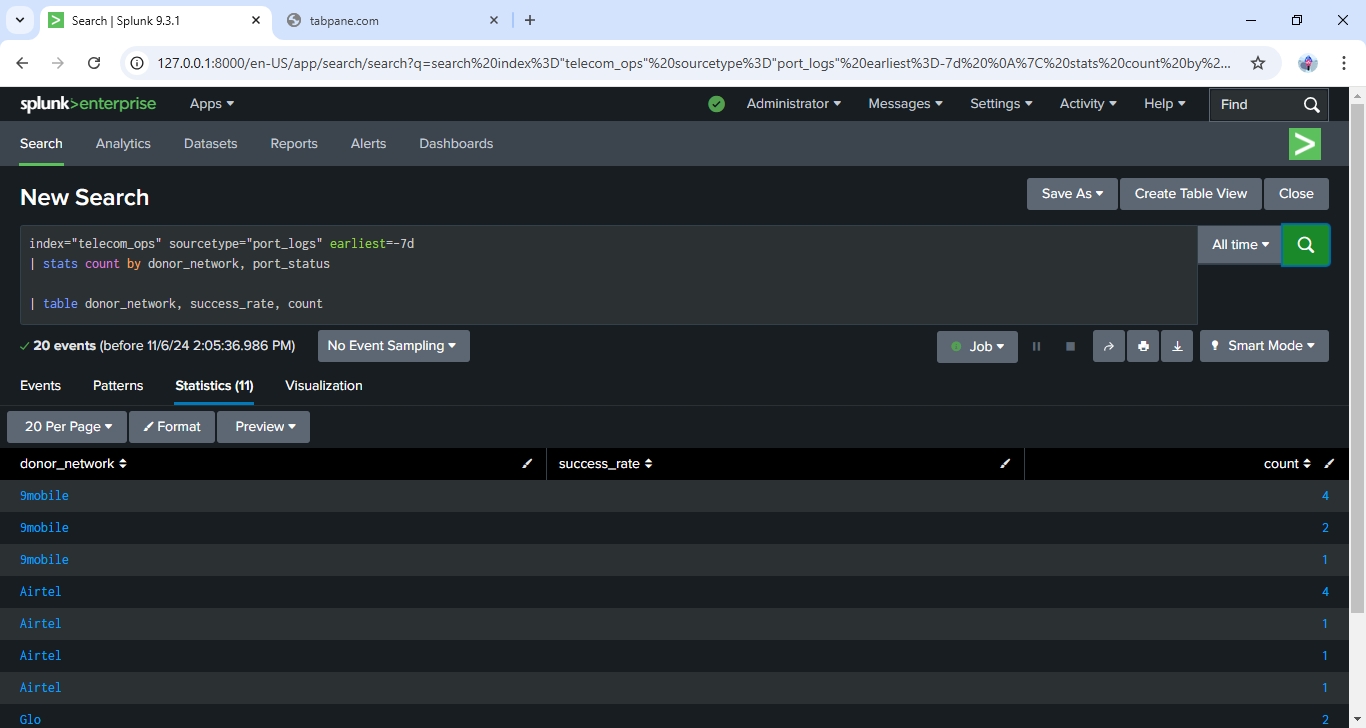
In this instance we wrote SPL query to generate a report that shows SIM Swap request over a duration. The successful swap request and the reason for the request by country was displayed. This report can then be sent to higher management or the incident response team.



*Report for SIM Swap request by country and reason for request*

SIM Porting Request Analysis

A report is also generated from this query that shows the sim porting request based on a duration. It shows the donor network and the count of porting request.

******

*Result for SIM porting request*

*Result for Quality of Service*

QOS Performance Dashboard

In this scenario the quality of service is monitored and daily dashboard can be generated to show the performance of the network.

So far from the result, it is seen that 3G and 4G network are working well, with the 4G network having an “***excellent***”.

Correlation Search

Finally we wrote a query to correlate the logs from ***sim\_swap\_logs*** and ***sim\_boxing\_logs***



Author: Praise Jah Olotu

Date Written: 06/11/2024

©2024

**No part of this article can be modified, published, transmitted without author’s authorization and acknowledgement.**