CYBERSECURITY PRESENTATION PREP

Understanding your 15-minute time constraint with a live demo included, I'll help you streamline the presentation to focus only on the most essential topics.

Here's a focused outline for a 15-minute presentation that includes time for a live demo:

**Essential Topics for 15-Minute Presentation (with Demo)**

**1. Brief Introduction (2 minutes)**

* Quick definition of Blue Teaming: "The defensive side of cybersecurity"
* One striking statistic: "Average data breach costs $4.45 million"
* Why it matters to your audience specifically

**2. Core Blue Team Functions (3 minutes)**

Focus on just these three critical functions:

* **Threat Detection**: Identifying potential security incidents
* **Incident Response**: Containing and remediating threats
* **Continuous Monitoring**: Maintaining vigilance across systems

**3. What is SIEM? (2 minutes)**

* Simple definition: "A tool that collects and analyzes security data from multiple sources"
* The problem it solves: "Connecting dots across disparate systems"
* Quick visual showing basic SIEM workflow (collection → analysis → alerting)

**4. Live Demo (5 minutes)**

* Show a basic SIEM dashboard (Splunk free version or similar)
* Demonstrate a simple use case: brute force attack detection
* Walk through the alert, investigation, and response process

**5. Key Defensive Strategies (2 minutes)**

Focus on just two practical strategies:

* **Effective Log Management**: "You can't detect what you don't see"
* **Automated Response**: How SIEM can trigger actions to contain threats

**6. Conclusion (1 minute)**

* One key takeaway: "Proactive defense is more cost-effective than recovery"
* Next steps for the audience
* Brief Q&A if time permits

**Tips for Your 15-Minute Presentation**

1. **Practice your demo repeatedly** to ensure it runs smoothly within the time limit
2. Have a backup plan (screenshots/video) in case of technical issues
3. Limit each slide to one key concept with minimal text
4. Use visuals rather than text wherever possible
5. For the demo, prepare a simple script with clear steps to follow
6. Focus on practical value rather than technical details
7. Consider preparing handouts with additional information for those who want to learn more

This streamlined approach covers the essentials while allowing time for your live demonstration, which will be the most valuable and memorable part of your presentation.

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

Network Security Best Practices (#31) – MATCHES OUR TOPIC

**Blue Teaming & SIEM: Defending Against Cyber Threats**

**Introduction**

So when we talk about cybersecurity, there are two main approaches - attacking and defending. Blue teaming is all about defense. These are the people working behind the scenes to protect organizations from cyber threats.

Think of it like this: while hackers are trying to break in, blue teams are the ones building walls, setting up alarms, and watching for suspicious activity. What's shocking is that the average data breach now costs companies about $4.45 million - that's why this work matters so much.

**Core Blue Team Functions**

Blue teams have three main jobs that are absolutely essential:

First, they detect threats - basically looking for anything suspicious in the network. This could be unusual login attempts, strange file activities, or connections to suspicious websites.

Second, they respond to incidents. Once something suspicious is found, they need to contain it before it spreads, figure out exactly what happened, and then fix it. It's like being a cybersecurity firefighter.

Third, they monitor everything continuously. Security isn't a one-and-done thing - it's 24/7 vigilance across all systems. They're constantly watching logs, network traffic, and user activities for anything that doesn't look right.

**What is SIEM?**

This is where SIEM comes in - Security Information and Event Management. It's basically the blue team's radar system.

A SIEM collects logs and security data from all over your network - your firewalls, servers, workstations, cloud services, everything. Then it analyzes this data and connects the dots between events that might seem unrelated.

For example, a failed login on its own might not be concerning, but when combined with unusual network traffic and a new process running on that same machine, the SIEM can flag this as a potential attack.

The beauty of SIEM is that it can analyze more data than humans ever could, and it can do it in real-time.

**Live Demo**

[For this section, I'd show a basic SIEM dashboard in real-time]

Let me show you what this looks like in practice. Here's a SIEM dashboard - notice how it gives us visibility across the entire network.

Now, let's simulate a brute force attack. This is where someone tries to guess a password by attempting many combinations.

See how the SIEM is collecting these failed login attempts? At first, they look like normal failures. But watch what happens when we hit a threshold of, say, 10 failed attempts in 2 minutes from the same IP address.

The SIEM automatically generates this alert, categorizing it as a potential brute force attack. Now as a blue team analyst, I can click into this alert and see all the details - the username being targeted, the source IP, the timestamps of each attempt.

If I determine this is a real attack, I can take action right from the SIEM. Let me show you how I can automatically block this IP address across all our firewalls with just a couple of clicks.

**Key Defensive Strategies**

Beyond having a SIEM, there are two critical strategies every organization needs:

First, effective log management. You simply can't detect what you don't see. If your servers, firewalls, or cloud services aren't sending logs to your SIEM, you have blind spots that attackers can exploit. It's like trying to secure a house but not putting sensors on some of the windows.

Second, automated response is key. The average breach takes over 200 days to detect and another 70 days to contain. But with automation, your systems can respond in seconds. For example, if the SIEM detects a compromised account, it can automatically disable that account before the attacker does more damage.

**Conclusion**

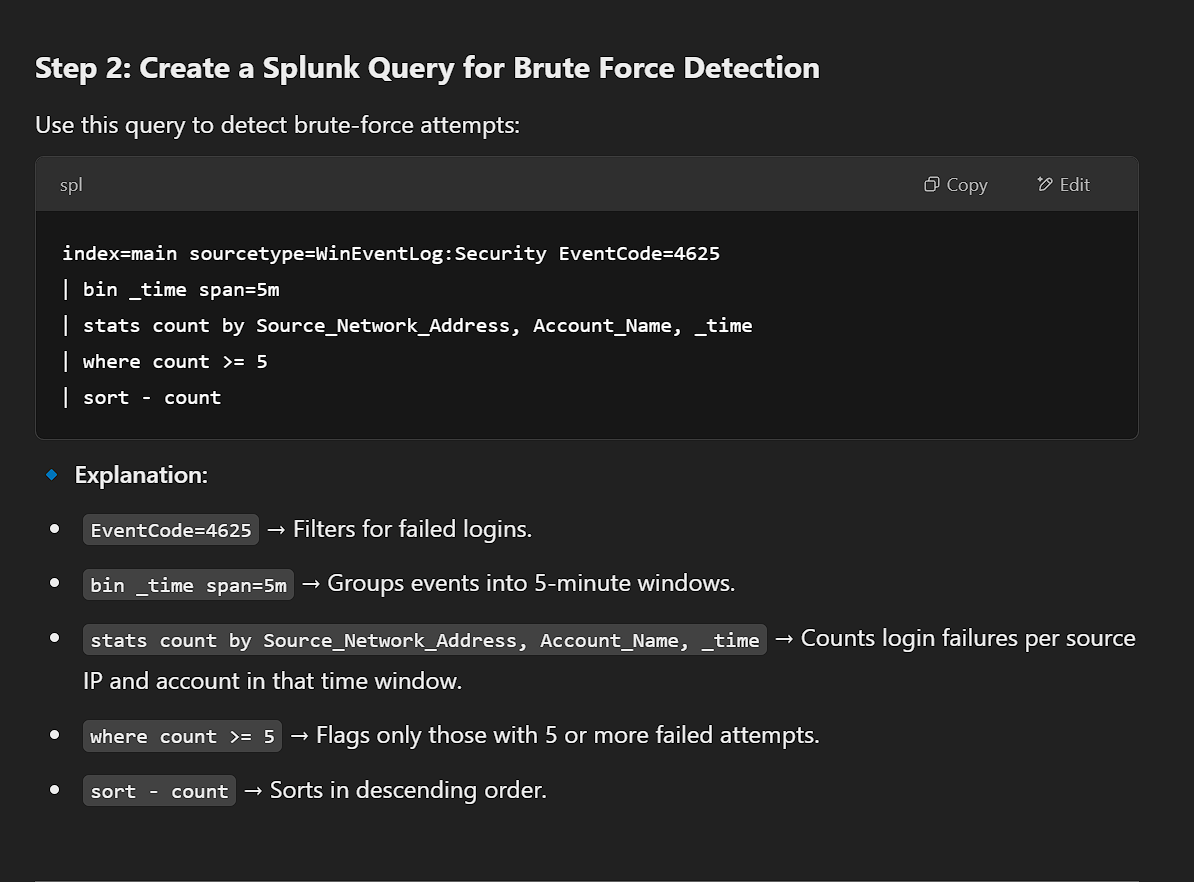
The bottom line is this: cyberattacks are inevitable, but having effective blue team operations with tools like SIEM dramatically reduces both the likelihood and impact of breaches. It's always cheaper to prevent an attack than to recover from one.

For those of you interested in this field, starting as a SOC Analyst is a great entry point. The skills you learn there - log analysis, incident response, threat detection - these are foundational to a career in cybersecurity.

Are there any questions about blue teaming or SIEM that I can answer for you?

<https://chatgpt.com/share/67ddbdad-13c0-8012-9a55-c434476f0c34>

refer above link for practicle SIEM simulation live demo



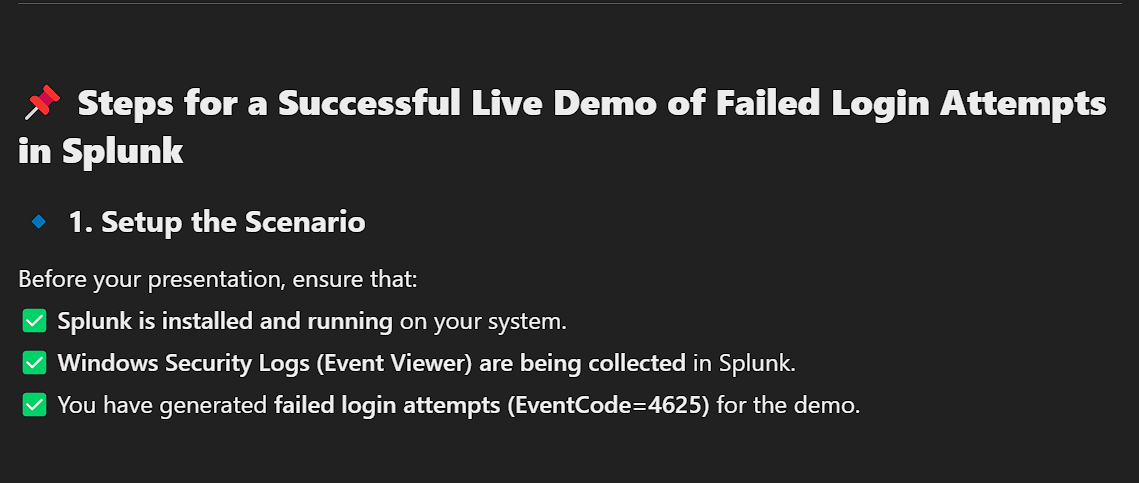
index=main sourcetype=WinEventLog:Security EventCode=4625

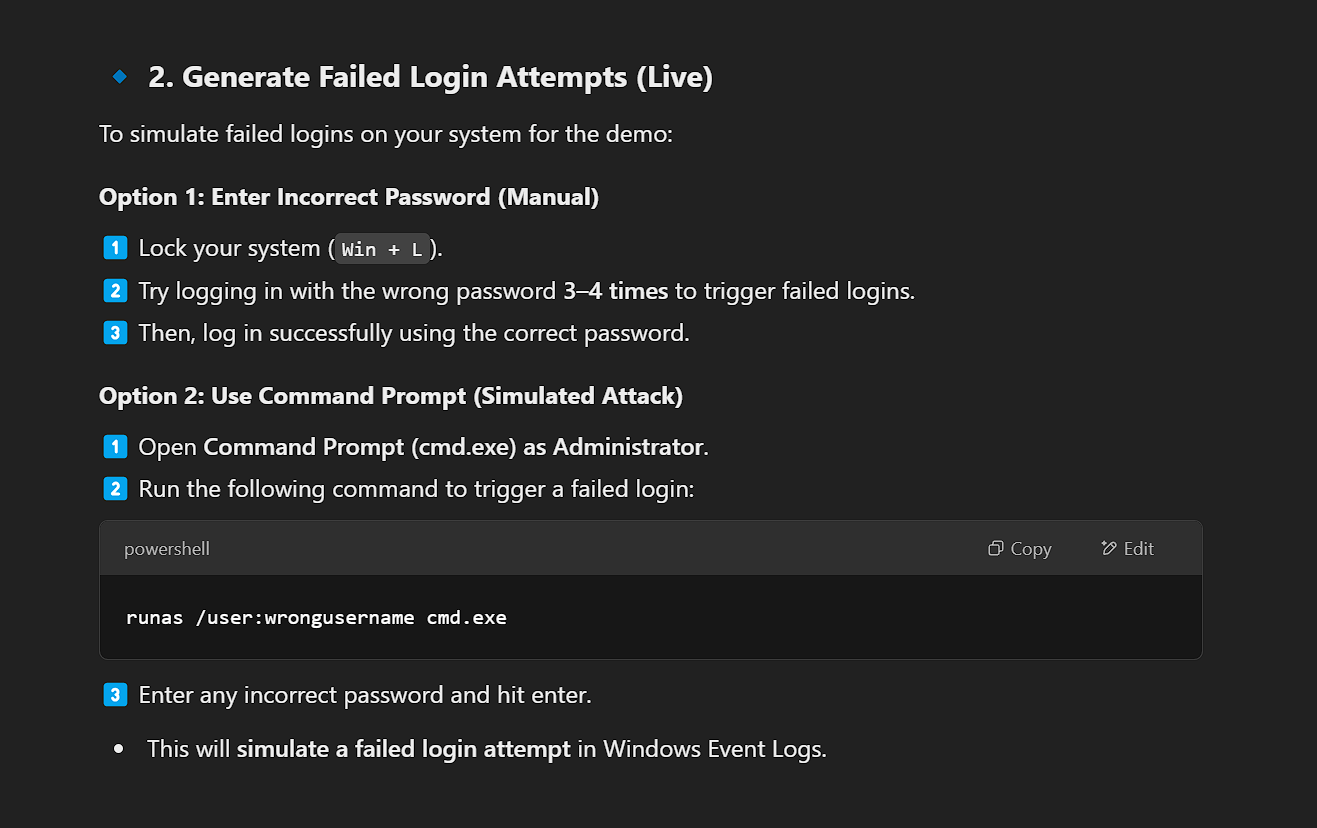
| bin \_time span=5m

| stats count by Source\_Network\_Address, Account\_Name, \_time

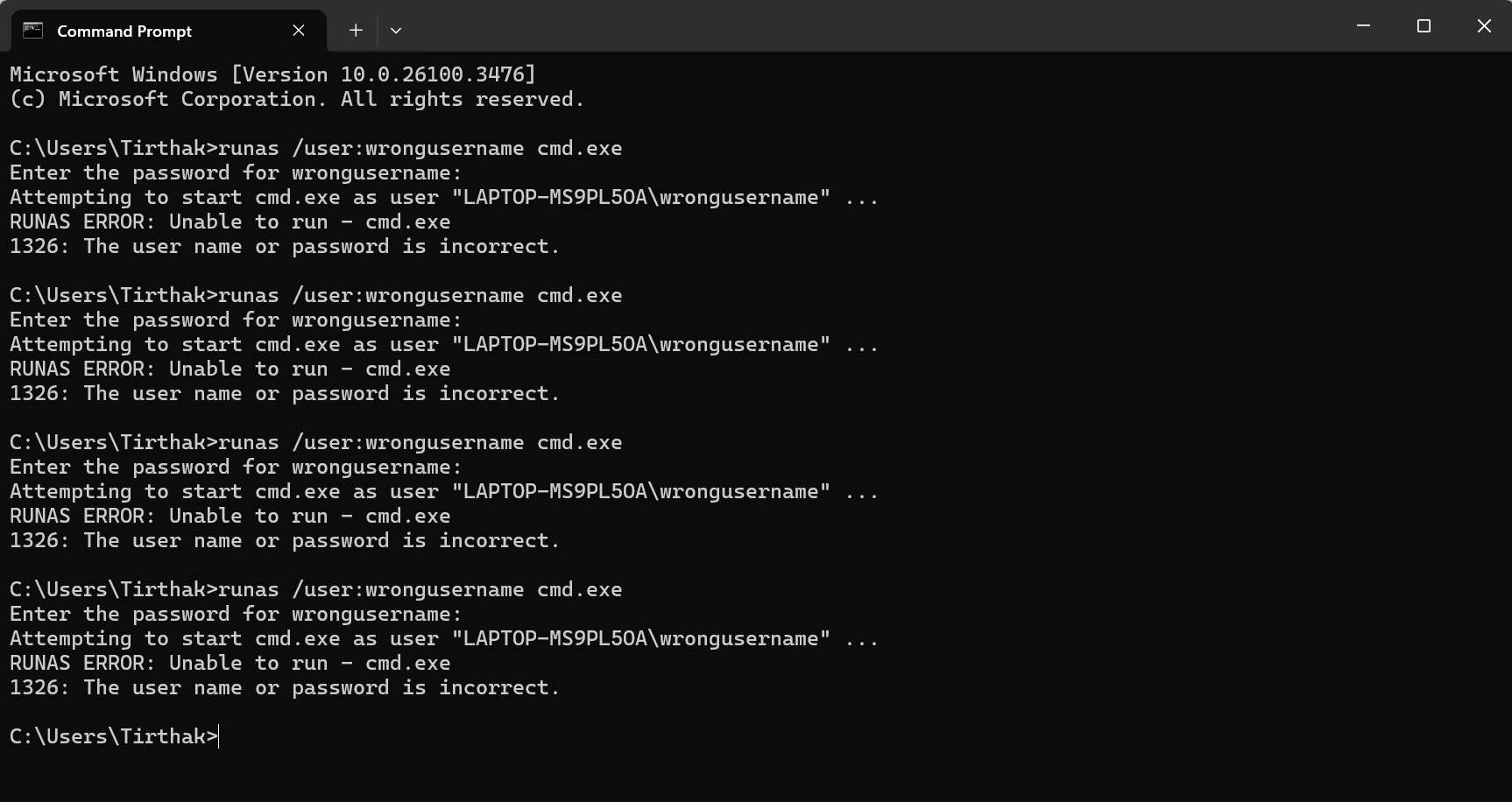
| where count >= 5

| sort – count

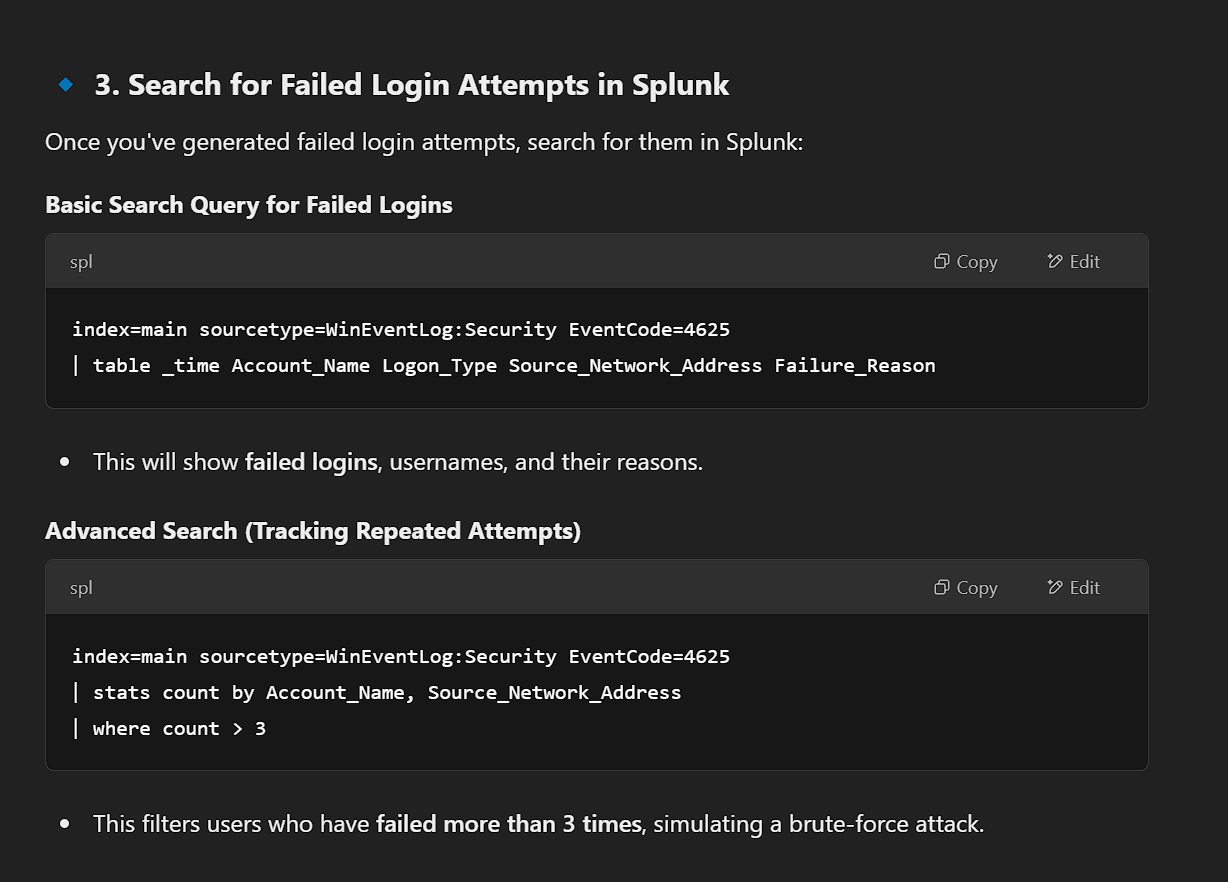




runas /user:wrongusername cmd.exe



Now this will generate failed Login attempts in the windows log

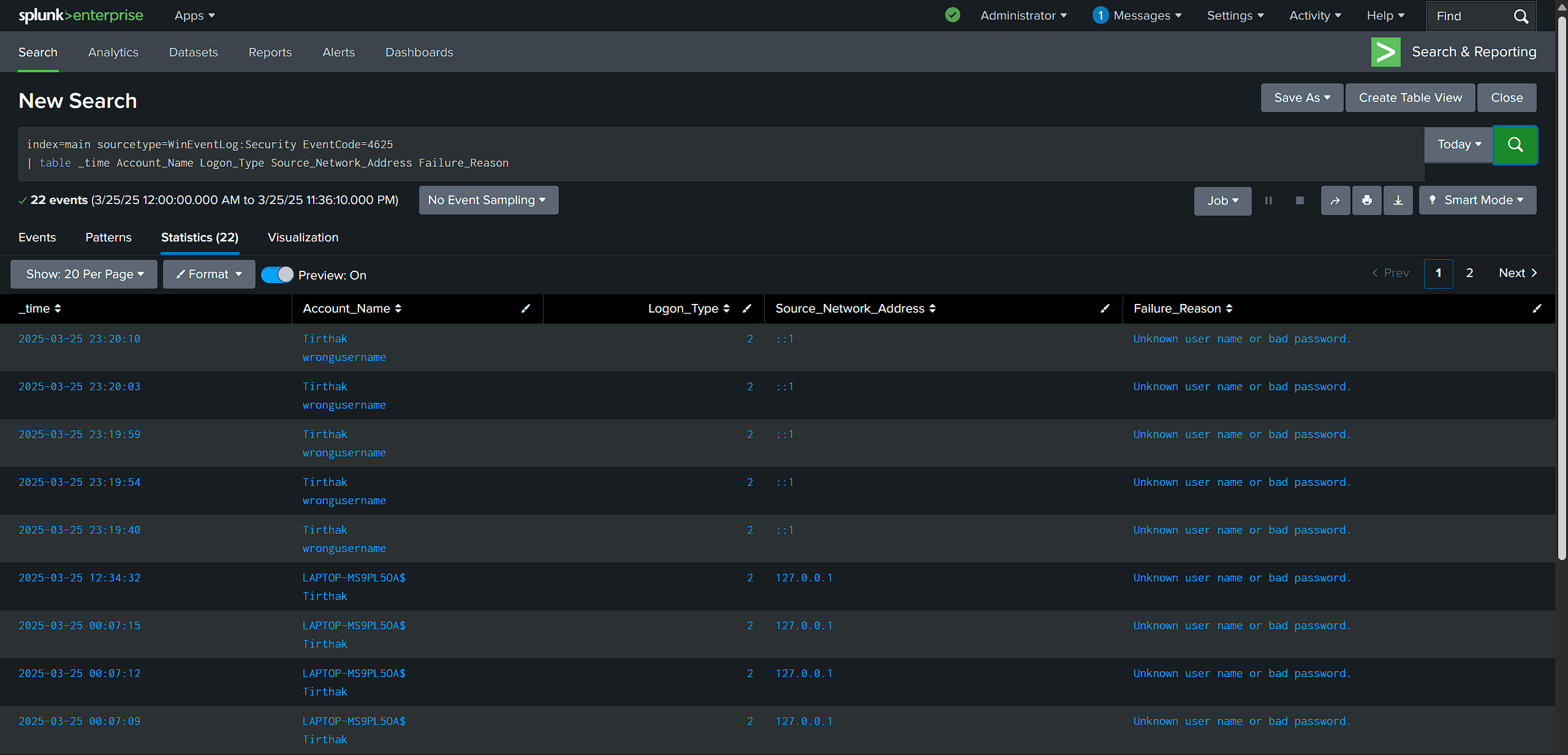


**O)Basic Search Query for Failed Logins**

index=main sourcetype=WinEventLog:Security EventCode=4625

| table \_time Account\_Name Logon\_Type Source\_Network\_Address Failure\_Reason

This will show ***failed logins, usernames, and their reasons*.**



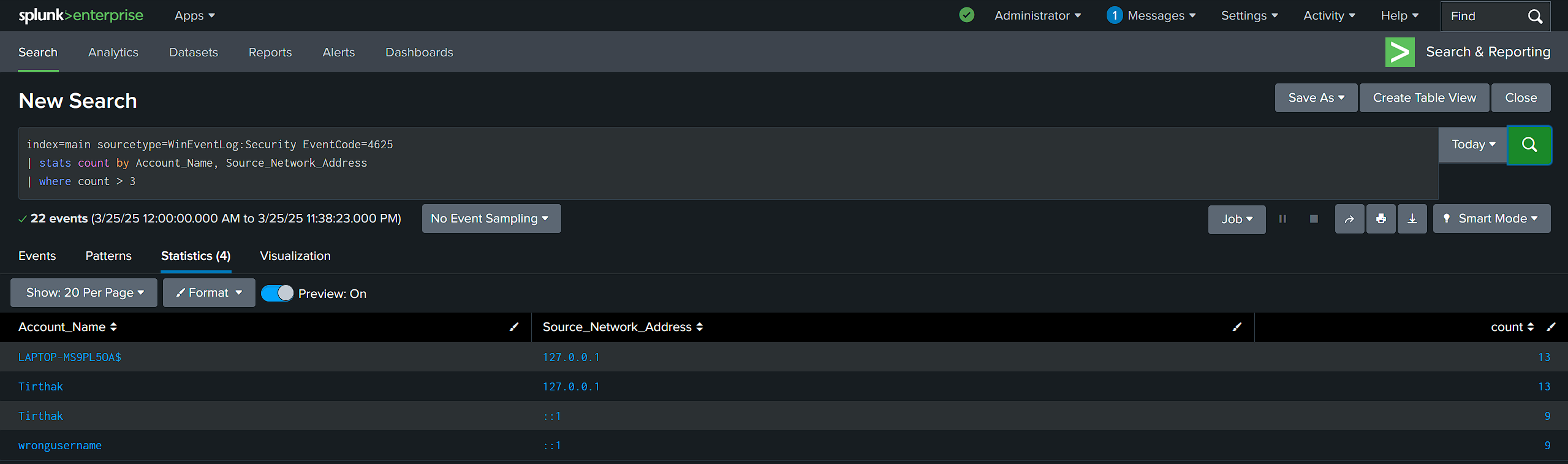
**O)Advanced Search (Tracking Repeated Attempts)**

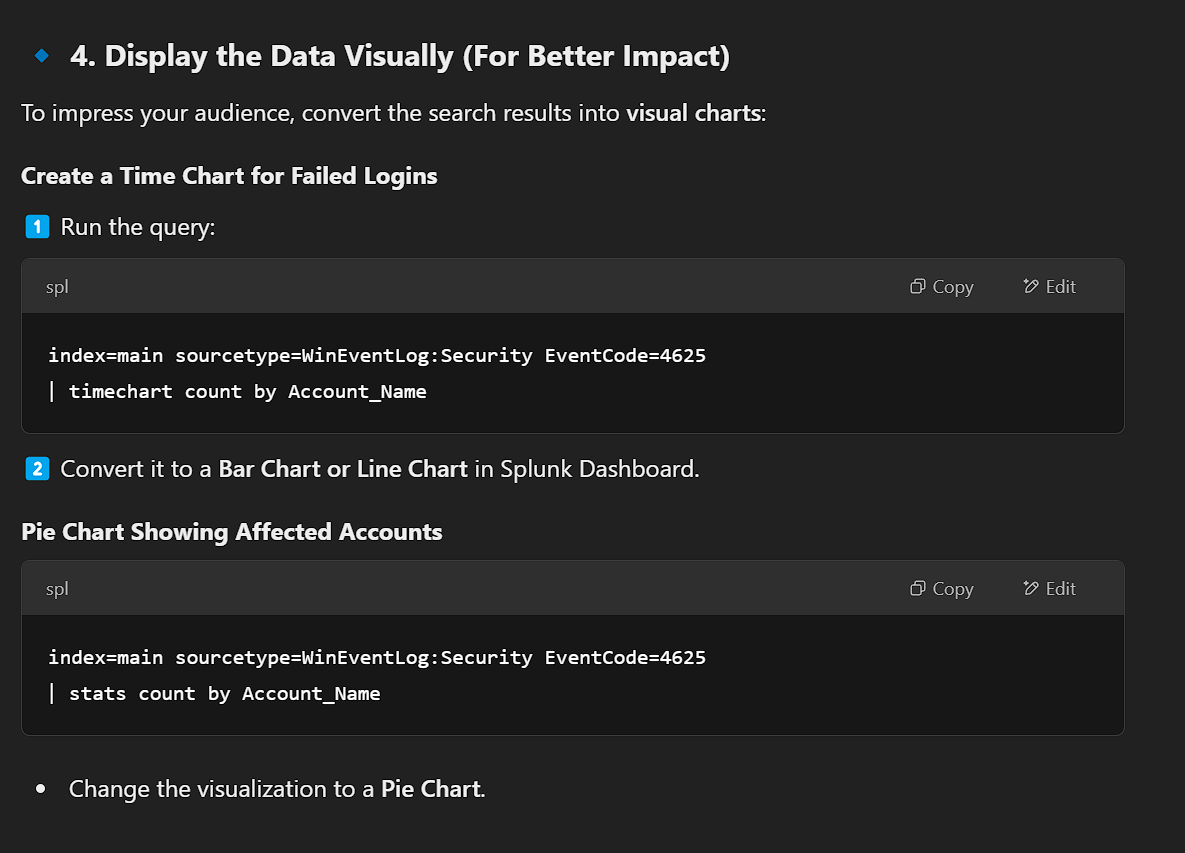
index=main sourcetype=WinEventLog:Security EventCode=4625

| stats count by Account\_Name, Source\_Network\_Address

| where count > 3

This filters users who have **failed more than 3 times**, simulating a brute-force attack.



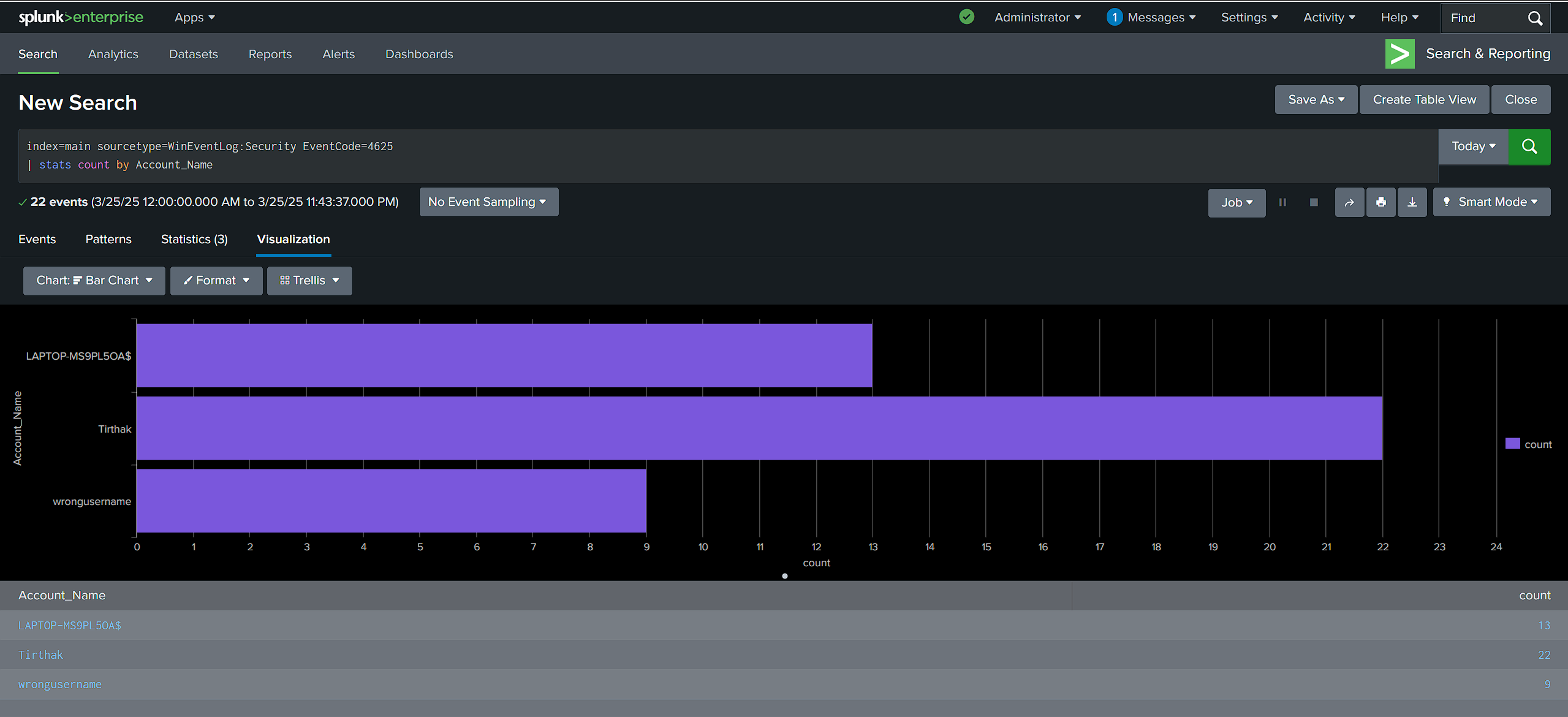


**O)Create a Time Chart for Failed Logins**

index=main sourcetype=WinEventLog:Security EventCode=4625

| timechart count by Account\_Name

Convert it to a **Bar Chart or Line Chart** in Splunk Dashboard.

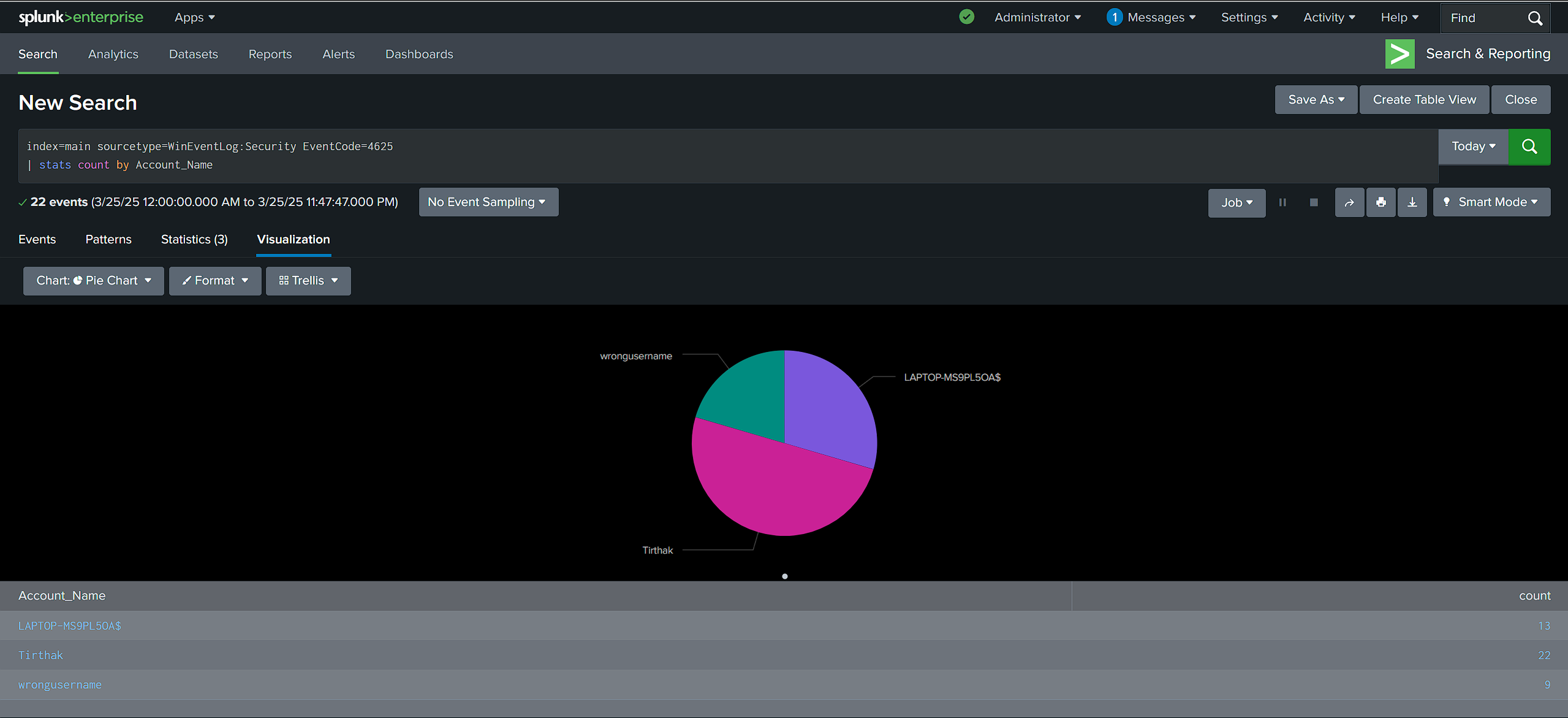


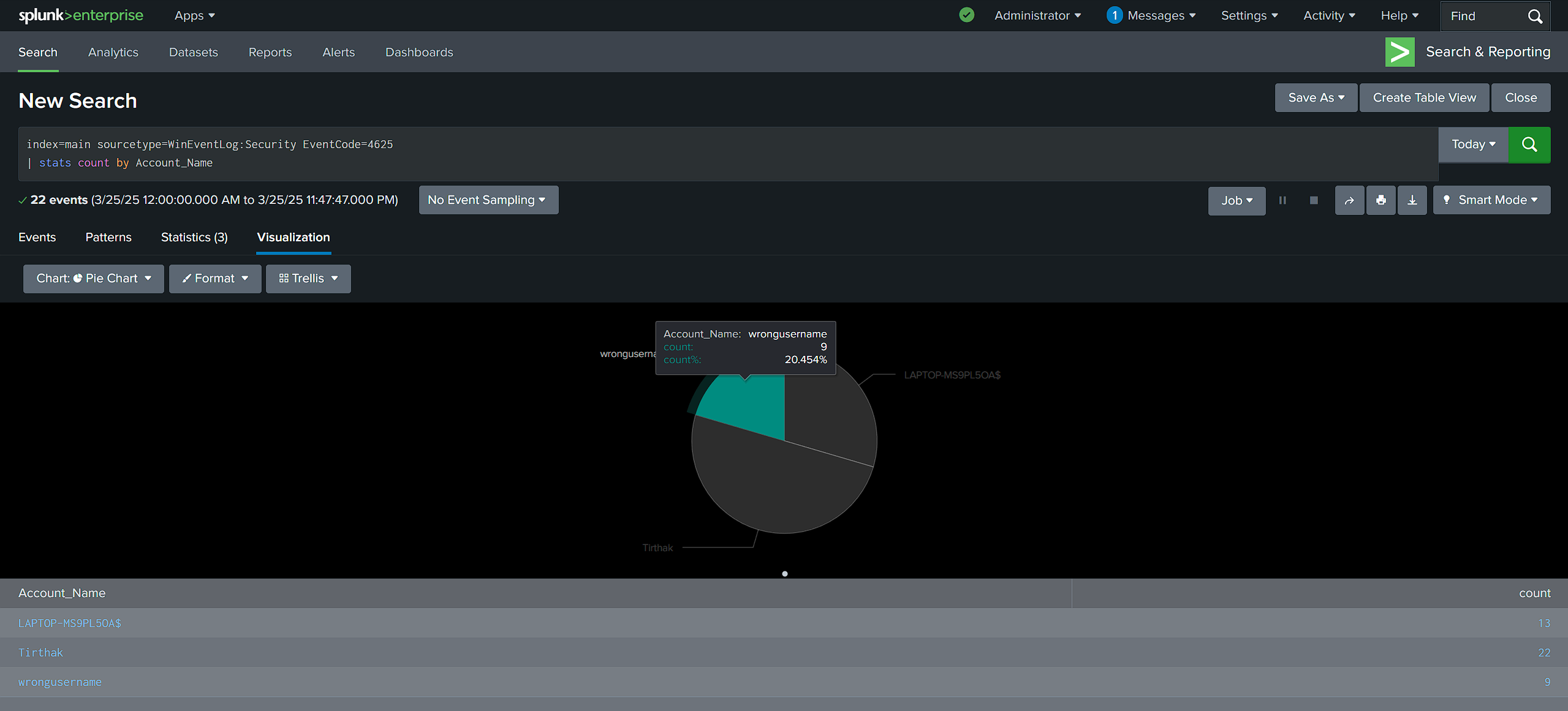
**O) Pie Chart Showing Affected Accounts**

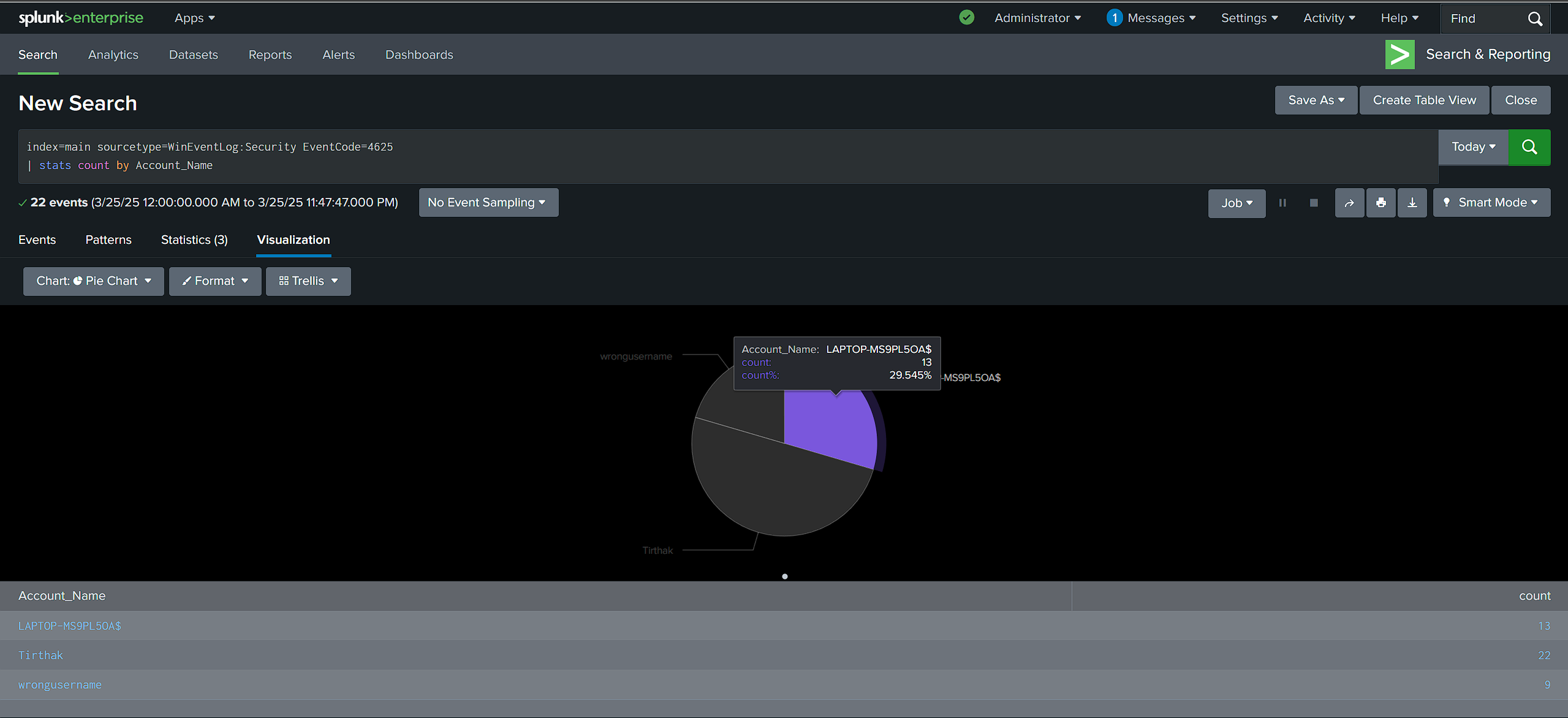
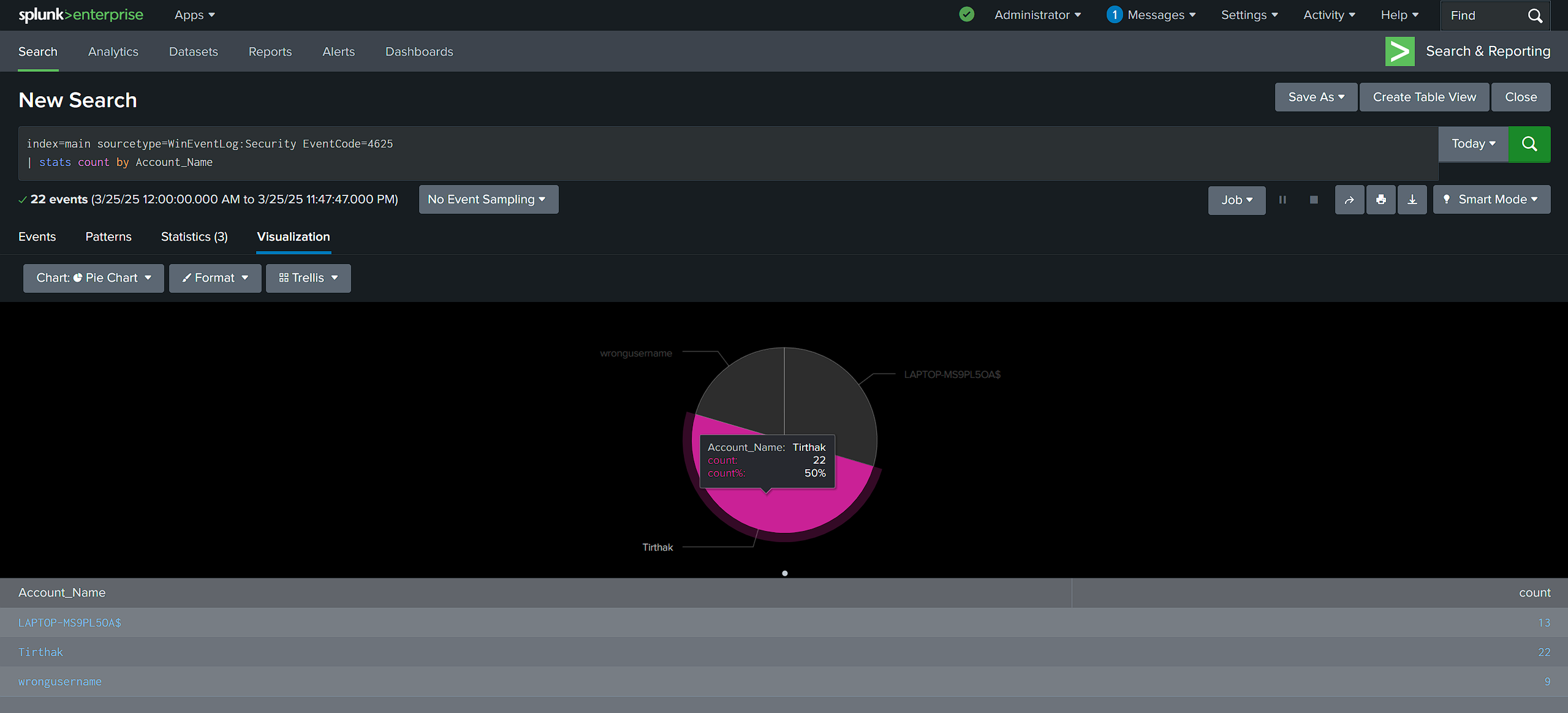
index=main sourcetype=WinEventLog:Security EventCode=4625

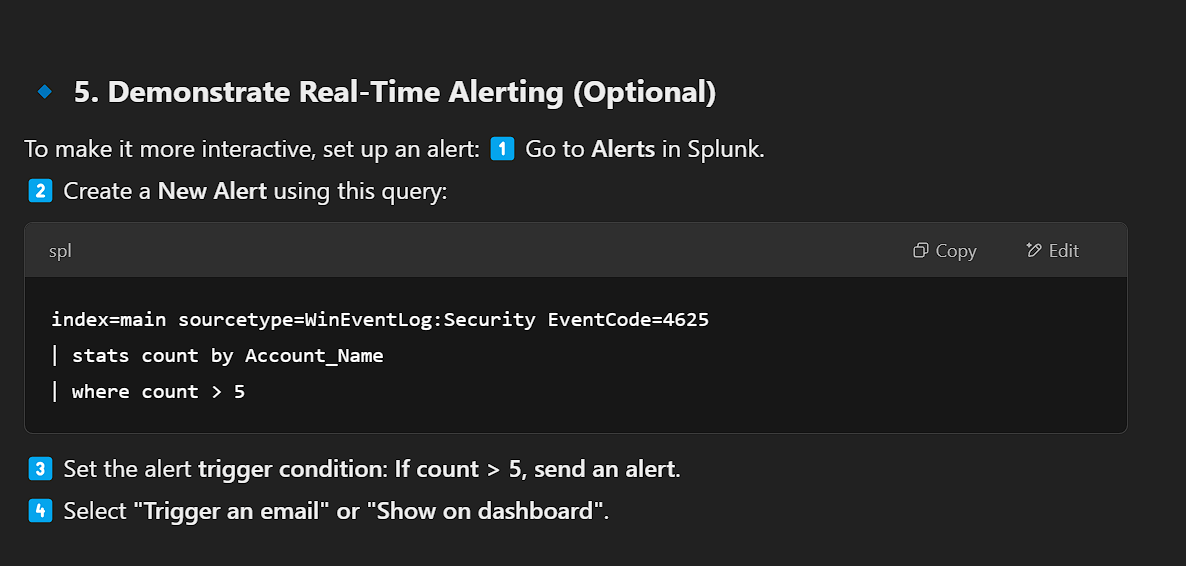
| stats count by Account\_Name

Change the visualization to a **Pie Chart**.







**O)Create a New Alert using this query**

index=main sourcetype=WinEventLog:Security EventCode=4625

| stats count by Account\_Name

| where count > 5

Set the alert **trigger condition**: **If count > 5, send an alert**.  
Select **"Trigger an email" or "Show on dashboard"**.

