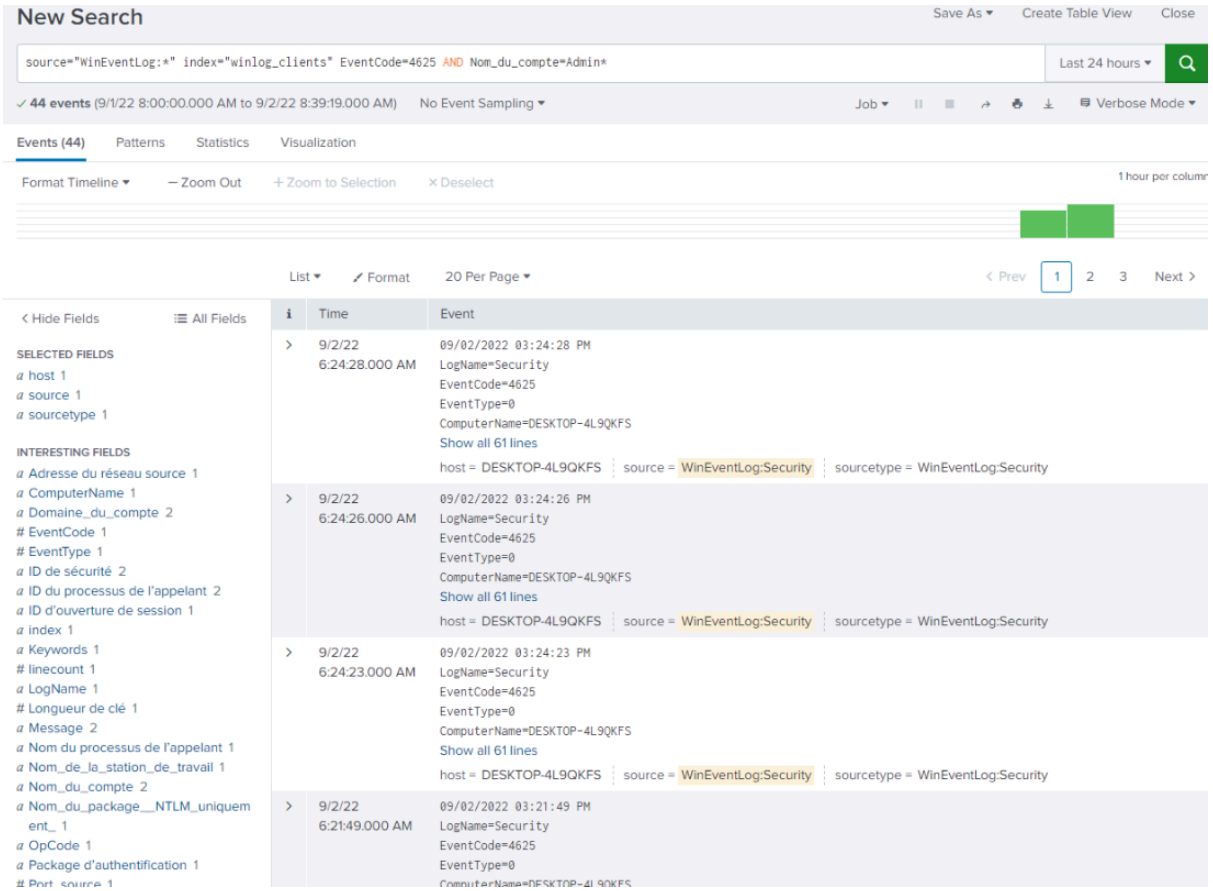
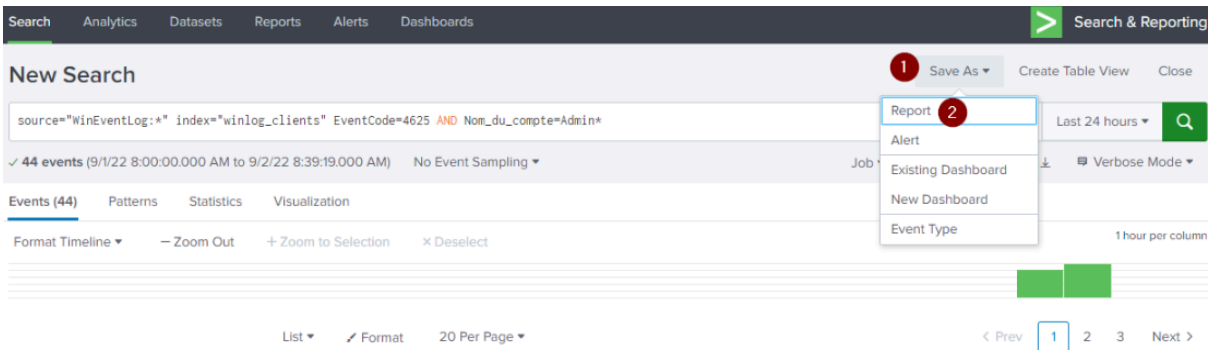
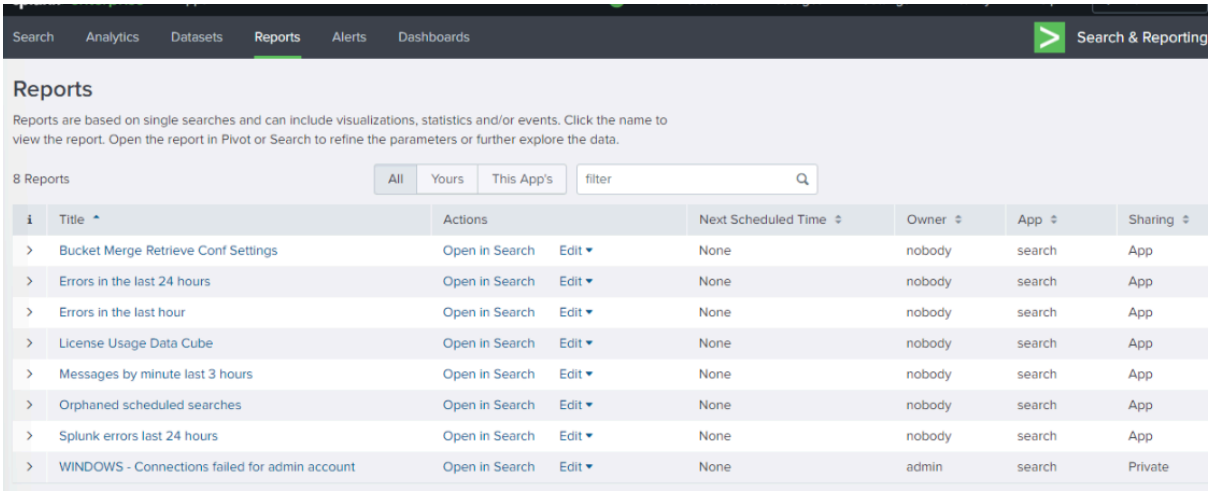
Reports on Splunk

Reports are essentially saved results. These can be executed as required or scheduled







Example:

```
index=security sourcetype=firewall action=blocked
| stats count by src_ip, dest_ip
| sort - count
```

This query finds all *blocked firewall connections* and aggregates the counts by source and destination IP addresses.

Once tested, you can save it as a **report** and:

- Give it a title and description.
- Set permissions (private or shared across an app/team).
- Schedule it (e.g., run every 6 hours).
- Configure alerts based on thresholds (e.g., “trigger if >1000 blocked IPs in 1 hour”).

Security Monitoring

Goal: Detect brute-force login attempts.
Query:

```
index=auth sourcetype=linux_secure "Failed password"
| stats count by user, src_ip
| where count > 5
```

Schedule this report hourly to detect repeated failed login attempts. If the count exceeds a threshold, it can automatically trigger an **alert** and generate a **PDF report** for the SOC team.

Web Application Monitoring

Goal: Identify top 10 URLs returning HTTP 500 errors.
Query:

```
index=web sourcetype=access_combined status=500
| stats count by uri_path
| sort - count
| head 10
```

Visualization: Bar chart showing the most error-prone endpoints.

Business Value:
Helps the DevOps or Security team quickly identify failing APIs or possible attack surfaces in real-time.

Real life use cases:

Build a report combining multiple searches (failed logins, blocked IPs, suspicious PowerShell).

Schedule it to run daily at 06:00.

Deliver via email as a **PDF or CSV** to your SOC team.

Optionally include a summary dashboard view.