

Reports on Splunk

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

New Search Save As Create Table View Close

source="WinEventLog:*" index="winlog_clients" EventCode=4625 AND Nom_du_compte=Admin* Last 24 hours Q

✓ 44 events (9/1/22 8:00:00.000 AM to 9/2/22 8:39:19.000 AM) No Event Sampling Job

Events (44) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page Prev 1 2 3 Next

	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS a Adresse du réseau source 1 a ComputerName 1 a Domaine_du_compte 2 # EventCode 1 # EventType 1 a ID de sécurité 2 a ID du processus de l'appelant 2 a ID d'ouverture de session 1 a index 1 a Keywords 1 # linecount 1 a LogName 1 # Longueur de clé 1 a Message 2 a Nom du processus de l'appelant 1 a Nom_de_la_station_de_travail 1 a Nom_du_compte 2 a Nom_du_package___NTLM_uniquem ent_ 1 a OpCode 1 a Package d'authentification 1 # Port source 1	>	9/2/22 6:24:28.000 AM	09/02/2022 03:24:28 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 61 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	9/2/22 6:24:26.000 AM	09/02/2022 03:24:26 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 61 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	9/2/22 6:24:23.000 AM	09/02/2022 03:24:23 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-4L9QKFS Show all 61 lines host = DESKTOP-4L9QKFS source = WinEventLog:Security sourcetype = WinEventLog:Security
	>	9/2/22 6:21:49.000 AM	09/02/2022 03:21:49 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-4L9QKFS

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search 1 Save As Create Table View Close

source="WinEventLog:*" index="winlog_clients" EventCode=4625 AND Nom_du_compte=Admin* Last 24 hours Q

✓ 44 events (9/1/22 8:00:00.000 AM to 9/2/22 8:39:19.000 AM) No Event Sampling Job

Events (44) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page Prev 1 2 3 Next

Report 2
Alert
Existing Dashboard
New Dashboard
Event Type

Search Analytics Datasets Reports Alerts Dashboards							
Search & Reporting							
Reports							
Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.							
8 Reports							
All Yours This App's filter							
i	Title ^	Actions		Next Scheduled Time ↕	Owner ↕	App ↕	Sharing ↕
>	Bucket Merge Retrieve Conf Settings	Open in Search	Edit ▼	None	nobody	search	App
>	Errors in the last 24 hours	Open in Search	Edit ▼	None	nobody	search	App
>	Errors in the last hour	Open in Search	Edit ▼	None	nobody	search	App
>	License Usage Data Cube	Open in Search	Edit ▼	None	nobody	search	App
>	Messages by minute last 3 hours	Open in Search	Edit ▼	None	nobody	search	App
>	Orphaned scheduled searches	Open in Search	Edit ▼	None	nobody	search	App
>	Splunk errors last 24 hours	Open in Search	Edit ▼	None	nobody	search	App
>	WINDOWS - Connections failed for admin account	Open in Search	Edit ▼	None	admin	search	Private

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.