🔐 Windows SIEM Project Report

📌 Objective

The goal of this project was to set up a Security Information and Event Management (SIEM) environment using **Elasticsearch, Kibana, and Winlogbeat** to collect and analyse Windows security events.

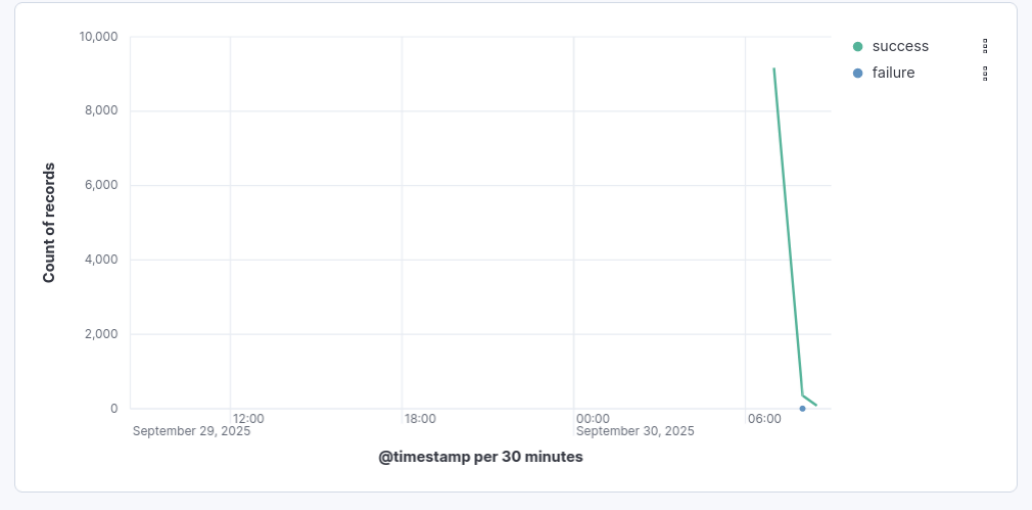
🖥️ Setup

- **Virtual Machines:**
  - Ubuntu VM running **Elasticsearch + Kibana**
  - Windows VM running **Winlogbeat** to forward logs
- **Networking:** Host-only adapter (`192.168.56.0/24`) used for communication between VMs.
- **Data Source:** Windows Security Event Logs (event codes such as 4624 – successful logins, 4625 – failed logins).

📊 Key Visualisations

Login Trends Over Time

- Compared successful logins (4624) vs failed logins (4625).
- Helps detect spikes in failed login attempts.
- Visualisation shows successful logins in green and failed logins in blue
- This visualisation spanned over a 24-hour time period



Top Usernames from Failed Logins

- Table visualisation showing which usernames are targeted most often.

Top 5 values of winlog.user.type	Count of records	Minimum of @timestamp
User	4,436	Sep 30, 2025 @ 08:16:57.020

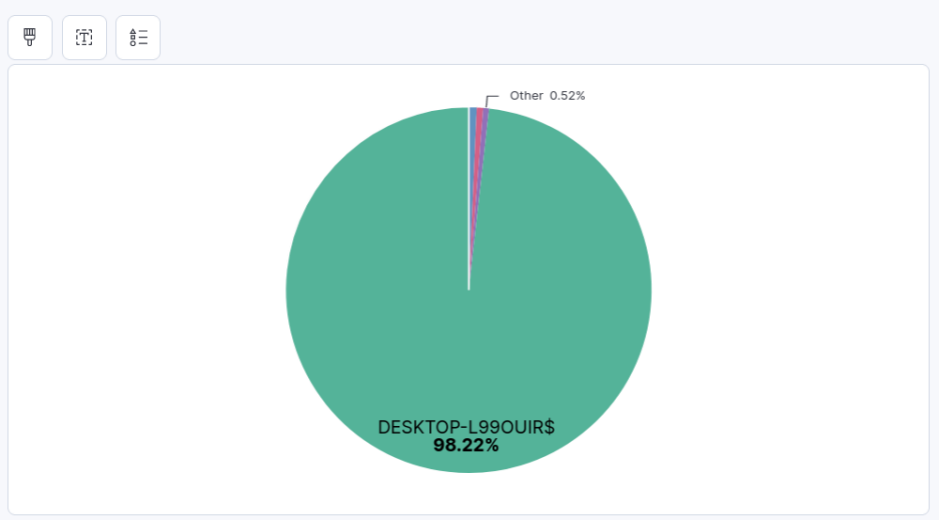
Failed Logins by Source IP

- Table visualiation showing which IP addresses generate the most failed login attempts.
- Useful for spotting brute-force activity or suspicious sources.

Top 5 values of winlog.event_data.SourceIp	@timestamp per 30 minutes	Count of records
192.168.56.101	05:00	-
192.168.56.101	05:30	-
192.168.56.101	06:00	-
192.168.56.101	06:30	-
192.168.56.101	07:00	-
192.168.56.101	07:30	-
192.168.56.101	08:00	56
192.168.56.101	08:30	146
192.168.56.101	09:00	84

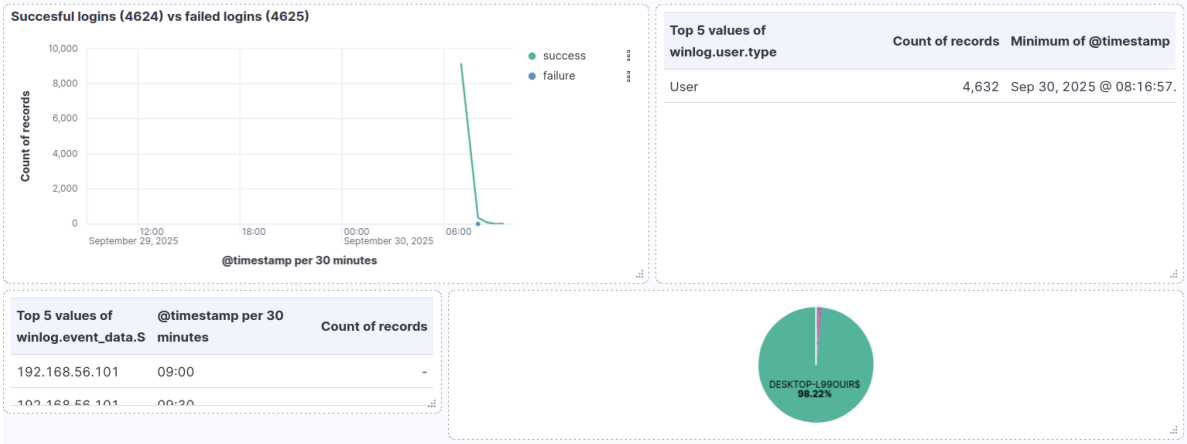
Login Distribution by Event Code

- Pie chart showing proportion of successful vs failed logins.



📈 Dashboard

All visualisations were pinned to a single dashboard called “SIEM” for centralised monitoring.



✅ Outcome

- Successfully configured Elasticsearch to ingest Windows logs via Winlogbeat.
- Built multiple visualisations to analyse authentication events.
- Created a SIEM dashboard that provides visibility into login patterns, suspicious usernames, and source IPs.
- This project demonstrates practical experience with log collection, parsing, and security event analysis using the Elastic stack.