1. **Find the top 5 most frequently attacked destination IP addresses.**
2. **Identify how many attacks were blocked versus ignored in the last 30 days.**
3. **Find the top 3 most common protocols used in attacks.**
4. **Analyze the severity level distribution of all logged attacks.**
5. **Find the total packet size of all attack attempts per network segment.**
6. **List the top 5 users who experienced the most attacks.**
7. **Find the most common geo-location for cyber attacks.**
8. **Detect patterns in IDS/IPS alerts—find the top alert-generating log sources.**
9. **Determine if there is an increasing trend in attacks over the last 7 days.**
10. **Identify attack attempts involving a specific source IP (e.g., 103.216.15.12).**
11. **Correlate Firewall Logs and IDS/IPS Alerts to Identify Potential Breaches**
12. **Detect Source IPs That Have Attacked Multiple Destinations**
13. **Identify the Most Targeted Ports for Each Protocol14. Investigate Peak Attack Hours**
14. **Find Recurring Attack Patterns by Grouping Similar Payloads**