## ***Questions about Wazuh - IDISC - Group 8***

1. ***Challenges in Setup:*** What are the primary challenges users face when setting up Wazuh for log analysis and intrusion detection?

2. ***Handling Large Log Volumes:*** How does Wazuh handle the processing of large volumes of logs efficiently, especially in real-time scenarios?

3. ***Identifying Malicious Logs:*** What specific features does Wazuh offer for identifying and categorizing malicious logs?

4. ***Integration with AI Tools:*** Can Wazuh integrate with other AI tools or platforms to enhance its capability to discriminate against malicious logs?

5. ***Analyst Training:*** What kind of training or expertise is required for cybersecurity analysts to effectively utilize Wazuh for analyzing logs and identifying security incidents?

6. ***Limitations and Blind Spots:*** Are there any known limitations or blind spots in Wazuh's detection capabilities that users should be aware of when developing a cybersecurity app?

7. ***Handling False Positives:*** How does Wazuh handle false positives in log analysis, and what mechanisms are in place to minimize them?

8. ***Customization:*** What level of customization does Wazuh offer in terms of creating rules and policies tailored to specific cybersecurity needs or environments?

9. ***Best Practices for Integration:*** Are there any best practices or recommended workflows for incorporating Wazuh into a larger cybersecurity infrastructure, particularly for passing flagged logs to analysts efficiently?

10. How would we be able to have access to the company's logs? In real-time? Using Wazuh, looking for a more technical answer.