In [ ]:

```
Training Day 26 Report– 18 July 2025
 Introduction
 Day 26 covered IDS/IPS fundamentals and log monitoring concepts that enable c
 and response activities.
 Key Concepts Discussed
 Wedifferentiated signature-based detection from anomaly detection and discuss
 strategies to reduce false positives while maintaining detection coverage.
 Lab Preparation in Theory
 The course described how to design rule sets in an isolated lab, how to evalu
 and how to build triage workflows for security operations teams.
 Practical Understanding (Theory)
 We examined the role of SIEM systems and log retention strategies for forensi
 as well as how to prioritize incidents for investigation.
 Key Takeaways
 Detection capability depends on both sensor placement and intelligent tuning;
 essential for post-incident analysis.
 Conclusion
 Next we will explore network border defenses and firewall design principles.
```