Logging and Alerting

- Audit logs are valuable for intrusion investigation
- Inform on application or attacker behaviour during / post breach
- E.g Authentication audits, critical transactions, successful attack mitigation
- Can be enabled on application and all intermediaries
- Rules or alerts triggers to inform administrators on anomalous behaviour

Web Application Firewalls

- Internal or external component performing intrusion prevention or detection in the capacity of a reverse-proxy
- Often leverages payload signatures or customized rules or policies for detection
- Often parses HTTP requests and response therefore could also be vulnerable to bypasses
- May protect against CSRF, XSS, SQLi etc