

1>What is OSSEC and what are its key features/benefits.

2>What is the architecture of OSSEC?

3> Where is the configuration file how can you configure/customise OSSEC behavior?

4> Where is OSSEC output stored?

5> How do we control/fine tune events reported by OSSEC?

6> Where are rules stored? How are rules matched?

8>What are different rules levels and what do they signify?