SIEM - Interview Sheet

Top 10 SIEM Interview Questions - Security

Q1. What is SIEM and what security threat or domain does it address?

Answer:

Q2. Explain the core mechanism or model that SIEM uses to provide security.

Answer:

Q3. How do you configure SIEM for a typical production web application?

Answer:

Q4. What are common misconfigurations or pitfalls when using SIEM?

Answer:

Q5. How does SIEM integrate with identity providers or authentication systems?

Answer:

Q6. Explain how SIEM handles key management, certificate rotation, or credential lifecycle.

Answer:

Q7. How do you audit and monitor events in SIEM to detect anomalies?

Answer:

Q8. How does SIEM support compliance requirements (SOC 2, PCI-DSS, GDPR)?

Answer:

Q9. How do you test SIEM configurations for vulnerabilities or weaknesses?

Answer:

Q10. What are the performance implications of SIEM and how do you minimize overhead?

Answer: