

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

A: SIEM is a security tool, protocol, or service that mitigates a specific class of threats authentication bypass, data exfiltration, network intrusion, or credential theft. Understanding the threat model is prerequisite to correct configuration.

Q2. What is the core mechanism SIEM uses to provide security?

A: SIEM uses one or more security primitives: asymmetric cryptography, symmetric encryption, certificate chains, role-based access control, or anomaly detection. These primitives are combined to provide the claimed security properties.

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

A: Production configuration requires strong cipher suites, certificate rotation, revocation checking, and minimal permission grants. Use a well-reviewed configuration reference (CIS Benchmark, OWASP) rather than default settings.

Q4. What are the most common SIEM misconfigurations to avoid?

A: Common mistakes include using outdated algorithms (MD5, SHA1, RC4), leaving default credentials, ignoring certificate expiry, granting excessive permissions, and not testing the config before going live in production.

Q5. How does SIEM integrate with identity providers?

A: SIEM delegates identity verification to an IdP via SAML, OIDC, or LDAP. Users authenticate once (SSO) and receive a token that SIEM validates. This centralizes user management and avoids duplicating auth logic across services.

Q6. How do you audit and monitor SIEM events?

A: Enable SIEM's audit log and stream it to a SIEM (Splunk, Elastic SIEM). Define alert rules for high-severity events: repeated failed logins, privilege escalation, and unusual access patterns. Review logs regularly.

Q7. How does SIEM handle key or credential rotation?

A: Automate rotation using a secrets manager that generates new credentials and updates consumers transparently. Test rotation in staging. Have a break-glass procedure for emergency rotation when a credential is compromised.

Q8. How does SIEM help meet compliance requirements?

A: SIEM generates audit trails, enforces access policies, and provides encryption that satisfy controls required by SOC 2, PCI-DSS, HIPAA, and GDPR. Map SIEM's capabilities to the specific framework controls in your compliance program.

Q9. How do you test your SIEM configuration for weaknesses?

A: Run an automated scanner (SSL Labs for TLS, ScoutSuite for cloud IAM, OWASP ZAP for web app auth) against your SIEM config. Conduct penetration tests annually and after significant config changes.

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

A: Cryptographic operations, token validation, and authorization checks add latency. Mitigate with session caching, hardware-accelerated TLS (AES-NI), connection reuse, and async authorization where possible.