Security Logging Implementation Checklist

Required events, standards, and compliance

Required Security Events

- ■ Authentication events (success, failure, lockout, MFA)
- ■ Authorization failures (access denied, privilege escalation attempts)
- ■ Account lifecycle (creation, modification, deletion, password reset)
- ■ Data access events (sensitive data read/write/export)
- ■ Configuration changes (security settings, permissions, roles)
- ■ API activity (rate limit hits, invalid requests, unusual patterns)

Logging Standards

- ■ Structured format (JSON) with consistent field names
- ■ Include: timestamp (UTC/ISO 8601), event type, user ID, source IP, resource, outcome
- ■ Correlation ID included for distributed tracing
- ■ Log levels used correctly (ERROR for security events, not DEBUG)

Data Protection in Logs

- ■ No passwords, tokens, or API keys in logs
- ■ No PII beyond what's necessary (mask SSN, credit card, etc.)
- ■ No session tokens or bearer tokens logged
- ■ Request/response bodies sanitized before logging

SIEM Integration

- ■ Logs forwarded to centralized SIEM/log aggregation
- ■ Alert rules configured for critical security events
- ■ Log retention meets compliance requirements (90 days min)
- ■ Log integrity protection enabled (write-once, tamper-evident)