Intermediate Level

Advanced Logging Practices

Comprehensive Logging Architecture

Multi-Tier Logging Framework:

- **Collection Layer**
  - **Log agents and forwarders (Filebeat, Fluentd, NXLog)**
  - **Buffer mechanisms for reliability**
  - **Load balancing for high-volume environments**
  - **Filtering and preprocessing at source**
- **Processing Layer**
  - **Log parsing and normalization**
  - **Event enrichment with context**
  - **Correlation of related events**
  - **Transformation to standard formats**
- **Storage Layer**
  - **Hot storage for recent logs (1-3 months)**
  - **Warm storage for medium-term retention (3-12 months)**
  - **Cold storage for long-term archiving (1+ years)**
  - **Immutable storage options for compliance**
- **Analysis Layer**
  - **Real-time analytics engines**
  - **Machine learning capabilities**
  - **Correlation rules engine**
  - **Search and investigation tools**
- **Presentation Layer**
  - **Dashboards and visualization**
  - **Reporting capabilities**
  - **Alert management interfaces**
  - **Mobile accessibility**

Enhanced Log Quality and Integrity

Structured Logging Implementation:

- **Implementing JSON, CEF, or LEEF formats**
- **Schema definition for log entries**
- **Consistent field naming conventions**
- **Standardized enumeration values**
- **Hierarchical logging levels (DEBUG, INFO, WARN, ERROR, FATAL)**

Log Integrity Protection:

- **Cryptographic signing of log entries**
- **Hash-chain mechanisms for tamper detection**
- **Write-once storage systems**
- **Blockchain-based logging for critical events**
- **Separation of duties for log administration**

Data Quality Assurance:

- **Log validation mechanisms**
- **Error handling for logging failures**
- **Monitoring of logging pipelines**
- **Log completeness verification**
- **Clock synchronization (NTP with monitoring)**

Advanced Event Types to Monitor

Advanced Application Monitoring:

- **Business logic abuse attempts**
- **Abnormal function execution times**
- **Memory usage anomalies**
- **Unusual API call patterns**
- **Serialization/deserialization operations**
- **Server-side request forgery attempts**
- **XML parsing events**

Security Control Monitoring:

- **WAF bypass attempts**
- **Antivirus/EDR disabling attempts**
- **DLP trigger events**
- **Certificate validation failures**

- **Encryption/decryption operations**
- **Key management events**
- **HTTPS downgrade attempts**

Cloud-Specific Monitoring:

- **IAM policy changes**
- **Resource provisioning events**
- **Cross-account activity**
- **Cloud storage permission changes**
- **Serverless function invocations**
- **Container orchestration events**
- **Cloud provider API calls**

Advanced Threat Indicators:

- **DNS tunneling attempts**
- **Beaconing patterns**
- **Data staging activities**
- **Living-off-the-land techniques**
- **Process injection events**
- **Unusual registry modifications**
- **Scheduled task creation**

Log Management Best Practices

Capacity Planning:

- **Calculating log storage requirements**
- **Estimating ingest rates and peaks**
- **Planning for log growth (typically 15-25% annually)**
- **Implementing tiered storage strategies**
- **Horizontal scaling capabilities**

Performance Optimization:

- **Indexing strategies for fast searches**
- **Sharding for distributed environments**
- **Caching mechanisms for frequent queries**
- **Query optimization techniques**

- **Resource allocation for peak periods**

Log Data Governance:

- **Classification of log data sensitivity**
- **Access control matrices for log data**
- **Audit trails for log access**
- **Data masking for sensitive fields**
- **Data loss prevention for log exports**

Detection Engineering

Detection Rule Development:

- **Creating detection logic based on TTPs**
- **MITRE ATT&CK framework alignment**
- **Rule testing methodology**
- **False positive mitigation strategies**
- **Rule versioning and management**

Analytics Development:

- **Statistical analysis for anomaly detection**
- **Baselining techniques**
- **Threshold determination methodologies**
- **Sliding window analysis**
- **Outlier detection algorithms**

Rule Tuning Process:

- **Performance impact assessment**
- **Coverage analysis**
- **False positive/negative measurement**
- **Feedback loop implementation**
- **Continuous improvement cycles**

Monitoring Integration Points

Security Tool Integration:

- **SIEM integration patterns**
- **EDR/XDR data consumption**
- **Vulnerability management correlation**

- **Threat intelligence platform feeds**
- **Security orchestration and automation**

Business System Integration:

- **CMDB integration for asset context**
- **ITSM ticketing system workflow**
- **Business context enrichment**
- **Risk management platform integration**
- **Business impact correlation**

Compliance-Specific Requirements

Regulatory Logging Requirements:

- **PCI DSS**
    - **User identification**
    - **Type of event**
    - **Date and time**
    - **Success or failure indication**
    - **Origination of event**
    - **Identity or name of affected data, system component, or resource**
    - **1-year retention with 3 months immediately available**
- **HIPAA**
    - **Information system activity reviews**
    - **Audit controls**
    - **6-year retention requirement**
    - **Hardware/software function tracking**
- **SOX**
    - **System access logs**
    - **Configuration change logs**
    - **User activity tracking**
    - **Data modification logs**
    - **7-year retention for some components**
- **GDPR**
    - **Data access logging**

- **Data processing records**
- **Consent management logs**
- **Data transfer logs**
- **Right to be forgotten request tracking**

Intermediate Implementation Strategies

SIEM Implementation Methodology

Implementation Phases:

1. **Requirements Gathering**
   - **Use case definition**
   - **Data source identification**
   - **Performance requirements**
   - **Compliance mapping**
2. **Architecture Design**
   - **Deployment model selection (on-prem, cloud, hybrid)**
   - **Sizing and capacity planning**
   - **High availability design**
   - **Disaster recovery planning**
3. **Data Onboarding**
   - **Log source prioritization**
   - **Parser development**
   - **Field normalization**
   - **Data quality validation**
4. **Content Development**
   - **Alert rule creation**
   - **Dashboard development**
   - **Report template creation**
   - **Playbook integration**
5. **Operational Readiness**
   - **Monitoring procedures**
   - **Backup and recovery testing**
   - **Performance tuning**

    - **Knowledge transfer**

SOC Integration Guidelines

SOC Workflow Integration:

- **Alert triage procedures**
- **Escalation matrices**
- **Investigation runbooks**
- **Case management integration**
- **Shift handover processes**

Alert Management:

- **Severity classification framework**
- **SLA definition by alert type**
- **Assignment routing rules**
- **Alert correlation procedures**
- **False positive management**

Metrics and KPIs:

- **Alert volume trends**
- **Mean time to detect (MTTD)**
- **Mean time to respond (MTTR)**
- **False positive rates**
- **Alert-to-incident conversion rates**
- **Coverage gaps measurement**

Testing Logging and Monitoring

Validation Methods:

- **Controlled attack simulations**
- **Log generation test scripts**
- **Failure injection testing**
- **Log pipeline resilience testing**
- **Disaster recovery scenarios**

Purple Team Exercises:

- **Evasion technique testing**
- **MITRE ATT&CK scenario validation**

- **Detection gap identification**
- **Alert tuning opportunities**
- **Documentation of findings**