LOG360 – LAYERED ARCHITECTURE

1 DATA INGESTION LAYER

Collect, validate and normalize logs from across the environment

- Network Devices
- Servers & Apps
- Cloud Services
- Security Tools
- Databases
- Directories
- Endpoints

Agents

750+ sources

Endpoint logs Network devices Cloud apps Security tools

Access Gateway

DMZ / Proxy

SSL/TLS Load balancing
Authentication
Throttling

Log Processor Cluster

Round-robin / Failover

Horizontal scalability
High availability

2 PROCESSING & STORAGE LAYER

Process, correlate and store at scale

QUEUE ENGINE

Topics → Partitions → Replication → Brokers → Producers/Consumers

Processing Engine

Parse | Normalize
Enrich | Dedupe

Correlation Engine

Event Correlation
Rule Evaluation

Search Engine

Index | Aggregate
Fast Retrieval

Alert Engine

Thresholds | Anomalies
Real-time Alerts

TIERED STORAGE

Hot Storage
Elasticsearch Cluster
High-speed Indexing
Search

Cold Storage
Archive
Long-term Retention
Cost Optimized

Metadata Storage
PostgreSQL
Config | Metadata
Audit Info

3 DETECTION LAYER

Detect threats and prioritize risks

CENTRALIZED DETECTION CONSOLE

- 2,000+ Rules
- MITRE Mapping
- Object-Level Filtering
- Risk Scoring
- Behavior Analytics (UEBA)

4 INVESTIGATION LAYER

Investigate alerts with deep context

Incident Workbench

Case management Evidence notes Collaboration

Alert Investigation Agent

- LLM-powered Analysis
- Entity Extraction
- Enrichment Threat Intel
- Timeline Reconstruction
- MITRE Mapping

5 RESPONSE & AUTOMATION LAYER

Automate actions and integrate with ecosystem

SOAR Playbooks

Automate orchestration
Respond faster

Ticketing Integrations

ServiceDesk Plus
ServiceNow

Notifications

Email / SMS
Alert escalation

REST APIs / Webhooks

Bi-directional integration
Custom workflows

6 VISIBILITY & COMPLIANCE LAYER

Gain visibility, ensure compliance and maintain trust

Customizable Dashboards

Real-time visibility
Role-based views

Compliance Reports

1000+ reports
Ready for audit

Hybrid Monitoring

On-prem | Cloud
Multi-tenant

Tamper-Detecting Audit Trails

Immutable logs
End-to-end integrity

Data Flow · Control Flow · Storage · Processing · Analytics · Security · Integration · User/Action