

NetEye Elastic Log Management Training Agenda

Condensed overview of objectives, key topics and practical labs

Module Title	Module Purposes	Day
Log Manager and Data Ingestion	Objectives: Understand NetEye Log Manager with Elastic; collect and structure logs and metrics; prevent common ingestion and parsing errors. Key topics: Elastic Log and Security architecture; Elastic Agent and integrations; logs versus metrics; ECS and custom fields; ingest pipelines; Discover, Data Views, Streams and core query languages. Practical lab: Install Elastic Agent; enable system and Windows integrations; analyze data in Discover and Security; build queries; use Streams.	Day 1
Data Modeling and Search	Objectives: Analyze logs and fields; optimize data mappings; build effective searches Key topics: Explicit and dynamic mappings; multi-fields; text analyzers; date formats; dynamic templates; identifying and troubleshooting mapping conflicts. Practical lab: Create mappings and index documents; use text and keyword fields; compare analyzers; configure date formats and dynamic templates.	Day 2
Aggregation and Data Processing	Objectives: Create KPIs with aggregations; transform and enrich documents; optimize data through denormalization; manage ingestion pipelines. Key topics: Metric and bucket aggregations; Transform APIs; ingest processors; Enrich; Painless scripts; reindex and update-by-query; runtime fields; host-data enrichment; real-time log signing. Practical lab: Build aggregations and a pivot transform; apply processors and enrich data; update and reindex documents; create calculated fields; enrich logs with host information.	Day 3

Module Title	Module Purposes	Day
Elproxy, Investigation, Data Management and Cluster Administration	Objectives: Sign and verify logs with Elproxy; investigate threats; understand distributed data; manage the data lifecycle and diagnose cluster issues. Key topics: Elproxy and missing-log alerts; Elastic Security detection rules, timelines and Endpoint Protection; shards and replicas; distributed indexing and search; ILM and data tiers; snapshots; cluster monitoring and Health API. Practical lab: Configure Windows administrator-access logs and verify signatures; enable Elastic Endpoint; observe shard distribution and simulate failover; create an ILM policy; troubleshoot with the Health API and Monitoring UI.	Day 3