DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Elastic SIEM Advanced Training

Run Elastic Security for large or multi-tenant SOCs with tiered storage, hardened clusters, measured detections and a SIEM migration plan.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	50 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/elastic/elastic-siem-advance-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the Elastic SIEM course path, you will be able to:

1

Onboard security data correctly

Collect endpoint, network and cloud data with Elastic Agent and map it to ECS for reliable detection.

2

Detect and investigate threats

Write and tune query, EQL, ES|QL, threshold and ML rules and investigate alerts through to response.

3

Run a scalable SOC platform

Design, harden and measure Elastic Security for large, multi-tenant or regulated environments.

WHAT THE ADVANCED LEVEL ADDS

Scale, multi-tenancy, hardening and SOC maturity

Hands-on: Capstone: purple-team detection exercise. Emulate a multi-stage intrusion across endpoint, cloud and identity data, prove each stage is detected, contain it with response actions and report SOC metrics.

WHO SHOULD ATTEND

- Experienced Elastic SIEM practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot Elastic SIEM solutions.
- Teams making Elastic SIEM an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Hunt threats with ES|QL, add threat intelligence and ML detections, and manage rules as code with tested, tuned changes.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO ADVANCED

Elastic SIEM Advanced Training agenda

50 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: Elastic Security setup, data onboarding and detection

Included from Foundation

1. SIEM fundamentals: log sources, normalisation, correlation, detection and response in a SOC workflow
2. Elastic Stack for security: Elasticsearch, Kibana, Elastic Agent and Fleet Server, Elastic Cloud versus self-managed
3. Lab setup: Elasticsearch and Kibana with security enabled, TLS, users and the Security app
4. Elastic Security introduction: Overview, Alerts, Rules, Explore, Timelines and Cases pages
5. Host and network event analysis: Hosts, Network and Users views for SIEM threat detection
6. Getting security data in: enrolling Elastic Agent with Fleet, agent policies, System and Windows integrations
7. Elastic Common Schema: field sets, event.category and event.action, onboarding custom and third-party sources
8. Beats-supported sources: Winlogbeat, Auditbeat, Packetbeat and Filebeat modules next to Elastic Agent
9. Querying security data: KQL and Lucene in Discover, filters, time ranges and saved searches
10. Detection engine: rule schedules, additional look-back time, required index privileges and rule actions
11. Prebuilt and custom rules: installing Elastic prebuilt community rules and writing a custom query rule
12. Managing alerts: alert statuses, assignees, grouping and bulk acknowledge or close
13. Reducing noise: rule exceptions, shared exception lists and value lists

DAY 2 — Essential: Endpoint telemetry, rule types, investigations and cases

Included from Essential

14. Windows telemetry: Sysmon through Elastic Agent, Security log events 4624, 4625 and 4688, PowerShell script block logging
15. Linux telemetry: Auditd Manager integration, authentication logs and process events from Elastic Defend
16. Threshold and new terms rules: brute force and password spraying, first-seen users, hosts and processes
17. EQL rules: event sequences such as an Office app spawning a script interpreter, maxspan and by clauses
18. ES|QL for security: ES|QL queries in Discover, aggregations and ES|QL detection rules
19. Timeline investigations: building a timeline from an alert, pinned events, notes and saved timelines
20. Visual event analyzer and Session View: process ancestry and interactive Linux session replay
21. Cases: opening cases from alerts, attachments, observables and Jira, ServiceNow or email connectors
22. Elastic Defend: installing endpoint protection, malware, ransomware, memory threat and behaviour prevention
23. Response actions: isolate host, kill or suspend process, get-file and execute from the response console
24. Risk context: host and user risk scores, asset criticality and alert enrichment
25. SOC dashboards: Lens visualisations for alert trends, top rules, hosts and users

DAY 3 — Intermediate: Threat hunting, intelligence, ML and detection-as-code

Included from Intermediate

26. Threat hunting: hypothesis-driven hunts over endpoint, network and identity data with ES|QL and EQL
27. MITRE ATT&CK coverage: mapping rules to tactics and techniques and closing detection gaps
28. Threat intelligence: Abuse.ch, AlienVault OTX and MISP integrations, Intelligence page and indicator match rules
29. Machine learning detections: prebuilt anomaly jobs for rare processes, unusual logins and DNS tunnelling
30. Detection-as-code: the detection-rules repository, Kibana detection APIs, rule versioning and CI checks

31. Rule tuning: rule preview, false-positive review, alert suppression windows and severity overrides
32. Custom ingest: ingest pipelines with grok and dissect, custom log integrations mapped to ECS
33. Cloud security posture: CSPM and KSPM findings, cloud audit logs from AWS, Azure and Google Cloud
34. Automation and connectors: Slack, PagerDuty and webhook actions feeding SOAR playbooks
35. Elastic AI Assistant for Security: alert summaries, query generation and Attack Discovery
36. SOC access control: Kibana Spaces and Security privileges for analyst, hunter and engineer roles
37. Troubleshooting: rule execution gaps and failures, missing indices, agent health and unmapped fields
38. Security data lifecycle: ILM policies, data stream rollover and snapshot schedules

DAYS 4-5 **Advanced: Scale, multi-tenancy, hardening and SOC maturity** **New at this level**

39. SIEM architecture at scale: dedicated node roles, hot, warm, cold and frozen tiers with searchable snapshots
40. Distributed SOCs: cross-cluster search and detection rules that query remote regional clusters
41. Multi-tenancy: per-tenant Spaces, rule and exception scoping and MSSP data separation
42. Hardening the platform: TLS everywhere, API keys, least-privilege roles, audit logging and secure settings
43. High-volume ingest: Fleet scaling, agent output tuning, Kafka and Logstash buffering for high event rates
44. Adversary emulation: Atomic Red Team and Caldera tests to validate detections before release
45. Endpoint policy engineering: trusted applications, event filters, blocklists and staged policy rollout
46. Compliance evidence: retention, audit trails and reports for PCI DSS, ISO 27001 and SOC 2 controls
47. SOC performance: mean time to detect and respond, rule efficacy, alert-to-case ratio and noise budgets
48. SIEM migration: mapping Splunk or QRadar searches and data sources to Elastic rules and integrations
49. Resilience: snapshot and restore, cross-cluster replication and recovery drills for security data
50. Capstone: purple-team exercise detecting, investigating and containing a multi-stage intrusion

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION

Detect a brute-force login attempt

Enroll a Linux and a Windows host with Elastic Agent, confirm ECS-mapped events arrive, and enable a rule that alerts on repeated failed logins with an exception for a scanner.

ESSENTIAL

Investigate a malicious PowerShell chain

Trigger a scripted attack on a Windows host, catch it with an EQL sequence rule, investigate it in Timeline and Analyzer, isolate the host and record the case.

INTERMEDIATE

Ship tested detections from Git

Write two custom rules in a Git repository, validate and deploy them with the detection-rules tooling, then tune them against a week of lab data with suppression.

ADVANCED

Capstone: purple-team detection exercise

Emulate a multi-stage intrusion across endpoint, cloud and identity data, prove each stage is detected, contain it with response actions and report SOC metrics.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four Elastic SIEM levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR ELASTIC SIEM TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/elastic/

ENROL OR RESERVE A SEAT **Elastic SIEM Advanced Training**	WHATSAPP · INDIA **+91 99057 40781**
WHATSAPP · USA **+1 (469) 756-6329**	EMAIL **contact@DevOpsSchool.com**