DevOpsSchool

Course curriculum · November 2026

LEVEL 01 OF 04 · FOUNDATION

Elastic SIEM Fundamentals Training

Explain how Elastic Security works as a SIEM, onboard host and network data with Elastic Agent and manage rules and alerts.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **1 day · Day 1**	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 1 day · This curriculum	**Essential** 2 days · Next step	**Intermediate** 3 days · Later	**Advanced** 5 days · Later

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	11 topics · Foundation
Hands-on labs	1 lab
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-fundamental.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

Collect endpoint, network, cloud and identity data into Elastic Security with Elastic Agent and ECS.

2

Detect and investigate threats

Build and tune detection rules and investigate alerts with Timeline, analyzers, cases and response actions.

3

Operate a scalable SOC

Run Elastic Security across teams and regions with detection-as-code, hardening and measurable outcomes.

WHAT THE FOUNDATION LEVEL ADDS

Elastic Security, detection engine and data onboarding

Hands-on: Onboard hosts and fire first alerts. Enroll a Windows and a Linux host with Elastic Agent, enable prebuilt detection rules, trigger a test attack technique and tune the resulting alert with an exception.

WHO SHOULD ATTEND

- Beginners and working professionals who are new to Elastic SIEM and want a solid, hands-on start.
- Engineers, analysts, testers and students preparing to use Elastic SIEM on real work.
- Leads and managers who want first-hand familiarity with Elastic SIEM.

BEFORE YOU START

- No prior Elastic SIEM experience is needed.
- 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

Elastic SIEM Fundamentals Training agenda

11 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, detection engine and data onboarding

New at this level

1. SIEM concepts: log collection, correlation, detection, alert triage and the role of a SOC
2. Elastic Security introduction: the Security app in Kibana, SIEM and endpoint protection in one solution
3. Analysis of host and network security events: Hosts, Network and Users pages, events and timelines
4. Getting security data in: ingesting security data with Elastic Agent, Fleet policies and security integrations
5. Elastic Common Schema (ECS): how ECS lets Elastic Security work with custom and third-party data sources
6. Beats for security data: Winlogbeat, Auditbeat, Packetbeat and Filebeat modules alongside Elastic Agent
7. Detection engine: how rules run on a schedule, look-back time, rule actions and required privileges
8. Prebuilt and custom rules: installing and updating Elastic prebuilt rules and writing a custom query rule
9. Managing alerts: alerts table, statuses, assignees, grouping and bulk actions
10. Rule exceptions: adding exceptions and shared exception lists to reduce noise
11. Setup checklist: Fleet Server, Kibana Security privileges, detection index and alert data streams

PRACTICE

Hands-on labs

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

FOUNDATION

Onboard hosts and fire first alerts

Enroll a Windows and a Linux host with Elastic Agent, enable prebuilt detection rules, trigger a test attack technique and tune the resulting alert with an exception.

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)	1 day 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 Fundamentals Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com

Next step after this level: Elastic SIEM Essential Training - Write detections with KQL, EQL, threshold and ES|QL rules and investigate alerts end to end with Timeline, analyzers and cases.