DevOpsSchool

Course curriculum · November 2026

ELASTIC LOGSTASH KIBANA FULL STACK (ELK) · TRAINING PROGRAM

# Elastic SIEM Essentials Training

A practical, hands-on Elastic SIEM Essentials Training curriculum: 56 topics over 3 days. Learn live online in a small batch, as a private corporate batch, or self-paced with one year of LMS access.

| | | |
|---|---|---|
| LIVE ONLINE<br>**Max 8-10 hours** | CORPORATE<br>**Private team batch, on demand** | SELF-PACED VIDEO<br>**1-year LMS access** |
| BATCH SIZE<br>**Max 10 learners** | NEXT BATCHES<br>**1st of every month · weekends: first Saturday** | CERTIFICATE<br>**Verifiable certificate of completion** |

## INSIDE THIS CURRICULUM


| | |
|---|---|
| Who should attend | Objectives, audience, prerequisites |
| Agenda | 56 topics over 3 days |
| 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-essentials.html
**Talk to us:** WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

COURSE FIT

# Who this program is for

Use this page to decide whether Elastic SIEM Essentials Training matches your role and experience.

1

### Objectives

Understand the core concepts and usage model, apply practical workflows through examples and guided tasks, and prepare for implementation, certification or team adoption.

2

### Who should attend

Developers, DevOps engineers, administrators, SREs, security engineers, platform teams, release teams, technical leads and corporate teams working with this topic.

3

### Before you start

Basic computer literacy and awareness of software, operations, cloud, DevOps or security workflows is helpful. Deep programming experience is not needed unless the topic requires it.

AGENDA AT A GLANCE · 56 TOPICS OVER 3 DAYS

**Day 1**

12 topics · SIEM Introduction

**Day 2**

26 topics · Enable modules and configuration options

**Day 3**

18 topics · Understanding SIEM UI

AGENDA · 56 TOPICS OVER 3 DAYS

# Elastic SIEM Essentials Training agenda

Days are for corporate (day-wise) delivery; live online batches cover the agenda in max 8-10 hours.

## DAY 1

12 topics

1. SIEM Introduction
2. SIEM Components
3. Setup and Configure ELK
4. Understanding a types of Threats
5. Introduction to threat hunting on an endpoint platform
6. Hunt types
7. Install Beats shippers
8. Filebeat for forwarding and centralizing logs and files
9. Auditbeat for collecting security events
10. Winlogbeat for centralizing Windows event logs
11. Packetbeat for analyzing network packets
12. Data Source in ELK for Security Scanning

## DAY 2

26 topics

13. Enable modules and configuration options
14. Auditbeat & Discover Anomaly detection
15. System module - Linux, macOS, Win
16. packages
17. processes
18. logins
19. sockets
20. users and groups
21. Auditd module (Linux Kernel Audit info)
22. File integrity module (FIM) - Linux, macOS, Win
23. Filebeat & Discover Anomaly detection
24. system logs (auth logs) - Linux
25. Santa - macOS
26. Winlogbeat & Discover Anomaly detection
27. Windows event logs - Windows
28. Packetbeat & Discover Anomaly detection
29. Flows
30. DNS
31. other protocols
32. Zeek NMS module
33. Suricata IDS module
34. Iptables/Ubiquiti module

35. CoreDNS module
36. Envoy proxy module (Kubernetes)
37. Palo Alto Networks firewall module
38. Cisco ASA firewall module

**DAY 3** 18 topics

39. Understanding SIEM UI
40. Timelines
41. Hosts
42. Network
43. Raw Event Data
44. Threat Hunting with Kibana
45. Introduction to the threat hunting and the Elastic Stack
46. Network data
47. Host data
48. Data enrichment
49. Threat hunting
50. Guided Hunt
51. Elastic Endpoint Security Triage and Response
52. Triage and tune
53. Alert management
54. Detection and response
55. Hunting malicious activity
56. Advanced tradecraft analytics

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 | This program plus 20+ more courses and 50+ tools, at your own pace. | **INR 833/month** billed yearly at INR 9,996 |
| **Corporate** | Planned with your team | A private batch for your team, on demand, with examples mapped to your platforms. | **Quote on request** |

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on tasks and assignments. 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 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 courses: www.devopsschool.com/courses/

ENROL OR RESERVE A SEAT
**Elastic SIEM Essentials Training**

WHATSAPP · INDIA
**+91 99057 40781**

WHATSAPP · USA
**+1 (469) 756-6329**

EMAIL
**contact@DevOpsSchool.com**

**More Elastic Logstash Kibana Full Stack (ELK) training: www.devopsschool.com/courses/elastic/**