DevOpsSchool

Course curriculum · November 2026

SPLUNK · TRAINING PROGRAM

Splunk Enterprise Security Training

A practical, hands-on Splunk Enterprise Security Training curriculum: 284 topics over 5 days. Learn live online in a small batch, as a private corporate batch, or self-paced with one year of LMS access.

LIVE ONLINE **Max 8-10 hours**	CORPORATE **Private team batch, on demand**
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**

INSIDE THIS CURRICULUM

Who should attend	Objectives, audience, prerequisites
Agenda	284 topics over 5 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/splunk/splunk-enterprise-security-siem-course.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 Splunk Enterprise Security 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 · 284 TOPICS OVER 5 DAYS

Day 1
76 topics · Splunk Fundamentals

Day 2
75 topics · Splunk Intermediate

Day 3
41 topics · Splunk Enterprise System Administration

Day 4
48 topics · Using Splunk Enterprise Security

Day 5
44 topics · Administering Splunk Enterprise Security

AGENDA · 284 TOPICS OVER 5 DAYS

Splunk Enterprise Security Training agenda

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

DAY 1

76 topics

1. Splunk Fundamentals
2. Splunk Fundamentals Course Topics
3. Introduction to Splunk's interface
4. Basic searching
5. Using fields in searches
6. Search fundamentals
7. Transforming commands
8. Creating reports and dashboards
9. Datasets
10. The Common Information Model (CIM)
11. Creating and using lookups
12. Scheduled Reports
13. Alerts
14. Using Pivot
15. Splunk Fundamentals Course Objectives
16. Module 1 - Introduction
17. Module 2 - What is Splunk?
18. Splunk components
19. Installing Splunk
20. Getting data into Splunk
21. Module 3 - Introduction to Splunk's User Interface
22. Understand the uses of Splunk
23. Define Splunk Apps
24. Customizing your user settings
25. Learn basic navigation in Splunk
26. Module 4 - Basic searching
27. Run basic searches
28. Use autocomplete to help build a search
29. Set the time range of a search
30. Identify the contents of search results
31. Refine searches
32. Use the timeline
33. Work with events
34. Control a search job
35. Save search results
36. Module 5 - Using Fields in Searches

37. Understand fields
38. Use fields in searches
39. Use the fields sidebar
40. Module 6 - Search Language Fundamentals
41. Review basic search commands and general search practices
42. Examine the search pipeline
43. Specify indexes in searches
44. Use autocomplete and syntax highlighting

Use SPL search commands to perform searches

45. Module 7 - Using Basic Transforming Commands
46. The top command
47. The rare command
48. The stats command
49. Module 8 - Creating Reports and Dashboards
50. Save a search as a report
51. Edit reports
52. Create reports that include visualizations such as charts and tables
53. Create a dashboard
54. Add a report to a dashboard
55. Edit a dashboard
56. Module 9 - Datasets and the Common Information Model
57. Naming conventions
58. What are datasets?
59. What is the Common Information Model (CIM)?
60. Module 10 - Creating and Using Lookups
61. Describe lookups
62. Create a lookup file and create a lookup definition
63. Configure an automatic lookup
64. Module 11 - Creating Scheduled Reports and Alerts
65. Describe scheduled reports
66. Configure scheduled reports
67. Describe alerts
68. Create alerts
69. View fired alerts
70. Module 12 - Using Pivot
71. Describe Pivot
72. Understand the relationship between data models and pivot
73. Select a data model object
74. Create a pivot report
75. Create an instant pivot from a search
76. Add a pivot report to a dashboard

DAY 2 75 topics

77. Splunk Intermediate
78. Splunk Intermediate Course Topics
79. Transforming commands and visualization
80. Filtering and formatting
81. Results
82. Correlating events
83. Knowledge objects
84. Fields (Field aliases, field extractions, calculated fields)
85. Tags and event types
86. Macros
87. Workflow actions
88. Data models
89. Splunk Common Information Model (CIM)
90. Splunk Intermediate Course Objectives
91. Overview of Buttercup Games Inc.
92. Lab environment
93. Module 2 Beyond Search Fundamentals
94. Search fundamentals review
95. Case sensitivity
96. Using the job inspector to view search performance
97. Module 2 Using Transforming Commands for Visualizations
98. Explore data structure requirements
99. Explore visualization types
100. Create and format charts and timecharts
101. Module 3 Using Transforming Commands for Visualizations
102. Module 4 Using Mapping and Single Value Commands
103. The iplocation command
104. The geostats command
105. The geom command
106. The addtotals command
107. Module 5 Filtering and Formatting Results
108. The eval command
109. Using the search and where commands to filter results
110. The filnull command
111. Module 6 Correlating Events
112. Identify transactions
113. Group events using fields
114. Group events using fields and time
115. Search with transactions

116. Report on transactions
117. Determine when to use transactions vs. stats
118. Module 7 Introduction to Knowledge Objects
119. Identify naming conventions
120. Review permissions
121. Manage knowledge objects
122. Module 8 Creating and Managing Fields
123. Perform regex field extractions using the Field Extractor (FX)
124. Perform delimiter field extractions using the FX
125. Module 9 Creating Field Aliases and Calculated Fields
126. Describe, create, and use field aliases
127. Describe, create and use calculated fields
128. Module 10 Creating Tags and Event Types
129. Create and use tags
130. Describe event types and their uses
131. Create an event type
132. Module 11 Creating and Using Macros
133. Describe macros
134. Create and use a basic macro
135. Define arguments and variables for a macro
136. Add and use arguments with a macro
137. Module 12 Creating and Using Workflow Actions
138. Describe the function of GET, POST, and Search workflow actions
139. Create a GET workflow action
140. Create a POST workflow action
141. Create a Search workflow action
142. Module 13 Creating Data Models
143. Describe the relationship between data models and pivot
144. Identify data model attributes
145. Create a data model
146. Use a data model in pivot
147. Module 14 Using the Common Information Model (CIM) Add-On
148. Describe the Splunk CIM
149. List the knowledge objects included with the Splunk CIM
150. Add-On
151. Use the CIM Add-On to normalize data

DAY 3 41 topics

152. Splunk Enterprise System Administration
153. Splunk Enterprise System Administration Course Topics
154. Splunk Deployment Overview

155. License Management
156. Splunk Apps
157. Splunk Configuration Files
158. Users, Roles, and Authentication
159. Getting Data In
160. Distributed Search
161. Introduction to Splunk Clusters
162. Splunk Enterprise System Administration Course Objectives
163. Splunk overview
164. Identify Splunk components
165. Identify Splunk system administrator role
166. Identify license types
167. Describe license violations
168. Add and remove licenses
169. Describe Splunk apps and add-ons
170. Install an app on a Splunk instance
171. Manage app accessibility and permissions
172. Describe Splunk configuration directory structure
173. Understand configuration layering process
174. Use btool to examine configuration settings
175. Describe index structure
176. List types of index buckets
177. Create new indexes
178. Monitor indexes with Monitoring Console
179. Apply a data retention policy
180. Backup data on indexers
181. Delete data from an index
182. Restore frozen data
183. Describe user roles in Splunk
184. Create a custom role Add Splunk users
185. Integrate Splunk with LDAP
186. List other user authentication options Describe the steps to enable Multifactor Authentication in Splunk
187. Describe the basic settings for an input
188. List Splunk forwarder types Configure the forwarder
189. Add an input to UF using CLI
190. Describe how distributed search works
191. Explain the roles of the search head and search peers Configure a distributed search group
192. List search head scaling options

DAY 4 48 topics

193. Using Splunk Enterprise Security

194. Splunk Enterprise Security Course Topics
195. ES concepts
196. Security monitoring and Incident investigation
197. Assets and identities
198. Detecting known types of threats
199. Monitoring for new types of threats
200. Using analytical tools
201. Analyze user behavior for insider threats
202. Use risk analysis and threat intelligence tools
203. Use protocol intelligence and live stream data
204. Use investigation timelines and journal tools
205. Build glass tables to display security status
206. Splunk Enterprise Security Course Objectives
207. Provide an overview of Splunk for Enterprise Security (ES)
208. Identify the differences between traditional security threats and new adaptive threats
209. Describe correlation searches, data models and notable events
210. Describe user roles in ES
211. Log on to ES
212. Use the Security Posture dashboard to monitor enterprise security status
213. Use the Incident Review dashboard to investigate notable events
214. Take ownership of an incident and move it through the investigation workflow
215. Use adaptive response actions during incident investigation
216. Create notable events
217. Suppress notable events
218. Use ES investigation timelines to manage, visualize and coordinate incident investigations
219. Use timelines and journals to document breach analysis and mitigation efforts
220. nvestigate access domain events
221. Investigate endpoint domain events
222. Investigate network domain events
223. Investigate identity domain events
224. Understand and use Risk Analysis
225. Use the Risk Analysis dashboard
226. Manage risk scores for objects or users
227. Use HTTP Category Analysis, HTTP User Agent Analysis, New Domain Analysis, and Traffic Size Analysis to spot new threats
228. Filter and highlight events
229. Evaluate the level of insider threat with the user activity and access anomaly dashboards
230. Understand asset and identity concepts
231. Use the Asset Investigator to analyze events
232. Use the Identity Investigator to analyze events
233. Use the session center for identity resolution (UBA integration)

234. Use the Threat Activity dashboard to analyze traffic to or from known malicious sites
235. Inspect> the status of your threat intelligence content with the threat artifact dashboard
236. Describe Stream events data is input into Splunk events
237. Use ES predictive analytics to make forecasts and view trends
238. Build glass tables to display security status information
239. Add glass table drilldown options
240. Create new key indicators for metrics on glass tables

DAY 5

44 topics

241. Administering Splunk Enterprise Security
242. Administering Splunk Enterprise Security Course Topics
243. Monitoring and Investigation
244. Security Intelligence
245. Forensics, Glass Tables and Navigation Control
246. ES Deployment
247. Installation and Configuration
248. Validating ES Data
249. Custom Add-ons
250. Tuning Correlation Searches
251. Creating Correlation Searches
252. Lookups and Identity Management
253. Threat Intelligence Framework
254. Administering Splunk Enterprise Security Course Objectives
255. Overview of ES features and concepts
256. Security Posture
257. Incident Review
258. Notable events management
259. Overview of security intel tools
260. Explore forensics dashboards
261. Examine glass tables
262. Configure navigation and dashboard permissions
263. Identify deployment topologies
264. Examine the deployment checklist
265. Understand indexing strategy for ES
266. Understand ES Data Models
267. Prepare a Splunk environment for installation
268. Download and install ES on a search head
269. Test a new install
270. Understand ES Splunk user accounts and roles
271. Post-install configuration tasks
272. Plan ES inputs

273. Configure technology add-ons
274. Design a new add-on for custom data
275. Use the Add-on Builder to build a new add-on
276. Configure correlation search scheduling and sensitivity
277. Tune ES correlation searches
278. Create a custom correlation search
279. Configuring adaptive responses
280. Search export/import
281. Identify ES-specific lookups
282. Understand and configure lookup lists
283. Understand and configure threat intelligence
284. Configure user activity analysis

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
Splunk Enterprise Security Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com

More Splunk training: www.devopsschool.com/courses/splunk/