DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

Securonix Intermediate Training

Build custom detections and SOAR playbooks, monitor cloud and SaaS sources, and administer and troubleshoot a Securonix deployment.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **3 days · Days 1-3**	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 · This curriculum	5 days · Next step

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	33 topics · Foundation to Intermediate
Hands-on labs	3 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/securonix/securonix-intermediate-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 Securonix course path, you will be able to:

1

Operate Securonix SIEM

Onboard data, search events and navigate violations and cases in Securonix.

2

Detect threats with analytics

Use policies, UEBA, threat models and risk scoring to surface high-fidelity threats.

3

Automate and scale detection

Build custom content, SOAR playbooks and governed detection programmes at enterprise scale.

WHAT THE INTERMEDIATE LEVEL ADDS

Custom content, SOAR playbooks, cloud and administration

Hands-on: Automate response with a playbook. Write a custom detection for suspicious cloud sign-ins, tune it, and attach a SOAR playbook that enriches, notifies and disables the account after approval.

WHO SHOULD ATTEND

- Regular Securonix users who want to automate, integrate and manage it at a deeper level.
- Specialists who support Securonix for colleagues or customers.
- Leads preparing Securonix for wider use across projects.

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Configure policies, threat models and risk scoring, then triage violations and investigate cases with Securonix analytics.
- 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 INTERMEDIATE

Securonix Intermediate Training agenda

33 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: SIEM and UEBA concepts, Securonix platform and navigation

Included from Foundation

1. SIEM and UEBA fundamentals: log management, correlation, behaviour analytics and where Securonix fits
2. Securonix platform overview: cloud-native SIEM, UEBA, SOAR and threat content in Unified Defense SIEM
3. Architecture: SaaS tenant, data lake, ingestion layer and the Remote Ingester Node (RIN)
4. Users and access: login, roles, granular access control and user preferences
5. Navigating the console: Security Command Center, dashboards, violations and cases
6. Data sources and connectors: syslog, Windows events, cloud connectors and API-based collection
7. Installing a Remote Ingester Node: sizing, network requirements and connecting it to the tenant
8. Parsing and normalisation: parsers, the Securonix data model and enrichment with identity data
9. Identity and asset context: HR and directory feeds, users, peers and asset attributes
10. Spotter search basics: search syntax, filters, time ranges and saving searches
11. MITRE ATT&CK in Securonix: how content and violations map to tactics and techniques

DAY 2 — Essential: Policies, violations, threat models and investigations

Included from Essential

12. Policies: policy types, conditions, analytics such as rare behaviour, spikes and peer anomalies
13. Policy violations: viewing violations, risk scores and supporting events
14. Behaviour analytics: baselining users and entities, peer groups and anomaly detection
15. Threat models and threat chains: chaining violations across the kill chain to raise high-fidelity threats
16. Risk scoring: entity risk, score decay and prioritising the riskiest users and assets
17. Watchlists and lookup tables: whitelists, high-risk users, privileged accounts and threat intelligence lists
18. Threat intelligence: integrating TI feeds and matching IOCs against events
19. Case management: creating cases, assignment, comments, evidence and closure workflows
20. Investigation workflow: pivoting from violations to raw events and related entities
21. Dashboards and reports: building SOC dashboards and scheduled reports
22. Content packages: deploying out-of-the-box use cases for insider threat, cloud and data exfiltration

DAY 3 — Intermediate: Custom content, SOAR playbooks, cloud and administration

New at this level

23. Custom policies: building detections with Spotter-driven logic, thresholds and suppression
24. Tuning content: reducing false positives with whitelists, policy conditions and risk weights
25. SOAR playbooks: playbook design, enrichment actions, approvals and automated response
26. Integrations: EDR, firewall, identity, ticketing and messaging tools for response actions
27. Cloud and SaaS monitoring: AWS, Azure, Google Cloud and Microsoft 365 data sources and use cases
28. Threat hunting: hypothesis-driven hunts with Spotter and automated threat sweeps for new IOCs
29. Data pipeline management: filtering, routing and reducing noisy or low-value data to control cost
30. Administration: tenant settings, user and role management and audit logs

31. Ingestion health: monitoring connectors and RIN status, event volumes and parsing failures
32. Troubleshooting: missing data, time and timezone issues, parser errors and delayed violations
33. APIs: Securonix REST APIs for searching, case updates and automation scripts

PRACTICE

Hands-on labs

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

FOUNDATION

Onboard data and search with Spotter

Connect Windows, firewall and cloud logs through a Remote Ingester Node, verify parsing and identity enrichment, and investigate activity with Spotter.

ESSENTIAL

Investigate an insider threat case

Enable insider-threat policies and a threat model, raise a violation chain from lab activity, then triage it and document the case end to end.

INTERMEDIATE

Automate response with a playbook

Write a custom detection for suspicious cloud sign-ins, tune it, and attach a SOAR playbook that enriches, notifies and disables the account after approval.

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 Securonix levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	3 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 SECURONIX 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/securonix/

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

Next step after this level: Securonix Advanced Training - Run Securonix at enterprise scale with ATT&CK-driven detection engineering, data governance, compliance reporting and SIEM migration.