DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

Cyber Security Intermediate Training

Detect, investigate and respond to attacks using SIEM, MITRE ATT&CK and a structured incident response process.

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	36 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/cybersecurity/cyber-security-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 Cyber Security course path, you will be able to:

1

Defend systems and networks

Assess, harden and monitor networks, endpoints and web applications using industry tools.

2

Detect and respond confidently

Investigate alerts with SIEM and ATT&CK and run a structured incident response.

3

Lead risk-based security

Design zero-trust architecture and governance aligned with NIST CSF 2.0 and ISO 27001.

WHAT THE INTERMEDIATE LEVEL ADDS

SOC monitoring, incident response and penetration testing

Hands-on: Detect and respond to a simulated breach. Run a simulated attack in the lab, detect it in Wazuh with ATT&CK-mapped rules, and write the incident timeline, containment steps and report.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Scan, assess and harden systems and web applications with Nmap, Wireshark, Burp Suite and vulnerability scanners in a lab.
- 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

Cyber Security Intermediate Training agenda

36 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: Security concepts, threats and a home lab

Included from Foundation

1. Security fundamentals: CIA triad, authentication, authorization and accounting, non-repudiation and defence in depth
2. Threat landscape: malware, ransomware, phishing, social engineering, insider threats and supply chain attacks
3. Threat actors and motives: cybercriminals, hacktivists, nation-state groups and the cyber kill chain
4. Risk basics: assets, threats, vulnerabilities, likelihood, impact and risk treatment options
5. Networking for security: OSI and TCP/IP models, ports and protocols, DNS, HTTP and TLS handshakes
6. Cryptography basics: symmetric and asymmetric encryption, hashing, digital signatures, certificates and PKI
7. Identity basics: passwords, MFA, single sign-on and the principle of least privilege
8. Operating system security: Linux and Windows users, permissions, services, patching and logs
9. Security frameworks overview: NIST Cybersecurity Framework 2.0 functions, ISO/IEC 27001:2022 and CIS Controls v8
10. Security roles and careers: SOC analyst, penetration tester, security engineer, GRC analyst and incident responder
11. Law and ethics: authorised testing only, responsible disclosure, IT Act 2000, GDPR and India DPDP Act 2023
12. Lab setup: VirtualBox or VMware with Kali Linux, an Ubuntu server and a Windows target on an isolated network

DAY 2 — Essential: Network defence, scanning, web security and hardening

Included from Essential

13. Network reconnaissance: Nmap host discovery, port and service scans, version detection and NSE scripts
14. Traffic analysis: Wireshark and tcpdump filters, following streams, spotting clear-text credentials and anomalies
15. Firewalls and segmentation: stateful firewalls, iptables and nftables, Windows Defender Firewall, VLANs and DMZ design
16. Vulnerability scanning: Greenbone OpenVAS and Nessus Essentials scans, CVSS scores, CVE and false-positive review
17. Web application security: OWASP Top 10 including injection, broken access control, XSS and security misconfiguration
18. Burp Suite basics: proxy, repeater and intruder against DVWA or OWASP Juice Shop
19. System hardening: CIS Benchmarks, disabling unused services, secure SSH configuration and patch management
20. Endpoint protection: antivirus and EDR concepts, Microsoft Defender, application allow-listing
21. Email and phishing defence: SPF, DKIM, DMARC, header analysis and user awareness
22. Password security: hashing with salt, password managers, credential stuffing and cracking demonstrations with Hashcat
23. Wireless security: WPA2 and WPA3, rogue access points and secure Wi-Fi configuration
24. Backup and recovery basics: 3-2-1 rule, immutable backups and ransomware recovery planning

DAY 3 — Intermediate: SOC monitoring, incident response and penetration testing

New at this level

25. Security monitoring: log sources, Windows event IDs, Sysmon, Linux auditd and centralised logging
26. SIEM operations: Wazuh, Splunk or Microsoft Sentinel ingestion, correlation rules, dashboards and alert triage

27. MITRE ATT&CK: tactics, techniques, mapping detections and identifying coverage gaps
28. Detection engineering basics: Sigma rules, YARA signatures, tuning thresholds and reducing false positives
29. Incident response: NIST SP 800-61 phases, preparation, containment, eradication, recovery and lessons learned
30. Digital forensics basics: evidence handling, chain of custody, memory capture and disk imaging
31. Threat intelligence: IOCs, threat feeds, MISP and enriching alerts with reputation data
32. Penetration testing methodology: scoping, rules of engagement, reconnaissance, exploitation and reporting
33. Exploitation in the lab: Metasploit framework, privilege escalation and lateral movement concepts
34. Active Directory security: Kerberos, NTLM, common attack paths and BloodHound for defenders
35. Identity and access management: RBAC, privileged access management, MFA policies and access reviews
36. Automation for responders: Python and PowerShell scripts for log parsing and IOC lookups

PRACTICE

Hands-on labs

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

FOUNDATION

Build an isolated security practice lab

Set up Kali Linux, Ubuntu and Windows virtual machines on a host-only network and capture a TLS handshake and DNS lookup in Wireshark.

ESSENTIAL

Find and fix lab vulnerabilities

Scan the lab network with Nmap and OpenVAS, exploit a web flaw in Juice Shop with Burp Suite, then harden the target and rescan to prove the fix.

INTERMEDIATE

Detect and respond to a simulated breach

Run a simulated attack in the lab, detect it in Wazuh with ATT&CK-mapped rules, and write the incident timeline, containment steps and report.

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 Cyber Security 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 CYBER SECURITY 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/cybersecurity/

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

Next step after this level: Cyber Security Advanced Training - Design a zero-trust security architecture, secure cloud workloads and run a risk-based security programme across the enterprise.