

OSDA — SOC-200 Security Defense Analyst Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

At a glance

COURSE	OSDA — SOC-200 Security Defense Analyst	WHAT IS INCLUDED ✓ Instructor-led delivery by practitioners who also work our SOC ✓ Hands-on lab access for the duration of the course ✓ Course materials and lab guides ✓ Hacky Security certificate of completion ✓ Post-course support by email
TRACK	OffSec	
DOMAIN	Cyber Security	
LEVEL	Intermediate	
DURATION	On request	
DELIVERY	Classroom · Online live · On-site at your office	
LANGUAGE	English	
CLASS SIZE	Small cohorts — everyone gets lab time	

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

OSDA is the defensive certification in OffSec's catalogue — the one that puts you on the other side of the glass. Everything the OSCP and OSEP candidate does to stay hidden, the OSDA analyst is trained to catch. The course behind it, SOC-200, is built for people working in or moving into a Security Operations Centre who want detection skill that is grounded in how attacks actually unfold, not in vendor dashboards.

What makes this course unusual is that it is taught by an offensive-security company. The detections you learn to write are aimed at the exact techniques their own red-team courses teach. You watch an attack chain from the defender's seat and learn to see the signal each stage leaves behind.

The exam is a 24-hour practical. You are given a live environment with attacker activity in it, and you have to detect, investigate and document what happened — the analyst's job under time pressure.

Module 01 — The attacker's methodology, from the defender's chair

You cannot detect what you do not understand. This module walks the attack lifecycle so every later detection has a reason.

- The stages of an intrusion, from initial access to objective
- What each stage looks like in logs and telemetry
- The MITRE ATT&CK framework as a shared map between attacker and defender
- Why detection engineering starts with knowing the offence

Module 02 — Windows and Active Directory as a source of signal

Most enterprise attacks live in Windows and AD. This is where the evidence is.

- Windows event logs: which IDs matter and what they actually record
- Sysmon: what it captures that the default logs miss, and how to configure it
- Authentication events and what abnormal ones look like
- Building a baseline so anomalies stand out

Module 03 — Detecting initial access

Catching the intrusion at its earliest, cheapest point.

- Phishing and malicious document execution in the logs
- Suspicious process ancestry: when Word spawns PowerShell
- Detecting the client-side execution techniques OSEP teaches
- Writing a detection rule that fires on the behaviour, not the filename

Module 04 — Detecting execution and persistence

Finding the attacker settling in.

- PowerShell and script-block logging: reading obfuscated commands
- Detecting living-off-the-land binary abuse
- Persistence mechanisms: scheduled tasks, services, registry run keys, and their log signatures
- Separating an administrator's normal activity from an attacker imitating one

Module 05 — Detecting privilege escalation and credential theft

The middle of the attack, where the damage compounds.

- Credential-dumping techniques and the telemetry they generate
- Detecting token manipulation and process access to LSASS
- Kerberos abuse: Kerberoasting, ticket attacks, and their log footprints
- Escalation attempts and the events that reveal them

Module 06 — Detecting lateral movement

Watching the attacker spread, which is where a good SOC stops the incident.

- Remote execution techniques and how each one logs
- SMB, WMI and remote service abuse in the events
- Correlating activity across hosts to see a movement path
- Distinguishing legitimate administration from lateral movement

Module 07 — Detection engineering

Turning understanding into rules that fire reliably and do not drown the analyst.

- Writing detections that survive the attacker's evasion attempts
- Tuning: the balance between missed attacks and false positives
- The cost of a noisy rule, and how alert fatigue turns detection off
- Testing a detection against the real technique

Module 08 — Investigation and response under time pressure

The analyst's actual job, and the exam.

- Triaging an alert: is this real, and how bad
- Reconstructing an attack timeline from scattered evidence
- Scoping the compromise: what was reached, what was taken
- Documenting the investigation so it stands up to a second reader — the exam deliverable

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/osda/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 19 September 2026.