

# SOC-200 - Foundational Security Operations and Defensive Analysis (OSDA) - Self-paced

INCLUSIONS

**OSDA exam**

LENGTH

**90 days access**

## OFFSEC AT LUMIFY WORK

Security professionals from top organisations rely on OffSec to train and certify their personnel. Lumify Work is an Official Training Partner for OffSec.



## WHY STUDY THIS COURSE

Learn the foundations of cybersecurity defence with Foundational Security Operations and Defensive Analysis (SOC-200), a course designed for job roles such as Security Operations Center (SOC) Analysts and Threat Hunters.

Learners gain hands-on experience with a SIEM, identifying and assessing a variety of live, end-to-end attacks against a number of different network architectures.

Learners who complete the course and pass the exam earn the OffSec Defence Analyst (OSDA) certification, demonstrating their ability to detect and assess security incidents.

This self-paced course includes:

- Over 7 hours of video
- 450 pages of online content
- 4 lab machines
- OSDA exam voucher
- Closed Captioning is available for this course

About the OSDA exam:

- The SOC-200 course and online lab prepares you for the OSDA certification
- Proctored exam

[Learn more about the exam.](#)

## WHAT YOU'LL LEARN

<https://www.lumifywork.com/en-ph/courses/soc-200-foundational-security-operations-and-defensive-analysis-osda-self-paced/>

# SOC-200 - Foundational Security Operations and Defensive Analysis (OSDA) - Self-paced



*My instructor was great being able to put scenarios into real world instances that related to my specific situation.*

*I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.*

*I learnt a lot and felt it was important that my goals by attending this course were met.*

*Great job Lumify Work team.*



**AMANDA NICOL**  
**IT SUPPORT SERVICES**  
**MANAGER - HEALTH WORLD**  
**LIMITED**

- › Recognise common methodologies for end-to-end attack chains (MITRE ATT&CK® framework)
- › Conduct guided audits of compromised systems across multiple operating systems
- › Use a SIEM to identify and assess an attack as it unfolds live
- › Develop a working knowledge of security operations and best practices
- › Investigate the evidence left behind in log files from a wide variety of common attack methods
- › Configure and monitor a SIEM for active attacks on a network
- › Manually inspect logs in order to be able to recognise both normal and abnormal or benign and malicious activity

<https://www.lumifywork.com/en-ph/courses/soc-200-foundational-security-operations-and-defensive-analysis-osda-self-paced/>

# SOC-200 - Foundational Security Operations and Defensive Analysis (OSDA) - Self-paced

## COURSE SUBJECTS

The course covers the following topics:

- Attacker Methodology Introduction
- Windows Endpoint Introduction
- Windows Server Side Attacks
- Windows Client-Side Attacks
- Windows Privilege Escalation
- Windows Persistence
- Linux Endpoint Introduction
- Linux Server Side Attacks
- Network Detections
- Antivirus Alerts and Evasion
- Network Evasion and Tunnelling
- Active Directory Enumeration
- Windows Lateral Movement
- Active Directory Persistence
- SIEM Part One: Intro to ELK
- SIEM Part Two: Combining the Logs

View the full syllabus [here](#).

### Lumify Work Customised Training

*We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.*

*For more information, please contact us on [02 8286 9429](tel:0282869429).*

<https://www.lumifywork.com/en-ph/courses/soc-200-foundational-security-operations-and-defensive-analysis-osda-self-paced/>

# SOC-200 - Foundational Security Operations and Defensive Analysis (OSDA) - Self-paced

## WHO IS THE COURSE FOR?

Job roles such as:

- Security Operations Center (SOC) Tier 1, Tier 2 and Tier 3 Analysts
- junior roles in Threat Hunting and Threat Intelligence Analysts
- junior roles in Digital Forensics and Incident Response (DFIR)

Anyone interested in detection and security operations, and/or committed to the defence or security of enterprise networks.

## PREREQUISITES

All prerequisites for SOC-200 can be found within the Offsec Fundamentals Program, included with a [Learn Fundamentals](#) subscription

Prerequisite topics include:

- SOC-100: Linux Basics 1 and 2
- SOC-100: Windows Basics 1 and 2
- SOC-100: Networking Basics

The supply of this course by Lumify Work is governed by the booking terms and conditions. Please read the terms and conditions carefully before enrolling in this course, as enrolment in the course is conditional on acceptance of these terms and conditions.

<https://www.lumifywork.com/en-ph/courses/soc-200-foundational-security-operations-and-defensive-analysis-osda-self-paced/>