CINPAA | INTERNATIONAL COOPERATIVE FOR TRAINING & CONSULTING

سينبا | التعاونية الدولية للتدريب والاستشارات



Training programme:

Microsoft Security Operations Analyst Training

Delivered in several cities and dates

OUR INTERNATIONAL PARTNERS:

ISDE Law Business School — *Higher Institute of Law and Business (ISDE)*

Professional Development Institute — *Professional Development Institute*

Universidad Camilo José Cela — *Camilo José Cela University*

SEK EDUCATION GROUP

ISO 29993:2017 Learning services for non-formal education and training

ISO 9001:2015

Microsoft Security Operations Analyst Training

About the programme:

This programme focuses on security operations concepts and practices within the Microsoft Security Operations Analyst subject area, connecting operational understanding with the analysis of security activities.

Objectives:

Developing participants' skills, knowledge, values and professional approaches in:

a. The Microsoft Security Operations Analyst training is designed to provide learners with a comprehensive understanding of security operations concepts and practices. By the end of this course, participants should be able to:

b. Understand security operations concepts and techniques.

c. Develop and implement a security incident response plan.

d. Use various tools and techniques to identify and investigate security incidents.

e. Analyze and report on security incidents.

f. Implement threat protection technologies to prevent future security incidents.

g. Use Microsoft Defender XDR to monitor and respond to security incidents.

h. Develop and implement a vulnerability management program.

i. Secure identities and access using Microsoft Entra ID.

Target audience:

a. Security analysts monitoring and investigating incidents.

b. Security engineers maintaining enterprise protection controls.

c. IT operations staff contributing to incident response.

Daily programme:

• Day 1: Security operations concepts and techniques

a. Security operations overview: the role of the security operations function in an organisation

b. Common security operations tasks: monitoring, triage, escalation and handover between shifts

c. Developing a security operations plan with defined scope, roles and service hours

d. Alert sources, log collection and the data a security analyst needs to investigate

e. Workshop: drafting a security operations plan for a mid-sized public organisation

f. Day output: security operations plan outline with roles and escalation paths

• Day 2: Security incident response

a. Developing a security incident response plan and the phases it must cover

b. Incident classification, severity levels and the criteria for escalation

c. Security incident investigation techniques: timeline building, scoping and evidence handling

d. Incident response reporting and communication with management and affected units

e. Case study: reconstructing the timeline of a phishing-led account compromise

f. Day output: incident response plan with severity matrix and reporting template

• Day 3: Threat protection with Microsoft Defender XDR

a. Introduction to threat protection technologies for endpoints, email, identities and cloud apps

b. Implementing threat protection policies and tuning them to reduce false positives

c. Monitoring and responding to security incidents in Microsoft Defender XDR

d. Correlating alerts into incidents and using automated investigation and response

e. Workshop: investigating a correlated multi-stage incident in Microsoft Defender XDR

f. Day output: incident investigation record with containment actions taken

• Day 4: Vulnerability management

a. Developing and implementing a vulnerability management programme and its governance

b. Identifying vulnerabilities through asset inventories, scanning and configuration reviews

c. Prioritising and remediating vulnerabilities by exposure, exploitability and business impact

d. Reporting on vulnerability management progress with remediation timelines and exceptions

e. Case study: prioritising a backlog of vulnerabilities across servers and user devices

f. Day output: prioritised remediation plan with reporting indicators

• Day 5: Identity and access management with Microsoft Entra ID

a. Microsoft Entra ID overview: identities, groups, roles and authentication methods

b. Implementing identity and access management controls using Microsoft Entra ID

c. Multi-factor authentication, conditional access and least-privilege role assignment

d. Detecting risky sign-ins and investigating suspected identity compromise

e. Workshop: designing conditional access and privileged role rules for an administrative unit

f. Day output: identity protection baseline and analyst action checklist

Training methods and certificates:

Our programmes are built on modern pedagogy that combines theoretical knowledge with practical application, in line with participants' needs and the demands of the workplace. Methods include:

· **Interactive workshops:** analysis of real data and group discussions that strengthen practical understanding.

· **Case studies:** examples from international organisations that highlight real successes and challenges.

· **Realistic simulations:** participants train through professional scenarios that mirror real situations requiring decisions and situation management.

· **Advanced tools and technologies:** hands-on practice with up-to-date training software and tools suited to each field.

Certificates:

On successful completion, participants receive a certificate issued by CINPAA, a training institute officially registered in the European Union, Spain and the United Kingdom.

CINPAA - Cooperative International for Training and Consulting

Our programmes are delivered within academic and professional partnerships, cooperation agreements and memoranda of understanding with a number of academic and professional institutions, including:

• Camilo José Cela University - Spain

• ISDE - Law & Business School - International

• Professional Development Institute - United Kingdom

These partnerships aim to exchange expertise, develop training content and raise programme quality in line with

international best practice.

Kind regards,
International Programmes Department
"CINPAA" INTERNATIONAL COOPERATIVE FOR TRAINING & CONSULTING

Course details and registration

Course Details | Registration

Programme	**Microsoft Security Operations Analyst Training**	Course Title
Language	**English**	Course Language
Venue	**Several cities and dates – see the table below**	Venue
Financial offer	**Sent separately, according to the number of participants and the delivery conditions.**	Financial Offer

Registration and confirmation:

To register, please use one of the following:

a. Complete the programme request form on our website.

b. Or send an email from your training department.

c. Or a nomination letter from your organisation.

Send your confirmation by:

Email	info@cinpaa.org
WhatsApp	+34 635 867 686

Our team is ready to advise on accommodation and logistics before and during your stay.

Planned programme dates:

City	Dates
Madrid, Spain	21 - 25 Dec 2026
Madrid, Spain	04 - 08 Jan 2027
Barcelona, Spain	05 - 09 Apr 2027
London, United Kingdom	05 - 09 Jul 2027
Cairo, Egypt	04 - 08 Oct 2027

The programme can be delivered in other cities and on other dates to suit your organisation, at the length you need. The cities are listed on the last page.

Cities where we deliver our programmes:

This programme can be delivered in any of the following cities, and elsewhere on request.

Albania Tirana, Saranda	**Australia** Sydney	**Austria** Vienna, Hallstatt, Salzburg / Zell am See	**Azerbaijan** Baku
Bahrain Manama	**Belgium** Brussels, Bruges	**Bosnia and Herzegovina** Sarajevo	**Canada** Toronto, Montreal
China Hong Kong, Shanghai, Beijing, Guangzhou	**Croatia** Dubrovnik	**Cyprus** Nicosia, Limassol, Larnaca	**Czech Republic** Prague
Egypt Cairo, Sharm El Sheikh, Alexandria, Hurghada	**France** Paris	**Georgia** Tbilisi, Batumi	**Germany** Munich, Berlin, Düsseldorf, Frankfurt
Greece Athens, Rhodes	**Hungary** Budapest	**Indonesia** Bali, Jakarta	**Ireland** Dublin
Italy Rome, Florence, Milan, Venice, Como	**Japan** Tokyo	**Jordan** Amman, Aqaba	**Kuwait** Kuwait City
Malaysia Kuala Lumpur	**Maldives** Maldives	**Mauritius** Mauritius	**Montenegro** Budva, Kotor
Morocco Casablanca, Marrakech, Tangier, Rabat	**Netherlands** Amsterdam	**Oman** Muscat, Salalah	**Philippines** Manila
Poland Krakow, Warsaw	**Portugal** Lisbon, Porto	**Qatar** Doha	**Russia** Moscow
Saudi Arabia Riyadh, Jeddah, Dammam	**Serbia** Belgrade	**Slovenia** Ljubljana	**South Korea** Seoul
Spain Madrid, Barcelona, Valencia, Alicante, Benidorm, Malaga / Marbella, San Sebastian, Granada, Cordoba, Canary Islands, Seville, Bilbao	**Switzerland** Geneva, Luzern, Zurich, Interlaken, Zermatt, Lugano	**Thailand** Bangkok, Phuket	**Tunisia** Tunis
Turkey Istanbul, Antalya, Trabzon, Bursa, Izmir, Bodrum, Antakya (Hatay)	**United Arab Emirates** Dubai, Abu Dhabi	**United Kingdom** London, Edinburgh, Manchester, Birmingham	**United States** Miami, New York, Los Angeles, Washington