PARCOURS COMPÉTENCES+

SOC (SECURITY OPERATIONS CENTER) ANALYST

Cours pratique de 10 jours

NEW

Prix : 5990 CHF E.T.

DESCRIPTION

This certification program is designed to train participants in the key responsibilities of a SOC analyst, from understanding cybersecurity challenges to detecting, analyzing, and managing security incidents. It is based on a structured learning path, immersive workshops, and active intersessions that prepare participants for the final certification exam.

INTENDED AUDIENCE

SOC analysts, security engineers, CERT/CSIRT teams, and deputy CISOs, as well as security managers seeking to strengthen their operational practices.

TEACHING OBJECTIVES

At the end of the training, the participant will be able to:

- Understanding Cybersecurity Challenges and the Strategic Role of a SOC
- Detect, analyze, and classify security incidents
- Implement an appropriate response to incidents
- Continuously Improving the Operation of a SOC
- Anticipating Threats with Threat Intelligence
- Present and discuss a case study in an SOC context

PREREQUISITES

Have a basic understanding of systems, networks, and cybersecurity, and be comfortable using IT tools and reading logs.

FINANCING SOLUTIONS

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.

Découvrez-les sur notre page :
Comment financer sa formation ou contactez votre conseiller formation

PARTICIPANTS

SOC analysts, security engineers, CERT/CSIRT teams, and deputy CISOs, as well as security managers seeking to strengthen their operational practices.

PREREQUISITES

Have a basic understanding of systems, networks, and cybersecurity, and be comfortable using IT tools and reading logs.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

TIMES

THE TRAINING SESSIONS TAKE PLACE FROM 9.00 AM TO 5.30 PM, WITH A LUNCH BREAK OF BETWEEN 1 HOUR AND 1 HOUR 30 MINUTES.

For four- and five-day hands-on courses, sessions end at 16:00 on the last day of the course, regardless of the teaching mode..

POURQUOI CHOISIR LE PARCOURS SOC (Security Operations Center) Analyst

Move from reactive monitoring to proactive threat detection

- Detect and analyze security incidents more quickly
- Reduce response times and improve the reliability of diagnoses
- Effectively coordinate efforts with the security and IT teams
- Mastering the operational tools and processes of a SOC

A Practical Approach to Enhancing Your Operational Effectiveness Against Threats

VOTRE CERTIFICATION

Compétences+ Certification_backtocartlinebreak

01 **CERTIFICATION PROCEDURES_BACKTOCARTLINEBREAKTHE COMPÉTENCES ANALYST CERTIFICATION TAKES PLACE EXCLUSIVELY AT THE END OF THE PROGRAM, DURING THE ONE-DAY CERTIFICATION MODULE.**

The work completed during the intersessions allows the candidate to gradually prepare for their final presentation.
This work is not subject to graded assessment.back-to-cart-out-of-lineback-to-cart-out-of-line

02 **ASSESSMENT PROCEDUREBACK-TO-CART-OUT-OF-LINETHE ASSESSMENT IS ON AN ORAL PRESENTATION OF A PRACTICAL CASE STUDY DEVELOPED FRC SITUATIONS AND WORK PRODUCED DURING THE PROGRAM.BACKTOCHAR**

In particular, the candidate presents: the context and safety issues, the observed elements and identified alerts, the analysis anc of the incident, the proposed response actions, corrective measures, and areas for improvement, and the lessons learned study.backtrottoleapbacktrottoleap

03 **DISCUSSIONS WITH THE JURYBACKTROTTOLEAPAT THE END OF THE PRESENTATION, THE CANDIDATE ENGAGES IN A DISCUSSION WITH THE JURY.BACKTOCHARIOT**

These discussions allow the candidate to deepen their analysis, demonstrate their ability to justify their choices, and assess th the skills required in an operational SOC context.returncarriagebreakreturncarriagebreak

04 **PREPARATORY WORKRETURNCARRIAGEBREAKTHE WORK PRODUCED DUF THE INTERSESSIONS SERVES AS A FOUNDATION FOR THE FINAL PRESENTATI INCLUDING: INCIDENT REPORTS, ALERT ANALYSES, INVESTIGATION LOGS, P INCIDENT REPORTS, LESSONS LEARNED, AND MONITORING OF EMERGING THREATS.RETURNCHARIOT**

MON PARCOURS

DISPOSITIF PÉDAGOGIQUE HYBRIDE : 5 modules, 4 inter-sessions répartis sur 4 à 5 mois

- **Module** : Sessions en présentiel et distanciel
- **Inter-session** : Travaux en autonomie + accompagnement + plateforme dédiée
- Un formateur référent + un ingénieur pédagogique ORSYS dédié à toute la coordination
- Un suivi individualisé, du démarrage au passage de la certification

MODULE 01
Cybersecurity and the Role of the SOC

2 JOURS
- Immersive Workshop: “The Day Everything Changed.”
- Cybersecurity Overview.
- Collaborative workshop: “Who Am I?”
- Role and Responsibilities of the SOC.
- SOC Tools and Technologies.
- Organization and Operational Functioning.
- Diagnostic Workshop: “Are We Ready?”

INTER-SESSION

- Observe a real or simulated security alert or incident and identify the key indicators for detection.
- Complete a simplified incident report (symptoms, severity, initial actions).
- Compare the analyses across participants to identify best practices and common mistakes.
- Receive a summary from the instructor regarding the accuracy of the diagnosis and the relevance of the detection.

MODULE 02
Incident Monitoring, Detection, and Analysis

3 JOURS
- Immersive Workshop: “The Phantom Alert.”
- Real-time monitoring and detection.
- Collaborative Workshop: “In Search of the False Positive.”
- Analysis and classification of alerts.
- Incident Management and Communication.
- Hands-on Workshop: Visualizing Cybersecurity in Real Time.

INTER-SESSION

- Review an alert and document the qualification steps (context, severity, escalation).
- Issue a reasoned verdict: “true threat,” “false positive,” or “incomplete incident.”
- Compare the decisions made to understand the differences in interpretation.
- Collectively adjust the qualification criteria and strengthen the rigor of the analysis.

MODULE 03
Incident Response and Investigation

2 JOURS
- Immersive Workshop: “Live Cyber Crisis.”
- Incident Response Process.
- Investigative Tools and Techniques.
- Hands-on workshop: “On the Trail of the Pirate.”
- Communication in the Event of an Incident.
- Collaborative Workshop: “Communicating Under Pressure.”

INTER-SESSION

- Write an investigative news story based on a real or simulated incident.
- Produce an excerpt from a post-incident report (executive summary plus key lessons learned).
- Discuss the differences in investigative methods among participants.
- Receive personalized feedback on the clarity of the report and the relevance of the conclusions.

MODULE 04
Continuous Improvement and Threat Intelligence

2 JOURS
- Immersive Workshop: “A Retrospective on Chaos.”
- Continuous improvement of the SOC.
- Threat Intelligence and Threat Prediction.
- Collaborative Workshop: “The Eye of Intelligence.”
- Attack simulation and proactive detection.
- Hands-on Workshop: “Red Team vs. Blue Team Challenge.”

INTER-SESSION

- Write a feedback report (errors, corrective actions, indicators).
- Publish a security alert regarding an emerging threat (ransomware, vulnerability, new technique).
- Comment on other participants' contributions to enrich our shared knowledge base.
- Participate in a collective review of the effectiveness of corrective actions and shared monitoring.

MODULE 05
Competence_Plus SOC Analyst Certification

1 JOUR
- Oral presentation of the case study serving as the central theme.
- Discussions with the jury.

Hands-on work :
The work produced during the intersessions serves as a foundation for the final presentation.

CALENDRIER PROMO 2026

This programme is an original creation, developed by the teaching teams at ORSYS Formation. Any reproduction, representation, adaptation or use, in whole or in part, without the prior written authorisation of ORSYS, is strictly prohibited. ORSYS reserves the right to take any action necessary to protect its intellectual property rights.