PARCOURS COMPÉTENCES+

ANALYSTE SOC (SECURITY OPERATIONS CENTER)

Cours pratique de 10 jours

NEW

Prix : 5100 € H.T.

DESCRIPTION

Ce parcours certifiant vise à former les participants aux missions clés d'un analyste SOC, de la compréhension des enjeux de la cybersécurité à la détection, l'analyse et la gestion des incidents de sécurité. Il s'appuie sur une progression pédagogique structurée, des ateliers immersifs et des intersessions actives préparant à la certification finale.

PUBLIC CONCERNÉ

Analystes SOC, ingénieurs sécurité, équipes CERT/CSIRT et RSSI adjoints, ainsi que responsables sécurité souhaitant renforcer leurs pratiques opérationnelles.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les enjeux de la cybersécurité et le rôle stratégique d'un SOC
- Détecter, analyser et qualifier les incidents de sécurité
- Mettre en œuvre une réponse adaptée aux incidents
- Améliorer en continu le fonctionnement d'un SOC
- Anticiper les menaces grâce à la Threat Intelligence
- Présenter et argumenter un cas pratique en contexte SOC

PRÉREQUIS

Disposer de bases en systèmes, réseaux et cybersécurité, et être à l'aise avec les outils informatiques ainsi que la lecture de logs.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

PARTICIPANTS

Analystes SOC, ingénieurs sécurité, équipes CERT/CSIRT et RSSI adjoints, ainsi que responsables sécurité souhaitant renforcer leurs pratiques opérationnelles.

PRÉREQUIS

Disposer de bases en systèmes, réseaux et cybersécurité, et être à l'aise avec les outils informatiques ainsi que la lecture de logs.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

SOLUTIONS DE FINANCEMENT

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

HORAIRES

LES FORMATIONS ONT LIEU DE 9H À 17H30, AVEC UNE PAUSE DE 1H À 1H30 POUR LE DÉJEUNER.

Pour les formations de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 16h le dernier jour.

POURQUOI CHOISIR LE PARCOURS Analyste SOC (Security Operations Center)

Passez d'une surveillance réactive à une détection proactive des menaces

- Détecter et analyser plus rapidement les incidents de sécurité
- Réduire les temps de réaction et fiabiliser les diagnostics
- Coordonner efficacement ses actions avec les équipes sécurité et IT
- Maîtriser les outils et processus opérationnels d'un SOC

Un parcours concret pour renforcer votre efficacité opérationnelle face aux menaces

VOTRE CERTIFICATION

Certification Parcours Compétences+

MODALITÉS DE CERTIFICATION

01

La certification Compétences+ Analyste SOC se déroule exclusivement en fin de parcours, lors du module Certification d'un travaux réalisés pendant les intersessions permettent au candidat de préparer progressivement sa restitution finale.
Ils ne font pas l'objet d'une évaluation notée.

DÉROULEMENT DE L'ÉVALUATION

02

L'évaluation repose sur la présentation orale d'un cas pratique fil conducteur construit à partir des situations et product pendant le parcours. Le candidat présente notamment : le contexte et les enjeux de sécurité, les éléments observés et les alert l'analyse et la qualification de l'incident, les actions de réponse proposées, les mesures correctives et les pistes d'am enseignements tirés de l'étude de cas.

ÉCHANGES AVEC LE JURY

03

À l'issue de la présentation, le candidat échange avec le jury. Ces échanges permettent d'approfondir son analyse, de vérifier argumenter ses choix et d'évaluer sa maîtrise des compétences mobilisées dans un contexte opérationnel de SOC.

TRAVAUX PRÉPARATOIRES

04

Les productions réalisées pendant les intersessions constituent une base de travail pour la restitution finale, notamme d'incident, les analyses d'alertes, les journaux d'investigation, les rapports post-incident, les retours d'expérience, les travaux d menaces émergentes.

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
La cybersécurité et le rôle du SOC

2 JOURS
- Atelier immersif : “Le jour où tout a basculé”.
- Panorama de la cybersécurité.
- Atelier collaboratif : “Qui suis-je ?”.
- Rôle et missions du SOC.
- Outils et technologies du SOC.
- Organisation et fonctionnement opérationnel.
- Atelier diagnostic : “Sommes-nous prêts ?”.

INTER-SESSION

- Observer une alerte ou un événement de sécurité réel ou simulé et identifier les indices clés de détection.
- Rédiger une fiche d’incident simplifiée (symptômes, gravité, premières actions).
- Comparer les analyses entre participants afin d’identifier bonnes pratiques et erreurs fréquentes.
- Bénéficier d’un retour synthétique du formateur sur la précision du diagnostic et la pertinence de la détection.

MODULE 02
Surveillance, détection et analyse des incidents

3 JOURS
- Atelier immersif : “L’alerte fantôme”.
- Supervision et détection en temps réel.
- Atelier collaboratif : “À la recherche du faux positif”.
- Analyse et qualification des alertes.
- Gestion et communication d’incident.
- Atelier pratique : visualiser la cybersécurité en temps réel.

INTER-SESSION

- Rejouer une alerte et formaliser les étapes de qualification (contexte, gravité, escalade).
- Produire un verdict argumenté : “vraie menace”, “faux positif” ou “incident incomplet”.
- Comparer les décisions prises pour comprendre les écarts d’interprétation.
- Ajuster collectivement les critères de qualification et renforcer la rigueur d’analyse.

MODULE 03
Réponse aux incidents et investigation

2 JOURS

- Atelier immersif : “Cybercrise en direct”.
- Processus de réponse aux incidents.
- Outils et techniques d’investigation.
- Atelier pratique : “Sur la trace du pirate”.
- Communication en cas d’incident.
- Atelier collaboratif : “Communiquer sous pression”.

INTER-SESSION

- Rédiger un journal d’investigation à partir d’un incident réel ou simulé.
- Produire un extrait de rapport post-incident (résumé exécutif + enseignement clé).
- Discuter des différences de méthode d’investigation entre participants.
- Recevoir des commentaires personnalisés sur la clarté du rapport et la pertinence des conclusions.

MODULE 04
Amélioration continue et Threat Intelligence

2 JOURS
- Atelier immersif : “La rétrospective du chaos”.
- Amélioration continue du SOC.
- Threat Intelligence et anticipation des menaces.
- Atelier collaboratif : “L’oeil du renseignement”.
- Simulation d’attaque et détection proactive.
- Atelier pratique : “Red Team vs Blue Team Challenge”.

INTER-SESSION

- Rédiger une fiche de retour d’expérience (erreurs, actions correctives, indicateurs).
- Publier une alerte de veille sur une menace émergente (ransomware, vulnérabilité, nouvelle technique).
- Commenter les contributions des autres participants afin d’enrichir la base commune.
- Participer à une synthèse collective sur la pertinence des actions correctives et de la veille partagée.

MODULE 05
Certification compétence+ Analyste SOC

1 JOUR
- Présentation orale du cas pratique fil conducteur.
- Échanges avec le jury.

Travaux pratiques :
Les productions réalisées lors des intersessions constituent une base de travail pour la restitution finale.

CALENDRIER PROMO 2026

PROMO Nov.

DATES DU PARCOURS Début : 17 novembre 2026 Fin : 16 mars 2027

Module 1	Du 17 au 18 novembre 2026	Paris
Module 2	Du 15 au 17 décembre 2026	Paris
Module 3	Du 19 au 20 janvier 2027	Paris
Module 4	Du 16 au 17 février 2027	Paris
Module 5	Le 16 mars 2027	Paris

Ce programme est une création originale, conçu par les équipes pédagogiques d'ORSYS Formation. Toute reproduction, représentation, adaptation ou exploitation, totale ou partielle, sans autorisation préalable écrite d'ORSYS, est strictement interdite. ORSYS se réserve le droit d'engager toute action nécessaire à la protection de ses droits de propriété intellectuelle.