Présentation &
Programme de la filière

ANALYST SOC

Filière de 57 jours / 399 heures

Version 2025 1,0

PRÉSENTATION DE LA FILIÈRE

Distanciel
5586 € HT / participant
57 jours / 399 heures

La durée et le prix correspondent à une inscription en inter-entreprises. Toute demande intra-entreprise fait systématiquement l'objet d'un devis sur-mesure devant être approuvé pour acceptation.

Objectifs

Maîtriser les fondamentaux de la cyber sécurité défensive.

Se familiariser avec les attaques pour mieux les contrer.

Comprendre les vulnérabilités et leur exploitation.

Protéger son architecture. Détecter des menaces SOC.

Déployer, paramétrer et utiliser le SOC.

Manager la sécurité, les niveaux d'alerte et corrélation d'événements.

Réaliser une veille technologique pour adapter son SOC /SIEM aux nouvelles menaces

Acquérir le savoir être du consultant.

Public

Demandeurs d'emploi souhaitant exercer le métier de Systèmes et Réseaux

Prérequis

Bac+ 2 minimum, candidats intéressés par les activités numériques.

Modalités et délais d'accès

Les postulants devront passer une série d'entretiens pour intégrer la formation

Ils seront informés de leur inscription au plus tard 15 jours avant le début de la session

Accessibilités aux personnes en situation de handicap

Les personnes en situation de handicap sont invitées à nous communiquer leurs besoins spécifiques. Nous ferons tout pour les mettre dans les meilleures conditions de suivi de la formation possibles (compensation, accessibilité…)

Modalités d'évaluation

A l'issue de chaque module, le formateur évaluera chacun des participants en fonction des cas pratiques et exercices effectués

La fin de la formation sera consacrée à un projet final reprenant l'ensemble des acquis de la formation. Les apprenants participeront à une soutenance pour présenter leur projet devant un jury et démontrer leurs nouvelles compétences

Attestation/certification

Une attestation de fin de stage sera remise à tous les participants à l'issue de leur parcours

AJC FORMATION est une S.A.S au capital de 100 000 Euros R.C.S PARIS 500 967 021
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)
6, rue Rougemont - 75009 Paris Tél.: 01 87 58 00 00
eclairezmoi@ajc-formation.fr - www.ajc-formation.fr

PRÉSENTATION DE LA FILIÈRE

Distanciel
5586 € HT / participant
57 jours / 399 heures

La durée et le prix correspondent à une inscription en inter-entreprises. Toute demande intra-entreprise fait systématiquement l'objet d'un devis sur-mesure devant être approuvé pour acceptation.

Méthodes mobilisées

Alternance d'exercices, cas pratiques, QCM et de notions théoriques, projet Fil Rouge avec une répartition du temps de travail : 40% théorie, 60% pratique. Des présentations théoriques des concepts clés illustrés par des démonstrations du formateur (Ex : code live …) seront suivies de mises en pratique des apprenants

Evaluations régulières et retour du formateur sur les points moins bien assimilés. ; les apprenants réaliseront tout au long de la formation des exercices, QCM, mises en situation, TP, TD qui seront corrigés pour faciliter l'acquisition de compétences.

En classe virtuelle, accès à notre plateforme à distance, à des machines virtuelles en local ou dans le cloud contenant les logiciels utiles et les supports de cours en français seront mis à disposition via notre la plate-forme de téléchargement AJC Classroom

Accès à notre plateforme à distance de Classe Virtuelle : mêmes possibilités et interactions avec votre formateur que lors d'une formation présentielle: votre formation se déroulera en connexion continue 7h/7 :

- Echanges directs avec le formateur et l'équipe pédagogique à travers la visioconférence, les forums et chats
- Vérification de l'avancement de votre travail et évaluation par votre formateur à l'aide d'exercices et de cas pratiques
- Suivi pédagogique et conseils personnalisés pendant toute la formation

Vous recevrez les informations de connexion par mail dès votre inscription. En cas de problème de connexion, vous pourrez joindre notre équipe à tout moment (avant ou même pendant la formation) au 01 82 83 72 41 ou par mail (hotline@ajc-formation.fr)

En présentiel, mise à disposition d'ordinateurs portables (16Go RAM, SDD); nos salles sont équipées de matériels pédagogiques (Tableau blanc, vidéo projecteur, tableau tactile…) et informatiques

AJC FORMATION est une S.A.S au capital de 100 000 Euros R.C.S PARIS 500 967 021
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)
6, rue Rougemont - 75009 Paris Tél.: 01 87 58 00 00
eclairezmoi@ajc-formation.fr - www.ajc-formation.fr

PROJET CYBERSOC

Enoncé :

Enoncé : Le projet Fil Rouge de la formation, rendra le stagiaire capable d'assurer les fonctions d'analyste d'un Security Operations Center (SOC), principalement la détection et l'analyse des intrusions, l'anticipation et la mise en place des protections nécessaires.

- Installation d'un SOC
- Utilisation de Splunk
- Durcissement d'un serveur Linux
- …

AJC FORMATION est une S.A.S au capital de 100 000 Euros R.C.S PARIS 500 967 021
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)
6, rue Rougemont - 75009 Paris Tél.: 01 87 58 00 00
eclairezmoi@ajc-formation.fr - www.ajc-formation.fr

CONTENU PÉDAGOGIQUE

COMPORTEMENTAL	RÔLE ET COMPORTEMENT DU CONSULTANT OBJECTIF « QUALITÉ » DE LA MISSION	2 jours
	TRAVAIL EN ÉQUIPE	1 jour
INTÉGRATION	LES FONDAMENTAUX DE LA SÉCURITÉ DÉFENSIVE	2 jours
COMPRENDRE LES ATTAQUES POUR MIEUX LES CONTRER	EXEMPLES D'ARCHITECTURES	1 jour
	DÉFINITION D'UNE VULNÉRABILITÉ	1 jour
	LES DIFFÉRENTS ACCÈS À RISQUES (EXTERNE, WEB, INTERNES, MOBILES …….)	2 jours
	LES DIFFÉRENTES TYPOLOGIES D'ATTAQUES	1 jour
	LES OUTILS OFFENSIFS DE DÉTECTION DES VULNÉRABILITÉS	3 jours
	EXPLOITATION D'UNE VULNÉRABILITÉ	2 jours
	LES OUTILS DÉFENSIFS DE DÉTECTION DES ATTAQUES ET COMPROMISSIONS	2 jours
	VULNERABILITY SCORING & RISK SCORING (CVSS, CVE …..)	1 jour
PROJET	PROJET ATTAQUES	2 jours
SECURISATION DE L'ARCHITECTURE ET DES APPLICATIONS	SÉCURISATION SYSTÈME (LINUX, WINDOWS, AD ….)	2 jours
	SÉCURISATION RÉSEAU (FIREWALL, IPS, IDS…..)	2 jours
	DÉVELOPPEMENT SÉCURISÉ (DEVSECOPS)	1 jour
	SÉCURITÉ VPN, SANS-FIL ET MOBILITÉ	1 jour
	SENSIBILISATION À LA SÉCURITÉ DES APPAREILS ANDROID ET IOS	1 jour
	LES PROTOCOLES (SSH, SSL……)	1 jour
PROJET	PROJET SÉCURISATION	2 jours
SURVEILLANCE ET MANAGEMENT DE LA SECURITE : LE SOC/SIEM	QU'EST CE QU'UN SOC/SIEM	2 jours
	MISE EN PLACE D'UN SOC / SIEM	2 jours
	LES DIFFÉRENTS SOC ET SIEM	1 jour
	LES POINTS DE CONTRÔLE ET NIVEAUX D'ALERTE	2 jours
	DÉTECTION DES MENACES (CORRÉLATION D'ÉVÈNEMENTS)	2 jours
	INVESTIGATION SUR LES INCIDENTS (ANALYSE DES LOGS…..)	2 jours
	SUIVI ET SUPPORT À LA REMÉDIATION	2 jours

AJC FORMATION est une S.A.S au capital de 100 000 Euros R.C.S PARIS 500 967 021
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)
6, rue Rougemont - 75009 Paris Tél.: 01 87 58 00 00
eclairezmoi@ajc-formation.fr - www.ajc-formation.fr

CONTENU PÉDAGOGIQUE

SURVEILLANCE ET MANAGEMENT DE LA SECURITE : LE SOC/SIEM	MISE EN PLACE DE MESURES CORRECTIVES (PATCH MANAGEMENT …)	2 jours
PROJET	PROJET SURVEILLANCE	2 jours
LES NOUVELLES MENACES APT	VEILLE TECHNOLOGIQUE SUR LES NOUVELLES MENACES	1 jour
	MISE EN PLACE DES MESURES PRÉVENTIVES	1 jour
	LA PRODUCTION DES INDICATEURS	1 jour
COMPORTEMENTAL	PRÉSENTER MES NOUVELLES COMPÉTENCES	1 jour
	REDIGER MON CV ET MA LETTRE DE MOTIVATION	1 jour
PROJET	PROJET FINAL & SOUTENANCE - MISE EN PLACE, PARAMÉTRAGE D'UN SOC/SIEM ET DÉTECTION D'ALERTES	5 jours

57 JOURS

AJC FORMATION est une S.A.S au capital de 100 000 Euros R.C.S PARIS 500 967 021
N° de déclaration d'activité 117542701 75 (ce numéro ne vaut pas agrément de l'Etat)

6, rue Rougemont - 75009 Paris Tél.: 01 87 58 00 00
eclairezmoi@ajc-formation.fr - www.ajc-formation.fr