CIRLABS

CERTIFICAT INTERNATIONAL RHOPEN LABS

CYBERSEC

Devenir Analyste CyberSOC, c'est rejoindre une profession d'élite pour assurer la surveillance des systèmes d'information des organisations et entreprises africaines, afin d'aider ces dernières à anticiper, détecter, analyser et gérer les incidents et crises de cybersécurité dont elles sont régulièrement victimes.

Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

1. PRESENTATION DE L'ENTREPRISE

Filiale du Groupe RHOPEN basé en France, RHOPEN LABS est une entreprise de services et prestations numériques qui accompagne ses clients dans la réalisation de leurs projets digitaux.

C'est également un centre de compétences et une plateforme de talents avec pour vocation de recruter, former, placer et accompagner des ingénieurs talentueux dans divers domaines tels que l'Ingénierie logicielle, l'Infogérance, la Cybersécurité. Notre principal objectif est de faire de notre Capital Humain le principal maillon de notre chaîne de valeur. La finalité étant de contribuer, à notre façon, à la lutte contre le chômage endémique qui sévit en Afrique francophone, par la formation des jeunes sur des technologies numériques de pointe au service du développement local. D'où l'accent que nous mettons sur la création des parcours de formation innovants. En tant que certification internationale, CIRLABS Cybersec est un produit de RHOPEN LABS.

1.1 Pourquoi ce parcours?

Il est désormais admis que la forte pénurie de main-d'œuvre qualifiée dans les métiers de la cybersécurité constitue l'un des principaux freins à l'amélioration du niveau de maturité cyber sur le continent africain. Cependant, l'augmentation exponentielle récente des cyberattaques contre les organisations africaines et la recrudescence des incidents de cybersécurité qui en ont découlé ont mis en évidence la pénurie plus chronique d'un profil en particulier : l'Analyste CyberSOC. Il s'agit d'un métier en haute tension dans le monde entier, et particulièrement en Afrique. C'est pour contribuer à combler ce manque que RHOPEN LABS a conçu et développé le parcours de formation continue CIRLABS Cybersec, voulu comme le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain : des Analystes CyberSOC.

Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

CIRLABS
CERTIFICAT INTERNATIONAL RHOPEN LABS
CYBERSEC

2- DESCRIPTION DU METIER D'ANALYSTE CYBERSOC

2.1 Qu'est-ce qu'un **SOC ?**

Un SOC (Security Operation Center) désigne l'ensemble constitué par des personnes, des procédés et des technologies chargé d'assurer la supervision et l 'administration de la sécurité du système d'information d'une organisa- tion.

L'objectif du SOC est de détecter, analyser et remédier aux incidents de cybersécurité à l'aide d'outils et solutions technologiques (SIEM, SOAR, etc.), ainsi que de mettre en place un ensemble de procédés et de démarches afin de veiller à ce que les failles et incidents de sécurité soient identifiés, traités, compris et contrôlés. Dans un environnement mature, le SOC est la cellule de sécurité du système d'information d'une organisation.

2.2 Le métier d'Analyste CyberSOC

L'Analyste CyberSOC est un professionnel de la cybersécurité chargé d'identifier, de catégoriser, d'analyser et de qualifier les événements de sécurité en temps réel ou de manière asynchrone sur la base de rapports d'analyse sur les menaces. Il contribue au traitement des incidents de sécurité avérés en support des équipes de réponse aux incidents de sécurité. Il s'assure également du maintien à jour des dispositifs de supervision et d'analyse de la sécurité comme le SIEM (Software Information Event Management), principal outil de surveillance des incidents en temps réel afin d'en évaluer la dangerosité.

2.3 Principales missions de l'Analyste CyberSOC

- Surveillance, Identification, Analyse et Qualification des événements de sécurité en temps réel dans un système d'information ;
- Évaluation de la gravité des incidents de sécurité ;
- Notification / rapport sur les incidents de sécurité, avec escalade le cas échéant ;
- Contribution à la mise en place des outils SOC / SIEM (détection, analyse, investigation, etc.) ;
- Participation au développement et au maintien des règles de corrélation d'événements.

2.4 Nos atouts pour proposer cette formation

- Programme d'apprentissage axé sur la pratique et la mise en situation professionnelle ;
- Accompagnement personnalisé par des experts du domaine ;
- Coaching RH pour faciliter les entretiens d'embauche, la rédaction de bon CV/lettre de motivation, l'intégration en entreprise ;
- Projet fil rouge tout au long de la formation ;
- Simulateur pour s'exercer dans les mêmes conditions qu'en entreprise ;
- Acquisition des compétences nécessaires pour valider plusieurs certifications d'éditeurs ;
- Reconnaissance étatique et académique en cours.

2.5 Ce que vous obtenez en suivant la formation **CIRLABS CyberSec**

- Développez des compétences techniques recherchées et boostez votre CV;
- Préparez-vous au très demandé profil d'Analyste CyberSOC et accélérez votre insertion professionnelle ;
- Devenez directement employable sur le marché international.

3. NOTRE EQUIPE

François-Xavier DJIMGOU – Président RHOPEN LABS, Responsable formation Cybersécurité Titulaire d'un MBA Exécutif option Cybersécurité à l'Ecole de Guerre Economique de Paris, détenteur de plusieurs certifications en la matière et fort de ses années d'expérience à l'international en tant que consultant, conférencier, enseignant et même auteur sur les thématiques de Cybersécurité et de Cyberdéfense, François-Xavier a conçu et élaboré le cursus CIRLABS CyberSec. Il est responsable du contenu et garant de l'approche pédagogique ainsi que de la qualité de cette formation.

Patrick AZOGNI– CTO RHOPEN LABS, Référent Technique Consultant DevOps Senior / Architecte Cloud avec à son actif plus de 17 ans d'expérience, Patrick détient également plusieurs certifications dans le domaine. Passionné par l'ingénierie logicielle et l'approche DevOps, il a piloté avec son équipe d'experts le développement et la mise en place de notre plateforme de simulation SOC Labs utilisé tout au long de cette formation.

Leslie MBANGO - Responsable formation & coach RH Dotée d'une maîtrise en Gestion des Ressources Humaines, Leslie est aussi diplômée et consultante Junior dans le même domaine. Passionnée par le développement des compétences, elle est responsable de la mise en œuvre et du bon déroulement de la formation. En cela, elle assure le coaching RH et accompagne les apprenants depuis la conception de leur CV et jusqu'à leur intégration professionnelle.

CIRLABS
CERTIFICAT INTERNATIONAL RHOPEN LABS
CYBERSEC

4. NOTRE DEMARCHE PEDAGOGIQUE

Le but de cette formation est de vous rendre directement opérationnelle dans l'exercice du métier d'Analyste CyberSOC ou de consultant en cybersécurité. A l'issue du parcours, les apprenants seront en mesure de détecter, d'analyser et de gérer les événements et incidents de sécurité au sein d'une organisation.

Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

Afin d'atteindre cet objectif, nous avons développé une approche pédagogique unique qui se décline comme suit :

4.1 Session de bienvenue

Cette session est mise en place afin de :

- Expliquer le déroulement de la formation dans le temps, la liste des compétences à acquérir, et la présentation de l'environnement technique ;
- Présenter les ressources documentaires et la façon d'y accéder ;
- Présenter la liste de certifications professionnelles d'éditeurs des solutions de Cybersécurité à obtenir durant son parcours.

4.2 Format hybride

Cette formation intensive et pratique est dispensée en français de façon hybride :
Une partie (35%) constituée de cours théoriques ou masterclass donnés par nos enseignants praticiens, afin que les auditeurs puissent bien maîtriser les concepts liés au métier de consultant en cybersécurité en général, et d'Analyste CyberSOC en particulier. Ce sera soit en visioconférence, soit en présentiel dans notre siège à Douala.
L'autre partie (65%) est consacrée à vos exercices pratiques et votre projet fil rouge, avec l'accompagnement pédagogique de nos formateurs experts en cybersécurité, notamment à travers nos canaux de communication en ligne.
Ce format donne la flexibilité nécessaire à l'apprenant, en lui permettant de s'organiser par rapport à ses autres activités (académiques et / ou professionnelles).

4.3 Masterclass

Un planning des masterclass est établi en début de formation. Il peut être réalisé en présentiel ou à distance selon la thématique abordée. Les objectifs et les formats pédagogiques de chaque Masterclass peuvent varier en fonction des sujets abordés. Il peut s'agir d'une discussion autour des cas d'usage concrets, un cours d'approfondissement sur des sujets techniques, ou encore la découverte de thématiques spécifiques et intéressantes pour améliorer le profil des apprenants (gestion des projets, leadership, management, entreprenariat, etc.).

4.4 Simulateur et travaux pratiques

Durant la formation, les auditeurs auront accès à notre simulateur SOC Labs. Il s'agit d'un laboratoire en ligne développé par RHOPEN LABS pour une mise en situation professionnelle par des scenarii d'analyse et traitement des incidents de sécurité, ce qui permet ainsi à nos apprenants de s'exercer sur les procédés et solutions SOC qu'ils retrouveront effectivement en entreprise. C'est dans cet environnement que chaque apprenant va mener un projet concret dont l'objectif est de simuler une attaque informatique réelle pour lui permettre de mieux comprendre les différentes techniques utilisées par les cybercriminels. L'idée est de mettre en pratique les compétences qu'il est en train d'acquérir en matière d'anticipa- tion, de détection, d'analyse et de traitement des incidents de cybersécurité. Ce projet nécessite un investissement d'environ 100 à 120 heures de travaux pratiques tout au long de la formation. Des séances d'accompagnement sont organisées régu- lièrement par les enseignants pour orienter et coacher les apprenants. Cela permet de passer efficacement de la théorie à la pratique et de s'assurer que chacun maîtrise les compétences du profil d'Analyste CyberSOC. C'est aussi un projet fortement apprécié par les entreprises. Il confirme les compétences et connaissances pratiques acquises à l'issue de la formation CIRLABS Cybersec. L'auditeur pourra alors justifier de ses compétences en Cybersécurité opérationnelle à l'aide d'un projet abouti pendant ses entre- tiens d'embauche.

4.5 Coaching et accompagnement RH

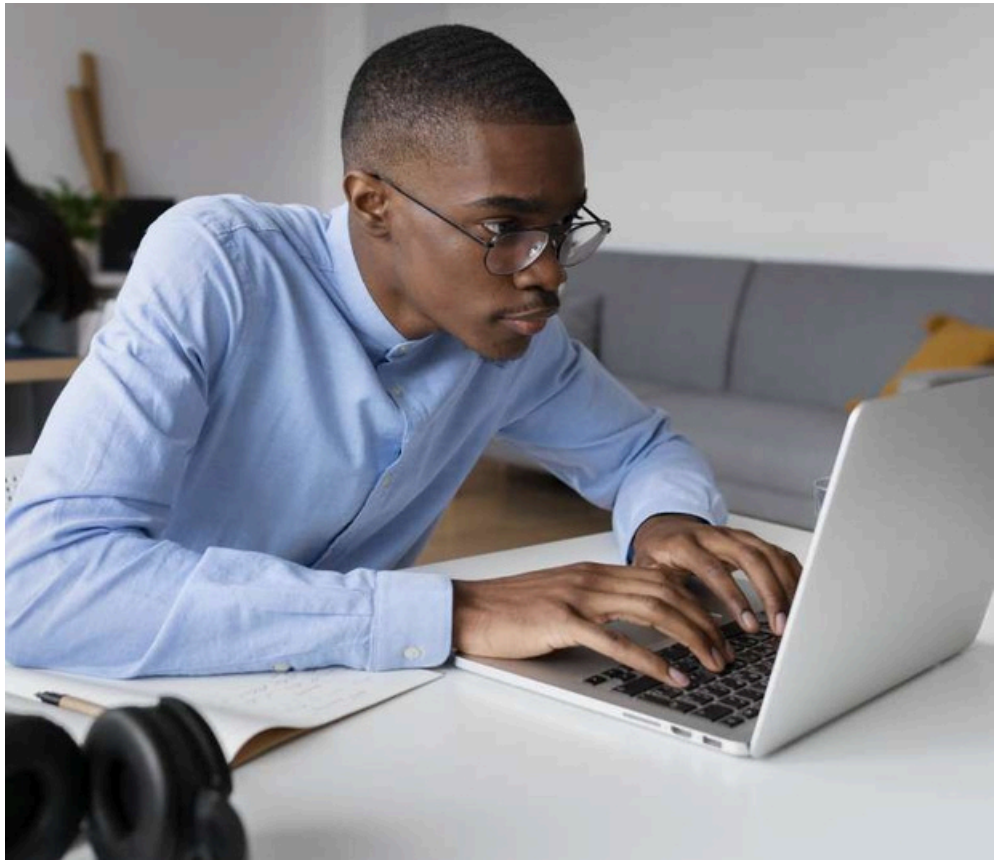
Notre équipe RH suit chaque apprenant tout au long de son parcours et lui offre la possibilité de profiter d'un coaching carrière individualisé. Par ailleurs, nous offrons un accompagnement dans la rédaction de CV et lettre de motivation ainsi que la préparation pour les entretiens d'embauche.

AUTRES MODALITÉS PÉDAGOGIQUES

Durée de la formation

Le parcours CIRLABS CyberSec est une formation continue conçue pour s'adapter aux contraintes académiques et professionnelles des apprenants. Elle s'étale sur une année académique, avec un rythme estime de 10 à 12h par semaine.
Elle est décomposée en 2 parcours indépendants à savoir :

- Parcours Analyste SOC Confirmé : la formation s'étend sur 10 mois ;
- Parcours Analyste SOC Junior : la formation s'étend sur 03 mois.



Méthode d'évaluation

Chaque apprenant sera évalué de la façon suivante :
• Validation du niveau d'expérience requis pour chaque type d'activité ;
• Restitution du projet Fil rouge (présentation et soutenance) ;
• Evaluation positive suite à un entretien technique ;
• Réussite à l'examen de certification.

Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

CIRLABS
CERTIFICAT INTERNATIONAL RHOPEN LABS
CYBERSEC

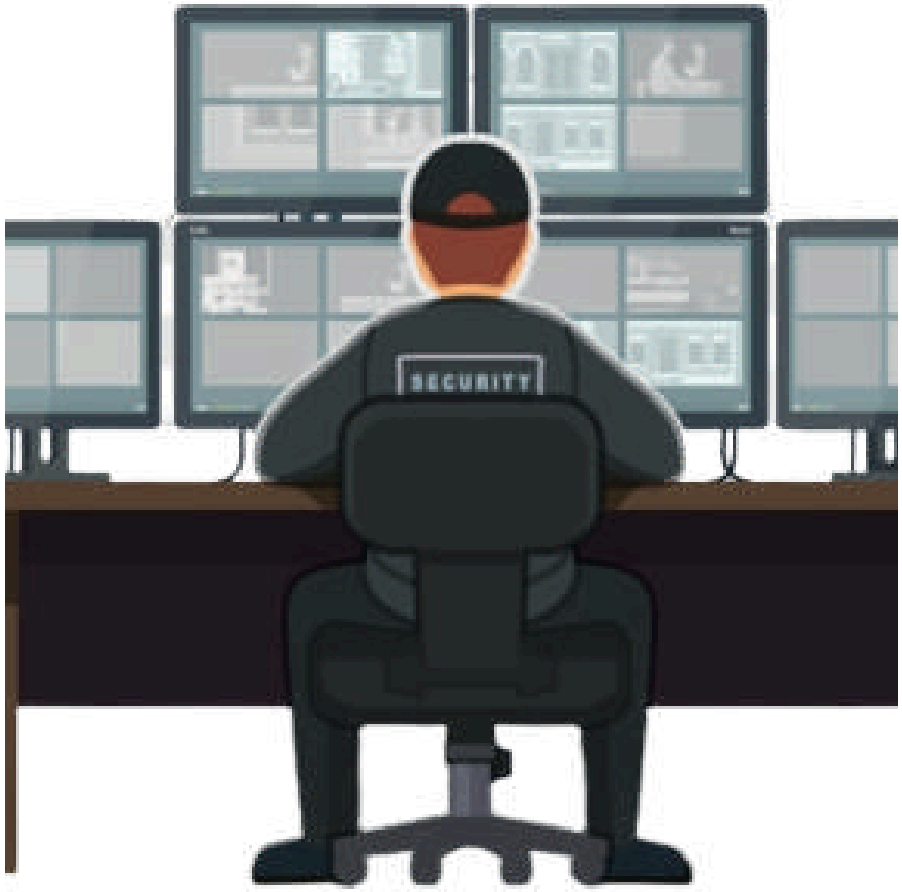
5. LES ACTIVITÉS TYPES DE LA FORMATION

Choisir de suivre ce parcours de Certification Internationale chez RHOPEN LABS, c'est s'assurer de devenir un Analyste CyberSOC qualifié et prêt pour le marché de l'emploi. Au cours de cette formation, les apprenants vont acquérir de solides connaissances sur des activités types relevant du profil d'Analyste CyberSOC qui sont liées à des compétences professionnelles dans divers domaines très techniques globalement restituées dans le tableau suivant : :

Activités types	Compétences professionnelles
Surveillance, Détection et Qualification des menaces / événements de sécurité	Identifier les événements de sécurité en temps réel, les analyser et les qualifier Évaluer la gravité des incidents de sécurité Notifier les incidents de sécurité, escalader le cas échéant
Analyse et gestion des incidents de sécurité	Réaliser une analyser approfondie et élaborer un plan d'action de traitement d'un des incidents de sécurité Faire des recommandations sur les mesures de remédiation immédiates et assister à leur mise en œuvre Participer au développement, à l'optimisation et au maintien des règles de détection et de corrélation d'événements de sécurité
Elaboration et mise en œuvre d'une stratégie de veille et d'amélioration continue pour optimiser la gestion des incidents	Collaborer à l'amélioration continue des procédures de traitement des nouveaux types d'incidents Contribuer à la définition de la stratégie de collecte des journaux d'évènements, ainsi qu'à l'optimisation des outils de détection (SIEM, etc.) Contribuer à la veille permanente sur les menaces, les vulnérabilités et les méthodes d'attaques

CIRLABS
CERTIFICAT INTERNATIONAL RHOPEN LABS
CYBERSEC

CONTENU DE LA FORMATION



Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

Parcours Analyste SOC Confirmé

Les fondamentaux de la cybersécurité

- Compréhension des enjeux de la cybersécurité, des cybermenaces d'aujourd'hui et des méthodes les plus adaptées pour sécuriser les données; - Connaissance des bonnes pratiques.

Théorie de la connaissance et introduction au métier d'analyste

Une série de lectures obligatoires et de masterclass portant sur les notions de connaissance, d'information, de rationalité, de paradigme, de perception et représenta- tion du monde, de méthodologie d'analyse, etc.

Introduction à la sécurité opérationnelle des SI

- Installation, configuration et administration des équipements de cybersécurité (parefeu, proxy, IPS, IDS, IDM, etc); - Sécurisation des systèmes d'exploitation et des protocoles réseaux, etc.

Supervision, analyse et gestion des incidents de sécurité

- Identification, analyse et qualification des événements de sécurité en temps réel;
- Évaluation la gravité des incidents de sécurité;
- Notification / rapport sur les incidents de sécurité, avec escalade le cas échéant, etc.

Etude des stratégies d'attaque et de défense

'- Comprendre les concepts de hacking et de la cyberkill chain;
- Connaître les principaux outils et méthodes d'attaques;
- Comprendre le processus d'une attaque, etc.

Renseignement et investigation sur les menaces cyber

- Savoir reconnaître et identifier les différents types de menace cyber;
- Connaître les différentes catégories d'acteurs de la menace cyber;
- Comprendre les modes opératoires, etc.

Introduction à la gouvernance Cyber

'- Evaluation et gestion des risques cyber;
- Pilotage d'un projet de cybersécurité;
- Sensibiliser et former sur les bonnes pratiques de cybersécurité, etc.

gestion de projet informatique

Connaître le processus de gestion, de planification et de développement, les méthodes de gestion de projet et les outils propres au domaine de l'informatique.

Parcours Analyste SOC Junior

Les fondamentaux de la cybersécurité

- Compréhension des enjeux de la cybersécurité, des cybermenaces d'aujourd'hui et des méthodes les plus adaptées pour sécuriser les données; - Connaissance des bonnes pratiques.

Introduction à la sécurité opérationnelle des SI

- Installation, configuration et administration des équipements de cybersécurité (parefeu, proxy, IPS, IDS, IDM, etc); - Sécurisation des systèmes d'exploitation et des protocoles réseaux, etc.

Etude des stratégies d'attaque et de défense

'- Comprendre les concepts de hacking et de la cyberkill chain;
- Connaître les principaux outils et méthodes d'attaques;
- Comprendre le processus d'une attaque, etc.

Supervision, analyse et gestion des incidents de sécurité

- Identification, analyse et qualification des événements de sécurité en temps réel; - Évaluation la gravité des incidents de sécurité; - Notification / rapport sur les incidents de sécurité, avec escalade le cas échéant, etc.

Renseignement et investigation sur les menaces cyber

- Savoir reconnaître et identifier les différents types de menace cyber;
- Connaître les différentescatégories d'acteurs de la menace cyber;
- Comprendre les modes opératoires, etc.

6. DÉBOUCHÉS PROFESSIONNELS

Selon le parcours et l'expérience, l'apprenant pourra postuler aux profils suivants à l'issu de la formation :

- Analyste SOC/SIEM;
- Analyste en Cybersécurité Opérationnelle;
- Opérateur Analyste CyberSOC;
- Consultant en cybersécurité;
- Analyste CyberSOC;
- Analyste détection d'incident;
- Veilleur-Analyste;
- Expert en sécurité des systèmes d'information.

A l'issu de sa formation, nous pouvons également accompagner l'apprenant vers les débouchés suivants :

- Possibilité d'intégration professionnelle au sein du future SOC de RHOPEN LABS ;
- Possibilité de contrat en Freelance RHOPEN LABS ;
- Possibilité de recommandation professionnelle (lettre de recommandation).

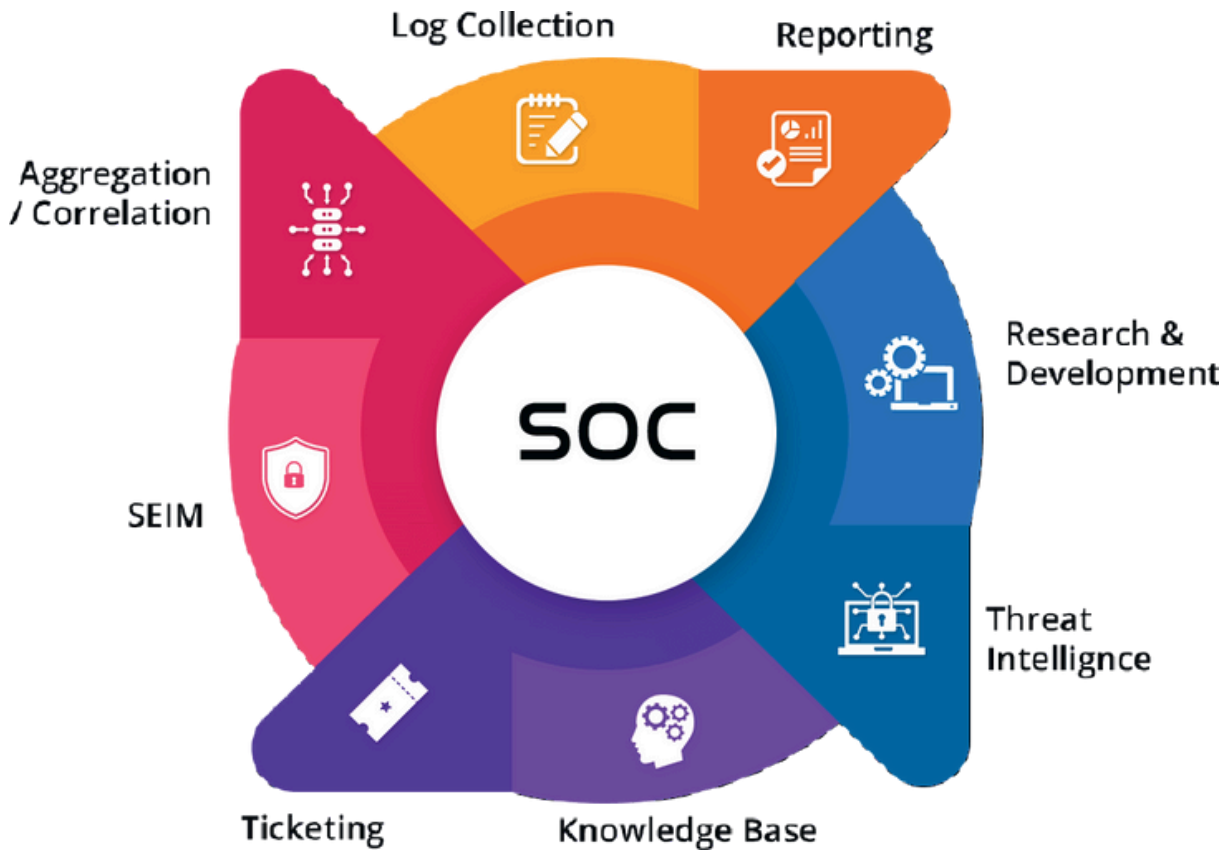
CIRLABS
CERTIFICAT INTERNATIONAL RHOPEN LABS
CYBERSEC

7. NOTRE PLUS

Tout au long du parcours de formation, l'apprenant obtiendra toutes les compétences nécessaires à la validation (s'il le souhaite et à ses frais) de plusieurs certifications professionnelles d'éditeurs de solutions de Cybersécurité, notamment les suivantes :

- NSE1;
- NSE2;
- NSE3;
- CompTIA Security+;
- CCNA Security;
- CompTIA Cybersecurity Analyst (CySA+);
- Cisco CyberOps Associate;
- Microsoft Security Operations Analyst;
- Certified Ethical Hacker (CEH);
- OffSec Defense Analyst (OSDA);

Nous recommandons aux apprenants de passer au moins une de ces certifications professionnelles d'éditeurs.



Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

CIRLABS
CERTIFICAT INTERNATIONAL RHOPEN LABS
CYBERSEC

8. INSCRIPTION ET ADMISSION

Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

8.1 Prérequis

Afin d'accéder à notre parcours CIRLABS CyberSec qui prépare au prestigieux métier d'Analyste CyberSOC, les candidats doivent obligatoirement justifier des prérequis suivants :

- Être titulaire au minimum d'un diplôme de niveau Bac+3 en informatique, Système et Réseaux ou équivalent, idéalement avec une spécialité en sécurité des systèmes d'information;
- Présenter une première certification en sécurité de l'information;
- Une précédente expérience dans n'importe quel domaine de la cybersécurité serait un vrai plus;
- Être muni d'un ordinateur (PC ou Mac);
- Avoir une bonne connexion Internet.

8.2 Coût de la formation

Pour sa toute première session, la formation CIRLABS CyberSec est au prix promotionnel de

- 2.200.000 FCFA, pour le **parcours confirmé,** dont une avance exigible dès l'inscription et le reste en 3 tranches, la totalité étant versées selon l'échéancier
- 600.000 FCFA, pour le **parcours junior**, dont une avance de 100.000 FCFA pour l'inscription et le reste payable en plusieurs tranches.

CIRLABS
CERTIFICAT INTERNATIONAL RHOPEN LABS
CYBERSEC

8.3 Comment candidater?

Pour postuler au programme CIRLABS CyberSec, déposez votre candidature sur le site :
www.academy.rhopenlabs.africa

La procédure d'admission est la suivante :

- Vérification des prérequis ;
- Test d'aptitudes techniques ;
- Entretien de motivation ;
- Décision d'admission ou d'ajournement.

Avant de postuler, n'hésitez pas à contacter notre équipe d'admission qui est disponible pour répondre à toute préoccupation relative à ce parcours.
Se former au métier d'Analyste CyberSOC, c'est rejoindre une profession d'élite au service du cyberespace africain !

Le creuset des veilleurs, protecteurs et défenseurs du cyberespace africain.

RHOPEN LABS Academy

NOS DOMAINES D'INTERVENTION

- INGÉNIERIE LOGICIELLE
- CYBERSÉCURITÉ
- GESTION DES INFRASTRUCTURES CLOUD
- FORMATION

NOS FORMATIONS

- CYBERSÉCURITÉ
- BLOCKCHAIN
- DEVOPS

KOTTO, BP: 5979, DOUALA - CAMEROUN
233 472 249 / 696 174 812
academy@rhopenlabs.africa
www.academy.rhopenlabs.africa