DATAPROTECT
Security is our commitment

Bloc	Contenu	
Header	**Titre de la filière**	Analyste SOC
	Logo de l'opérateur de formation	DATAPROTECT Security is our commitment
	Sous – titre	Deviens Analyste SOC en 6 mois
	Durée	6 mois
	Lieu de formation	DATAPROTECT - Casanearshore
	Prochaine session	Mars 2024
	Prérequis	• Être titulaire au minimum d'un Bac+2 en informatique • Être prédisposé et engagé à se reconvertir vers un métier de la cybersécurité
Débouchés : les postes que vous pourrez occuper après cette formation	L'analyste SOC est un professionnel de la cybersécurité qui travaille à identifier et à gérer les cybermenaces. ▪ **Surveillance des Menaces :** Il surveille les systèmes d'information pour détecter toute activité suspecte. Il utilise des rapports et des analyses pour comprendre et classer ces menaces. ▪ **Gestion des Incidents :** Quand un problème de sécurité est confirmé, il aide à le résoudre. ▪ **Évaluation et Réparation des Dommages :** Si une intrusion se produit, l'analyste SOC évalue les dégâts et travaille avec d'autres professionnels du domaine pour trouver des solutions et remettre les systèmes en marche. ▪ **Mise à Jour des Outils de Sécurité :** Il s'assure que les outils de surveillance de la sécurité, comme le SIEM (un système qui aide à	

	relier et à évaluer les incidents de sécurité), sont à jour et fonctionnent correctement. ▪ **Prévention et Conseil :** L'analyste SOC joue également un rôle préventif en éduquant les utilisateurs sur les meilleures pratiques de sécurité et en donnant des conseils sur comment garder les systèmes sûrs. En résumé, l'analyste SOC est crucial pour protéger les systèmes informatiques des entreprises contre les cybermenaces, en surveillant les activités, en gérant les incidents et en conseillant sur les meilleures pratiques de sécurité.
Pourquoi devenir Analyste SOC en 2023 ?	Devenir analyste SOC présente de nombreux avantages et opportunités, en raison de l'évolution rapide du paysage de la cybersécurité et de la demande croissante de professionnels qualifiés dans ce domaine. **Forte demande face à une pénurie de ressources :** Avec l'augmentation constante des cyberattaques, la demande pour des analystes SOC qualifiés est en hausse. Les entreprises cherchent à renforcer leurs défenses contre les menaces face à une rareté significative des profils. **Rôle Vital dans la Cybersécurité :** Les analystes SOC jouent un rôle clé dans la protection des informations sensibles et des infrastructures critiques contre les cybermenaces. **Potentiel de Carrière et de Croissance :** Le rôle d'analyste SOC offre des possibilités de progression vers des postes de niveau supérieur, tels que gestionnaire d'incidents de sécurité, consultant en cybersécurité, ou même des rôles de direction des centres de supervision. **Diversité des Secteurs :** Tous les secteurs d'activité ont besoin de protéger leurs données et systèmes, ce qui offre aux analystes SOC une grande variété de domaines où travailler, allant de la finance à la santé, en passant par le gouvernement et le commerce de détail. **Rémunération Attractive :** En raison de leur rôle crucial et de la demande croissante, les analystes SOC bénéficient souvent de salaires compétitifs et d'avantages attractifs.

Compétences : ce que vous allez apprendre	▪ Sécurité des systèmes d'exploitation ▪ Sécurité des réseaux et protocoles ▪ Pratique de l'analyse de journaux (systèmes ou applicatifs) ▪ Pratique de l'analyse de flux réseaux ▪ Connaissance d'outils et de méthodes de corrélation de journaux d'événements (SIEM) ▪ Connaissances des solutions de supervision de sécurité ▪ Connaissance des techniques d'attaques et d'intrusions ▪ Connaissances des vulnérabilités des environnements ▪ Scripting
Programme de la formation	**Tronc Commun : (8 Semaines de formation et travaux pratiques)** 1. Comprendre et mettre en œuvre un réseau informatique 2. Appréhender Windows Server 3. Gérer et administrer un Système Linux 4. Méthodes et techniques de la gestion de projets 5. Conformité aux normes de cybersécurité et aux exigences règlementaires (DNSSI, Loi 09-08, ISO27001) 6. Gestion de risques 7. Introduction à la Cryptographie 8. Introduction à la programmation Python 9. Introduction aux métiers de la Cybersécurité **Spécialisation en Analyste SOC (8 semaines de formation et Labs)** 1. Rôles et fonctions du SOC 2. Cyber Defense Frameworks 3. Threat Intelligence 4. Sécurité des Réseaux et Analyse du Trafic 5. Endpoint Security Monitoring 6. Security Information and Event Management 7. Digital Forensics and Incident Response 8. Methodes et outils de Phishing **Pratique intensive et professionnalisation (8 Semaines)** **Soft Skills et préparation professionnelle (En continu)** 1. Personal Branding

	2. Techniques de communication en entretien d'embauche 3. Intelligence relationnelle en milieu professionnel
Notre méthode	En tant que bras éducatif de DATAPROTECT, nous tirons parti d'une connaissance terrain profonde et d'un retour d'expérience inégalé. Cette immersion directe dans le domaine nous offre une perspective unique, nous permettant d'anticiper les besoins réels des entreprises et de former nos participants en conséquence. Notre méthode de formation place les participants dans un environnement professionnel réel tout au long du parcours en mode Learning By Doing.
À quoi s'attendre pendant le Bootcamp ?	**Acquisition de Connaissances :** ▪ Les participants recevront une formation approfondie sur les principes fondamentaux de la cybersécurité, y compris les rôles, les fonctions et les outils d'un analyste SOC. Ils apprendront à identifier et à réagir aux différentes formes de cyberattaques et à comprendre le paysage changeant des menaces en ligne. **Acquisition de Compétences Pratiques :** ▪ Des sessions pratiques en laboratoire et des simulations réalistes permettront aux participants de mettre en œuvre les concepts appris en classe. ▪ Ils pratiqueront des techniques telles que l'analyse du trafic réseau, la surveillance de la sécurité des Endpoints, et l'utilisation de SIEM pour la gestion des événements de sécurité. **Professionnalisation par Projets Réels :** ▪ Les participants travailleront sur des projets réels pour acquérir une expérience concrète. ▪ Ces projets offrent une opportunité d'appliquer les compétences apprises dans un contexte professionnel, en abordant des problèmes réels de cybersécurité.

	Encadrement par des Experts du métier : ▪ Des professionnels expérimentés avec une solide expérience terrain fourniront des conseils et partageront leurs connaissances pratiques. **Encadrement Individualisé et travaux de groupes :** ▪ Chaque participant bénéficiera d'un suivi personnalisé pour garantir une progression adaptée à ses besoins et objectifs. ▪ Les participants seront encouragés à collaborer en petits groupes, favorisant l'apprentissage par les pairs et le développement de compétences en travail d'équipe. ▪ Ces sessions renforcent la résolution de problèmes collaboratifs et la communication efficace. **Outils de Pratique Avancés :** ▪ Le programme offre l'accès à des outils de cybersécurité de pointe et des plateformes de simulation pour une expérience d'apprentissage enrichissante. **Préparation à une Certification Internationale (Optionnelle) :** ▪ À la demande, une préparation spécifique pour une certification reconnue internationalement en cybersécurité peut être intégrée. ▪ Cette option ajoute une valeur significative à la formation, en offrant une reconnaissance professionnelle et en ouvrant des portes sur le marché de l'emploi. Ce Bootcamp est conçu pour offrir une expérience d'apprentissage complète et immersive, qui prépare les participants à devenir des analystes SOC compétents et prêts à faire face aux défis actuels de la cybersécurité.

Présentation de l'operateur	Depuis notre création en 2009, DATAPROTECT s'est imposé comme un leader incontesté dans l'écosystème de la cybersécurité, en démontrant un engagement sans faille à offrir une expertise pointue et un accompagnement 360° au profit de plus de 500 clients actifs sur 3 continents, y compris une centaine de banques. Notre approche personnalisée prend en compte les particularités de chaque client, enrichissant notre vaste bibliothèque de use-cases et renforçant notre expertise déjà solide. Notre équipe, composée de plus de 150 consultants Full Security, opère pour renforcer la sécurité des systèmes d'information de nos clients, les assister dans leur conformité aux normes réglementaires, et protéger leurs données sensibles et leur image de marque. Grace à notre expérience, nous avons développé le Cybersecurity Skills Lab qui se présente comme une solution chirurgicale à la problématique de la pénurie des ressources, à travers des solutions disruptives incluant des programmes UPSKILL de montée en compétences spécialisées, des certifications reconnues à l'international et des parcours RESKILL de reconversion vers les métiers d'avenir dans le domaine de la cybersécurité. Grace à une infrastructure immersive nos apprenants sont placés dans un Bootcamp de Learning By Doing permettant une professionnalisation opérationnelle rapide et efficace.
Candidature	**Pré-requis :** • Disposer au minimum d'un Bac+2 en informatique **Critères de sélection :** • Étude de dossier • Motivation du participants **Candidature :** • Inscription en ligne sur la plateforme JobInTech • Présélection • Test de positionnement & Entretien • Validation et inscription au programme