Analyste SOC (Security Operations Center)

Durée: 8 Jours Réf de cours: GKSOC Version: 1.0 Méthodes d'apprentissage: Classe à distance

Résumé:

Le métier d'analyste SOC (Security Operations Center) est au cœur des dispositifs de cybersécurité des organisations.
Chargé de détecter, analyser et réagir face aux incidents de sécurité, l'analyste SOC joue un rôle clé dans la protection des systèmes d'information.
Ce cursus a été conçu pour répondre aux exigences croissantes du métier : il offre une formation complète, mêlant théorie, exercices pratiques, outils spécialisés et compréhension des menaces. Il constitue ainsi une passerelle essentielle vers un poste opérationnel en cybersécurité défensive.

Mise à jour : 16.12.2025

Public visé:

Techniciens et administrateurs Systèmes et Réseaux, responsables informatiques, consultants en sécurité, ingénieurs, responsables techniques, architectes réseaux, chefs de projets...

Objectifs pédagogiques:

- A l'issue de la formation, vous pourrez:
- Connaître le rôle et les missions d'un analyste SOC
- Maîtriser les fondamentaux de la cybersécurité défensive
- Utiliser les outils et technologies du SOC
- Analyser et corréler les événements de sécurité
- Gérer les incidents de sécurité
- Rédiger des rapports techniques
- Travailler en coordination avec les autres équipes de cybersécurité
- Faire de la veille (cybermenaces, techniques d'attaques)

Pré-requis:

Prérequis :

- Avoir des connaissances en réseau
- Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.
- GKCYBER - Parcours introductif à la Cybersécurité

Contenu:

Journée 1 – Fondamentaux sécurité ; gestion des risques :

- Démarrage de la formation
- Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.

Module 1. Principes fondamentaux SOC et cybersécurité

- Enjeux de la sécurité de l'information et rôle d'un SOC
- Terminologie clé : événement, incident, alerte, vulnérabilité
- Cadres normatifs : ISO 27005, ISO 31000
- Identification et évaluation des risques (quantitatif/qualitatif)

LAB : QCM + cas d'identification de risques

Module 2. Sécurité défensive

- Traitement des risques : atténuation, transfert, acceptation
- Mesures organisationnelles, techniques, humaines
- Exemples concrets

LAB : Étude de scénarios + application de mesures de sécurité

Journée 2 – SOC, métiers, logs et Syslog :

Module 3. Comprendre le SOC

- Historique, besoins, missions
- Architecture, modèle SOC 1 à 3 niveaux
- Technologies : SIM, SIEM, SEM
- Rôles SOC : analyste, superviseur, incident handler

Module 4 Métier de l'analyste SOC

- Compétences clés
- Missions quotidiennes : surveillance, investigation, rapport
- Organisation des shifts

Module 5. Les logs et le serveur Syslog

- Définition, formats, sources
- Protocole Syslog et architecture
- Utilisation pratique

LAB : Installation d'un serveur Syslog + collecte de logs simulés

LAB :

- Déploiement d'un mini-SIEM (ELK, Graylog ou Wazuh)
- Ingestion de logs, configuration d'alertes
- Requête et tableaux de bord

Journées 4 – Organisation du SOC ; Gestion des incidents :

Module 7. Gestion des incidents

- Typologie, normes (ISO 27035, NIST SP800-61)
- Processus : détection, qualification, traitement
- Équipes CERT et CSIRT
- Obligations légales

LAB : Cas pratiques d'incident + journal d'analyse

Journées 5 – Gestion des vulnérabilités ; Cadre MITRE ATT;CK

Module 8. Gestion des vulnérabilités

- CVE, CVSS, remédiation

Outils : Nessus, OpenVAS

LAB : Scan réseau + priorisation + rapport

Module 9. Gestion des menaces : MITRE ATT;CK

- Tactiques, techniques, IOC
- Utilisation d'ATT;CK Navigator
- Mapping des incidents

LAB : Identification des TTPs sur incident simulé

Journées 6 – Introduction à la CTI ; Typologie de menaces

Module 10 Introduction à la CTI

- Objectifs, terminologie, cycle du renseignement
- Sources ouvertes / fermées
- Typologie des menaces : APT, ransomware, insiders

LAB : QCM + analyse de menaces

Journées 7 –

Outils de CTI ; intégration SOC

Module 11. Outils de CTI

- MISP, OpenCTI, Threat feeds
- Intégration avec le SOC
- IOC, TTP et enrichissement automatique

LAB : Installation OpenCTI / MISP + ingestion d'IOC

Module 12. Intégration de la CTI

- Définition d'un programme CTI
- Processus et procédures internes
- Rattachement au SOC et reporting

LAB : QCM + architecture de CTI d'entreprise

Journée 8 – Elastic SIEM :

Module 13. Mise en œuvre complète Elastic Stack

- Elastic NV, Beats, Logstash, Kibana
- Syntaxe Lucene, filtres, tableaux de bord
- Corrélation d'alertes

LAB : Déploiement complet d'un SIEM avec données simulées

- Clôture de la formation

Journée 3 – SIEM : installation ; corrélation :

Module 6 Exploration des SIEM

- Composants d'un SIEM moderne
- Architecture type : agent, collecteur, indexeur, interface
- Préparation des sources et parsing
- Recherche et corrélation

Méthodes pédagogiques :

Répartition théorie / pratique

40 % Théorie
60 % Pratique (labs et simulations)

Accès à un espace de partage sécurisé contenant :
-Le support de cours officiel au format électronique
-Les QCM d'entraînement
-Les fichiers d'exercices et corrigés
-Les modèles de documents utilisés dans les travaux pratiques

Suivi qualité et évaluation
-Avant la formation : Questionnaire de positionnement / diagnostic envoyé aux participants afin de recueillir les attentes, le niveau initial et détecter d'éventuels besoins spécifiques (techniques, pédagogiques ou liés à l'accessibilité)
-Pendant la formation : Évaluation à chaud en fin de première journée pour recueillir les ressentis immédiats et ajuster l'animation pédagogique si besoin ,Quiz, exercices, cas pratiques, Mises en situation, Échanges pédagogiques avec le formateur
-À l'issue de la formation : Questionnaire de satisfaction à chaud (participant + formateur), Une attestation de suivi de fin de formation sera délivrée à chaque participant

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement