< RECOMMANDATIONS DE FORMATION DES ANALYSTES CLOUD >

Fiches métiers

CAMPUS CYBER 2025

< SOMMAIRE >

AVANT-PROPOS

Ce document présente les recommandations émises par la Communauté d'Intérêt (CI) « Détection dans le cloud » et formalisées dans le cadre des travaux du Groupe de Travail (GT) « Formation des analystes Cloud ».

L'objectif du GT est d'identifer les compétences nécessaires aux analystes Cloud, en fonction de leur niveau d'expertise et des responsabilités qui leur sont confiées. Des fiches métiers ont ainsi été produites, complétées de cadrages d'exercices et de recommandations de certifications.

Pour produire ces livrables, les membres du GT se sont appuyés sur des ressources existantes, disponibles en libre accès : les fiches métiers de l'ANSSI et la « Matrice des compétences » établie par la CI « Formation » du Studio des Communs. Les références faites à ces documents sont explicitement indiquées par le code couleur suivant :

- Fiches métier ANSSI « Analyste réponse aux incidents de sécurité », « Responsable du SOC » et « Administrateur de solutions de sécurité ».
- Matrice de Compétences du Campus Cyber Opérateur analyste SOC.
- Recommandations du GT Formation des Analystes Cloud

CONTRIBUTIONS

Coordinateur du GT et contributeur : Pierre Parrend (EPITA)
Contributeurs actifs : Timothé Penisson (Bouygues Telecom), Nadège Lesage (Hexatrust), Umut Sarioglu (CEFCYS).
Autres contributeurs : Christophe Kattnig (INRIA) , Arnaud Kob (Bouygues Telecom), Christine Grassi (CEFCYS)

DÉFINITIONS

- **SOC** : Security Operations Center - Centre des Opérations de Sécurité
- **Niveau N1 de SOC** : Triage et première qualification des alertes
- **Niveau N2 de SOC** : Détection et caractérisation d'activité malveillante au sein du système d'information
- **Niveau N3 de SOC** : En appui aux niveaux 1 et 2 sur des incidents nouveaux et/ou complexes

< AVANT-PROPOS >

RÉCAPITULATIF DES LIVRABLES

Fiches métiers

- Analyste SOC pour le Cloud - N1
- Analyste SOC pour le Cloud - N2
- Analyste SOC pour le Cloud - N3
- Responsable de SOC
- Administrateur technique de SOC

Cadrage d'exercices

- Cadrage des pratiques encadrées, par métier.
- Cadrage d'un exercice d'intrusion, transversal.

Recommandation de certifications

- Référentiel de certification pour les analystes SOC de niveau 1, 2, 3.

ANALYSTE SOC POUR LE CLOUD - N1

- **Autres titres équivalents :** Analyste CyberSOC, Analyste détection d'incident, Veilleur-Analyste, Opérateur analyste SOC.
- **Equivalence en anglais :** SOC Analyst - N1.

MISSION ESSENTIELLE

L'analyste réponse aux incidents de sécurité SOC niveau 1 intervient au sein d'un SOC (Security Operation Center - Centre des Opérations de Sécurité). Ses missions reposent sur le triage des alertes ainsi que la réalisation d'une première qualification des alertes, en s'appuyant sur des fiches de tâches pour chaque typologie d'alertes. En cas de difficulté de traitement sur une alerte ou si cela sort de son périmètre, l'analyste N1 a la possibilité d'escalader l'alerte au niveau supérieur.

ACTIVITÉS ET TÂCHES

Anticipation

- Collecter les informations techniques d'un large ensemble de systèmes d'information interne (on-premise) et cloud (infrastructure, plate-forme, conteneurs, services), réaliser la recherche d'indicateurs de compromission.
- Trier les alertes en provenance du SIEM et des outils de détection afin de prioriser les alertes par ordre de criticité.
- Réaliser une première qualification et analyse sur les alertes.

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation

Formation Bac +3, dont spécialisation en cybersécurité.

Expériences précédentes

Exploitant solutions de sécurité.

Pré-requis techniques

Connaissance des concepts fondamonteaux cloud (terminologie).

COMPÉTENCES

Compétences coeur de métier

Gestion du SI

- Maîtriser le système d'information, l'urbanisation et l'architecture du SI.
- Utiliser les outils de supervision de la sécurité du SI.
- Développer des scripts en python et bash.

Traitement des logs

- Analyser les flux réseaux.
- Caractériser les traces d'attaques après incident.
- Mettre en place, analyser et corréler les journaux : utiliser les outils et les formats.

Gestion des vulnérabilités

- Evaluer les environnements et leurs configurations pour identifier les vulnérabilités.
- Réaliser des audits techniques de sécurité pour rechercher des vulnérabilités connues.

Compétences comportementales et transverses

- Agir avec rigueur et éthique.
- Etre capable de résister à la pression.
- Collaborer au sein d'une équipe.

TENDANCES ET FACTEURS D'ÉVOLUTION DU METIER

L'analyste réponse aux incidents de sécurité peut être spécialisé en tant qu'analyste système, analyste réseau, analyste de codes malveillants.

Evolution professionnelle

- Analyste N2.

ANALYSTE SOC POUR LE CLOUD - N2

- **Autres titres équivalents :** Analyste CyberSOC, Analyste détection d'incident, Veilleur-Analyste, Operateur analyste SOC
- **Equivalence en anglais :** SOC Analyst - N2

MISSION ESSENTIELLE

L'analyste réponse aux incidents de sécurité SOC niveau 2 intervient au sein d'un SOC (Security Operation Center - Centre de Sécurité des Opérations). Sa mission est centrée sur la détection d'activités malveillantes au sein du système d'information. Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Pour cela, il traite les alertes de sécurité issues des règles de corrélation d'évènements issus du SIEM ou d'alertes déjà qualifiées émanant d'outils de détection (EDR, sondes réseau, remédiation déterminer la nature d'une alerte, il est amené à procéder à des investigations pour comprendre et analyser le comportement détecté et apporter ou proposer des mesures de remédiation si le caractère malveillant est avéré.

ACTIVITÉS ET TÂCHES

Anticipation

- Réaliser une veille sur les nouvelles vulnérabilités, sur les nouvelles technologies et sur les méthodes des attaques relatives aux différents composants du système d'information interne (on-premise) et cloud (infrastructure, plateforme, conteneurs, services).
- Maintenir et développer des outils d'investigation.

Analyse des incidents

- Collecter les informations techniques d'un large ensemble de systèmes d'information interne (on-premise) et cloud (infrastructure, plate-forme, conteneurs, services), réaliser la recherche d'indicateurs de compromission.
- Analyser les relevés techniques réalisés afin d'identifier le mode opératoire et l'objectif de l'attaquant et de qualifier l'étendue de la compromission.
- Rédiger les rapports d'investigation.
- Mettre en oeuvre les outils SIEM, sondes réseaux (NIDS NIPS).
- Définir des règles de détection.

< ANALYSE SOC POUR LE CLOUD - N2 >

Gestion de l'environnement cloud

- Utiliser des consoles d'administration des fournisseurs cloud.
- Exploiter des services de sécurité des principaux fournisseurs cloud (par exemple Guardduty pour AWS...).
- Exploiter le CSPM.

Conseil

- Préconiser des mesures de contournement et de remédiation de l'incident (assainissement et durcissement).
- Préconiser des mesures d'amélioration des capacités d'analyse (extraction des indicateurs de compromission).
- Préparer des rapports.

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation

Formation Bac +5, dont spécialisation en cybersécurité.

Expériences précédentes

- 1 à 3 ans en tant qu'architecte cloud.
- Analyste N1.

Pré-requis techniques

- Connaissances protocoles réseaux.
- Connaissance sur les principaux vecteurs d'attaques sur les environnements cloud.
- Veille sur les menaces cyber.

COMPÉTENCES

Fondations

- Compétences coeur de métier des Analystes SOC N1.
- Compétences comportementales et transverses des Analystes SOC N1.

Compétences coeur de métier

Gestion du SI

- Automatiser les outils SSI.

Traitement des logs

- Mettre en place, analyser et corréler les journaux d'évènements : prendre en compte la spécificité du périmètre cloud (coûts et volumétrie de la centralisation des journaux d'événement dans un SIEM).
- Développer des règles de détection selon des scénarios d'attaque définis.

< ANALYSE SOC POUR LE CLOUD - N2 >

Gestion des vulnérabilités

- Caractériser les vulnérabilités des environnements et des configurations et y remédier

Techniques d'attaques

- Caractériser les techniques d'attaques et d'intrusions, et y remédier

Compétences comportementales et transverses

- Être capable de restituer et de vulgariser pour des publics non techniques
- Rédiger des rapports externes et internes adaptés à différents niveaux d'interlocuteurs

TENDANCES ET FACTEURS D'ÉVOLUTION DU METIER

- L'analyste réponse aux incidents de sécurité peut être spécialisé en tant qu'analyste système, analyste réseau, analyste de codes malveillants.
- Nouveaux outils : XDS, SOAR, BAS.
- Évolution professionnelle : Analyste N3 / Analyste CSIRT.

ANALYSTE SOC POUR LE CLOUD - N3

- **Autres titres équivalents:** Analyste CyberSOC, Analyste détection d'incident, Veilleur-Analyste, Operateur analyste SOC.
- **Equivalence en anglais :** SOC Analyst - N3.

MISSION ESSENTIELLE

L'analyste réponse aux incidents de sécurité SOC niveau 3 intervient au sein d'un SOC (Security Operation Center - Centre des Opérations de Sécurité) en appui aux niveaux 1 et 2 sur des incidents nouveaux et/ou complexes. En cas de soupçons sur une activité malveillante ou d'attaque au sein du système d'information, l'analyste réponse aux incidents de sécurité niveau 3 analyse les symptômes et réalise les analyses techniques sur le système d'information.

Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit et met en œuvre des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués. En complément, il est en charge de formaliser et de restituer des comptes-rendus au management.

ACTIVITÉS ET TÂCHES

Anticipation

- Réaliser une veille sur les nouvelles vulnérabilités, sur les nouvelles technologies et sur les méthodes des attaques relatives aux différents composants du système d'information interne (on-premise) et cloud (infrastructure, plateforme, conteneurs, services).
- Alimenter les bases de renseignement sur les menaces (threat intelligence).
- Maintenir et développer des outils d'investigation.
- Autoévaluer et améliorer en continu les mesures de sécurité du SI.

Analyse des incidents

- Collecter les informations techniques d'un large ensemble de systèmes d'information interne (on-premise) et cloud (infrastructure, plateforme, conteneurs, services), réaliser la recherche d'indicateurs de compromission.
- Analyser les relevés techniques réalisés afin d'identifier le mode opératoire et l'objectif de l'attaquant et de qualifier l'étendue de la compromission.
- Rédiger les rapports d'investigation.
- Piloter les dispositifs de gestion de crise (si cellule activée).
- Appliquer le processus ITIL de gestion d'un incident.

< ANALYSE SOC POUR LE CLOUD - N3 >

Gestion de l'environnement cloud

- Utiliser les consoles d'administration et les services de sécurité des fournisseurs cloud.
- Utiliser les solutions CSPM (revue des configurations) et CWPP (gestion des vulnérabiltés).
- Maitriser les principaux vecteurs d'attaques sur les environnements cloud.
- Point de contact avec les fournisseurs cloud.

Conseil

- Préconiser et implémenter des mesures de contournement et de remédiation d'un incident (assainissement et durcissement).
- Préconiser et implémenter des mesures d'amélioration des capacités d'analyses (extraction des indicateurs de-compromission).
- Préparer des rapports.
- Optimiser les processus de réponse à incident.

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation

Formation Bac +5, dont spécialisation en cybersécurité.

Experiences précédentes

- Architecte système ou réseau.
- Analyste N2.

COMPÉTENCES

Fondations

- Compétences coeur de métier des Analystes SOC N1 et N2.
- Compétences comportementales et transverses des Analystes SOC N1 et N2.

Compétences coeur de métier

<u>Gestion du SI</u>

- S'adapter aux évolutions apportées par les fournisseurs cloud.
- Déployer des nouveaux outils pour la supervision de la sécurité du SI.

<u>Gestion des vulnérabilités</u>

- Évaluer les risques liés à l'exploitation des vulnérabilités des environnements et des configurations, et les exploiter.
- Réaliser des audits techniques de sécurité et des tests d'intrusion pour rechercher de nouvelles vulnérabilités.

Techniques d'attaques

- Expérimenter de nouvelles techniques d'attaques et d'intrusions.
- Réaliser une rétro-ingénieurie pour rechercher des nouveaux mécanismes d'attaques.

Analyse après incident

- Réaliser une investigation après incident.
- Maitriser les outils d'analyse post-mortem (forensic).
- Maitriser les procédures légales d'analyses post-mortem (forensic).

Compétences comportementales et transverses

- Être force de proposition.
- Avoir le sens relationnel (relations inter et intra équipe).

TENDANCES ET FACTEURS D'ÉVOLUTION DU METIER

L'analyste réponse aux incidents de sécurité niveau 3 peut être spécialisé en tant qu'analyste ou architeche système et réseau, analyste de codes malveillants, ou évoluer vers une fonction de manager d'une équipe d'analystes réponse aux incidents de sécurité.

Son activité peut également être facilitée avec l'intégration de l'IA permettant une automatisation de certaines tâches courantes (corrélation des événements, exécution de scripts).

RESPONSABLE DE SOC

- **Autres titres équivalents :** Responsable du centre opérationnel de sécurité, responsable du centre de Cyberdéfense, responsable du service de détection des incidents de sécurité.
- **Equivalence en anglais :** Security Operation Center manager, Operational security manager.

MISSION ESSENTIELLE

Le responsable du SOC (Security Operation Center) planifie et organise les opérations quotidiennes du SOC afin d'évaluer le niveau de vulnérabilité et de détecter des activités suspectes ou malveillantes. Il met en place le service de détection des incidents de sécurité. Il valide la bonne exécution des processus de supervision et de gestion des évènements de sécurité et assure un reporting complet et précis des indicateurs clés. Il définit et pilote le plan d'amélioration des services du SOC.

ACTIVITÉS ET TÂCHES

Pilotage des opérations

- Planifier et organiser les opérations quotidiennes du SOC.
- Assurer un appui opérationnel à la gestion de crise de sécurité en cas d'incidents de sécurité majeurs.
- Assurer les relations avec les équipes de réponse à incidents CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team), notamment en situation de crise pour coordonner les différentes équipes de sécurité opérationnelle.

Stratégie de prévention et de détection

- Définir la stratégie du SOC, assurer la cohérence technique, prendre en compte les exigences réglementaires.
- Définir et mettre en œuvre les outils du SOC pour la collecte des évènements, l'accès aux plateformes de sécurité, la recherche d'évènements suspects, la gestion des alertes, les workflows de suivi d'incidents de sécurité.
- Alimenter la stratégie de détection à partir d'une vision globale de la nature et du niveau de vulnérabilité du SI.
- Définir les cas d'usages de détection et les intégrer dans les outils de détection.
- Définir et mettre en place les processus de notification et d'escalade.
- Évaluer et valider l'efficacité des outils déployés dans le SOC et conduire les plans d'action correctifs nécessaires le cas échéant.
- Créer des synergies avec les autres équipes de sécurité en partageant les informations sur les menaces identifiées (en interne comme en externe).

< RESPONSABLE DE SOC >

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation

Formation Bac +5, dont spécialisation en cybersécurité.

Expériences précédentes

5 ans minimum au sein d'un SOC.

COMPÉTENCES

Compétences coeur de métier

- Sécurité des systèmes d'exploitation.
- Sécurité des réseaux et protocoles.
- Cyberdéfense : connaissance en gestion de crise.
- Cyberdéfense : pratique de l'analyse de journaux (systèmes ou applicatifs).
- Cyberdéfense : pratique de l'analyse de flux réseaux.
- Cyberdéfense : connaissance d'outils et de méthodes de corrélation de journaux d'évènements (SIEM).
- Cyberdéfense : connaissance des solutions de supervision sécurité.
- Cyberdéfense : connaissance des techniques d'attaques et d'intrusions.
- Cyberdéfense : connaissance des vulnérabilités des environnements.
- Scripting.
- Superviser la sécurité du SI.
- Construire la stratégie cybersécurité de l'organisation.
- Réaliser une rétro-ingénierie.
- Analyser le SI après incident.

Compétences comportementales et transverses

- Management d'équipe.
- Capacité à travailler en transverse dans l'organisation.
- Capacité à travailler en équipe.
- Capacité à résister à la pression.
- Intégrer les enjeux métiers.
- Réaliser une veille en cybersécurité.
- Communiquer par écrit et à l'oral en interne et en externe en français et en langues étrangères.
- Agir avec rigueur et éthique.

< RESPONSABLE DE SOC >

TENDANCES ET FACTEURS D'ÉVOLUTION DU METIER

Le responsable du SOC doit acquérir une bonne compréhension des besoins de supervision pour les activités métiers critiques afin d'assurer le développement des cas d'usages applicatifs et spécifiques (e.g. surveillance des SI industriels). De plus, le responsable du SOC doit gérer de plus en plus d'incidents de sécurité et doit par conséquent développer une bonne compréhension des menaces qui pèsent sur son périmètre.

Cette compréhension fine des menaces lui permet de concevoir au mieux les actions de prévention et de détection et d'être efficace dans la réponse apportée. Pour suivre l'évolution des tendances, il pourra être amené à développer des compétences en machine learning et en threat intelligence afin de renforcer les capacités de détection. Sa connaissance des enjeux techniques et métiers font de lui un interlocuteur clé pour les actions d'avant-vente.

ADMINISTRATEUR TECHNIQUE DU SOC

• **Equivalence en anglais :** SOC Administrator

MISSION ESSENTIELLE

L'administrateur des plateformes de SIEM et autres outils de cybersécurité œuvre pour assurer leur fonctionnement nominal et en toute sécurité. Cela s'entend par la qualification préalable des outils et des plateformes, l'adaptation de leur implémentation et paramétrage et par leur optimisation.
L'administrateur de solutions de sécurité installe, met en production, administre et exploite des solutions de sécurité (antivirus, sondes, firewalls, IAM, etc.). Il participe au bon fonctionnement des solutions de sécurité en garantissant le maintien en conditions opérationnelles et de sécurité.

ACTIVITÉS ET TÂCHES

Qualification

- S'assurer de l'adéquation des solutions de sécurité aux besoins fonctionnels exprimés.
- S'assurer de l'adéquation des solutions de sécurité aux besoins de sécurité exprimés.
- S'assurer du bon niveau d'information reçu.
- S'assurer de disposer du niveau de support adéquat aux enjeux.
- S'assurer des compétences internes pour une utilisation pertinente.

Administration

- S'assurer du fonctionnement optimal des solutions de sécurité dont il a la charge.
- Contribuer au paramétrage des solutions de sécurité, gérer les changements.
- Configurer les solutions en conformité avec les normes et standards définis par les experts du domaine, effectuer des revues régulières des règles et paramétrages mis en place.
- Mettre en place la collecte des logs et des alertes issues des solutions vers un service de détection d'incidents.
- Assurer un suivi des actions et une documentation des processus.
- Définir une matrice de rôles et de droits.
- Attribuer les privilèges en fonction des profils disponibles.

Exploitation

- Valider l'installation des outils dans l'environnement de production.
- Gérer les droits d'accès aux solutions en fonction des profils.

- Traiter les incidents ou anomalies ainsi que les exceptions.
- Veiller au fonctionnement de la remontée des logs et des alertes.

Maintenance

- Maintenir et faire évoluer les solutions de sécurité de son périmètre, dans un objectif de qualité, de productivité et de sécurité globale.
- Assurer le suivi et la remédiation des vulnérabilités identifiées.

Communication

- Contribuer à la sensibilisation et à la formation des utilisateurs aux solutions de sécurité.

FORMATION / EXPÉRIENCE PROFESSIONNELLE

Formation

Formation Bac +3, dont spécialisation en informatique.

Expériences précédentes

Expérience souhaitée en réseau, en système, en virtualisation.
Métier accessible à partir d'une expérience préalable en environnement de production, d'exploitation ou de support.

COMPÉTENCES

Compétences coeur de métier

- Maîtrise du système d'information, de l'urbanisation et de l'architecture du SI.
- Maîtrise des processus de production.
- Sécurité des systèmes d'exploitation.
- Sécurité des réseaux et protocoles.
- Configuration des outils liés à la sécurité.
- Choisir et implémenter les protocoles sécurisés.
- Sécuriser les réseaux.
- Appliquer les normes & standards de la SSI.

Compétences comportementales et transverses

- Rigueur.
- Curiosité.
- Patience.
- Travail sous contraintes.
- Travail d'équipe.
- Capacité à définir des procédures.
- Intégrer les enjeux métiers.
- Automatiser les outils SSI.
- Analyser et synthétiser.
- Prioriser ses actions selon les contraintes.

TENDANCES ET FACTEURS D'ÉVOLUTION DU METIER

Évolution professionnelle :

- Analyste SOC.
- Architecte.

< Studio des Communs >

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX

CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT DANS LE CADRE DU PROGRAMME D'INVESTISSEMENTS D'AVENIR