< RECOMMANDATIONS DE FORMATION DES ANALYSTES CLOUD >

Référentiel de certification

CAMPUS CYBER 2025

< SOMMAIRE >

1. 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 métiers 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 ».

1.1 CONTRIBUTION

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

1.2 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'activités malveillantes au sein du système d'information.
- **Niveau N3 de SOC** : En appui aux niveaux 1 et 2 sur des incidents nouveaux et/ou complexes.

1.3 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.

< REFÉRENTIEL DE CERTIFICATION POUR ANALYSTES SOC >

Type de compétences	Compétences	Typologie	Priorité	N1	N2	N3
Coeur de métier	Maitriser le système d'information, l'urbanisation et l'architecture du Système d'Information	A. Gestion du SI	1	X		
Coeur de métier	Utiliser les outils de supervision de la sécurité du SI	A. Gestion du SI	2	X		
Coeur de métier	Développer des scripts en python et bash	A. Gestion du SI	3	X		
Coeur de métier	Analyser les flux réseaux	B. Traitement des logs	1	X		
Coeur de métier	Caractériser les traces d'attaques après incident	B. Traitement des logs	2	X		
Coeur de métier	Mettre en place, analyser et corréler les journaux : utiliser les outils et les formats	B. Traitement des logs	3	X		
Coeur de métier	Evaluer les environnements et leurs configurations pour identifier les vulnérabilités	C. Gestion des vulnérabilités	1	X		
Coeur de métier	Réaliser des audits techniques de sécurité pour rechercher des vulnérabilités connues	C. Gestion des vulnérabilités	2	X		
Coeur de métier	Etre capable d'identifier les techniques d'attaques et d'intrusions	D. Techniques d'attaques	1	X		
Coeur de métier	Réaliser une rétro-ingénierie : recherche des mécanismes d'attaques connus	D. Techniques d'attaques	2	X		
Coeur de métier	Agir avec rigueur et éthique	F. Savoir être	1	X		
Comportementales et transverses	Etre capable de résister à la pression	F. Savoir être	1	X		
Comportementales et transverses	Collaborer au sein d'une équipe	F. Savoir être	1	X		
Comportementales et transverses	Automatiser les outils SSI	A. Gestion du SI	1		X	
Coeur de métier	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'évènements dans un SIEM)	B. Traitement des logs	1		X	
Coeur de métier	Développer des règles de détection selon des scénarios d'attaques définis	B. Traitement des logs	2		X	
Coeur de métier	Mettre en place, analyser et corréler les journaux d'événements : prendre en compte la spécificité du périmètre cloud (coûts et volumétrie de la centralisation des journaux d'un événement SIEM)	B. Traitement des logs	1		X	

< REFÉRENTIEL DE CERTIFICATION POUR ANALYSTES SOC >

Type de compétences	Compétences	Typologie	Priorité	N1	N2	N3
Coeur de métier	Caractériser les vulnérabilités des environnements et des configurations et y remédier	C. Gestion des vulnérabilités	1		X	
Coeur de métier	Caractériser les vulnérabilités des environnements et des configurations et y remédier	D. Techniques d'attaques	1		X	
Comportementales et transverses	Être capable de restituer et de vulgariser pour des publics non techniques	F. Savoir être	1		X	
Comportementales et transverses	Rédiger des rapports externes et internes adaptés à différents niveaux d'interlocuteurs	F. Savoir être	1		X	
Coeur de métier	S'adopter aux évolutions apportées par les fournisseurs cloud	A. Gestion du SI	1			X
Coeur de métier	Déployer de nouveaux outils pour la supervison de la sécurité du SI	A. Gestion du SI	2			X
Coeur de métier	Evaluer les risques liés à l'exploitation des vulnérabilités des environnements et des configurations, et les exploiter	C. Gestion des vulnérabilités	1			X
Coeur de métier	Réaliser des audits techniques de sécurité et des tests d'intrusion pour rechercher de nouvelles vulnérabilités	C. Gestion des vulnérabilités	2			X
Coeur de métier	Expérimenter de nouvelles techniques d'attaques et d'intrusions	D. Techniques d'attaques	1			X
Coeur de métier	Réaliser une rétro-ingénieurie pour rechercher des nouveaux mécanismes d'attaques	D. Techniques d'attaques	2			X
Coeur de métier	Réaliser une investigation après incident	E. Analyse après incident	1			X
Coeur de métier	Maitriser les outils d'analyses post-mortem (forensic)	E. Analyse après incident	2			X
Coeur de métier	Maitriser les procédures légales d'analyses post-mortem (forensic)	E. Analyse après incident	3			X
Comportementales et transverses	Être force de proposition	F. Savoir être	1			X
Comportementales et transverses	Faire preuve de relationnel dans les relations inter et intra-équipes	F. Savoir être	1			X

< EXERCICES ENCADRÉS >

Type de compétences	Compétences
Analyste N1	• Analyse de trames réseau • Analyse manuelle de logs • Interprétation des principaux messages d'erreur de différentes sources systèmes, web, virtualisation • Mise en place d'une architecture virtuelle
Analyste N2	• Familiarisation avec les consoles d'administration des fournisseurs cloud et de leurs services de sécurité principaux • Utilisation d'un CSPM • Définition de règles de détection autour du cloud
Analyste N3	• Etude de cas sécurité Cloud • Threat hunting en environnement cloud • Réponse et réaction sur incident cloud
Administrateur de l'environnement technique du SOC	• Gestion des infra cloud • Gestion fine des droits (RBAC, etc.) • Politique de mises à jour • Dimensionnement des ressources techniques
Responsable de SOC	• Optimisation de la qualification des alertes et réduction des faux positifs pour la prise de décision • Cas d'usages de détection • Conception technique d'architectures de SOC • Définition et mise en place d'un schéma d'escalade et de gestion de crise • Conformité et contraintes réglementaires pour l'usage des outils (ex : pentest) • Gestion des conflits interpersonnels

< 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