< RECOMMANDATIONS DE FORMATION DES ANALYSTES CLOUD >

Cadrage d’exercices

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 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.

1.1 CONTRIBUTIONS

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

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.

2. CADRAGE DES PRATIQUES ENCADRÉES PAR MÉTIERS

OBJECTIFS

L'objectif de ce document est de lister les pratiques encadrées recommandées pour la formation des professionnels œuvrant en Centre des Opérations de Sécurité (Security Operation Center – SOC) pour les environnements Cloud.

PRATIQUES ENCADRÉES

Analyste SOC pour le Cloud - 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 SOC pour le Cloud - 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 SOC pour le Cloud - N3

- Étude de cas sécurité Cloud.
- Threat hunting en environnement cloud.
- Réponse et réaction sur incident cloud.

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'architecture de SOC.
- Définition et mise en place d'un schéma d'escalade et de gestion de crise.
- Gestion des conflits interpersonnels.
- Conformité et contraintes réglementaires pour l'usage des outils (ex: pentest).

<CADRAGE DES PRATIQUES ENCADRÉES PAR MÉTIERS>

Administrateur technique de SOC

- Gestion des infrastructures Cloud.
- Tests et recettes.
- Gestion fine des droits (RBAC, etc.).
- Politique de mises à jour.
- Dimensionnement des ressources techniques.

3.CADRAGE D'EXERCICE D'INTRUSION

PÉRIMÈTRE

L' objectif de ce document est de lister les pratiques encadrées recommandées pour la formation des analystes Cloud. Ce cadrage d'un exercice d'intrusion peut être réalisé aux différents niveaux d'analyse :

- N1 : Identification et qualification de scénarios connus.
- N2 : Analyse en volume et de bout en bout de scénarios connus et qualifiés.
- N3 : Analyse d'évènements nouveaux et/ou complexes.
- Transverse : exercice d'équipe avec l'ensemble des rôles.

MISSION ESSENTIELLE

L' exercice d'intrusion consiste en une simulation d'intrusion du SI opérée par une équipe dite « Red team » chargée de reprendre les techniques employées par les cyberattaquants et compromettre l'environnement, et une équipe dite « Blue team » chargée de neutraliser l'intrusion et sécuriser l'environnement. Les exercices suivent généralement le cadre MITRE ATT&CK qui regroupe les méthodes et les techniques des cyberattaquants.

COMPOSITION

Red team

- Experts en cybersécurité offensive.
- Pentesters.

Blue team

- Experts en cybersécurité défensive.
- Anaystes SOC.

OBJECTIFS

- Évaluer la maturité de l'entreprise en matière de prévention, de détection et de correction d'une intrusion.
- Identifier les points de vulnérabilité (techniques, fonctionnels, organisationnels).
- Optimiser les processus de réponse à incident et les capacités d'analyse.

<CADRAGE DES PRATIQUES ENCADRÉES PAR MÉTIERS>

DÉROULÉ

1. Cadrage de l'exercice avec la Red team sans en informer la Blue team.
- Définition des objectifs.
- Définition du périmètre.
- Définition de la durée (habituellement plusieurs semaines).

2. Réalisation de l'exercice par la Red team.
- Reconnaissance de l'environnement et collecte d'informations afin d'identifier les vulnérabilités.
- Exploitation des vulnérabilités identifiées.
- Prise de contrôle des systèmes et mouvement latéral jusqu'à atteindre la cible.
- Extraction des données.

3. Détection et prévention des attaques par la Blue team.
- Analyse des journaux d'événements.
- Mise en œuvre de solutions pour contrecarrer la Red team .

4. Fin de l'exercice.
- Conditions : Red team contrecarrée ou temps imparti dépassé.

5. Rapport de fin d'exercice.
- Chemins d'attaques exploités.
- Chemins d'attaques identifiés.
- Succès et échecs.
- Recommandations pour renforcer le niveau de sécurité des systèmes.
- Recommandations pour la réalisation de nouveaux exercices.

MOYENS

Red team

Collecte d'informations
- Social Engineering.
- Phishing.
- Analyse des paquets réseaux.
- Inventaire des systèmes déployés (technologies, versions, etc.).

Identification des vulnérabilités
- Open Source Intelligence (OSINT) : référentiel public des vulnérabilités sur les systèmes.

Exploitation des vulnérabilités

- Brute force des mots de passe.
- Mauvaises pratiques de configuration des systèmes.
- Failles liées aux versions des systèmes déployés.
- Failles Zero Day.

Blue team

Analyse des journaux d'événements

- Protection systèmes : Endpoint Detection and Response (EDR).
- Protection réseaux : Firewall, Network Access Control (NAC), Intrusion Detection and Prvention System (IDPS).

Contre-attaque

- Mise à jour des systèmes.
- Correction des mauvaises pratiques de configuration des systèmes.
- Isolation des systèmes corrompus.

RÉCAPITULATIF DES COMPÉTENCES CLÉS

On liste ici les compétences travaillées lors d'un exercice d'intrusion de type « transverse ».

Red team

- Mettre en œuvre les techniques d'attaques et d'intrusions.
- Exploiter les vulnérabilités des environnements.
- Développer des scripts.
- Réaliser de la rétro-ingénierie.

Blue team

Compétences coeur de métier issues de la Fiche métier « Analystes SOC ».

- Maîtriser le système d'information, l'urbanisation et l'architecture du SI.
- Maîtriser les outils d'analyse et réaliser la corrélation des journaux.
- Pratiquer l'analyse de flux réseaux.
- Analyser le SI après incident.

Compétences comportementales issues de la Fiche métier « Analystes SOC ».

- Travail en équipe.
- Capacité à résister à la pression.
- Sens éthique.
- Sens relationnel.
- Être force de proposition.

< 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