SIMPLON.CO

55 rue de Vincennes
93100 Montreuil

Référentiel de certification et évaluation

Analyser les incidents de sécurité détectés

Référentiels d'activités et de compétences et d'évaluation

Prérequis : Justifier d'une expérience professionnelle d'un an minimum en tant que technicien systèmes et réseaux ou assimilé.

REFERENTIEL D'ACTIVITES *Décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *Identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *Définit les critères et les modalités d'évaluation des acquis*	
		MODALITES D'EVALUATION	**CRITÈRES D'ÉVALUATION**
A1. Élaboration de l'analyse des événements de sécurité - Définition des règles de détection des incidents de sécurité redoutés - Documentation des règles de détection selon les recommandations de l'ANSSI (identifiant, auteur, date…)	C1. Analyser les événements collectés afin de détecter des incidents de sécurité à partir des règles préalablement définies	**E1 : Projet professionnel** À partir d'une base de données d'événements issus d'un cas d'entreprise réelle ou fictive, le/la candidat(e) doit : - réaliser une analyse des événements collectés et produire une liste de règles permettant d'identifier les incidents redoutés.	- Les règles permettant le tri et la détection des incidents sont programmées, - une analyse des événements collectés est présentée. Elle est cohérente avec les règles de détection établies et avec les recommandations de l'ANSSI. **Indicateur(s) :** - La liste des règles

- Implémentation de l'ensemble des règles de détection dans les outils techniques d'analyse - Appréciation de la véracité (vrai/faux positif, incident avéré ou non) des incidents - Appréciation du niveau de gravité (impacts fonctionnels, informationnels, etc.) des incidents			d'identification des incidents est complète
	C2. Qualifier un incident de sécurité détecté sur la base d'une analyse des impacts sur l'organisation de manière à apporter une réponse adaptée	**E1 : Projet professionnel** Le/la candidat(e) doit : - expliciter sa méthodologie de qualification des incidents.	- Les incidents dans la base de données des événements de sécurité sont qualifiés, - l'urgence de traitement du risque est déterminée de façon réaliste. **Indicateur(s) :** - le niveau de criticité et de sévérité est évalué, - la portée de l'incident est identifiée.
A2. Analyse et gestion des incidents de sécurité - Réalisations de recherches en sources ouvertes à partir d'informations collectées ou issues des analyses (empreintes cryptographiques, noms de fichiers ou de codes malveillants, chaînes de caractères contenues dans des codes malveillants, noms de domaines et adresses IP, etc.)	C3. Identifier les tactiques et techniques d'attaques ainsi que les objectifs de l'attaquant de manière à proposer des préconisations adaptées au mode opératoire utilisé	**E1 : Projet professionnel** Le/la candidat(e) doit : - identifier le mode opératoire d'un attaquant à partir de recherches dans la base de données fournies, - exploiter les ressources externes disponibles pour caractériser l'attaque et les objectifs.	- Le mode opératoire de l'attaquant est identifié, - la réponse est justifiée correctement en explicitant les sources exploitées afin de parvenir à cette conclusion. **Indicateur(s) :** - des incidents similaires au sein d'autres organisations sont identifiés.

- Identification du mode opératoire et des objectifs de l'attaquant - Préconisation de mesures de remédiation - Identification des ressources humaines et matérielles nécessaires à la résolution de l'incident - Création d'un ticket pour chaque incident détecté (date, classification, gravité…) - Mise en place de notifications en cohérence avec la stratégie de communication des incidents - Rédaction d'un compte rendu d'incident	C4. Rédiger un rapport d'alerte sous la forme d'un compte rendu d'incident à destination du commanditaire afin de préconiser des mesures de remédiation en vue du traitement de l'incident de sécurité	**E1 : Projet professionnel** Le/la candidat(e) doit : - rédiger un compte rendu d'incident à destination d'un commanditaire en respectant les standards de rédaction	Le/la candidat(e) rédige un compte rendu comprenant : - une description complète de l'incident - la règle de détection permettant d'assurer la véracité de l'incident - un audit réaliste de la gravité de l'incident - les conséquences de l'incident - une liste de préconisations cohérente avec les causes de l'incident - l'identification des ressources (humaines et matérielles) nécessaires pour un retour à la normal.
A3. Élaboration et mise en oeuvre d'une stratégie de veille technologique pour optimiser la gestion des risques - Sélection des sources d'information pertinentes	C5. Concevoir un système de veille technologique permettant de collecter, classifier, analyser et diffuser l'information liés à la cybersécurité aux différents acteurs de l'organisation/du commanditaire afin d'améliorer la sécurité du SI	**E1 : Projet professionnel** Le/la candidat(e) doit : - réaliser un état de l'art en explicitant le choix de leur sources et en proposer une analyse.	- Un état de l'art des méthodologies et outils existants est dressé sur la thématique donnée. - Les sources d'information sont identifiées et leur fiabilité évaluée.

- Rédaction d'un état de l'art en français et anglais - Collecte des données/informations liées à la cybersécurité en général et aux nouvelles vulnérabilités découvertes en particulier - Analyse des informations collectées	du commanditaire		- Une analyse pertinente de cet état de l'art est exposée. - Une conclusion technique en fonction de cet état de l'art et de l'analyse est proposée. **Indicateur(s) :** - les sources, canaux et fréquences sont identifiées dans la méthodologie de collecte

55 rue de Vincennes
93100 Montreuil

Modalités d'évaluations :

EVALUATIONS	DÉROULEMENT (Contenu, durée, support autorisé, jury, nombre de page attendu, etc.)
E1 : Projet professionnel	Contenu : À partir d'une base de données d'événements issus d'un cas d'entreprise réelle ou fictive, le/la candidat(e) doit élaborer une stratégie de détection d'incidents. Pour se faire, il/elle doit : - Réaliser une analyse des événements collectés, - Produire une liste de règles permettant d'identifier les incidents redoutés, - Expliciter sa méthodologie de qualification des incidents, - Identifier le mode opératoire d'un attaquant à partir de recherches dans la base de données fournies. Il/elle exploite les ressources externes disponibles pour caractériser l'attaque et les objectifs, - Rédiger un compte rendu d'incident à destination d'un commanditaire en respectant les standards de rédaction, - Réaliser un état de l'art en explicitant le choix de leur sources et en proposer une analyse. Correction : Un jury composé de 3 personnes, *dont au moins un professionnel.* Rendus attendus : ● A l'écrit : Un rapport de 15 à 20 pages comprenant : - Une introduction, - Une première partie sur la compréhension de la mécanique des incidents redoutés et sur la méthodologie de détection, - Une seconde partie sur la mise en oeuvre des règles, - Une troisième partie sur le bilan de projet et les améliorations possibles, - Une conclusion ● A l'oral : Une présentation orale de 40 mn découpée en 2 parties :

	- Présentation du rapport (20mn), - Echange avec le jury (20mn).