SIMPLON.CO

55 rue de Vincennes
93100 Montreuil

Référentiel de certification et évaluation

Surveiller un système d'information sur des critères de sécurité informatique

Référentiels d'activités , 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. Analyse des métiers du commanditaire et évaluation globale de la vulnérabilité de son système d'information - Sélection d'une méthodologie d'évaluation du risque	C1. Evaluer la criticité des risques liés aux métiers du commanditaire sur le système d'information en exploitant des méthodologies d'identification et de classification des risques.	**E1 : Projet professionnel** Le/la candidat(e) doit : - cartographier les métiers existants au sein de l'organisation, - dresser l'ensemble des risques liés à un métier particulier,	- La cartographie proposée est claire, - le tableau des risques liés à chacun des métiers s'appuie sur la documentation disponible, les

- Identification des risques liés aux métiers du commanditaire impactant le système d'information - Élaboration de la liste des incidents redoutés et des impacts associés - Élaboration d'une échelle de gravité des incidents redoutés - Analyse de l'architecture réseau - Analyse des protocoles de sécurité en place - Élaboration de la liste des incidents redoutés et des impacts associés - Élaboration d'une échelle de gravité des incidents redoutés		résultant de la spécificité des interactions du collaborateur avec le système d'information, - à partir de cette analyse, évaluer et classifier les risques liés à ces interactions.	connaissances du/de la candidat(e) et un état de l'art des incidents opérationnels découlant de sa veille technologique, - la classification des risques redoutés est cohérente. **indicateur(s) :** - L'ensemble des risques sont présents - À chaque risque est associé un degré de criticité - L'ensemble des métiers par secteur présents dans l'organisation sont identifiés.
	C2. Analyser l'architecture* d'un système d'information et des protocoles de sécurité du commanditaire à l'aide de la documentation existante afin d'évaluer les risques de sécurité potentiels et leurs impacts éventuels	**E1 : Projet professionnel** Le/la candidat(e) doit : - réaliser une étude du système d'information de l'entreprise et en proposer une analyse complète, - procéder à une première identification des incidents de sécurité redoutés.	- L'analyse du système d'information est réalisé à partir de la documentation existante et pertinente. **indicateur(s) :** - L'analyse comprend l'architecture, les protocoles de sécurité, les incidents redoutés et les impacts associés.

			- Pour chaque incident redouté, est indiqué l'impact et le degré de gravité - L'analyse
A2. Élaboration et mise en oeuvre d'une stratégie de collecte d'événements en provenance du système d'information du commanditaire - Sélection des sources de collecte de données, des collecteurs* et des évènements à collecter - Identification des règles de filtre - Élaboration des méthodes de collecte (protocoles, applications, propriétés de sécurité, etc.) et des fréquences de collecte - Définition des règles de stockage des événements collectés : durée, quantité, … dans le respect des lois/réglementations	C3. Elaborer une stratégie de collecte d'évènement provenant d'un système d'information comprenant la collecte, le stockage, les règles de filtres et l'exploitation des données dans le respect des lois et réglementations en vigueur	**E1 : Projet professionnel** Le/la candidat(e) doit : - présenter une stratégie de collecte des événements en détaillant sa méthodologie.	- La stratégie de collecte d'événements est cohérente avec les enjeux du commanditaire. **Indicateurs :** - Les règles de filtre permettent de collecter les événements susceptibles d'indiquer un incident de sécurité redouté. La fréquence planifiée de la collecte de données est faite de manière optimale, et il/elle sélectionne les méthodes adaptées.
	C4. Programmer les règles de filtre du collecteur permettant la collecte des événements à surveiller de manière à alimenter l'application de détection des incidents	**E2 : Mise en situation professionnelle** Sous la forme d'une mise en situation professionnelle, le/la candidat(e) doit : - programmer des règles imposées de collecte et de filtre des événements.	- Les règles de collecte et de filtre sont fonctionnelles et respecte la demande imposée. **Indicateur :** - Les règles ont permis la détection d'incidents.

- Installation et configuration de sondes dédiées - Programmation de la collecte des événements en provenance des équipements réseau identifiés - Stockage des événements collectés - Détection d'incidents			
A3. Élaboration et mise en oeuvre d'une stratégie de veille technologique pour renforcer la gestion des risques - Sélection des sources d'information pertinentes - 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	C.5 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 du commanditaire	**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, - les sources d'information sont identifiées et leur fiabilité évaluée, - une méthodologie de collecte de l'information claire est mise en place (sources, canaux, fréquence…), - une analyse pertinente de cet état de l'art est proposée. **indicateur(s) :** - L'analyse a permis d'enrichir la surveillance du système d'information du

- Analyse des informations collectées			commanditaire sur des critères de sécurité

Glossaire :

- **Architecture** : Organisation d'équipements de transmission, de logiciels, de protocoles de communication et d'infrastructure filaire ou radioélectrique permettant la transmission des données entre les différents composants.
- **Collecteur ou agent de collecte** : Application permettant de récolter les événements en provenance des différents équipements réseau sous forme de journaux (logs).
- **SIEM** : Application qui permet de gérer et de corréler les logs.

SIMPLON.CO

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'un cas d'entreprise réelle ou fictive, le/la candidat(e) doit produire une liste d'incidents redoutés et développer une stratégie de collecte d'événements correspondante. Pour se faire, il/elle doit : - Réaliser une analyse écrite des métiers de l'entreprise ainsi que de son système d'information en expliquant leurs caractéristiques principales, - Produire la liste des incidents redoutés, - Rédiger une stratégie de collecte d'événements, - Établir la liste des équipements à interroger, - Expliciter sa méthodologie de collecte (protocoles, applications, propriétés de sécurité, fréquence de collecte etc.), - Programmer la collecte des événements en provenance des équipements identifiés, - Réaliser un état de l'art en explicitant le choix de ses 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 des métiers du client et de son système d'information, un état de l'art des incidents redoutés, - Une seconde partie sur la stratégie de collecte, - 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).
E2 : mise en situation professionnelle	Contenu : Sous la forme d'une mise en situation professionnelle, le/la candidat(e) doit programmer des règles imposées de collecte des événements. Correction : Un jury composé de 3 personnes, *dont au moins un professionnel.* Rendus attendus : - Programmation des règles dans le SIEM* (Security Information and Event Management) - Un compte-rendu oral (5 à 10 mn) des résultats obtenus