

Cours

Infos du cours

Discussion générale

Progression

Glossaire

Bibliographie

S0 : Informations générales

S1 : La donnée et la cybersécurité au cœur de nos vies

S2 : La cybersécurité pour le citoyen : la Data Privacy comme levier d'engagement

S3 : règles juridiques de la cybersécurité

S4 : Introduction à la cybersécurité logicielle

S5 : Attaques et défenses en intelligence artificielle

S6 : Les « Security Information and Event Management » (SIEM)

Introduction

SIEM : introduction et définitions

Les SIEM modernes

Les logs

Les SIEM et la Cyber Threat Intelligence

Remontées d'alertes et d'incidents

Machine Learning

Quiz semaine 6

Evaluation finale

Echéance le 09, 2023 at 22:00 UTC

Demandez votre badge

1) QUESTION À CHOIX UNIQUE (1/1 point)

Que permet le SIEM ?

☐ La détection des virus sur les postes de travail et la lutte contre la prolifération de malwares

☐ La mise en œuvre d'une politique de gestion des mots de passe

☒ Le stockage et l'interprétation des logs permettant une analyse des évènements de sécurité ✓

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

2) QUESTION À CHOIX UNIQUE (1/1 point)

Un SIEM seul peut-il assurer à lui seul la sécurité des activités d'une entreprise ?

☐ Oui, car le SIEM permet de détecter en temps réel les incidents de sécurité et d'y remédier

☐ Non, pour cela il doit être intégré à un Security Operation Center

☒ Non, elle est assurée par des règles et mesures organisationnelles et opérationnelles adéquates ✓

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

3) QUESTION À CHOIX UNIQUE (1/1 point)

Un SIEM doit pouvoir assurer les fonctions ?

☐ De déploiement des mises à jour logicielles sur son système d'information

☒ De recherche, d'analyse et de corrélation d'évènements de sécurité ✓

☐ De cryptage digital des rapports d'audit

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

4) QUESTION À CHOIX UNIQUE (1/1 point)

Quel type d'information doit être envoyé au SIEM pour assurer son bon fonctionnement ?

☒ Des évènements de sécurité du périmètre à sécuriser ✓

☐ Les mots de passes des utilisateurs du périmètre à sécuriser

☐ Les bulletins de paye des salariés du périmètre à sécuriser

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

5) QUESTION À CHOIX UNIQUE (1/1 point)

La complexité de l'architecture de SIEM est liée :

☒ À la complexité du Système d'information et à la volumétrie de logs à intégrer ✓

☐ Aux spécifications fixées par l'éditeur de la solution

☐ Au talent des commerciaux des intégrateurs de solution de sécurité

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

6) QUESTION À CHOIX UNIQUE (1 point possible)

Qu'est-ce que la corrélation ?

☒ Le référencement de manière unique de la catégorie de chaque champ de log ✗

☐ La création de rapports et de tableaux de bord de sécurité

☒ Le process de rapprochement des évènements depuis différents systèmes ✓

EXPLANATION

Voir les vidéos Définitions et Les SIEM modernes

MASQUER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

7) QUESTION À CHOIX UNIQUE (1/1 point)

Lors de l'archivage des évènements de sécurité, de quoi doit-on principalement s'assurer ?

☒ Que l'intégrité des données soit préservée, notamment pour des raisons de conformité et de gestion de preuves ✓

☐ Que les évènements aient bien été normalisés, permettant d'optimiser leur prochaine utilisation au sein du SIEM

☐ Que les données ne contiennent pas de mots de passes en clair car elles peuvent facilement être récupérées par un hacker

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

8) QUESTION À CHOIX UNIQUE (1 point possible)

Quelle est l'utilité principale de la CTI ?

☐ La CTI permet de dérober des informations sur les prochaines cibles d'acteurs de la menace cyber

☐ La CTI permet en permanence de comprendre et de caractériser l'état de la menace permettant aux entreprises et organisations d'adapter leurs défenses ✓

☒ La CTI permet aux autorités d'identifier et d'interpeller des individus en lien avec des acteurs de la menace cyber ✗

EXPLANATION

Voir la vidéo CTI

MASQUER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

9) QUESTION À CHOIX UNIQUE (1/1 point)

La CTI permet à une organisation :

☒ D'adapter à la fois sa gestion stratégique et opérationnelle de la sécurité ✓

☐ D'adapter sa gestion stratégique de la sécurité

☐ D'adapter sa gestion opérationnelle de la sécurité

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

10) QUESTION À CHOIX UNIQUE (1/1 point)

En quoi le renseignement de la menace cyber peut-il être utile dans le cadre de la gestion des évènements de sécurité d'une entreprise ?

☐ La CTI permet de dérober des informations sur les prochaines cibles d'acteurs de la menace cyber

☒ La CTI permet d'identifier plus rapidement des incidents de sécurité et facilite la réponse à incidents associée ✓

☐ La CTI permet d'optimiser la configuration de son serveur Web apache2

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

11) QUESTION À CHOIX UNIQUE (1/1 point)

Qu'est-ce qu'un CERT ?

☐ Un Centre d'Evaluation et de Recrutement de Talents cyber

☒ Une équipe de réaction face aux incidents cyber ✓

☐ Une équipe de développeurs Web

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

12) QUESTION À CHOIX UNIQUE (1 point possible)

Le SOC est :

☐ Une réponse purement technique à l'insécurité du numérique du monde digital

☒ La direction de la sécurité informatique de l'entreprise ✗

☒ La structure et les hommes permettant d'assurer la cyberdéfense de l'entreprise ✓

EXPLANATION

Voir la vidéo Les SIEM modernes

MASQUER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

13) QUESTION À CHOIX UNIQUE (1/1 point)

Le SOC est constitué :

☐ D'une équipe opérationnelle et experte en matière de cybersécurité

☒ D'équipements matériels et logiciels mis en œuvre par une équipe de spécialistes ✓

☐ De logiciels Microsoft installés par des prestataires de qualité

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

14) QUESTION À CHOIX UNIQUE (1/1 point)

L'offre logicielle des SIEM est :

☐ Concentrée chez quelques éditeurs états-unien et asiatiques

☐ Uniquement développée en France

☒ Commerciale et open-source en partie gratuite ✓

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

15) QUESTION À CHOIX UNIQUE (1/1 point)

Pourquoi est-il important de normaliser la remontée d'incidents de sécurité ?

☐ Pour que cela soit plus lisible par les équipes de sécurité

☒ Pour améliorer l'automatisation des traitements et opérations de sécurité ✓

☐ Pour renforcer la cohésion des équipes de sécurité

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

16) QUESTION À CHOIX MULTIPLE (1/1 point)

Identifiez les propositions permettant de caractériser un IOC :

☒ Un IOC a une durée de vie très limitée dans le temps

☒ Un IOC est un artefact technique

☐ Un IOC permet d'identifier de manière précise le nom d'un acteur de la menace

✓

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

17) QUESTION À CHOIX UNIQUE (1/1 point)

En France, existe-t-il plusieurs CSIRT ?

☒ Oui ✓

☐ Non

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

18) QUESTION À CHOIX UNIQUE (1/1 point)

Quel est l'utilité des logiciels UEBA ?

☒ Grâce à de l'analyse comportementale, permet d'identifier des comportements malveillants sur les systèmes du périmètre à sécuriser ✓

☐ De collecter des informations qui seront ensuite utilisées pour du ciblage publicitaire

☐ De collecter des évènements de sécurité

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

19) QUESTION À CHOIX UNIQUE (1/1 point)

Un Firewall peut-il générer des Logs ?

☒ Oui ✓

☐ Non

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

20) QUESTION À CHOIX UNIQUE (1/1 point)

Au sein d'une organisation, quelle entité est en charge du maintien en conditions opérationnelles du SIEM ?

☒ SOC ✓

☐ CSIRT

☐ SOC et CSIRT

AFFICHER LA RÉPONSE

Vous avez utilisé 1 essais sur 1

←

→

A propos


Aide et Contact


Conditions générales d'utilisation


Charte utilisateurs

Politique de confidentialité


Mentions légales

FUN MOOC

f



POWERED BY

OPENeX