FORMATIONSSI

Contenu détaillé des épisodes

ÉPISODE 1

Contexte politique et industrie de la cybercriminalité

• Maîtriser les fondamentaux de la cybersécurité pour comprendre les enjeux liés à la sécurité des systèmes d'information en entreprise.

• Connaître le contexte géopolitique, de l'industrie de la cybercriminalité, et des organismes régulateurs.

• Comprendre les impacts d'une attaque et celui de la transformation digitale sur la cybersécurité.

1

ÉPISODE 2

Définition et langage commun de la sécurité de l'information

• Connaître les concepts, les termes et acronymes usuels de sécurité des systèmes d'information.

• Connaître : le hacking et connaître les différents types de hackers, la taxonomie des incidents informatiques proposée par l'ENISA et être capable d'y associer les principaux types d'incidents.

• Connaître les normes et méthodes utilisées pour évaluer la sécurité des systèmes d'information, les différents outils de sécurité et comprendre leur fonctionnement global.

2

ÉPISODE 3

Différents types d'attaques liées au réseau d'information et de communication

• Connaître les différents types d'attaques liées aux systèmes d'information et leurs scénarios.

• Connaissance et compréhension des scénarios d'attaque type : exemple de l'APT, DDOS.

• Avoir connaissance des bonnes pratiques à respecter et prendre conscience de l'importance du facteur humain dans la protection du système d'information.

3

ÉPISODE 4

Définition et maîtrise des principes de gestion du risque

- Connaître les définitions associées au traitement du risque.

- Savoir différencier les différents types de traitement du risque et être capable de classifier le risque en fonction de son impact et de sa vraisemblance.

- Connaître des outils et les bonnes pratiques permettant la mise en place de politique de sécurité adaptée aux organisations et aux collaborateurs.

4

ÉPISODE 5

Conception d'architecture de sécurité

- Connaître les règles d'élaboration d'une architecture de sécurité.

- Maîtriser les notions de couches réseau et être capable d'identifier pour chaque couche des outils de sécurité.

- Comprendre les scénarios d'attaques types et savoir quels outils permettent de les empêcher.

- Être capable d'appliquer les bonnes pratiques concernant la virtualisation, le cloisonnement, le cloud et l'externalisation.

5

ÉPISODE 6

Maintien en condition de sécurité

- Connaître des outils permettant d'auditer le parc informatique d'une organisation.

- Avoir conscience de l'importance de la mise à jour des systèmes d'information, connaître les principaux outils utiles au maintien d'une veille technologique efficace et savoir anticiper l'obsolescence.

- Différencier vulnérabilité logicielle et faille de configuration, comprendre le processus de patch management et le principe de durcissement et ses différentes couches.

6

ÉPISODE 7

Gestion de l'identité, de l'authentification et des accès

• Savoir gérer les identités, connaître les 3 principales architectures de la gestion des identités.

Connaître les bonnes pratiques en matière d'authentification, être capable de créer un mot de passe robuste et une authentification forte.

• Comprendre les 4 piliers fondamentaux de l'accès aux systèmes d'information et son cycle de vie, l'intérêt du «moindre privilège», le fonctionnement du provisioning des comptes utilisateurs, le principe de la méthode RBAC.

7

ÉPISODE 8

Enjeux liés au maintien de la sécurité

• Comprendre les enjeux et les bonnes pratiques liés à l'administration des systèmes d'information.

• Avoir conscience des risques liés l'administration à distance.

• Connaître des outils et les bonnes pratiques permettant la mise en place de politique de sécurité adaptée aux organisations et aux collaborateurs.

8

ÉPISODE 9

Principes de cryptographie

• Connaître la définition et les grands principes du chiffrement asymétrique.

• Savoir identifier les protocoles utilisés pour le chiffrage en fonction des pratiques (e-mails, téléchargement de fichier, supports de stockages, etc.) ; être averti de l'existence de failles dans les protocoles.

• Connaître des bonnes pratiques associées au chiffrement.

9

ÉPISODE 10

Besoin de sécurité d'une information

• Comprendre les besoins de sécurité d'une information (DICT) et les bonnes pratiques liées à la protection des données.

• Connaitre les grandes étapes du cycle de vie d'une information : classification, stockage, communication et destruction.

• Comprendre le principe de classification des informations, le niveau de classification national, la réglementation encadrant les informations lassifiées.

10

ÉPISODE 11

SOC – Security Operating Center

- Connaitre le rôle, l'organisation et le périmètre d'action du SOC.
- Identifier les acteurs liés à la sécurité du système d'information et leur rôle.
- Connaître les technologies liées à la sécurité du système d'information et leurs évolutions.

11

ÉPISODE 12

Traiter les incidents

- Maîtriser les notions d'événements et d'incident, savoir définir les 4 étapes du processus de gestion d'un incident.

- Comprendre l'importance de l'aspect humain et d'une bonne communication en cas de gestion de crise.

- Connaître les acteurs intervenant dans la gestion d'incidents et identifier leurs rôles.

- Connaître les principaux plans liés à la gestion de crise, comprendre l'importance des tests et répétitions des procédures de gestion de crise.

12

Évaluation finale

Test d'évaluation final pour valider les acquis du parcours.

Pour obtenir votre certificat You Are Digital | CyberSecurity, vous devez obtenir un score minimum de 80%.

FORMATIONSSI

support@formation-ssi.com

SBT Human(s) Matter
40 Avenue Alsace-Lorraine
38 000 Grenoble
FRANCE