# CYBERDEF101-MODULE 3-QUIZZ

1. **CD101-Mod3-Q1**

   Quand on parle de gestion de vulnérabilités dans l'entreprise on parle ?

   (a) de répertorier les vulnérabilités informatiques sur internet (0%)
   (b) de constituer une base de données de ses propres fragilités pour plus tard (50%)
   (c) d'identifier ses vulnérabilités et de les corriger au plus tôt (50%)

2. **CD101-Mod3-Q2**

   Dans la gestion de l'évènement de sécurité d'un SIEM, donner le premier et le dernier des processus de gestion de l'évènement :

   (a) détection (50%)
   (b) corrélation (0%)
   (c) collecte (0%)
   (d) alerte (50%)

3. **CD101-Mod3-Q3**

   La norme ISO 27035 traite en particulier de :

   (a) gestion des vulnérabilités (0%)
   (b) gestion des incidents (100%)
   (c) gestion des menaces informatiques (0%)
   (d) gestion de crise (0%)

4. **CD101-Mod3-Q4**

   Le Forensic dans la réponse à incident comprend :

   (a) l'analyse de traces dans les réseaux (25%)
   (b) l'analyse de documents cachés dans une machine (25%)
   (c) la recherche d'indices de compromission (25%)
   (d) l'identification de l'attaquant (25%)

5. **CD101-Mod3-Q5**

   La sécurité opérationnelle comporte :

   (a) le maintien en condition de sécurité au sein de la DSI (33.33333%)

(b) le pilotage les audits techniques (pentests) sur l'environnement (33.33333%)
(c) les opérations du SOC : Security Operation Center (33.33333%)
(d) la gestion de la continuité d'activité de l'entreprise (0%)
(e) la construction des politiques de sécurité (0%)
(f) la supervision du fonctionnement du système d'information (0%)

6. **CD101-Mod3-Q6**

Quelle la signification dans le domaine des systèmes d'information du terme MTTR

(a) le temps moyen entre deux attaques (0%)
(b) le temps moyen entre deux bugs (0%)
(c) le temps moyen pour réparer (100%)
(d) la gestion de la continuité d'activité (0%)

7. **CD101-Mod3-Q7**

Un CERT privé peu fournir moyennant paiement des services sur :

(a) des vulnérabilités pour faire des tests d'entreprise (50%)
(b) des bases de données d'applications sures (0%)
(c) des attaques informatiques rendues inoffensives pour les pentests (0%)
(d) des alertes liées à la sécurité informatique (50%)

8. **CD101-Mod3-Q8**

A quoi peut-on associer le terme : WannaCry

(a) Un ransonware (100%)
(b) Un spyware (0%)
(c) Un antivirus (0%)
(d) Un réseau social (0%)

9. **CD101-Mod3-Q9**

Un plan de cyberdéfense comporte

(a) Le périmètre de certification ISO 27001 (0%)
(b) La liste des actifs critiques (33.33333%)
(c) Les évènements les plus redoutés (33.33333%)

(d) Un annuaire de crise (33.33333%)
(e) La liste des politiques de sécurité de l'entreprise (0%)

10. **CD101-Mod3-Q10**

Un SIEM intègre les évènements de détection de

(a) IPS / IDS (33.33333%)
(b) AD (0%)
(c) WAF (33.33333%)
(d) Proxy (33.33333%)

11. **CD101-Mod3-Q11**

L'orchestration dans la gestion de vulnérabilités comporte

(a) L'automatisation des patchs (0%)
(b) La gestion et le suivi des vulnérabilités des actifs (50%)
(c) La gestion des scans de vulnérabilités (50%)

12. **CD101-Mod3-Q12**

La recherche récurrente hebdo de vulnérabilités passe principalement par

(a) Le scan de vulnérabilités (50%)
(b) Les tests d'intrusion (Pentest) (0%)
(c) Le bug-bounty (0%)
(d) L'analyse statique de code source (50%)

13. **CD101-Mod3-Q13**

Quelles sont les deux priorités d'un RSSI en SECOPS

(a) Déployer la gestion de vulnérabilités (50%)
(b) Mettre en place une fonction de détection (50%)
(c) Mettre à jour ses Firewalls (0%)
(d) Déployer un VPN pour l'accès à distance (0%)

14. **CD101-Mod3-Q14**

Que signifie l'acronyme APT ?

(a) Array Processor Tampering (0%)

(b) Advanced Persistent Threat (100%)
(c) Advanced Programming Theory (0%)
(d) Agnostic Programming Threat (0%)

15. **CD101-Mod3-Q15**

Une faille 0 day est une faille ?

(a) Qui a été corrigée depuis moins de 24h (0%)
(b) Qui a été découverte depuis moins de 24h (0%)
(c) Qui n'a pas encore de correctif de sécurité disponible (100%)
(d) Qui n'a pas encore été exploitée (0%)

16. **CD101-Mod3-Q16**

Qu'est qu'un outil SIEM ne fait pas ou n'est pas dans son scope à ce jour

(a) Identification de la menace (0%)
(b) Enregistrement de l'incident (0%)
(c) Classement de l'incident (0%)
(d) Escalade d'un incident (0%)
(e) Diagnostic d'impact (50%)
(f) Résolution et rétablissement du service (50%)

17. **CD101-Mod3-Q17**

En cybersécurité, le terme SOAR veut dire

(a) Strength Orchestration, for Automation and Response (0%)
(b) Strengths, Opportunities , Aspirations, Results (0%)
(c) Security Orchestration, Automation and Response (100%)
(d) Security Organisation, Automation and Reaction (0%)

18. **CD101-Mod3-Q18**

Une équipe CSIRT conduit dans

(a) L'investigation sur incident (50%)
(b) La remédiation sur le système attaqué (0%)
(c) L'anticipation par recherche de vulnérabilité (0%)
(d) Le hunting (chasse à la menace) (50%)

19. **CD101-Mod3-Q19**

La norme 22301 doit être utilisée dans

(a) L'organisation de la gestion de crise (100%)
(b) La gestion des incidents non critiques (0%)
(c) La mise en place du SMSI (Système de management système de gestion de la sécurité) (0%)

20. **CD101-Mod3-Q20**

Dans la gestion des incidents de sécurité, l'équipe SECOPS Incidents doit gérer

(a) La détection et l'enregistrement des incidents (25%)
(b) L'exploitation de l'IT (0%)
(c) La classification et l'aide initiale (25%)
(d) L'enquête et le diagnostic (25%)
(e) La restauration des données (0%)
(f) La cloture de l'incident (25%)
(g) La communication de crise (0%)