Contenu et déroulement du cours CyberOps Associate (CA) v1.0

Dernière mise à jour le 20 décembre 2020

Introduction

Les entreprises d'aujourd'hui se doivent de détecter rapidement les failles de cybersécurité et de répondre efficacement aux incidents. Les centres opérationnels de sécurité (SOC) surveillent étroitement les systèmes de sécurité et protègent les entreprises en détectant et en éliminant les exploits et les menaces. Le cours CyberOps Associate prépare les candidats à travailler en tant qu'analystes dans les centres opérationnels de sécurité.

Profil des participants

Le cours CyberOps Associate est destiné aux élèves de la Cisco Networking Academy® qui veulent développer des compétences professionnelles basiques d'analystes de la sécurité. Les profils visés incluent les étudiants dans le domaine des technologies et les professionnels IT qui souhaitent poursuivre leur carrière dans un centre opérationnel de sécurité (SOC). Pendant ce cours, les étudiants développeront toutes les connaissances fondamentales nécessaires pour détecter et analyser les menaces de cybersécurité de base, et les transmettre aux personnes les plus à même de les traiter, à l'aide d'outils Open Source.

Connaissances préalables requises

Les élèves du cours CyberOps Associate doivent posséder les compétences et les connaissances suivantes :

- Compétences en matière de navigation sur PC et sur Internet
- Notions de base sur les systèmes Windows et Linux
- Notions de base sur les réseaux informatiques (niveau CCNA ITN)
- Compréhension du système binaire et hexadécimal
- Maîtrise de Cisco Packet Tracer

Certifications visées

Ce cours s'aligne sur la certification Cisco Certified CyberOps Associate (CBROPS). Les candidats doivent passer l'examen CBROPS 200-201 pour obtenir la certification Cisco Certified CyberOps Associate. L'examen CBROPS teste les connaissances et les compétences d'un candidat en matière de sécurité, de surveillance, d'analyse basée sur l'hôte, d'analyse des intrusions réseau et des politiques et procédures de sécurité.

Description du cours

Le cours comporte de nombreuses fonctionnalités pour aider les élèves à maîtriser ces concepts :

- Le cours comprend vingt-huit (28) modules. Chaque module est composé de rubriques.
- Les modules mettent l'accent sur l'esprit critique, la résolution des problèmes, la collaboration et l'application pratique des compétences.

- Chaque module propose une mise en pratique et une évaluation de la compréhension de l'élève, comme un travail pratique ou une activité Packet Tracer. Ces activités dans chaque module s'accompagnent de commentaires qui indiquent à l'élève s'il maîtrise les compétences requises. Les élèves peuvent vérifier leur niveau de compréhension avant de passer un questionnaire noté ou un examen.
- Chaque rubrique fait l'objet d'un questionnaire interactif ou d'un autre type d'évaluation de la bonne compréhension des élèves, comme des travaux pratiques ou une session Packet Tracer. Ces évaluations sont conçues pour que les élèves sachent s'ils ont une bonne compréhension du sujet ou s'ils doivent réviser avant de poursuivre. Ils peuvent vérifier leur niveau de compréhension avant de passer un questionnaire noté ou un examen. Les questionnaires de vérification de la compréhension des élèves n'ont aucun impact sur la note globale.
- Les contenus multimédias riches, notamment des activités interactives, des vidéos et des questionnaires, s'adaptent à de nombreux styles de formation pour favoriser l'assimilation des connaissances.
- Des environnements virtuels simulent des scénarios de cyberattaque concrets et permettent de s'entraîner à la surveillance, à l'analyse et à la résolution de problèmes de sécurité.
- Les exercices pratiques aident les étudiants à développer leur capacité à résoudre les problèmes complexes et leur esprit critique.
- Grâce aux évaluations innovantes, les élèves reçoivent des commentaires instantanés de la part de l'instructeur pour mieux évaluer le niveau de connaissances et de compétences atteint.
- Les concepts techniques sont présentés dans un langage adapté aux élèves de tous niveaux, et des activités interactives intégrées au cours interrompent la lecture du contenu et aident à améliorer la compréhension.
- Le cursus encourage les étudiants à envisager une formation supplémentaire en informatique, mais met aussi l'accent sur les compétences mises en œuvre et l'expérience pratique.
- Les exercices Cisco Packet Tracer sont conçus pour Packet Tracer 7.3.0 ou version ultérieure.

Objectifs du cours

Le cours CyberOps Associate v1.0 vous permet d'acquérir les connaissances et les compétences nécessaires pour prendre en charge les tâches et les responsabilités d'un analyste de cybersécurité débutant travaillant dans un centre opérationnel de sécurité (SOC).

À l'issue du cours *CyberOps Associate v1.0*, les élèves seront en mesure d'effectuer les tâches suivantes :

- Installer des machines virtuelles afin de créer un environnement sécurisé pour la mise en œuvre et l'analyse des incidents de cybersécurité.
- Expliquer le rôle de l'analyste de cybersécurité dans l'entreprise.
- Expliquer les fonctionnalités et les caractéristiques du système d'exploitation Windows nécessaires pour renforcer les analyses de cybersécurité.
- Expliquer les fonctionnalités et les caractéristiques du système d'exploitation Linux.
- Analyser le fonctionnement des services et des protocoles réseau.
- Expliquer le fonctionnement de l'infrastructure de réseau.
- Classer les divers types d'attaques réseau.
- Utiliser des outils de surveillance du réseau pour identifier les attaques contre les services et les protocoles réseau.

- Expliquer comment empêcher un accès malveillant aux réseaux informatiques, aux hôtes et aux données.
- Expliquer les effets de la cryptographie sur la surveillance de la sécurité du réseau.
- Expliquer comment enquêter sur les attaques et les vulnérabilités des terminaux.
- Évaluer les alertes de sécurité du réseau.
- Analyser les données liées aux intrusions réseau afin d'identifier les hôtes compromis.
- Appliquer des modèles de gestion des incidents liés à la sécurité du réseau.

Conditions requises pour les équipements utilisés lors des travaux pratiques

Ce cours ne nécessite aucun équipement physique autre que le PC destiné aux travaux pratiques. Il utilise plusieurs machines virtuelles pour créer une expérience pratique.

Bundle d'équipements de base :

- Configuration système minimale requise pour les PC
  - CPU : Intel Pentium 4, 2,53 GHz ou équivalent avec prise en charge de la virtualisation
  - Systèmes d'exploitation, tels que Microsoft Windows, Linux et Mac OS
  - Processeur 64 bits
  - RAM : 8 Go
  - Stockage : 40 Go d'espace disque disponible
  - Résolution d'affichage : 1 024 x 768
  - Polices de langue prenant en charge le codage Unicode (en cas d'affichage dans des langues autres que l'anglais)
  - Derniers pilotes de cartes vidéo et mises à jour du système d'exploitation
- Connexion Internet pour les ordinateurs des étudiants et ceux des ateliers pratiques

Logiciels sur le PC de l'élève :

- Machine virtuelle Oracle VirtualBox Manager (version 6.1 ou ultérieure)
- Poste de travail virtuel CyberOps
  - Téléchargeable à partir du cours
  - Nécessite 1 Go de RAM et 20 Go d'espace disque
- Machine virtuelle Security Onion
  - Téléchargeable à partir du cours
  - Nécessite 4 Go de RAM (minimum), 8 Go de RAM (fortement recommandé) et 20 Go d'espace disque

Description du cours CyberOps Associate

Vous trouverez ci-dessous l'ensemble des modules et les compétences associées présentés dans ce cours. Chaque module constitue une unité d'apprentissage intégrée, se composant de contenus, d'activités et d'évaluations qui ciblent un ensemble spécifique de compétences. La taille du module dépend du niveau de connaissances et d'aptitudes nécessaires pour maîtriser la compétence. Certains modules sont considérés comme fondamentaux, étant donné que les éléments présentés, bien qu'ils ne soient pas évalués, traitent de concepts qui sont couverts lors de l'examen de certification CBROPS.

Tableau 1. Description du cours CyberOps Associate v1.0

Module/rubriques	Objectifs
Module 1. Le danger	**Expliquer pourquoi les réseaux et les données sont la cible d'attaques.**
1.0 Introduction	Une brève introduction au cours et au premier module.
1.1 Histoires de guerre	Décrire les spécificités des incidents de cybersécurité.
1.2 Hackers	Expliquer les raisons qui motivent les hackers à l'origine d'incidents de sécurité spécifiques.
1.3 Impact des menaces	Expliquer l'impact potentiel des attaques du réseau.
1.4 Résumé : les dangers	Un résumé et le questionnaire du module.
Module 2. Les combattants de la guerre contre la cybercriminalité	**Expliquer comment se préparer à une carrière dans les opérations de cybersécurité.**
2.0 Introduction	Une introduction au module.
2.1 Le centre opérationnel de sécurité moderne	Expliquer la mission du centre opérationnel de sécurité (SOC).
2.2 Devenir un acteur de la protection	Décrire les ressources disponibles pour se préparer à une carrière dans les opérations de cybersécurité.
2.3 Résumé : les combattants de la guerre contre la cybercriminalité	Un résumé et le questionnaire du module.
Module 3. Le système d'exploitation Windows	**Présenter les fonctionnalités de sécurité du système d'exploitation Windows.**
3.0 Introduction	Une introduction au module.
3.1 L'histoire de Windows	Décrire l'histoire du système d'exploitation Windows.
3.2 Architecture et fonctionnement de Windows	Expliquer l'architecture de Windows et son fonctionnement.
3.3 Configuration et surveillance de Windows	Expliquer comment configurer et surveiller Windows.
3.4 La sécurité Windows	Expliquer comment Windows peut être sécurisé.
3.5 Résumé : le système d'exploitation Windows	Un résumé et le questionnaire du module.
Module 4. Présentation de Linux	**Mettre en œuvre la sécurité Linux de base.**
4.0 Introduction	Une introduction au module.
4.1 Notions de base sur Linux	Expliquer pourquoi les compétences Linux sont essentielles pour la surveillance de la sécurité du réseau et l'investigation.
4.2 Utilisation du shell Linux	Utiliser le shell Linux pour manipuler des fichiers texte.
4.3 Serveurs et clients Linux	Expliquer le fonctionnement des réseaux client-serveur.
4.4 Administration de base du serveur	Expliquer comment un administrateur Linux localise et manipule les fichiers journaux de sécurité.

Module/rubriques	Objectifs
4.5 Le système de fichiers Linux	Gérer le système de fichiers Linux et les autorisations.
4.6 Utiliser l'interface graphique Linux	Expliquer les composants de base de l'interface graphique Linux.
4.7 Utiliser un hôte Linux	Utiliser les outils pour détecter les malwares sur un hôte Linux.
4.8 Résumé : les principes de base de Linux	Un résumé et le questionnaire du module.
Module 5. Protocoles réseau	**Expliquer comment les protocoles permettent d'exploiter le réseau.**
5.0 Introduction	Une introduction au module.
5.1 Processus de communication du réseau	Expliquer le fonctionnement de base des communications de données en réseau.
5.2 Les protocoles de communication	Expliquer comment les protocoles permettent d'exploiter le réseau.
5.3 L'encapsulation des données	Expliquer comment l'encapsulation de données permet la transmission des données sur le réseau.
5.4 Résumé : les protocoles réseau	Un résumé et le questionnaire du module.
Module 6. Ethernet et protocole IP	**Expliquer comment les protocoles Ethernet et IP assurent la communication réseau.**
6.0 Introduction	Une introduction au module.
6.1 Ethernet	Expliquer comment Ethernet prend en charge la communication réseau.
6.2 IPv4	Expliquer comment le protocole IPv4 prend en charge la communication réseau.
6.3 Notions de base sur l'adressage IP	Expliquer comment les adresses IP assurent la communication réseau.
6.4 Les types d'adresses IPv4	Présenter les types d'adresses IPv4 qui permettent la communication réseau.
6.5 La passerelle par défaut	Expliquer comment la passerelle par défaut assure la communication réseau.
6.6 Longueur du préfixe IPv6	Expliquer comment le protocole IPv6 assure la communication réseau.
6.7 Résumé : les protocoles Ethernet et IP	Un résumé et le questionnaire du module.
Module 7. Principes de sécurité du réseau	**Vérification de la connectivité.**
7.0 Introduction	Une introduction au module.
7.1 ICMP	Expliquer comment le protocole ICMP sert à tester la connectivité du réseau.
7.2 Utilitaires ping et Traceroute	Utiliser les outils Windows, ping et Traceroute pour vérifier la connectivité du réseau.

Module/rubriques	Objectifs
7.3 Résumé : la vérification de la connectivité	Un résumé et le questionnaire du module.
Module 8. Protocole ARP (Address Resolution Protocol)	**Analyser les unités de données du protocole ARP sur un réseau.**
8.0 Introduction	Une introduction au module.
8.1 Les adresses MAC et IP	Comparer les rôles de l'adresse MAC et de l'adresse IP.
8.2 ARP	Analyser ARP en examinant les trames Ethernet.
8.3 Les problèmes liés à ARP	Expliquer l'impact qu'ont les requêtes ARP sur le réseau et les performances des hôtes.
8.4 Résumé : le protocole ARP (Address Resolution Protocol)	Un résumé et le questionnaire du module.
Module 9. La couche de transport	**Expliquer comment les protocoles de la couche de transport prennent en charge la fonctionnalité du réseau.**
9.0 Introduction	Une introduction au module.
9.1 Les caractéristiques de la couche de transport	Expliquer comment les protocoles de la couche de transport prennent en charge les communications réseau.
9.2 Établissement de sessions dans la couche de transport	Expliquer comment la couche de transport établit des sessions de communication.
9.3 Fiabilité de la couche de transport	Expliquer comment la couche de transport établit des communications fiables.
9.4 Résumé de la couche de transport	Un résumé et le questionnaire du module.
Module 10. Services réseau	**Expliquer comment les services réseau assurent la fonctionnalité du réseau.**
10.0 Introduction	Une introduction au module.
10.1 DHCP	Expliquer comment les services DHCP assurent la fonctionnalité du réseau.
10.2 DNS	Expliquer comment les services DNS assurent la fonctionnalité du réseau.
10.3 NAT	Expliquer comment les services NAT assurent la fonctionnalité du réseau.
10.4 Les services de transfert et de partage des fichiers	Expliquer comment les services de transfert des fichiers assurent la fonctionnalité du réseau.
10.5 Les e-mails	Expliquer comment les services de messagerie assurent la fonctionnalité du réseau.
10.6 HTTP	Expliquer comment les services HTTP assurent la fonctionnalité du réseau.
10.7 Résumé : les services réseau	Un résumé et le questionnaire du module.

Module/rubriques	Objectifs
Module 11. Les périphériques de communication réseau	**Expliquer comment les périphériques réseau assurent les communications réseau filaires et sans fil.**
11.0 Introduction	Une introduction au module.
11.1 Les périphériques réseau	Expliquer comment les périphériques réseau assurent les communications réseau.
11.2 Les communications sans fil	Expliquer comment les périphériques sans fil assurent les communications réseau.
11.3 Résumé : les appareils de communication réseau	Un résumé et le questionnaire du module.
Module 12. L'infrastructure de sécurité du réseau	**Expliquer comment les périphériques et les services renforcent la sécurité du réseau.**
12.0 Introduction	Une introduction au module.
12.1 Les topologies du réseau	Expliquer comment les conceptions de réseau influent sur le flux de trafic transitant via le réseau.
12.2 Les périphériques de sécurité	Expliquer comment les périphériques spécialisés renforcent la sécurité du réseau.
12.3 Les services de sécurité	Expliquer comment les services renforcent la sécurité du réseau.
12.4 Résumé : l'infrastructure de sécurité du réseau	Un résumé de ce module.
Module 13. Les hackers et leurs outils	**Expliquer comment les réseaux sont attaqués.**
13.0 Introduction	Une introduction au module.
13.1 Qui attaque notre réseau ?	Expliquer l'évolution des menaces ciblant le réseau.
13.2 Outils des hackers	Décrire les différents types d'outils d'attaque utilisés par les hackers.
13.3 Résumé : les hackers et leurs outils	Un résumé et le questionnaire du module.
Module 14. Les attaques et les menaces fréquentes	**Expliquer les divers types de menaces et d'attaques.**
14.0 Introduction	Une introduction au module.
14.1 Les malwares	Décrire les types de programmes malveillants.
14.2 Les attaques réseau courantes : reconnaissance, accès et ingénierie sociale	Expliquer les attaques de reconnaissance, d'accès et d'ingénierie sociale.
14.3 Les attaques réseau : déni de service, dépassement de la mémoire tampon et contournement	Expliquer les attaques par déni de service, dépassement de la mémoire tampon et contournement.
14.4 Résumé : les menaces et les attaques courantes	Un résumé et le questionnaire du module.
Module 15. Observation du fonctionnement du réseau	**Expliquer la surveillance du trafic réseau.**
15.0 Introduction	Une introduction au module.

Module/rubriques	Objectifs
15.1 Présentation de la surveillance du réseau	Expliquer l'importance de la surveillance du réseau.
15.2 Présentation des outils de surveillance du réseau	Expliquer comment la surveillance de réseau est effectuée.
15.3 Résumé : les outils et la surveillance du réseau	Un résumé et le questionnaire du module.
Module 16. Attaques ciblant les fondements du réseau	**Expliquer comment les vulnérabilités TCP/IP favorisent les attaques réseau.**
16.0 Introduction	Une introduction au module.
16.1 Informations sur les unités de données de l'adresse IP	Expliquer la structure de l'en-tête des adresses IPv4 et IPv6.
16.2 Les vulnérabilités IP	Expliquer comment les vulnérabilités IP favorisent les attaques réseau.
16.3 Les vulnérabilités TCP et UDP	Expliquer comment les vulnérabilités TCP et UDP favorisent les attaques réseau.
16.4 Résumé : les attaques ciblant les fondements du réseau	Un résumé et le questionnaire du module.
Module 17. Attaques ciblant les activités	**Expliquer pourquoi les applications et les services réseau fréquemment utilisés sont vulnérables face aux attaques.**
17.0 Introduction	Une introduction au module.
17.1 Les services IP	Expliquer les vulnérabilités des services IP.
17.2 Les services d'entreprise	Expliquer comment les vulnérabilités des applications réseau favorisent les attaques réseau.
17.3 Résumé : les attaques ciblant les activités	Un résumé et le questionnaire du module.
Module 18. Comprendre les mécanismes de défense	**Expliquer les approches en matière de protection du réseau.**
18.0 Introduction	Une introduction au module.
18.1 Une défense en profondeur	Expliquer comment la stratégie de défense approfondie protège les réseaux.
18.2 Les politiques de sécurité, les réglementations et les standards	Présenter les standards, les réglementations et les politiques de sécurité en vigueur.
18.3 Résumé : comprendre la défense	Un résumé et le questionnaire du module.
Module 19. Contrôle d'accès	**Expliquer comment le contrôle d'accès protège un réseau.**
19.0 Introduction	Une introduction au module.
19.1 Les concepts de contrôle d'accès	Expliquer comment le contrôle d'accès protège les données du réseau.
19.2 Utilisation et fonctionnement du modèle AAA	Expliquer comment le modèle AAA contrôle l'accès au réseau.
19.3 Résumé : le contrôle d'accès	Un résumé et le questionnaire du module.
Module 20. Threat Intelligence	**Utiliser diverses sources d'informations pour localiser les**

Module/rubriques	Objectifs
	menaces actuelles.
20.0 Introduction	Une introduction au module.
20.1 Sources d'informations	Décrire les sources d'information utilisées pour indiquer les nouvelles menaces de sécurité du réseau.
20.2 Les services de Threat Intelligence	Décrire les divers services de Threat Intelligence.
20.3 Résumé : la Threat Intelligence	Un résumé et le questionnaire du module.
Module 21. Cryptographie	**Expliquer comment l'infrastructure à clé publique assure la sécurité du réseau.**
21.0 Introduction	Une introduction au module.
21.1 Intégrité et authenticité	Expliquer le rôle de la cryptographie pour garantir l'intégrité et l'authenticité des données.
21.2 La confidentialité	Expliquer comment les méthodes cryptographiques améliorent la confidentialité des données.
21.3 La cryptographie à clé publique	Expliquer la cryptographie à clé publique.
21.4 Les autorités et le système d'infrastructure à clé publique	Expliquer comment l'infrastructure à clé publique fonctionne.
21.5 Les utilisations et les effets de la cryptographie	Expliquer comment l'utilisation de la cryptographie a un impact sur les opérations de cybersécurité.
21.6 Résumé : la cryptographie	Un résumé de ce module.
Module 22. La protection des terminaux	**Expliquer comment un site web d'analyse des malwares génère un rapport.**
22.0 Introduction	Une introduction au module.
22.1 Protection antimalware	Expliquer les méthodes de protection contre les malwares.
22.2 La prévention des intrusions basée sur l'hôte	Expliquer les entrées de journal IPS/IDS basées sur l'hôte.
22.3 La sécurité des applications	Expliquer comment la fonction de sandboxing permet d'analyser les programmes malveillants.
22.4 Résumé : la protection des terminaux	Un résumé et le questionnaire du module.
Module 23. Évaluation des vulnérabilités des terminaux	**Expliquer comment les vulnérabilités des terminaux sont évaluées et gérées.**
23.0 Introduction	Une introduction au module.
23.1 Profilage du réseau et du serveur	Expliquer l'intérêt du profilage du réseau et des serveurs.
23.2 Le système d'évaluation des vulnérabilités (CVSS)	Expliquer comment les rapports CVSS permettent de décrire les vulnérabilités de sécurité.
23.3 Gestion sécurisée des périphériques	Expliquer comment les techniques de gestion sécurisée des

Module/rubriques	Objectifs
	périphériques protègent les données et les ressources.
23.4 Les systèmes de gestion de la sécurité de l'information (ISMS)	Expliquer comment les systèmes de gestion de la sécurité de l'information sont utilisés pour protéger les ressources.
23.5 Résumé : évaluation des vulnérabilités des terminaux	Un résumé et le questionnaire du module.
Module 24. Les technologies et les protocoles	**Expliquer l'incidence des technologies de protection sur la surveillance de la sécurité.**
24.0 Introduction	Une introduction au module.
24.1 Les protocoles courants en surveillance	Expliquer le comportement des protocoles réseau courants dans le cadre de la surveillance de la sécurité.
24.2 Les technologies de sécurité	Expliquer comment les technologies de sécurité affectent la surveillance des protocoles réseau courants.
24.3 Résumé : les technologies et protocoles	Un résumé et le questionnaire du module.
Module 25. Les données sur la sécurité du réseau	**Expliquer les types de données sur la sécurité du réseau que vous utilisez pour surveiller la sécurité.**
25.0 Introduction	Une introduction au module.
25.1 Les types de données de sécurité	Décrire les types de données utilisées pour surveiller la sécurité.
25.2 Les journaux des terminaux	Décrire les éléments du fichier journal d'un terminal.
25.3 Les journaux du réseau	Décrire les éléments du fichier journal d'un périphérique réseau.
25.4 Résumé : les données de sécurité réseau	Un résumé et le questionnaire du module.
Module 26. L'évaluation des alertes	**Expliquer le processus d'évaluation des alertes.**
26.0 Introduction	Une introduction au module.
26.1 Les sources d'alertes	Identifier la structure des alertes.
26.2 Présentation de l'évaluation des alertes	Expliquer comment les alertes sont classées.
26.3 Résumé : évaluation des alertes	Un résumé et le questionnaire du module.
Module 27. L'utilisation des données sur la sécurité du réseau	**Interpréter les données afin de déterminer la source d'une alerte.**
27.0 Introduction	Une introduction au module.
27.1 Une plate-forme de données commune	Expliquer comment les données sont préparées pour une utilisation dans un système de surveillance de la sécurité du réseau (NSM).
27.2 Examiner les données du réseau	Utiliser les outils Security Onion pour examiner les événements de sécurité du réseau.
27.3 Améliorer le travail des analystes en cybersécurité	Décrire les outils de surveillance du réseau qui améliorent la gestion du workflow.

Module/rubriques	Objectifs
27.4 Résumé : l'utilisation des données sur la sécurité du réseau	Un résumé et le questionnaire du module.
Module 28. Analyse et réponse aux incidents numériques	**Expliquer comment CyberOps Associate répond aux incidents de cybersécurité.**
28.0 Introduction	Une introduction au module.
28.1 La gestion des preuves et l'attribution des attaques	Expliquer le rôle des processus d'analyse numérique.
28.2 La chaîne de frappe	Identifier les étapes de la chaîne de frappe.
28.3 Analyse du modèle d'intrusion en diamant	Classer un événement d'intrusion à l'aide du modèle en diamant.
28.4 La réponse aux incidents	Appliquer les procédures de gestion des incidents 800-61r2 du NIST par rapport à un scénario donné.
28.5 Résumé : enquêtes techniques et analyse et réponse aux incidents	Un résumé de ce module.
28.6 Préparez-vous à votre examen et lancez votre carrière !	Préparation à la certification, bons de réduction et autres ressources professionnelles.