CompTIA CySA+ Cybersecurity Analyst

Durée: 5 Jours **Réf de cours: GK5867** **Version: CS0-003**

Résumé:

CompTIA Cybersecurity Analyst (CySA+) est une certification destinée aux cyber-professionnels chargés de la détection, de la prévention et de la réponse aux incidents par le biais d'une surveillance continue de la sécurité.
Mise à jour : 27.02.2024

Public visé:

Cette formation s'adresse aux analystes de la sécurité, aux analystes SOC, aux analystes de la réponse aux incidents, aux analystes de la gestion des vulnérabilités et aux ingénieurs de la sécurité.

Objectifs pédagogiques:

- À l'issue de la formation, les participants seront capables de :
- Surveiller et détecter de manière proactive : Démontrez vos compétences en matière de détection et d'analyse des indicateurs d'activités malveillantes à l'aide des méthodes et des outils les plus récents, tels que le renseignement sur les menaces, la gestion des informations et des événements de sécurité (SIEM), la détection et la réponse des endpoints (EDR) et la détection et la réponse étendues (XDR).
- Répondre aux menaces, aux attaques et aux vulnérabilités : Démontrez vos connaissances des processus de réponse aux incidents et de gestion des vulnérabilités et mettre en évidence les compétences de communication essentielles à l'analyse de la sécurité et à la conformité.
- Démontrer ses compétences en matière de tendances actuelles : Les membres de l'équipe peuvent démontrer leur connaissance des tendances actuelles qui affectent le travail quotidien des analystes de sécurité, telles que les environnements cloud et hybrides.

Pré-requis:

Expérience recommandée :

- Network+, Security+ ou connaissances équivalentes.
- Au moins 4 ans d'expérience pratique en tant qu'analyste de réponse aux incidents ou analyste SOC, ou expérience équivalente.

Test et certification

Préparation recommandée à l'examen : CS0-003

La certification CompTIA Cybersecurity Analyst (CySA+) vérifie que les candidats ont les connaissances et les compétences requises pour détecter et analyser les indicateurs d'activité malveillante, comprendre les renseignements sur les menaces et la gestion des menaces, répondre aux attaques et aux vulnérabilités, effectuer une réponse aux incidents, et rapporter et communiquer les activités connexes.

- Nombre de questions : 85 questions au maximum
- Type de questions : Choix multiple
- Durée de l'examen : 165 minutes
- Note de passage : 750 (sur une échelle de 100 à 900)

Contenu:

Opérations de sécurité

- Expliquer l'importance des concepts d'architecture de système et de réseau dans les opérations de sécurité.
- Analyser les indicateurs d'activités potentiellement malveillantes.
- Utiliser les outils ou techniques appropriés pour déterminer les activités malveillantes.
- Comparer et opposer les concepts de renseignement sur les menaces et de chasse aux menaces.

Expliquer l'importance de l'efficacité et de l'amélioration des processus dans les opérations de sécurité.

Gestion de la vulnérabilité

- Mettre en œuvre des méthodes et des concepts d'analyse des vulnérabilités.
- Analyser les résultats des outils d'évaluation des vulnérabilités.
- Analyser les données pour classer les vulnérabilités par ordre de priorité.
- Recommander des contrôles pour atténuer les attaques et les vulnérabilités des logiciels.
- Expliquer les concepts liés à la réponse, au traitement et à la gestion des vulnérabilités.

Gestion de la réponse aux incidents

- Expliquer les concepts liés aux cadres méthodologiques des attaques.
- Réaliser des activités de réponse aux incidents.

Expliquer les phases de préparation et d'activité post-incident du cycle de vie de la gestion des incidents.

Rapports et communication

- Expliquer l'importance des rapports et de la communication en matière de gestion des vulnérabilités.
- Expliquer l'importance du reporting et de la communication en matière de réponse aux incidents.

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

Un support de cours officiel sera remis aux stagiaires.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement