MFE-IT

Formation CompTIA CySA+

Analyste cybersécurité avancé — examen officiel inclus

CompTIA CySA+ (CS0-003)

Référence : SM-CYSA+

Durée : 5 jours • **Volume horaire : 35 h**

Distanciel · Sessions garanties dès 1 inscrit · 60 % de pratique

DESCRIPTION

Cette formation CompTIA CySA+ prépare les professionnels IT à devenir des analystes de cybersécurité capables de surveiller, détecter et répondre aux menaces avec des outils modernes. Vous apprendrez à analyser les vulnérabilités, à utiliser des solutions SIEM/EDR, et à gérer des incidents complexes.

Le programme couvre également la génération de rapports et la communication des résultats de sécurité. Des ateliers pratiques et des simulations d'examen vous rendront prêt pour l'obtention de la certification CompTIA CySA+.

OBJECTIFS PÉDAGOGIQUES

- Développer les compétences d'un analyste en cybersécurité capable de surveiller, analyser et répondre aux menaces dans des environnements IT modernes.
- Savoir mettre en œuvre des techniques de détection proactive des attaques et utiliser des outils comme SIEM, EDR/XDR.
- Analyser les vulnérabilités et proposer des stratégies d'atténuation efficaces.
- Concevoir et exécuter une réponse aux incidents suivie d'une communication claire des résultats.
- Préparer et optimiser la réussite de l'examen officiel CompTIA CySA+ (CS0-003 ou version la plus récente) grâce à des exercices pratiques et des cas réels.

PRÉREQUIS

- Avoir suivi les formations CompTIA Network+ et Security+ ou posséder des connaissances équivalentes en réseaux et sécurité.
- Expérience pratique d'environ 4 ans en tant qu'analyste SOC ou dans des fonctions similaires en cybersécurité.
- Un entretien préalable permet d'ajuster le programme selon le profil et les objectifs professionnels du participant.

PUBLIC VISÉ

- Analystes SOC, analystes sécurité, ingénieurs cybersécurité ou toute personne en charge de la surveillance et de la réponse aux menaces dans une organisation.
- Professionnels IT expérimentés souhaitant se certifier sur l'analyse de la cybersécurité et la défense proactive.

PROGRAMME DÉTAILLÉ

Module 1 — Opérations de sécurité

- Architecture de systèmes et réseau liés à la sécurité.
- Analyse des indicateurs d'activités malveillantes et des événements SIEM.
- Concepts avancés de threat hunting et renseignement sur les menaces.

Module 2 — Réponse aux incidents

- Principes de cycle de vie de la gestion des incidents.
- Techniques de réponse opérationnelle (IDS, EDR, capture de preuves).
- Post-incident : leçons, remédiation et amélioration continue.

Module 3 — Gestion des vulnérabilités

- Mise en œuvre de scans de vulnérabilités.
- Analyse des résultats, priorisation des risques et mise en place de contrôles.
- Stratégies d'atténuation des vulnérabilités.

Module 4 — Reporting et communication

- Génération de rapports de sécurité clairs et exploitables.
- Communication avec les équipes IT, les décideurs et les parties prenantes.

Module 5 — Préparation à l'examen CompTIA CySA+

- Exercices pratiques, QCM et simulations basées sur des scénarios réels.
- Révision des domaines clés de l'examen.

MODALITÉS PÉDAGOGIQUES

Format et déroulement

MFE-IT privilégie un format en mini-groupe (1 à 3 participants), garanti dès un seul inscrit (sauf cas de force majeure). La formation se déroule en distanciel (classe virtuelle synchrone, sessions également enregistrées) ou en présentiel dans vos locaux. Le programme alterne apports théoriques, ateliers pratiques et simulations d'examen.

Format ultra-personnalisé

Un entretien préalable est organisé avec le participant et/ou un représentant de l'entreprise afin d'adapter le contenu à son niveau, à ses besoins et à ses enjeux professionnels.

Moyens techniques

Un support pédagogique complet est remis à chaque participant. Les sessions s'appuient sur des labs (SIEM/EDR), des QCM et des simulations d'examen. Une connexion internet et un poste de travail sont requis pour les sessions à distance.

Évaluation des acquis

Tout au long de la formation, le formateur évalue la progression des participants au moyen de quiz, de mises en situation et de simulations d'examen. Une attestation de fin de formation est remise à l'issue du parcours.

Accessibilité et handicap

Nos formations peuvent être adaptées aux personnes en situation de handicap. Merci de nous contacter en amont afin d'étudier ensemble les modalités d'accueil et d'aménagement (référent handicap : contact@mfe-it.com).

Assistance post-formation

Chaque participant bénéficie d'un accompagnement de 30 jours après la formation pour toute question relative au contenu abordé.

INFORMATIONS PRATIQUES

Prise en compte du handicap

MFE-IT s'engage à étudier toute demande d'aménagement. Un échange avec notre référent handicap permet d'adapter les conditions d'accueil et de déroulement de la formation.

Modalités pédagogiques et techniques

Formation en distanciel (classe virtuelle synchrone) ou en présentiel dans vos locaux, en mini-groupe. Alternance de théorie, d'ateliers pratiques et de simulations d'examen.

Moyens du formateur

Formateur expert certifié, support de cours complet, labs (SIEM/EDR) et simulations d'examen.

Validation et sanction

Attestation de fin de formation. Cette formation inclut le passage de l'examen officiel CompTIA CySA+ (CS0-003).

Type de formation

Action de formation professionnelle continue : acquisition et perfectionnement de compétences.

Suivi de l'exécution

Feuilles de présence signées, évaluations en cours de formation et attestation de fin de formation.

Modalités d'évaluation

Quiz, mises en situation, QCM et simulations d'examen tout au long de la formation.

Aide à l'orientation

La CompTIA CySA+ prolonge le parcours cybersécurité après les certifications CompTIA Network+ et Security+.