

Mis à jour le 13/06/2025

S'inscrire

Formation Digital Forensics & Incident Response

4 jours (28 heures)

PRÉSENTATION

Notre formation DFIR vous permettra de maîtriser les techniques essentielles pour gérer efficacement les incidents informatiques complexes et réaliser des analyses forensiques approfondies. Cette formation couvre en détail les méthodologies et outils avancés adaptés aux environnements modernes et variés tels que les systèmes Windows, les infrastructures réseau, et les plateformes SIEM.

Dans cette formation, spécialement conçue pour les analystes en sécurité avancés, les administrateurs systèmes et réseaux expérimentés, ainsi que les responsables et consultants en sécurité informatique chargés d'investiguer, de répondre et de prévenir les incidents complexes.

À travers des conférences détaillées et une série d'ateliers pratiques réalistes, vous développerez une expertise opérationnelle directe sur les méthodes avancées d'analyse des artefacts, d'investigation réseau, de Threat Hunting proactif et de gestion de crise. Vous apprendrez aussi à intégrer ces compétences dans un cadre opérationnel structuré et à produire des rapports professionnels d'incidents.

Comme dans toutes nos formations, celle-ci est actualisée en permanence afin de refléter les dernières évolutions en matière de DFIR.

Objectifs

- Expliquer en détail les concepts avancés et les méthodologies DFIR
- Structurer efficacement une équipe DFIR avancée et gérer les incidents complexes
- Maîtriser l'utilisation et l'intégration des outils DFIR avancés
- Identifier et analyser en profondeur les artefacts système et réseau avancés
- Mettre en œuvre des techniques avancées d'analyse de mémoire et de logs
- Automatiser les processus d'investigation et de réponse aux incidents
- Déployer des méthodologies avancées de Threat Hunting proactif
- Gérer efficacement les crises et coordonner les équipes multidisciplinaires
- Rédiger des rapports d'incident détaillés et professionnels

- Implémenter des stratégies proactives de prévention et de réponse aux incidents

Public visé

- Professionnels iT
- Administrateurs systèmes
- Administrateurs réseau
- Ingénieurs DevOps
- Analystes en sécurité

Pré-requis

- Connaissance préalable des concepts fondamentaux de la cybersécurité
- Expérience pratique dans l'utilisation d'outils forensiques de base
- Familiarité avec les systèmes d'exploitation Windows et réseaux TCP/IP
- Compétences basiques en scripting (Python, PowerShell ou Bash)

Programme de notre formation DFIR

Jour 1 : Introduction avancée au DFIR

Concepts et Méthodologies avancés

- Rappels essentiels des concepts fondamentaux du DFIR
- Structuration et rôles au sein d'une équipe DFIR avancée
- Méthodes avancées de gestion des incidents complexes
- Techniques de priorisation et de gestion des ressources
- Atelier pratique : Mise en place et configuration d'un environnement DFIR avancé

Outils et Cas pratiques avancés

- Présentation et sélection des outils DFIR de pointe
- Intégration d'outils et automatisation dans les workflows DFIR
- Étude approfondie d'incidents réels complexes
- Atelier pratique : Simulation et analyse d'un incident réel complexe
- Bonnes pratiques en sécurité opérationnelle et prévention

Jour 2 : Analyse forensique avancée des systèmes Windows

Artefacts et mémoire avancée

- Identification avancée et extraction des artefacts Windows

- Analyse poussée du registre et des Event Logs
- Atelier pratique : Analyse approfondie de la mémoire RAM
- Utilisation des frameworks Volatility et Rekall
- Techniques avancées de détection d'activités malicieuses

Techniques avancées d'analyse de logs

- Exploitation avancée de Sysmon et Event Tracing
- Détection d'activités suspectes et attaques ciblées
- Atelier pratique : Extraction et analyse des logs avancés
- Investigation des techniques d'attaque (lateral movement, persistance, credential dumping)
- Méthodes avancées d'automatisation des analyses

Frameworks avancés et scripting

- Présentation approfondie de KAPE
- Scripting et automatisation pour accélérer les investigations
- Atelier pratique : Écriture de scripts de collecte d'artefacts
- Optimisation des workflows d'analyse
- Techniques de validation d'intégrité et de preuves forensiques

Jour 3 : Analyse réseau et Threat Hunting avancés

Capture et analyse approfondie du trafic réseau

- Techniques avancées d'analyse de captures PCAP
- Utilisation avancée de Zeek et Suricata
- Atelier pratique : Identification approfondie de menaces réseau
- Détection d'activités malveillantes par l'analyse comportementale
- Identification et analyse d'anomalies réseau

Threat Hunting proactif et automatisation

- Méthodologies avancées de Threat Hunting
- Automatisation et scripting avancés en Threat Hunting
- Atelier pratique : Chasse proactive des menaces en temps réel
- Utilisation avancée des plateformes SIEM
- Stratégies de veille technologique et de renseignement sur les menaces

Réponse proactive et outils de prévention

- Techniques avancées de réponse proactive aux incidents
- Intégration proactive DFIR dans les politiques de sécurité
- Atelier pratique : Mise en œuvre d'une réponse proactive automatisée
- Prévention proactive et amélioration continue

- Bonnes pratiques d'intégration DFIR dans les opérations IT

Jour 4 : Gestion avancée des incidents et rédaction des rapports

Coordination et gestion de crise

- Techniques avancées de gestion de crise
- Coordination des équipes multidisciplinaires
- Atelier pratique : Simulation d'une gestion de crise en temps réel
- Communication efficace et gestion des parties prenantes
- Techniques de contrôle des dommages et de restauration

Documentation et rétro-ingénierie

- Techniques avancées de rédaction de rapports DFIR
- Atelier pratique : Élaboration d'un rapport d'incident détaillé
- Techniques rapides de rétro-ingénierie de malware
- Optimisation des processus post-incident
- Intégration des retours d'expérience pour améliorer les processus DFIR

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.