Inforensique sur équipement mobile – perfectionnement et expert

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Investigation, réponses à incidents

Rubrique : Investigation numérique - inforensic

Code de formation : IEM2

PRÉSENTATION

Objectifs & compétences

Objectifs & compétences

À l'issue de la formation, les participants seront capables de :

- Réaliser des acquisitions avancées sur terminaux Android et iOS.
- Exploiter les systèmes de fichiers mobiles et leurs artefacts.
- Analyser les applications de communication et de réseaux sociaux.
- Extraire et interpréter des données supprimées ou cachées.
- Construire une chronologie détaillée des événements.
- Identifier des indicateurs de compromission et des traces de logiciels malveillants mobiles.
- Produire un rapport d'expertise technique conforme aux bonnes pratiques forensic.
- Conduire une investigation mobile complexe dans un contexte d'incident de sécurité ou d'enquête judiciaire.

Public visé

Analystes forensic, Répondants à incidents, Experts cybersécurité, Enquêteurs numériques, Auditeurs techniques, Investigateurs judiciaires

Pré-requis

Prérequis :

- Avoir suivi la formation IEM1 – Initiation ou disposer de connaissances équivalentes.
- Connaissances fondamentales d'Android et d'iOS.
- Maîtrise des principes de préservation de la preuve numérique.

Avoir suivi la formation IEM1 – Initiation ou disposer de connaissances équivalentes.
Connaissances fondamentales d'Android et d'iOS.
Maîtrise des principes de préservation de la preuve numérique. [Réf_IEM1_I...initiation | PDF], [intelligen...rityit.com]

PROGRAMME

Jour 1 – Acquisition avancée et architecture des terminaux mobiles

• Évolution des mécanismes de sécurité mobiles

- Architecture Android récente
- Architecture iOS récente
- Chiffrement des données
- Secure Enclave
- Android Keystore
- Trusted Execution Environment (TEE)

€ Tarifs

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 21 heures

Rythme : 3 jours. 6 au 8 Octobre 20262 au 4 Décembre 2026

Délai d'accès : Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

- **Acquisition avancée des données**

- Acquisition logique
- Acquisition système de fichiers
- Acquisition physique : possibilités et limites
- Collecte des sauvegardes locales et cloud
- Extraction des données chiffrées

- **Préservation de la preuve**

- Gestion des terminaux verrouillés
- Intégrité et traçabilité des données
- Vérification des empreintes numériques
- Documentation des opérations d'acquisition

- **Travaux pratiques**

- Acquisition complète d'un smartphone Android
- Acquisition complète d'un iPhone
- Contrôle d'intégrité des données acquises

Jour 2 – Analyse approfondie des artefacts et récupération de données

- **Analyse des artefacts utilisateurs**

- SMS, MMS et appels
- Carnets d'adresses
- Historique de navigation
- Courriels
- Calendriers et notes

- **Analyse des applications de messagerie**

- WhatsApp
- Signal
- Telegram
- Messenger
- Teams et applications professionnelles

- **Analyse des données de localisation**

- Géolocalisation GPS
- Réseaux Wi-Fi
- Bluetooth
- Antennes cellulaires

- **Analyse multimédia avancée**

- Métadonnées EXIF
- Miniatures
- Historique des modifications
- Recherche de contenus supprimés

- **Exploitation des bases SQLite**

- Structure des bases de données mobiles
- Analyse des journaux applicatifs
- Reconstruction d'activités utilisateur

- **Travaux pratiques**

- Extraction d'artefacts à partir d'applications réelles
- Récupération de données supprimées
- Reconstitution des actions d'un utilisateur
- Indicateurs de compromission (IOC)

Jour 3 – Investigation experte, détection de compromission et restitution

- **Investigation avancée**

- Corrélation des traces système et applicatives
- Construction d'une timeline complète
- Analyse comportementale utilisateur

- **Détection de compromission mobile**

- Introduction aux malwares mobiles

- Spyware et stalkerware
- Applications malveillantes dissimulées
- Recherche d'indicateurs de compromission (IOC)

- **Investigation dans un contexte de cyberattaque**

- Exfiltration de données
- Vol d'identifiants
- Compromission d'applications mobiles
- Analyse des traces de persistance

- **Étude de cas expert**

Les participants réalisent une investigation complète comprenant :

- Acquisition des données
- Analyse technique
- Corrélation des événements
- Recherche d'indices de compromission
- Reconstruction chronologique
- Identification des actions de l'utilisateur et de l'attaquant

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise

Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT, Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex Teams

Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels

Méthode

Fin de formation : entretien individuel
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation
Assiduité : certificat de réalisation (validation des acquis)