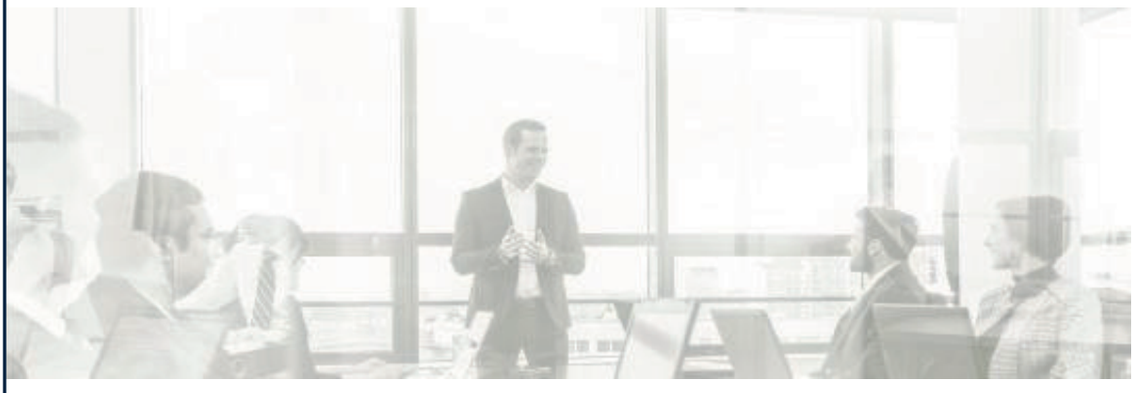
Catalogue des formations



Nos formations

- Veille sur internet
- Cybersécurité
- Big Data
- Data science et Intelligence Artificielle

Choisir H-Intelligence pour vous assurer de l'efficacité de votre formation !

Qui sommes-nous ?

- Hamis Intelligence est une entreprise de conseil et de formation créée en 2017, à Roissy en France.
- Nous proposons des formations sur la Veille et l'Intelligence Economique, la Cybersécurité, le Big Data, la Data science et l'Intelligence Artificielle et, enfin, nous proposons des formations « sur-mesure » en langues étrangères destinées aux entreprises.
- Toutes nos formations sont dispensées en présentiel car le contact humain et le partage direct entre formateurs et stagiaires nous semblent essentiel. Les formations peuvent se dérouler, selon vos souhaits, en inter ou intra-entreprises. Nous disposons de plusieurs salles de formation à Villepinte, dans le Parc d'activité de Paris Nord 2, à deux pas du RER.

Nos choix pédagogiques

- Les enseignements dispensés ont été conçus et développés avec des formateurs spécialistes ayant tous au minimum 7 ans d'expérience dans leurs domaines de compétences.
- Nos formations font l'objet d'une pré-évaluation, par questionnaire, des connaissances et des besoins précis de chaque stagiaire, et ce, plusieurs semaines avant la formation et par une vérification de niveau, en début de stage, par le formateur.
- Ces étapes peuvent être précédées d'un échange avec le Responsable Formation ou le RRH de l'entreprise, ainsi qu'avec le Responsable hiérarchique « Métier » du ou des futurs stagiaires le cas échéant.
- La transmission de la connaissance ne tient pas uniquement dans l'information donnée. L'empathie du formateur, la reformulation dont il constate la nécessité en observant son ou ses stagiaires, sont des vecteurs uniques de la bonne compréhension, de la mémorisation et de la réussite du stagiaire.

Nos pratiques

- Durant nos formations, chaque stagiaire dispose d'un poste informatique propre. Le matériel utilisé est de dernière génération, équipé des environnements Windows et Linux. Pour l'organisation des formations intra-entreprises dans vos locaux, le matériel devra être fourni par vos soins. Nous vous offrons, néanmoins, la possibilité de vous mettre à disposition le matériel sur devis.
- À l'issue de chaque formation, les participants reçoivent un support formation numérique. Une assistance mail est proposée à l'issue de nos stages pratiques.

Notre équipe est à votre disposition pour répondre à toutes vos problématiques spécifiques car

Pour vous comme pour nous, chaque client est unique !

FORMATIONS

CYBERSECURITE

Les fondamentaux

Protection des systèmes et des réseaux

Intrusion et vulnérabilités

Cybercriminalité et investigation numérique

CYBERSECURITE

Les fondamentaux

Sensibilisation à la cybersécurité

INFOS PRATIQUES

- **Réf :** SCS
- **Durée :** 1 jour
- **Prix :** 690€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 27 mai 2019
- 01 juillet 2019
- 18 novembre 2019

PUBLIC VISE

- Toute personne souhaitant comprendre les menaces et les enjeux liés à la cybersécurité

PRÉ-REQUIS

- Aucun

RESSOURCES

- Supports pédagogiques
- 70% de théorie et de présentation
- 30% de pratique
- 1 PC par personne / Internet

OBJECTIFS :

- Découvrir la sécurité informatique : Les risques, les menaces
- Comprendre ce que sont les attaques informatiques et leurs conséquences
- Identifier les mesures de protection de l'information
- Apprendre les bonnes pratiques nécessaires à la protection de ses données

PROGRAMME DE FORMATION:

Qu'est-ce que la sécurité en informatique ?

- Dimensions et critères CIADN

Typologie des risques

- Accès physique
- Interception de communications
- Dénis de service
- Intrusions
- Ingénierie sociale

Quelques exemples historiques

- Menaces et outils du quotidien : mots et phrases de passe, logiciels de chiffrement, tunnels VPN

Focus pratique sur l'ingénierie sociale

- Le phishing

Atelier : construction d'un modèle de menace simple

Les bonnes pratiques pour se protéger

- Les logiciels
- La gestion des accès
- La réaction face aux anomalies

Focus pratique sur un logiciel de chiffrement : Veracrypt

Introduction à la sécurité informatique

INFOS PRATIQUES

- **Réf :** ISI
- **Durée :** 2 jours
- **Prix :** 1270€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 06 et 07 mai 2019
- 03 et 04 juillet 2019
- 20 et 21 novembre 2019

PUBLIC VISE

- Toute personne intéressée par la sécurité informatique

PRÉ-REQUIS

- Bonnes connaissances des communications en réseau

RESSOURCES

- Supports pédagogiques
- 60% de théorie et de présentation
- 40% de pratique
- 1 PC par personne / Internet

OBJECTIFS :

- Connaître et comprendre les attaques qui pèsent sur un système d'information
- Découvrir les principaux équipements de sécurité et leurs rôles
- Identifier les vulnérabilités
- Savoir mettre en œuvre les outils de base à la sécurisation des réseaux

PROGRAMME DE FORMATION:

Qu'est-ce que la sécurité en informatique ?

- Dimensions et critères CIADN

Typologie des risques

- Accès physique
- Interception de communications
- Dénis de service
- Intrusions
- Ingénierie sociale

Équipements de sécurité

- Terminal client
- Switch
- Routeur (filtrant)

Défense en profondeur

- Pare-feu
- NIDS

Atelier : mise en place d'un pare-feu logiciel open-source

Catégories d'attaque

- Niveau Machine hôte (Virus, Vers, Malware)
- Niveau Réseau (Botnet)
- Niveau Applicatif (Injections)

Le déni de service

- Du DOS au DDOS

L'intrusion

- Exemple de l'injection SQL

APT et escalade de privilèges

- Exemples historiques

Atelier : crack de mot de passe

CYBERSECURITE

Protection des systèmes et des réseaux

Sécurité des systèmes et des réseaux NIVEAU 1 – Débutant

INFOS PRATIQUES

- **Réf :** SSR
- **Durée :** 3 jours
- **Prix :** 1980€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 15 au 17 mai 2019
- 11 au 13 septembre 2019
- 12 au 14 novembre 2019

PUBLIC VISE

- Techniciens / administrateurs systèmes et réseaux
- RSSI
- Ingénieurs

PRÉ-REQUIS

- Bonnes connaissances en systèmes et réseaux

RESSOURCES

- Supports pédagogiques
- 40% de théorie et de présentation
- 60% de pratique
- 1 PC par personne / Internet

OBJECTIFS :

- Connaître et comprendre les attaques qui pèsent sur un système d'information
- Découvrir les principaux équipements de sécurité et leurs rôles
- Identifier les vulnérabilités
- Créer et organiser une architecture de sécurité efficace
- Mettre en œuvre les outils de base nécessaires à la sécurisation des réseaux

PROGRAMME DE FORMATION:

Contexte et enjeux

- Introduction à la sécurité.
- Etat des lieux de la sécurité informatique.

Risques et menaces

- Attaques "couches basses".
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP-SYNflood, SMURF, etc.
- Déni de service et déni de service distribué.
- Attaques applicatives.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- DNS

La terminologie de la sécurité.

- Vulnérabilités
- Attaques (exploits)
- Contre-mesures
- Menaces

Cartographie de la SSI

- Cartographie du système d'information
- Cartographie des risques

Famille des normes ISO 27000

- ISO 2700x

La gestion de la sécurité des systèmes d'information et des réseaux

- Sécurité des données
- Sécurité des échanges
- Sécuriser un système, le « hardening »

Contrôle interne et audit lié à la SSI

- Les outils et techniques disponibles.
- Tests d'intrusion : outils et moyens
- Impacts organisationnels
- Veille technologique

Diagnostique des vulnérabilités

- Détection des vulnérabilités (scanners, sondes IDS, etc.).
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure.

Identification des mesures de sécurité

- Réagir efficacement en toutes circonstances.
- Supervision et administration

Plan d'actions de la sécurité

Sécurité des systèmes et des réseaux NIVEAU 2 – Avancé

INFOS PRATIQUES

- **Réf :** SSRA
- **Durée :** 4 jours
- **Prix :** 2380€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 03 au 06 juin 2019
- 23 et 26 septembre 2019
- 25 au 28 novembre 2019

PUBLIC VISE

- Techniciens / administrateurs
- Architectes sécurité
- Ingénieurs
- RSSI / DSI
- Consultants

PRÉ-REQUIS

- Bonnes connaissances en systèmes et réseaux
- TCP/IP
- Administration Windows / Linux

RESSOURCES

- Supports pédagogiques
- 30% de théorie
- 70% de pratique
- 1 PC par personne / Internet / Environnement Windows et Linux

OBJECTIFS :

- Identifier et comprendre les attaques qui pèsent sur un système d'information
- Maîtriser les principaux équipements de sécurité et leurs rôles
- Vérifier le niveau de sécurité du système d'information
- Connaître les principales méthodes d'audit, de détection et d'intrusions
- Corriger les vulnérabilités
- Mettre en œuvre les outils adaptés à la sécurisation des réseaux

PROGRAMME DE FORMATION:

Rappels

- Protocole TCP/IP
- Architecture des réseaux
- Firewall
- Proxys et reverse-proxy
- DMZ.

Les outils d'attaque

- Appréhension des outils d'attaques des SI et aide à la gestion pour les SI.
- Définition de la politique de la sécurité des SI

La cryptographie, application

- Historique
- Rôle et responsabilité de la Cryptographie symétrique et asymétrique
- Gestion des algorithmes
- Certificat
- Hachage
- Clé de sessions

Architecture AAA liée aux routeurs ou NAS

- Protocoles RADIUS, Diameter, TACACS, TACACS+

Détection d'intrusions

- Définition
- Mise en œuvre des outils de tests d'intrusion

Vérification de l'intégrité du système

- Méthode pour pouvoir s'assurer que l'intégrité du Système d'Information est maintenue

Gestion des événements de sécurité

- Méthode SIEM (Security Information and Event Management)

Sécurisation des réseaux Wifi.

- Méthodologie pour pouvoir s'assurer que le WIFI est protégé

Sécurisation de la téléphonie sur IP

- Mise en place de la voix sur IP au sein du SI sans compromettre la véracité du SI

Sécurisation de la messagerie

- Méthodologie
- Mise en œuvre
- Eviter les attaques de votre SI

Sécurité des systèmes et des réseaux NIVEAU 3 – Expert

INFOS PRATIQUES

- **Réf :** SSRE
- **Durée :** 5 jours
- **Prix :** 3170€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- Sur demande

PUBLIC VISE

- Techniciens / administrateurs
- Architectes sécurité
- Ingénieurs
- Consultants
- Développeurs

PRÉ-REQUIS

- Connaissances équivalentes à celles du stage SSRA
- TCP/IP
- Administration Windows / Linux
- Notions de Hacking
- Bonnes connaissances en programmation

RESSOURCES

- Supports pédagogiques
- 30% de théorie et de présentation
- 70% de pratique
- 1 PC par personne / Internet / Environnement Windows et Linux

OBJECTIFS :

- Connaître et comprendre les attaques des pirates informatiques
- Evaluer le niveau de sécurité du système d'information
- Créer et organiser un test de pénétration
- Corriger les vulnérabilités
- Maîtriser les méthodes de sécurité avancées pour contrer les attaques

PROGRAMME DE FORMATION:

Réseau

- Techniques de scan
- Détection de filtrage
- Plan d'infrastructure
- Forger les paquets
- Sniffer les paquets

Système

- Metasploit
- Attaques d'un service à distance
- Attaque d'un client et bypass d'antivirus
- Utilisation du Meterpreter
- Attaque d'un réseau Microsoft

Web

- Infrastructure et technologies associées
- Recherche des vulnérabilités

Applicatif

- Shellcoding Linux
- Buffer Overflow avancé sous Linux

TP FINAL

CYBERSECURITE

Intrusion et vulnérabilités

Audit et test d'intrusion - PENTEST

INFOS PRATIQUES

- **Réf :** TIA
- **Durée :** 4 jours
- **Prix :** 2480€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :
- 02 au 05 avril 2019
- 17 au 20 juin 2019
- 17 au 20 septembre 2019

PUBLIC VISE

- Techniciens / administrateurs
- Architectes sécurité
- Ingénieurs
- Consultants
- Développeurs

PRÉ-REQUIS

- Connaissances équivalentes à celles du stage SSRA
- Expérience requise

RESSOURCES

- Supports pédagogiques
- 40% de théorie et de présentation
- 60% de pratique
- 1 PC par personne / Internet / Environnement Windows et Linux

OBJECTIFS :

- Connaître la méthodologie de mise en place d'un audit de sécurité de type test de pénétration sur un système d'information (PENTEST)
- Savoir rédiger un rapport final d'audit
- Émettre des recommandations de sécurité selon les résultats des tests

PROGRAMME DE FORMATION:

Éléments théoriques et reconnaissance

Qu'est-ce que la sécurité en informatique ?
- Dimensions et critères CIADN

Typologie des risques
- Accès physique
- Interception de communications
- Dénis de service
- Intrusions
- Ingénierie sociale

Les 5 phases du hacking
- Reconnaissance
- Analyse
- Exploitation
- Maintien de l'accès
- Couverture des traces

Les différents types de pentest et leur périmètre
- Poste client
- Réseau
- Serveur
- Applicatif web

La récolte d'informations ouvertes (doxing)
- Méthodologie
- Outils
- Cadre légal

Atelier : scan de port et reconnaissance d'empreintes avec Nmap

Les protocoles réseaux

- TCP/IP
- OSI

Sniffing de mot de passe

- Analyse réseau avec Wireshark

Interception de données

- Attaque MITM avec Ettercap

Déni de service

- Montage d'attaque avec Scapy

Attaque système, attaque physique, attaque d'ingénierie sociale

Les protocoles de chiffrement de données

- Tour d'horizon
- Attaques sur les implémentations et configurations

Atelier : crack de mot de passe (guessing, dictionnaires, rainbow tables)

Attaque physique

- Linux
- Windows

Techniques d'ingénierie sociale

- Tailgating
- Usurpation téléphonique
- Phishing

Rédiger un rapport et émettre des recommandations

Les différents types de rapports

- Business
- Stratégique
- Technique

L'évaluation des risques selon OWASP

- Top 10

Les fondamentaux de la communication

- Savoir présenter
- Savoir synthétiser
- Savoir proposer

Détection d'intrusion

INFOS PRATIQUES

- **Réf :** DEI
- **Durée :** 4 jours
- **Prix :** 2380€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 25 au 28 juin 2019
- 28 au 31 octobre 2019
- 09 au 12 décembre 2019

PUBLIC VISE

- Techniciens / administrateurs
- Architectes sécurité
- RSSI

PRÉ-REQUIS

- Connaissances équivalentes à celles du stage SSRA
- TCP/IP
- Connaissance des environnements Windows et Linux

RESSOURCES

- Supports pédagogiques
- 30% de théorie et de présentation
- 70% de pratique
- 1 PC par personne / Internet / Environnement Windows et Linux

OBJECTIFS :

- Connaître et comprendre les différentes méthodes d'analyse et de détection
- Identifier et mettre en œuvre les outils de prévention et de détection d'intrusion
- Etre en mesure d'apporter des solutions adaptées aux différents types d'intrusion (cadre juridique lié, comment gérer un incident d'intrusion…)

PROGRAMME DE FORMATION:

Utilité et mise en place des systèmes de détection d'intrusions

Travaux pratiques : Les menaces existantes à contrer

Problèmes de sécurité de TCP/IP et comment y remédier

Principes de la recherche des vulnérabilités, outils de détection d'intrusions et de vulnérabilité :

- Logiciels libres
- Logiciels commerciaux
- Exemples d'utilisation (TCPdump, Wiresharck, Snort, Kali, Nessus, DenyAll et Nikto)

Architecture d'un système de détection d'intrusions :

- Comparaison de IDS vs IPS

Erreurs à éviter

- Les faux positifs
- Les faux négatifs

Permettre l'aide à la mise en place de la Politique de Sécurité

Protection des serveurs et des postes de travail

- Sécurisation de votre infrastructure (Intérêt de l'audit)

Analyse de traces commentées

- Maîtriser l'analyse des traces
- Corriger les failles constatées

Principe des autopsies (Inforensique)

- Analyser les failles
- Vérifier l'impact sur le système d'information

Gestion des incidents de sécurité

- Plan d'action afin de se préparer à réagir après une intrusion.
- Mise en place de la politique en sécurité du SI à destination du DSI ou du RSSI

Gestion et analyse de la mise en place d'un système de détection d'intrusions

Travaux pratiques : Analyses de traces

Auditer son site web

INFOS PRATIQUES

- **Réf :** ASW
- **Durée :** 3 jours
- **Prix :** 1980€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 16 au 18 avril 2019
- 22 au 24 octobre 2019

PUBLIC VISE

- Techniciens / administrateurs
- Ingénieurs
- Consultants
- Développeurs

PRÉ-REQUIS

- Connaissances équivalentes à celles du stage SSRA
- Connaissance des langages de développement
- Administration Windows / Linux

RESSOURCES

- Supports pédagogiques
- 40% de théorie et de présentation
- 60% de pratique
- 1 PC par personne / Internet / Environnement Windows et Linux

OBJECTIFS :

- Détecter et comprendre les vulnérabilités d'un site web
- Contrôler la sécurité de ses propres applications web
- Organiser la sécurisation des applications web grâce à des mesures de base

PROGRAMME DE FORMATION:

Éléments théoriques et reconnaissance

Les 5 phases du hacking

- Reconnaissance
- Analyse
- Exploitation
- Maintien de l'accès
- Couverture des traces

Les différents types de pentest et leur périmètre

- Poste client
- Réseau
- Serveur
- Applicatif web

La récolte d'informations ouvertes (doxing)

- Méthodologie
- Outils
- Cadre légal

Atelier : TheHarvester

Travaux pratiques : scan de port et reconnaissance d'empreintes avec Nmap

Failles applicatives

La sécurité web aujourd'hui

- Les menaces actuelles selon OWASP

L'injection SQL

- Le mécanisme de l'attaque
- Contourner l'échappement

Mécanismes des failles web

- Remote File Inclusion (RFI)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

Exploiter des ressources CVE

- Méthodes de recherche
- Apprécier la criticité

Autres failles

Les failles niveau Transport

- L'attaque DOS
- L’attaque DDOS

La faille humaine

- Exemples de fuites d'informations confidentielles
- L’ingénierie sociale

Atelier : outil d'audit de CMS Wordpress

CYBERSECURITE

Cybercriminalité et investigation numérique

Introduction à la cybercriminalité

INFOS PRATIQUES

- **Réf :** ILC
- **Durée :** 1 jour
- **Prix :** 780€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- Sur demande

PUBLIC VISE

- DSI / RSSI
- Risk Manager
- Techniciens informatiques

PRÉ-REQUIS

- Aucun

RESSOURCES

- Supports pédagogiques
- 1 PC par personne
- Internet

OBJECTIFS :

- Identifier et comprendre les risques et les menaces liés à la cybercriminalité
- Connaître les différents acteurs
- Appréhender l'aspect législatif français lié à la cybercriminalité

PROGRAMME DE FORMATION:

Qu'est-ce que la cybercriminalité ?

- Définition
- Enjeux
- Acteurs
- Usages

Les acteurs de la lutte contre la cybercriminalité

- Gendarmerie nationale (IRCGN)
- Police nationale (OCLCTIC)
- Tracfin
- Douanes
- Agence de confiscation des avoirs criminels
- Préfecture de police (BEFTI)

Législation

- Loi informatique et libertés
- Règlement général sur la protection des données (RGPD)
- Le rôle de la CNIL

Qu'est-ce que l'investigation numérique ?

- Définition
- Méthodes
- Outils

Réponse en cas d'attaque

- Quelle réaction avoir ?
- Collecte de preuves
- Etablissement des constatations
- Investigation numérique
- Actions judiciaires à mettre en œuvre

Analyse forensique – Les fondamentaux

INFOS PRATIQUES

- **Réf :** AIF
- **Durée :** 2 jours
- **Prix :** 1370€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 20 et 21 mai 2019
- 17 et 18 octobre 2019

PUBLIC VISE

- Responsables sécurité
- Professionnels de l'investigation légale
- Ingénieurs / administrateurs système

PRÉ-REQUIS

- Connaissance générale des attaques et vulnérabilités
- Connaissances de base en sécurité informatique
- Bonnes connaissances en réseaux et systèmes

RESSOURCES

- Supports pédagogiques
- 40% de théorie
- 60% de pratique
- 1 PC par personne / Internet
- Environnement Windows et Linux

OBJECTIFS :

- Connaître les procédures en cas d'intrusion sur un matériel
- Collecter les preuves et veiller à leur intégrité
- Analyser, à postériori, les empreintes numériques laissées

PROGRAMME DE FORMATION:

Introduction à l'analyse forensique

Forensique réseau

- Les différentes évidences réseau
- Capture et analyse de pcap
- Investigation sur les logs systèmes
- Investigation sur les logs réseaux (proxy, firewall, waf…)
- Analyse des logs IDS/IPS

Investigation live forensique

- Analyse de processus
- Analyse des points d'auto démarrage
- Acquisition de preuves
- Scripts et outils de live forensique

Analyse de la mémoire

- Méthodes de dump de ram sur Windows & Linux
- Fonctionnement de la mémoire
- Architecture de la mémoire
- Prise en main de l'outil Volatility

Analyse de systèmes de fichiers

- Méthodes de dump de disque
- Notion de système de fichier
- Découverte des artéfacts Windows
- Forensique et chiffrement
- Carving

Analyse forensique avancée et réponse à incidents

INFOS PRATIQUES

- **Réf :** AIA
- **Durée :** 4 jours
- **Prix :** 2470€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 04 au 07 juin 2019
- 03 au 06 décembre 2019

PUBLIC VISE

- Responsables sécurité
- Professionnels de l'investigation légale
- Ingénieurs / administrateurs système

PRÉ-REQUIS

- Connaissance générale des attaques et vulnérabilités
- Bonnes connaissances en sécurité informatique
- Bonnes connaissances en réseaux et systèmes

RESSOURCES

- Supports pédagogiques
- 30% de théorie
- 70% de pratique
- 1 PC par personne / Internet
- Environnement Windows et Linux

OBJECTIFS :

- Maîtriser les procédures en cas d'intrusion sur un matériel
- Collecter les preuves et veiller à leur intégrité
- Etre en mesure d'identifier et d'analyser, à postériori, les empreintes numériques laissées

PROGRAMME DE FORMATION:

Introduction à l'analyse Inforensique

Gestion des incidents

- Préparation : outillages, techniques et procédure de gestion des incidents
- Détection et analyse des incidents cybersécurité
- Threat hunting et Threat intelligence

Analyse live Inforensique

- Concept et intérêt du live inforensique
- Détection de présence de malware
- Détection d'intrusion
- Prise en main des outils SysInternals

Méthode de récolte de preuve : dump de ram et de disque

- Méthode de récolte de preuve inforensique
- Respect de la chaîne de confiance
- Dump de ram : dumpit, fmem, lime, FTK Imager
- Dump disque : dd, dcfldd, FTK Imager

Analyse de la mémoire

- Fonctionnement de la mémoire
- Architecture de la mémoire
- Identification de processus malveillants
- Analyse des artefacts réseau
- Détection et analyse d'injection de code
- Détection et analyse de rootkit
- Récupération de fichiers et informations présentes en mémoire
- Prise en main de l'outil Volatility

Analyse du système de fichier

- Découverte des artefacts Windows
- Volume Shadow Copy
- Organisation des systèmes de fichiers NTFS, FAT32, EXT3 et ET4
- Création et analyse de timeline avec TheSleuthit (TSK)
- Création et analyse de supertimeline avec Plaso
- Etudes des différentes méthodes de carving

Détection, identification et élimination des malwares

INFOS PRATIQUES

- **Réf :** MAL
- **Durée :** 3 jours
- **Prix :** 2080€ HT
- **Horaires :** 09h00 – 17h30

DATES 2019

Formations :

- 24 au 26 juin 2019
- 28 au 30 octobre 2019

PUBLIC VISE

- Responsables gestion incident
- Techniciens réponse incident
- Auditeurs techniques
- Analystes de sécurité

PRÉ-REQUIS

- Bonnes connaissances du Système Microsoft Windows

RESSOURCES

- Supports pédagogiques
- 30% de théorie
- 70% de pratique
- 1 PC par personne / Internet
- Environnement Windows et Linux

OBJECTIFS :

- Connaître les différents types de malwares
- Identifier un malware
- Analyser un malware
- Mettre en œuvre des contre-mesures efficaces

PROGRAMME DE FORMATION:

Typologie et fonctionnement des malwares

- Rootkit
- RAT
- Bot
- Ransomware
- Trojan
- Worm
- Spywares
- Droper

Méthodes d'infection des malwares

- Phishing
- Exploit Kit
- Drive by download
- Social engeniering
- Malwaretising

Méthodes d'évasion des malwares

- DLL injection
- PE Injection
- Process hollowing
- Fileless malware
- Détection de l'environnement

Méthodes de persistances des malwares

- Registry key
- Bootkit
- Folder autostart point

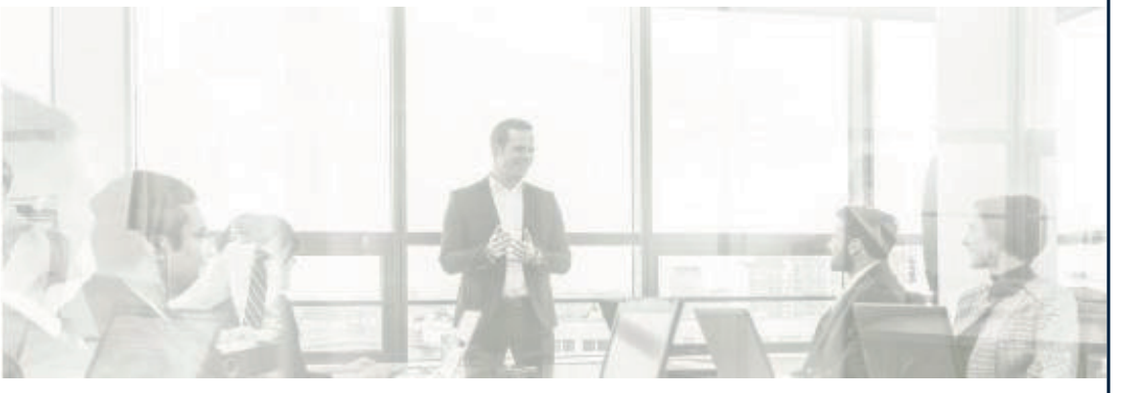
Techniques avancées des malwares

- Compression et packing
- Elévation de privilège
- Domain Generation Algorithm

Analyse de malware

- Mise en place d'un laboratoire d'analyse
- Analyse dynamique de malware via Sandbox : Cuckoo Sandbox
- Analyse de dropper type office : doc, xls, docm, xlsm
- Analyse de droper type pdf, scripting
- Analyse de binaire

Threat hunting grace à la threat intelligence



Bâtiment Raphaël

Parc d'Activités Paris Nord 2

22, Avenue des Nations

BP 58425

93420 – Villepinte

Téléphone : 01.49.38.06.49
Email : contact@h-intelligence.com

H-INTELLIGENCE