Cybersecurity Academy

Vue d'ensemble du programme ESD mastère (BAC +5)

---- Bloc offensif

Module 1 - Lead pentester (10 jours)

Module 2 - Techniques de Hacking avancées (5 jours)

Module 3 - Test d'intrusion avec Python (4 jours)

Module 4 - Wargame (5 jours)

---- Bloc défensif

Module 5 - Cyberdéfense (5 jours)

Module 6 - Analyste SOC (5 jours)

---- Bloc investigation

Module 7 - Investigation numérique - réseau et Windows (5 jours)

Module 8 - Fondamentaux à l'analyse de malware (4 jours)

---- Bloc gouvernance

Module 9 - Gestion de projets et Juridique- (5 jours)

Module 10 - Gestion des risques SI avec ISO 27005 & EBIOS RM (5 jours)

Module 11 - Intégration SMSI avec ISO 27001 (5 jours)

Module 12 - Plan de continuité (PCA) avec ISO 22301 (5 jours)

Module 13 - DevOps security manager (5 jours)

Lead Pentester

Durée	10 jours
Public	Étudiant en sécurité informatique, administrateur système, Pentester, RSSI, consultant en sécurité de l'information
Pré-requis	Connaissances générales en système, réseau, et développement
Objectifs	Comprendre les différentes phases composant un test d'intrusion. Savoir accompagner et encadrer un profil technique intervenant pour le test. Centraliser les informations récoltées et les modes de communication. Réaliser une fine analyse de la situation et être en mesure de restituer un rapport présenté de manière non-technique auprès d'un comité de direction
Plan de cours	**Jour 1 matin** ❏ Section 1 - Contexte actuel ❏ Statistiques récentes ❏ Terminologie ❏ Principes de la sécurité de l'information ❏ Les différentes phases d'une attaque ❏ Définition d'un test d'intrusion ❏ Aspects légaux et réglementaires liés aux tests d'intrusion ❏ Méthodes et framework pour un test d'intrusion ❏ Section 2 - Cadrage et objectifs ❏ Identification des objectifs ❏ Définition du périmètre ❏ ***TD**/ Framework pentest ESD Academy* ❏ **TP 1/** *Questionnaire de pré-engagement* **Jour 1 après-midi** ❏ Gestion et affectation des ressources ❏ Suivi des objectifs du test ❏ Règles de pré-engagement (RoE) ❏ **TP 2/** *Rédaction d'un contrat de pré-engagement* **Jour 2 matin** ❏ Section 3 : Préparer son test d'intrusion ❏ Préparation d'une machine pour test d'intrusion

- Automatisation et scripting
- Outils matériel connus
  - ***TD/*** *Rubber Ducky*
- Templating de documents
  - ***TD/*** *Suivi test d'intrusion*

- Section 4 - Collecte d'informations
  - Ingénierie des sources publiques (OSINT)
  - Relevé passif et actif d'informations sur l'organisation cible
    - ***TD/*** *Présentation des outils d'OSINT*
    - **TP 3/** *Relevé d'informations & Reconnaissance*

Jour 2 après-midi

- Section 5 - Enumération de l'infrastructure
  - Énumération du périmètre
  - Enumération des protocoles
    - ***TD/*** *Présentations des outils d'énumeration*
    - **TP 4/** *Enumération de l'infrastructure*

Jour 3 matin

- Section 6 - Analyse des vulnérabilités
  - Scan de vulnérabilités
  - Présentation des différents outils
    - ***TD/*** *Présentation OpenVAS*
  - Les vulnérabilités connues
    - **TP 5/** *Identification des vulnérabilités*

- Section 7 - Exploitation
  - Recherche d'Exploits

Jour 3 après-midi

  - Présentation des outils/frameworks d'attaques
    - ***TD/*** *Présentation metasploit*
  - Exécution de charge
    - **TP 6/** *Exploitation des vulnérabilités*
  - Bruteforcing

Jour 4

- Section 8 - Post-Exploitation
  - Élévation de privilèges (Méthodes, outils, vulnérabilités linux, …)
  - Etude des persistances (ADS, base de registre,

planificateur de tâches, services)
- ❏ Mouvements latéraux et pivoting

Jour 5

- ❏ ***TP 7/*** *Post-Exploitation et mouvement lateraux*

---------- Deuxième Semaine ----------

Jour 6 matin

- ❏ Section 9 - Sécurité Wi-Fi
  - ❏ Introduction
  - ❏ Les normes 802.11
  - ❏ Protocoles de sécurité & algorithmes (WEP/WPS/WPA)
  - ❏ Méthodes et attaques des réseaux sans fil
  - ❏ ***TD 1/*** *Présentation de la suite aircrack-ng*

Jour 6 après-midi

- ❏ Etude détaillée du protocole WPA2(Four Way Handshake)
- ❏ ***TD 2/*** *Intrusion Wi-Fi (WPA2)*
- ❏ ***TP 1/*** *Intrusion WI-FI*
- ❏ Contre-mesures et sécurisation (WIDS/802.1x)

Jour 7 matin

- ❏ Section 10 - Sécurité des applications Web
- ❏ Panorama de la sécurité web
- ❏ Références AppSec
- ❏ Client/serveur, AJAX, DOM
- ❏ Protocole HTTP(S)
- ❏ L'outil burpsuite
- ❏ ***TD*** */ Ouverture sur Burp suite*

Jour 7 après-midi

- ❏ Top 10 OWASP 2017
- ❏ Injections (SQL, LDAP, code, etc)
- ❏ ***TD /*** *Injection SQL manuelle et automatisée*
- ❏ ***TP1/*** *Injection*

Jour 8 matin

- ❏ Faiblesse d'authentification
  - ❏ ***TD/*** *Bruteforce via burp suite*
- ❏ Exposition de données sensibles
  - ❏ **TP /** *Exposition de donnée sensible*
- ❏ XXE/XPATH
- ❏ Faiblesse des contrôles d'accès
  - ❏ ***TP*** *LFI / RFI / CSRF / VERB Tampering*

Jour 8 après-midi

- ❏ Mauvaise configuration de sécurité
- ❏ Cross-Site Scripting-XSS (Stored/Reflected/DOM Based)
- ❏ **TP /** Attaque XSS

Jour 9 matin

- ❏ Désérialisation non sécurisée
- ❏ Composants vulnérables
- ❏ **TP /** scan de vulnérabilité (WPScan, Nikto, Openvas, NMAP) et framework offensif (Metasploit)
- ❏ Fuzzing & post exploitation

Jour 9 matin & après-midi

- ❏ Section 11 - Analyse et rapport
  - ❏ Étude et analyse des résultats
  - ❏ Mise en perspective des résultats
  - ❏ Rédaction de rapport
  - ❏ Restitution de livrables exploitable par un CODIR
  - ❏ Recommandations, plan d'actions et suivi

Jour 10

- ❏ **TP** : Réalisation d'un test d'intrusion complet & Rapport

Programme - Techniques de Hacking avancées

Techniques de Hacking avancées	
Durée	5 jours
Public	Consultant en cybersécurité, administrateur système/sécurité, ingénieur en informatique, pentester
Pré-requis	Connaissances requises en système windows, Active Directory, réseau, powershell, linux
Objectifs	Faire l'état des lieux des menaces récentes et des faiblesses d'infrastructure courantes - Comprendre et expérimenter des techniques de hacking avancées - Appréhender des méthodes et séquences offensives dans la pratique
Plan de cours	**Jour 1 matin** ❏ Section 1- Préparation et initialisation des phases à l'exploitation ❏ Introduction et Terminologie ❏ Étude des séquences d'exploitation ❏ Focus sur les types de charges ❏ Création de différents types de charges pour l'exploitation ❏ Déclencher les charges **Jour 1 Après-midi** ❏ Automatiser l'exploitation ❏ ***TP1*** / Création et intégration d'une charge **Jour 2 Matin** ❏ Section 2- Positionnement - Attaquant Externe ❏ Introduction sur les attaques externes ❏ Social Engineering (Phishing, détournement de messagerie, …) ❏ Recherche d'identifiants sur les bases de "Leak" **Jour 2 après-midi** ❏ Section 3- Positionnement - Attaquant Interne ❏ Introduction sur les attaques internes

- ❏ Attaque sur le protocole NTLM
- ❏ ***TP2*** / Attaque de type “relay” LLMNR & NBT-NS

Jour 3 matin

- ❏ Attaque sur le protocole Kerberos

❏ Section 4- Phases de Post-Exploitation

- ❏ Enumération Post-Exploitation
- ❏ Identification des chemins d’attaques

Jour 3 après-midi

- ❏ Obtention d’identifiants supplémentaires
- ❏ ***TP 3*** /Extraction des credentials en mémoire)
- ❏ Mouvement latéral
- ❏ ***TP4 /*** Mouvement latéral

Jour 4 matin

- ❏ Pivoting
- ❏ ***TP 5*** / Pivoting
- ❏ Escalade de privilèges verticale

Jour 4 Après-midi

- ❏ ***TP 6*** / escalade de privilège verticale
- ❏ Escalade de privilèges horizontale
- ❏ Zoom sur la sécurité des systèmes industriels

Jour 5 Matin

❏ Section 5 - Persistance

- ❏ Golden Ticket / Silver Ticket
- ❏ Skeleton Key / Admin SDHolder
- ❏ DCSync

Jour 5 Après-midi

- ❏ ***TP 7***/ Intrusion Externe

Python pour test d'intrusion	
Durée	4 jours
Public	Développeurs / Administrateurs / Pentesters
Pré-requis	Connaissances généralistes en programmation
Objectifs	Acquérir les compétences nécessaires en scripting pour créer ses propres outils en python pour un test d'intrusion
Plan de cours	**Jour 1 matin** ❏ Section 1 - Introduction ❏ Introduction à Python et à la cybersécurité ❏ Environnement Python et mise création du "lab" ❏ rappel des bases python et différentes API ❏ Monter un exécutables en Python **Jour 1 après-midi** ❏ Section 2 - Réseau ❏ gestion des sockets ❏ Création d'un scan de ports ❏ Introduction à la bibliothèque SCAPY ❏ Mise en place d' ARP poisoning (MITM) avec Scapy ❏ Subprocess : Reverse Shell ❏ **TP** / Exfiltration de données **Jour 2 matin** ❏ Section 3 - Système ❏ Win32ClipBoard : Manipuler le presse-papier ❏ Programme auto-répliquant ❏ Cryptographie : Ransomware ❏ Détection et protection en temps réel d'un ransoware **Jour 2 après-midi** ❏ Fonctionnement d'un Keylogger ❏ pe, protocole)

- ❏ Exfiltration FTP : Screenshots
- ❏ **TP** / Création d'une Exfiltration (ty RAT

Jour 4 matin

- ❏ Section 3 - Web
  - ❏ Introduction aux bibliothèques WEB (BeautilfulSoup, Request)
  - ❏ Protocole HTTP et fonctionnement
  - ❏ Requêtes HTTP(s)
  - ❏ BeautifulSoup : Crawler

Jour 4 après-midi

- ❏ Injection dans le DOM
- ❏ MITMproxy : Frame Injection
- ❏ API Web : Shodan
- ❏ **TP** / C&C Twitter

Cyberdéfense

Durée	5 jours
Public	Administrateur système, consultant en sécurité de l'information
Pré-requis	Connaissances en environnements Windows, Active Directory et gestion de projet
Objectifs	Comprendre les menaces courantes pesant sur les systèmes d'information en vue d'établir un plan de défense adapté aux différents types de menaces actuelles.
Plan de cours	**Jour 1 matin** ❏ Section 1- Introduction à la cybersécurité en France ❏ Introduction aux menaces pesant sur les organisations ces dernières années ❏ Vision des dirigeants vis-à-vis de la cybersécurité ❏ Présentation des différents corps d'état liés à la cybersécurité Française **Jour 1 après-midi** ❏ Zoom sur l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : PSSIE, Homologations ANSSI, Les visas, Le RGS, Instruction 901, Ebios RM ❏ ***TP 1/*** Étude de cas - Identification du niveau de sécurité ❏ La cybersécurité sur le plan Français et Européen **Jour 2 matin** ❏ Section 2 - Audit de la cybersécurité des systèmes d'information ❏ Principe d'audit SSI ❏ Séquencement d'un projet d'audit de la sécurité de l'information et réalisation d'un rapport **Jour 2 après-midi** ❏ Auditer et Identifier les écarts vis-à-vis d'un référentiel ❏ **TP 2**/ Étude de cas - Alignement des mesures de sécurité vis-à-vis du guide d'hygiène de l'ANSSI

- ❏ Restitution des points stratégiques du rapport en CODIR

Jour 3 Matin

- ❏ ***TP 3*** / Etude de cas - Réaliser une présentation pour la restitution d'audit au CODIR

Jour 3 après-midi

- ❏ Section 3 - Durcissement des infrastructures Windows
  - ❏ Sécurité des droits d'administration (Tiers model, comptes à privilèges, bastion, LAPS)

Jour 4 matin

- ❏ Durcissement des postes et serveurs
- ❏ Durcissement des protocoles réseaux

Jour 4 après-midi

- ❏ **TP 4 /** Mettre en oeuvre un renforcement de sécurité en environnement Microsoft

Jour 5 matin

- ❏ Journalisation et surveillance avancée (DLP, sysmon, log, …)
- ❏ **TP 5 /** Auditer son architecture et préparer un plan de contre mesure

Jour 5 après-midi

- ❏ Section 4 - Une défense alignée aux attaques
  - ❏ Revue de la segmentation des phases d'un attaquant
  - ❏ Présentation des différents groupes APT
  - ❏ Étude avancée des étapes d'une attaque APT au travers ATT&CK

Analyste SOC programme	
Durée	5 jours
Public	Étudiant en sécurité informatique, administrateur système, Pentester, RSSI, consultant en sécurité de l'information
Prérequis	Connaissances générales en sécurité offensive et défensive telles que les techniques de hacking, le durcissement des infrastructures.
Certification	• Soutenance de 40 minutes devant un jury en ligne • Le candidat doit pouvoir résoudre un scénario devant un jury de professionnels. • Le candidat a accès pendant 90 jours à une plateforme d'entraînement avant de planifier son examen. • Un diplôme numérique et physique est attribué au candidat. • Certification permettant de valider ¼ des blocs du mastère spécialisé ESD (Expert(e) en sécurité digital)
Objectifs	Comprendre l'état de l'art du SOC et répondre aux besoins des enjeux cybers et des menaces par le métier d'analyste SOC
Plan de cours	**Jour 1 - SOC et métier d'analyste** ❏ Section 1 - Etat de l'art du Security Operation Center ❏ Définition du SOC ❏ Les avantages, l'évolution du SOC ❏ Les services intégrés au SOC, les données collectées, playbook ❏ Le modèle de gouvernance du SOC (approche SSI, type de SOC, CERT, CSIRT) ❏ Pré requis et rôles d'un analyste SOC (techniques, soft skills, rôles, modèles) ❏ Les référentiels (ATT&CK, DeTT&CT, Sigma, MISP) ❏ **Démonstration 1** - utilisation du framework ATT & CK via Navigator (attaque et défense) ❏ Section 2 - Focus sur l'analyste SOC ❏ Quel travail au quotidien ❏ Triage des alertes ❏ Révision et état de sécurité ❏ Identification et rapport ❏ Threat hunting

- ❏ **Démonstration 2**- utilisation de l'outil SYSMON

❏ Section 3 - Les sources de données à monitorer

- ❏ Indicateur Windows (processus, firewall, etc.)
- ❏ Service WEB (serveur, WAF, activité)
- ❏ IDS/IPS
- ❏ EDR, XDR
- ❏ USB
- ❏ DHCP, DNS
- ❏ Antivirus, EPP
- ❏ DLP, whitelist
- ❏ Email
- ❏ **Exercice 1** / cas d'usage et ligne de défense

Jour 2 (Découverte & mise en place du SIEM)

❏ Section 4 - Tour d'horizon du SIEM

- ❏ Contexte du SIEM
- ❏ Solution existante
- ❏ Principe de fonctionnement d'un SIEM
- ❏ Les objectifs d'un SIEM
- ❏ Solution de SIEM

❏ Section 5 - Présentation de la suite Elastic

- ❏ Les agents BEATS, sysmon
- ❏ Découverte de Logstash
- ❏ Découverte de Elasticsearch
- ❏ Découverte de Kibana
- ❏ **TP 1** / mise en place d'ELK et première remontée de log

Jour 3 (Analyse, Logstash, Elastic search)

❏ Section 6 - Logstash (ETL)

- ❏ Fonctionnement de Logstash
- ❏ Les fichiers input & output
- ❏ Enrichissement: Les filtres Groks et sources externes

❏ Section 7 - ElasticSearch

- ❏ Terminologie
- ❏ Syntax Lucene
- ❏ Alerte avec ElasticAlert et Sigma
- ❏ **TP 2** / création d'alertes, alarmes

- ❏ **Démonstration 3** / utilisation d'Elastalert et Sigmac

❏ Section 8 - Kibana

- ❏ Recherche d'événements
- ❏ Visualisation des données
- ❏ **Démonstration 4** / création d'un filtre sur Kibana
- ❏ Ajout de règles de détection, IoC
- ❏ Allez plus loin dans l'architecture ELK avec HELK

Jour 4 (Cyber entraînement)

❏ Section 9 - Mise en situation

- ❏ à travers des outils ESD Academy, l'analyste SOC est en situation et doit identifier plusieurs scénarios d'attaque lancés par le formateur
- ❏ **TP 3** / Configurer un SIEM et l'exploiter

Investigation numérique Windows	
Durée	5 jours
Public	Administrateur, analyste SOC, ingénieur sécurité
Pré-requis	Connaissance sur l'OS Windows, TCP/IP, Linux
Objectifs	Acquérir les compétences et la méthodologie pour une investigation numérique sur le système d'exploitation Windows
Plan de cours	**Jour 1 matin** ❏ **Section 1** - Etat de l'art de l'investigation numérique ❏ Introduction à l'investigation numérique ❏ Vocabulaire, taxonomie ❏ Les différentes disciplines ❏ Indicateur de compromission ❏ Méthodologie d'investigation ❏ ATT&CK et Arbres d'attaque **Jour 1 après-midi** ❏ **Section 2** - Les fondamentaux Windows ❏ Fondamentaux Windows ❏ Structure des répertoires ❏ Séquence de boot ❏ Bases de Registres ❏ Logs et événements ❏ Services ❏ Volume Shadow Copy Service ❏ Généralités sur les disques durs ❏ Fondamentaux NTFS ❏ ***TP1 Questionnaire*** **Jour 2 matin** ❏ **Section 3** - Collecte des données ❏ Analyse live ❏ Analyse offline : imaging ❏ Analyse offline : collecte ❏ Les outils d'analyse

Jour 2 après-midi

- ❏ **Section 4** - Artefacts
  - ❏ Différents artefacts internet
    - ❏ Pièces jointes
    - ❏ Open/Save MRU
    - ❏ Flux ADS Zone.Identifier
    - ❏ Téléchargements
    - ❏ Historique Skype
    - ❏ Navigateurs internet
    - ❏ Historique
    - ❏ Cache
    - ❏ Sessions restaurées
    - ❏ Cookies
  - ❏ Différents artefacts exécution
    - ❏ UserAssist
    - ❏ Timeline Windows 10
    - ❏ RecentApps
    - ❏ Shimcache
    - ❏ Jumplist
    - ❏ Amcache.hve
    - ❏ BAM/DAM
    - ❏ Last-Visited MRU
    - ❏ Prefetch

Jour 3 + 4

  - ❏ Différents artefacts fichiers/dossiers
    - ❏ Shellbags
    - ❏ Fichiers récents
    - ❏ Raccourcis (LNK)
    - ❏ Documents Office
    - ❏ IE/Edge Files
  - ❏ Différents artefacts réseau
    - ❏ Termes recherchés sur navigateur
    - ❏ Cookie
    - ❏ Historique
    - ❏ SRUM (ressource usage monitor)
    - ❏ Log wifi
  - ❏ Différents artefacts comptes utilisateur
    - ❏ Dernières connexions
    - ❏ Changement de mot de passe
    - ❏ Echec/Réussite d'authentification
    - ❏ Évènement de service (démarrage)
    - ❏ Evènement d'authentification
    - ❏ Type d'authentification
    - ❏ Utilisation du RDP
  - ❏ Différents artefacts USB

- Nomination des volumes
- Evénement PnP (Plug & Play)
- Numéros de série
- Différents artefacts fichiers supprimés
- tools
- Récupération de la corbeille
- Thumbcache
- Thumb.db
- WordWheelQuery
- Spécificités Active Directory
- ***TP 3*** */ Première investigation*
- ***TP 4*** */ Deuxième investigation*

Jour 5 Matin

- **Section 5** - Analyse mémoire
- Acquisition
- Volatility
- ***TP 5*** */ Investigation mémoire*

Jour 5 après-midi

- **Section 6** - Anti Forensic
- Principes
- Techniques
- Tools
- ***TP*** */ Anti Forensic*

Analyse de Malwares – Les fondamentaux	
Durée	4 jours
Public	Développeurs / Pentesters / administrateurs / Analystes
Pré-requis	Connaissances généralistes en programmation et système / réseaux
Objectifs	Acquérir des connaissances généralistes sur le fonctionnement des malwares / Découverte d'une méthodologie d'analyse statique et dynamique / Création de charges encodées
Plan de cours	**Jour 1 matin** ❏ **Section 1** – État de l'art ❏ Introduction ❏ Historique ❏ Vecteurs d'infection ❏ Impacts business ❏ Réponse à incident ❏ Défenses classiques **Jour 1 après-midi** ❏ **Section 2** – Infrastructure d'analyse ❏ Infrastructure ❏ Environnement d'analyse **Jour 2 matin** ❏ **Section 3** – Méthodologie d'analyse ❏ Analyse statique basique (Principe, outils, PDF, Office, YARA) ❏ TP 1 / Analyse PDF malveillant ❏ TP 2 / Analyse fichier office malveillant ❏ TP 3 / Analyse exe malveillant **Jour 2 après-midi** ❏ Analyse dynamique basique (Principe, outils, méthode) ❏ TP 4 / Analyse de fichiers

malveillants

Jour 3

- ❏ Analyse dynamique avancée
- ❏ Rappel bases systèmes
- ❏ Introduction à l'assembleur

Jour 4

- ❏ TP 5 / Analyse de fichiers malveillants

- ❏ **Section 4** – Introduction au shellcodes
  - ❏ TP6/ Programme ASM & shellcoding

Gestion de projets & Juridique	
Durée	5 jours (1,5 jours gestion de projets + 3,5 jours juridique)
Public	Étudiant, administrateur système, consultant en sécurité de l'information
Pré-requis	Connaissances générales SI, Notions excel
Objectifs	Comprendre et implémenter une gestion propre des projets SSI au sein d'une organisation S'aligner au cadre juridique s'imposant aux métiers de la SSI
Plan de cours	**Jour 1 matin** ❏ Section 1 - Gestion de projet ❏ Acteurs et vie d'un projet ❏ Définition du projet ❏ Objectifs SMART ❏ Fiche de définition ❏ Montage du projet ❏ Budget ❏ OBS et WBS ❏ Planification du projet et Gantt ❏ Rôles et Responsabilité ❏ ***TP 1*** / Compréhension et analyse de votre environnement **Jour 1 après-midi** ❏ Exécution du projet ❏ Indicateur et état d'avancement ❏ Analyse d'écarts ❏ Réunions et instances de pilotage ❏ Comptes-rendu ❏ Conseils en gestion de projet ❏ ***TP 2*** / Gestion de projet (En groupe) **Jour 2 matin** ❏ Section 2 - Gestion des risques au sein d'un projet ❏ L'identification des risques ❏ Humains ❏ Économiques

- Temporels
- Autres
- Priorisation des risques
- Réflexions et traitements des risques
- Suivi des risques
- ***TP 3*** / Analyse des risques “projet” (En groupe)

Jour 2 après-midi

- Section 3 - Réglementation RGPD

  - RGPD : définitions et historique
  - Nouvelles obligations
  - Organismes concernés
  - Acteurs et intervenants
  - ***TP 4 /*** *Identification de traitement de données à caractère personnel*

Jour 3 matin

- Étapes clés d’une mise en conformité
- ***TP 5 /*** *Analyse d’impact relative à la protection des données (AIPD)*

Jour 3 après-midi

- Utilisation du SI pour une mise en conformité
- Erreurs courantes
- ***TP 6 /*** *Situation exceptionnelle vs RGPD*

Jour 4

- Section 4 - Sécurité de l’information et juridique

  - Responsabilité légale du RSSI
  - Forensic : limites légales
  - Charte informatique
  - BYOD au sein des organisations
  - Sécurité de l’information vs utilisation personnelle du SI
  - Liens utiles
  - ***TP 7 /*** *CHU de Rouen : Identification des problèmes*

	Jour 5 ❏ Section 5 - Prise de poste : bonnes pratiques ❏ Analyse de l'existant ❏ Étude des processus ❏ Schéma directeur SSI

Gestion des risques avec ISO/IEC 27005 Programme	
Durée	5 jours
Public	Etudiant, consultant en sécurité de l'information, Risk manager
Prérequis	Connaissances générales en sécurité des systèmes d'information
Objectifs	Avoir les acquis nécessaires pour établir une analyse des risques avec les concepts de l'ISO/IEC 27005
Plan de cours	**Jour 1 matin (ISO/IEC 27005:2022)** ❏ **Section 1** - fondamentaux de la gestion des risques ❏ Définition du risque (dictionnaire, ISO/IEC 27005:2022, EBIOS Risk Manager) ❏ Composante d'un risque (actif, vulnérabilité, menaces, scénario, calcul du risque) ❏ Interaction entre les composantes d'un risque ❏ Exercice 1 : composer un risque ❏ Étude des risques ? Méthodes et normes ❏ Norme vs méthodologie ❏ Rappel d'une norme ISO/IEC ❏ Lien entre l'ISO 27001 & 27005 ❏ La gouvernance, risque, ISO/IEC 27005:2022, lien avec l'ISO/IEC 27001 ❏ Développer un programme de gestion des risques ❏ **Section 2** - présentation de la norme ISO/IEC 27005:2022 ❏ Présentation de l'ISO/IEC 27005:2022 (clauses) structure de la norme ISO/IEC 27005:2022 ❏ Cycle de la norme ❏ PDCA (roue de Deming)

- ❏ Approche processus
- ❏ Évolution ISO/IEC 27005:2022 vs 2022

- ❏ **Section 3** - la phase de contexte par ISO/IEC 27005:2022
  - ❏ Définition d'une organisation, appétit du risque
  - ❏ Identification des exigences de base des parties prenantes
    - ❏ **Exercice 2** : établir le contexte d'une organisation
  - ❏ Identifier les objectifs, cycle d'itération
  - ❏ Considéré la gestion des risques dans une organisation
  - ❏ Critères d'acceptation des risques
  - ❏ Critère d'évaluation des risques
  - ❏ Critères pour la conséquence
  - ❏ Critères pour la probabilité
  - ❏ Critères de détermination du niveau de risque.
    - ❏ **Exercice 3** : établir les critères d'une organisation

Jour 1 après-midi (ISO/IEC 27005:2022)

- ❏ **Section 4** - Cycle d'analyse
  - ❏ Définition du cycle d'analyse
  - ❏ Approche par événements / par asset

- ❏ **Section 5** - Phase d'identification des risques
  - ❏ Identification des actifs
  - ❏ Identification des vulnérabilités
  - ❏ Identification des conséquences
    - ❏ **Exercice 4** : identifier les actifs, les événements et les porteur du risque
  - ❏ Identifier les sources de risques et objectifs visés
    - ❏ **Exercice 5** : identifier sources de risques et les objectifs visés
  - ❏ Identifications des parties prenantes
    - ❏ **Exercice 6** : identifier les parties prenantes et des chemins d'attaque
  - ❏ Valeur et liens entre les actifs
    - ❏ **Exercice 7** : identifier les actifs supports
  - ❏ Identifier les scénarios opérationnels
    - ❏ **Exercice 8** : identifier les scénarios opérationnels

Jour 2 matin (ISO/IEC 27005:2022)

- ❏ **Section 6** - phase d'estimation et d'évaluation des risques
  - ❏ Approche qualitative vs quantitative
  - ❏ Les différentes méthodes de calcul des risques
  - ❏ Estimer le niveau de sévérité de la conséquence

- **Exercice 9** : estimer la sévérité de la conséquence
- Estimer la probabilité d'occurrence
  - **Exercice 10** : estimer la probabilité d'occurrence
- Déterminer le niveau de risque
  - **Exercice 11** : déterminer le niveau de risque
- Comparer le résultat de l'estimation des risques avec les critères de risque
- Prioriser les risques
  - **Exercice 12** : prioriser les risques
- Établir un plan de traitement des risques

Jour 2 après-midi (ISO/IEC 27005:2022)

- **Section 7** - phase de traitement et d'acceptation des risques
  - Les différentes options de traitement du risque
  - Déterminer les contrôles nécessaires à la mise en oeuvre des options de traitement
  - Comparaison les contrôles avec ceux de l'annexe a iso/iec 27001
    - **Exercice 13** : comparer les contrôles avec l'annexe a de l'ISO/IEC 27001
  - Produire une déclaration d'applicabilité (dda)
  - Mettre en place un plan de traitement des risques
    - **Exercice 14** : mettre en place un plan de traitement des risques
  - Notions de risques bruts, nets, résiduels
  - Évaluer le risque résiduel
  - Approuver par les porteurs des risques

Jour 3 matin (ISO/IEC 27005:2022)

- **Section 8** - communication et surveillance
  - Établir un plan de communication
  - Mettre en place les indicateurs pour une surveillance optimal dans un modèle PDCA Jour 3 après-midi (ISO/IEC 27005:2022)

- **Section 9** - alignement au SMSI
  - Contexte de l'organisation
  - Leadership et engagement
  - Phase de communication
  - Créer une matrice de communication
    - **Exercice 15** : créer une matrice de communication
  - Communiquer les risques résiduels au PCA et la réponse à incident
  - Phase de documentation

	❏ Informations documentées sur les processus ❏ Informations documentées sur les résultats ❏ Surveillance et révision des facteurs influençant les risques ❏ Exemple du sfdt (source-function-destination-trigger) ❏ **Exercice 16** : créer un scénario de surveillance ❏ Action corrective ❏ Amélioration continue **Jour 4 et 5 (ISO/IEC 27005:2022)** ❏ **Section 10** – Analyse de risques avec EBIOS RM

Intégration SMSI avec ISO 27001	
Durée	5 jours
Public	Étudiants, administrateurs système, consultants en sécurité de l'information, responsables des risques, directeurs des systèmes d'information
Pré-requis	Compréhension des architectures SI actuelles, gestion d'un système d'information (processus, documentation etc..)
Objectifs	Comprendre et savoir implémenter un système de management de la continuité d'activité au travers les exigences de la norme ISO 27001
Plan de cours	**Jour 1 matin** ❏ Section 1 - Introduction et définitions ❏ Rappels ❏ Définition ❏ Chiffres Iso ❏ Section 1 - Normes ISO 2700X ❏ ISO 27002 - ISO 27001 Comparaison et usage des 2 normes ❏ ISO 27003 Implémentation d'un SMSI

- ISO 27004 Indicateurs du SMSI
- ISO 27005 Appréciation des risques
- ISO 27007 Audit du SMSI
- ISO 27008 Revue des mesures de sécurité
- ISO 27035 Gestion des incidents de sécurité
- ISO 27 552 Extension ISO 27001
- Normes et réglementation

Jour 1 après-midi

- Section 3 - Système de management
  - Définition et nature du projet
  - Système de management intégré
  - Maturité des processus

Jour 2 matin

- Section 4 - Sécurité de l'information
  - Introduction
  - Définition
  - Rappels

Jour 2 après midi

- Section 5 - La norme ISO 27001:2017
  - Introduction
  - Contexte de l'organisation
  - **TP 1 /** Analyse SWOT-ISO 27001

Jour 3 matin

  - Leadership
  - **TP 2 /** Conception de la structure de la politique de sécurité
  - Planification
  - **TP 3 /** Norme 27001 et exigences vis-à-vis de la gestion des risques
  - Planification (suite)
  - **TP 4 /** Etude DDA

Jour 3 après-midi

  - Support
  - **TP 5 /** Mesures de sécurité
  - Fonctionnement
  - Evaluation des performances
  - **TP 6 /** Création d'indicateur de performance

Jour 4 matin

  - Evaluation des performances (suite)
  - **TP 7** / Analyse des non conformité

	❏ Amélioration ❏ **TP 8 /** Séquencement d'implémentation de la norme ISO 27001 **Jour 4 après-midi** ❏ Section 6 - Implémentation ISO 27001/SMSI ❏ Définition et nature du projet ❏ Séquencement de l'implémentation ❏ Principales erreurs ❏ Processus de certification ❏ **TP 9 /** Audit à blanc ❏ **Examen**

Plan de continuité d'activité (PCA) avec ISO 22301	
Durée	5 jours
Public	Étudiants, administrateurs système, consultants en sécurité de l'information, responsables des risques, directeurs des systèmes d'information
Pré-requis	Compréhension des architectures SI actuelles, gestion d'un système d'information (processus, documentation etc..)
Objectifs	Comprendre et savoir implémenter un système de management de la continuité d'activité au travers les exigences de la norme ISO 22301
Plan de cours	**Jour 1 matin** ❏ Section 1 - Cadrage ❏ Terminologie et Définitions ❏ PCA (Plan de continuité d'activité) ❏ PRA (Plan de reprise d'activité ❏ PCI (Plan de continuité informatique) ❏ PRI (Plan de reprise informatique) ❏ Continuité vs reprise d'activité les différences ❏ Les erreurs courantes liés au PCA/PRA **Jour 1 après-midi** ❏ Section 2 - PCA et entreprise

- ❏ Compréhension du positionnement d'un PCA dans une stratégie d'entreprise
- ❏ Alignement de la gestion des risques SI au PCA
- ❏ Vision globale d'un projet PCA au sein d'une organisation
- ❏ Assurance des biens tangibles/intangibles
- ❏ **TP 1 /** Etat des lieux

❏ Section 3 - Etude de la norme ISO 22301

- ❏ PCA et l'aspect normatif
- ❏ Zoom sur la norme internationale ISO 22301
- ❏ Appréhender la notion de système intégré

Jour 2 matin

❏ Section 4 - ISO 22301 "Contexte"

- ❏ Compréhension des besoins en sécurité de l'information de l'entreprise et de son contexte
- ❏ Identification et recensement des besoins et attentes des parties intéressées
- ❏ Etude des exigences légales et réglementaires applicables
- ❏ Identification du domaine d'application du SMCA
- ❏ TP 2 / Exigences légales et réglementaires

Jour 2 après-midi

❏ Section 5 - ISO 22301 "Leadership"

- ❏ Engagement de la direction
- ❏ Etablissement d'une politique de continuité d'activité
- ❏ Définition et affectation des rôles, responsabilités et autorisé au sein du SMCA

❏ Section 6 - ISO 22301 "Planification"

- ❏ Planification des actions face aux différents risques et opportunités
- ❏ Définition d'objectifs de continuité d'activité associés à des plans permettant de les atteindre
- ❏ TP 3 / Objectif de continuité d'activité

Jour 3 matin

❏ Section 7 - ISO 22301 "Support"

- ❏ Affectation des ressources au SMCA
- ❏ Gestion des compétences
- ❏ Sensibilisation
- ❏ Encadrement de la communication
- ❏ Implémentation de cycle de vie documentaire

Jour 3 après-midi

- ❏ Section 8 - ISO 22301 “Fonctionnement”

  - ❏ Gestion de la planification opérationnelle
  - ❏ Analyse des impacts sur l’activité
  - ❏ TP 4 / DIMA

Jour 4 matin

  - ❏ Appréciation des risques
  - ❏ TP 5 / EBCA
  - ❏ Mise en oeuvre de stratégie de continuité d’activité
  - ❏ Etablissement de procédures de continuité d’activité
  - ❏ TP 6 / DIMA/EBCA Plan de continuité d’activité
  - ❏ TP 7 / Exercices et tests

Jour 4 après-midi

- ❏ Section 9 - ISO 22301 “Evaluation des performances”

  - ❏ Surveillance, mesurage
  - ❏ Analyse et évaluation
  - ❏ Audit interne du SMCA
  - ❏ Mise en place de revue de direction
  - ❏ TP 8 / Indicateur de gestion de la continuité

- ❏ Section 10 - ISO 22301 “Amélioration”

  - ❏ Etudes des non-conformités
  - ❏ Actions correctives
  - ❏ Amélioration continue
  - ❏ TP 9 / Scénario PCA/PRA

Jour 5

- ❏ **Examen**

DevOps Security Manager

Durée	5 jours
Public	Développeurs / Pentesters / administrateurs / Chefs de projet informatique
Pré-requis	Connaissances généralistes en programmation web, administration serveur web, management
Objectifs	Acquérir des compétences en programmation et sécuriser efficacement un serveur web / une application, gérer la sécurité au travers d'un projet informatique, mettre en place des outils liés à la sécurité applicative.
Plan de cours	**Jour 1 matin** ❏ Section 1 - Introduction ❏ Panorama du web ❏ Référentiels ❏ Cadre juridique ❏ **TP 1 /** Questionnaire **Jour 1 après-midi** ❏ Section 2 - Principes de sécurité web ❏ Rappels sur l'environnement web ❏ Les vulnérabilités web **Jour 2 matin** ❏ Section 3 - Tester son application ❏ BurpSuite ❏ Fuzzing ❏ Analyse de code **Jour 2 après-midi** ❏ Tests d'intrusion ❏ **TP 2 /** Test d'intrusion applicatif

Jour 3 matin

- ❏ Section 4 - Durcissement applicatif
  - ❏ Sécuriser son code
  - ❏ Durcissement client/serveur

Jour 3 après-midi

- ❏ **TP 3 /** Durcissement d'une application

Jour 4 matin

- ❏ Section 5 - Management de la sécurité applicative (SDLC)
  - ❏ Paradigmes DevOps
  - ❏ Secure Development LifeCycle
  - ❏ Modélisation de menaces
  - ❏ Réduction des attaques de surfaces

Jour 4 après-midi

- ❏ Données à caractère personnels
- ❏ Défense en profondeur
- ❏ Séparation des privilèges
- ❏ Sécurisation par défaut

Jour 5 matin

- ❏ Section 6 - Intégration continue
  - ❏ Dépôts de code
  - ❏ Outils de déploiement
  - ❏ Suivi des bugs

- ❏ Section 7 - Les modèles de maturité
  - ❏ OPENSAMM
  - ❏ BISMM

Jour 5 après-midi

- ❏ **TP 4 /** Etude de cas SDLC

Wargame	
Durée	5 jours
Public	Développeurs / Administrateurs / pentester
Pré-requis	Connaissances cybersécurité / infrastructure / Offensif
Objectifs	Semaine durant laquelle les élèves préparent des challenges de hacking et les échangent par la suite pour se mesurer par petites équipes.