Identification du module

Numéro de module	684	
Titre	Procéder à une investigation numérique des systèmes	
Compétence	Inspecter les données persistantes, temporaires ou volatiles des systèmes quant à la présence de maliciels ou de traces numériques suspectes, exploiter et présenter les résultats de l'investigation de façon probante et en adéquation avec le groupe cible.	
Objectifs opérationnels	1	Clarifier et définir avec le mandant l'objet de suspicion, les objectifs et les conditions cadres d'une investigation numérique.
	2	Définir, en tenant compte des objectifs et des conditions cadres, la méthode et la procédure de l'investigation numérique.
	3	Vérifier la conformité légale d'une investigation numérique et engager, si nécessaire, des mesures correctives.
	4	Acquérir les systèmes à inspecter et sauvegarder les données persistantes, temporaires ou volatiles.
	5	Inspecter les données préservées quant à la présence de traces suspicieuses ou d'indicateurs de maliciels et procéder à l'enregistrement continu et exhaustif des étapes de l'investigation numérique.
	6	Analyser les fichiers suspects à des fins de détection de fonctions nuisibles ou indésirables et décrire les indicateurs relatifs aux maliciels identifiés.
	7	Evaluer l'investigation, consigner les résultats dans un rapport final probant et présenter les résultats aux décideurs en adéquation avec le groupe cible.
Domaine de compétence	Security/Risk Management	
Objet	Données persistantes, temporaires ou volatiles sur des serveurs, des terminaux et périphériques fixes ou mobiles, des solutions de stockage et des applications.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	684
Titre	Procéder à une investigation numérique des systèmes
Compétence	Inspecter les données persistantes, temporaires ou volatiles des systèmes quant à la présence de maliciels ou de traces numériques suspectes, exploiter et présenter les résultats de l'investigation de façon probante et en adéquation avec le groupe cible.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les phases et activités usuelles d'une investigation numérique (p. ex. identification de l'objet d'investigation, collecte et conservation des données, investigation, rapport) et pouvoir citer des normes ou standards établis (p. ex. guides NIST, Guide to IT Forensics du BSI).
	1.2	Connaître les sous-domaines typiques de la forensique numérique (p. ex. analyse forensique des disques durs, des systèmes d'exploitation, des réseaux) et pouvoir expliquer leur pertinence dans l'inspection de serveurs, de terminaux et de périphériques fixes ou mobiles, de solutions de stockage et d'applications.
	1.3	Connaître des types de données pertinents pour les investigations numériques (p. ex. données de configuration, données de processus, données d'application, données de session, données de protocole de communication, métadonnées) et pouvoir expliquer des exemples et les différences entre les types de données.
	1.4	Connaître des conditions cadres organisationnelles et techniques pertinentes pour les investigations numériques (p. ex. identification de tous les systèmes et collaborateurs concernés, temps requis et dilemme par rapport au rétablissement rapide du fonctionnement normal, risques relevant de la responsabilité, accès à l'infrastructure et aux réseaux, proportionnalité).
2	2.1	Connaître les conditions, les possibilités et les limites des analyses post mortem (dead box, hors ligne) et des analyses live (live box, en ligne) et pouvoir expliquer les différences entre ces deux approches.
	2.2	Connaître les différences entre une procédure orientée données et une procédure orientée incidents dans le cadre des investigations numériques et pouvoir expliquer la pertinence de la chronologie dans leur exécution.
	2.3	Connaître les conditions, les possibilités et les limites des analyses statiques et dynamiques de maliciels et pouvoir expliquer les différences entre ces deux approches.
3	3.1	Connaître les dispositions pertinentes de la protection des données dans le cadre d'investigations numériques effectuées par des organisations privées (p. ex. ordonnance d'investigation, communication et annonce, protection de la personnalité).
	3.2	Connaître les dispositions et les limites pénales pertinentes relatives aux investigations numériques effectuées par des organisations privées (p. ex. li-

Connaissances opérationnelles nécessaires

		mitation à la propre infrastructure, soustraction de données, accès indu à un système informatique, détérioration des données).
	3.3	Connaître les conditions applicables aux investigations numériques effectuées par les autorités d'instruction pénale et pouvoir citer les possibilités étendues qu'elles détiennent (p. ex. accès aux données de tiers par décision de justice ou par demande d'entraide judiciaire).
	3.4	Connaître les exigences à remplir par un processus d'investigation numérique (p. ex. intégrité des données, admissibilité et crédibilité des méthodes, reproductibilité, documentation) et pouvoir expliquer leur pertinence pour une chaîne de traçabilité solide (chain of custody) et la recevabilité juridique des éléments de preuve.
4	4.1	Connaître les exigences à remplir par la sauvegarde forensique de supports de données physiques avec des données persistantes (p. ex. copie de travail et copie d'archive, exhaustivité, traitement des erreurs, intégrité) et pouvoir expliquer avec quelles mesures ces exigences peuvent être remplies (p. ex. utilisation de bloqueurs d'écriture matériels ou logiciels, copie bit par bit, somme de contrôle cryptographique).
	4.2	Connaître les exigences à remplir par la sauvegarde forensique de mémoire volatile et de fichiers d'échange (swap files) temporaires et pouvoir expliquer quelles informations doivent être préservées en sus pour l'analyse d'une copie-image (p. ex. date et heure système, liste des applications et des processus actifs, connexions réseau actives).
	4.3	Connaître des outils appropriés pour créer des copies forensiques de supports de données et regrouper des supports de données (systèmes RAID).
	4.4	Connaître des outils appropriés pour créer des images mémoire (p. ex. Volatility, Autopsy, The Sleuth Kit).
	4.5	Connaître des possibilités, des techniques et des outils pour la sauvegarde de systèmes virtualisés (p. ex. copies de fichiers RAM ou de fichiers HDD, instantané de stockage [snapshot]).
5	5.1	Connaître les caractéristiques déterminantes de l'architecture des appareils fixes ou mobiles (p. ex. processeur, mémoire, interfaces) et pouvoir expliquer leurs différences et leur pertinence pour des analyses forensiques numériques.
	5.2	Connaître des systèmes d'exploitation courants d'appareils fixes ou mobiles (p. ex. Windows, Unix/Linux, Mac OS, iOS, Android) et pouvoir expliquer leurs caractéristiques et différences au regard des analyses forensiques numériques (p. ex. noyau, appels système, gestion des processus, formats de fichiers exécutables, processus de démarrage, emplacement de stockage des données de configuration).
	5.3	Connaître des concepts courants de partitionnement des supports de données (p. ex. DOS/MBR, partition Apple, partition BSD, table de partitionnement GUID [GPT]) et de regroupement ou de concaténation de supports de données (p. ex. RAID, disk spanning, JBOD, NRAID) et pouvoir expliquer leurs caractéristiques, leurs différences et leur pertinence pour des analyses forensiques numériques.
	5.4	Connaître des systèmes de fichiers courants (p. ex. FAT, NTFS, ExtX, UFS) et pouvoir expliquer leurs caractéristiques, leurs différences et leur pertinence pour des analyses forensiques numériques (p. ex. structure des données, noms de fichiers et de répertoires, journalisation, récupération de données [carving]).

Connaissances opérationnelles nécessaires

	5.5	Connaître des procédures cryptographiques courantes pour le chiffrement des données (p. ex. RSA, ECDHE, ECDSA, SHA, 3DES, AES) et pouvoir expliquer leurs fonctions (échange de clés, authentification, fonction de hachage et chiffrement) ainsi que leur influence sur les analyses forensiques numériques.
	5.6	Connaître des indicateurs typiques de détection de maliciels (p. ex. valeurs de hachage, noms de fichiers, clé de registre, règles YARA) et des sources pertinentes pour de tels indicateurs (p. ex. OpenIOC, YARA Repository, CTI de l'organisation).
	5.7	Connaître des outils appropriés pour l'analyse des fichiers et de leur contenu.
	5.8	Connaître les principaux contenus d'un rapport d'investigation probant et compréhensible (p. ex. identification, chronologie et horodatage, activité, outils et paramètres, résultats, justificatifs, preuves).
6	6.1	Connaître des outils appropriés pour l'analyse statique de maliciels et pouvoir expliquer la finalité de leur utilisation (p. ex. détermination des propriétés des fichiers et des métadonnées, éditeurs Hex, identification de motifs, désassemblage, rétro-ingénierie).
	6.2	Connaître les défis typiques à relever dans le cadre de l'analyse statique de maliciels (p. ex. compression, chiffrement, déguisement ou camouflage de maliciels au moyen de run time packers, de crypteurs et de méthodes d'obfuscation du code source) et pouvoir expliquer des procédures alternatives.
	6.3	Connaître des outils appropriés pour l'analyse dynamique de maliciels et pouvoir expliquer la finalité de leur utilisation (p. ex. isolation/sandboxing, simulation, débogage).
	6.4	Connaître les défis typiques à relever dans le cadre de l'analyse dynamique de maliciels (p. ex. différences au niveau du langage, de l'architecture système ou du système d'exploitation; détection de machines virtuelles ou de sandboxes par le maliciel, mesures anti-débogage du maliciel par chiffrement ou camouflage) et pouvoir expliquer des procédures ou méthodes alternatives.
	6.5	Connaître des formats courants pour décrire les indicateurs de maliciels (p. ex. STIX, format OpenIOC, Intrusion Detection Message Exchange Format [IDMEF], Incident Object Description Exchange Format [IODEF], règles YARA).
7	7.1	Connaître des méthodes et des techniques appropriées de synthèse et de présentation des informations (p. ex. réduction des données, création de ratios, tableaux de fréquence et histogrammes, agrégation au moyen de tableaux croisés et de tableaux croisés dynamiques, diagramme de corrélation, analyse de séries temporelles et analyse des tendances).
	7.2	Connaître les principaux contenus d'un rapport final d'investigation (p. ex. synthèse, contexte, objet de l'analyse, méthodes, résultats, constats, options d'action, recommandation avec justification) et pouvoir expliquer leur contribution à la prise de décisions.
	7.3	Connaître le contenu et la structure d'une bonne présentation et pouvoir expliquer en quoi ses propres compétences en termes d'expression et de comportement en public influencent le travail de persuasion.

Version du module	1.0

Connaissances opérationnelles nécessaires

Créé le	11.02.2021