Identification du module

Numéro de module	679
Titre	Collecter des informations sur les menaces et les traiter
Compétence	Dans le cadre de la Cyber Threat Intelligence (CTI) d'une organisation, collecter et analyser en continu les informations sur les menaces potentielles du cyberespace et consigner les résultats sous forme adéquate, conformément à leur finalité et aux groupes cibles.
Objectifs opérationnels	1 Collecter de façon continue, proactive et autodirigée des informations sur les menaces actuelles du cyberespace. 2 Vérifier et évaluer la crédibilité des informations. 3 Evaluer le potentiel de risque des menaces en tenant compte de la stratégie de sécurité de l'information et de l'infrastructure informatique d'une organisation. 4 Analyser les informations sur les menaces et documenter les résultats sur les plans tactique et opérationnel de la CTI. 5 Traiter les résultats issus de la CTI et les communiquer aux parties prenantes internes ou externes sous forme adéquate, conformément aux groupes cibles et aux niveaux concernés.
Domaine de compétence	Security/Risk Management
Objet	Organisation avec une infrastructure informatique complexe, une stratégie de sécurité de l'information donnée et une organisation structurelle et fonctionnelle définie en termes de Cyber Threat Intelligence (CTI).
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	679
Titre	Collecter des informations sur les menaces et les traiter
Compétence	Dans le cadre de la Cyber Threat Intelligence (CTI) d'une organisation, collecter et analyser en continu les informations sur les menaces potentielles du cyberespace et consigner les résultats sous forme adéquate, conformément à leur finalité et aux groupes cibles.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître la finalité de la Cyber Threat Intelligence (CTI) et ses différents niveaux (p.ex. stratégique, tactique et opérationnel).
	1.2	Connaître diverses causes de menace (p.ex. acte délibéré, vulnérabilités, défaillance technique, com-portement humain inadéquat, cas de force majeure) et pouvoir en expliquer la pertinence quant à la sécurité de l'information et à la cybersécurité.
	1.3	Connaître des sources d'informations internes et externes sur les menaces (p.ex. organisations CERT, catalogue des menaces MELANI, ENISA et BSI, listes d'adresses électroniques, avis et rapports de sécu-rité de fabricants et de prestataires tiers, rapports sandbox, échange d'expériences au sein du réseau de relations, OWASP Top 10, SANS Top 20).
	1.4	Connaître diverses formes de menace et de vecteurs d'attaque (p.ex. maliciels, menace persistante avancée [APT], rançongiciel, attaques DDoS, spoofing, phishing, attaques DNS, bots et réseaux de bots, injection de script, vol de session [session hijacking], ingénierie sociale, courriers indésirables) et pouvoir les expliquer sous l'angle de la voie d'attaque, de la technique d'attaque et de l'objectif de l'attaque (p. ex. panne du système, utilisation abusive du système, vol, fraude, chantage).
2	2.1	Connaître des indicateurs pour évaluer la crédibilité des informations (p.ex. auteur, éditeur, format, indication des sources, actualité, vérifiabilité, reproductibilité) et pouvoir en expliquer la pertinence pour différentes sources.
3	3.1	Connaître les directives et les éléments déterminants de la stratégie de sécurité de l'information d'une organisation (p.ex. appétence au risque, tolérance au risque, objectifs de sécurité stratégiques, inven-taire et classification des valeurs [assets]).
	3.2	Connaître l'infrastructure informatique et le paysage système d'une organisation et pouvoir expliquer la pertinence d'une menace pour les systèmes, réseaux et applications spécifiques à une organisation.
	3.3	Connaître des modèles courants d'évaluation des risques et des menaces (p.ex. matrice des risques, méthodologie d'évaluation des risques de l'OWASP, système d'évaluation standardisé de la criticité des vulnérabilités [CVSS]).

Connaissances opérationnelles nécessaires

4	4.1	Connaître l'importance des descriptions de tactiques, techniques et procédures (TTP) et pouvoir en expliquer l'utilité pour la cybersécurité d'une organisation.
	4.2	Connaître l'importance des indicateurs d'attaque (IoA) et pouvoir citer des exemples typiques (p.ex. anomalies dans le trafic réseau, anomalies dans les heures d'utilisation, requêtes DNS suspectes, redirection des utilisateurs).
	4.3	Connaître l'importance des indicateurs de compromission (IoC) et pouvoir citer des exemples typiques (p.ex. valeurs de hachage, signatures numériques, noms de domaine, adresses IP, URL, adresses e-mail, X-Mailer, HTTP User Agent).
	4.4	Connaître des normes et des modèles courants de classification des menaces (p.ex. taxonomie CERT, taxonomie MISP, taxonomie eCSIRT, Europol Common Taxonomy for Law Enforcement and CSIRTs).
5	5.1	Connaître les parties prenantes internes ou externes déterminantes de la CTI (p.ex. management, CISO, analystes SOC, incident response team [CERT/CIRT], gestion des vulnérabilités et des correctifs, architectes système, administrateurs système, autorités en charge des poursuites pénales) et pouvoir expliquer leurs besoins spécifiques en informations.
	5.2	Connaître divers canaux de communication (p.ex. rapports écrits ou verbaux, collecticiel [groupware], wiki, base de connaissances, forums, médias sociaux) et pouvoir expliquer leurs différences quant à leur impact, fiabilité et sécurité.
	5.3	Connaître des plateformes et des cadres d'échange d'informations courants dans le domaine de la CTI (p.ex. Malware Information Sharing Platform [MISP], Collective Intelligence Framework [CIF], Collaborative Research Into Threats [CRITs], Open Threat Exchange [OTX]).
	5.4	Connaître des formats usuels d'informations CTI (p.ex. STIX, OpenIOC, Intrusion Detection Message Exchange Format [IDMEF], Incident Object Description Exchange Format [IODEF]) et des standards pour l'échange de données CTI lisible par machine (p.ex. TAXII).

Version du module	1.0
Créé le	11.02.2021