Identification du module

Numéro de module	682	
Titre	Gérer les incidents de sécurité	
Compétence	Piloter et surveiller le traitement des incidents de sécurité identifiés tout au long de leur cycle de vie conformément aux structures et aux processus définis dans le cadre de la gestion des incidents de sécurité d'une organisation.	
Objectifs opérationnels	1	Analyser, catégoriser et prioriser les incidents de sécurité dans le cadre du fonctionnement opérationnel et définir, selon le plan de réponse aux incidents, la future marche à suivre pour traiter les différents incidents.
	2	Engager des mesures immédiates appropriées et efficaces en vue de réduire les répercussions d'un incident de sécurité.
	3	Coordonner avec les divisions spécialisées compétentes les mesures techniques requises pour un retour à la normale.
	4	Garantir, si nécessaire, la préservation des éléments de preuve et communiquer les incidents de sécurité pertinents aux divisions ou organes compétents en vue de procéder à des analyses forensiques numériques détaillées.
	5	Soutenir et conseiller de façon ciblée et conformément aux besoins l'organisation d'urgence ou de crise en cas de graves incidents de sécurité.
	6	Documenter et surveiller le traitement d'un incident de sécurité tout au long du cycle de vie et, si nécessaire, procéder à une escalade.
	7	Evaluer périodiquement les incidents de sécurité et faire en sorte que les enseignements tirés soient intégrés dans l'organisation.
Domaine de compétence	Service Management	
Objet	Organisation dotée de structures et de processus définis en vue de détecter et de traiter les incidents de sécurité (Security Incident Management).	
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	682
Titre	Gérer les incidents de sécurité
Compétence	Piloter et surveiller le traitement des incidents de sécurité identifiés tout au long de leur cycle de vie conformément aux structures et aux processus définis dans le cadre de la gestion des incidents de sécurité d'une organisation.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître l'importance et le contenu d'un plan de réponse aux incidents pour le traitement des incidents de sécurité.
	1.2	Connaître des facteurs d'influence pour l'analyse et le tri des incidents de sécurité (p. ex. degré de gravité des répercussions, niveau d'urgence de la réponse, ampleur, personnes et services touchés).
	1.3	Connaître des concepts de catégorisation et de priorisation des incidents de sécurité.
	1.4	Connaître des outils permettant d'administrer les incidents de sécurité de l'information (p. ex. système de gestion des incidents de sécurité, système de suivi de problèmes [issue tracking system], banque de données répertoriant les problèmes).
2	2.1	Connaître des mesures techniques immédiates de blocage des vecteurs d'attaque (p. ex. séparation, isolation, désactivation, déconnexion, sinkholding).
	2.2	Connaître des critères d'évaluation de l'adéquation des mesures immédiates (p. ex. danger potentiel, complexité et chances de réussite, temps requis, niveau de gravité des préjudices, ampleur de l'impact).
3	3.1	Connaître les divisions ICT spécialisées et les processus concernés au sein de l'organisation et pouvoir expliquer leurs compétences et besoins pour un retour à la normale (p. ex. Service Operations, Service Continuity Management, Release and Deployment Management, Service Asset and Configuration Management, Service Level Management).
	3.2	Connaître les différences entre style de direction directif et participatif, entre procédure orientée structures, orientée processus et orientée personnes ainsi qu'entre une communication formelle et informelle et pouvoir expliquer leur adéquation situationnelle respective lors de la coordination des parties prenantes.
	3.3	Connaître les directives de l'entreprise relatives à la reprise d'activité (business recovery) et pouvoir expliquer les objectifs déterminants dans le cadre du retour à la normale (p. ex. recovery time objective [RTO], recovery point objective [RPO]).
	3.4	Connaître les directives de l'entreprise en termes de Business Continuity Management (BCM) et pouvoir expliquer la pertinence des mesures BCM planifiées pour le retour à la normale.

Connaissances opérationnelles nécessaires

4	4.1	Connaître les principes des investigations numériques (p. ex. intégrité, crédibilité, reproductibilité, documentation).
	4.2	Connaître les exigences en termes de recevabilité légale des éléments de preuve (p. ex. duplication forensique, principe des quatre yeux, journalisation exhaustive).
	4.3	Connaître les directives de l'entreprise et les compétences en matière d'analyses forensiques numériques (p. ex. Incident Response Team [CERT/CIRT], spécialistes externes, autorités de poursuites pénales).
5	5.1	Connaître les caractéristiques des situations d'urgence et des crises et pouvoir expliquer les différences par rapport à un fonctionnement opérationnel normal.
	5.2	Connaître les compétences et les processus d'une organisation dans le cadre de la maîtrise des crises et des situations d'urgence.
	5.3	Connaître les principes de base de la communication de crise (rapidité, véracité, langage compréhensible, cohérence) et les différents groupes cibles (p. ex. personnes concernées, autorités, médias, parties impliquées) et pouvoir expliquer l'importance d'une communication adaptée au public cible.
6	6.1	Connaître les éléments de contenu d'une documentation claire et compréhensible relative aux incidents de sécurité (rapport d'incident [incident record]).
	6.2	Connaître des standards et des modèles permettant une description et une classification structurée des incidents de sécurité (p. ex. taxonomie CERT, taxonomie MISP, taxonomie eCSIRT, Europol Common Taxonomy for Law Enforcement and CSIRTs).
	6.3	Connaître des éléments déclencheurs d'un processus d'escalade (p. ex. liés à la quantité dans le temps, à la qualité du contenu, à des personnes) et pouvoir expliquer des exemples typiques de la gestion des incidents de sécurité (p. ex. priorité de l'incident de sécurité, niveaux de service issus des SLA et niveaux opérationnels issus des OLA, RTO et RPO en ce qui concerne la reprise après sinistre [disaster recovery]).
	6.4	Connaître le processus d'escalade et la hiérarchie d'escalade d'une organisation dans le cadre de la gestion des incidents de sécurité.
7	7.1	Connaître des valeurs statistiques et des indicateurs clés de performance (ICP) dans le contexte de la gestion des incidents de sécurité.
	7.2	Connaître des méthodes et des techniques appropriées pour synthétiser et représenter les informations (p. ex. 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).
	7.3	Connaître les directives de l'entreprise en matière d'amélioration continue et pouvoir expliquer les besoins en informations spécifiques et les compétences des parties prenantes concernées (p. ex. management, CISO, CTI, gestion des changements, compliance, ressources humaines, divisions ICT, collaborateurs).

Version du module	1.0
Créé le	11.02.2021