Identification du module

Numéro de module	681	
Titre	Détecter et contrer les attaques ciblant l'infrastructure informatique	
Compétence	Choisir des solutions techniques de surveillance et de protection en vue de détecter et de contrer les attaques ciblant les systèmes, les réseaux et les applications d'une organisation et les mettre en service.	
Objectifs opérationnels	1	Définir, en tenant compte de la situation des menaces, les indicateurs, signatures et motifs pertinents pour détecter des attaques contre l'infrastructure informatique d'une organisation.
	2	Choisir des solutions de surveillance et de protection pour la détection d'attaques basée réseau et leur blocage et mettre celles-ci en service.
	3	Choisir des solutions de protection et de durcissement appropriées pour la détection d'attaques basée hôte et application et leur blocage et mettre celles-ci en service.
	4	Choisir, au regard des directives de l'organisation relatives à la classification des informations, des solutions appropriées de protection des données sensibles contre leur diffusion non autorisée et mettre celles-ci en service.
	5	Choisir, si nécessaire, des solutions appropriées pour leurrer les attaquants et mettre celles-ci en service.
	6	Configurer, en tenant compte des dispositions légales en matière de protection de la personnalité et des données, la journalisation des données concernées dans les solutions de surveillance et de protection.
	7	Tester régulièrement le fonctionnement et l'efficacité des solutions de surveillance et de protection et corriger, si nécessaire, la configuration.
	8	Intégrer les solutions de surveillance et de protection dans un système supérieur de gestion des événements et des informations de sécurité (SIEM).
Domaine de compétence	System Management	
Objet	Organisation dotée d'une infrastructure informatique complexe.	
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		681
Titre		Détecter et contrer les attaques ciblant l'infrastructure informatique
Compétence		Choisir des solutions techniques de surveillance et de protection en vue de détecter et de contrer les attaques ciblant les systèmes, les réseaux et les applications d'une organisation et les mettre en service.
Objectifs opérationnels et connaissances opérationnelles nécessaires		
1	1.1	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, pourriels) 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).
	1.2	Connaître des concepts fondamentaux de détection d'attaques (p.ex. recherche basée sur des motifs ou des règles, détection d'anomalies, inspection de paquets et du contenu, vérification de l'intégrité des fichiers, surveillance des processus, contrôle des journaux).
	1.3	Connaître l'importance des tactiques, techniques et procédures (TTP), des indicateurs d'attaque (IoA) et des indicateurs de compromission (IoC) pour la détection des attaques.
2	2.1	Connaître des normes de réseau courantes (IEEE 802) pour les réseaux locaux (LAN), les réseaux locaux sans fil (WLAN), les réseaux personnels ainsi que les réseaux personnels sans fil (PAN, WPAN) et pouvoir expliquer leurs caractéristiques.
	2.2	Connaître des protocoles d'application courants dans les réseaux TCP/IP (p.ex. HTTP, protocoles de messagerie, DHCP, DNS, annuaires, protocoles de transfert de fichiers, protocoles de gestion des réseaux).
	2.3	Connaître des protocoles de réseau et de transport courants en termes de sécurité cryptographique (p.ex. IPSec, TLS) et leur champ d'application pour un transfert sécurisé des données (p.ex. HTTPS, SMTPS, SIPS, FTPS, SFTP, LDAPS).
	2.4	Connaître des concepts de séparation physique ou logique des réseaux sur différentes couches OSI (p.ex. Spanning Tree Protocol [STP], commutateur de couche 2 et de couche 3, subnetting, VLAN, pare-feu, zone démilitarisée [DMZ], proxy inverse, serveur d'entrée Web [WES], pare-feux applicatifs Web [WAF], répartition de charge [load balancing] et pouvoir expliquer leur fonction.
	2.5	Connaître des outils appropriés pour surveiller le trafic réseau (p.ex. analyseur de paquets Wireshark, MRTG, Nmap, Nagios, lignes de commande pertinentes).

Connaissances opérationnelles nécessaires

	2.6	Connaître les fonctions, les possibilités et les limites des systèmes de détection et de prévention d'intrusion basés réseau (NIDS/NIPS) et pouvoir citer des outils courants (p.ex. Snort, Suricata).
	2.7	Connaître l'importance et le principe de fonctionnement des tarpits pour lutter contre les spams et les vers et pouvoir citer des outils usuels (p.ex. LaBrea, Netfilter).
3	3.1	Connaître des concepts fondamentaux de durcissement des systèmes (p.ex. administration des utilisateurs et authentification, contrôle des accès, désactivation ou limitation des services, chiffrement du disque dur) et pouvoir citer des sources relatives aux meilleures pratiques en matière du durcissement de systèmes d'exploitation courants (p.ex. Windows, Unix/Linux, Mac OS, iOS, Android).
	3.2	Connaître des sources de guides, de directives et de standards courants en matière de durcissement de systèmes et d'applications spécifiques (p.ex. CIS Benchmarks, OpenSCAP, Microsoft Security Baselines, STIG de la DISA, guides de durcissement de la sécurité propres à des produits).
	3.3	Connaître les fonctions, les possibilités et les limites de systèmes de détection et de prévention d'intrusion basés hôte (HIDS/HIPS) et pouvoir citer des outils courants (p.ex. Open Source Tripwire, IDDS, Botshield, Samhain, armes cybernétiques).
	3.4	Connaître les fonctions, les possibilités et les limites de solutions de protection pertinentes basées application (p.ex. WAF basé hôte, filtre anti-spam) et pouvoir citer des outils courants (p.ex. ModSecurity, Fortinet, SpamAssassin, RSPAMD).
4	4.1	Connaître les lignes directrices de l'organisation sur la classification des données quant à leur confidentialité (p.ex. secret, confidentiel, diffusion restreinte, interne et public) et à leur intégrité (p.ex. vital, important, normal) et pouvoir expliquer leur pertinence en ce qui concerne la protection des données sensibles.
	4.2	Connaître des possibilités techniques de protection des données en mouvement (data in motion) sur différents canaux (p.ex. Web, courrier électronique, partages).
	4.3	Connaître des possibilités techniques de protection des données traitées (data at use).
	4.4	Connaître des possibilités techniques de protection des données stockées (data at rest) sur différents supports de stockage (magnétique, optique ou électronique) et dans diverses architectures de stockage (p.ex. NAS, SAN, cloud).
	4.5	Connaître différentes architectures et des fonctions typiques des solutions de protection dans le domaine de la prévention de la perte ou fuite de données (DLP).
5	5.1	Connaître l'importance des honeypots et des honeynets pour leurrer les attaquants et analyser les attaques et pouvoir expliquer leurs caractéristiques en termes d'architecture (client/serveur, physique/virtuelle) et d'interaction (basse/élevée).
	5.2	Connaître des outils courants pour les serveurs honey (p.ex. Honeyd, HoneyTrap, Argos) et les honey clients (p.ex. PhoneyC, mapWOC).
	5.3	Connaître la finalité des honey links dans les applications Web et pouvoir expliquer leur traitement dans les pare-feux applicatifs Web (WAF).

Connaissances opérationnelles nécessaires

6	6.1	Connaître les dispositions régissant la surveillance du comportement personnel issues de la loi sur le travail et de la loi sur la protection des données.
	6.2	Connaître les dispositions de la protection des données en termes de pseudonymisation et d'anonymisation des données à caractère personnel et pouvoir expliquer comment observer les principes de licéité, de proportionnalité, de finalité et de transparence à l'aide d'exemples types d'application.
7	7.1	Connaître des techniques et des outils appropriés de simulation d'attaques (p.ex. scanner de ports, scripts d'exploit, générateurs de charge utile, générateurs SYN flood, générateurs de tests de stress et générateurs de faux positifs).
	7.2	Connaître l'importance des faux positifs dans les solutions de surveillance et de protection et pouvoir expliquer par quels moyens les détecter et les réduire.
	7.3	Connaître les principaux éléments de description des cas de test (p.ex. identification, conditions, consignes d'exécution, procédures et outils, comportement attendu) et établir un protocole de test clair et compréhensible (p.ex. responsabilité, horodatation de l'exécution des tests, résultats des tests, traitement des anomalies et mesures).
8	8.1	Connaître les principales fonctions des systèmes SIEM (collecte et agrégation des données au moyen de collecteurs/agents, présentation des résultats, alarme, application des règles, archivage des données) et pouvoir citer des outils courants (p.ex. ELK Stack, Apache Metron, OSSEC, AlienVault OSSIM, Splunk).
	8.2	Connaître des formats courants d'échange de données lisible par machine entre divers clients et le SIEM (p.ex. Interface for Metadata Access Points [IF-MAP], Common Event Format [CEF], formats Syslog, CSV, XML, valeur-clé).

Version du module	1.0
Créé le	11.02.2021