Dictionnaire de la cybersécurité

by

METSYS

© Copyright 2022 METSYS. Tous droits réservés - www.metsys.fr

Ransomware, cheval de Troie, SOC, firewall... autant de termes techniques couramment utilisés lorsque l'on parle de cybersécurité. Difficile de s'y retrouver ! Pourtant, si l'on veut lutter efficacement contre les cyberattaques, surtout en qualité de dirigeant sur qui repose la responsabilité de protéger son entreprise, il est important de maîtriser ces terminologies.

C'est ce que nous vous proposons dans ce document, qui a pour objectif d'être le plus exhaustif possible pour vous aider à vous approprier la sémantique liée à la cybersécurité.

Avec ce glossaire, plus besoin de Google !

Bonne lecture !

comme

Alerte Cybersécurité : document créé et diffusé lorsqu'une vulnérabilité ou faille de sécurité est détectée. Cette alerte détaille tous les éléments liés à cette vulnérabilité (nom, risques, systèmes affectés, solutions). En France, elles sont rédigées et diffusées par le CERT-FR, centre gouvernemental de vielle, d'alerte et de réponse aux attaques informatiques dépendant de l'ANSSI.

Analyse forensique : est une méthode d'investigation pour identifier les preuves numériques d'une cyberattaque, en vue d'une procédure judiciaire. Elle permet également de comprendre la chronologie des événements et d'identifier l'origine et les causes de l'attaque.

Anti-virus : est une solution qui protège le poste de travail, la tablette, le mobile ou l'ordinateur portable de toute intrusion, via différentes méthodes : recherche de la signature virale (portion du virus informatique), analyse du comportement du code malveillant... Le principe de l'antivirus est de s'appuyer sur une bibliothèque de signatures identifiées par les créateurs de ces logiciels de sécurité. L'anti-virus peut détruire, mais également empêcher l'exécution du code malveillant. Une nouvelle catégorie d'anti-virus a été développée, appelée « next gen » qui utilise les méthodes de l'intelligence artificielle, ils bloquent à la source les attaques avant même qu'elles atteignent les infrastructures.

APT : ou menace persistante avancée, est une attaque informatique ciblée et prolongée qui nécessite un haut niveau technique. Les cibles sont principalement les grandes entreprises et les états, mais pour atteindre ces grandes organisations, les pirates peuvent être amenés à lancer leurs attaques sur de plus petites entreprises (prestataires, partenaires). Ce type d'attaque cherche à voler des informations sur une longue période.

Attaque Cyber ou Cyber-Attaque : est une attaque informatique menée soit par des cybercriminels dans un but malveillant (vol de données, fraude, extorsion...). Elles peuvent être lancées sous la forme d'un ransomware, d'une campagne de phishing, d'attaque par déni de service (DDoS), par injection SQL.

Attaque DDoS : ou attaque par déni de service, cette attaque pour objectif de surcharger le trafic d'un système, d'un site web, d'un serveur, d'un réseau afin d'en épuiser la bande passante. Elles empêchent ainsi les utilisateurs (ou internautes) d'accéder aux ressources ou au site web ciblé. Le trafic provient de plusieurs milliers de sources, souvent via des machines zombies.

Attaque "Man-in-the-Middle" : a pour but de capter, de manière furtive, les échanges entre deux parties afin d'exfiltrer des données (codes bancaires, documents, ...). Ces attaques s'appuient principalement sur des points d'entrée courants : un réseau wi-fi public non sécurisé ou via une faille qui lui aura permis d'installer un logiciel malveillant.

Audit de Sécurité : est une approche qui a pour objectif d'analyser la robustesse d'un système informatique, d'une application, d'un serveur, ... il recense les points forts, mais surtout les éventuelles failles de sécurité, qui pourraient permettre à des cyberattaquants de les exploiter à des fins malveillantes.

C comme

Backdoor : ou porte dérobée, qui donne un accès secret, inconnu par l'utilisateur, aux données contenues dans un logiciel ou sur un matériel. Parfois créée par les développeurs pour résoudre des problèmes ou des failles dans la programmation, ces portes dérobées sont également très souvent exploitées par les cybercriminels pour y introduire un logiciel malveillant, pour surveiller l'activité de l'utilisateur, voire prendre le contrôle de la machine.

Black Hat vs White Hat : Un black hat est un hacker malveillant qui tire profit de ses compétences à des fins frauduleuses. Quant au white hat, ou ethical hacker (hacker éthique), il utilise ses connaissances techniques en informatiques pour réaliser des tests d'intrusion (pentest) afin d'assurer la sécurité des systèmes d'information d'une organisation. Son objectif est, pour l'ehtical hacker, d'identifier des failles et/ou vulnérabilités persistantes.

Botnet : contraction de l'anglais « robot net » qui veut dire réseau de robots, un botnet est donc un réseau d'appareils électriques infectés et contrôlés par des malwares. Couramment utilisés par les cybercriminels pour mener des attaques par déni de services /DDoS (ou d'autres types d'attaques), les botnets ont fait la une des médias lors d'une attaque menée contre OVH en 2016. L'assaut avait été lancé via un réseau de caméras !

Brute force : cette catégorie d'attaque consiste à tester, une à une, des combinaisons possibles de mots de passe ou de clés pour accéder aux services, serveurs ou applications ciblés.

Bug Bounty : prime aux bugs en français, est une gratification financière qu'une entreprise offre à qui trouvera la ou les failles/vulnérabilités dans son système ou dans une de ses applications. Apple a lancé son bug bounty avec la clé jusqu'à un million de dollars pour une vulnérabilité majeure détectée dans son iOS (système d'exploitation des iPhone) !

Bug informatique : dysfonctionnement d'un programme informatique.

C comme

CERT / CSIRT : (**C**omputer **E**mergency **R**esponse **T**eam ou **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam) est une équipe constituée d'analystes et d'experts dont les objectifs sont de réagir face aux incidents informatiques, de prévenir en instaurant des campagnes de sensibilisation et d'information, mais surtout d'alerter les entreprises et administrations en cas de cyberattaques.

Cheval de Troie : comme dans le mythe de la guerre du même nom, un cheval de Troie est un logiciel qui semble à première vue inoffensif. Cependant une fois intégré dans le système, il agit comme un logiciel malveillant. Le cheval de Troie est classé dans la catégorie des malwares.

Clé de chiffrement : est une suite de chiffres et de lettres issue d'une opération cryptographique, qui sert à coder un message afin de le rendre inviolable.

Cryptographie : discipline de la cryptologie, ce terme générique regroupe toutes les techniques pour protéger des messages, afin d'en assurer la confidentialité, l'authenticité et l'intégrité.

Cryptomonnaie : est une monnaie numérique qui utilise des algorithmes cryptographiques et un protocole appelé « blockchain » qui assure la fiabilité et la traçabilité lors des transactions. Elles sont stockées dans des portefeuilles numériques. Elles ne dépendent pas d'une Banque centrale. Les plus connues sont le Bitcoin, l'Ethereum, le Ripple, l'EOS...

Cyber-hacktivisme : est une forme de militantisme utilisant des compétences en piratage informatique pour arriver à ses fins, principalement dans le cadre d'actions visant à obtenir une justice politique, sociale ou religieuse. Anonymous est l'un des groupes de cyberactivisme les plus connus, on peut également mentionner Julian Assanges, le fondateur de Wikileaks.

Cyber-résilience : capacité d'une organisation à surmonter les conséquences d'un choc. On parle de cyber-résilience dans le cadre d'un processus d'amélioration continue, qui s'appuie sur deux axes : une démarche préventive et une meilleure réactivité en cas d'incident.

O comme

Dark Web / Dark Net : est l'ensemble des sites web disponibles uniquement via un navigateur spécifique et conçu à cet effet. Il permet de préserver l'anonymat et la confidentialité des activités sur Internet ; il est d'ailleurs très utilisé pour échapper à la censure, mais également dans le cadre d'activités illégales. Le dark web est un élément du Deep Web.

Deep Web : partie de la toile non indexée par les principaux moteurs de recherche.

Data Breach (Fuite de donnée) : est souvent la conséquence d'un incident grave de sécurité. Cela se traduit par la divulgation d'informations au sein d'environnements non sécurisés, tels que le Dark Web.

Doxing : pratique qui consiste à rechercher et à diffuser sur Internet des informations sur l'identité et la vie privée d'une personne afin de lui nuire. Cette méthode est particulièrement utilisée par les cyberactivistes.

comme

EDR : EndPoint Detection and Response, est une catégorie de solutions de sécurité dont l'objectif est de fournir des fonctionnalités plus poussées qu'un simple antivirus. Ces solutions sont capables de collecter des données comportementales et d'identifier des anomalies, permettant ainsi aux équipes cybersécurité de mener des actions correctives.

comme

Firewall : Première défense technologique face aux cyberattaques qui permet d'appliquer les règles de sécurité du réseau définies par l'entreprise ; celles-ci déterminent ainsi le type de communication autorisé, ou non. Le firewall surveille et contrôle les applications et les flux de données.

comme

Incident Cyber ou Cyber-Incident : est un événement qui porte atteinte à l'intégrité et à la disponibilité d'un système d'information. Par exemple, un vol de mot de passe, un vol d'équipement informatique, une intrusion, etc...

Ingénierie Sociale : consiste à manipuler psychologiquement une personne à des fins d'escroquerie. Par ce biais, les cybercriminels incitent leurs victimes à partager des informations confidentielles. Cela peut se traduire par des attaques de type phishing, ou tout simplement, par un appel téléphonique au ton un peu pressant pour convaincre la victime à mettre à jour ses informations bancaires par exemple.

Injection SQL : est un type de cyberattaque. L'injection de commandes SQL permet au pirate, via des requêtes spécifique, d'introduire son propre code dans un site web pour collecter des informations depuis la base de données de celui-ci sans pour autant avoir les privilèges nécessaires.

M comme

Machine zombie : est un ordinateur contrôlé, via un ver ou un virus, par un cybercriminel à des fins malveillantes.

Malware : est un logiciel malveillant et développé dans le but de porter préjudice à une entreprise, une organisation ou un particulier en infectant l'intégrité de son système d'information. Exemple de malware : ransomware, cheval de Troie, virus, etc...

MFA : Multi Factor Authentication ou en français,: authentification à plusieurs facteurs, est un dispositif d'authentification électronique composé de plus d'un élément de preuve de l'identité de l'utilisateur (empreinte digitale, reconnaissance faciale, réponse à une question, envoi d'un code, etc...)

MSP : ou Management Service Provider, est un fournisseur de services managés spécialisé dans les solutions de sécurité. Il gère à distance les outils de sécurité pour le compte d'entreprises et d'organisations.

comme

PASSI : Prestataire d'Audit de la Sécurité des Systèmes d'Information. Cette certification délivrée par l'ANSSI – Agence Nationale de Sécurité et des Systèmes d'Information – atteste du niveau d'exigence et d'expertise des prestataires certifiés pour les analyses, les évaluations et l'accompagnement en cybersécurité.

PDIS : Prestataire de Détection d'Incident de Sécurité. Délivrée par l'ANSSI, cette certification permet d'attester du niveau de compétence et de maturité d'une société proposant des services de SOC, après avoir fait l'objet d'une évaluation, afin d'en éprouver son bon niveau de sécurité.

Pentest : penetration testing ou test d'intrusion. Permet d'évaluer la sécurité d'un système d'information, d'un réseau informatique ou encore d'une application. Un pentester (la personne réalisant le pentest) applique les mêmes méthodes que celles utilisées par de vrais cyberattaquants.

Phishing ou Hameçonnage : technique largement utilisée par les cybercriminels qui mettent leur victime en situation d'urgence, ou à contrario, en confiance pour les inciter à réaliser une action, comme cliquer sur un lien pour introduire un malware (type ransomware) ou mettre à jour ses données bancaires. Pour duper leur cible, les cyberattaquants peuvent par exemple usurper l'identité visuelle d'une banque ou d'un site de ecommerce dans un mail.

PSSI : Politique de Sécurité du Système d'Information, est un plan d'actions visant à maintenir un bon niveau de sécurité au sein d'une organisation.

comme

Ransomware ou Rançongiciel : est un logiciel malveillant (malware) qui prend en otage les données, les fichiers, voire les ordinateurs afin d'extorquer de l'argent à l'entreprise ou à son propriétaire.

Risk Management : est l'évaluation des risques éventuels auxquels une entreprise doit faire face. Il permet de les anticiper, de prendre les mesures de contrôle adéquates, et ainsi de permettre la continuité de l'entreprise en cas d'incident.

Risk Assessment : désigne en cybersécurité l'identification des failles de sécurité liées aux équipements et aux données d'une entreprise et permet ainsi d'évaluer son importance au sein de l'organisation.

comme

Shadow IT : constitue tout ce qui est mis en place (applications, équipements...) au sein de l'entreprise sans l'accord de la direction informatique.

SIEM : Security Information and Event Management, est une technologie liée à la cybersécurité qui permet de surveiller, détecter et alerter tout événement ou incident lié à la sécurité du système d'information. Il fournit une vision globale et centralisée de la posture de sécurité d'une infrastructure IT.

SOC : Le Security Operation Center rassemble des analystes et des experts en cybersécurité dont la mission est de surveiller et d'analyser en permanence le dispositif d'une entreprise. L'équipe en charge du SOC travaille donc de concert pour détecter, analyser, réagir, signaler, prévenir et remédier en cas d'incident de sécurité.

Spear Phishing : désigne une variante du phishing qui, au lieu de s'adresser à un très large public, cible très finement les victimes en utilisant des informations concrètes et réalistes.

Spoofing : consiste à usurper une adresse électronique pour atteindre sa cible.

SSO : Single Sign One, est une méthode qui permet d'accéder à diverses solutions et applications grâce à une seule authentification.

Supply Chain Attack : est une attaque qui cherche à infester une organisation par le biais d'un des éléments de sa chaîne d'approvisionnement ou de prestataires.

comme

Threat Intelligence : est une logique de défense fondée sur le renseignement des menaces via la collecte, l'analyse et le partage en continu de données, avec pour objectif la prévention des cyberattaques. Les données sont contextualisées par des spécialistes afin d'identifier les éventuelles menaces.

comme

Vulnérabilité : ou faille de sécurité est un point faible au sein d'un système informatique permettant aux cyberattaquants d'y pénétrer.

comme

Web de surface : ou web visible ou indexable, est la partie du World Wide Web accessible par tous les utilisateurs et identifiée par les moteurs de recherche.

METSYS

Besoin d'une expertise cyber ?

Contactez-nous

Cédric MATHARAN
Directeur commercial cybersécurité
cedric.matharan@metsys.fr

© Copyright 2022 METSYS. Tous droits réservés - www.metsys.fr