Glossaire de la Cybersécurité

Terme	Définition
SIEM (Security Information and Event Management)	Centralisation, corrélation et analyse des événements de sécurité.
EDR (Endpoint Detection and Response)	Protection avancée des terminaux, détection et réponse aux menaces.
XDR (Extended Detection and Response)	Évolution de l'EDR intégrant plusieurs couches (endpoint, réseau, cloud, email).
IDS (Intrusion Detection System)	Système de détection d'intrusion qui alerte en cas d'anomalie.
IPS (Intrusion Prevention System)	Version proactive de l'IDS qui bloque automatiquement les attaques.
UEBA (User and Entity Behavior Analytics)	Analyse des comportements pour détecter des anomalies (fraudes, insiders).
NOC (Network Operations Center)	Centre de supervision réseau (disponibilité/performance).
SOC (Security Operations Center)	Centre de supervision sécurité (détection et réponse aux incidents).
CERT (Computer Emergency Response Team)	Équipe de gestion des incidents de cybersécurité.
CSIRT (Computer Security Incident Response Team)	Variante souvent interne d'un CERT.
DPO (Data Protection Officer)	Responsable de la conformité RGPD et protection des données personnelles.
Vulnerability (Vulnérabilité)	Faiblesse exploitable dans un système.
Exploit	Code ou technique qui tire parti d'une vulnérabilité.
Zero-Day	Vulnérabilité inconnue de l'éditeur, sans correctif.
Patch Management	Gestion et application des correctifs de sécurité.
Pentest (Penetration Testing)	Test d'intrusion simulant une attaque réelle.
Red Team	Équipe offensive simulant des attaques.
Blue Team	Équipe défensive protégeant et détectant les attaques.
Purple Team	Collaboration Red/Blue Team pour améliorer les défenses.
APT (Advanced Persistent Threat)	Attaque ciblée, discrète et de longue durée, souvent sponsorisée par un État.
Phishing	Technique d'ingénierie sociale visant à voler des données sensibles.
Ransomware	Malware qui chiffre les données et réclame une rançon.
Botnet	Réseau de machines compromises contrôlées par un attaquant.
VPN (Virtual Private Network)	Tunnel chiffré pour sécuriser les communications.
Firewall (Pare-feu)	Filtrage du trafic réseau selon des règles.
DMZ (Demilitarized Zone)	Zone réseau intermédiaire entre Internet et le réseau interne.

Reverse Proxy	Serveur intermédiaire qui protège et distribue les requêtes vers les serveurs internes.
Load Balancer	Répartiteur de charge entre plusieurs serveurs pour fiabilité/performance.
Cryptographie	Science de la protection de l'information par transformation mathématique.
Clé Symétrique	Une seule clé utilisée pour chiffrer et déchiffrer.
Clé Asymétrique	Couple clé publique/clé privée pour chiffrer, signer ou authentifier.
PKI (Public Key Infrastructure)	Infrastructure gérant certificats et clés cryptographiques.
Certificat numérique	Preuve électronique d'identité, émise par une autorité de certification.
TLS (Transport Layer Security)	Protocole de sécurisation des communications réseau (HTTPS).
Hachage (Hashing)	Transformation irréversible d'une donnée (ex. SHA-256).
Signature numérique	Garantie de l'authenticité et de l'intégrité d'un message.
OTP (One-Time Password)	Mot de passe à usage unique pour renforcer l'authentification.
MFA (Multi-Factor Authentication)	Authentification combinant plusieurs facteurs (mot de passe, SMS, biométrie).
IAM (Identity and Access Management)	Gestion des identités et des droits d'accès.
RBAC (Role-Based Access Control)	Attribution des accès selon le rôle de l'utilisateur.
SSO (Single Sign-On)	Authentification unique donnant accès à plusieurs services.
OAuth 2.0	Standard d'autorisation déléguée (utilisé par Google, Facebook, etc.).
OIDC (OpenID Connect)	Extension d'OAuth 2.0 pour l'authentification.
IaaS (Infrastructure as a Service)	Mise à disposition d'infrastructures virtuelles (VM, stockage).
PaaS (Platform as a Service)	Plateforme prête à l'emploi pour développer/déployer des applications.
SaaS (Software as a Service)	Logiciel hébergé et accessible via Internet (ex : O365).
Cloud hybride	Combinaison de cloud public et privé.
Conteneurisation	Isolation d'applications dans des conteneurs (ex. Docker).
Kubernetes	Orchestrateur de conteneurs pour automatiser le déploiement et la gestion.
Zero Trust	Modèle de sécurité qui ne fait confiance à aucun utilisateur ou appareil par défaut, même en interne.