Glossaire
Sécurisez votre chaîne de développement logiciel avec l'OWASP

ANSSI : *Agence nationale de la sécurité des systèmes d'information*. Autorité française de référence en matière de cybersécurité.

API : *Application Programming Interface*. Interface permettant à des applications ou composants logiciels de communiquer.

AppSec : *Application Security*. Sécurité applicative regroupant les pratiques destinées à sécuriser les logiciels tout au long de leur cycle de vie.

ASPM : *Application Security Posture Management*. Approche centralisant et contextualisant les données de sécurité pour dédupliquer les alertes et prioriser les risques.

ASVS : *Application Security Verification Standard*. Standard OWASP définissant des exigences de sécurité applicative précises et vérifiables selon plusieurs niveaux d'assurance.

CE : *Conformité Européenne*. Marquage dont le CRA adapte la logique aux produits intégrant des éléments numériques.

CERT-FR : *Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*. Entité citée pour la diffusion d'alertes et la réponse aux incidents.

CI/CD : *Continuous Integration / Continuous Delivery ou Deployment*. Chaîne automatisant notamment l'intégration, les tests et la livraison ou le déploiement du logiciel.

CICD-SEC : *CI/CD Security*. Préfixe employé pour identifier les catégories de risques du référentiel OWASP Top 10 CI/CD Security.

CLUSIF : *Club de la Sécurité de l'Information Français*. Réseau professionnel de cybersécurité cité comme relais d'influence et de partage d'expérience.

CoDir : *Comité de Direction*. Instance dirigeante auprès de laquelle l'AppSec Manager présente notamment la stratégie et les besoins du programme de sécurité.

COMEX : *Comité exécutif*. Instance de direction à laquelle peut être présentée une vision consolidée des risques applicatifs.

CRA : *Cyber Resilience Act*. Règlement européen imposant notamment des exigences de sécurité, de gestion des vulnérabilités et de transparence logicielle.

CSIRT : *Computer Security Incident Response Team*. Équipe chargée de piloter et coordonner la réponse opérationnelle aux incidents.

CTF : *Capture The Flag*. Exercice pratique permettant de développer les compétences en attaque et en défense.

CVE : *Common Vulnerabilities and Exposures*. Référence permettant d'identifier des vulnérabilités connues, notamment dans les dépendances logicielles.

CVSS : *Common Vulnerability Scoring System*. Système de notation de la sévérité des vulnérabilités.

DAST : *Dynamic Application Security Testing*. Analyse dynamique simulant des attaques sur une application en cours d'exécution.

DORA : *Digital Operational Resilience Act*. Règlement européen du secteur financier imposant notamment une gestion stricte des risques liés aux prestataires TIC.

ECSO : *European Cyber Security Organisation*. Réseau européen de cybersécurité cité parmi les relais permettant le partage de pratiques et la veille.

ENISA : *European Union Agency for Cybersecurity*. Agence européenne de cybersécurité intervenant dans l'écosystème réglementaire présenté dans le cours.

GDPR : *General Data Protection Regulation*. Réglementation citée parmi les contraintes pouvant être prises en compte pendant la définition des exigences du S-SDLC.

GRC : *Gouvernance, Risques, Conformité*. Fonction chargée de piloter les problématiques de gouvernance, de risques et de conformité.

IA : *Intelligence Artificielle*. Technologie pouvant générer du code, assister la qualification des alertes ou faciliter la remédiation, tout en conservant une supervision humaine.

IAST : *Interactive Application Security Testing*. Contrôle de sécurité cité comme une brique plus complexe à envisager après la maîtrise des contrôles fondamentaux.

IDE : *Integrated Development Environment*. Environnement de développement dans lequel des contrôles peuvent fournir un retour de sécurité précoce aux développeurs.

KPI : *Key Performance Indicator*. Indicateur permettant de mesurer la performance du programme AppSec, comme la couverture des contrôles ou le MTTR.

MFA : *Multi-Factor Authentication*. Authentification multifacteur recommandée pour sécuriser notamment les dépôts et les infrastructures CI/CD.

MLSecOps : *Machine Learning Security Operations*. Sécurisation des processus et pipelines liés au machine learning, citée parmi les évolutions technologiques à suivre.

MTTR : *Mean Time To Remediation*. Temps moyen écoulé entre l'identification confirmée d'une vulnérabilité et sa résolution effective.

NDA : *Non-Disclosure Agreement*. Engagement de confidentialité recommandé avant de partager une matrice ASVS détaillée avec des auditeurs ou clients qualifiés.

NIS 2 : *Network and Information Security 2*. Directive européenne imposant notamment aux entités concernées de maîtriser les risques liés à leur chaîne d'approvisionnement.

OIDC : *OpenID Connect*. Mécanisme cité pour permettre une authentification dynamique et l'utilisation d'identifiants temporaires dans les pipelines.

OIV : *Opérateur d'Importance Vitale*. Organisation dont les exigences de sécurité peuvent être répercutées contractuellement sur ses fournisseurs.

OpenSSF : *Open Source Security Foundation*. Organisation associée dans le cours au framework SLSA consacré à la sécurisation de la chaîne de fabrication logicielle.

OWASP : *Open Worldwide Application Security Project*. Écosystème open source fournissant des standards et méthodes de sécurité comme SAMM, ASVS et WSTG.

PPE : *Poisoned Pipeline Execution*. Attaque consistant à empoisonner ou détourner l'exécution d'un pipeline CI/CD.

QA : *Quality Assurance*. Fonction qualité citée parmi les équipes concernées par la montée en compétences liée au S-SDLC.

RACI : *Responsible, Accountable, Consulted, Informed*. Matrice permettant de répartir clairement les rôles et responsabilités.

RASP : *Runtime Application Self-Protection*. Technologie de protection active intégrée à l'application pendant son exécution.

RBAC : *Role-Based Access Control*. Contrôle d'accès fondé sur les rôles permettant d'attribuer des droits adaptés aux différents acteurs.

ReCyF : *Référentiel Cyber France*. Référentiel de l'ANSSI présenté comme traduisant NIS 2 en moyens acceptables de conformité.

RETEX : *Retour d'Expérience*. Analyse collective d'incidents ou de situations passées afin d'en tirer des enseignements.

RSSI : *Responsable de la Sécurité des Systèmes d'Information*. Responsable participant à la gouvernance globale de la sécurité et aux obligations réglementaires.

SaaS : *Software as a Service*. Modèle cité dans l'approche « SaaS-first », qui exploite notamment les fonctionnalités natives des forges logicielles.

SAMM : *Software Assurance Maturity Model*. Modèle OWASP permettant d'évaluer et de faire progresser la maturité d'un programme de sécurité logicielle.

SAST : *Static Application Security Testing*. Analyse du code source sans l'exécuter afin de détecter des vulnérabilités et des pratiques de programmation dangereuses.

SBOM : *Software Bill of Materials*. Nomenclature recensant les composants et dépendances intégrés dans un logiciel.

SCA : *Software Composition Analysis*. Analyse des composants et dépendances tierces visant notamment à identifier leurs vulnérabilités connues.

SCM : *Source Code Management*. Système de gestion du code source et des dépôts dont les accès, branches et configurations doivent être protégés.

SDLC : *Software Development Life Cycle*. Cycle regroupant les différentes étapes de fabrication d'un logiciel, de sa conception à son exploitation.

SLA : *Service Level Agreement*. Engagement définissant notamment les délais attendus pour corriger certaines catégories de vulnérabilités.

SLSA : *Supply-chain Levels for Software Artifacts*. Framework destiné à renforcer l'intégrité de la chaîne de fabrication logicielle et la provenance des artefacts.

SPDX : *Software Package Data Exchange*. Format standard cité pour produire et échanger des SBOM.

SSO : *Single Sign-On*. Authentification unique recommandée pour maîtriser les accès aux SCM et aux serveurs de build.

S-SDLC : *Secure Software Development Life Cycle*. Cycle de développement dans lequel la sécurité est intégrée de manière transversale et continue à toutes les phases.

STRIDE : *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*. Méthodologie citée pour réaliser la modélisation des menaces.

TIC : *Technologies de l'Information et de la Communication*. Catégorie de prestataires tiers dont DORA impose une gestion stricte des risques.

TMT : *Threat Modeling Tool*. Outil Microsoft cité comme support à la modélisation des menaces.

WSTG : *Web Security Testing Guide*. Guide OWASP fournissant une méthodologie opérationnelle pour tester la sécurité des applications web.

XSS : *Cross-Site Scripting*. Vulnérabilité d'injection de scripts que l'encodage contextuel des sorties vise notamment à prévenir.

L1 : *Level 1*. Niveau 1 de l'ASVS correspondant aux fondamentaux applicables à toutes les applications.

L2 : *Level 2*. Niveau 2 de l'ASVS destiné notamment aux applications traitant des données sensibles.

L3 : *Level 3*. Niveau 3 de l'ASVS réservé aux systèmes hautement critiques.

R : *Responsible*. Dans une matrice RACI, acteur chargé de réaliser l'activité.

A : *Accountable*. Dans une matrice RACI, acteur portant la responsabilité finale.

C : *Consulted*. Dans une matrice RACI, acteur consulté pour contribuer à une activité ou une décision.

I : *Informed*. Dans une matrice RACI, acteur devant être tenu informé.