LiveCampus

Apprentissage connecté

Sommaire (gouvernance & contexte organisationnel)

LiveCampus

Apprentissage connecté

Les outils

Le SWOT permet de déterminer les forces, les faiblesses, les opportunités et les menaces d'un produit, d'un système, d'un service

LiveCampus

Apprentissage connecté

Exemple d'un SWORT pour Security by design

Forces (Strengths)	Faiblesses (Weaknesses)
- Intégration précoce de la sécurité dans le cycle de vie.	- Coût initial plus élevé dû à la formation et aux outils spécialisés.
- Réduction du nombre de failles de sécurité dans le produit final.	- Nécessite un changement de culture d'entreprise (DevSecOps).
- Conformité aux normes (ISO 27001, RGPD).	- Complexité des outils et méthodologies à maîtriser (ASVS, STRIDE).
- Meilleure image de marque auprès des clients.	- Temps de développement potentiellement rallongé.

LiveCampus

Apprentissage connecté

Opportunités (Opportunities)	Menaces (Threats)
- Demande croissante de solutions sécurisées.	- Évolution rapide des cybermenaces.
- Aides publiques pour la cybersécurité (France Relance, Europe).	- Risque de non-conformité si mauvaise mise en œuvre.
- Intégration dans les marchés publics exigeant une sécurité intégrée.	- Attaques ciblées malgré les protections (APT).

LiveCampus

Apprentissage connecté

Exemple de Pestel

Il s'agit là de déterminer par facteurs, les impacts.

LiveCampus

Apprentissage connecté

Facteurs	Impacts pour Security by Design
Politique	- Renforcement des législations (NIS2, RGPD).- Normes obligatoires pour certains secteurs (santé, finance).
Économique	- Investissements en cybersécurité encouragés.- Risques financiers liés aux fuites de données.
Socioculturel	- Sensibilisation croissante du public à la protection des données.- Attentes élevées des utilisateurs en matière de sécurité.
Technologique	- Apparition de nouvelles techniques de protection (Zero Trust, IA).- Automatisation des tests de sécurité.
Environnemental	- Consommation énergétique des outils de sécurité à considérer (cloud, cryptographie).
Légal	- Contraintes réglementaires strictes (CNIL, eIDAS, ISO).- Obligation de notification d'incident sous 72h (RGPD).

LiveCampus

Apprentissage connecté

La politique de sécurité de l'information formalise les engagements de l'organisation en matière de protection des actifs numériques et physiques. Elle constitue le socle de la gouvernance sécurité et s'applique à l'ensemble des collaborateurs, sous-traitants et partenaires, dans le respect des exigences réglementaires et contractuelles.

Objectifs
Assurer la confidentialité, l'intégrité et la disponibilité des informations.
Réduire les risques de sécurité, notamment les fuites de données et les interruptions de service.
Garantir la conformité aux réglementations (RGPD, NIS2, ISO 27001).
Promouvoir une culture de la sécurité au sein de l'organisation.
Soutenir les objectifs métiers par une sécurité intégrée.

LiveCampus

Apprentissage connecté

Portée

- S'applique à **toutes les informations traitées**, stockées ou transmises.
- Couvre **l'ensemble des ressources informatiques** (systèmes, réseaux, applications, équipements mobiles, cloud, etc.).
- Concerne **tous les collaborateurs** internes et externes.

LiveCampus

Apprentissage connecté

Responsabilités	Commentaires
Direction	approuve la politique, soutient les ressources nécessaires.
RSSI	définit, met à jour et pilote la mise en œuvre de la politique.
DPO	veille à la conformité RGPD en matière de données personnelles.
Managers	s'assurent que leurs équipes appliquent les directives.
Collaborateurs	responsables du respect des règles de sécurité dans leurs activités quotidiennes.

LiveCampus

Apprentissage connecté

Les directives

- Gestion des accès : utilisation de l'authentification forte (MFA), politique de mots de passe, gestion des droits par rôle (RBAC).
- **Protection des données** : chiffrement, classification, sauvegardes, règles de conservation.
- **Sécurité des postes de travail**

LiveCampus

Apprentissage connecté

- **Protection des données** : chiffrement, classification, sauvegardes, règles de conservation.
- **Sécurité du développement : intégration des contrôles dans le SDLC (DevSecOps).**
- Formation continue : campagnes de sensibilisation régulières.

LiveCampus

Apprentissage connecté

Révision et diffusion

Révision annuelle par le RSSI ou en cas de changement majeur (nouvelle menace, évolution légale, audit, inciden

- Validation obligatoire par la direction générale.
- Communication à tous les collaborateurs, via :L'intranet ou le LMS sécurité.

- des sessions de présentation pour les nouveaux arrivants.
- des rappels lors de campagnes de sensibilisation.

LiveCampus

Apprentissage connecté

Documents associés

- **Charte informatique** : décrit les droits et devoirs de chaque utilisateur.
- **Plan de continuité d'activité (PCA)** et **plan de reprise d'activité (PRA)**.
- **Registre des traitements de données (RGPD)**.
- **Politique de classification de l'information**.
- **Procédures de gestion des incidents de sécurité**.
- **Politique de contrôle d'accès et gestion des identités (IAM)**.

LiveCampus

Apprentissage connecté

Exemple de charte informatique

1. Accès aux ressources
- Chaque utilisateur dispose d'un identifiant personnel et d'un mot de passe confidentiel.
- Les sessions doivent être verrouillées en cas d'absence temporaire.

2. Utilisation acceptable
- L'usage du SI est strictement réservé aux activités professionnelles.
- L'utilisation de logiciels ou matériels non validés est interdite.

LiveCampus

Apprentissage connecté

3. Messagerie
- L'utilisation de la messagerie professionnelle doit rester conforme à l'éthique.
- Aucun fichier suspect ne doit être ouvert sans vérification.

4. Internet
- L'accès aux réseaux sociaux ou plateformes de streaming est interdit sauf autorisation expresse.

5. Sécurité
- Toute suspicion d'incident (phishing, virus…) doit être immédiatement signalée au RSSI.
- L'installation d'antivirus et de correctifs de sécurité est obligatoire.

LiveCampus

Apprentissage connecté

6. Confidentialité

- Les données sensibles ne doivent pas être partagées en dehors des circuits autorisés.
- L'usage de supports amovibles est restreint et doit être chiffré.

7. Sanctions

- Tout manquement à la charte pourra entraîner des sanctions disciplinaires, voire des poursuites.

8. Signature

Nom : _____ Date : __/__/____ Signature : _____

LiveCampus

Apprentissage connecté

Exemple de PCA

1. Analyse d'impact (BIA)
- Activité critique : Facturation
- Délai de reprise maximal (RTO) : 24h
- Perte de données tolérable (RPO) : 1h

2. Scénarios de crise couverts
- Cyberattaque (ransomware)
- Panne majeure des serveurs
- Catastrophe naturelle ou incendie

LiveCampus

Apprentissage connecté

3. Plans de secours
- Basculer sur un site de repli (hébergement cloud AWS à Paris).
- Réplication automatique des bases de données toutes les heures.
- Kit de continuité papier pour gestion manuelle des commandes.

4. Organisation
- Responsable PCA : Marc Dupuis (DSI)
- Equipe de crise : Direction, RSSI, Communication, RH
- Liste des contacts d'urgence : prestataires IT, services publics

LiveCampus

Apprentissage connecté

5. Tests et exercices
- Simulation ransomware : tous les 6 mois
- Revue annuelle du PCA avec mise à jour

6. Communication
- Message-type à envoyer en cas d'interruption
- Plateforme de communication alternative : WhatsApp Pro / SMS / Teams

7. Archivage
- Document stocké sur SharePoint sécurisé, sauvegardé quotidiennement.

LiveCampus

Apprentissage connecté

Exemple du registre des traitements de données

Traitement	Finalité	Catégorie des données	Durée de conservation	Responsable	Sous-traitant	Sécurité de mise en oeuvre
Gestion RH	Contrats, paie, congés	Noms, coordonnées, RIB	5 ans	Responsable RH	Paie	Accès restreint, chiffrement
Vidéosurveillance	Protection des locaux	Visages, horaires	30 jours	Responsable sécurité	Aucun	Enregistrement chiffré localement

LiveCampus

Apprentissage connecté

Exemple de gestion des procédures des incidents de sécurité

1. Détection
- Déclencheur : SIEM (ELK), alerte antivirus, utilisateur.
- Niveau de gravité : Faible / Moyen / Critique.

2. Contention
- Isolement du poste ou serveur concerné.
- Arrêt des flux réseau suspects.

3. Notification
- Informer le RSSI, la DSI, et le DPO si données personnelles.
- Notification à la CNIL si applicable (72h).

LiveCampus

Apprentissage connecté

4. Analyse
- Outils : Wireshark, Suricata, journaux systèmes.
- Évaluation de l'origine : phishing, malware, exploit vulnérabilité.

5. Remédiation
- Suppression de la menace.
- Réinitialisation des mots de passe.
- Patch des failles exploitées.

LiveCampus

Apprentissage connecté

6. Rétablissement
- Restauration à partir de la dernière sauvegarde saine.
- Vérification de l’intégrité des systèmes.

7. REX (Retour d'expérience)
- Rédaction d’un rapport d'incident (type PDF).
- Amélioration des procédures / formation du personnel.

8. Historisation
- Journal des incidents : date, nature, impact, réponse apportée.

LiveCampus

Apprentissage connecté

Rôles et responsabilités

Responsable de la Sécurité des Systèmes d'Information (RSSI)

- Définit la stratégie de sécurité.
- Pilote les audits, les plans de remédiation et les exercices de gestion de crise.
- Interagit avec la direction générale pour aligner sécurité et stratégie métier.
- Met en place un **SMSI** selon ISO 27001

LiveCampus

Apprentissage connecté

Délégué à la Protection des Données (DPO)

- Garant de la conformité au RGPD.
- Encadre les traitements de données personnelles.
- Fait le lien entre l'entreprise, la CNIL et les personnes concernées.
- Accompagne l'implémentation du principe de **Privacy by Design**.

LiveCampus

Apprentissage connecté

Développeurs et DevSecOps

- Appliquent les règles de codage sécurisé (ex : OWASP Top 10).
- Automatisent les contrôles de sécurité dans la CI/CD.
- Intègrent des outils comme SonarQube, Trivy, ou Snyk.

LiveCampus

Apprentissage connecté

Architectes

•Conçoivent des architectures segmentées, résilientes, et compatibles avec le modèle Zero Trust.
•Choisissent les solutions de chiffrement, de filtrage réseau, d'isolation.

LiveCampus

Apprentissage connecté

Utilisateurs finaux

•Appliquent les bonnes pratiques de sécurité (mots de passe robustes, MFA, vigilance face au phishing).
•Signalent les comportements suspects ou les incidents.
•Respectent la charte informatique.

LiveCampus

Apprentissage connecté

Direction Générale

- Valide les budgets cybersécurité.
- Intègre la sécurité dans la culture d'entreprise.
- Assume la responsabilité juridique en cas de non-conformité.

LiveCampus

Apprentissage connecté

Gestion des risques en cybersécurité

- Identification des actifs
- Identification des menaces
- Évaluation des impacts

LiveCampus

Apprentissage connecté

- Évaluation de la vraisemblance
- Calcul du risque brut
- Définition des mesures de sécurité
- Acceptation, traitement ou transfert du risque.

LiveCampus

Apprentissage connecté

Méthodes courantes

EBIOS Risk Manager (ANSSI) : *Scénarios redoutés & cartographie des événements*

Objectif : Identifier et analyser les "scénarios redoutés", c'est-à-dire les combinaisons d'événements qui pourraient gravement compromettre les missions de l'organisation.

LiveCampus

Apprentissage connecté

Caractéristiques :

•Approche orientée menaces et impacts métier.
•Forte implication des métiers pour définir ce qu'on redoute vraiment.
•Étapes : contexte ⟶ événements redoutés ⟶ sources de menace ⟶ scénarios ⟶ mesures de sécurité.

LiveCampus

Apprentissage connecté

Exemple :

Dans un hôpital :

- **Événement redouté** : indisponibilité du système de gestion des urgences.
- **Source de menace** : ransomware ciblé.
- **Scénario** : phishing ciblé → exécution de malware → chiffrement des systèmes critiques.
- **Mesures** : durcissement des postes, EDR, PRA (Plan de reprise d'activité).

LiveCampus

Apprentissage connecté

MEHARI : ***Pondération et cotation rigoureuse des risques***

Objectif : Fournir une analyse quantitative ou semi-quantitative avec des grilles de cotation précises.

LiveCampus

Apprentissage connecté

Caractéristiques :

- Basée sur des référentiels de vulnérabilités, de menaces, et d'impacts.
- Distingue clairement les **actifs**, **vulnérabilités**, **mesures existantes**, **menaces**, **impacts**.
- Propose une **grille de cotation** (gravité, vraisemblance, niveau de risque).

LiveCampus

Apprentissage connecté

Critère	Cotation	Exemple
Gravité impact	4 (fort)	Perte de 100 000€
Vraisemblance	3 (moy)	1 incident tous les 2 ans
Niveau de risque	Élevé	Risque à traiter prioritairement

LiveCampus

Apprentissage connecté

Exemple :
Pour une société de e-commerce :

- **Actif** : base clients.
- **Menace** : fuite de données via injection SQL.
- **Vulnérabilité** : absence de contrôle des entrées utilisateur.
- **Impact** : atteinte à la réputation + sanction RGPD.
- ⟶ Cotation : très élevée ⟶ priorisation immédiate de la remédiation.

LiveCampus

Apprentissage connecté

ISO/IEC 27005 : ***Gestion des risques alignée sur l'ISO 27001***

Objectif : Soutenir la mise en œuvre d'un SMSI (Système de Management de la Sécurité de l'Information) conforme à l'ISO 27001.

LiveCampus

Apprentissage connecté

Caractéristiques :

- Complément de l'ISO 27001 (quoi faire) en expliquant **comment** gérer les risques.
- Structure cyclique : identification des actifs → estimation → évaluation → traitement → surveillance.
- Forte documentation exigée (politiques, rapports, preuves).

LiveCampus

Apprentissage connecté

Exemple :

Dans une entreprise certifiée ISO 27001 :

•L'actif "serveur web de production" est critique.

•Les risques sont analysés en lien avec la clause A.18 (conformité) et A.12 (protection contre les logiciels malveillants).

•Les traitements incluent des actions documentées, testées et auditées.

LiveCampus

Apprentissage connecté

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) : *Actifs critiques métiers en priorité*

Objectif : Identifier les risques à partir de la **valeur métier des actifs** et des pratiques organisationnelles.

LiveCampus

Apprentissage connecté

Caractéristiques :

- Approche itérative et collaborative.
- Forte implication des équipes non techniques (RH, finances, production…).
- Se concentre d'abord sur les actifs métiers **critiques**, avant d'évaluer les menaces et vulnérabilités techniques.
- Privilégie l'organisation plutôt que l'outil.

LiveCampus

Apprentissage connecté

Exemple :

Dans une PME de logistique :

- **Actif critique** : système de gestion des livraisons en temps réel.
- **Impact métier** : perte de contrat si livraison en retard.
- **Scénario** : panne prolongée du système → interruption des opérations.
- Traitements : mise en place de redondance, test PRA, sensibilisation utilisateurs.

LiveCampus

Apprentissage connecté

Les outils

Tableaux de bord GRC (Governance Risk Compliance)
Exemple : Tableau de bord dans un outil comme RiskCloud ou ServiceNow GRC

LiveCampus

Apprentissage connecté

Affiche en temps réel :

•Le niveau de conformité par norme (ISO 27001, NIS2, RGPD).
•Les incidents de sécurité signalés et leur statut de traitement.
•Les risques critiques non traités ou dépassant les seuils de tolérance.
•Les actions de remédiation en cours, avec échéances.

LiveCampus

Apprentissage connecté

Cas d'usage : Une entreprise du secteur bancaire utilise un tableau GRC pour piloter la conformité PCI-DSS et identifier les points faibles sur les flux de paiement.

LiveCampus

Apprentissage connecté

Matrices de risque

Impact \ Probabilité	Très faible	Faible	Moyenne	Élevée	Très élevée
Très grave	Modéré	Élevé	Élevé	Critique	Critique
Grave	Faible	Modéré	Élevé	Critique	Critique
Modéré	Faible	Faible	Modéré	Élevé	Critique
Mineur	Négligeable	Faible	Faible	Modéré	Élevé

LiveCampus

Apprentissage connecté

Cas d'usage : Évaluation du risque d'exposition publique de données de santé :

•Impact = Très grave (vie privée, RGPD)
•Probabilité = Moyenne (vulnérabilité connue, non corrigée)
→ Niveau de risque = **Critique**, traitement prioritaire requis.

LiveCampus

Apprentissage connecté

Arbre de défaillance ou d'attaque

Exemple : Arbre d'attaque (Attack Tree)
But recherché : Vol d'identifiants d'un utilisateur administrateur

Niveau 0 : **Vol d'identifiants admin**

- Niveau 1 :
  - [A] Phishing ciblé (email frauduleux)
  - [B] Exploitation d'une faille XSS
  - [C] Interception réseau (man-in-the-middle)
- Niveau 2 :
  - [B.1] Injection de script malveillant dans un champ commentaire
  - [C.1] Accès au Wi-Fi non sécurisé

LiveCampus

Apprentissage connecté

Utilisation : En phase de conception, cet arbre permet d'identifier les vecteurs d'attaque à mitiger, comme l'obligation du HTTPS, ou la validation côté serveur des entrées utilisateur.

LiveCampus

Apprentissage connecté

Simulations Red Team / Blue Team

Exemple de simulation Red/Blue Team

- **Contexte** : Simulation d'une attaque sur un système de gestion RH.

LiveCampus

Apprentissage connecté

Simulations Red Team / Blue Team

Red Team (attaquants) :

- Réalise une reconnaissance (scan Nmap, OSINT sur les employés).
- Exploite une faille de configuration sur un serveur Jenkins exposé.
- Déploie une charge utile (reverse shell) pour exfiltrer des données.

LiveCampus

Apprentissage connecté

Simulations Red Team / Blue Team

Blue Team (défense) :

- Détecte une activité anormale grâce à un SIEM (ex : Wazuh).
- Isole le poste compromis via une politique de segmentation réseau.
- Analyse les logs et enclenche une réponse automatique via SOAR.

LiveCampus

Apprentissage connecté

Simulations Red Team / Blue Team

But pédagogique : Tester l'efficacité des mécanismes de détection, les procédures de réponse, et la résilience du système.

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

RGPD	Directive NIS 2 (UE)	LPM (France)	CNIL (France)	ISO 27001
Base légale pour les traitements de données personnelles.	Renforce la cybersécurité des secteurs critiques (énergie, santé, finances).	Loi de programmation militaire.	Autorité de contrôle des données personnelles.	Norme de certification des systèmes de gestion de la sécurité de l'information.
Droits des personnes (accès, rectification, effacement).	Implique des obligations de signalement, d'audits, et de mise en conformité.	Obligations renforcées pour les OIV et opérateurs essentiels (OE).	Pouvoir de sanction (jusqu'à 20M€ ou 4 % du CA mondial).	Couvre les aspects organisationnels, techniques et humains.
Obligations : registre de traitement, DPO, notification sous 72h.	Prévoit des amendes administratives significatives.			Auditable par des tiers accrédités.

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Cartographie des traitements et des flux de données

[Utilisateur] ---> (Application Web) ---> [Serveur Applicatif] ---> [Base de Données]

- Données collectées : nom, e-mail, paiement
- Transfert : HTTPS
- Stockage : chiffrement AES-256

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Cartographie des traitements et des flux de données

Exemple concret :
Pour un site e-commerce :
- Traitement : commande en ligne.
- Données : identité, adresse, CB.
- Responsable : DSI.
- Transferts : de l'interface utilisateur vers Stripe via API.
- Stockage : dans un SGBD MySQL sur serveur dédié sécurisé.

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Procédures de gestion des violations de données
Exemple visuel :
Une **checklist** ou **workflow** simplifié :

- Détection (SIEM, alertes de logs)
- Qualification (mineur/majeur)
- Confinement (isolation des systèmes)
- Notification (CNIL sous 72h, clients si nécessaire)
- Rapport post-incident (analyse des causes, mesures correctives)

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Exemple concret :

- Une base client est exfiltrée → Détection via une alerte sur requêtes SQL anormales.
- Le RSSI est notifié → Active les procédures de confinement.
- La CNIL est informée via le portail officiel.

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Journalisation et traçabilité des accès sensibles
Exemple visuel :
Extrait de journal (log) horodaté, filtré par activité critique :

2025-05-06 10:34:21 | admin@crm-app | LOGIN_SUCCESS | IP:192.168.1.20
2025-05-06 10:34:30 | admin@crm-app | EXPORT_CLIENTS | 5.300 records

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Exemple concret :

- Tous les accès à la base RH sont tracés.
- Les logs sont centralisés dans un **SIEM** comme **Graylog** ou **Splunk**.
- Seuls les administrateurs habilités ont accès aux journaux, conservés 1 an.

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Gestion des droits et principe du moindre privilège

Rôle	Accès Lecture	Écriture	Suppression	Accès admin
Visiteur	✅	❌	❌	❌
RH	✅	✅	❌	❌
Admin Système	✅	✅	✅	✅

LiveCampus

Apprentissage connecté

Conformité légale et règlementaire

Exemple concret :

- Un développeur a uniquement accès à la base de test (lecture/écriture).
- Aucun accès en production sans justification validée par le RSSI.
- Utilisation d'un **gestionnaire d'identités (IAM)** avec audits réguliers des permissions.

LiveCampus

Apprentissage connecté

Glossaire

A

•**ASVS** (Application Security Verification Standard) : Standard de vérification de la sécurité des applications édité par l'OWASP.

•**Authentification forte** : Méthode d'authentification combinant au moins deux facteurs (mot de passe, biométrie, appareil).

LiveCampus

Apprentissage connecté

Glossaire

B

- **Bell-LaPadula** : Modèle de sécurité centré sur la confidentialité.

- **Biba** : Modèle de sécurité centré sur l'intégrité des données.

LiveCampus

Apprentissage connecté

Glossaire

C

- **CI/CD** (Continuous Integration / Continuous Deployment) : Intégration et déploiement continus dans le développement logiciel.
- **Clark-Wilson** : Modèle de sécurité axé sur l'intégrité des processus métier.
- **CNIL** (Commission Nationale de l'Informatique et des Libertés) : Autorité française de protection des données.
- **Conformité** : Respect des exigences réglementaires, normatives ou contractuelles.
- **CRAMM** (CCTA Risk Analysis and Management Method) : Méthode d'analyse des risques développée par le Royaume-Uni.

LiveCampus

Apprentissage connecté

Glossaire

D

- **DFD** (Data Flow Diagram) : Diagramme des flux de données.
- **DPO** (Data Protection Officer) : Délégué à la protection des données.
- **DevSecOps** : Intégration de la sécurité dans la démarche DevOps.

LiveCampus

Apprentissage connecté

Glossaire

E

•**EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) : Méthode française d'analyse de risques.

F

•**Failover** : Basculement automatique vers un système de secours en cas de défaillance.

•**Firewall** : Pare-feu, dispositif de filtrage du trafic réseau.

LiveCampus

Apprentissage connecté

Glossaire

G

- **GRC** (Governance, Risk & Compliance) : Ensemble des outils et méthodes de gouvernance des risques et conformité.
- **Git** : Système de gestion de versions distribué.
- **GitLab** : Plateforme DevOps basée sur Git.

LiveCampus

Apprentissage connecté

Glossaire

I

- **IA** (Intelligence Artificielle)
- **ISO 27001/27002** : Normes de sécurité de l'information.

J

- **Journalisation** : Enregistrement structuré des événements (logs).

LiveCampus

Apprentissage connecté

Glossaire

M

- **MEHARI** : Méthode d'analyse de risques française.

- **MFA** (Multi-Factor Authentication) : Authentification multi-facteurs.

- **Modèle STRIDE** : Modèle de catégorisation des menaces : Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.

LiveCampus

Apprentissage connecté

Glossaire

N

- **NIS2** : Directive européenne sur la sécurité des réseaux et systèmes d'information.

- **NIST** (National Institute of Standards and Technology) : Organisme américain proposant des cadres en cybersécurité.

LiveCampus

Apprentissage connecté

Glossaire

O

•**OWASP** (Open Worldwide Application Security Project) : Projet communautaire dédié à la sécurité des applications.

•**OTP** (One-Time Password) : Mot de passe à usage unique.

P

•**PESTEL** : Analyse des facteurs Politique, Économique, Socioculturel, Technologique, Environnemental et Légal.

LiveCampus

Apprentissage connecté

Glossaire

R

•**RGPD** (Règlement Général sur la Protection des Données) : Règlement européen sur la protection des données personnelles.

•**ROI** (Return on Investment) : Retour sur investissement.

•**RSSI** (Responsable de la Sécurité des Systèmes d'Information)

LiveCampus

Apprentissage connecté

Glossaire

S

- **SAMM** (Software Assurance Maturity Model) : Cadre d'évaluation de la maturité en sécurité logicielle.
- **SDLC** (Software Development Life Cycle) : Cycle de vie du développement logiciel.
- **Security by Design** : Approche qui intègre la sécurité dès la conception.
- **STRIDE** : Voir Modèle STRIDE ci-dessous.
- **SWOT** : Analyse des Forces, Faiblesses, Opportunités et Menaces.

LiveCampus

Apprentissage connecté

Glossaire

T

- **Threat Modeling** : Modélisation des menaces.

Z

- **Zero Trust** : Approche de sécurité où aucun utilisateur ou système n'est implicitement digne de confiance.

LiveCampus

Apprentissage connecté

Modèle STRIDE

Modèle STRIDE	**Description**	**Exemple concret**	**Contremesures recommandées**
Spoofing (Usurpation d'identité)	Un attaquant se fait passer pour un autre utilisateur.	Connexion avec un mot de passe faible ou volé.	- Authentification forte (MFA)- Politique de mots de passe strictes- Captchas
Tampering (Altération)	Modification non autorisée de données.	Modification d'un montant de virement via un proxy (ex : Burp Suite).	- Signature des requêtes (HMAC)- Chiffrement côté transport (TLS)- Intégrité des journaux
Repudiation (Répudiation)	L'utilisateur nie avoir effectué une action.	Un utilisateur affirme ne jamais avoir effectué un virement frauduleux.	- Journalisation horodatée et signée- Horodatage sécurisé des événements- Preuves numériques non falsifiables
Information Disclosure (Divulgation)	Fuite d'informations sensibles.	Fuite des soldes ou des données personnelles via une API mal protégée.	- Chiffrement des données au repos et en transit- Contrôle d'accès aux ressources- Masquage des erreurs
Denial of Service (Déni de service)	Rendre l'application indisponible.	Envoi massif de requêtes qui bloque le serveur (attaque DDoS).	- WAF, CDN, et anti-DDoS- Limitation de taux (rate limiting)- Surveillance active
Elevation of Privilege	Obtenir des droits d'accès plus élevés que ceux prévus	L'application ne vérifie pas le rôle de l'utilisateur côté serveur. Résultat : l'utilisateur "user" peut accéder à la page d'administration et potentiellement modifier des données sensibles (produits, comptes utilisateurs, etc.).	Implémenter une vérification stricte des autorisations sur chaque point d'entrée (routes API, pages sensibles). Principe du moindre privilège Séparation des rôles. Journalisation et surveillance Tests de sécurité automatisés Revue du code Formation des développeurs

Exemples de tableaux pour EBIOS Risk Manager

Cas pratique

Bénéfices métiers	Conséquences en cas de compromission	Criticité	Événement redouté	Sources de menace
Augmentation des ventes en ligne	Perte de données client, réputation ternie	Très élevé	Compromission de la base de données client	Cyberattaque (phishing)
Amélioration du service client	Réduction de la qualité de service, plainte des clients	Moyen	Défaillance du serveur de support	Panne matérielle

Exemples de tableaux pour EBIOS Risk Manager

Cas pratique

Événement redouté	Source de menace	Mode opératoire	Vulnérabilité	Gravité	Vraisemblance	Niveau de risque
Compromission de la base de données	Attaque par injection SQL	Exploitation d'une faille SQL	Paramètres non filtrés	Très élevé	Élevée	Très élevé
Perte de données client	Panne serveur	Défaillance du stockage	Sauvegarde non redondée	Élevée	Moyenne	Élevé

LiveCampus

Apprentissage connecté

Exemples de tableaux pour MEHARI

Cas pratique

Actif	Valeur de l'actif	Vulnérabilité	Menace	Impact	Probabilité	Risque brut
Serveur de base de données	Élevée	Failles logicielles	Attaque par malware	Perte de données	Élevée	Très élevé
PC du collaborateur	Moyenne	Mots de passe faibles	Phishing	Vol de données perso	Moyenne	Moyen

LiveCampus

Apprentissage connecté

Exemples de tableaux pour MEHARI

Cas pratique

Risque	Mesures existantes	Mesures proposées	Risque résiduel	Responsable	Échéance
Perte de données client	Sauvegardes hebdomadaires	Mettre en place des sauvegardes quotidiennes et redondées	Faible	Responsable IT	1 mois
Attaque par phishing	Formation de sensibilisation au phishing	Installer une solution anti-phishing	Très faible	Responsable Sécurité	2 semaines

Exemples de tableaux pour OCTAVE

Cas pratique

Actif critique	Propriétaire	Menace	Vulnérabilité	Impact	Gravité estimée	Recommandation
Base de données clients	Responsable des données	Piratage	Sécurisation insuffisante	Vol d'identité	Très élevé	Renforcer la sécurité de la base de données
Application web	Responsable développement	Attaque DDoS	Détection tardive	Panne de service	Élevée	Mettre en place une solution de protection DDoS

Exemples de tableaux pour OCTAVE

Cas pratique

Processus métier	Exigence de sécurité	Menace organisationnelle	Failles humaines/processus	Recommandation
Gestion des données clients	Confidentialité des informations	Mauvaise gestion des droits d'accès	Accès non autorisés par des utilisateurs internes	Réviser les droits d'accès aux données sensibles
Support client	Disponibilité des services	Perte de données des clients	Mauvaise gestion des backups	Automatiser les sauvegardes et les tester régulièrement

LiveCampus

Apprentissage connecté

Cas pratique