Module 1 – Fondamentaux techniques et règlementaires

Fondamentaux de la sécurité des SI et réseaux

Séquence 1 : Introduction à la SSI

OIDANEOS

Présentation de la séquence
Objectifs et notions abordées

Identifier les grandes familles de SI et leurs vulnérabilités

- La définition de la sécurité des systèmes d'information
- Les principes et concepts en SSI
- L'écosystème des cyberattaques
- Les acteurs de la SSI
- La gestion des risques SSI

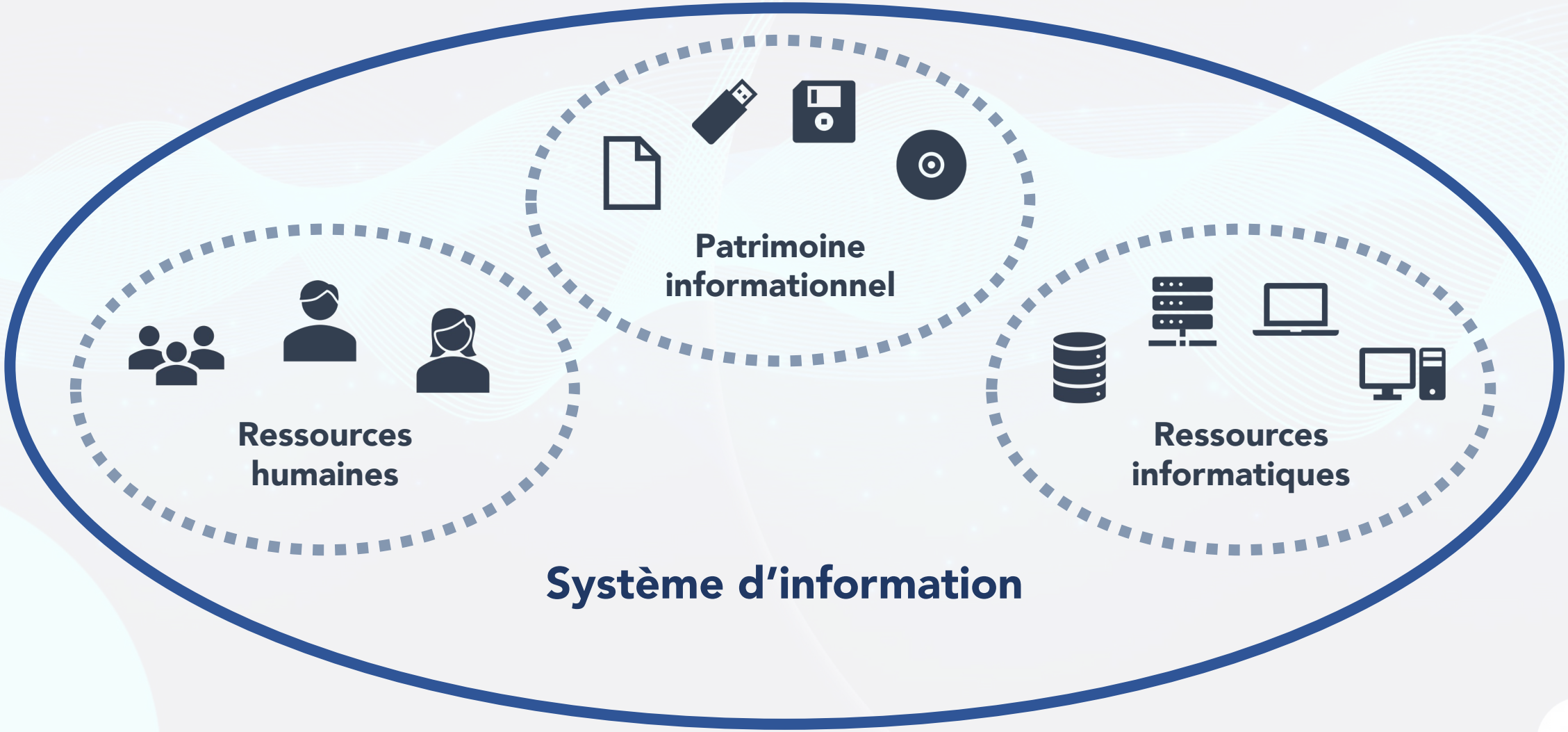
La définition de la sécurité des systèmes d'information

?

Qu'est-ce qu'un système d'information ?

La définition de la sécurité des systèmes d'information

Les enjeux d'un SI et de sa sécurité pour les organisations



La définition de la sécurité des systèmes d'information

La notion de système d'information

Système d'information

Ensemble organisé de ressources permettant de traiter et diffuser de l'information en fonction des objectifs d'une organisation

Système informatique

Réseaux, serveurs, postes de travails, logiciels, applications, BDD… faisant partie du système d'information. L'informatique nomade en fait partie

La définition de la sécurité des systèmes d'information

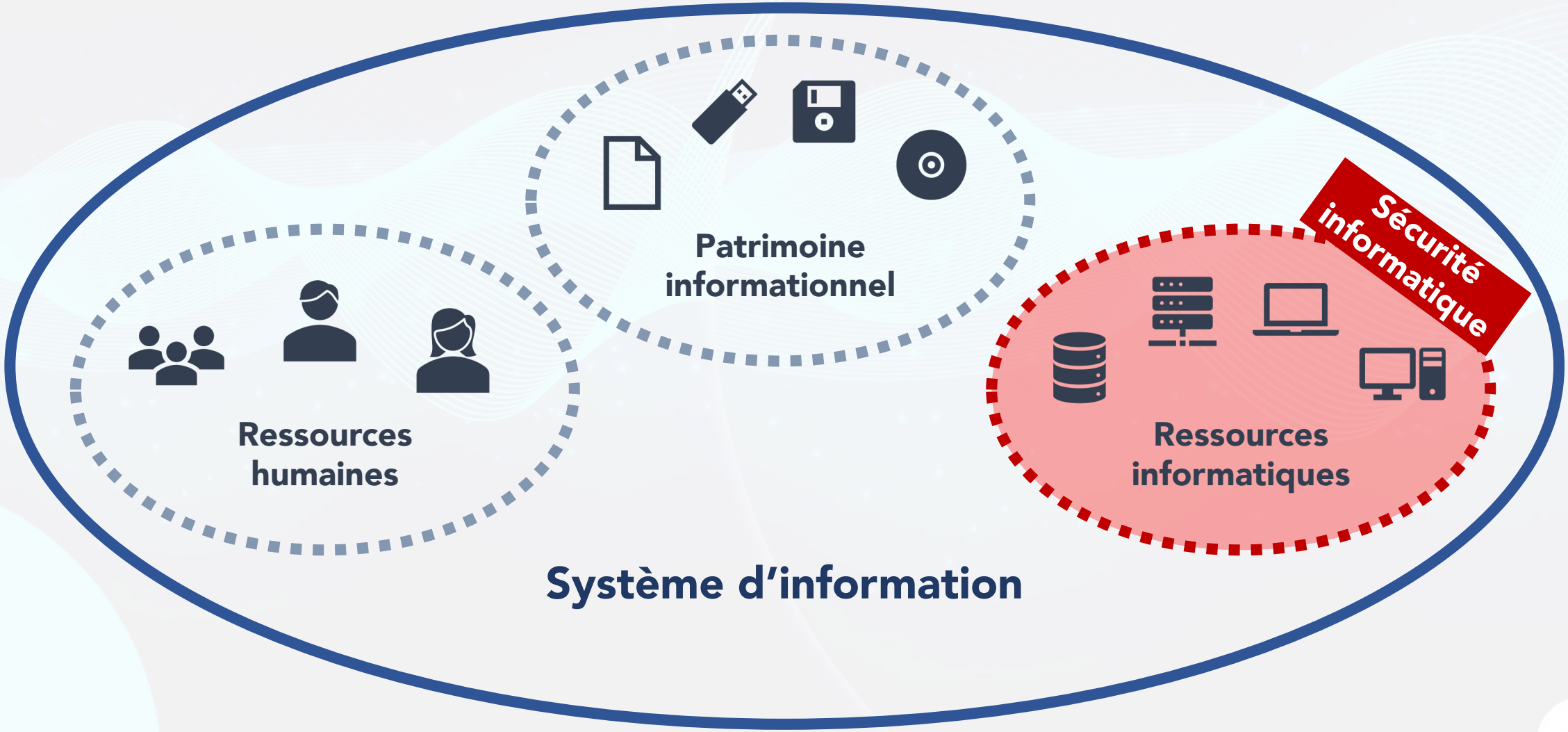
La notion de système d'information

?

Quelle différence entre **sécurité informatique**, **sécurité de l'information** (ou sécurité du système d'information) et **cybersécurité** ?

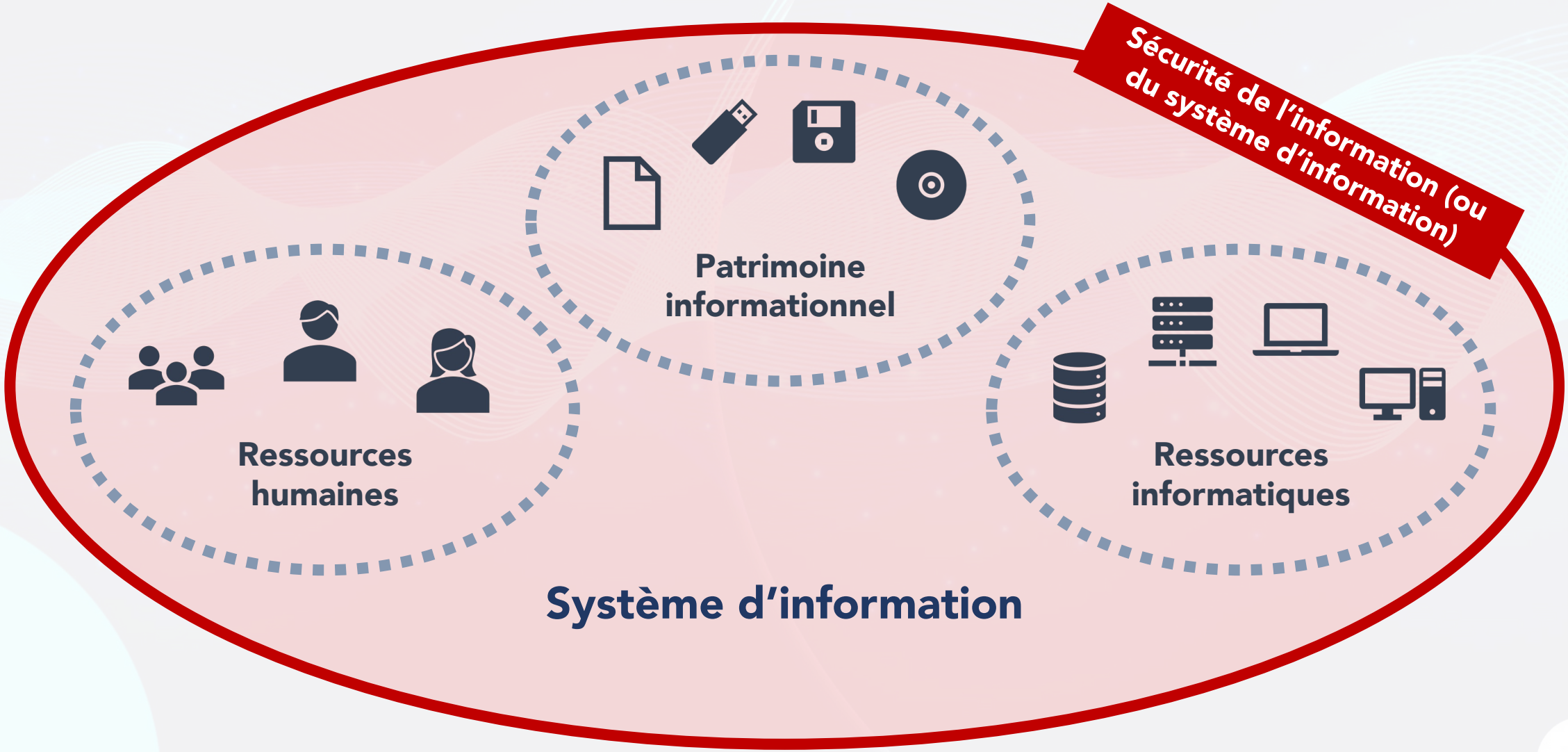
La définition de la sécurité des systèmes d'information

La notion de système d'information



La définition de la sécurité des systèmes d'information

La notion de système d'information



La définition de la sécurité des systèmes d'information

La notion de système d'information

Sécurité informatique

Ensemble des règles, procédures techniques et outils utilisés pour préserver la confidentialité, l'intégrité et la disponibilité des données traitées par les systèmes informatiques.

Sécurité de l'information *(sécurité du système d'information)*

La sécurité de l'information a pour objectif de protéger la confidentialité, l'intégrité et la disponibilité des informations de n'importe quel type et de n'importe quelle origine. La sécurité de l'information est menacée par des actes volontaires mais aussi des actes involontaires, des dysfonctionnements techniques ou encore des menaces environnementales…

La définition de la sécurité des systèmes d'information

Quelques exemples de SI et des risques associés

Les SI bureautiques et collaboratifs

Menaces	Vulnérabilités	Impacts
• Phishing, spear-phishing, fraude au président • Compromission de comptes (credential stuffing) • Exfiltration de données via des partages cloud ou des liens publics • Malware via des pièces-jointes ou macro	• Absence d'authentification multi facteur (ou mauvais déploiement) • Réutilisation de mots de passe • Droits de partage trop permissifs • Postes non durcis • Sensibilisation insuffisante et processus de validation faible	• Fuite de données (RH, clients) • Usurpation d'identité • Blocage (ransomware) • Pertes financières • Atteintes à la réputation

La définition de la sécurité des systèmes d'information

Quelques exemples de SI et des risques associés

Les SI de gestion (ERP / CRM / SIRH)

Menaces	Vulnérabilités	Impacts
• Fraude interne ou externe (modifications de RIB fournisseurs, commandes fictives) • Exploitation de vulnérabilités applicatives (injections, RCE) • Ransomware visant les serveurs applicatifs • Vol de données massives (clients, salaires)	• Comptes à privilèges excessifs • Interfaces d'intégration • Patch management lent • Absence de séparation des environnements • Insuffisance de journalisation	• Altération de la comptabilité • Arrêt de la facturation • Non-conformité (RGPD) : risques de pertes financières, litiges…

La définition de la sécurité des systèmes d'information

Quelques exemples de SI et des risques associés

Les SI web / e-commerce

Menaces	Vulnérabilités	Impacts
• Attaques applicatives : SQLi, XSS, CSRF, SSRF • Déni de service distribué • Défacement • Fraude de paiement • Bots et scraping • Supply chain (plugins, dépendances)	• Mauvaise gestion des sessions • Authentification faible • Dépendances non maîtrisées • Exposition des secrets • Pare-feu applicatif absent ou mal réglé • Durcissement serveur insuffisant • Mauvaise séparation des rôles	• Vol de données bancaires • Fuite de données de comptes clients • Indisponibilité du site Internet

La définition de la sécurité des systèmes d'information

Quelques exemples de SI et des risques associés

L'utilisation du cloud

Menaces	Vulnérabilités	Impacts
• Compromission d'identités cloud • Exposition de stockage ou fuite par mauvaise configuration • Ransomware par synchronisation / partages • Mouvement latéral par les interconnexions	• Mauvaises configurations IAM • Absence de segmentation réseau • Logs / audit non activés, alerting inexistants • Gestion des secrets faibles (variables, fichiers de conf)	• Exfiltration rapide à grande échelle • Surcoûts, perte de contrôle, interruption de services

La définition de la sécurité des systèmes d'information

Quelques exemples de SI et des risques associés

Les systèmes industriels (OT)

Menaces	Vulnérabilités	Impacts
• Ransomware qui se propage de l'IT vers l'OT • Accès distant compromis • Sabotage ou altération de paramètres • Matériel obsolète ciblé avec des attaques opportunistes	• Équipements anciens avec des protocoles non sécurisés • Segmentation IT/OT insuffisante • Supervision limitée, inventaire incomplet • Procédures de changement et sauvegardes OT insuffisantes	• Arrêt de production • Défaut de qualité • Risques pour la sécurité des personnes

La définition de la sécurité des systèmes d'information

Les sphères de la sécurité des systèmes d'information

La définition de la sécurité des systèmes d'information
Les sphères de la sécurité des systèmes d'information

- **Sécurité matérielle, physique et environnementale**
  - Fiabilité des matériaux et usage d'équipements qui possèdent un bon degré de sûreté de fonctionnement, de fiabilité et de robustesse
  - Protection des sources énergétiques et de la climatisation
  - Protection de l'environnement
  - Mesures de gestion et de contrôle des accès physiques aux locaux, équipements et infrastructures
  - Redondance physique
  - Marquage des matériels
  - Plan de maintenance préventive et corrective des équipements

La définition de la sécurité des systèmes d'information
Les sphères de la sécurité des systèmes d'information

- **Sécurité de l'exploitation**
  - Parc informatique
  - Configurations et mises à jour
  - Incidents et résolution
  - Performances
  - Sauvegardes, secours et continuité
  - Maintenance et contrats de maintenance
  - Logs et fichiers de journalisation

La définition de la sécurité des systèmes d'information

Les sphères de la sécurité des systèmes d'information

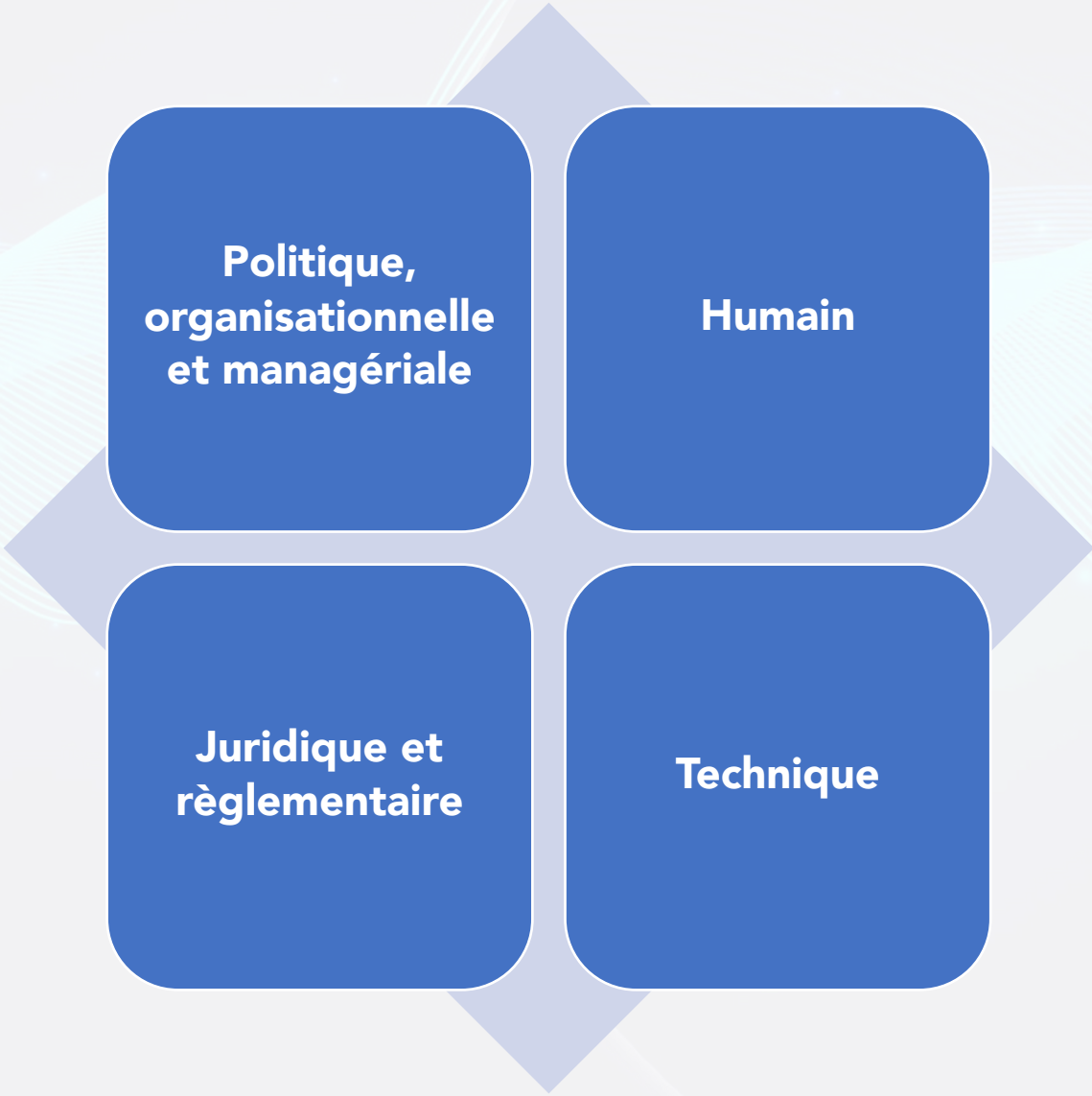
- **Sécurité des réseaux de télécommunication**
  - Infrastructure de transmission
  - Infrastructures de routage et de transport
  - Infrastructure applicative
  - Sphère informationnelle et de l'utilisateur

La définition de la sécurité des systèmes d'information
Les sphères de la sécurité des systèmes d'information

- **Sécurité logicielle, applicative et de l'information**
  - Sécurité logique : protection des services, des traitements informatiques et des données par des logiciels
    - Qualité du développement logiciels
    - Mise en œuvre adéquate de la cryptographie
    - Procédures de contrôle d'accès logique
    - Procédures de détection de logiciel malveillant, d'intrusion et d'incidents, réactions aux problèmes
    - Dimensionnement des ressources
  - Sécurité applicative : offrir aux programmes un niveau de sécurité suffisant pour garantir la confiance des utilisateurs
    - Méthodologie de développement
    - Robustesse des applications
    - Contrôles et jeux de tests
    - Intégration des mécanismes de sécurité
    - Choix des fournisseurs et sous-traitants
    - Élaboration et gestion des contrats
    - Plan de migration des applications
    - Évaluation, audit des programmes

La définition de la sécurité des systèmes d'information

Les dimensions de la sécurité des systèmes d'information

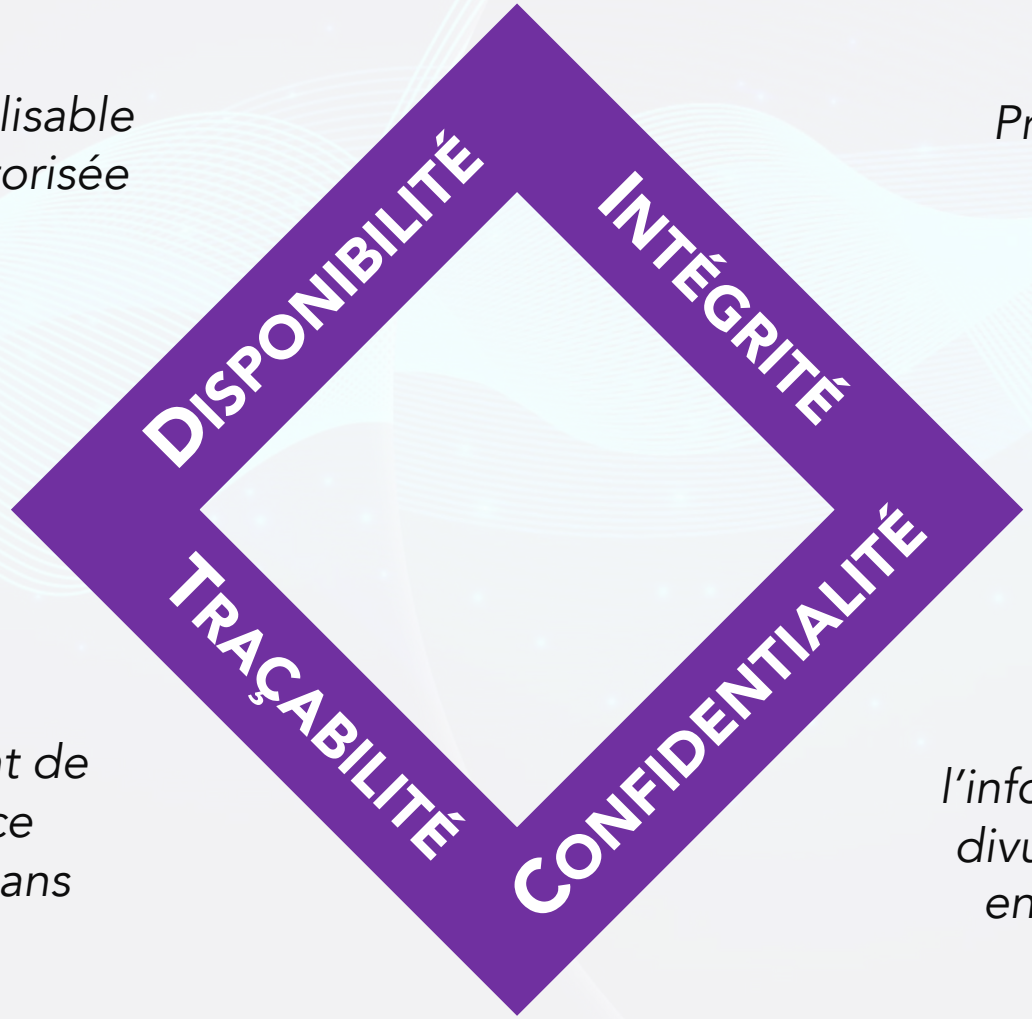


Les principes et concepts en SSI

Les principes et concepts en SSI

Les piliers de la SSI : les critères DICT

Propriété d'être accessible et utilisable à la demande par une entité autorisée (ISO 27000, 3.7)



Propriété d'exactitude et de complétude (ISO 27000, 3.6)

Authentification

Non-répudiation

Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue (ANSSI, CyberEdu)

Propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés (ISO 27000, 3.10)

Les principes et concepts en SSI
Le critère de disponibilité

Les informations sont accessibles comme requis, au moment requis, là où c'est requis et pour qui c'est requis

Exemple de données concernées

- L'indisponibilité de commandes passés par des clients sur un site Internet peut entraîner un retard dans les livraisons

Mesures SSI globales pour assurer la sécurité

- Mise en place d'un PCA/PRA et des plans de secours associés
- Répartition de charge (load-balancing)
- Sauvegarde

Les principes et concepts en SSI
Le critère d'intégrité

Les informations et les données sont exactes et authentiques

Exemple de données concernées

- Des données comptables qui peuvent impacter judiciairement et financièrement l'organisme si elles sont fausses
- Des données d'instruments de mesure pour le pilotage d'une drague

Mesures SSI globales pour assurer la sécurité

- Contrôle d'intégrité avec la somme de contrôle ou des outils spécifiques

Les principes et concepts en SSI
Le critère de confidentialité

Seuls les utilisateurs autorisés ont accès aux données sensibles et confidentielles

Exemple de données concernées

- Des documents stratégiques divulgués peuvent impacter la compétitivité d'une entreprise
- Les données clients ayant fuité peuvent créer des risques d'usurpation

Mesures SSI globales pour assurer la sécurité

- Authentification sur les systèmes
- Contrôle d'accès logique et physique
- Chiffrement des données

Les principes et concepts en SSI

Les critères DICT en matière de cybersécurité

Quels seraient les besoins en sécurité pour un site vitrine d'une entreprise lui permettant de faire la promotion de ses services ?

Critère	Niveau	Justification
Disponibilité		
Intégrité		
Confidentialité		
Traçabilité		

Echelle de niveau à utiliser

- Fort
- Moyen
- Faible

Les principes et concepts en SSI
Les critères DICT en matière de cybersécurité

Quels seraient les besoins en sécurité pour un site vitrine d'une entreprise lui permettant de faire la promotion de ses services ?

Critère	Niveau	Justification
Disponibilité	Fort	Un haut niveau de disponibilité du site Web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaître ses services au public.
Intégrité	Fort	L'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site Web pour y insérer des informations erronées (ce qui serait dommageable).
Confidentialité	Faible	Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature.
Traçabilité	Moyen	Ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

Les principes et concepts en SSI
Identity, Authentication, Authorization and Accounting

- **Identity**
  - Ce que l'on prétend être
  - Exemple : son adresse mail, son nom d'utilisateur

- **Authentication**
  - Mécanisme qui va prouver que la personne qui a clamé son identité est bien elle
  - Facteurs d'authentification :
    - *Facteurs de connaissance : mot de passe, code PIN*
    - *Facteurs de possession : smartphone, jeton d'authentification*
    - *Facteurs d'inhérence : empreintes digitales, reconnaissance faciale*
    - *Facteurs de localisation : géolocalisation, adresse IP*
    - *Facteurs de comportement*

- **Authorization**
  - L'utilisateur se voit accorder des privilèges et des droits pour accéder à certaines ressources

- **Accounting**
  - Traçabilité des activités des utilisateurs pour détecter et/ou investiguer

L'écosystème des cyberattaques

L'écosystème des cyberattaques

Les principaux vecteurs d'attaques utilisés par les cybercriminels

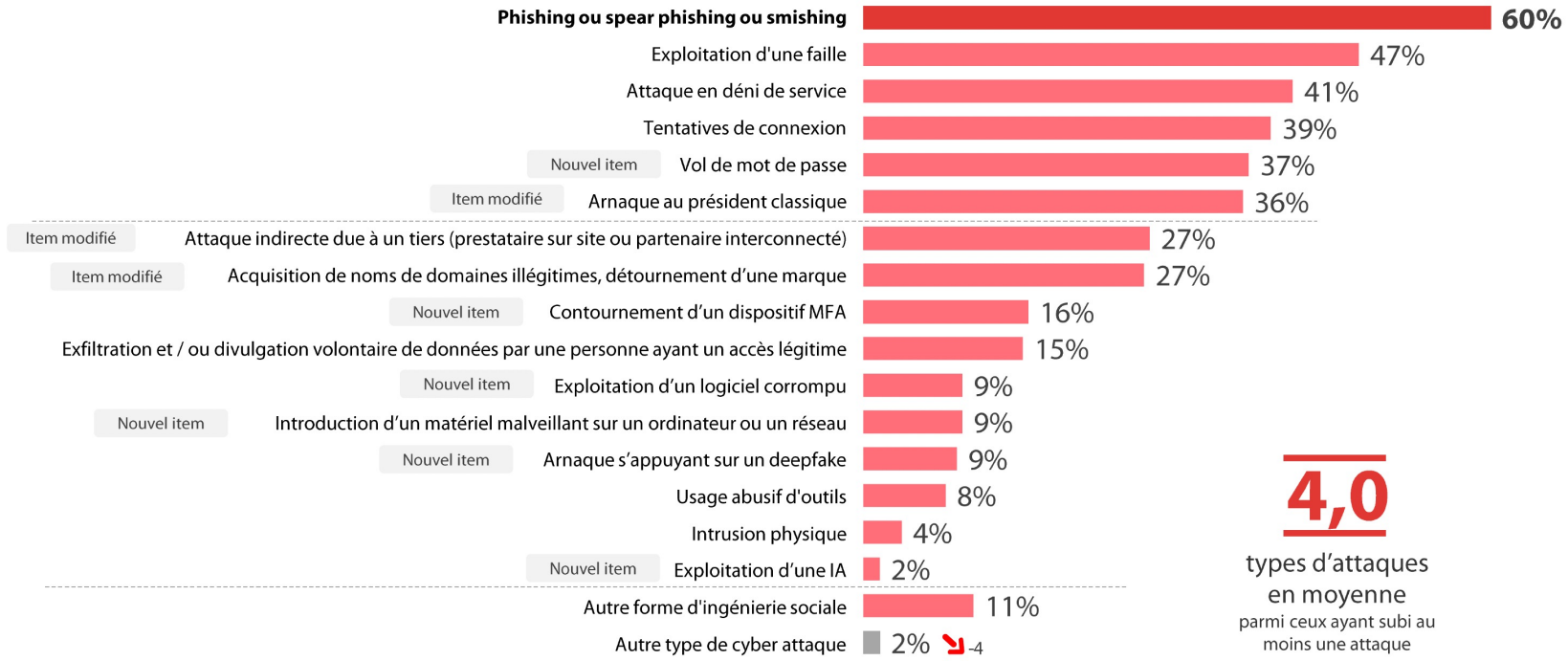
Avec en moyenne 4 vecteurs, le phishing reste en tête des attaques, suivi par l'exploitation d'une faille existante. Les stratégies d'attaque sont similaires à l'année précédente.

190 personnes

Q5A. Parmi les vecteurs d'attaques suivants, lesquels ont impacté votre entreprise au cours des 12 derniers mois ?

Base : ont constaté une attaque - plusieurs réponses possibles

47% des entreprises ont subi au moins une cyberattaque en 2023



4,0

types d'attaques en moyenne

parmi ceux ayant subi au moins une attaque

L'écosystème des cyberattaques

Les principaux impacts des cybercriminels

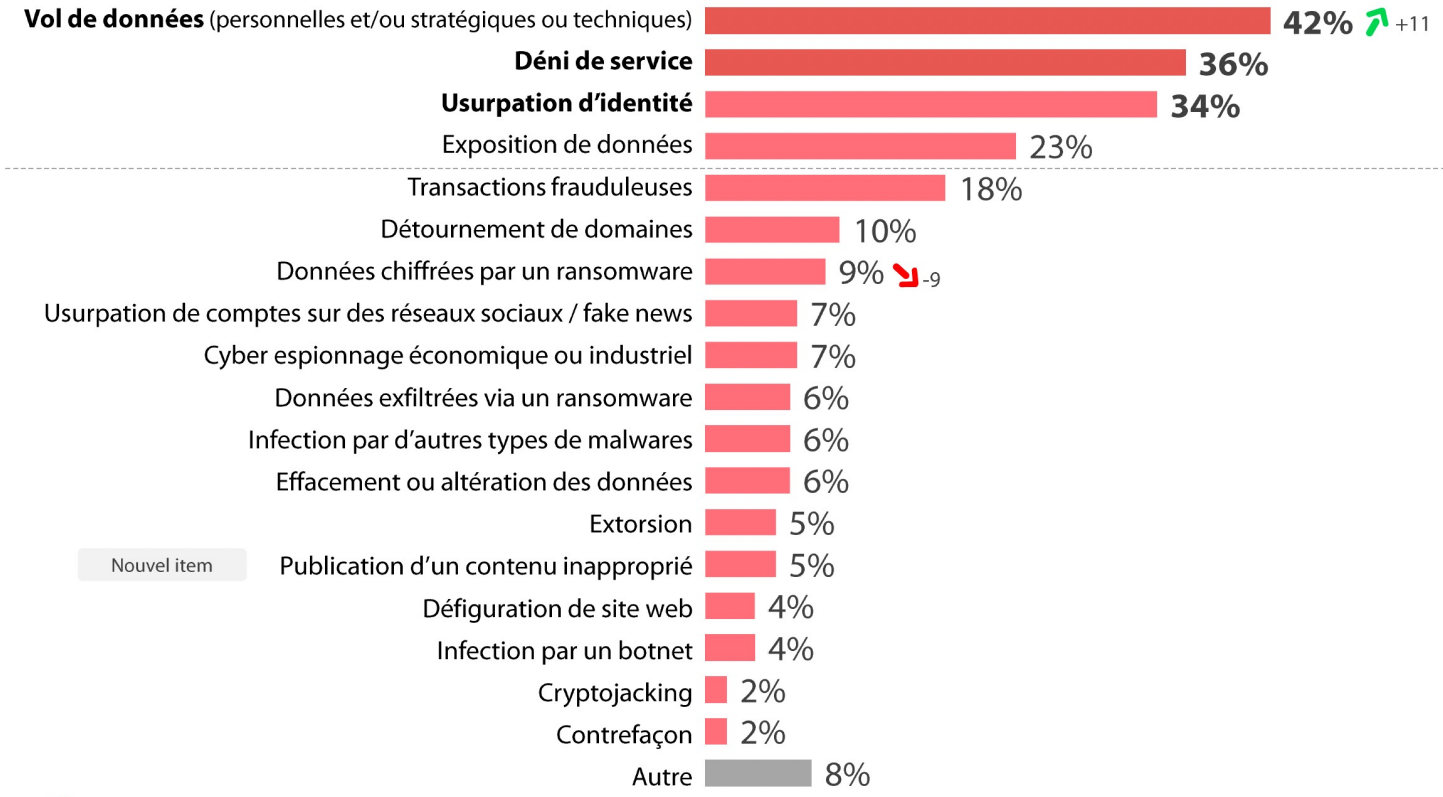
Le vol de données demeure en tête des conséquences de ces attaques et gagne même du terrain. Le déni de service et l'usurpation d'identité sont ensuite constatés par plus d'1/3 des entreprises. A noter, la baisse des données chiffrées par un ransomware.

190 personnes

Q5B. Et quelles ont été les conséquences de cette/ces attaque(s) ?

Base : ont constaté une attaque - plusieurs réponses possibles

47% des entreprises ont subi au moins une cyberattaque en 2023



L'écosystème des cyberattaques
La notion de cybercriminalité

L'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication, ainsi que celles dont la commission est facilitée ou liée à l'utilisation de ces technologies

Convention de Budapest (23 novembre 2001)

Infractions relatives au contenu

- Insultes racistes
- Négationnisme
- Pédopornographie
- Apologie du terrorisme
- Etc.

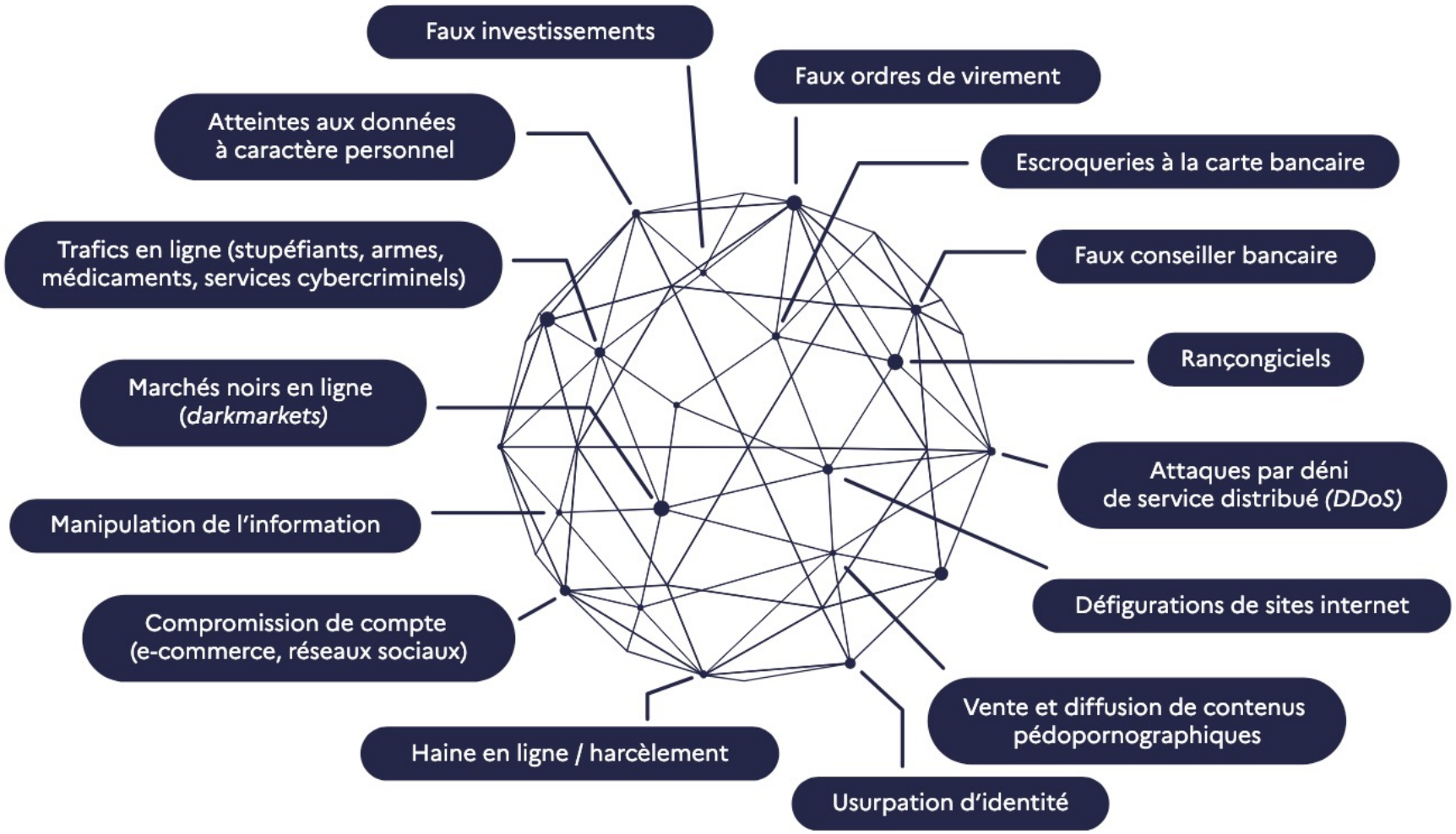
Infractions relatives à la propriété intellectuelle

- Mise en ligne de fichiers musicaux ou vidéos
- Diffusion de code sans autorisation de l'auteur

Infractions liées aux TIC

- Exploitation d'une vulnérabilité logicielle
- Diffusion de virus
- Escroquerie en ligne
- Intrusion de système

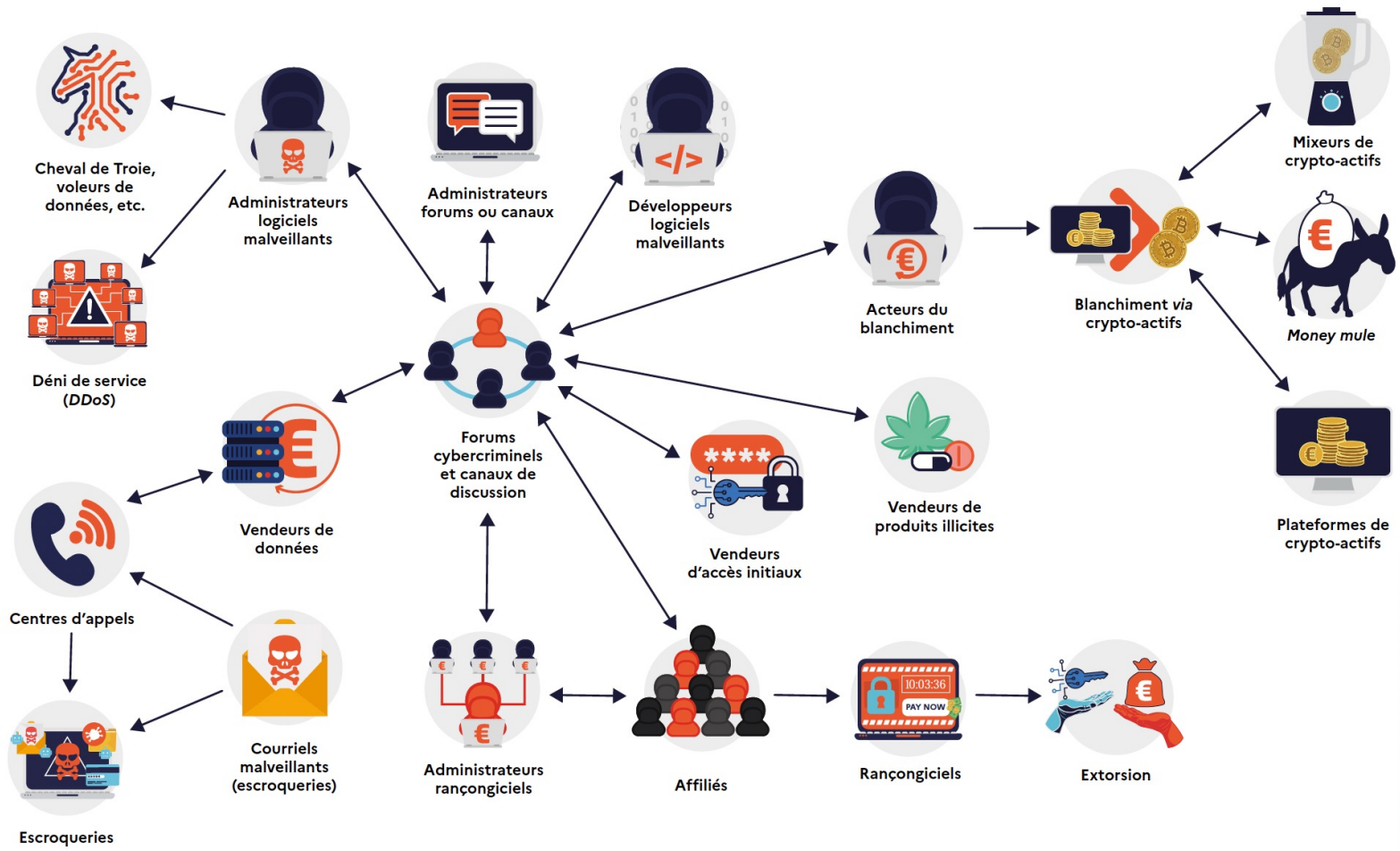
L'écosystème des cyberattaques
Quelques exemples de phénomènes cybercriminels



Exemples de phénomènes cybercriminels

L'écosystème des cyberattaques

La cybercriminalité : un écosystème avec de multiples acteurs



Exemple de modélisation d'un écosystème cybercriminel

Source : Rapport sur la cybercriminalité de 2024 du COMCYBER-MI

L'écosystème des cyberattaques
Les motivations principales

Gain financier

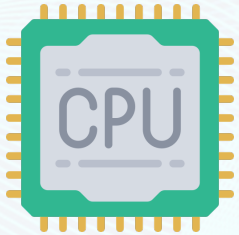
L'écosystème des cyberattaques
Les motivations des attaquants

Plusieurs mobiles peuvent pousser des cyber-délinquants à passer à l'acte

Gains financiers

Accès à de l'information, puis monétisation et revente :

- Utilisateurs, e-mails
- Organisation interne de l'entreprise
- Fichiers clients
- Mots de passe, n° de compte bancaire, cartes bancaires



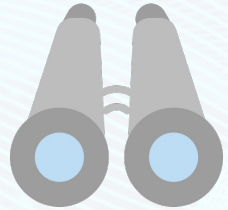
Utilisation de ressources

Utilisation, revente ou mise à disposition en tant que service :

- Bande passante & espace de stockage (hébergement de contenus illicites)
- Botnets
- Minage de cryptomonnaie
- Rebonds pour des attaques de la « supply-chain »

Chantage

- Déni de service
- Ransomware
- Fuite de données



Espionnage

- Industriel / concurrentiel
- Etatique

L'écosystème des cyberattaques
Les atteintes possibles pour les personnes

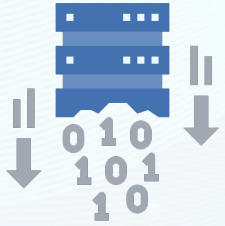
La cybercriminalité peut avoir différents impacts sur la vie privée des particuliers

Image / Vie privée

- Diffamation de caractère
- Divulgation d'informations personnelles
- Harcèlement / Cyber-bullying / Doxxing…

Usurpation d'identité

- Vol et réutilisation d'identifiants et d'informations personnelles pour effectuer des actions au nom de la victime



Perte de données

- Chiffrement des données
- Connexion frauduleuse à un compte « cloud » et suppression malveillante de l'ensemble des données

Financiers

- Usurpation de la carte bancaire pour des achats en ligne
- Chantage contre rançon

L'écosystème des cyberattaques
Les hacktivistes

- **Motivation idéologique :**
  - Révélation de scandales ou de mauvaises pratiques
  - Décrédibilisation d'une structure, d'une personne ou d'une organisation
  - Soutien à une cause

- **Actions possibles :**
  - Dysfonctionnement des systèmes pour attirer l'attention (DoS, DDoS)
  - Publication de messages idéologiques (défacement)
  - Publication d'informations volées
  - Déstabilisation des cibles (doxing)
  - Contournement des censures : geobombing, astroturfing, sites miroirs

L'écosystème des cyberattaques
Les cybercriminels

- **Motivation financière**
  - Menaces sur les particuliers : vol et revente de données de compte, fraude à la carte bancaire, demande de rançon après blocage de l'ordinateur, chantage à la webcam, arnaques de toute sorte…
  - Menaces sur les organisations privées et publiques
    - Vol de secret industriel ou stratégique
    - Fraude au président
    - Piratage de réseau d'une banque
    - Piratage de distributeurs de billets
    - Demandes de rançons

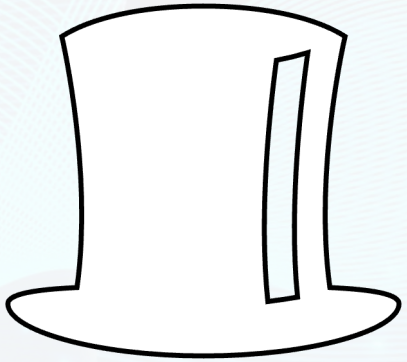
L'écosystème des cyberattaques
Les États

- **Espionnage**
- **Déstabilisation**
  - Désinformation classique
  - Vol de données réelles pour alimenter une campagne de désinformation et lui donner une grande crédibilité
  - Interruption du fonctionnement, voire sabotage d'organisations publiques comme privées
  - Sabotage d'infrastructures critiques
- **Appui aux opérations militaires**
  - Piégage des systèmes numériques à la source
  - Pré-positionnement sur les systèmes numériques des cibles
  - Ecoute et captation des données

L'écosystème des cyberattaques

Les chercheurs de failles

Black hat



White hat

Grey hat

L'écosystème des cyberattaques

La menace interne

Collusion

Malicieuse

Accidentelle

Menaces de tierce-partie

Délibérée

L'écosystème des cyberattaques

La mécanique d'une cyberattaque : la cyber kill chain

Approche proactive de la sécurité (protection, détection)

Approche réactive de la sécurité (réponse, rétablissement)

Les outils complémentaires à la cyber kill chain de Lockheed Martin

FIREEYE™ Le modèle alternatif de FireEye

MITRE ATT&CK® La matrice MITRE ATT&CK

Les acteurs de la SSI

Les acteurs de la SSI

Les institutions françaises, européennes et internationales

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

CERT-FR et CERTs sectoriels (CERT Santé, Maritime…)

CSIRTs régionaux

Commission Nationale Informatique et Libertés (CNIL)

Cybermalveillance (GIP ACYMA)

Associations professionnelles (CLUSIF, CESIN…)

Les acteurs de la SSI

Les institutions françaises, européennes et internationales

- European Union Agency for Cybersecurity (ENISA)
- European Data Protection Board (EDPB / CEPD)
- National Institute of Standards and Technology (NIST)
- Cybersecurity & Infrastructure Security Agency (CISA)
- Cloud Security Alliance (CSA)
- Open Web Application Security Project (OWASP)

Les acteurs de la SSI

La structuration de la cybersécurité dans une organisation

Gestion de la sécurité et pilotage des projets de sécurité

- Directeur Cyber
- RSSI
- Coordinateur sécurité
- Directeur de programme sécurité
- Responsable de projet de sécurité

Conception et maintien d'un SI sécurisé

- Chef sécurité de projet
- Architecte de sécurité
- Spécialiste sécurité dans un domaine
- Cryptologue
- Administrateur de solutions de sécurité
- Auditeur

Gestion des incidents et des crises de sécurité

- Responsable SOC
- Analyste SOC
- Responsable CSIRT
- Analyste CSIRT
- Gestionnaire de crise cybersécurité
- Analyste de la menace

Conseil, services et recherche

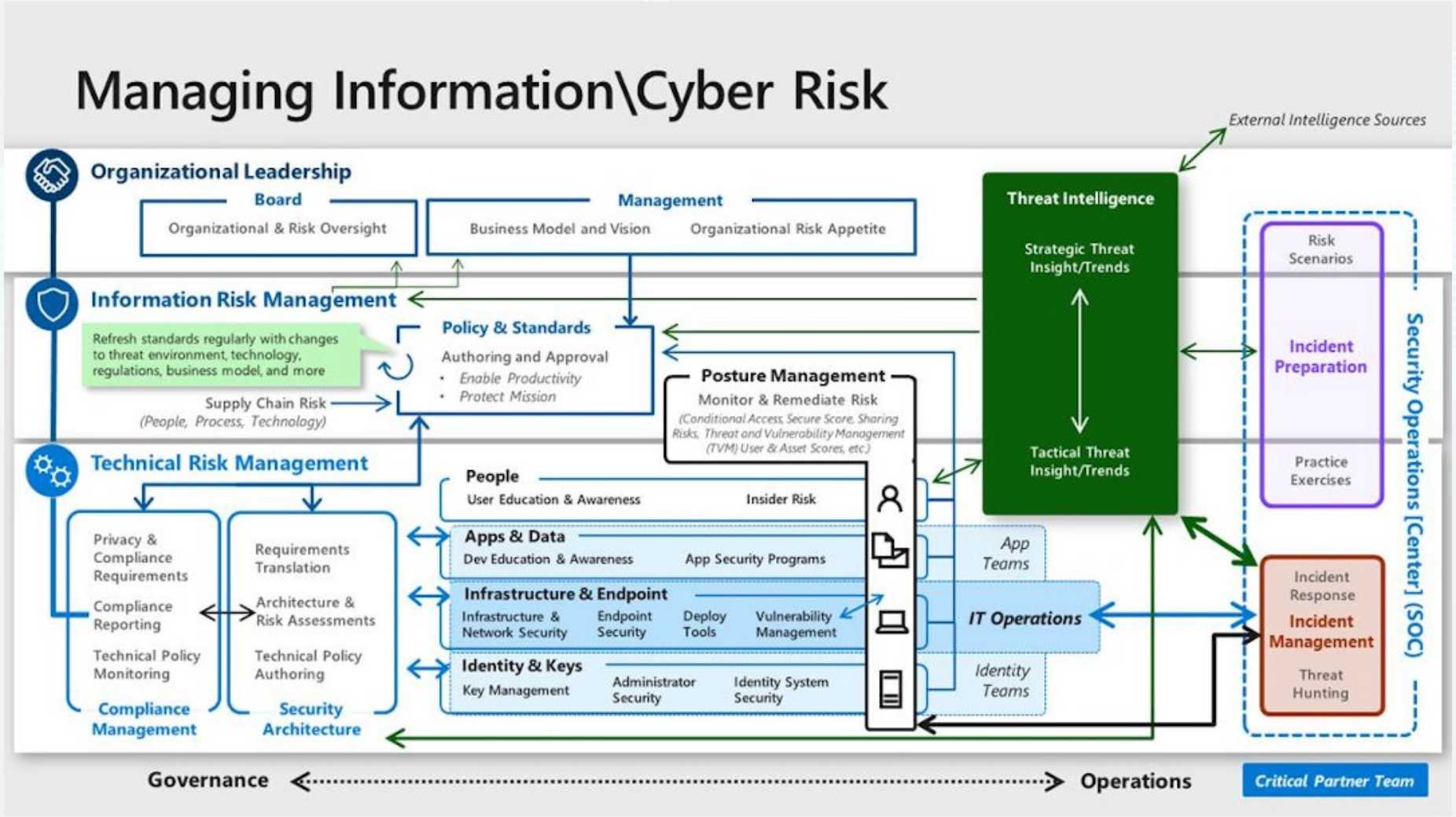
- Consultant
- Formateur
- Évaluateur
- Développeur
- Intégrateur
- Chercheur

Métiers connexes

- Responsable du plan de continuité d'activité (RPCA)
- Délégué à la protection des données
- Gestionnaire de risques / Risk Manager
- Directeur sûreté

Les acteurs de la SSI

La structuration de la cybersécurité dans une organisation



Source : Microsoft

La gestion des risques SSI

La gestion des risques SSI
La définition d'un risque cyber (ISO/IEC 27000)

« Le risque lié à la sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'un actif ou d'un groupe d'actifs informationnels et nuisent donc à un organisme»

ISO/IEC 27000, article 3.6.1 (note 6)

Vraisemblance (*probabilité d'occurrence*)

Conséquence (*impact*)

La gestion des risques SSI
La notion d'actifs

« Item, chose ou entité qui a une valeur potentielle ou réelle pour un organisme »

ISO 55000 article 3.2.1

Le S.I. regroupe des actifs primordiaux et des actifs supports

Actifs primaires

- Processus métiers
- Informations

Actifs supports

- Bâtiments / Locaux
- Matériels informatiques
- Logiciel
- Personnel / Prestataire
- Réseaux
- Compétences / Organisation

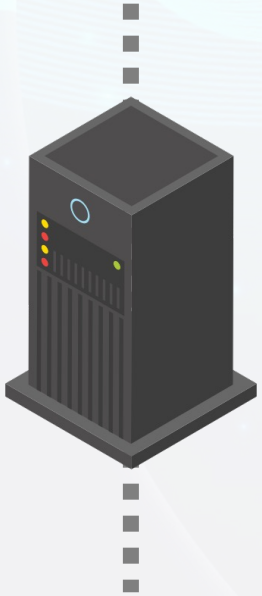
La gestion des risques SSI
La notion de vulnérabilité

« Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces »

ISO/IEC 27000, article 3.77

Vulnérabilité intrinsèque

Incapacité d'un serveur à traiter des données



Vulnérabilité extrinsèque

Serveur situé dans une zone sujette aux inondations saisonnières

La gestion des risques SSI
La notion de vulnérabilités : exemples

ISO/IEC 27005, Tableau A.11 (extrait)

Catégorie	Exemple de vulnérabilités
Matériel	• Maintenance insuffisante / mauvaise installation des supports de stockage • Insuffisance des programmes de remplacement périodique des équipements • Sensibilité aux variations de température
Logiciel	• Absence ou insuffisance des tests logiciels • Failles connues dans le logiciel • Téléchargement et utilisation non contrôlés de logiciels
Réseau	• Mécanismes insuffisants pour les preuves d'envoi ou de réception d'un message • Architecture réseau non sécurisée • Connexions au réseau public non protégées
Personnel	• Absence de personnel • Utilisation incorrecte du logiciel et du matériel • Faible sensibilisation à la sécurité
Site	• Utilisation inadaptée ou négligente du contrôle d'accès physique aux bâtiments et aux salles • Emplacement situé dans une zone sujette aux inondations • Protection physique insuffisante du bâtiment, des portes et des fenêtres
Organisme	• Procédure formelle de révision (supervision) des droits d'accès non élaborée, ou mise en œuvre inefficace • Insuffisante ou absence des rapports d'erreur enregistrés dans les journaux administrateurs et les journaux opérateurs • Absence ou insuffisance des dispositions (relatives à la sécurité de l'information) dans les contrats avec les employés

La gestion des risques SSI
La notion de menace

« Cause potentielle d'un incident lié à la sécurité de l'information qui peut entraîner des dommages pour un système ou porter préjudice à un organisme. »

ISO/IEC 27005, article 3.1.9

Menace

- Intentionnelle
- Accidentelle
- Environnementale

exploite

Vulnérabilité

- Organisationnelle
- Logique
- Physique

impactant

Actif support

Equipement et personnes sur lesquels reposent l'actif primaire

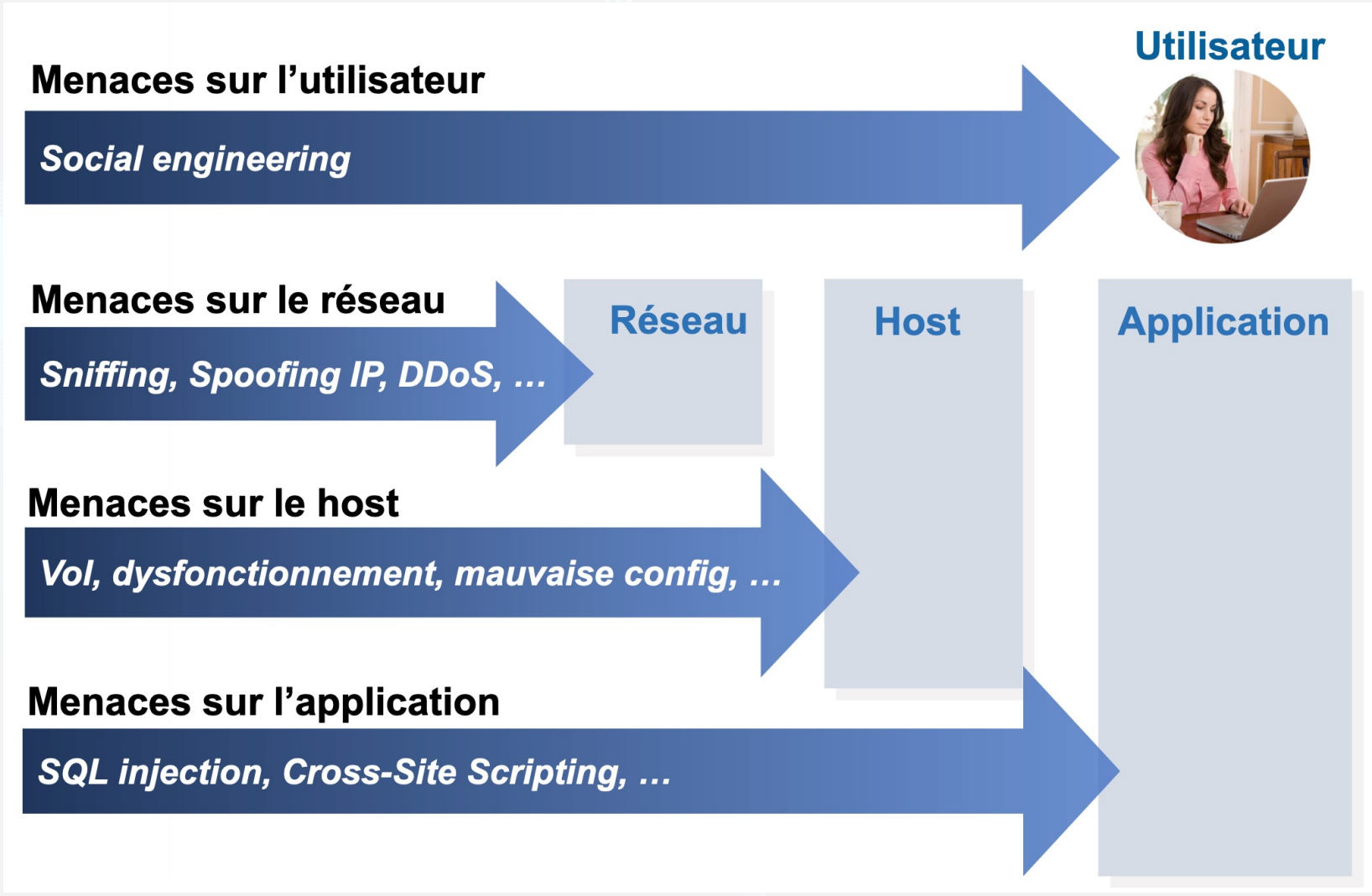
nuit

Actif primaire

Processus ou information clé de l'entreprise

ISO/IEC 27005, article 7.2.1

La gestion des risques SSI
La notion de menace



La gestion des risques SSI
La notion de menace

ISO/IEC 27005, Tableau A.10 (extrait)

Catégorie	Description	Source		
Menaces physiques	Incendie	A	D	E
	Eau	A	D	E
	Poussière, corrosion, congélation	A	D	E
Menaces naturelles	Phénomène climatique			E
	Phénomène sismique			E
Défaillances des infrastructures	Perte de la source d'alimentation en électricité	A	D	E
	Défaillance d'un réseau de télécommunication	A	D	E
Défaillances techniques	Défaillance des machines ou du système		D	
	Violation de la maintenabilité du système d'information	A	D	
Actions humaines	Terrorisme, attaque, sabotage		D	
	Ingénierie sociale		D	
	Traitement non autorisé de données à caractère personnel	A	D	
Compromission de fonctions ou de services	Erreur d'utilisation		D	
	Abus de droits ou de permissions	A	D	
	Falsification de droits ou de permissions		D	
Menaces organisationnelles	Manque de personnel	A		E
	Manque de ressources	A		E
	Violation de la législation ou de la règlementation	A		E

La gestion des risques SSI
Notion d'impact

La survenance d'un risque a un ou plusieurs impacts directs et indirects sur les actifs

Les impacts directs sur les actifs

Impacts sur la disponibilité

- Dégradation de la performance
- Interruption du service
- Indisponibilité du service
- Perturbation des opérations

Impacts sur la confidentialité

- Atteinte à la vie privée des utilisateurs ou des clients
- Atteinte à la vie privée des employés
- Fuite d'information confidentielle

Impacts sur l'intégrité

- Changement accidentel
- Changement délibéré
- Résultats incorrects
- Résultats incomplets
- Perte de données

La gestion des risques SSI
Notion d'impact

La survenance d'un risque a un ou plusieurs impacts directs et indirects sur les actifs

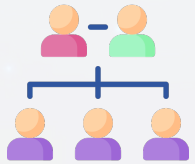
Les impacts métiers

Pertes financières (pertes d'exploitation, gestion de crise…)

Mise en danger de la sécurité du personnel ou des utilisateurs (attaque sur un SI industriel)

Sanctions pénales ou administratives liés à des manquements règlementaires ou contractuels

Perte de réputation (perte de confiance des clients, indisponibilité d'un service)



Atteinte à l'organisation (dysfonctionnement d'un service)

La gestion des risques SSI
La notion de niveau de risque

Estimations réalisées avec les échelles définies par l'organisation

Niveau et intensité des effets

😱 **Gravité**

📊 **Vraisemblance**

Faisabilité ou probabilité qu'un risque se réalise

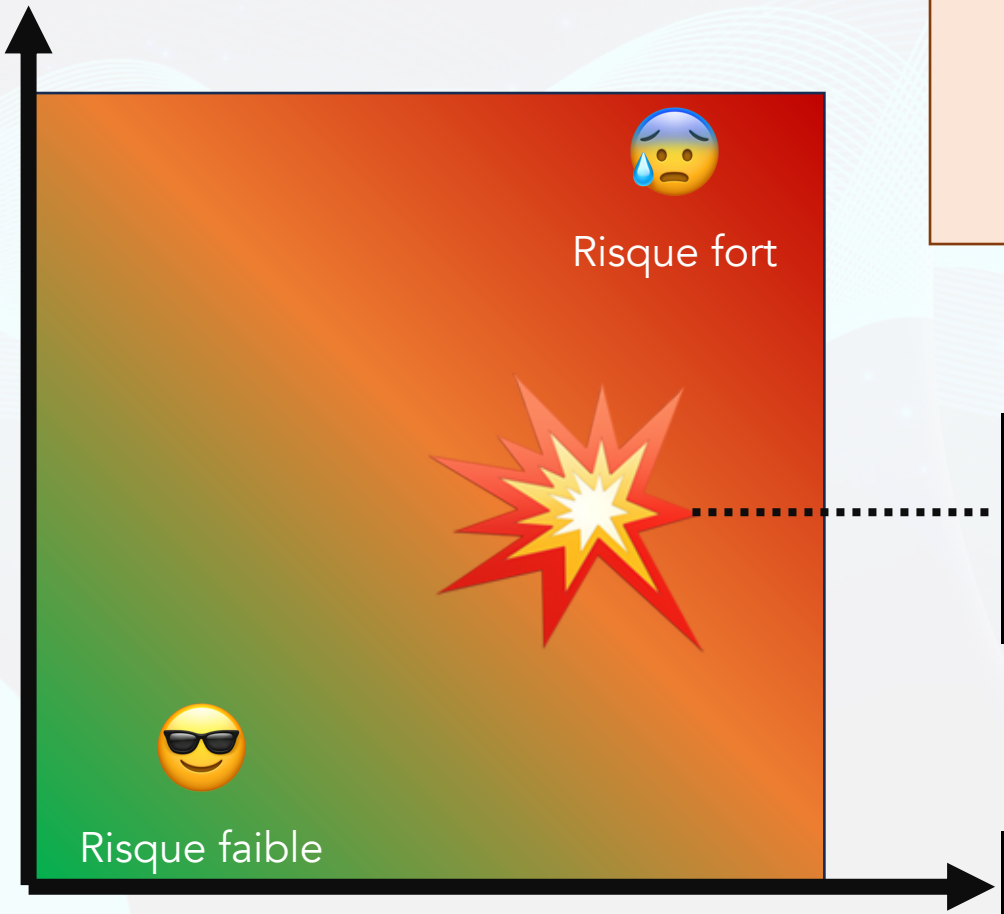
☠️

Niveau de risque

Importance (criticité) du risque

La gestion des risques SSI
La représentation d'un risque

Gravité *Mineur, significatif, grave, critique, catastrophique*



Les scénarios de risques sont représentés sur une « cartographie des risques » (appelé aussi diagramme de Farmer) selon leur niveau de vraisemblance et leur gravité

Événement redouté *Arrêt de la climatisation dans des locaux, vol d'un ordinateur portable contenant des données sensibles, chiffrement des données à cause d'un ransomware, séisme affectant un datacenter…*

Vraisemblance *Invraisemblable, peu vraisemblable, plausible, très vraisemblable, quasi-certain…*

La gestion des risques SSI

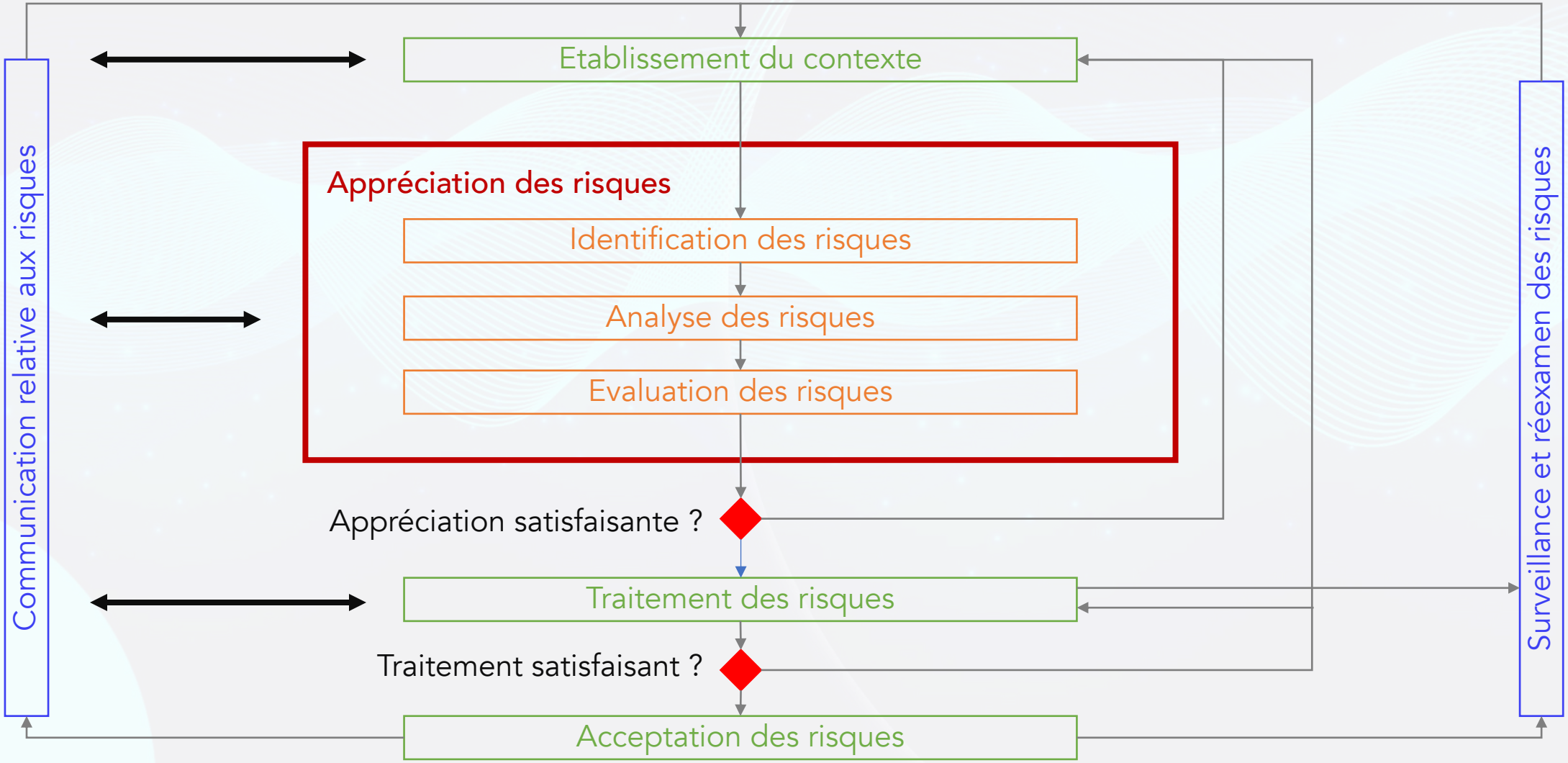
Les objectifs de la gestion des risques en cybersécurité

Gérer les risques cyber, c'est réduire l'incertitude sur les actifs informationnels d'un organisme

Où sommes-nous le plus vulnérable ?

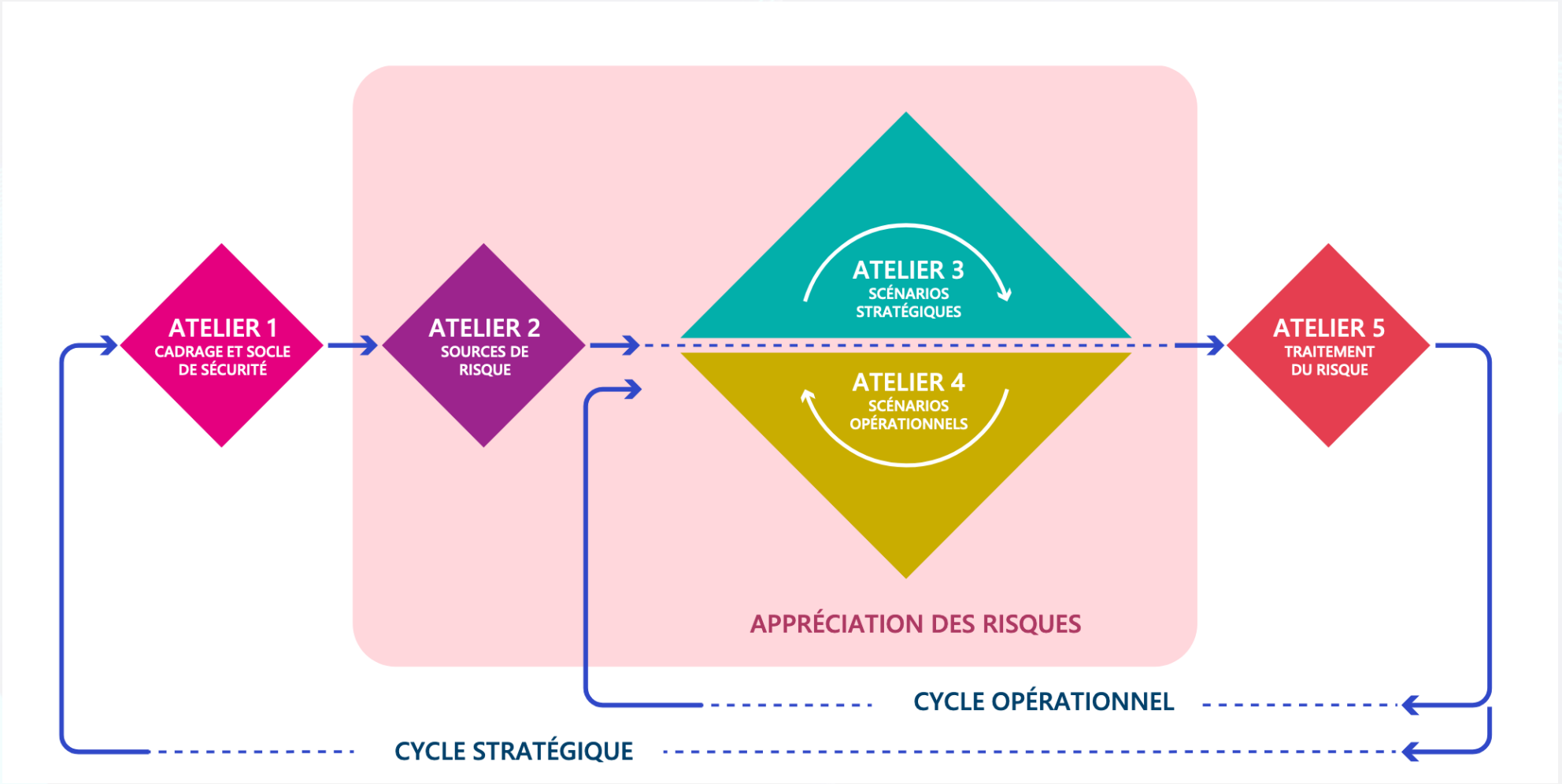
Comment devons-nous dépenser notre argent pour nous protéger contre les menaces cyber ?

La gestion des risques SSI
La démarche ISO 27005



La gestion des risques SSI

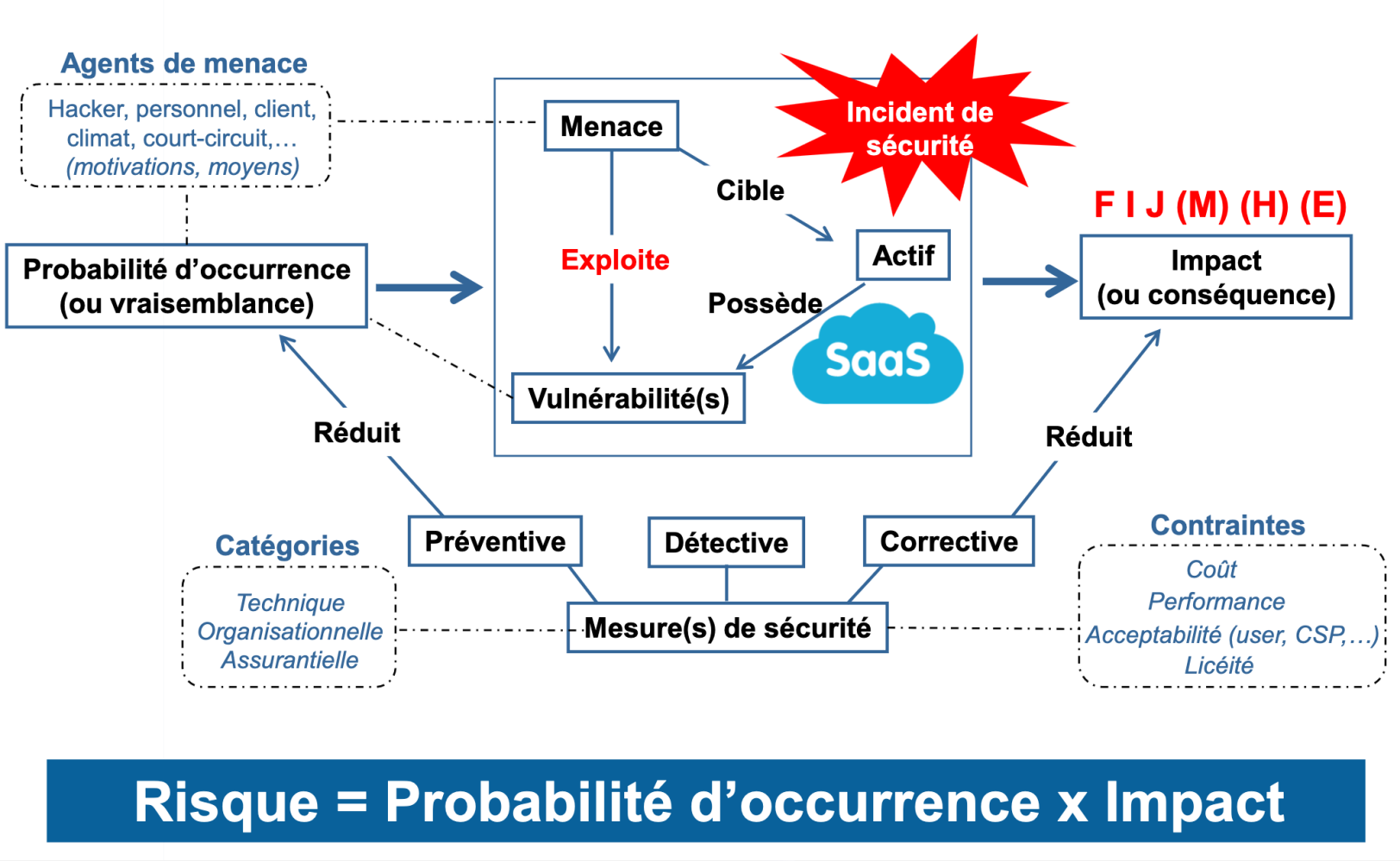
La méthodologie EBIOS RM : les cinq ateliers



Source : Formation EBIOS RM de l'ANSSI

La gestion des risques SSI

Une autre schématisation de la définition d'un risque



Source : VERISAFE