Master Informatique – parcours SIS
sebastien.duval@loria.fr

Sécurité des Systèmes d'Information

Chapitre 6 : Gestion de la sécurité au sein d'une organisation

2025/2026

Supports basés sur le cours de Laurent Vigneron

Plan du chapitre

1. **Normes et sécurité organisationnelle**
2. **Intégrer la sécurité dans les projets**
3. **Supervision et gestion centralisée – SIEM, SOC et plus**
4. **Difficultés liées à la prise en compte de la sécurité**
5. **Métiers liés à la cybersécurité**

1. Normes et sécurité organisationnelle

a) Préambule
b) Panorama des normes ISO 2700x
c) Système de Management de la Sécurité de l'Information (27001)
d) Code de bonnes pratiques pour le management de la sécurité de l'information (27002)
e) Gestion des risques (27005)
f) Classification des informations
g) Gestion des ressources humaines
h) Autres normes de sécurité

1. Intégrer la sécurité au sein d'une organisation

a. Préambule

- Les mesures de sécurité à mettre en place dépendent de l'activité, de l'organisation et de la réglementation et des contraintes de son écosystème.

- Afin d'évaluer le niveau de sécurité attendue, les questions suivantes peuvent être posées :
  - Qu'est ce que je veux protéger ?
  - De quoi je veux me protéger ?
  - A quel type de risques mon organisation est exposée ?
  - Qu'est ce que je redoute ?
  - Quelles sont les normes qui s'appliquent à mon organisation ?

- L'organisation peut s'inspirer de la famille de normes internationales ISO 27000 et des guides nationaux (ANSSI, CLUSIF, etc.), voire des politiques de sécurité en usage dans l'État (PSSIE, RGS, etc.) pour mettre en place la sécurité.

1. Intégrer la sécurité au sein d’une organisation

D’après vous ?

La sécurité informatique, c’est un métier technique ?

1. Intégrer la sécurité au sein d’une organisation

a. Préambule

- En pratique, une grande part de la sécurité n’est pas technique
  - Sensibilisation
  - Politique d’entreprise
  - Choix des fournisseurs et partenaires
  - Respect des normes de sécurité
- Beaucoup d’experts en sécurité juniors font de la technique, et beaucoup de seniors (> 30 ans, parfois même directement en 1er job parce qu’il y a un besoin en ce moment) ne font plus de technique

1. Intégrer la sécurité au sein d'une organisation

b. Panorama des normes ISO 27000

- Ensemble de normes internationales de sécurité de l'information, destinées à protéger l'information. Elles découlent d'une recherche de consensus commun sur le domaine.
- Néanmoins la conformité à une norme ne garantit pas formellement un niveau de sécurité. Les normes ne prennent pas en compte l'état de l'art récent et les exigences réglementaires.
- Quelques-unes des principales normes inclues dans la série 27000 :

27001	Systèmes de management de la sécurité de l'information
27002	Code de bonne pratique
27004	Surveillance, mesurage, analyse et évaluation
27005	Gestion des risques
27035	Gestion des incidents de sécurité
27037	Gestion des preuves numériques
…	...

1. Intégrer la sécurité au sein d'une organisation

b. Panorama des normes ISO 27000

- Dans le cadre de la mise en place de la sécurité au sein d'une organisation :
  - La norme **ISO 27001** permet à une organisation de **mettre en œuvre et d'améliorer le système de management de la sécurité** :
    - Une certification ISO 27001 délivrée par un organisme certificateur accrédité garantit suite à un audit qu'une organisation a bien appliqué les exigences de la norme en matière de sécurité. Cette certification est valable 3 ans, tous les ans un audit de contrôle est effectué.
    - Il peut être exigé d'une organisation d'avoir cette certification pour accéder à certains contrats : par exemple un organisme payeur d'aides agricoles européennes.
  - La norme **ISO 27002** définit un ensemble de « **bonnes pratiques** » en matière de sécurité réparties en plusieurs chapitres, l'organisation dispose :
    - d'un référentiel de mise en œuvre ;
    - d'une « check-list » en cas d'audit.
  - La norme **ISO 27005** définit des lignes directrices relatives à la **gestion des risques de sécurité** dans une organisation. Une organisation peut s'appuyer sur ce processus de gestion de risques pour intégrer la sécurité.

1. Intégrer la sécurité au sein d'une organisation

c. Management de la Sécurité de l'Information (27001)

Une démarche calquée sur ISO 9000 (**Plan / Do / Check / Act**).

Phase Plan : fixer des objectifs et des plans d'actions :

- Identification des actifs ou des biens.
- Analyse de risques.
- Choisir le périmètre du SMSI :
  - Quel périmètre ? C'est le domaine d'application du SMSI, son choix est libre, mais il doit être circonscrit, ce sont toutes les activités pour lesquelles l'organisation exige de la confiance.
  - Quelle politique de sécurité ?
  - Quel niveau de sécurité : intégrité, confidentialité, disponibilité de l'information au sein de l'organisation ?

Noter que la norme n'impose pas de niveau minimum de sécurité à atteindre.

Attention : une entreprise peut donc être certifiée ISO 27001 tout en ayant défini un périmètre réduit et une politique de sécurité peu stricte.

1. Intégrer la sécurité au sein d'une organisation

c. Management de la Sécurité de l'Information (27001)

- **Phase Do :** mise en œuvre et exploitation des mesures et de la politique
  - Établir un plan de traitement des risques.
  - Déployer les mesures de sécurité.
  - Former et sensibiliser les personnels.
  - Détecter les incidents en continu pour réagir rapidement.

- **Phase Check :** mesurer les résultats issus des actions mises en œuvre
  - Audits internes de conformité et d'efficacité du SMSI (ponctuels et planifiés).
  - Réexaminer l'adéquation de la politique SSI avec son environnement.
  - Suivre l'efficacité des mesures et la conformité du système.
  - Suivre les risques résiduels.

- **Phase Act :**
  - Planifier et suivre les actions correctrices et préventives.

1. Intégrer la sécurité au sein d'une organisation

c. Management de la Sécurité de l'Information (27001)

Avantages

- Description détaillée de la **mise en œuvre des objectifs et des mesures de sécurité.**
- **Audits réguliers** qui permettent le suivi entre les risques initialement identifiés, les mesures prises et les risques nouveaux ou mis à jour.

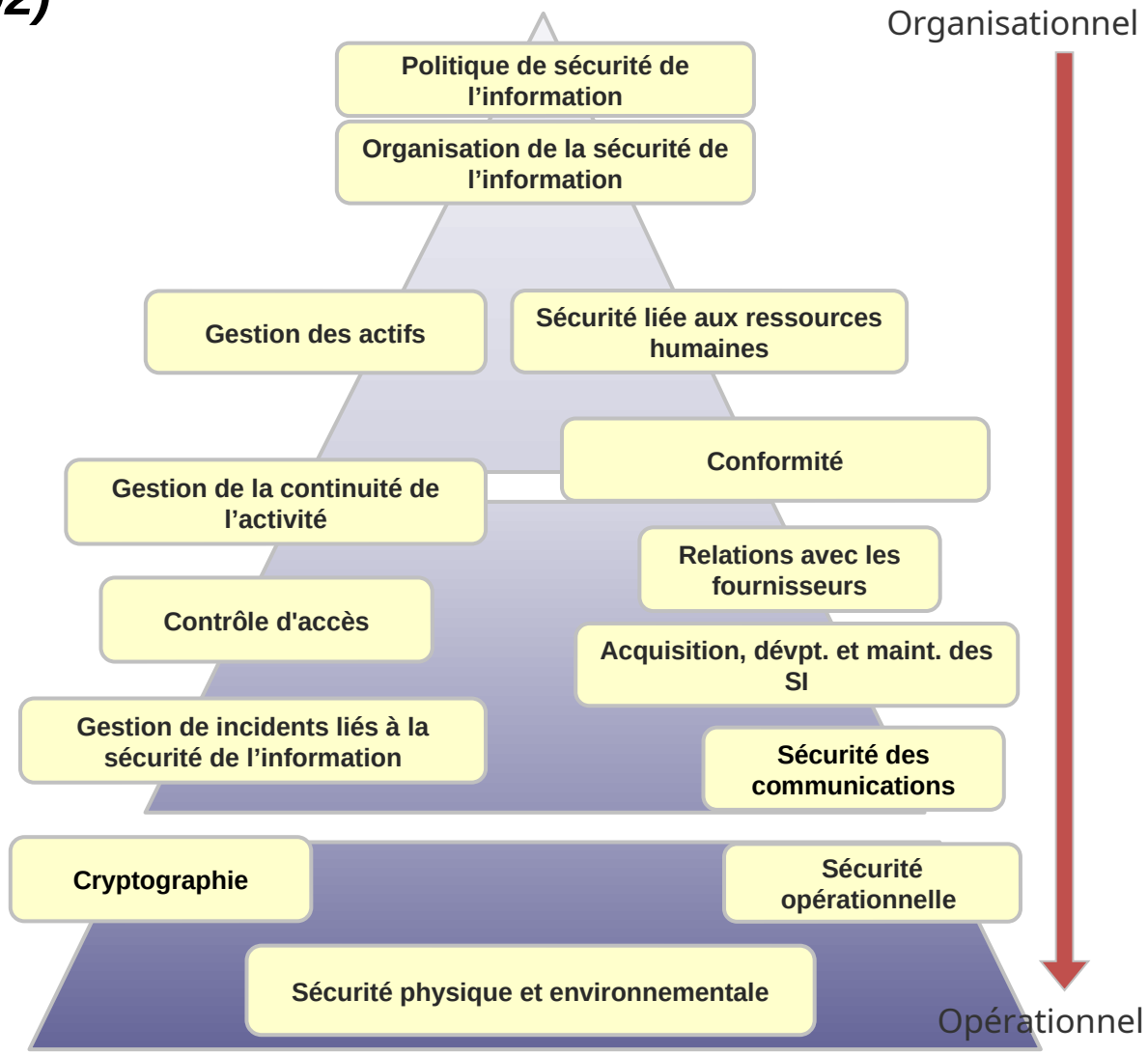
  Objectif **:** mesurer l'**efficacité** des mesures prises.
- **Sécurité** : une amélioration continue de la sécurité : donc un niveau croissant de sécurité et de maturité en SSI.
- Meilleure **maîtrise** des différents **risques.**
- Élimination des mesures de sécurité non usitées.
- Amélioration de la **confiance des associés, partenaires & clients**.
- **Référentiel international** qui facilite les échanges.
- **Indicateurs** clairs et fiables produisant des éléments de pilotage financier pour les dirigeants.

1. Intégrer la sécurité au sein d'une organisation

d. Code de bonne pratique (27002)

- La norme ISO/IEC 27002:2013 constitue un code de bonnes pratiques. Elle est composée de 114 mesures de sécurité réparties en 14 chapitres couvrant les domaines organisationnels et techniques ci-contre.

- C'est en adressant l'ensemble de ces domaines que l'on peut avoir une approche globale de la sécurité des S.I.



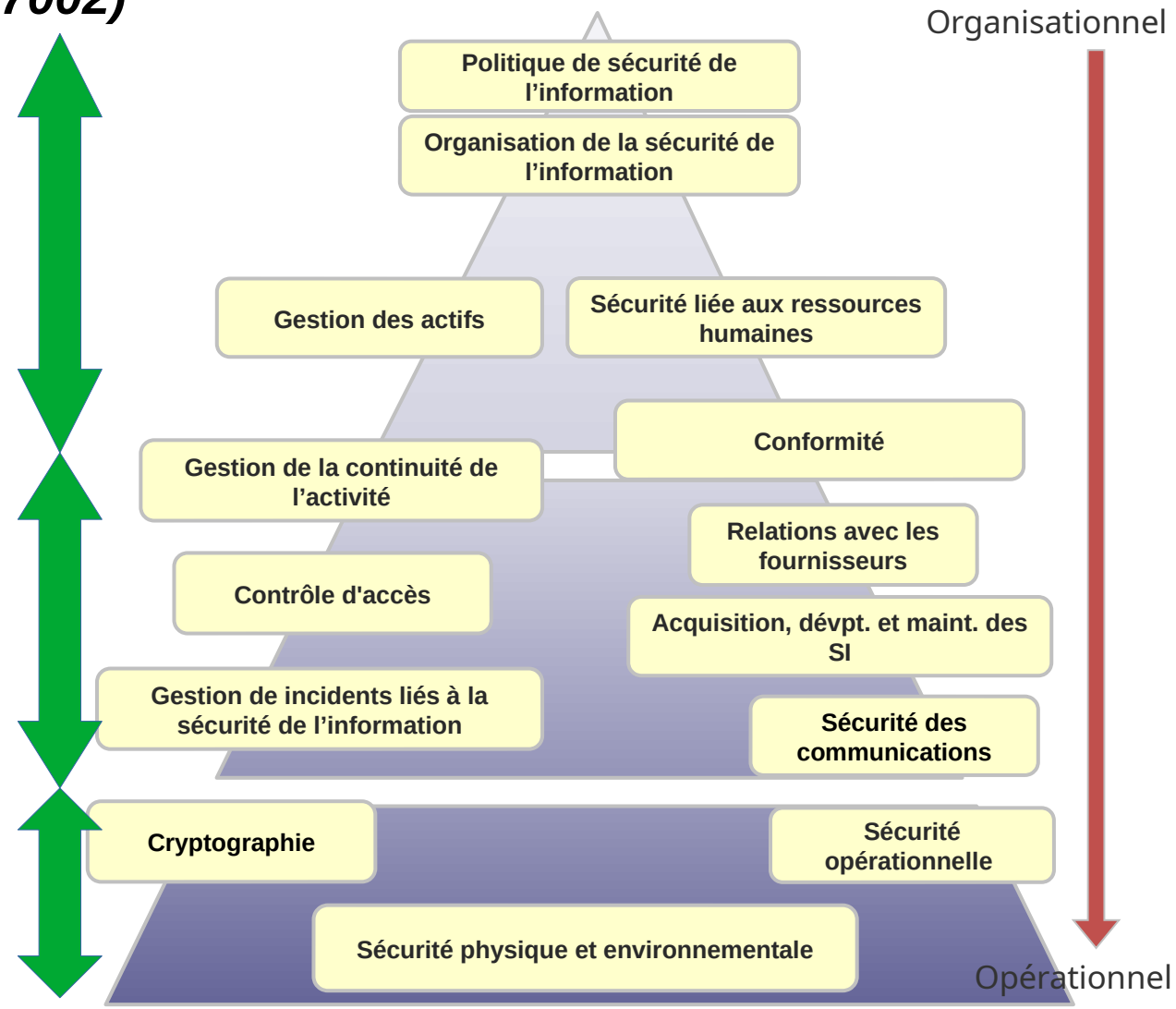
1. Intégrer la sécurité au sein d'une organisation

d. Code de bonne pratique (27002)

- *seniors*
- *auditeurs organisationnels*

- *juniors*
- *auditeurs techniques*

- *chercheurs*
- *auditeurs spécialisés (rares)*



1. Intégrer la sécurité au sein d'une organisation

d. Code de bonne pratique (27002)

- Exemples de mesures sur le chapitre « Contrôle d'accès » :
  - L'accès aux fichiers/répertoires doit être restreint conformément aux politiques de contrôle d'accès :
    - Seuls les professeurs autorisés doivent pouvoir accéder à un répertoire contenant les épreuves des futurs examens/concours.
  - Les propriétaires de l'information doivent vérifier les droits d'accès à intervalles réguliers :
    - Le responsable des concours doit contrôler les droits d'accès au répertoire contenant les épreuves des futurs examens/concours pour s'assurer qu'il n'y a pas d'étudiants qui auraient été rajoutés.

- Exemples de mesures sur le chapitre « Sécurité opérationnelle » :
  - L'installation et la configuration de logiciels doivent être encadrés :
    - Seuls les administrateurs doivent pouvoir installer un logiciel sur un poste.
  - Des sauvegardes doivent êtres régulièrement effectuées et testées :
    - Un espace de sauvegarde des données peut être mis à disposition des utilisateurs.

1. Intégrer la sécurité au sein d'une organisation

e. Gestion des risques (27005)

La norme 27005 présente **une démarche** :

- Établissement du contexte de l'analyse des risques.
- Définition de l'appréciation des risques SSI.
- Choix pour le traitement du risque SSI.
- Acceptation du risque.
- Communication et concertation relative aux risques SSI.
- Surveillance et revue du risque en SSI.

Avantages

- Définit une démarche rationnelle qui a donné lieu à des méthodes qui fonctionnent.
- Grande souplesse : utilisée en toutes circonstances, surtout lors des changements.
- Pragmatique et utilisable seule, elle peut aussi bien convenir aux petites organisations.

Limites

- L'organisation doit définir sa propre approche.
- Méthodes nécessitant souvent de la formation et non adaptables à toutes les situations.
- Dépendance vis-à-vis de la cartographie du SI : profondeur, étendue etc.
- Tendance à l'exhaustivité (liste blanche).
- Accumulation de mesures techniques sans cohérence d'ensemble.

1. Intégrer la sécurité au sein d'une organisation

f. Classification des informations

- La classification selon la confidentialité des informations aide à définir des mesures de protection appropriées pour chaque type d'information.

	Intitulé	Explication	Exemple	Risque
C1	Accès libre	Tout le monde peut y accéder	Informations publiées sur le site internet	Aucun
C2	Accès à l'organisation	Seul le personnel de l'organisation est autorisé à accéder à l'information	Nom, adresse des partenaires et fournisseurs de l'organisation	Atteinte à l'image, gêne passagère
C3	Diffusion limitée	Au sein de l'organisation, seul un groupe de personnes est autorisé, comme les membres du même projet	Plan technique d'un nouveau laboratoire ; Liste des personnes admissibles avant publication officielle…	Situation à risques ; pertes financières acceptables
C4	Confidentiel	L'information est accessible à une liste très restreinte d'utilisateurs à titre individuel	Contenu des brevets déposés ; Recherche en cours ; N° de sécurité sociale et noms…	Pertes financières inacceptables, poursuites judiciaires

1. Intégrer la sécurité au sein d'une organisation

f. Classification des informations

- Sur la base des niveaux de confidentialité définis, les mesures suivantes peuvent être implantées :
  - Une politique de gestion des informations est définie :
    - Création d'un modèle de document indiquant le niveau de confidentialité.
    - Sensibilisation du personnel et des partenaires à cette politique.
  - Les informations de niveau « **Confidentiel** » doivent être :
    - envoyées par mél de manière chiffrée et le mot de passe communiqué par SMS aux destinataires.
    - stockées localement dans des conteneurs chiffrés.
  - Les informations de niveau « **Diffusion limitée** » doivent être échangées au travers d'un système documentaire collaboratif ayant des accès nominatifs contrôlés, par exemple MS SharePoint (aujourd'hui, énormément de solutions existent).

1. Intégrer la sécurité au sein d'une organisation

g. Gestion des ressources humaines

- **Avant embauche** :
  - Sélection des candidats et interviews.
  - Vérification du CV du candidat (contacter les anciens employeurs, vérifier les diplômes, certifications…).
  - En fonction de la sensibilité du poste, un extrait de casier judiciaire peut être demandé.
- **Pendant l'embauche** :
  - Fourniture des accès logiques (création de comptes utilisateurs, accès aux répertoires nécessaires…) et physiques (badges) adaptés à la fonction.
  - Sensibilisation aux politiques et procédures internes de l'organisation.
  - Sensibilisation régulière à la sécurité adaptée aux fonctions.
  - Processus disciplinaire en cas de non respect.
- **Au terme du contrat de travail** :
  - Retrait des accès et restitution du matériel fourni (badge, ordinateur, …).

1. Intégrer la sécurité au sein d'une organisation

h. Autres normes de sécurité – CIS pour les TPE-PME

- CIS : Center for Internet Security
- Chartes d'évaluation (benchmarks) pour les technologies courantes (OS, logiciels...)
- Outil open-source CIS-CAT (+ version Pro) : test automatique de la configuration d'une machine vis-à-vis des benchmarks (scores sur 100) + propose un patch.

Summary — **CIS Ubuntu Linux 18.04**

Description	Tests					Scoring		
	Pass	Fail	Error	Unkn.	Man.	Score	Max	Percent
1 Initial Setup	**21**	**22**	**0**	**0**	**7**	**21.0**	**43.0**	**49%**
1.1 Filesystem Configuration	11	10	0	0	3	11.0	21.0	52%
1.1.1 Disable unused filesystems	0	7	0	0	0	0.0	7.0	0%
1.2 Configure Software Updates	0	0	0	0	2	0.0	0.0	0%
1.3 Configure sudo	1	2	0	0	0	1.0	3.0	33%
1.4 Filesystem Integrity Checking	0	2	0	0	0	0.0	2.0	0%
1.5 Secure Boot Settings	0	3	0	0	1	0.0	3.0	0%
1.6 Additional Process Hardening	2	2	0	0	0	2.0	4.0	50%
1.7 Mandatory Access Control	2	1	0	0	0	2.0	3.0	67%
1.7.1 Configure AppArmor	2	1	0	0	0	2.0	3.0	67%
1.8 Warning Banners	5	2	0	0	0	5.0	7.0	71%
1.8.1 Command Line Warning Banners	4	2	0	0	0	4.0	6.0	67%
2 Services	**24**	**2**	**0**	**0**	**1**	**24.0**	**26.0**	**92%**
2.1 inetd Services	2	0	0	0	0	2.0	2.0	100%
2.2 Special Purpose Services	18	1	0	0	1	18.0	19.0	95%
2.2.1 Time Synchronization	3	0	0	0	1	3.0	3.0	100%
2.3 Service Clients	4	1	0	0	0	4.0	5.0	80%
3 Network Configuration	**18**	**11**	**0**	**0**	**10**	**18.0**	**29.0**	**62%**

1. Intégrer la sécurité au sein d'une organisation

h. Autres normes de sécurité – NIST Cybersecurity Framework (CSF) v 2.0 et MITRE ATT&CK

- Instanciation plus bas-niveau d'ISO 27k
- Plus concret mais demande tout de même de l'adaptation
- Automatisation de certaines parties de la mise aux normes / vérification des normes
- Identifier les « kill-chains » : succession de vulnérabilités qui peuvent mener à une attaque grave (en ignorant les autres vulnérabilités)
- Basé sur l'approche MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) : classification et description de cyberattaques, beaucoup plus technique

1. Intégrer la sécurité au sein d’une organisation

Conclusion

- Une politique de sécurité doit être adaptée à l'organisme et à ses évolutions.
- La sécurité ne s'improvise pas et nécessite des professionnels.
- Les normes sont une aide pour mettre en œuvre une démarche d'amélioration continue de la sécurité.
- Les normes par nature ne délivrent pas un niveau de sécurité.
- Les normes ne prennent pas en compte toute la sécurité des systèmes d'information.

1. Intégrer la sécurité au sein d’une organisation

D’après vous ?

Comment on fait pour convaincre la direction qu’il faut changer la politique d’entreprise ?

2. Intégrer la sécurité dans les projets

a) Préambule
b) Sécurité dans l'ensemble du cycle de vie d'un projet
c) Sécurité prise en compte en fin de développement
d) Approche par l'analyse et le traitement du risque
e) Plan d'action SSI

2. Intégrer la sécurité dans les projets

a. Préambule

- Il s'agit de bien distinguer :
  - **la sécurité du système d'information** qui est un des objets du projet ;
  - **et la sécurité du projet en lui-même** (diffusion et traitement des informations).

- Concernant la sécurité du SI en lui-même :
  - toute activité étant gérée en mode projet, une bonne intégration de la sécurité dans l'organisation nécessite l'intégration de la sécurité dans chaque projet dans le respect de la réglementation ;

  - isoler les traitements de données sensibles au sein du projet pour avoir une meilleure maîtrise des risques et des mesures de sécurité à mettre en œuvre pour réduire ces risques.

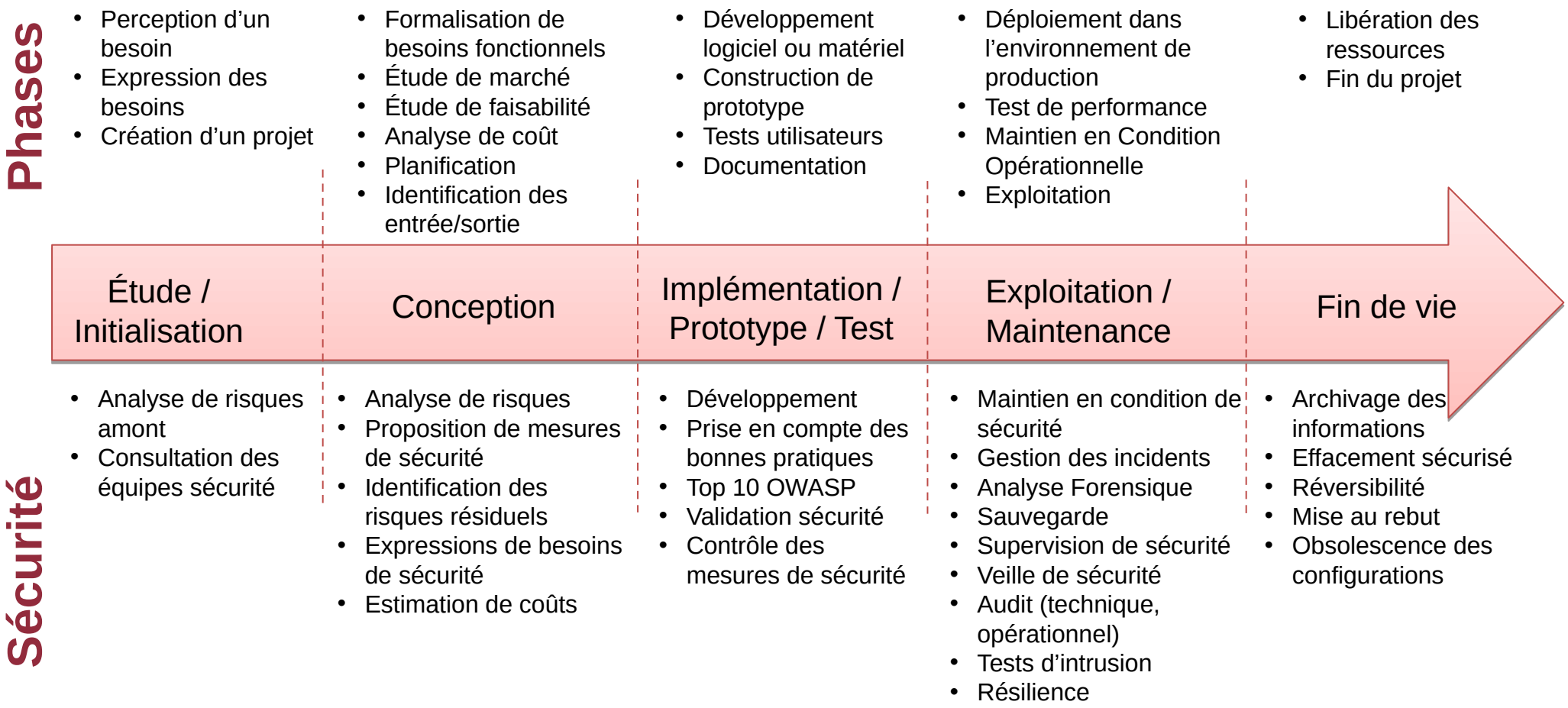
2. Intégrer la sécurité dans les projets

a. Préambule

- La sécurité doit être prise en compte dans **toutes les étapes** d'un projet :
  - Application de la démarche d'amélioration continue (c'est très adapté aux projets Agiles).
  - Respect des impératifs et des contraintes notamment juridiques et réglementaires.
  - Responsabilisation des acteurs, documentations, gestion du temps.

2. Intégrer la sécurité dans les projets

b. Exemple d'intégration de la sécurité dans le cycle de vie d'un projet



2. Intégrer la sécurité dans les projets

c. Sécurité prise en compte en fin de développement

- Exemple d'un projet de développement de site Web :
  - L'audit de sécurité fait le constat que :
    - Les versions de composants logiciels utilisés sont obsolètes et vulnérables.
    - La base de données n'a pas été correctement isolée, et les tables ont été créées à l'intérieur d'une autre base de données à accès public.
    - La politique de gestion de mots de passe n'est pas conforme aux bonnes pratiques : création de mots de passe faibles ; stockage de mots de passe en clair…
    - Le niveau de disponibilité attendu pour ce site ne peut être assuré avec l'infrastructure existante.
  - Conséquences :
    - Besoin de rachats de licences logicielles : coût supplémentaire.
    - Recréation de la base de données sur un espace dédié correctement protégé.
    - Redéveloppement des modules de gestion des mots de passe : coût supplémentaire.
    - Modification de l'infrastructure pour assurer le niveau de disponibilité requis.

Délai, coût et effort supplémentaires…

2. Intégrer la sécurité dans les projets

c. Sécurité prise en compte en fin de déploiement

- Exemple d'un projet de construction d'une nouvelle salle devant héberger les serveurs de l'organisation :
  - L'audit de sécurité fait le constat que :
    - Les baies de stockage des serveurs ne se ferment pas à clé.
    - Pas de mécanisme de contrôle d'accès (lecteur de badge) prévu pour tracer les accès.
    - Pas de redondance (alimentation, accès de télécommunications) des équipements.
    - Aucune alarme anti-intrusion ou incendie n'est prévue.
    - L'arrivée de câbles dans la salle est exposée à des actes de malveillances.
    - La salle est construite en zone inondable.
  - Conséquences :
    - Rachat de matériel et d'équipements => coût supplémentaire.
    - Re-câblage de la salle, et travaux de génie civil à prévoir.
    - Relocalisation de la salle ou reconstruction => coût supplémentaire très importante.

Reconstruction de la salle ou relocalisation de la salle, délai et coût supplémentaires…

2. Intégrer la sécurité dans les projets

d. L'approche par l'analyse et le traitement du risque

- L'analyse de risques doit être effectuée en amont du projet mais doit aussi évoluer au fur et à mesure de l'exploitation du système (analyse de risque dynamique dans la supervision du système) et fonction de l'évolution des risques (évolution des vulnérabilités, des menaces, du système d'information).

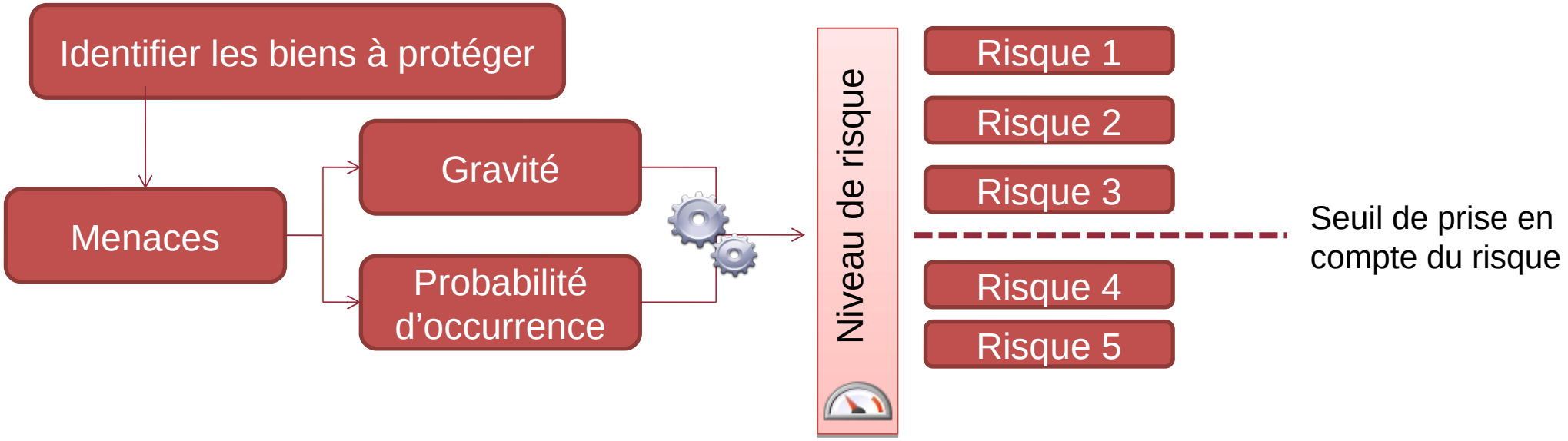
- L'analyse de risque consiste à :
  - identifier les biens à protéger,
  - analyser la fréquence et la gravité du danger pour évaluer la criticité du risque,
  - établir une hiérarchisation des risques : fréquence vs gravité,
  - établir un seuil d'acceptabilité pour chacun de ces risques,
    - seuil au-delà duquel le risque doit être pris en compte par les mesures de sécurité.
  - identifier des mesures de sécurité.

- Les mesures ainsi identifiées peuvent constituer un cahier de charges sécurité pour le projet, qu'il soit réalisé en interne ou externalisé.

2. Intégrer la sécurité dans les projets

d. L'approche par l'analyse et le traitement du risque

Une démarche d'analyse de risque peut être schématisée ci-dessous :



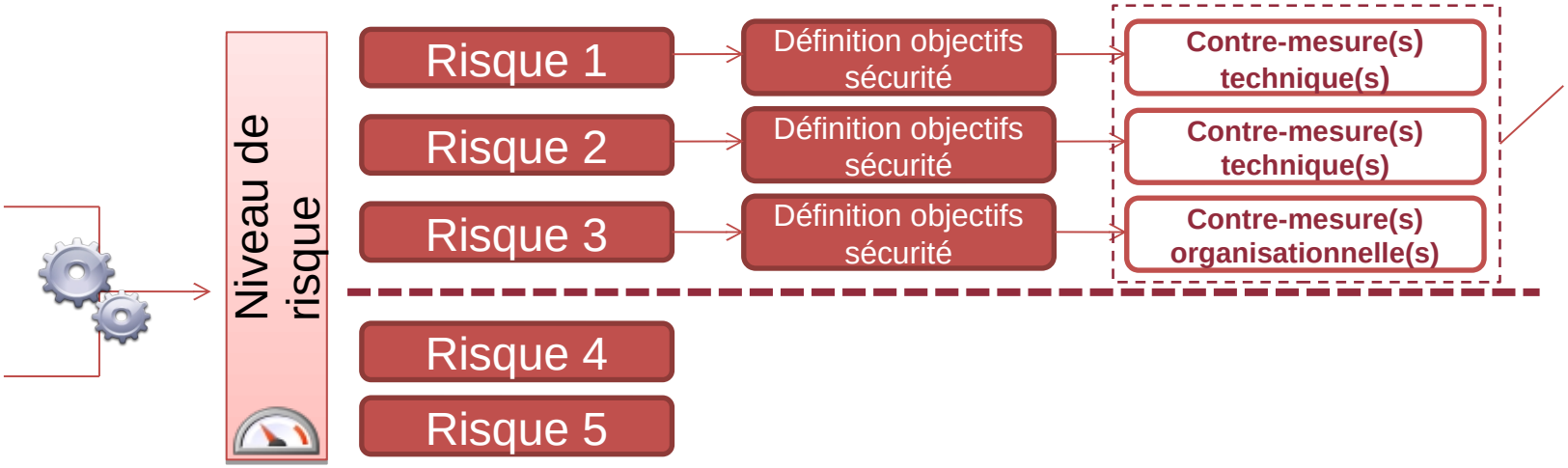
La hiérarchisation des risques permet de déterminer les risques qui :

- doivent absolument être traités et donc réduits par des mesures ;
- ceux qui sont acceptables et avec lesquels le système peut exister.

2. Intégrer la sécurité dans les projets

d. L'approche par l'analyse et le traitement du risque

- Pour les risques dont le niveau est supérieur au seuil de prise en compte :
  - Définir les objectifs de sécurité.
  - Définir les mesures techniques et organisationnelles qui vont permettre d'atteindre ces objectifs.
- Pour les risques dont le niveau est inférieur au seuil de prise en compte :
  - un risque résiduel est le risque subsistant après le traitement de risque (car – par exemple – le coût pour compenser ce risque est trop élevé par rapport au risque encouru).



Plan d'actions de SSI que l'entreprise va devoir mettre en œuvre pour protéger son S.I.

2. Intégrer la sécurité dans les projets

d. L'approche par l'analyse et le traitement du risque

Une analyse de risque peut être assez complexe et nécessite rigueur et méthode, il faut notamment trouver le bon niveau d'abstraction.

Voici 3 exemples de méthodes d'analyses de risques compatibles avec les lignes directrices de l'ISO 27005 :

- **EBIOS** : Expression des Besoins et Identification des Objectifs de Sécurité

  développée par le Club EBIOS auquel participe l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information

- **MEHARI** : MEthode Harmonisée d'Analyse de Risques

  développée par le CLUSIF, Club de la Sécurité de l'Information Français

- **OCTAVE** : Operationally Critical Threat, Asset, and Vulnerability Evaluation

  développée par l'Université de Carnegie Mellon.

2. Intégrer la sécurité dans les projets

d. L'approche par l'analyse et le traitement du risque

L'analyse de risque et la gestion des risques est une spécialité de master à part entière, donc on ne fait ici qu'effleurer ce domaine important.

2. Intégrer la sécurité dans les projets

e. Plan d'actions SSI

Le défi vis-à-vis de la mise en place des mesures de sécurité est asymétrique entre « attaquer » et « défendre » :

- L'attaque peut réussir par l'exploitation d'une seule vulnérabilité.
- Tandis que la défense doit prendre en compte l'ensemble du système.

Un plan d'action des mesures de sécurité à mettre en place à l'issue de l'analyse de risques devrait respecter le principe de « **défense en profondeur** » qui recommande :

- d'avoir plusieurs lignes de défenses indépendantes.
- que chaque ligne constitue une barrière autonome contre les attaques.
- que la perte d'une ligne de défense implique qu'on passe à un niveau de défense plus fort.

Les objectifs de la défense en profondeur sont :

- prévenir, bloquer, limiter, détecter, alerter, réagir, réparer.

2. Intégrer la sécurité dans les projets

D'après vous ?

Des exemples de sécurité en profondeur ?

2. Intégrer la sécurité dans les projets

e. Plan d'actions SSI

Politique de sécurité, procédure de secours, sensibilisation…

Gardiens, verrous, contrôle d'accès…

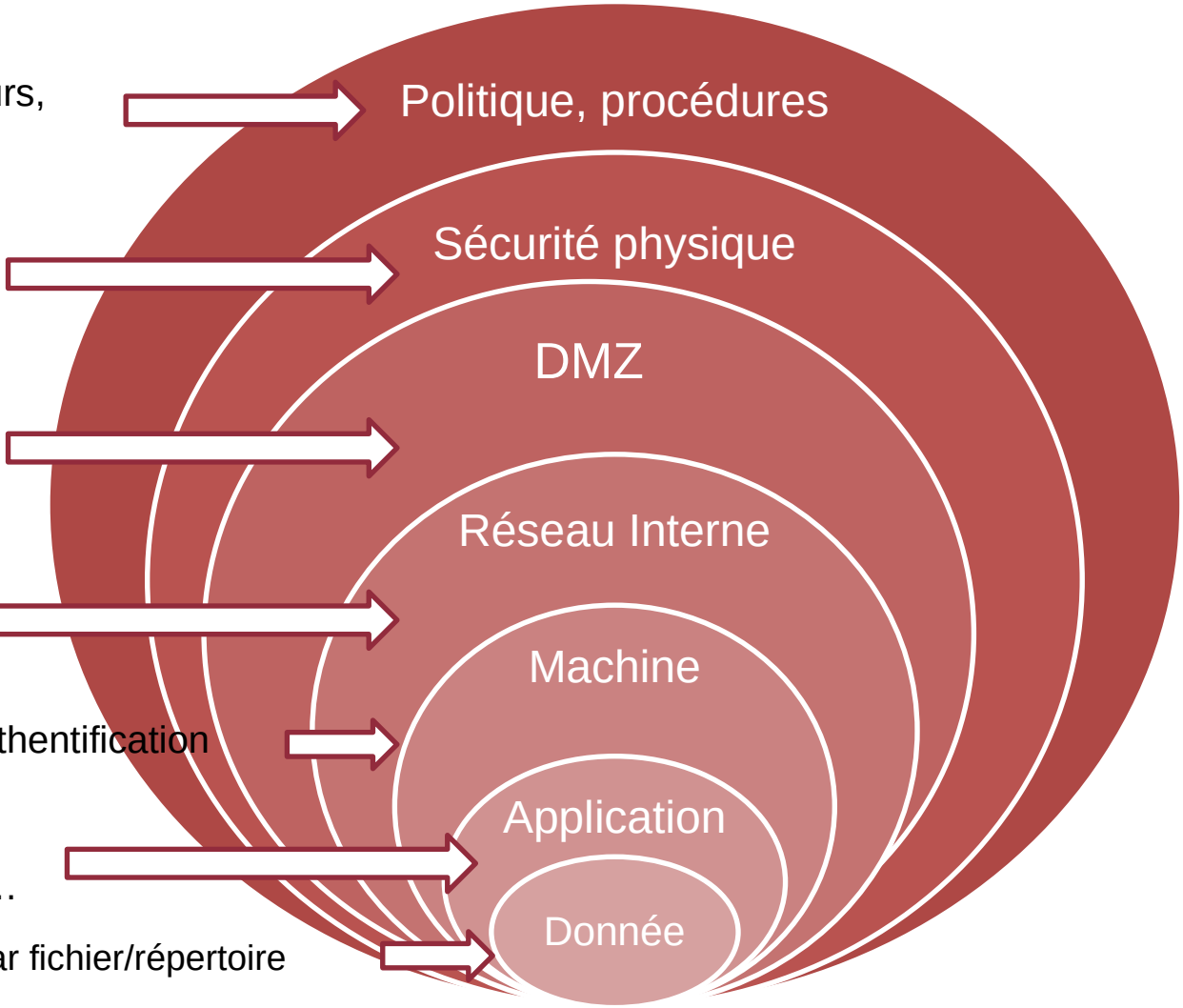
Pare-feu, VPN, Zone démilitarisée…

Sous-réseau, NIDS, VLAN…

Antivirus, Correctifs de sécurité, HIDS, Authentification

Contrôle des entrées, test d'intrusion, communication (https, ssh…), traçabilité…

Chiffrement, mots de passe, droit d'accès par fichier/répertoire



2. Intégrer la sécurité dans les projets

Conclusion

- La sécurité des systèmes d'information : un élément indispensable d'un projet.
- Une sécurité globale et cohérente, et non une accumulation de mesures et de produits de sécurité.
- Une politique de sécurité réaliste et pragmatique.
- Un élément clé : la connaissance du système d'information (cartographie) et de son niveau de sécurité (contrôle, audit).
- Une difficulté et une nécessité : le maintien en condition de sécurité du système d'information.
- Un accroissement des besoins de sécurité : besoin en compétences et en professionnels.

3. Supervision et gestion centralisée – SIEM, SOC et plus

a) SIEM – Définition
b) SIEM – Technologies courantes
c) EDR et SOC – Gestion d'alertes
d) Surcouches – Ticketing, Automatisation

3. Supervision et gestion centralisée – SIEM, SOC et +

a. SIEM – Définition – Security Information and Event Manager

3 composants :

- **Génération de logs** : sondes, agents (i.e. logiciel ou matériel qui tourne indépendamment des fonctionnalités dans un système et génère des logs) – dans les équipements réseau (pare-feux, switches, …), les nœuds du système (DMZ, Active Directory, …), les applications, …
- **Agrégation + enrichissement de logs** : centralisation des logs dans un serveur dédié, mise à un format commun, associations de logs (e.g. le log réseau d'IP *xxx.xxx.xxx.xxx* est lié au log appli de l'utilisateur *user*), enrichissement de logs (heure, classification, …).
- **Visualisation de logs** : une base de données de logs, c'est bien, une interface graphique avec une IHM utilisable, c'est mieux, ça permet d'afficher un beau message clignotant en cas d'alerte, de classifier les logs par type (info, alerte, …) et importance (urgent, secondaire, …).

3. Supervision et gestion centralisée – SIEM, SOC et +

b. SIEM – Technologies courantes

En 3 composants :

- **ELK** : ElasticSearch, Logstash, Kibana
  - agents/sondes : variés (dépendants des technos)
  - ElasticSearch comme base de donnée de logs
  - Logstash comme agrégateur + enrichisseur
  - Kibana comme visualiseur
  - Courant, passe bien à l'échelle, installation locale

Tout en 1 :

- **Splunk** – courant, adapté à toute entreprise, dans le Cloud
- **Graylog** – simple, adapté aux PME, installation locale

Plein d'alternatives, dépend du cas d'usage (prix, souveraineté, …).

3. Supervision et gestion centralisée – SIEM, SOC et +

c. EDR et SOC – Gestion d'alertes

SOC (Security Operations Center) – centre de réponse à incident

- Par-dessus un SIEM : on voit les alertes, maintenant il faut les traiter
- Équipe d'analystes
- Réaction à incident
- [Audit de prévention éventuel en plus, mais pas le cœur d'un SOC]

EDR (Endpoint Detection and Response)

- mini-SOC automatisé dans les équipements sensibles

3. Supervision et gestion centralisée – SIEM, SOC et +

c. Surcouches – Ticketing, Automatisation

Ticketing

- Application qui répartit automatiquement les alertes en catégories, importance, complexité, et les attribue à des analystes pour traitement

Automatisation

- SOAR (Security Orchestration Automatisation and Response) – on automatise les tâches usuelles pour accélérer la réponse à incident
- Tendance montante mais encore rare

4. Difficultés liées à la prise en compte de la sécurité

a) Compréhension insuffisante des enjeux
b) Implication nécessaire de la direction
c) Difficulté pour faire des choix en toute confiance
d) Délicat arbitrage entre commodité et sécurité
e) Suivre l'évolution des technologies
f) Frontières floues entre sphères professionnelle, publique, et privée

4. Difficultés liées à la prise en compte de la sécurité

a. Une compréhension insuffisante des enjeux…

…liée à un problème d'éducation

- L'information a une valeur importante pour l'entreprise, pour les concurrents, pour les États. On parle aujourd'hui de « guerre de l'information ».
  - Chaque année des centaines de compagnies en France sont victimes d'espionnage industriel ou économique :
    - écoute des conversations ;
    - espionnage des écrans d'ordinateurs ;
    - social engineering, etc.
  - Des actes aisés dans les transports : train, avion, etc.

1 ordinateur portable volé toutes les 53 secondes
70 millions de smartphones perdus par an

4. Difficultés liées à la prise en compte de la sécurité

a. Une compréhension insuffisante des enjeux…

…liée à un problème de formation

- Des dirigeants qui n'ont pas tous une culture sécurité.
- Des évolutions vers le poste de « RSSI », sans formation complémentaire adéquate (parce qu'il n'y a pas assez de gens compétents sur le marché) :
  - personnel issu de la technique : administrateur réseau, système…
  - personnel issu de la qualité : responsable qualité…
- Un coût lié à la sécurité qui rebute en période de crise :
  - Authentification forte : achats de jetons/carte à puce.
  - Plan de secours : acheter en double certains équipements.
  - Personnel : former aux bonnes pratiques en sécurité…

4. Difficultés liées à la prise en compte de la sécurité

a. Une compréhension insuffisante des enjeux…

…entraînant de nombreux risques pour l'entreprise ou pour l'organisation

- Perte d'informations essentielles.
- Arrêt de la production.
- Détérioration de l'image/réputation.
- Risques juridiques/réglementaires…

…entraînant de nombreux risques pour les États

- Indisponibilité de services.
- Perte de crédibilité.
- Divulgation d'informations sensibles.
- Risques de conflits avec d'autres États…

4. Difficultés liées à la prise en compte de la sécurité

b. L'implication nécessaire de la direction

Rien ne peut se faire sans l'aval de l'exécutif.

Le chef d'entreprise doit être conscient des enjeux de sécurité pour l'avenir de son entreprise :

- Être **proactif** plutôt que réactif. La PSSI est une réflexion stratégique : elle permet de prévoir l'avenir de l'organisation.

- **Prendre le temps** de comprendre, ne pas être absorbé que par ses marchés, ses clients, ses concurrents, son relationnel.

- La sécurité :
  - **va au-delà de la technique**. L'humain joue un rôle central ;
  - **ne doit pas rester un domaine d'experts**. La sécurité est l'affaire de tous et une préoccupation de tous les responsables ;
  - n'est pas seulement une contrainte coûteuse mais **elle est aussi un investissement**, un atout supplémentaire pour l'organisation.

4. Difficultés liées à la prise en compte de la sécurité

b. L'implication nécessaire de la direction

Investir dans la sécurité ne suffit pas. Il faut être conscient des enjeux vis-à-vis de l'organisation. La dynamique sécurité viendra de la direction.

- Le dirigeant doit **montrer l'exemple** d'abord en y accordant un intérêt : charismatique, il est le premier à sensibiliser les personnes concernées.
- **Motiver** son RSSI ou ses administrateurs pour faire appliquer la politique de sécurité de l'organisation et maîtriser leurs systèmes le mieux possible.
- **Responsabiliser** : en désignant un responsable de la coordination, qui distribuera les tâches au sein des équipes.
- **Réagir** en cas d'attaque avérée : mettre des ressources à disposition, permettre l'expertise juridique et porter plainte.
- **Impliquer** ses personnels, les sensibiliser et leur permettre de suivre des formations.

4. Difficultés liées à la prise en compte de la sécurité

c. Difficulté pour faire des choix en toute confiance

Il est important de faire des choix éclairés en prenant en compte la sécurité.

"L'implantation en France des chinois Huawei et ZTE pose une question de sécurité nationale"

Par **JMBockel** (Express Yourself) publié le 01/10/2012 à 15:12, mis à jour à 15:25

Sécurité et Huawei : un rapport britannique accablant

Le sort de l'équipementier pas encore scellé

Par Mathieu Chartier (@chartier_mat) | Publié le 29/03/19 à 17h02 | Édité par Noluenn Bizien

Vie privée : La NSA s'octroie un backdoor dans tous les systèmes Windows

Le Gouvernement Chinois a adopté une nouvelle régulation exigeant des entreprises qui vendent des ordinateurs aux banques chinoises de fournir le code source et de se soumettre à des audits.

4. Difficultés liées à la prise en compte de la sécurité

D'après vous ?

Quels sont les matériels/logiciels de confiance ?

Quels sont les prestataires de service de confiance ?

4. Difficultés liées à la prise en compte de la sécurité

c. Difficulté pour faire des choix en toute confiance

Quels sont aujourd'hui les matériels ou logiciels de confiance ?

- Ceux issus de l'industrie nationale vs ceux de nos partenaires de confiance : alliés, fournisseurs.
- Ceux issus du monde libre (« open source »).
- Les matériels qualifiés par l'ANSSI.

Quels sont les organismes de confiance ?

- Les entreprises nationales ou européennes (mais qui sont les actionnaires ?).
- Nos partenaires de longue date.
- Les autorités gouvernementales.
- Les prestataires de service qualifiés par l'ANSSI.

4. Difficultés liées à la prise en compte de la sécurité

D'après vous ?

Plus de sécurité, c'est mieux ?

4. Difficultés liées à la prise en compte de la sécurité

d. Le délicat équilibre entre productivité et sécurité : contexte

- Authentification requise pour chaque application dans l'entreprise
  - Problème pour l'utilisateur : « J'ai besoin de travailler chaque jour avec 5 applications et je dois à chaque fois y saisir un mot de passe différent ».
  - Réaction pour l'utilisateur : « Je note certains mots de passe sur papier ».
- Utiliser une application de chiffrement pour partager les fichiers chiffrés avec des partenaires
  - Problème pour l'utilisateur : l'interface de Crypt&Share n'est pas ergonomique.
  - Réaction de l'utilisateur : « Je vais utiliser DropBox pour partager les informations avec mes partenaires ».
- Les informations classifiées au niveau 4 (niveau de sensibilité le plus élevé) ne doivent pas sortir du S.I.
  - Problème pour l'utilisateur : J'ai besoin de l'avis d'un prestataire extérieur sur certaines informations de niveau 4.
  - Réaction de l'utilisateur : Déclassification des informations de manière à ne jamais avoir de niveau 4 mais uniquement des niveaux 3 ou 2.

4. Difficultés liées à la prise en compte de la sécurité

d. Le délicat équilibre entre productivité et sécurité

- Les usages fondent les pratiques… entre ce qui est acceptable par l'utilisateur, ce qui est nécessaire au bon fonctionnement de l'organisme et ses besoins de sécurité.

D'où l'importance :

- De la pédagogie : expliquer à quoi servent les procédures, leur bien fondé, leur intérêt pour l'organisation.
- De l'implication des dirigeants : qui viendront renforcer ces convictions.
- De la prise en compte des remarques et éventuelles oppositions des utilisateurs : ergonomie, pratique, simplicité de mise en œuvre, etc.
- La mise en place d'une charte informatique signée et connue de tous.
- De régulièrement rappeler les règles : changer les mots de passe, rejouer les procédures, créer une check-list, etc.
- De sensibiliser en évoquant les incidents réels qui se produisent et peuvent se produire dans l'organisation.

4. Difficultés liées à la prise en compte de la sécurité

d. Le délicat équilibre entre productivité et sécurité

- **Écouter les utilisateurs** et prendre en compte leurs besoins lors de l'étude de solutions de sécurité :
  - Proposer des mesures en concertation et avec l'adhésion des utilisateurs concernés autant que possible.
  - **Former les utilisateurs** pour les aider à prendre en main les nouveaux outils et à bien appliquer les mesures.

- **Tester les procédures**, dans le but d'évaluer leur efficacité (applicabilité, réalisation des objectifs, risques encourues) :
  - Éviter de multiplier les moyens de protection si ceux-ci ne sont pas respectés.
  - il faut parfois investir moins dans la sécurité mais avoir des procédures efficaces.

- **Confier la responsabilité de la sécurité à un collaborateur** qui a le pouvoir ou les ressources pour la faire appliquer.

- Choisir les solutions les plus adaptées à **sa propre structure**, à **son** fonctionnement, au niveau de maturité l'entreprise.

4. Difficultés liées à la prise en compte de la sécurité

e. Suivre l'évolution des technologies : le Cloud

- Les technologies Cloud se popularisent de plus en plus au sein des entreprises. Les raisons évoquées sont diverses et peuvent être :
  - Réduction des coûts
  - Meilleure accessibilité
  - Gestion confiée à un tiers
- Mais les mesures de sécurité et réglementaires constituent toutefois des « freins ».
- Le **SaaS** (**S**oftware **a**s **a** **S**ervice) est l'usage du Cloud le plus rencontré en entreprise :
  - SaaS est la fourniture d'applications sous forme de service à la carte. L'application est installée dans le Cloud (Datacenter) et l'utilisateur paye une licence d'utilisation.
- Les utilisateurs finaux souscrivent aujourd'hui à des services SaaS sans l'aval de la direction informatique et en dépit des règles de sécurité. Ils accèdent au SaaS à travers divers terminaux souvent non contrôlés par l'entreprise. On parle alors de « **Shadow IT** » :
  - Dans une entreprise du CAC, le DSI estimait à près de 100 le nombre total d'applications. Un audit de découverte du Cloud à révélé près de 2500 usages SaaS.

4. Difficultés liées à la prise en compte de la sécurité

e. Suivre l'évolution des technologies : le Cloud

Le recours à des services type Cloud pose de nouvelles problématiques que l'entreprise se doit de résoudre, notamment :

- Le choix d'un fournisseur
  - Est-ce que le fournisseur dispose de certifications relatives à l'hébergement (Exemple : SAS 70 II) ?
  - Est-ce que le fournisseur est agréé par une autorité nationale ?
- Le stockage
  - A qui appartiennent **légalement** les données lorsqu'elles sont hébergées ?
  - Quelles sont les mesures de protection des données stockées ?
  - Les systèmes sont-ils mutualisés avec d'autres clients ou nous sont-ils dédiés ?
  - Qui doit fournir les clés cryptographiques ?
  - Comment les données sont-elles sauvegardées, redondées ?
- Le transport des données
  - Qui fournit l'infrastructure de transport ?
  - Quels sont les mécanismes de sécurité en place ?
- Fin de contrat : réversibilité
  - Que deviennent les données lorsque le contrat expire ? Comment sont-elles restituées au client, supprimées du Cloud et qu'advient-il des données sauvegardées sur bande ?

4. Difficultés liées à la prise en compte de la sécurité

e. Suivre l'évolution des technologies : le Cloud

- Les guides suivants peuvent être utiles pour choisir un fournisseur SAAS :
  - Guide Contractuel SAAS : https://syntec-numerique.fr/conseil-juridique-numerique/guide-juridique/guide-contractuel-relatif-software-service-saas
  - Recommandations CNIL pour la souscription au SAAS : https://www.cnil.fr/fr/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services
  - Guide de l'ANSSI : « Sécurité de l'externalisation » : https://www.ssi.gouv.fr/entreprise/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/
- Les Cloud Access Security Brokers (CASB) ou les Cloud Security Gateway (CSG) sont des composants logiciels ou matériels qui se situent entre les utilisateurs et le fournisseur SaaS et permettent :
  - de protéger les données des utilisateurs de l'entreprise de manière à ce que l'éditeur SaaS ne puisse les lire ;
  - de gérer les accès et de l'authentification unique (SSO) ;
  - de conserver les données en local via de la tokenisation ou de les chiffrer avant de les envoyer vers le fournisseurs SaaS…
- Les services dans le Cloud tournent généralement en **conteneurs** (similaire à une VM) : gestionnaires de conteneurs à la mode : Docker, Kubernetes

4. Difficultés liées à la prise en compte de la sécurité

e. Suivre l'évolution des technologies : le Cloud

- Le Cloud pourrait à terme rendre les autres moyens de sauvegarde désuets :
  - sauvegarder une copie de son S.I. au sein du Cloud permettra à l'organisation de redémarrer une activité saine à tout moment en cas d'incident ;
  - à partir d'une sauvegarde, un espace de travail peut être accessible de n'importe quel endroit du monde pour tous ceux qui y sont autorisés.
- La fédération d'identité est un usage du Cloud qui peut permettre aux entreprises de mieux gérer les identités de ses utilisateurs et de :
  - centraliser les comptes utilisateurs ;
  - d'octroyer et de retirer facilement les droits d'accès sur plusieurs applications en interne ou en externe ;
  - tracer les utilisateurs et leurs actions…

4. Difficultés liées à la prise en compte de la sécurité

e. Suivre l'évolution des technologies : le Big Data

- « Big Data » recouvre l'exploitation des données massives impossibles à manipuler avec les outils classiques comme les bases de données.
  - Le « Big Data » comme outil de sécurité :
    - Modélisation des comportements et détection des anomalies sur la base de corrélation des données issues du trafic réseau.
    - Détection possible des attaques persistantes avancées (APT).
    - Meilleure efficacité des outils tels que des SIEM (supervision), IDS, ou IPS.
    - Surveillance du trafic réseau pour identifier des botnets.
  - Le « Big Data » représente un enjeu pour la sécurité des S.I. :
    - La source de données doit être fiable, et intègre (comme dans toute collecte d'information).
    - L'anonymisation des données manipulées représente une véritable difficulté compte tenu de leur volume important.
    - La localisation des données car le « big data » est souvent exploité dans le « cloud » et les réglementations applicables.
    - La protection de données exploitées est importante et le chiffrement peut être difficile à assurer. Un vol de données aura une ampleur beaucoup plus importante.
  - Technologie big data à la mode : Elasticsearch (en local ou dans le cloud)

4. Difficultés liées à la prise en compte de la sécurité

f. Des frontières floues entre sphères professionnelle, publique, et privée

Quel est le périmètre de confiance?

- Internet est un réseau mondial ouvert ; dans un monde concurrentiel, il est naturel qu'il soit source de menaces.
- Les réseaux d'entreprises sont des réseaux internes, généralement protégés de façon périmétrique, mais peu protégés en interne…
- Les multinationales possèdent souvent de grands réseaux ouverts à des exploitants, des services de télémaintenance et des sous-traitants qui ont des d'accès conséquents sur ces réseaux, et qui possèdent eux-mêmes leurs propres informations.
- De plus, de nombreux « nouveaux » appareils sont utilisés (smartphones, tablettes etc.) faiblement sécurisés et connectés directement à Internet (Wifi, 3G/4G, etc.) sans passer par les dispositifs de sécurité de l'entreprise.
- Les données personnelles peuvent ainsi être présentes sur le réseau d'entreprise.

4. Difficultés liées à la prise en compte de la sécurité

f. Des frontières floues entre sphères professionnelle, publique, et privée

BYOD - Focus sur le smartphone personnel (ou la tablette personnelle) :

- Il nous accompagne au travail, lors de nos déplacements.
- On le connecte à notre PC de bureau pour le recharger en USB.
- Il remplace souvent notre téléphone professionnel, peut-être moins performant ou restreint en terme de fonctionnalités.
- Pour des raisons de facilité, on y configure notre messagerie professionnelle, nos contacts, notre emploi du temps… autant d'informations qui peuvent potentiellement être sensibles pour l'entreprise.

- La frontière entre nos informations privées et nos informations professionnelles devient donc **très floue.**

- Dès que les informations sont stockées sur un smartphone personnel, l'entreprise en perd la maîtrise (l'équipement ne lui appartient pas, elle ne peut pas imposer ses règles…).

4. Difficultés liées à la prise en compte de la sécurité

f. Des frontières floues entre sphères professionnelle, publique, et privée

Raconter, partager sa vie privée sur l'Internet c'est y être pour la postérité…

- Nos données nous échappent dès l'instant où nous les publions : Dans le meilleur des cas, on pourra effacer notre propre publication, mais on ne pourra pas effacer les multiples copies que l'on ne contrôle pas (droit à l'oubli illusoire par manque de maîtrise de l'information).
- C'est permettre à tout inconnu, d'entrer dans notre sphère privée ; la restriction des accès aux « amis » n'est qu'illusoire dans l'absolu.
- C'est permettre aux Ressources Humaines de filtrer notre CV ; et déterminer le profil privé du candidat correspondant au profil professionnel recherché.
- C'est permettre à nos collègues et supérieurs d'interpréter nos propos…

4. Difficultés liées à la prise en compte de la sécurité

f. Des frontières floues entre sphères professionnelle, publique, et privée

Partager les problèmes que l'on rencontre au travail : personnels, techniques, relationnels ; consulter des sites personnels au travail…

- c'est peut-être mettre en danger son organisation : en offrant à un pirate ou un concurrent des informations précieuses (version d'un logiciel, faille de sécurité, fournisseurs, secrets commerciaux, informations RH…).
- transgresser la déontologie du travail, ou la charte de confidentialité.
- potentiellement s'exposer à des sanctions en interne qui peuvent aller jusqu'au pénal.

4. Difficultés liées à la prise en compte de la sécurité

Conclusion

- Évolution des modes, des besoins, des technologies, des habitudes.
- Au-delà des nouveautés, toujours le même problème : la non-prise en compte de la sécurité (développement, implémentation, exploitation, formation).
- Un périmètre d'attaque et d'accident plus étendu mais peu nouveau.
- Une prise en compte permanente des enjeux et de la sécurité par tous (hygiène informatique) et par le chef d'entreprise.
- Un accroissement des besoins de sécurité : besoin en compétences et en professionnels.

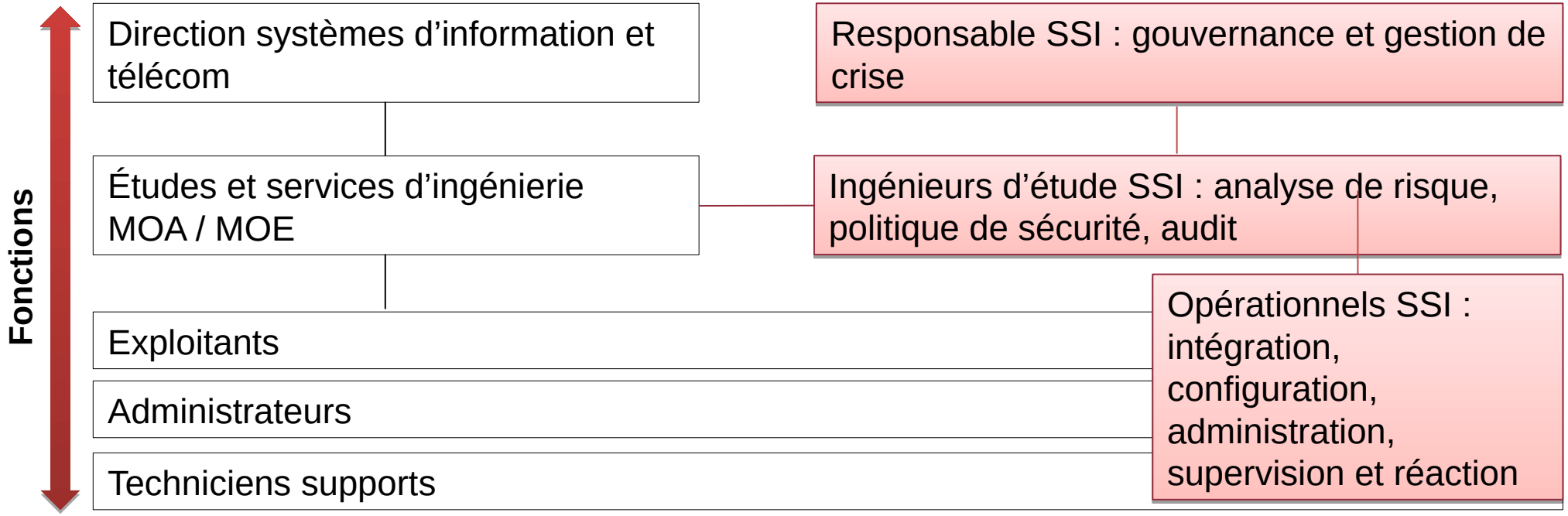
4. Les métiers en cybersécurité

a) Positionnement des métiers au sein des organisations
b) Cartographie des métiers et compétences
c) Profils et carrières
d) Perspectives d’embauche

4. Les métiers

a. Positionnement des métiers au sein des organisations

La cybersécurité est transverse à toute activité qui requiert de l'informatique et des réseaux de télécommunications, de la TPE à la multinationale, dans le domaine privé ou public.



4. Les métiers

a. Positionnement des métiers au sein des organisations

Selon la taille de l'organisation (PME/PMI/Grande entreprise…), les fonctions liées à la cybersécurité nécessitent une charge de travail qui varie. Il est possible d'avoir du personnel à temps partiel ou du personnel dédié à la sécurité.
Et cela sur l'ensemble des couches depuis la gouvernance jusqu'à l'opérationnel : par exemple.

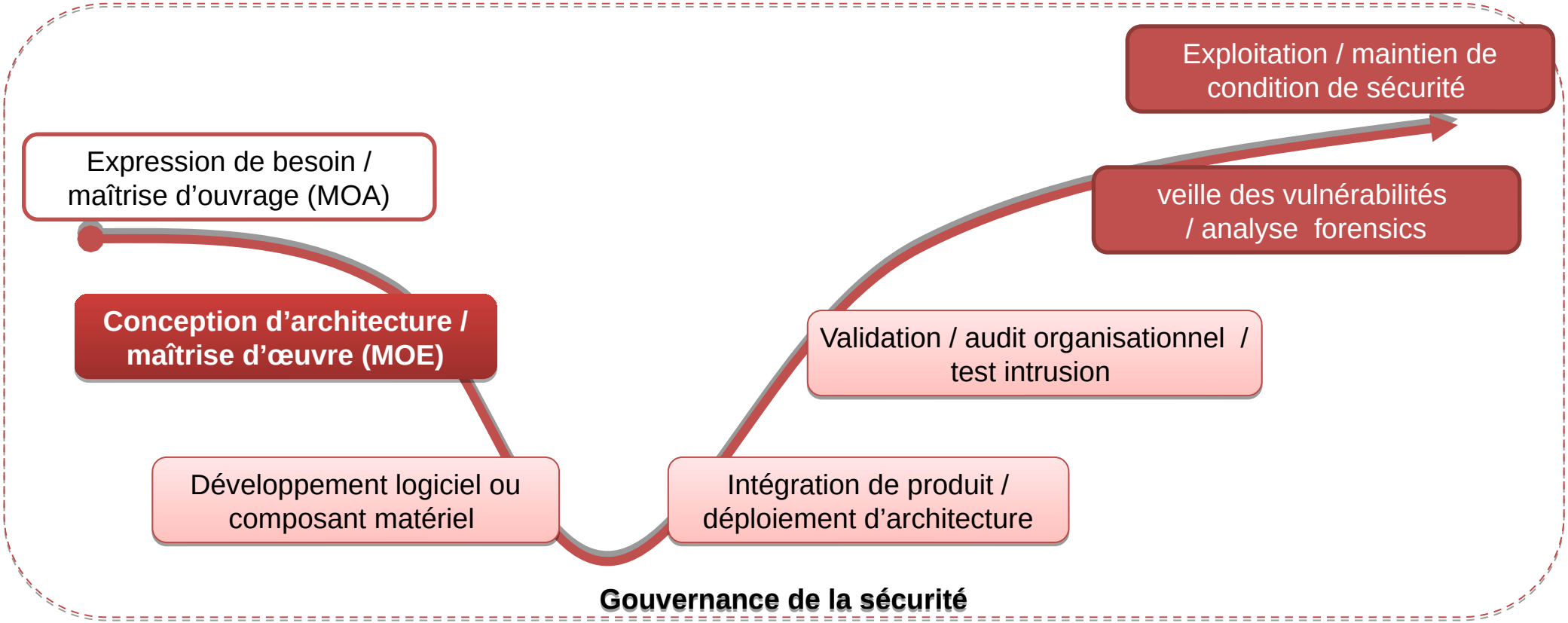
ETP = Équivalent Temps Plein
DSI = Direction des Systèmes d'Information
SSI = Sécurité des Systèmes d'Information
PSSI = Politique de Sécurité des Systèmes d'Information

	PME/PMI DSI 15 pers	Grande entreprise DSI 500 pers
Responsable SSI : gouvernance et gestion de crise	¼ ETP du Dir. du S.I.	3 à 5 ETP
Ingénieurs d'étude SSI : analyse de risque, mise en œuvre PSSI, audit…	¼ ETP des études S.I.	5 à 10 ETP
Opérationnels SSI : intégration, configuration, administration, supervision et réaction	1 ETP réparti sur l'exploitation du S.I.	20 à 50 ETP si H24 7/7

4. Les métiers

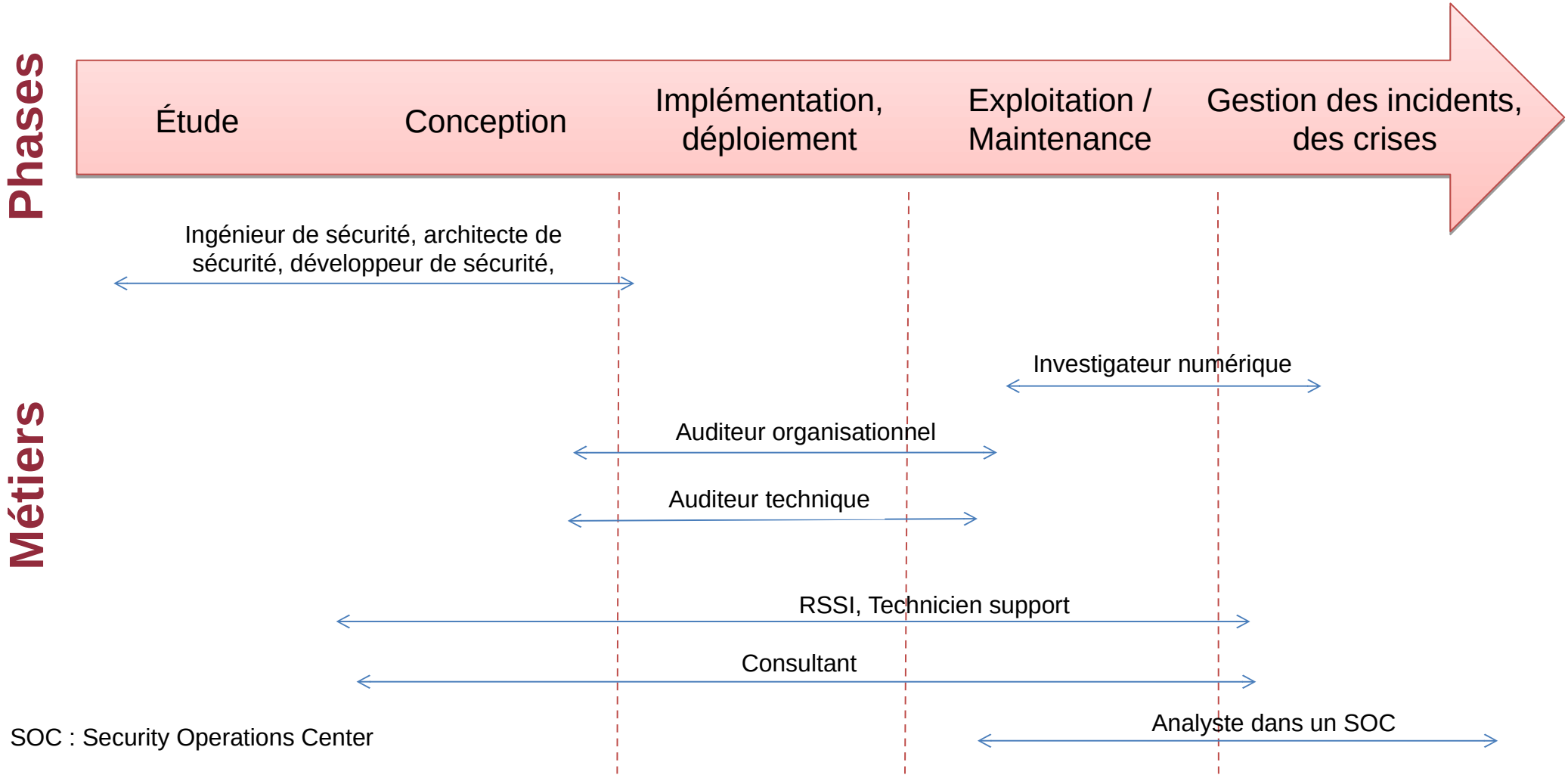
b. Cartographie des métiers et compétences en SSI

Les métiers se répartissent dans le cycle de vie d'un projet depuis l'expression de besoin jusqu'au retrait de l'exploitation sous la responsabilité de la gouvernance globale de l'organisation.



4. Les métiers

b. Cartographie des métiers et compétences en SSI



SOC : Security Operations Center

4. Les métiers

b. Cartographie des métiers et compétences en SSI

Les métiers se répartissent dans les familles de l'informatique et des réseaux.

	Nb année expérience	Compétence technique	Compétence management
Gouvernance des systèmes d'information			
•Responsable ou Directeur	15 à 20	X	XXX
•Chef de projet / Consultant MOA	5 à 15	XX	XX
Conception et déploiement de système d'information			
•Chef de projet / Consultant MOE	5 à 15	XX	XX
•Architecte système	10 à 15	XXX	
Développement logiciel et matériel			
•Architecte/concepteur logiciel/composant	5 à 10	XXX	
•Développeur logiciel (dont cryptologue)	0 à 10	XXX	
Exploitation			
•Technicien système et réseau	0 à 10	XXX	
•Administrateur système et réseau	0 à 10	XXX	X
•Analyste veille/gestion des incidents/forensics	0 à 10	XXX	X
Validation / Audit			
•Auditeur technique SSI (dont test intrusion)	0 à 10	XXX	X
•Auditeur organisationnel SSI	5 à 10	X	X

Compétence requise :
X : peu de compétence
XX : niveau moyen
XXX : forte compétence

4. Les métiers

c. Profils et carrières

- **Responsable de la Sécurité des Systèmes d'Information** (RSSI) : définit la politique de sécurité du SI et veille à son application ; il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.

- **Architecte [système, logiciel] sécurité** : structure les choix techniques, technologiques et méthodologiques d'un ensemble [système, logiciel] répondant à des exigences de sécurité.

- **Développeur [produit, logiciel] de sécurité** : le développeur de sécurité assure le sous-ensemble des activités d'ingénierie nécessaires à la réalisation d'éléments [produit, logiciels] répondant à des exigences de sécurité.

4. Les métiers

c. Profils et carrières

- **Technicien ou Administrateur système et réseau :** assure ou est responsable de diverses activités de support, de gestion ou d'administration de la sécurité aux plans techniques ou organisationnel.

- **Analyste :** assure la veille sur les vulnérabilités des produits et logiciel, recherche et détecte les incidents de sécurité coordonne le suivi de l'application des correctifs.

- **Auditeur Organisationnel :** contrôle la prise en compte de la sécurité au niveau organisationnel sur la gouvernance, les procédures de sécurité notamment vis-à-vis de la nome ISO27K. Il vérifie la conformité des mesures mises en œuvre.

- **Auditeur Technique** : contrôle les configurations des équipements et logiciels. Il est en mesure de pénétrer les défenses d'un système d'information et d'identifier les divers chemins d'intrusions possibles et leurs conséquences. Il vérifie l'efficacité des mesures en place pour protéger le système.

4. Les métiers

c. Profils et carrières

La majeure partie des postes SSI sont occupés actuellement par des personnes ayant une formation informatique ou télécom, s'étant spécialisées au cours de leur carrière par des formations / certifications.
Certaines certifications en SSI peuvent être effectuées en 5 jours et se terminer par un examen comme par exemple :

- ISO 27001 Lead Auditor
- ISO 27001 Lead Implementor
- ISO 27005 Risk Manager

Compétence Technique : X
Compétence Management : XXX

- CISSP : Certified Information System Security Professional

Compétence Technique : XX
Compétence Management : XXX

- CEH : Certified Ethical Hacker

Compétence Technique : XXX
Compétence Management : X

On note depuis une dizaine d'années, un accroissement des formations spécialisées en sécurité de niveau bac+4/5. Elles permettent généralement de démarrer une carrière sur des postes qui requièrent des compétences techniques.

Possibilité de progression de carrière depuis la production technique jusqu'à de la direction/management en passant par de la vente ou du marketing de produits/services.

4. Les métiers

d. Perspectives d'embauche

- Métiers avec une forte demande annoncée pour les 15 prochaines années :
  - **virtualisation des SI et intégration Cloud**,
  - révolution digitale des services aux usagers (B2C) et entre entreprise (B2B),
  - Internet des objets…
- Dans tous les secteurs privés banque, industrie, commerce…

- Ainsi que dans le secteur public : administration, collectivité territoriale, hôpitaux, universités…

- Mais surtout au sein de sociétés de service, principaux employeurs de diplômés depuis 20 ans pour intervenir en sous-traitance ou assistance technique pour les entreprises et les administrations :
  - les organisations tendent à se concentrer sur leur métier et faire de la délégation de service pour les fonctions supports dont la sécurité.

4. Les métiers

d. Perspectives d'embauche

- Exemples d'organisations spécialisées dans la cybersécurité et qui recrutent :
  - Éditeurs/Constructeurs de produit de sécurité (anti-virus, boîtier de chiffrement, pare-feu, ICG…) : développement, marketing et vente.
  - Tiers de confiance qui exploite des infrastructures pour des clients (produits/services de sécurité en mode IaaS, SaaS) : conception et déploiement, exploitation, marketing et vente.
  - Sociétés de service/cabinet de conseil : conseil, expertise, audit…
  - Organismes étatiques comme l'ANSSI, ministère de la défense (DGSE, Armées), ministère de l'intérieur (DGSI, police judiciaire, gendarmerie nationale), la CNIL : conseil, expertise, audit…
  - Entreprises proposant ou gérant des SOC.

4. Les métiers

d. Perspectives d'embauche

- Exemples de stages des années dernières :
  - Création d'une base de données pour la supervision (en python) + sécurisation d'un Active Directory (Limon-IT et Casino)
  - Création de superviseur de robots sécurisé (3Laws Robotics Inc., start-up)
  - Création d'une API HTTP bas niveau (en C) (Crédit Mutuel)
  - Sécurisation d'une solution de conteneurisation (configuration de scripts YAML) (Kubernetes) (Excellium / Thalès)
  - Supervision forensique (Elastic Stack) et déploiement automatique d'une base de données distribuée Elasticsearch (TRACIP)
  - Gestion d'incidents de sécurité + scanneur de vulnérabilités Web (réponse à des tickets, reproduction de bugs et vulnérabilités) (UBIKA)

4. Les métiers

d. Perspectives d'embauche

- Exemples de stages des années dernières :
  - Sensibilisation, création de CTF (Naval Group)
  - Mise en place de la supervision (Wazuh) sur le SI d'une entreprise d'IT (Arŋs)
  - Portage sécurisé d'un SI en Java vers du Java compilé (Banque Postale)
  - Tests de pénétration (Orange Cyberdéfense)
  - Gestion des contrôles d'accès (Excellium Thalès)
  - Analyse de risque et de conformité (Banque de Luxembourg)
  - Sécurisation de SI sur cluster Kubernetes (Orange)
  - Mise en conformité ISO 27000 + audit technique (Atoz)
  - Sécurisation de l'application d'un exploitant de vin (Trydea)
  - Mise en place d'une plateforme d'informations sur les cybermenaces (Loria)
  - Détection de malwares (Loria)

4. Les métiers

d. Perspectives d'embauche

- Exemples de stages des années dernières :
  - Audit organisationnel et audit technique (Inetum)
  - Déploiement d'antivirus sur un parc de serveurs (DXC)
  - Création d'un site Web (CORYS)
  - Méthodes formelles pour vérifier la sécurisation d'une méthode P2P (Loria)
  - Gestion de contrôles d'accès (HeadMind)
  - Évitement d'antivirus (Excellium Thalès)
  - Plateforme d'audit automatisé (CNS)
  - Mise en conformité (EBRC)

4. Les métiers

d. Perspectives d'embauche

- Exemples de stages des années dernières :
  - Recherche sur des réseaux sécurisés temps-réel (Loria)
  - Monitoring par Breach-and-Attack (simulation d'attaques) (Euro-Information)
  - Firewall d'un hôpital (CHU de Fès)
  - Monitoring et réponse automatique à incidents (Excellium Thalès)
  - Simulation d'attaque d'hôpital (Thalès Bruxelles)
  - SIEM ELK (ElasticSearch, Logstash, Kibana/Kubernetes) (UBCOM)
  - Traçabilité des données spatiales (FACTiven)
  - Cybersécurité d'OIVs (Eiffage – Clemessy)
  - Détection d'usurpation de DNS par IA (ANSSI)
  - Recherche et dev sur Kubernetes + pentest (Orange Cyberdéfense)
  - Sécurité d'un mainframe zOS (Euro-Information)
  - Sécurité d'un S.I. de l'armée de l'air (ESIOC)
  - Détection d'intrusion réseau (ANSSI)
  - DevSecOps avec ZAP et SonarQube / Monitoring (Exotec)

4. Les métiers

d. Perspectives d'embauche

- Exemples de stages de l'année dernière :
  - Hardening des OS dans les systèmes de brouillage (Thalès Cholet)
  - Déploiement d'une infra de test (Creos Luxembourg)
  - Licences, supervision (Venatech)
  - Pentest très basique (Advens)
  - Modernisation du SI (Agglomération de St-Dizier)
  - Modernisation du SI (Direction Générale des Vosges)
  - Modernisation du SI (Conseil départemental des Vosges)
  - Mise en place d'un SOAR (SOC semi-automatisé) (Soteria Lab)
  - Clone de l'infra pour test (Banque Internationale du Luxembourg)
  - Firewalls next-generation (Thalès Luxembourg)
  - Pentest avancé (PwC Luxembourg)
  - Sécurité d'infra industrielle (Eqiom)

4. Les métiers

d. Perspectives d'embauche

- Bilan :
  - Entreprises de 4 personnes à plusieurs milliers
  - Programmation de bas niveau (C), haut niveau (Python), hors-programmation (configuration de scripts YAML et alimentation de données XML)
  - 1/2 stage sur Windows (en particulier avec des Active Directories)
  - La cybersécurité n'est pas toujours le cœur du stage
  - Pas mal de bases de données (SQL, PostgreSQL, Elasticsearch et autres)
  - Beaucoup d'environnements virtuels (VM et conteneurs : Docker, Kubernetes)
  - Parfois en cloud, parfois en local
  - Différentes solutions de visualisation des données (majoritairement Grafana)
  - Protocoles : HTTP, SSH, TLS, GIT, UDP, TCP
  - 1/4 à mis en place des certificats de clef publique
  - Outils de scan courants : OWASP ZAP, Qualys, Metasploit, Burp Suite
  - Beaucoup de travail sur des serveurs, mais aussi des firewalls et proxies

4. Les métiers

d. Perspectives d'embauche

- Attention :
  - Certains offrent d'excellents stages sans opportunité d'embauche derrière (services publics, Thalès) mais ça ouvre des portes
  - Paradoxalement c'est difficile de trouver un stage (et même un premier emploi) : les boîtes cherchent toutes avec 3-4 ans d'expérience
    - (elles refusent de faire leur part dans la formation des jeunes et veulent des gens déjà 100 % opérationnels)
    - Il faut insister
    - N'hésitez pas à trouver un job moins intéressant au début (essayez de trouver quelque chose de formateur) et à changer au bout de 2-3 ans !
  - Il y a des offres sur Nancy, mais pas assez pour toute la promo (beaucoup veulent rester je le sais) ! Désolé, il faudra peut-être bouger.

Références liées au chapitre

https://cyber.gouv.fr/publications/devsecops
https://cyber.gouv.fr/publications/virtualisation
https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation
https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions

Pour aller plus loin…

Système, Supervision et Monitoring, Emmanuel Nataf

Gestion de projet, Marie-Laure Alves

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

DEVSECOPS

Le **DevSecOps** est une méthodologie qui vise à inclure les pratiques de sécurité dans le processus de développement et de mise en production d'applications. Les bonnes pratiques de sécurité suivantes sont à considérer.

→ **Réaliser et maintenir à jour une cartographie des applications utilisées** : les droits système, les secrets d'installation et de fonctionnement, les matrices de flux, les rôles des développeurs (relecture, validation, droits sur les environnements, etc.), les référents ayant la connaissance globale (technique et métier).

→ **Faire une analyse de risque globale** en prenant en compte les chemins de compromission des postes des développeurs, de la sous-traitance, de la chaîne CI/CD* (*Continuous Integration/Continuous Deployment*) et des technologies utilisées (ex. : *cloud*).

→ **Considérer que les actions réalisées par la CI/CD de production sont des actions d'administration.** Il est recommandé de dédier un poste d'administration pour la CI/CD de production, d'appliquer le principe de moindre privilège, de générer à la demande les jetons (*tokens*), et de journaliser et superviser la CI/CD.

→ **Gérer les secrets de manière sécurisée.** Il est recommandé d'utiliser un gestionnaire de secrets distinct par environnement (ex. : hors production, production). Il convient également de s'assurer de l'absence de secrets en dur dans le code source, dans les journaux d'événements des tâches (*jobs*), ou dans les dépôts de code.

→ **Gérer les dépendances avec rigueur** : les minimiser, les évaluer et appliquer les correctifs de sécurité avant déploiement.

→ **Prévoir des tests de sécurité automatisés dans la CI/CD** : tests de non-régression (pour éviter de nouvelles vulnérabilités), étanchéité entre profils d'utilisateurs, tests d'analyses statique et dynamique, tests de conformité de l'IaC (*Infrastructure as Code*).

→ **Sécuriser le déploiement en production des applications** en maintenant l'intégrité du code source de bout en bout, en signant et vérifiant les signatures des tags de version des artefacts.

→ **Implémenter une authentification multifacteur** pour l'accès aux dépôts et pour la signature des *commits*.

→ **Séparer les infrastructures CI/CD de développement et de production** et **ne pas les exposer directement sur Internet.**

→ **Réinstancier régulièrement l'infrastructure CI/CD** et ne pas y stocker de données persistantes.

→ **Être vigilants sur les besoins en confidentialité** vis-à-vis de l'infrastructure de CI/CD (ex. : localisation, tests du code source en SaaS public).

→ **Imposer des règles de développements sécurisés** dans les équipes.

→ **Appliquer des règles de durcissement sur les OS** hébergeant les applications (cf. https://cyber.gouv.fr/guide-linux).

(*) La chaîne CI/CD comprend plusieurs outils, par exemple : orchestrateur, dépôts de code source, tests automatisés, gestionnaire de secrets, outils de déploiements, artefacts.

V1.0 (02/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

VIRTUALISATION

La virtualisation est une technologie socle sur laquelle reposent de nombreux SI. **Les infrastructures de virtualisation** (c.-à-d. l'ensemble des logiciels et matériels nécessaires à la fourniture du service de virtualisation) **sont une cible de choix pour les attaquants** afin d'avoir accès plus rapidement et de manière généralisée aux données et applications qu'elles hébergent. Certaines bonnes pratiques permettent de réduire les risques ou les conséquences d'une compromission d'un SI virtualisé.

→ **Former régulièrement les administrateurs** sur les technologies utilisées dans les infrastructures de virtualisation.

→ **Considérer les infrastructures de virtualisation comme critiques pour le SI.** Elles doivent bénéficier des mesures de protection adéquates et être administrées depuis un SI d'administration à l'état de l'art.

→ **Regrouper les nœuds de calcul et le stockage associé par niveau homogène de sensibilité et d'exposition** des applications et/ou des données hébergées.

→ **Mettre en place de la segmentation réseau physique** entre les *zones de confiance** de sensibilité ou d'exposition différentes et **mettre en place de la micro-segmentation réseau** au sein de ces zones.

→ **Maintenir à jour les infrastructures de virtualisation.** Les mises à jour de sécurité doivent impérativement être appliquées en priorité, d'autant plus en cas d'exposition à Internet.

→ **Dédier une interface réseau à l'administration sur les hyperviseurs.** Cette interface doit être connectée à un réseau d'administration à l'état de l'art. Elle ne doit surtout pas être accessible depuis un réseau de production ou Internet.

→ **Prendre en compte l'ensemble du matériel en lien avec l'infrastructure de virtualisation** dans la stratégie d'administration : cartes de management (ex. : HP iLO, Dell iDRAC), baies de stockage, équipements réseau, équipements de sécurité, etc.

→ **Dédier des comptes d'administration** sur l'infrastructure de virtualisation et appliquer le principe de moindre privilège pour les administrateurs.

→ **Rendre les comptes d'administration de l'infrastructure de virtualisation indépendants** des annuaires (ex: Active Directory) utilisés en production ou sur le SI bureautique. Les chemins de contrôle de ces annuaires doivent être vérifiés régulièrement, de manière à ce qu'ils ne permettent pas d'élévation de privilège depuis les annuaires de production vers l'infrastructure de virtualisation et inversement.

→ **Sauvegarder les éléments nécessaires à la reconstruction des infrastructures de virtualisation** (ex. : configurations, binaires d'installation) de manière indépendante de la sauvegarde des machines virtuelles hébergées.

→ **Vérifier régulièrement les configurations** de l'infrastructure de virtualisation, en particulier sur les points cités dans ce document.

→ **Journaliser, centraliser et superviser les évènements de sécurité** liés à l'infrastructure de virtualisation (ex. : accès, changement de configurations).

(*) cf. https://cyber.gouv.fr/guide-admin-si

V1.0 (02/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr