Analyses de risques

CLUSIR InfoNord RSSI du 24 janvier 2012

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

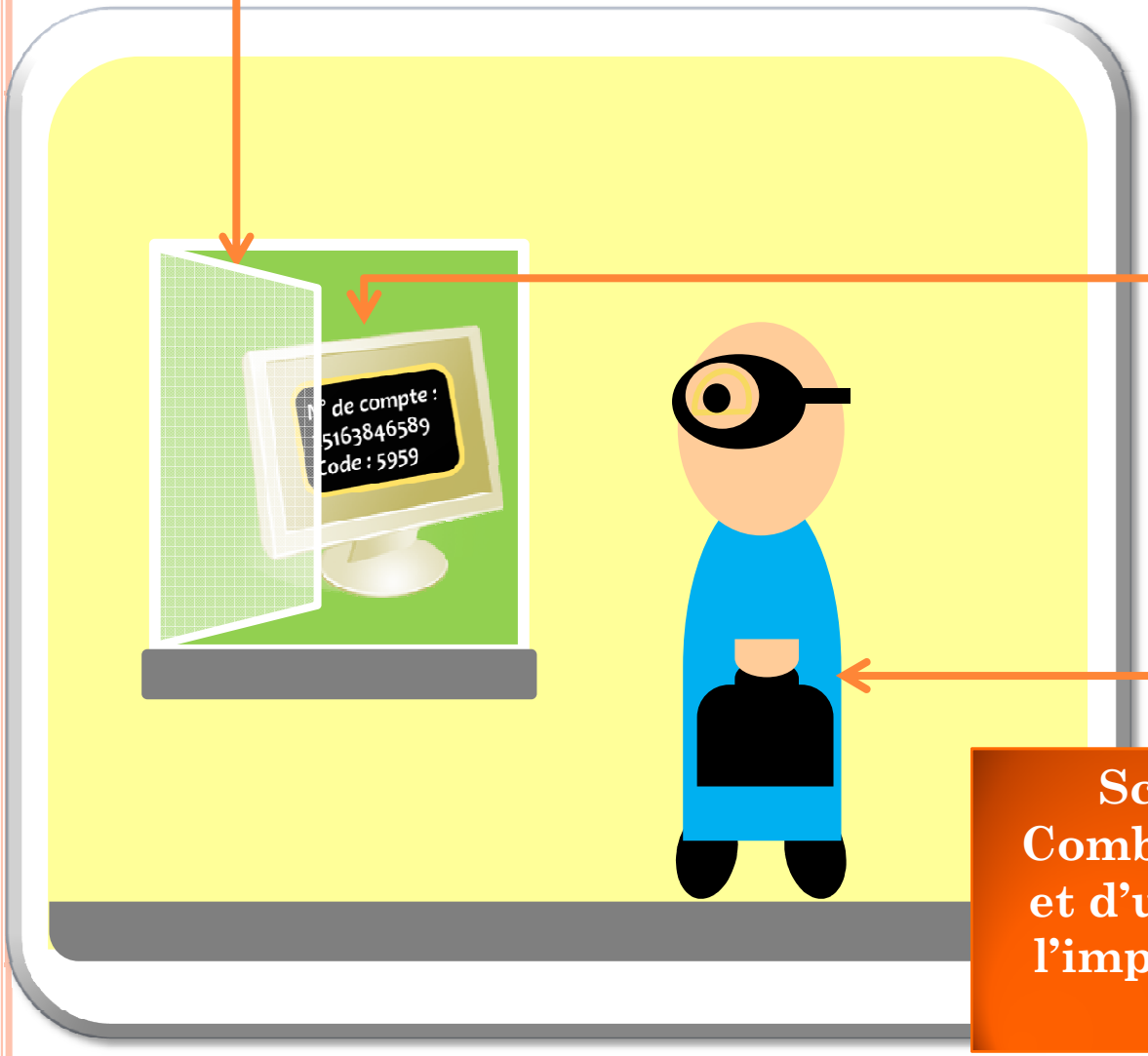
INTRODUCTION

- Objectifs :
  - A partir des principales normes et méthodologies actuelles, en présenter les principaux concepts puis apporter des retours d'expérience
  - Ceci afin de donner les clés permettant de réaliser des analyses de risque pertinentes et efficaces

- Limites :
  - La présentation se limitera à l'analyse de risque SI uniquement

Concepts et vocabulaire

Du risque au « scénario de risque »



Fenêtre ouverte = Vulnérabilité

Risque = Vol de matériel ou d'informations

Passant = Menace

Scénario de Risque = Combinaison d'une menace et d'une vulnérabilité dont l'impact sur l'activité n'est pas anodin.

CONCEPTS ET VOCABULAIRE

LA TERMINOLOGIE COURANTE (1/2)

- Menaces
  - Ce sont les choses ou les personnes à l'origine des risques. On peut distinguer plusieurs types de menaces (humaines, techniques, environnementales notamment)
- Vulnérabilité
  - Il s'agit d'une lacune dans les dispositifs et mesures de sécurité en place qui permettent ou facilitent la concrétisation du risque
- Actif/activité essentiel(le) (aussi appelé bien essentiel dans certaines méthodologies)
  - Ce sont les composants ou les activités sur lesquels on va « appliquer » l'analyse de risques
- Actif support (aussi appelé bien support dans certaines méthodologies)
  - Ce sont les composants d'un système d'information sur lesquels reposent les biens essentiels et/ou les mesures de sécurité. On trouvera généralement les biens relatifs aux systèmes d'informations et de téléphonie, ceux relatifs à l'organisation et ceux relatifs aux locaux.

CONCEPTS ET VOCABULAIRE

LA TERMINOLOGIE COURANTE (2/2)

- Probabilité d'occurrence (parfois appelé potentialité)
  - Probabilité que la menace se concrétise « dans l'absolu », sans tenir compte des vulnérabilités.
- Impact
  - Ce sont les conséquences d'une réalisation d'un scénario de risque sur l'activité métier. Il existe des impacts directs (financiers, image, par exemple) et des impacts indirects (désorganisation , réglementaire ou juridique). La mesure des impacts est primordiale dans le sens où c'est elle qui va déterminer le niveau du risque.
- Risque
  - Probabilité qu'une menace puisse exploiter une vulnérabilité d'un actif ou d'un groupe d'actifs et cause un impact non négligeable sur l'organisation ou ses activités (ISO 27005).

Concepts et vocabulaire

Traitement du risque

- Evitement
  - Arrêt de l'activité (ou du projet)
- Réduction
  - Implémentation de mesures de sécurité
- Transfert
  - Assurance
- Acceptation
  - Le métier décide de ne rien faire

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

Méthodologies et normes

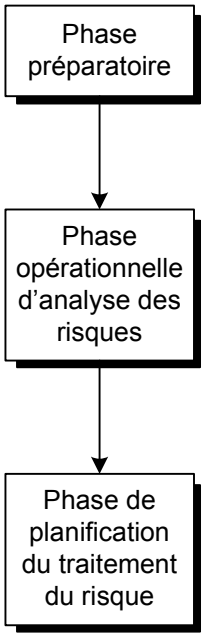
- Plus de 200 méthodologies existantes
  - Globales
  - Sectorielles
- En France, les plus connues sont
  - EBIOS, produite par l'ANSSI
    - Outil EBIOS
  - MEHARI, produite par le CLUSIF
    - 11 langues
    - 25.000 téléchargements de la base de connaissance
    - Outil RISICARE
  - IRAM, produite par l'ISF
    - Réservée aux membres de l'ISF
    - Plutôt pour des entreprises de grande ampleur internationale (méthodologie en anglais)

MÉTHODOLOGIES ET NORMES

MEHARI – CLUSIF

Méthodologie

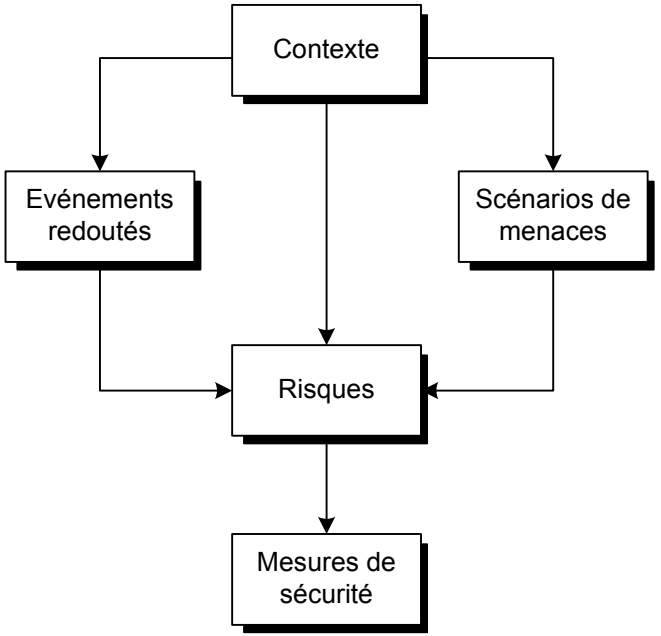
- Phase préparatoire
  - Prise en compte du contexte
  - Définition des métriques
  - Identification des activités essentielles
  - Identification des actifs support (potentialité et impact intrinsèques)
- Phase opérationnelle
  - Analyse des vulnérabilités
  - Analyse des menaces
  - Identification de la potentialité et de l'impact
  - Identification de la gravité
  - Confrontation de (la potentialité et de l'impact) avec la gravité
  - Décisions sur la gestion des risques
- Planification et traitement
  - Plan de traitement des risques et amélioration continue



MÉTHODOLOGIES ET NORMES

EBIOS – ANSSI

Méthodologie

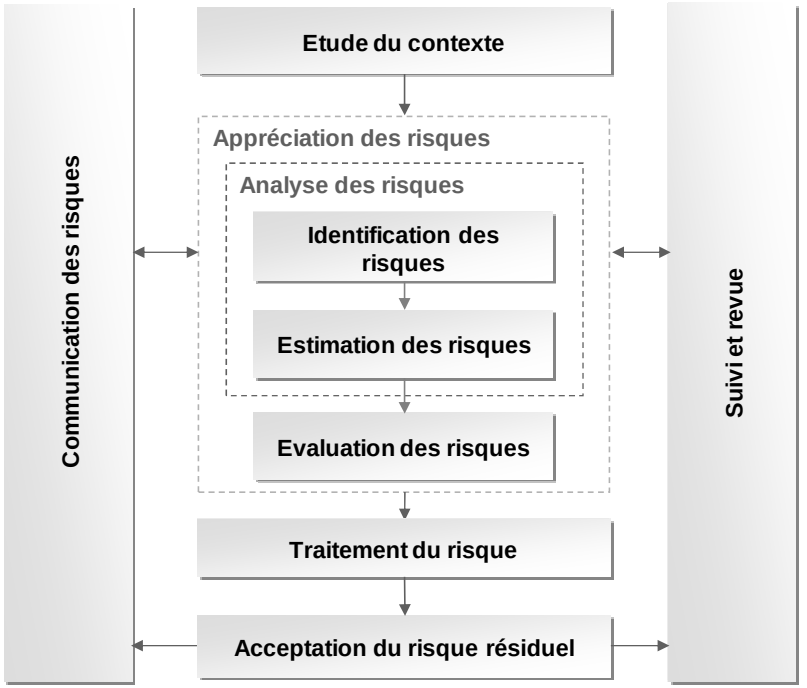


- Contexte
  - Prise en compte du contexte
  - Définition des métriques
  - Identification des activités essentielles
  - Identification des actifs support
- Evènements redoutés
  - Identification des impacts
- Scénarios de menace
  - Analyse des vulnérabilités
  - Analyse des menaces
  - Identification des probabilités d'occurrence
- Etude des risques
  - Confrontation des scénarios de menace (probabilité d'exploitation des vulnérabilités par les menaces) avec les évènements redoutés (impact)
  - Décisions sur la gestion des risques
- Etude des mesures de sécurité
  - Plan de traitement des risques et amélioration continue

Méthodologies et normes

Norme

ISO/IEC 27005 – International Standard Organisation



- Etude du contexte
  - Prise en compte du contexte
  - Définition des métriques
- Identification des risques
  - Identification des activités essentielles
  - Identification des actifs support
  - Analyse des menaces
  - Analyse des vulnérabilités
  - Identification des conséquences
- Estimation des risques
  - Confrontation des menaces avec les vulnérabilités et les conséquences possibles
  - Identification des probabilités d'occurrence
- Evaluation des risques (revue)
- Traitement du risque
- Amélioration continue

Méthodologies et normes
Synthèse

- Les méthodologies s'alignent sur la norme ISO/IEC 27005

- Les méthodologies sont semblables…
  - Implémentation des mêmes concepts
  - Propositions d'outils et de bases de connaissances
- Mais différentes
  - Vocabulaire
  - Organisation de la démarche

- L'ISO/IEC 27005 ne propose pas de méthode
  - Elle propose les règles pour concevoir une méthode
  - Par conséquent pas d'outils, mais des bases de connaissance issues d'EBIOS

Une alternative est de concevoir sa propre méthode, en s'alignant sur les concepts de l'ISO 27005. A défaut, EBIOS est assez proche.

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

Comment s'y prendre concrètement ?

Avant de se lancer

- Répondre à la question « A quoi vont me servir les résultats de l'analyse de risques » ?
  - A mettre en place un SMSI ou construire un schéma directeur sécurité ? (oui)
  - A identifier de nouvelles mesures de sécurité à mettre en place sur mon SI ? (non)
  - A identifier de nouvelles mesures de sécurité à mettre en place sur mon SI, en fonction des besoins métier ? (oui)
  - A identifier des éléments qui me serviront de levier pour déclencher un projet ou trouver du budget ? (oui)
  - A poursuivre mon projet en toute sérénité ? (oui)
- Suivant la réponse, on ne mènera pas le même type de démarche. Cependant, pour des raisons de cohérence, il sera intéressant de définir pour une même organisation une démarche simplifiée et une démarche complète.

COMMENT S'Y PRENDRE CONCRÈTEMENT ?

ATTENTION AUX DÉVIANCES !

Une analyse de risques, ça ne sert pas à…

- Faire beau pour dire d'en avoir fait une (risque de décrédibiliser l'ensemble de la démarche sécurité)
- Remplacer un audit
- Juger l'IT et évaluer son niveau de sécurité

Une analyse de risques, ça sert à…

- Définir un Schéma Directeur, initier un SMSI, de manière générale à appuyer une gestion de la sécurité basée sur les risques métiers
- Sensibiliser et communiquer sur les risques de l'organisation
- Obtenir des leviers « métier » pour dégager du budget, déclencher un projet

COMMENT S'Y PRENDRE CONCRÈTEMENT ?

L'ANALYSE DE RISQUES « GLOBALE »

Quand	Comment	Resp.	Impliqués
Approche globale (Schéma Directeur, SMSI, ..)	Définir : •Le périmètre (et ses limites) •Le niveau de granularité •Les échelles d'impact et de probabilité •Les bases de vulnérabilités et de menaces	RSSI	Direction (CODIR, ou équivalent) Métiers Managers

Lorsque c'est la toute première Analyse de Risques réalisée :

•Commencer sur un périmètre bien défini voire restreint avec une granularité très faible voire sans granularité

•Ce type d'analyse s'inscrit dans une démarche PDCA : l'analyse suivante pourra viser un périmètre plus large ou une granularité plus fine !

Comment s'y prendre concrètement ?

L'analyse de risques « Projet »

Quand	Comment	Resp.	Impliqués
En début de projet	Définir : •Le périmètre (limites techniques généralement) •Le niveau de granularité (modules fonctionnels) •Les échelles, adaptées au niveau d'impact du projet sur l'activité •Les bases de vulnérabilités et de menaces (un peu plus techniques)	Chef de projet, accompagné par un acteur sécurité	Métiers utilisateurs (besoins) Principaux acteurs IT du projet

Tout projet ne doit pas faire l'objet d'une Analyse de Risques complète. Il est préférable de réaliser d'abord une rapide « analyse de sensibilité », qui déterminera si le projet doit effectivement passer par une analyse de risques ou alors simplement par une analyse simplifiée et réalisée de manière autonome sans la sécurité (issu de l'AR globale qui a défini des mesures communes à toute l'organisation).

Comment s'y prendre concrètement ?

Au cas par cas

Quand	Comment	Resp.	Impliqués
Besoins ponctuels (benchmark, suivi des vulnérabilités, auto-évaluation, …)	•Méthodologies adaptées mais très simplifiées •Périmètre réduit à une tâche, un actif, etc.	Celui qui réalise la tâche, sans appui impératif de la sécurité	Dépendant du périmètre, généralement peu de personnes

Ce type d'analyse sera réalisé sur opportunité. On pourra l'appuyer par exemple sur la méthodologie simplifiée définie pour les projets par exemple, mais il sera nécessaire de s' assurer que les échelles employées correspondent au périmètre.

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

OUTILLAGE
L'ALTERNATIVE

- Utiliser les outils des méthodologies (EBIOS, MEHARI)

Avantages	Inconvénients
Bases de connaissances pré remplies	Adaptation de la méthode à l'outil
Mécanismes implémentés	Nécessite une formation et de l'expérience
	Perte de maîtrise sur la méthodologie

- Créer son propre outillage

Avantages	Inconvénients
Implémentation pas à pas	Bases de connaissance à renseigner
Formation par la pratique qui engendre une meilleure maîtrise des concepts	Automatisation des calculs à implémenter
L'outil s'adapte à la méthode et au contexte (bases de connaissances)	Nécessite d'être documenté

Quel que soit l'outil, il doit être maîtrisé (pour les ajustements) et réutilisable (pour la revue des risques)

Outillage

Méthodologie – HOWTO avec Excel

- Lire l'ISO/IEC 27005 (~ 20 pages utiles)
- Onglet 1
  - Définition du contexte (quelques lignes)
  - Définition du périmètre
    - Activités essentielles et leur classification (au sens métier)
    - Actifs de support (ATTENTION à la granularité !)
- Onglet 2
  - Définition des métriques (grilles de probabilité, impact, acceptation du risque)
- Onglet 3 (option pour l'automatisation)
  - Base des menaces et base des vulnérabilités
- Onglet 4
  - Cartographie des risques consolidée par niveau (PPT)

Un peu de feeling et de pragmatisme permettent de réduire les bases de menaces et de vulnérabilités et par conséquent d'être plus efficace

OUTILLAGE

MÉTHODOLOGIE – HOWTO AVEC EXCEL

Besoin de sécurité	Disponibilité	Intégrité	Confidentialité	Preuve
Faible	**Plus de 72h**	**Détectable**	**Public**	**Pas de traces**
1	Une indisponibilité, planifiée ou non, n'impacte pas les processus de soin	Une perte d'intégrité, détectée ou non, perturbe peu les processus et peut rapidement être corrigée	Une divulgation de l'information n'a aucun impact	Aucune exigence ni besoin de trace n'est à prendre en compte
Moyen	**Entre 24 et 72h**	**Maîtrisé**	**Limité**	**Traces simples**
2	Une indisponibilité, limitée dans le temps, perturbe légèrement les processus	Une perte d'intégrité engendre des perturbations des processus mais ne porte pas atteinte à la survie de l'entité	Une divulgation à l'extérieur de l'entité peut porter atteinte à son image	L'opération réalisée doit être enregistrée et conservée avec un minimum d'information
Fort	**Entre 4 et 24h**		**Réservé**	
3	Une indisponibilité, de courte durée, perturbe les processus mais ne porte pas atteinte à la survie de l'entité		Une divulgation aux personnes non autorisées nuit significativement à l'image et peut entrainer des pertes	
Très fort	**Moins de 4h**	**Intègre**	**Privé**	**Traces détaillées**
4	Une indisponibilité, même de courte durée, impacte directement les processus et peut porter atteinte à la survie de l'entité	Une perte d'intégrité porte gravement atteinte aux processus et éventuellement à la survie de l'entité	Une divulgation de l'information nuit très gravement à l'entité victime de la divulgation	L'opération réalisée doit être enregistrée et conservée, de façon à être en mesure d'être rejouée

Niveaux de risque		Probabilité du scénario de menace				
		Très faible (Très improbable)	Faible (Improbable)	Moyen (Possible)	Forte (Probable)	Très forte (Très probable)
Impacts métier	Très faible	0	1	2	3	4
	Faible	1	2	3	4	5
	Moyen	2	3	4	5	6
	Fort	3	4	5	6	7
	Très fort	5	6	6	7	8

OUTILLAGE

MÉTHODOLOGIE – HOWTO AVEC EXCEL

L'identification des bons actifs et du bon niveau de granularité est un facteur clé de succès (éviter l'effet tunnel).

Par exemple, on pourra considérer en actifs de support « les serveurs Windows », « les équipements réseau », etc. pour éviter d'avoir à analyser les risques sur chaque serveur.

Bien essentiel :		
Critère	**Niveau**	**Justification**
Disponibilité		
Intégrité		
Confidentialité		
Preuve		

Biens supports		
Systèmes informatiques et de téléphonie		
ID	**Matériels**	**Lien**
MAT1		LOC1
MAT2		LOC2
MAT3		LOC3
ID	**Logiciels**	**Lien**
LOG1		
LOG2		
LOG3		
LOG4		
LOG5		
LOG6		
LOG7		
ID	**Canaux informatiques et de téléphonie**	**Lien**
RSX1		
RSX2		

ID	Menaces (référentiel ISO 27005)	Prise en compte	Bien support	Vulnérabilités exploitées	Mesures de sécurité implémentées	Conséquences	Initial			Traitement
							P	I	R	
THEME 1 : Sinistres physiques										
01	INCENDIE	oui								
02	DÉGÂTS DES EAUX	oui								
03	POLLUTION	oui								
04	SINISTRE MAJEUR	oui								
04	SINISTRE MAJEUR	oui								
05	DESTRUCTION DE MATÉRIELS OU DE SUPPORTS	oui								
THEME 2 : Evènements naturels										
06	PHÉNOMÈNE CLIMATIQUE	oui								
07	PHÉNOMÈNE SISMIQUE	oui								
08	PHÉNOMÈNE VOLCANIQUE	oui								
09	PHÉNOMÈNE MÉTÉOROLOGIQUE	oui								
10	CRUE	oui								
THEME 3 : Perte de services essentiels										
11	DÉFAILLANCE DE LA CLIMATISATION	oui								

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

Retours d'experience

Approche globale

- Périmètre
  - Global SI
- Ce qu'il s'est passé
  - Projet porté par le DSI (membre du CODIR)
  - Volonté d'entamer une approche par les risques
  - Identification de risques IT mais aussi RH, juridiques…
  - Crainte de présenter les résultats en dehors de la DSI
- Conclusion
  - Belle analyse de risque… à la DSI
  - PTR IT mis en œuvre dans une grande majorité
  - PTR hors IT figé
  - L'entité n'était pas suffisamment mûre pour entamer une démarche globale de pilotage par les risques
  - Le périmètre aurait pu être cantonné au domaine IT OU des audits techniques auraient pu suffir

RETOURS D'EXPERIENCE

APPROCHE POUR UNE APPLICATION

- Périmètre
  - Analyse de risques sur un progiciel
- Ce qu'il s'est passé
  - Suite à discussion avec les métiers et la volonté client, découpage fin du périmètre en modules fonctionnels du progiciel (complexité et durée de l'analyse d'impact métier)
  - Au final, ce type d'application ne repose que sur quelques actifs support. Les risques (menaces et vulnérabilités) ne sont donc pas liés à un module particulier mais à l'ensemble du progiciel, qui repose sur les mêmes actifs
- Conclusions
  - Passer par une analyse simplifiée pour identifier sommairement les risques principaux et les fonctions métier les plus sensibles
  - Focaliser l'analyse d'impacts métiers sur ces fonctions
  - Globaliser l'analyse des vulnérabilités sur l'ensemble de l'architecture

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

FACTEURS CLÉS DE SUCCÈS

- **Impliquer le métier** (c'est lui le propriétaire)
- Avoir un **sponsor au bon niveau**
- Bien choisir son **périmètre** et sa **granularité**
- Utiliser une **méthodologie reproductible et partagée**
- **Adapter la méthodologie à son propre contexte** (signaux compromettants)
- **Produire plusieurs vues** des résultats adaptées à chaque destinataire (Direction, IT, CP, Métier…)

ECUEIL À ÉVITER

- Entamer une analyse de risque sans en avoir préalablement défini les objectifs
- Réaliser une analyse de risque alors que l'organisation n'est pas assez mûre
- Vouloir être exhaustif dès la première itération
- Confondre analyse de risque, audit, classification…
- Considérer l'analyse de risque comme un projet unitaire
- Se reposer uniquement sur l'outil
- Ne pas considérer les facteurs clés de succès ;)

Agenda

- Introduction et concepts
- Méthodologies et normes
- Concrètement
- Outillage
- Retours d'expérience
- Facteurs clés de succès
- Conclusion et questions

Conclusion

- L'analyse de risque est le meilleur processus pour un pilotage efficace et pragmatique de la sécurité
- Il nécessite de maîtriser les concepts (accompagnement sécurité)
- Il s'agit d'un processus chronophage qui implique beaucoup d'acteurs (Direction, métier, IT, activités support, …)
- Ce processus ne peut être implémenté que dans des organisations mûres, dans lesquelles le métier est souciant de la sécurité
  - Sinon, opter pour d'autres outils tels que des audits
  - Hormis si l'on souhaite l'utiliser comme outil de sensibilisation du métier
- **Le choix du périmètre et de la granularité est essentiel**

Questions / Réponses

Merci !

Claire BERNISSON

06.16.26.48.44
cbernisson@lexsi.com

Frédérick MEYER

06.77.63.22.71
frederick.meyer@advens.fr