



EBIOS Risk Manager

Etude de cas fictive « *Analytics for Talent Management* »



Thierry PERTUS - Consultant Senior (Enterprise Risk Manager - CEFAR, ISO 31000 RM, ISO/IEC 27005 RM, ISO/IEC 27001 LI, CISM)

Afaf FAFI - Consultante Cyber Security & Data Protection (EBIOS RM, ISO/IEC 25005 RM, ISO/IEC 27001 LA, DPO / Privacy Implementer, CISA)

Classification du document : **Public** (éligible à publication)

Groupe de travail au sein du Club EBIOS : **Action 55 - « Outils & Pratiques »**

Lien sur le Forum des membres : <https://club-ebios.org/forum/viewforum.php?f=55>

17/02/2020 - v1.2



- AP** **Avant-propos**
- 1** **Atelier 1 : Cadrage et socle de sécurité**
- 2** **Atelier 2 : Sources de risque**
- 3** **Atelier 3 : Scénarios stratégiques**
- 4** **Atelier 4 : Scénarios opérationnels**
- 5** **Atelier 5 : Traitement du risque**
- A** **Annexes : Métriques et catalogues**



Avant-propos

Avant-propos : Rappel du contexte



La startup française **DigiTalents NextGen (*)** (désignée par DT-NG), Société par Actions Simplifiée (S.A.S) dont le siège social est basé à Issy-les-Moulineaux (92), est une startup de services du numérique (ESN) spécialisée dans le domaine du « **Talent Management** » (gestion des ressources humaines sous un angle plus valorisant), visant à s'appuyer sur le digital et la collecte massive de données pour optimiser selon un cercle vertueux les activités de **recrutement**, de **gestion de carrière** et de **développement des compétences** au sein des organisations, de **mesure de la e-réputation** ou encore de **valorisation de viviers**.

En terme de positionnement stratégique sur un marché particulièrement concurrentiel, DT-NG mise sur une approche disruptive en termes de prospection, de management et d'aide à la décision à l'ère de la data grâce aux dernières avancées technologiques et analytiques liées à la **data science**, de façon à proposer à ses clients professionnels (mode B2B) des formules d'abonnement à des **services en ligne hébergés en cloud** (mode IaaS pour DT-NG, mode SaaS pour ses clients), le cas échéant (selon la formule choisie) interfacé au **SIRH** (bases GRH) de l'entreprise cliente.

Pour se faire, après avoir spécifié ses processus métier et support, DT-NG s'est fixé pour premier objectif opérationnel de commencer par se doter d'ici **Septembre 2018** d'une **plateforme en ligne hautement efficiente** désignée par **Smart Analytics for Business Enabling (S.A.B.E.)** s'appuyant sur une architecture de type WOA (*Web Oriented Architecture*) constituée notamment d'un système *big data* en capacité de collecter et stocker dans un *data lake* (à base de technologies type *Hadoop*) une certaine volumétrie, vitesse et variété des sources de données, couplé à des modules de traitement (*analytics*) pour l'analyse statistique (*data mining*) et prédictive (*machine learning*), et en bout de chaîne (*business intelligence*) à des modules spécialisés dans la recherche multicritères et la visualisation des résultats en temps réel (*data viz*), le reporting et la traçabilité (*data lineage*).

(*) Entité et dénomination fictives visant à illustrer la présente étude de cas, toute ressemblance avec des organismes existants serait purement fortuite.

Avant-propos : Rappel du contexte

Création de valeur et objectifs stratégiques affichés vis-à-vis de la clientèle



- Constituer et actualiser des viviers de compétences (clients actifs inclus) par secteur d'activité ou domaine d'expertise pour les revendre à divers courtiers

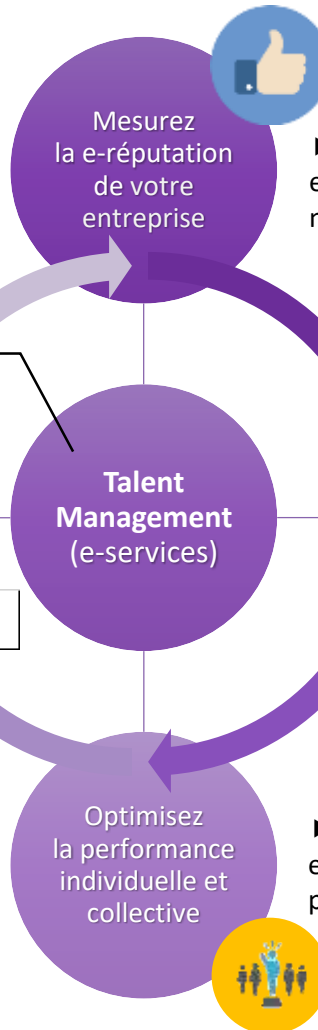


Maintenez vos collaborateurs à niveau et favorisez leur épanouissement

DEC.ADD.01

Renoncement provisoire à l'activité e-service de pérennisation des viviers de candidats

- Fidéliser et accroître les talents au sein de l'entreprise cliente par un plan de formation ou un accompagnement adaptés et alignés avec les objectifs opérationnels



Mesurez la e-réputation de votre entreprise

- Surveiller en continu l'attractivité de l'entreprise cliente et la résonance avec sa posture et ses valeurs notamment vis-à-vis des candidats à l'embauche potentiels

Recrutez les meilleurs profils correspondant à vos besoins

- Prospector et établir une sélection des profils recherchés et à fort potentiel susceptibles de rejoindre l'entreprise cliente

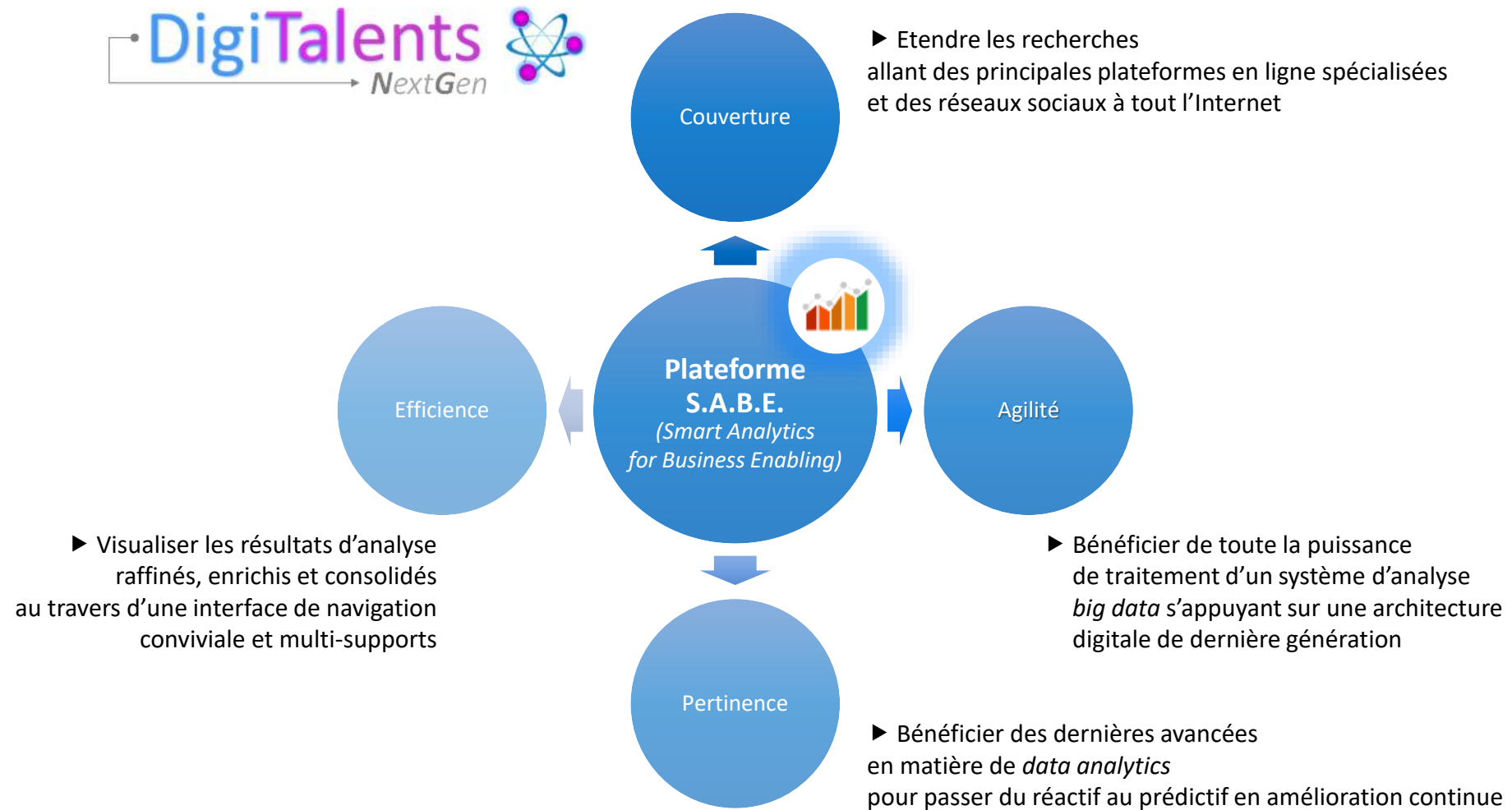
Optimisez la performance individuelle et collective

- Détecter et encourager les forces vives et talents émergents au sein de l'entreprise cliente par une gestion de carrière valorisante

(*) renoncement provisoire à cette mener cette activité potentiellement lucrative mais également sujette à controverse au regard du cadre réglementaire relatif à la protection des données personnelles

Avant-propos : Rappel du contexte

Critères différentiant et objectifs opérationnels affichés vis-à-vis de la clientèle



Avant-propos : Rappel du contexte

Compte tenu des points suivants :

- ✓ caractère relativement **critique** pour DT-NG de sa future **plateforme en ligne S.A.B.E** présentant une **dépendance extrême** du cœur de métier de DT-NG au « **monde digital connecté** » et par conséquent d'une **exposition intrinsèquement élevée à la cybermenace** ;
- ✓ **sensibilité de certaines données RH** mises à disposition par les entreprises clientes amenées à faire l'objet d'un **traitement analytique de masse** ;
- ✓ **enjeux juridiques majeurs** (sanctions pénales pouvant atteindre 4% du CA mondial ou 20 M€ au regard du dispositif RGPD) liés au renforcement du cadre légal en matière de **protection des données personnelles** ;
- ✓ **attentes croissantes** en termes de **pratiques éthiques** ou plus largement de « **confiance numérique** » exprimées par les clients (potentiellement par clauses contractuelles) et leurs propres parties prenantes ;

la Direction Générale de DT-NG avait décidé en 2017 de commanditer une **analyse de risques combinée « Security & Privacy by Design »** portant sur ladite plateforme telle que pressentie à la cible, et ce, en s'appuyant sur la méthode **EBIOS 2010**, faisant à l'époque référence en matière de management des risques liés à la sécurité de l'information.

Les objectifs étaient alors multiples : **dresser la liste des exigences** idoines en matière de **conformité légale** et plus largement de **confiance numérique** dans le cadre d'une démarche d'implémentation certifiable de **Système de Management de la Sécurité de l'Information (SMSI)** connoté « **Cloud computing** » et « **Privacy** » en vue de les intégrer au cahier des charges de la future plateforme, quitte à revoir au passage certaines lignes stratégiques du *business model* établi, tel que le renoncement provisoire à l'activité de pérennisation des viviers de candidats par le biais de la revente de données à des courtiers spécialisés (*data brokers*).

Avant-propos : Rappel du contexte

Si le **plan de traitement du risque** résultant de l'analyse EBIOS 2010 réalisée sur la base des éléments communiqués a globalement été suivi, en donnant lieu à la mise en œuvre de **mesures de sécurité organisationnelles et techniques** conformément aux recommandations s'appuyant sur le **cadre de référence** établi, certaines décisions postérieures à ladite analyse ont été prises. Parmi celles-ci, on notera, compte tenu de la difficulté à recruter et conserver des profils qualifiés dans le domaine, le recours à une prestation de sous-traitance auprès d'une société indienne basée à Bangalore et spécialisée en data science.

Par ailleurs, sur le plan de la prospection commerciale, DN-NG a entre temps remporté (en consortium avec un cabinet de conseil réputé) un marché public initié par une administration gouvernementale de premier plan (*), dans le cadre d'un PoC (*Proof of Concept*) visant à interfacer la base RH avec la plateforme S.A.B.E. officiellement dans l'optique de « rationaliser » la gestion de carrière du personnel (fonctionnaires et contractuels) et d'objectiver la délivrance de promotions pour l'accès aux fonctions clé de l'organisation.

(*) Scénario fictif visant à illustrer la présente étude de cas, toute ressemblance avec des organismes existants serait purement fortuite.

Avant-propos : Rappel du contexte

Fin décembre 2018, coup de théâtre, des fuites provenant d'un site d'information indépendant révèlent, éléments de preuve à l'appui, l'existence d'expérimentations auxquelles se serait livré une administration de l'Etat, consistant à établir, par corrélation et intelligence artificielle (IA), un profilage du personnel et à établir des grilles de compatibilité et d'incompatibilité avec certaines fonctions, sur la base de critères personnels « légalement contestables » (pour ne pas dire illicites) telles que les orientations politiques ou encore des accointances avec certaines personnalités ou courants de pensées, susceptibles d'être collectés et analysés aussi bien à partir de traces laissées sur Internet que de sources internes.

Après investigation et collecte de preuves numériques, les fuites en question tiendraient leur origine d'une exfiltration de données vraisemblablement opérée par une officine hacktiviste à tendance altermondialiste, qui auraient exploité certaines informations communiquées par un ex-employé data-scientiste soudoyé, afin de s'introduire dans le système de la plateforme S.A.B.E., par le biais de la connexion VPN, après avoir compromis par *spear phishing* un poste de développement localisé en Inde ...

Avant-propos : Rappel du contexte



So that **tomorrow**
will never look like **before** ...

Le pic de crise passé, après étouffement de l'affaire par le gouvernement avec la connivence des médias compte tenu des enjeux de réputation et de l'onde de choc provoqué par ce scandale, et après avoir procédé à un changement tactique de la raison sociale en « WeTalents » (*) (désigné par WT), les associés/actionnaires de l'ex-société DT-NG ont pris la décision de céder prématurément la société à des acteurs majeurs du numérique toujours présents sur les rangs.

Néanmoins, dans le cadre de la **due diligence**, il est demandé aux cadres dirigeants de WT d'apporter une **assurance raisonnable** sur le fait que l'exposition de la société au **risque cyber** est maîtrisé et durablement placé sous contrôle, selon un **angle de vision étendu** à l'ensemble de l'écosystème et aux vecteurs de compromission sous-jacents.

Pour se faire, une prestation d'expertise est confiée à une société spécialisée, qui préconise d'emblée de réaliser une **analyse de risques cyber approfondie**, assortie d'un audit de sécurité complet (pentest inclus), en s'appuyant cette fois-ci sur la méthode **EBIOS Risk Manager**, tout en capitalisant sur les livrables de l'analyse EBIOS 2010 précédemment réalisée sur ce même périmètre.

(*) Entité et dénomination fictives visant à illustrer la présente étude de cas, toute ressemblance avec des organismes existants serait purement fortuite.

Avant-propos : L'approche « par le risque » complémentaire à l'approche « par la conformité »

Démarche hybride EBIOS 2010 / EBIOS RM pour une approche proportionnée du management du risque numérique

Niveau de cybermenace potentiel > Risque cyber
[capacité, ciblage, sophistication des cyberattaques]



Avancé

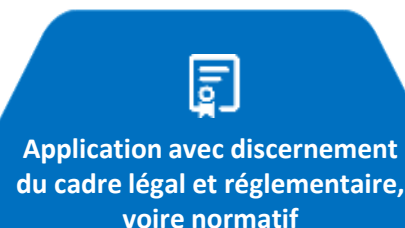


Approche **ciblée**,
par **modélisation de la cybermenace**
via des « **chemins d'attaque sophistiqués** »
considérés comme pertinents

Itération 2
(analyse raffinée)

Risques accidentels et environnementaux

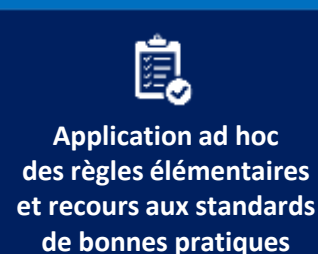
Elaboré



Approche à **large spectre**,
par **priorisation des mesures de sécurité**
issues du « **socle de sécurité** »
au regard des « **risques usuels** »

Itération 1
(analyse initiale)

Ordinaire



EBIOS 2010

Sources de risque numérique

Appréciation du risque numérique

Traitement du risque numérique

Adhérence normative avec l'ISO 31000:2018

Avant-propos : Méthodologie détaillée EBIOS Risk Manager



ATELIER 1 - CADRAGE ET SOCLE DE SÉCURITÉ

- a. définir le cadre de l'étude ;
- b. définir le périmètre métier et technique de l'objet étudié ;
- c. identifier les événements redoutés et évaluer leur niveau de gravité ;
- d. déterminer le socle de sécurité.

ATELIER 2 - SOURCES DE RISQUE

- a. identifier les sources de risque et les objectifs visés ;
- b. évaluer les couples SR/OV ;
- c. sélectionner les couples SR/OV jugés prioritaires pour poursuivre l'analyse.

ATELIER 3 - SCÉNARIOS STRATÉGIQUES

- a. construire la cartographie de menace numérique de l'écosystème et sélectionner les parties prenantes critiques ;
- b. élaborer des scénarios stratégiques ;
- c. définir des mesures de sécurité sur l'écosystème.

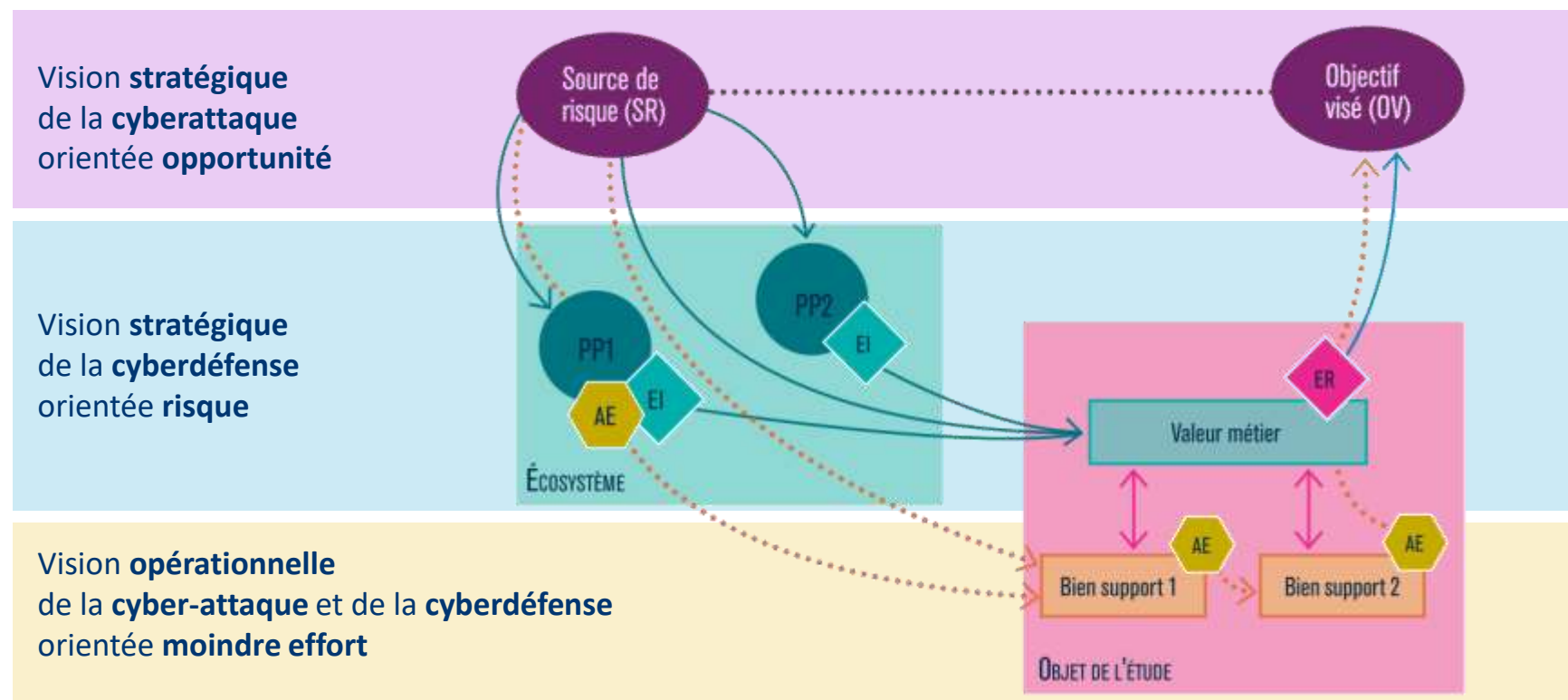
ATELIER 4 - SCÉNARIOS OPÉRATIONNELS

- a. élaborer les scénarios opérationnels ;
- b. évaluer leur vraisemblance.



ATELIER 5 - TRAITEMENT DU RISQUE

- a. réaliser la synthèse des scénarios de risque ;
- b. définir la stratégie de traitement du risque et les mesures de sécurité ;
- c. évaluer et documenter les risques résiduels ;
- d. mettre en place le cadre de suivi des risques.

Avant-propos : Modélisation d'un scénario de cyberattaque sous les angles attaque/défense



Légende :

-  Chemin d'attaque d'un scénario stratégique (CAS)
-  Mode opératoire d'un scénario opérationnel (MOD)
- AE** Action élémentaire sur un bien de support
- EI** Événement intermédiaire associé à une valeur métier de l'écosystème
- ER** Événement redouté relatif à une valeur métier de l'objet de l'étude
- PP** Partie prenante de l'écosystème





Atelier 1 : Cadrage et socle de sécurité

ATELIER 1 – CADRAGE ET SOCLE DE SÉCURITÉ

- a. définir le cadre de l'étude ;
- b. définir le périmètre métier et technique de l'objet étudié ;
- c. identifier les événements redoutés et évaluer leur niveau de gravité ;
- d. déterminer le socle de sécurité.

1a. définir le cadre de l'étude

Rappel du contexte et de l'objet de l'étude (cf. avant-propos ci-avant)

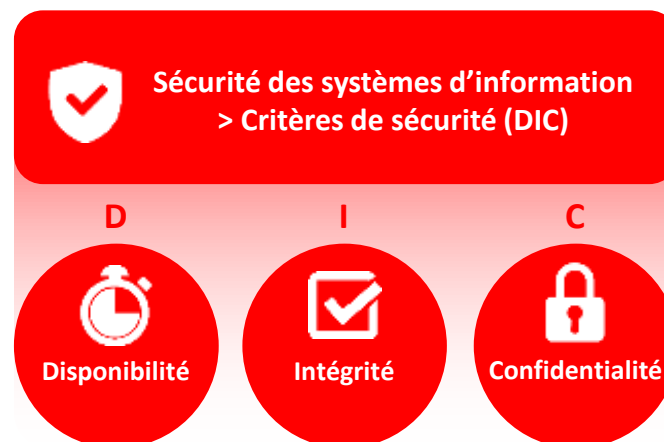
Dans le cadre de la **due diligence**, il est demandé aux cadres dirigeants de WT d'apporter une **assurance raisonnable** sur le fait que l'exposition de la société au **risque cyber** est maîtrisé et durablement placé sous contrôle, selon un **angle de vision étendu** à l'ensemble de l'écosystème et aux vecteurs de compromission sous-jacents.

Domaine d'application : Cybersécurité > Sécurité des systèmes d'information (SSI) sous l'angle de la cybermalveillance

Nature de l'étude : analyse de risques cyber, basé sur la méthode EBIOS Risk Manager (ANSSI)

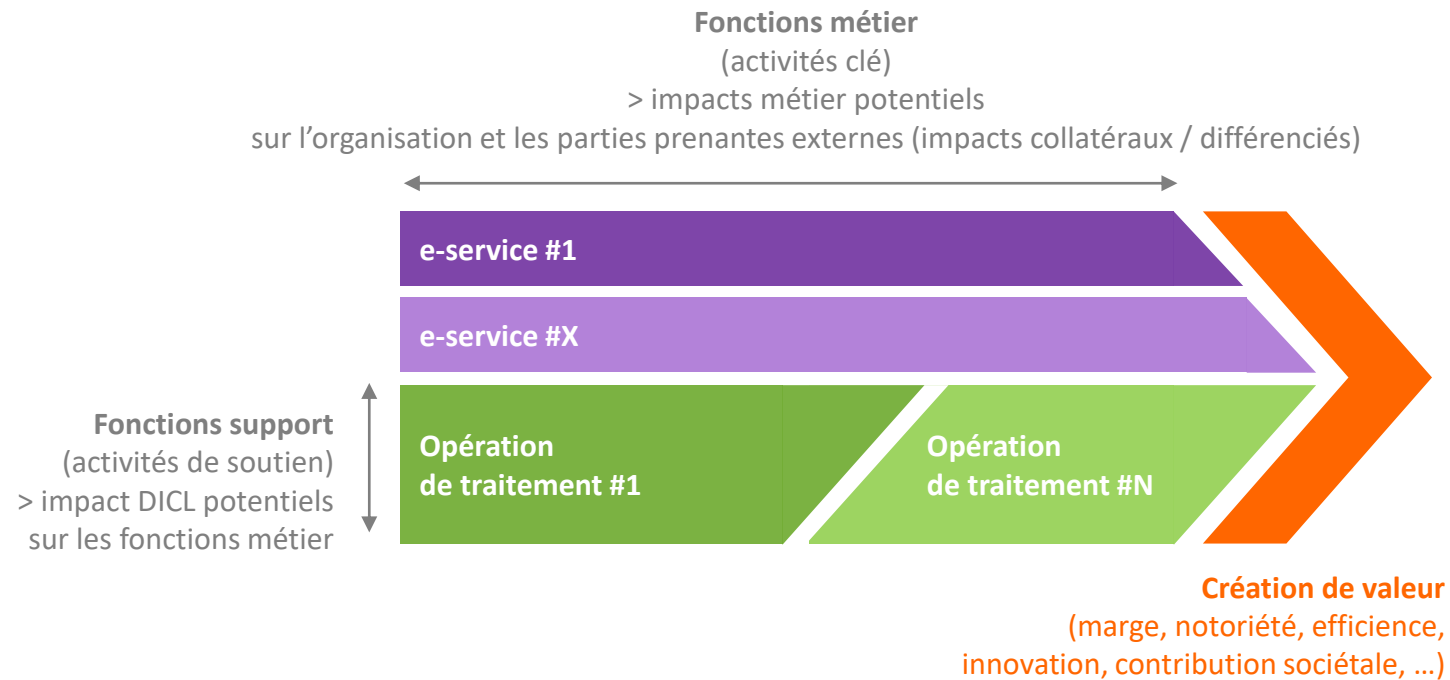
Finalité de l'étude : Utilisation des scénarios de risques pour conduire un audit de sécurité complet (pentest inclus)

Éléments d'entrée de l'étude : livrables de l'analyse de risques SSI, basé sur la méthode EBIOS 2010, précédemment réalisée



1b. définir le périmètre métier et technique de l'objet étudié

Modélisation des biens essentiels (fonctions essentielles)

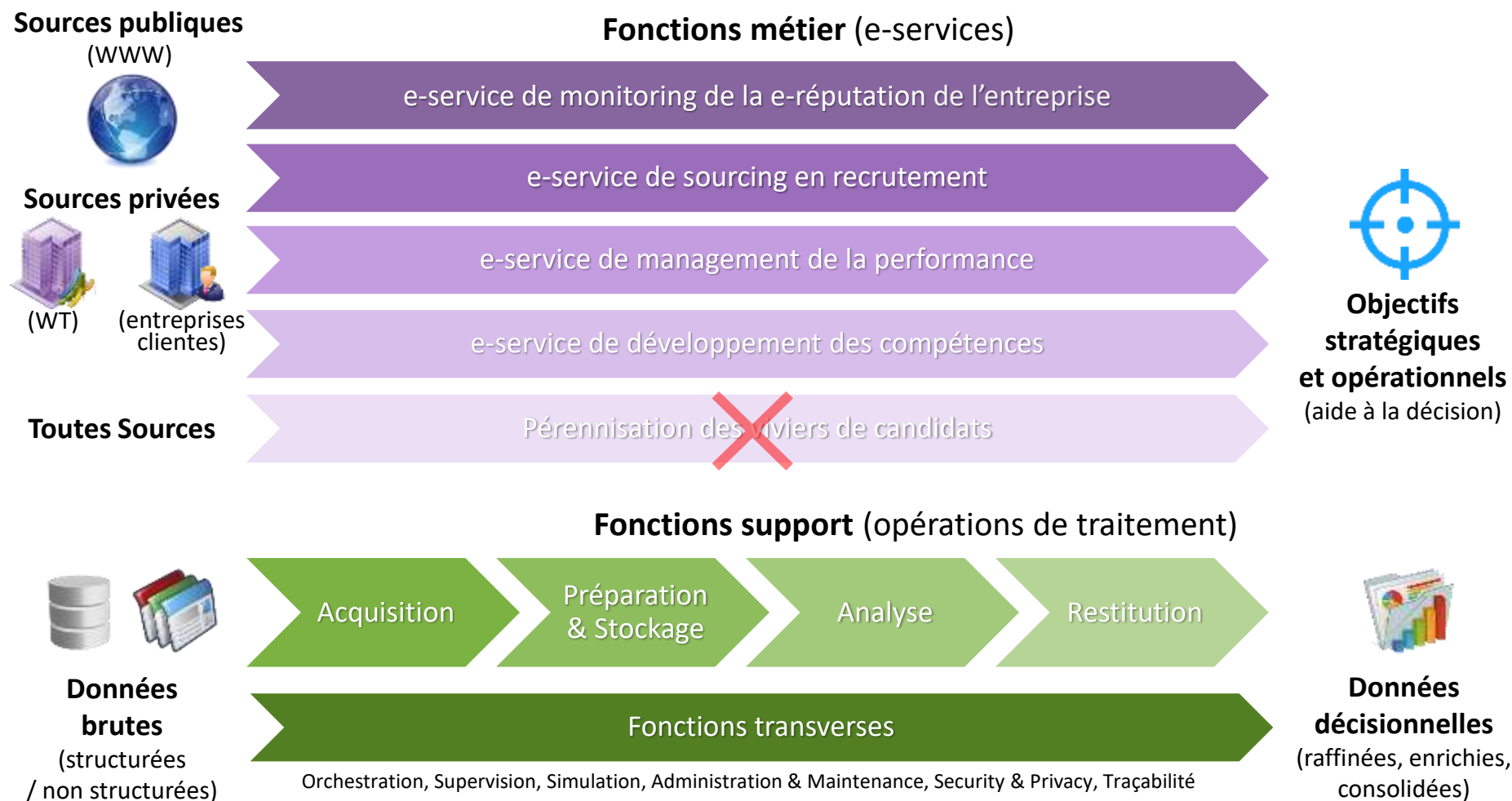


Modèle de la chaîne de valeur*

* Source : Modèle de la chaîne de valeur de Mickael Porter

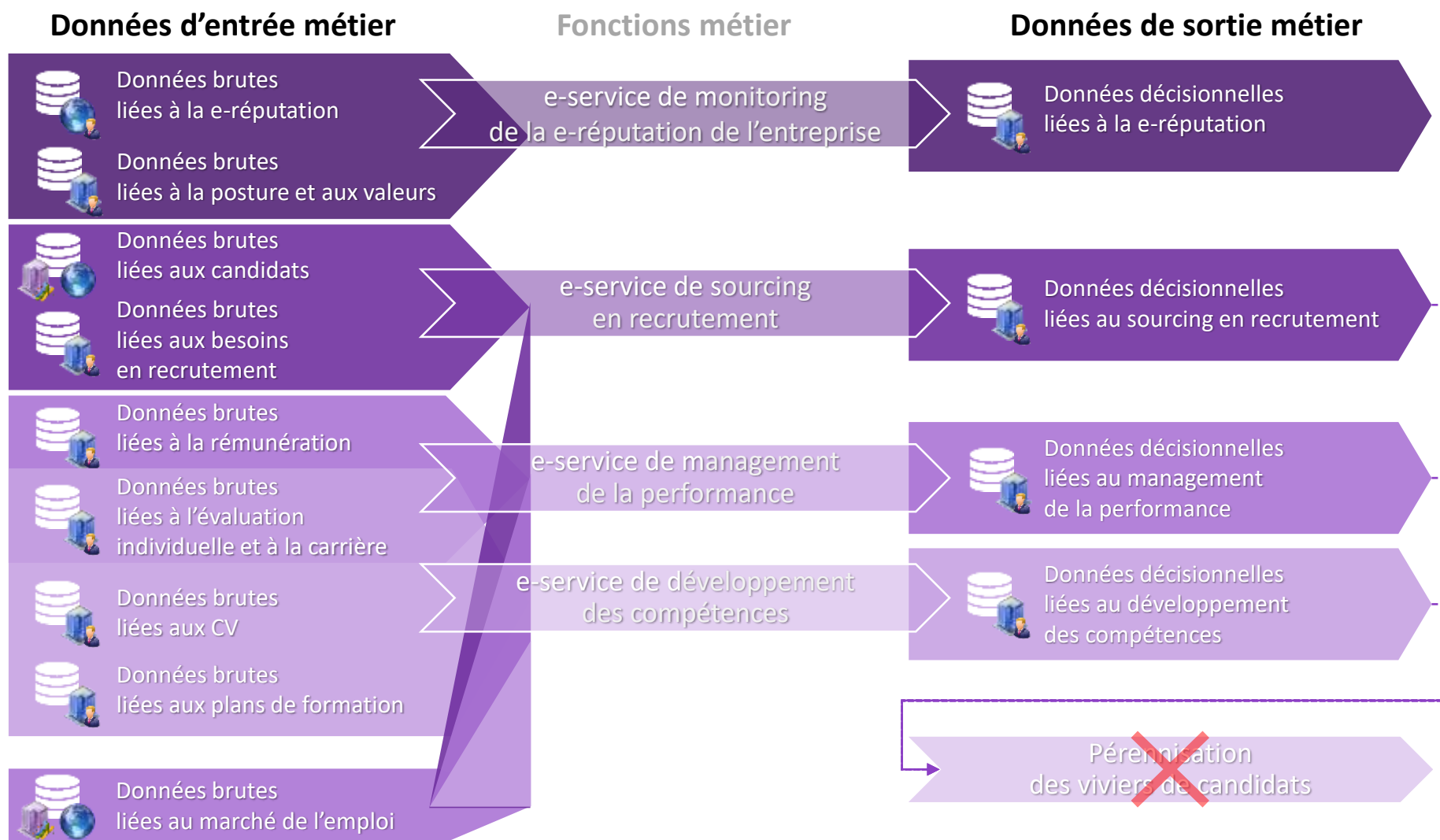
1b. définir le périmètre métier et technique de l'objet étudié

Modélisation des biens essentiels (fonctions essentielles)



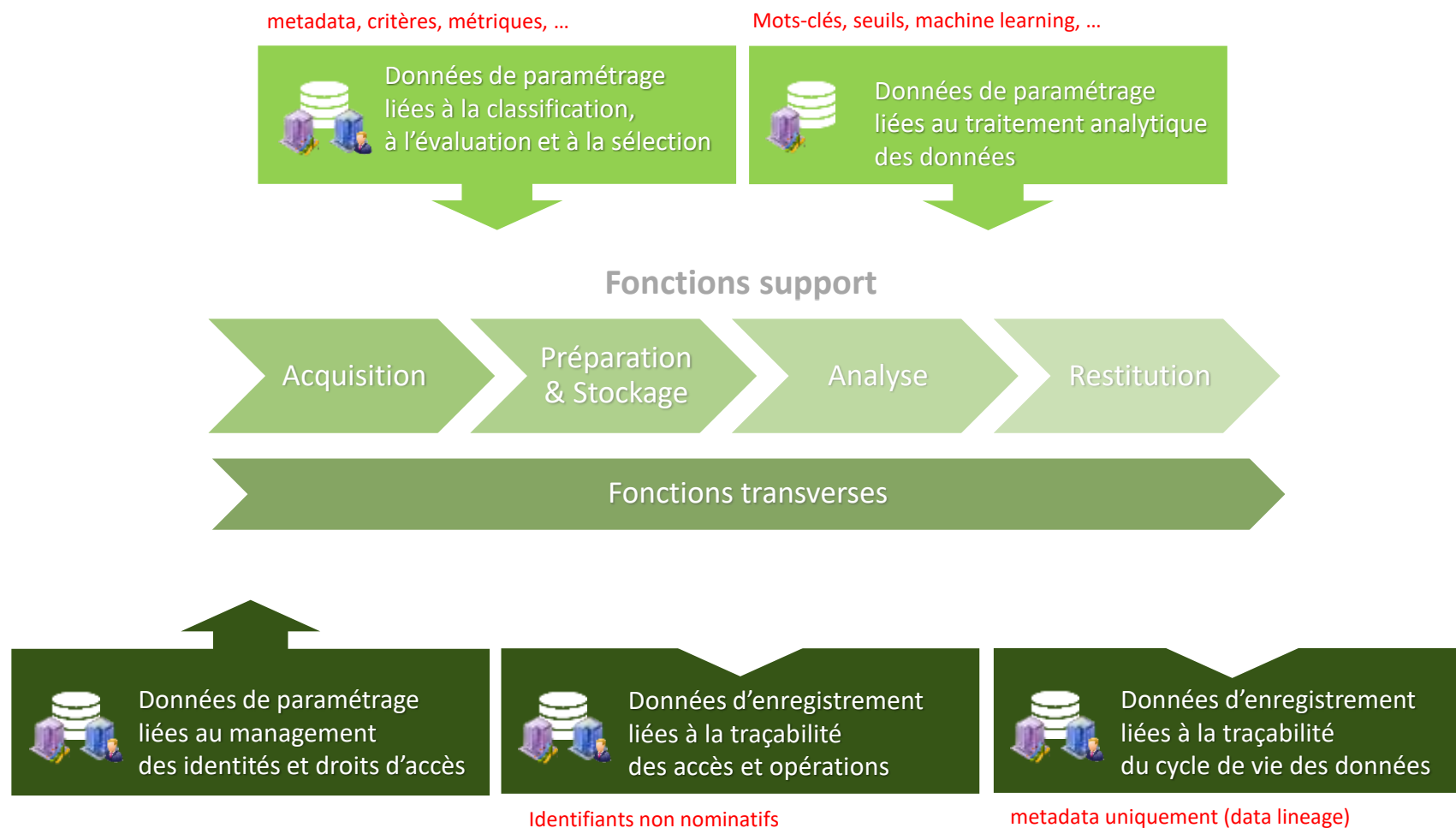
1b. définir le périmètre métier et technique de l'objet étudié

Modélisation des biens essentiels (informations essentielles liées aux fonctions métier)



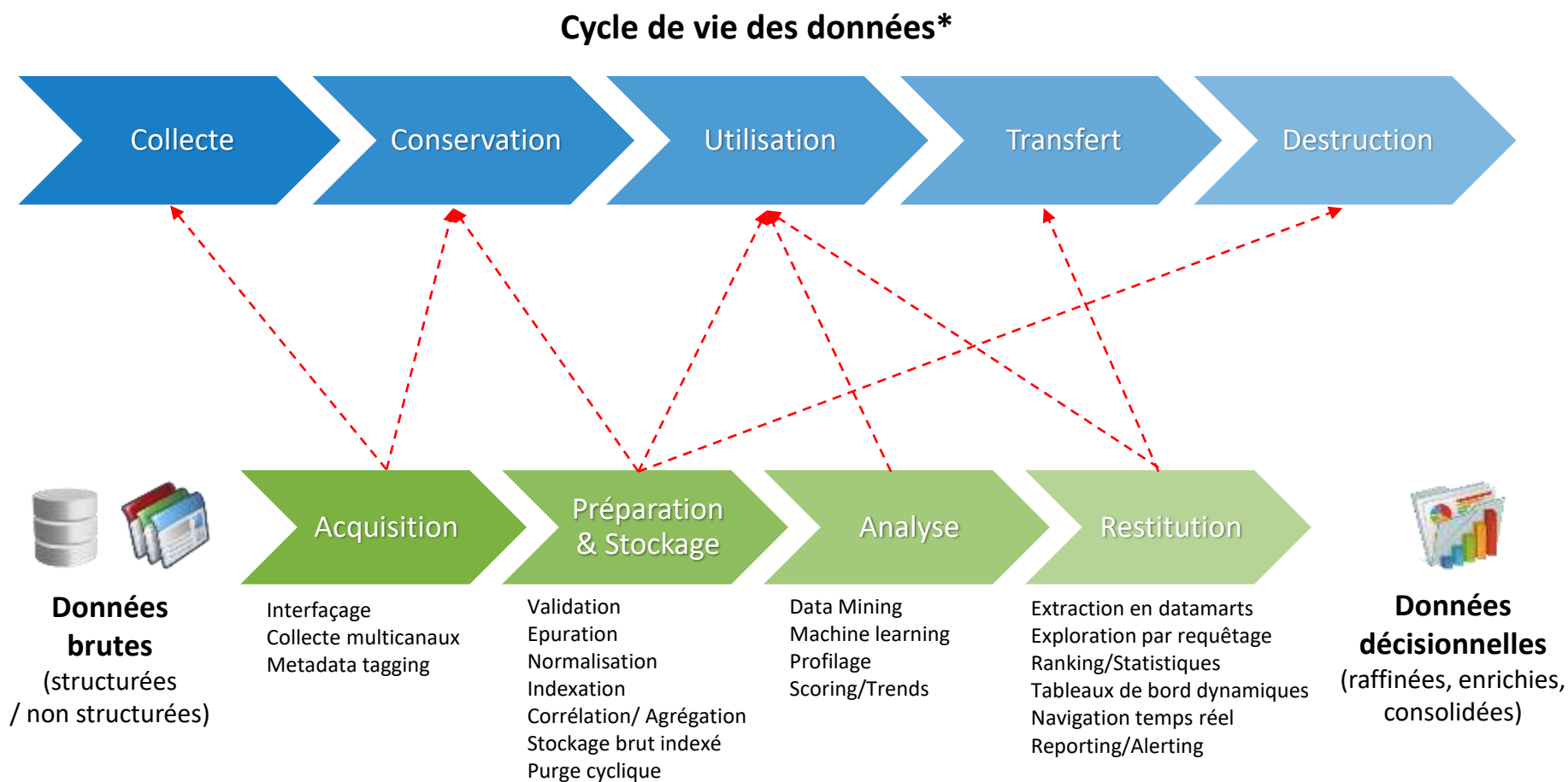
1b. définir le périmètre métier et technique de l'objet étudié

Modélisation des biens essentiels (informations essentielles liées aux fonctions support)



1b. définir le périmètre métier et technique de l'objet étudié

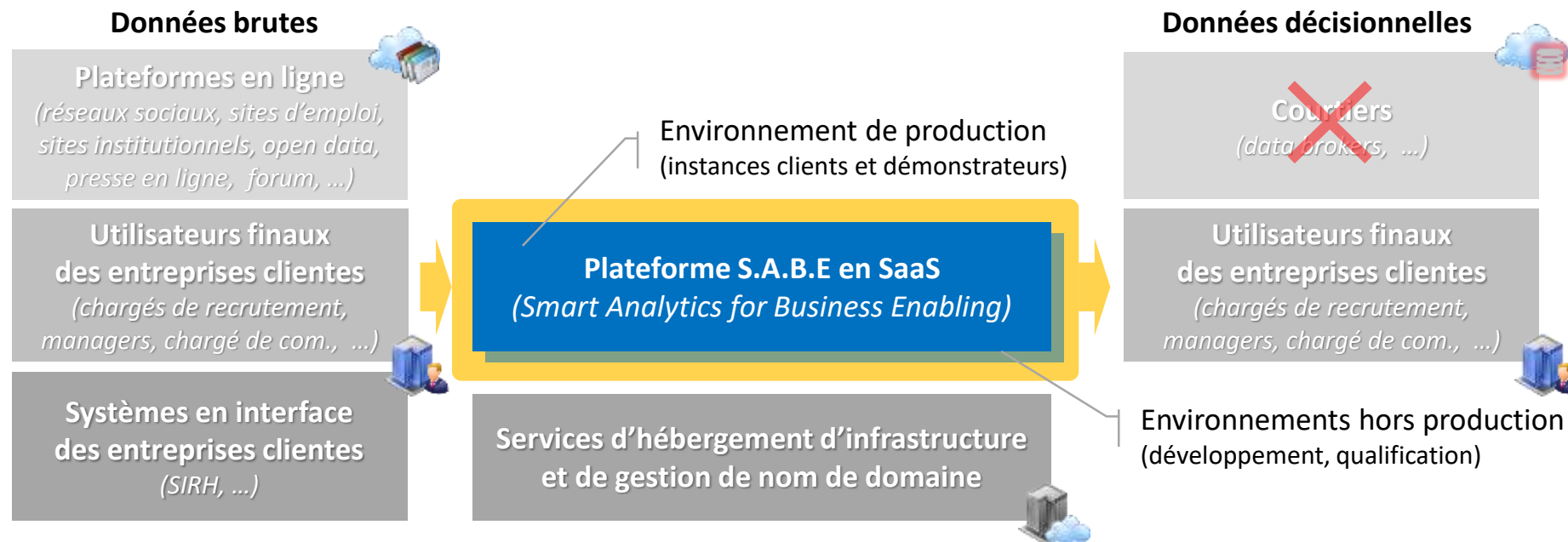
Correspondance entre fonctions essentielles et cycle de vie des données
(angle « Traitement DCP »)



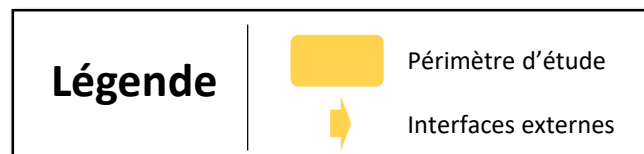
* Source : CNIL – guide PIA-2

1b. définir le périmètre métier et technique de l'objet étudié

Modélisation écosystémique du périmètre support (biens supports et flux de données)



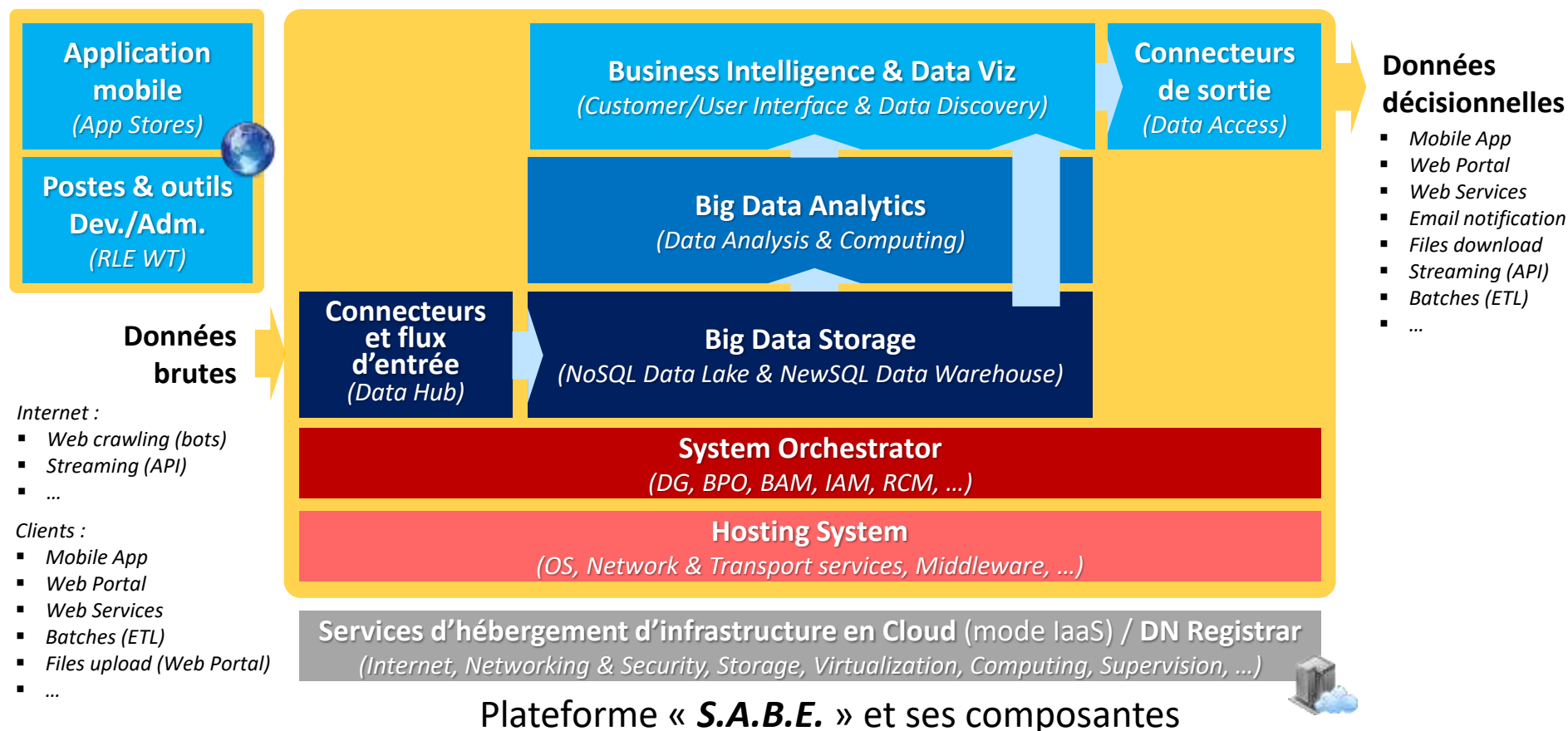
Plateforme « **S.A.B.E** » et son écosystème



IaaS : Infrastructure as a Service
SaaS : Software as a Service

1b. définir le périmètre métier et technique de l'objet étudié

Modélisation fonctionnelle du périmètre support (biens supports et flux de données)



Plateforme « **S.A.B.E.** » et ses composantes

Légende



Périmètre d'étude
Interfaces externes

DG : Data Governance (*)
BPO : Business Process Orchestration
BAM : Business Activity Monitoring
IAM : Identity & Access Management
RCM : Release & Change Management

(*) Source Selection, Metadata Categories, Data Quality & Consistency, Data Scrubbing & Protection, Data Lineage, Data Persistence, Data Ownership, Policy Compliance, ...

1b. définir le périmètre métier et technique de l'objet étudié

Rappel des biens essentiels et des dépendances établis lors de l'étude EBIOS 2010

X			PM01	PM02	PM03	PM04	PM05	PS01	PS02	PS03	PS04
	Label	[PM] Processus Métier / Désignation									
	PM01 [REP]	e-service de monitoring de la e-réputation de l'entreprise									
	PM02 [REC]	e-service de sourcing en recrutement									
	PM03 [PRF]	e-service de management de la performance									
	PM04 [CPT]	e-service de développement des compétences									
	PM05 [VIV]	e-service de pérennisation des viviers de candidats									
	Label	[PS] Processus Support / Désignation									
	PS01 [ACQ]	Acquisition									
	PS02 [P&S]	Préparation & Stockage									
	PS03 [ANL]	Analyse									
	PS04 [RST]	Restitution									
	Label	Désignation	Fonctions dépendantes								
	DMD01 [REP]	Données décisionnelles liées à la e-réputation	X								
	DMD02 [REC]	Données décisionnelles liées au sourcing en recrutement		X			X				
	DMD03 [PRF]	Données décisionnelles liées au management de la performance			X		X				
	DMD04 [CPT]	Données décisionnelles liées au développement des compétences				X	X				
	DMB01 [REP]	Données brutes liées à la e-réputation	X								
	DMB02 [POS]	Données brutes liées à la posture et aux valeurs	X								
	DMB03 [CAN]	Données brutes liées aux candidats		X							
	DMB04 [BES]	Données brutes liées aux besoins en recrutement		X							
	DMB05 [REM]	Données brutes liées à la rémunération			X						
	DMB06 [EVA]	Données brutes liées à l'évaluation individuelle et à la carrière			X	X					
	DMB07 [CUR]	Données brutes liées aux cursus et aptitudes				X					
	DMB08 [FOR]	Données brutes liées aux plans de formation				X					
	DMB09 [MAR]	Données brutes liées au marché de l'emploi		X	X	X					
	DST01 [CLA]	Données de paramétrage liées à la classification, à l'évaluation et à la sélection							X	X	X
	DST02 [ANL]	Données de paramétrage liées au traitement analytique des données							X	X	
	DST03 [IAM]	Données de paramétrage liées au management des identités et droits d'accès						X	X	X	X
	DST04 [TAO]	Données d'enregistrement liées à la traçabilité des accès et opérations						X	X	X	X
	DST05 [TCD]	Données d'enregistrement liées à la traçabilité du cycle de vie des données						X	X	X	X

ATELIER 1 – CADRAGE ET SOCLE DE SÉCURITÉ

ATELIER 1 - CADRAGE ET SOCLE DE SÉCURITÉ










Valeur Métier (VM)	Évènement redouté (ER) EBIOS 2010	Évènement redouté (ER)	DIC	Gravité (G)
DMB05, DMB06, DMD03, DMD04	ER09, ER10, ER13, ER14	ER101 - Divulgence de données décisionnelles liées au management des ressources humaines	C	4
DST01, DST02, DST03	ER22	ER102 - Divulgence de données techniques de paramétrage	C	4
PM03, PM04	ER02, ER03	ER103 - Altération des données brutes clients liées au management des ressources humaines	I	3



			Critères d'évaluation																							
			Gravité initiale		Gravité finale		Fonctions essentielles								Informations essentielles											
							Disponibilité				Fiabilité				Précision											
							D	I	C	L	F	R	E	P	P	M	N	V								
Label	Intitulé	Exemples / Précisions	Gi	Egi							Fonctions essentielles								Informations essentielles							
ER02	Altération des opérations de traitement dans le cadre du e-service de management de la performance	fourniture de recommandations inexactes	3	10			X				X															
ER03	Altération des opérations de traitement dans le cadre du e-service de développement des compétences	fourniture de recommandations inexactes	3	10			X				X															
ER09	Divulgation de données décisionnelles liées au management de la performance	fuite de données stratégiques	4	17					X					X												
ER10	Divulgation de données décisionnelles liées au développement des compétences	fuite de données stratégiques	4	17					X					X												
ER13	Divulgation de données brutes liées à la rémunération	fuite de données stratégiques	4	9					X							X										
ER14	Divulgation de données brutes liées à l'évaluation individuelle et à la carrière	fuite de données stratégiques	4	9					X							X										
ER22	Divulgation de données techniques de paramétrage	fuite de données liées au savoir	4	13					X								X	X								

1d. déterminer le socle de sécurité



	Sigle	Type de référentiel	Emetteur	Titre	Champ d'application	Application
	CSA-BD-S&P	Guide méthodologique	CSA	Big Data - Security and Privacy Handbook	Sécurité et Protection DP de systèmes Big Data	Ecarts majeurs
	ISO-27018	Norme internationale	ISO/IEC	Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	Protection DP en Cloud	Ecarts majeurs
	ISO-27017	Norme internationale	ISO/IEC	Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Sécurité de l'information en Cloud	Ecarts majeurs
	SMSI (DdA)	Norme internationale	ISO/IEC	Systèmes de management de la sécurité de l'information [ISO/IEC 27001:2013] - Annexe A / Déclaration d'Applicabilité (DdA)	Sécurité de l'information	Ecarts majeurs
	CNIL-GRH	Référentiel	CNIL	Référentiel relatif aux traitements de données a caractère personnel mis en œuvre par des organismes prives ou publics aux fins de gestion du personnel (version projet) Note : Référentiel adossé aux dispositions du règlement général sur la protection des données (RGPD - UE/2016/679), à la loi « Informatique et Libertés » (LIL - n° 78-17 modifiée), ainsi qu'au code du travail.	Protection DP	Ecarts majeurs
	WT-BCR	Référentiel interne	WT	Code de conduite relatif à la protection des données personnelles	Protection DP	Complète
	WT-PSSI	Référentiel interne	WT	Politique de Sécurité des Systèmes d'Information (PSSI)	Sécurité de l'information	Complète
	SEC-DP	Guide	CNIL	La sécurité des données personnelles (v2018)	Protection DP	Complète
	HYG-INF	Guide	ANSSI	Hygiène informatique (v2.0) – règles de niveau standard	Sécurité informatique	Complète

Application
Complète
Ecarts mineurs
Ecarts majeurs
Non-effective
N/A

Note : Le focus est fait ici par rapport aux référentiels directement applicables (normes et guides), le cadre de référence ayant déjà été spécifié lors de la première itération sous EBIOS 2010.

1d. déterminer le socle de sécurité

Structure et thématiques du guide ANSSI | Hygiène informatique [HYG-INF]



- I - Sensibiliser et former
- II - Connaitre le système d'information
- III - Authentifier et contrôler les accès
- IV - Sécuriser les postes
- V - Sécuriser le réseau
- VI - Sécuriser l'administration
- VII - gérer le nomadisme
- VIII - Maintenir à jour le système d'information
- IX - Superviser, auditer, réagir
- X - Pour aller plus loin

Application
Complète
Ecart mineurs
Ecart majeurs
Non-effective
N/A

1d. déterminer le socle de sécurité

Structure et thématiques du guide CNIL | Sécurité des données personnelles [SEC-DP]



- 1. Sensibiliser les utilisateurs
- 2. Authentifier les utilisateurs
- 3. Gérer les habilitations
- 4. Tracer les accès et gérer les incidents
- 5. Sécuriser les postes de travail
- 6. Sécuriser l'informatique mobile
- 7. Protéger le réseau informatique interne
- 8. Sécuriser les serveurs
- 9. Sécuriser les sites web
- 10. Sauvegarder et prévoir la continuité d'activité
- 11. Archiver de manière sécurisée
- 12. Encadrer la maintenance et la destruction des données
- 13. Gérer la sous-traitance
- 14. Sécuriser les échanges avec d'autres organismes
- 15. Protéger les locaux
- 16. Encadrer les développements informatiques
- 17. Chiffrer, garantir l'intégrité ou signer



Application
Complète
Ecarts mineurs
Ecarts majeurs
Non-effective
N/A

1d. déterminer le socle de sécurité

Structure et thématiques de la norme ISO/IEC 27001:2013 - Annexe A SMSI (DdA) étendue ISO/IEC 27017 et 27018



- A5. Politiques de sécurité de l'information
- A6. Organisation de la sécurité de l'information
- A7. Sécurité des ressources humaines
- A8. Gestion des actifs
- A9. Contrôle d'accès
- A10. Cryptographie
- A11. Sécurité physique et environnementale
- A12. Sécurité liée à l'exploitation
- A13. Sécurité des communications
- A14. Acquisition, développement et maintenance des systèmes d'information
- A15. Relations avec les fournisseurs
- A16. Gestion des incidents liés à la sécurité de l'information
- A17. Continuité de la sécurité de l'information
- A18. Conformité



Application
Complète
Ecarts mineurs
Ecarts majeurs
Non-effective
N/A

* Système de Management de la Sécurité de l'Information / Déclaration d'Applicabilité (DdA)

1d. déterminer le socle de sécurité

Structure et thématiques du guide **Cloud Security Alliance | Big Data - Security and Privacy Handbook [CSA-BD-S&P]**



- 1. Secure Computations in Distributed Programming Frameworks
- 2. Security Best Practices for Non-Relational Data Stores
- 3. Secure Data Storage and Transaction Logs
- 4. Endpoint Input Validation / Filtering
- 5. Real-Time Security / Compliance Monitoring
- 6. Scalable and Composable Privacy-Preserving Analytics
- 7. Cryptographic Technologies for Big Data
- 8. Granular Access Control
- 9. Granular Audits
- 10. Data Provenance

Application
Complète
Ecart mineurs
Ecart majeurs
Non-effective
N/A



Atelier 2 : Sources de risque

ATELIER 2 - SOURCES DE RISQUE

- a. identifier les sources de risque et les objectifs visés ;
- b. évaluer les couples SR/OV ;
- c. sélectionner les couples SR/OV jugés prioritaires pour poursuivre l'analyse.

2a. Identifier les sources de risque et les objectifs visés

Catégorisation		
Caractère ciblé / non-ciblé	SR	App.
Sources de risques liées aux attaques opportunistes (non-ciblées)	SR1 - Code malveillant	✓
	SR2 - Botnet	✓
	SR3 - Hacker isolé	✓
Sources de risques liées aux attaques ciblées	SR4 - Organisation cybercriminelle	✓
	SR5 - Organisation hacktiviste	✓
	SR6 - Organisation cyberterroriste	✗
	SR7 - Utilisateur client malhonnête	✗
	SR8 - Employé / Prestataire corrompu ou négligent	✓
	SR9 - Ex-partie prenante en quête de vengeance ou de profit (Employé / Prestataire / Utilisateur / Client)	✓

✓ Retenu
✗ Non retenu

Catégorisation		Types d'impact			
Motivation prédominante	OV	OPE	FIN	JUR	REP
Gain financier pour l'attaquant (SR)	OV1 - Fraude financière		●		
	OV2 - Rançonnage		●		
	OV3 - Vol de données		●		
	OV4 - Exploitation illégitime de données		●		
Préjudices pour la victime ou son écosystème	OV5 - Divulgence de données				●
	OV6 - Altération / Détournement de données	●			
	OV7 - Entrave au fonctionnement	●			
	OV8 - Atteinte à la trésorerie		●		
	OV9 - Poursuites judiciaires			●	
	OV10 - Atteinte à l'image				●
	OV11 - Désordre sociétal				●

Types d'impact : OPE : Opérationnel; FIN : Financier; JUR : Juridique; REP : Réputation

2b. évaluer les couples SR/OV

SR	OV	Motivation	Ressources	Activité	Pertinence	
SR1- Code malveillant	OV6, OV7	**	**	*	5	Moyenne
SR2 - Botnet	OV7	**	**	*	5	Moyenne
SR3 - Hacker isolé	OV1, OV3, OV10	*	*	*	3	Faible
SR4 - Organisation cybercriminelle	OV1, OV2, OV3, OV4, OV6, OV7	**	***	*	6	Moyenne
SR5 - Organisation hacktiviste	OV5, OV7, OV8, OV9, OV10	**	**	**	6	Moyenne
SR8 - Employé / Prestataire corrompu ou négligent	OV1, OV3, OV4	*	**	***	6	Moyenne
SR9 - Ex-partie prenante en quête de vengeance ou de profit	OV5, OV6, OV7, OV8, OV9, OV10	***	**	***	8	Elevé

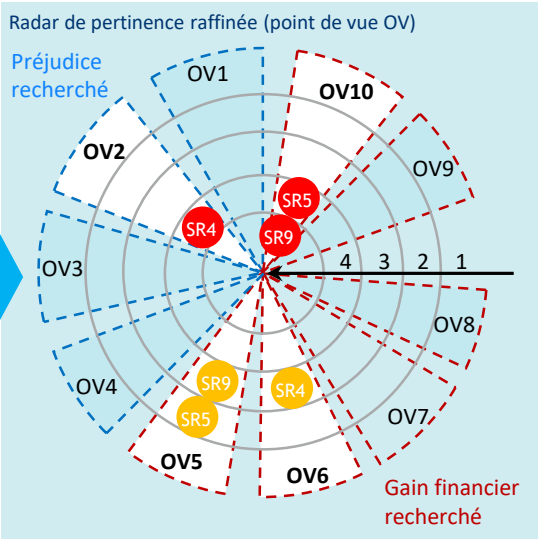
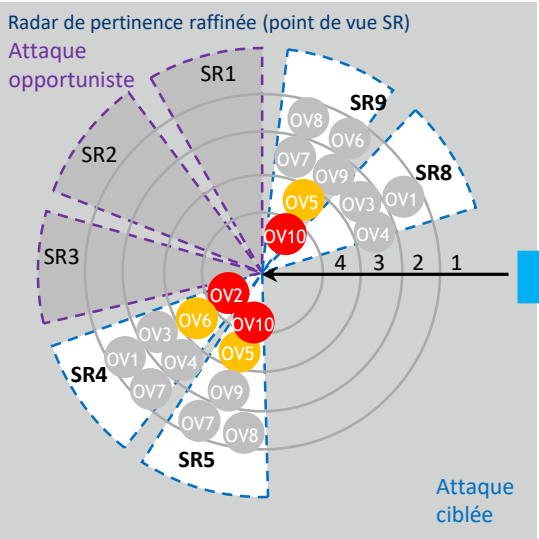
Proposition d'échelle de cotation de la pertinence :

- $\Sigma(\text{Mot, Res, Act}) = 3 \text{ à } 4$: Faible
- $\Sigma(\text{Mot, Res, Act}) = 5 \text{ à } 6$: Moyenne
- $\Sigma(\text{Mot, Res, Act}) = 7 \text{ à } 9$: Elevé

Sélection des couples SR/OV dont la pertinence est > 5
(parti pris au regard de la distribution des estimations)

2c. sélectionner les couples SR/OV jugés prioritaires pour poursuivre l'analyse

SR	OV	Pertinence
SR4 - Organisation cybercriminelle	OV1 - Fraude financière	Moyenne
	OV2 - Rançonnage	
	OV3 - Vol de données	
	OV4 - Exploitation illégitime de données	
	OV6 - Altération / Détournement de données	
	OV7 - Entrave au fonctionnement	
SR5 - Organisation hacktiviste	OV5 - Divulgation de données	Moyenne
	OV7 - Entrave au fonctionnement	
	OV8 - Atteinte à la trésorerie	
	OV9 - Poursuites judiciaires	
	OV10 - Atteinte à l'image	
SR8 - Employé / Prestataire corrompu ou négligent	OV1 - Fraude financière	Moyenne
	OV3 - Vol de données	
	OV4 - Exploitation illégitime de données	
SR9 - Ex-partie prenante en quête de vengeance ou de profit	OV5 - Divulgation de données	Elevée
	OV6 - Altération / Détournement de données	
	OV7 - Entrave au fonctionnement	
	OV8 - Atteinte à la trésorerie	
	OV9 - Poursuites judiciaires	
	OV10 - Atteinte à l'image	



- Couple SR/OV retenu
 - Couple SR/OV intermédiaire retenu
 - Couple SR/OV non retenu
- Concept expérimental

SR	Objectif Visé <u>intermédiaire</u> (OVi)	Objectif Visé (OV)	Pertinence raffinée
SR9 - Ex-partie prenante en quête de vengeance ou de profit	OV5 - Divulgation de données	OV10 - Atteinte à l'image	Elevée
SR5 - Organisation hacktiviste	OV5 - Divulgation de données	OV10 - Atteinte à l'image	Moyenne
SR4 - Organisation cybercriminelle	OV6 - Altération / Détournement de données	OV2 - Rançonnage	Moyenne





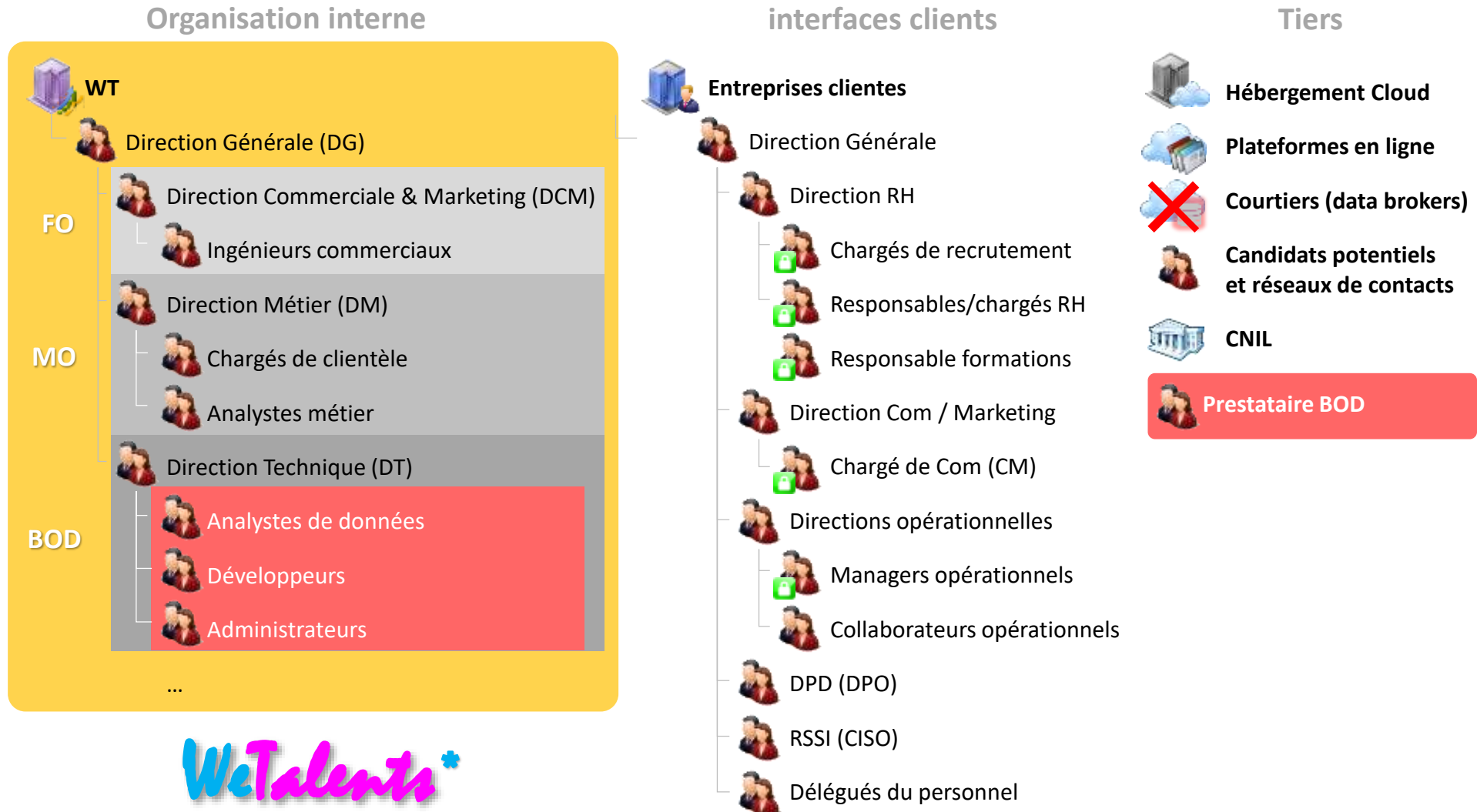
Atelier 3 : Scénarios stratégiques

ATELIER 3 - SCÉNARIOS STRATÉGIQUES

- a. construire la cartographie de menace numérique de l'écosystème et sélectionner les parties prenantes critiques ;
- b. élaborer des scénarios stratégiques ;
- c. définir des mesures de sécurité sur l'écosystème.

3a. construire la cartographie de menace numérique de l'écosystème [...]

Recensement des parties prenantes (acteurs internes et externes)



FO : Front-Office
MO : Middle-Office
BOD : Back-Office Digital
RH : Ressources Humaines
Com : Communication
CM : Community Manager
CISO : Chief Information Security Officer
DPO : Data Protection Officer

3a. construire la cartographie de menace numérique de l'écosystème [...]

Modification de la modélisation des biens supports antérieurement réalisée sous EBIOS 2010, comme suit :

			Objets (besoins) Fonctions essentielles PM01 [REP] PM02 [REC] PM03 [PRF] PM04 [CPT] PM05 [TVI] PS01 [ACQ] PS02 [P&S] PS03 [ANL] PS04 [RST] Informations essentielles													
Type	Label	Désignation	Responsable	Fonctions dépendantes												
Périmètre d'étude																
ORG	DT-NG	Organisation générale de DigiTalents NextGen S.A.S (Société par Actions Simplifiée)	DG			X	X	X	X	X	X	X	X	X		
PER	DT-NG.MO	Middle-Office (collaborateurs habilités à intervenir sur la plateforme S.A.B.E.)	DM			X	X	X	X	X	X	X	X	X		
PER	DT-NG.MO.CLT	Chargés de clientèle	Lié à l'arborescence			(X)	(X)	(X)	(X)	(X)						
PER	DT-NG.MO.ANL	Analystes métier	Lié à l'arborescence			(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)		
REL	DT-NG.BOD	Back-Office Digital (collaborateurs habilités à intervenir sur la plateforme S.A.B.E.)	DT			X	X	X	X	X	X	X	X	X		
REL	DT-NG.BOD.ANL	Analystes de données	Lié à l'arborescence			(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)		
REL	DT-NG.BOD.DEV	Développeurs	Lié à l'arborescence			(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)	(X)		
REL	DT-NG.BOD.ADM	Administrateurs (systèmes, middleware, applications, ...)	Lié à l'arborescence								(X)	(X)	(X)	(X)		
REL	TIER.CC.CGU	Contrats commerciaux et conditions générales d'utilisation liés à la plateforme S.A.B.E.	DM			X	X	X	X	X	X	X	X	X		
REL	HEB.CONT	Contrat d'hébergement en Cloud (mode IaaS)	Lié à l'arborescence			X	X	X	X	X	X	X	X	X		
REL	DNS.CONT	Contrat d'enregistrement et de gestion de noms de domaine internet	Lié à l'arborescence			X	X	X	X	X	X	X	X	X		
REL	WWW.CONT	Contrats d'abonnement aux services payants fournis par les plateformes en ligne pour la plateforme S.A.B.E	Lié à l'arborescence				X									
REL	WWW.CGU	Conditions générales d'utilisation des services fournis par les plateformes en ligne pour la plateforme S.A.B.E	Lié à l'arborescence				X									
REL	SABE.CONT.CGU.CUST	Contrats d'abonnement aux e-services S.A.B.E. et conditions générales d'utilisation pour les entreprises clientes	Lié à l'arborescence			U	U	U	U		U	U	U	U		
REL	SABE.CONT.CGU.BROK	Contrats d'abonnement aux e-services S.A.B.E. et conditions générales d'utilisation pour les courtiers (data brokers)	Lié à l'arborescence							U				U		
REL	STOR.CGU	Conditions générales d'utilisation des services de publication des magasins en ligne d'applications mobiles (app stores)	Lié à l'arborescence											(X)		

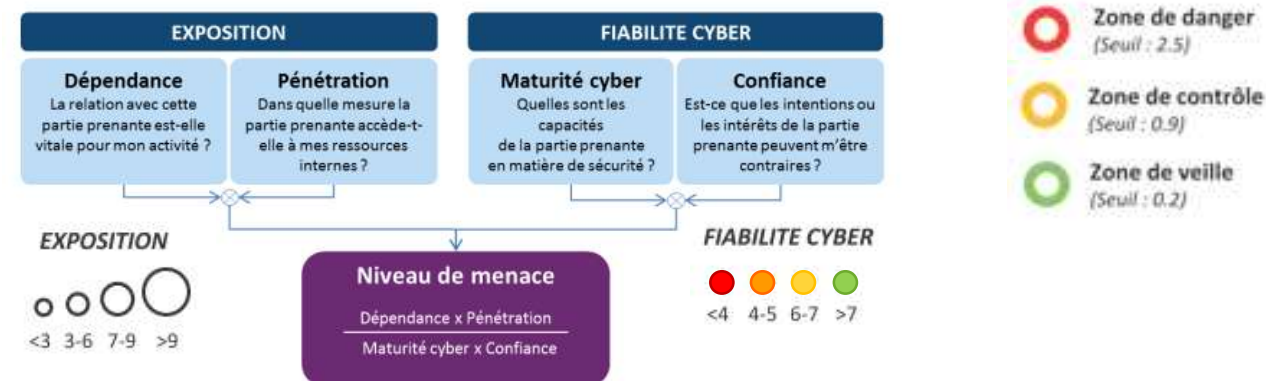
X : Support à la production

(X) : Support à l'intégration ou l'administration

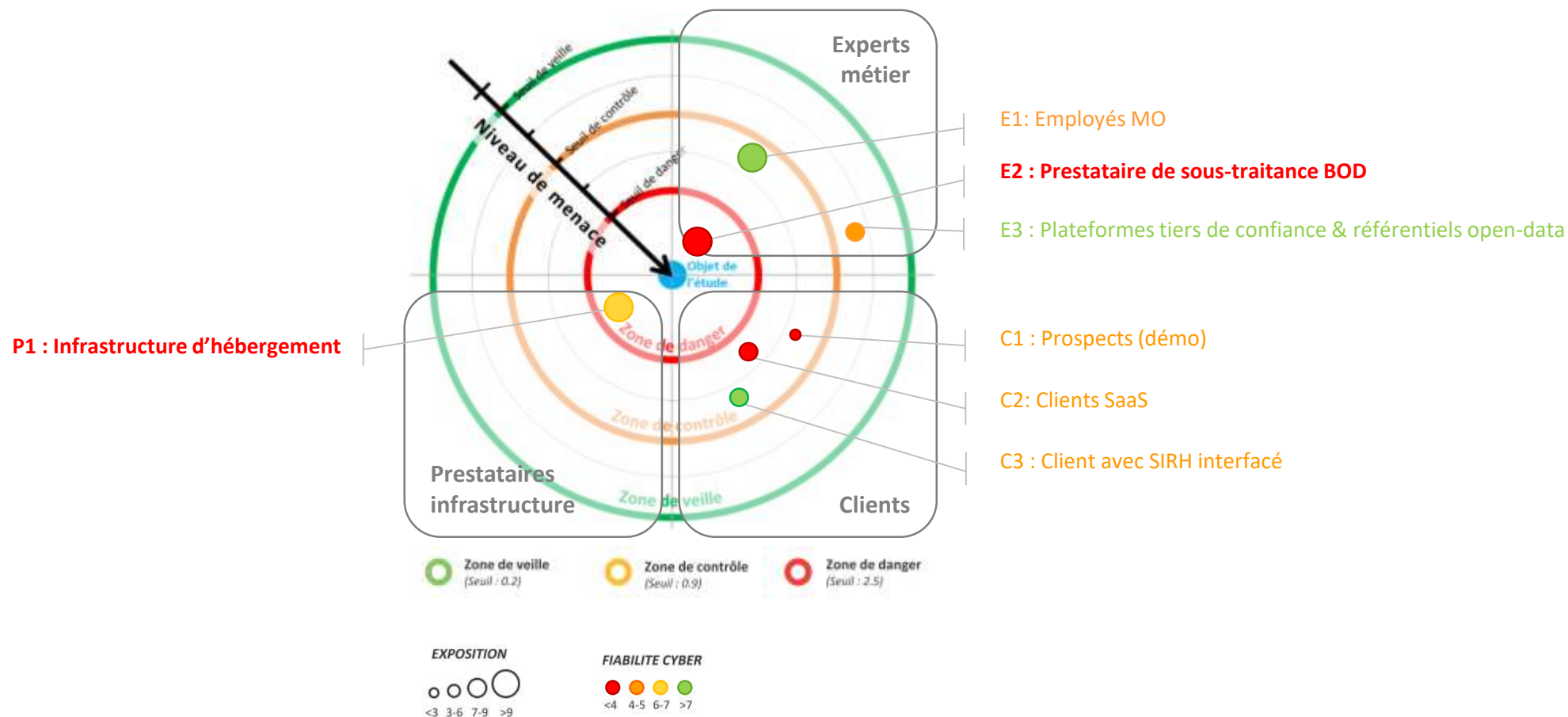
U : Support à l'utilisation

3a. évaluer le niveau de menace des parties prenantes

					Exposition / Fiabilité Cyber = Niveau de menace				
Catégorie	Index	Partie prenante	Dépendance fonctionnelle	Pénétration	Exposition	Maturité	Confiance	Fiabilité cyber	niv. de Menace
Client	C1	Prospects (Démonstration)	1	1	1 ○	1	1	1 ●	1
	C2	Clients SaaS	2	3	6 ○	1	3	3 ●	2
	C3	Client avec SIRH interfacé	2	3	6 ○	2	3	6 ●	1
Prestataires infrastructures	P1	Plateforme d'hébergement	4	4	16 ○	3	2	6 ●	2,7
Experts métiers	E1	Employés MO	4	3	12 ○	2	4	8 ●	1,5
	E2	Prestataires de sous-traitance BOD	3	4	12 ○	1	3	3 ●	4
	E3	Plateformes tiers de confiance & référentiels open-data	3	1	3 ○	2	2	4 ●	0,8

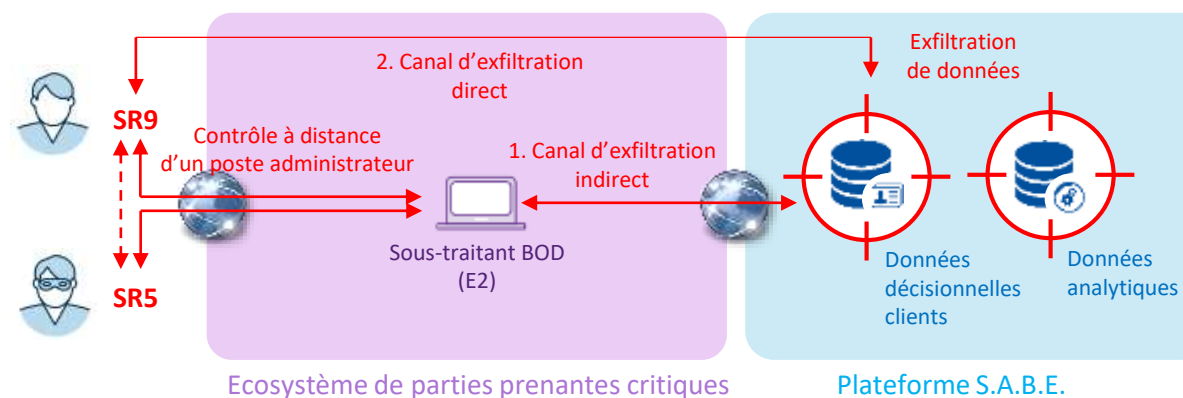


3a. sélectionner les parties prenantes critiques



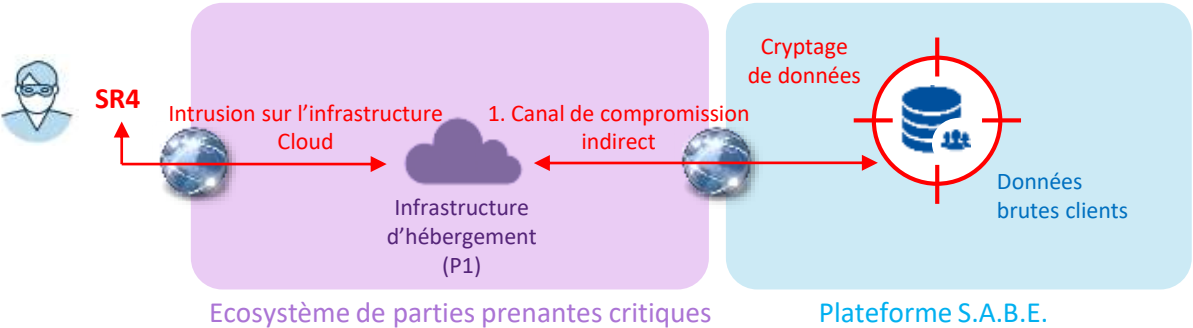
3b. élaborer des scénarios stratégiques (SR/OV/CAS)

Index	Source de Risque (SR)	Objectif Visé intermédiaire (OVi)	Objectif Visé (OV)	Scénario Chemin d'Attaque Stratégique (CAS)	ER	DIC	G
SST1	SR9 - Ex-partie prenante en quête de vengeance ou de profit SR5 - Organisation hacktiviste	OV5 - Divulgence de données	OV10 - Atteinte à l'image	Divulcation de données décisionnelles clients ou de données analytiques après exfiltration	ER101, ER102	C	4
				• 1. suite à une cyber-attaque ciblée indirecte via le sous-traitant BOD (E2)			
				• 2. suite à une cyber-attaque ciblée directe via usurpation de comptes d'accès clients (C2 / C3)			



3b. élaborer des scénarios stratégiques (SR/OV/CAS)

Index	Source de Risque (SR)	Objectif Visé intermédiaire (OVi)	Objectif Visé (OV)	Scénario Chemin d'Attaque Stratégique (CAS)	ER	DIC	G
SST2	SR4 - Organisation cybercriminelle	OV6 - Altération / Détournement de données	OV2 - Rançonnage	<div>Entrave au fonctionnement des e-services par cryptage de données brutes clients</div> <div><ul style="list-style-type: none">1. suite à une cyber-attaque opportuniste indirecte via l'infrastructure d'hébergement (P1)</div>	ER103	DI	3



3c. définir des mesures de sécurité sur l'écosystème

Catégorie	Index	Partie prenante	Scénario Chemin d'Attaque Stratégique (CAS)	Mesure de sécurité stratégique	niv. de Menace initial	niv. de Menace résiduel
Experts métiers	E2	Prestataires de sous-traitance BOD	SST1. Entrave au fonctionnement des e-services par cryptage de données brutes clients	Augmentation de la fiabilité cyber de la sous-traitance BOD en optant pour un contrat de service auprès d'une société localisée en zone UE (de facto soumise au RGPD) s'appuyant sur une due diligence en matière de sécurité de l'information au titre de l'auditabilité et intégrant des clauses de sécurité des développements et de protection des données applicable aux intervenants sur l'affaire Souscrire parallèlement à un contrat de cyberassurance en cas de cyber-attaque impactant les données clients de façon à couvrir les frais d'expertise et de défense en cas de procédure judiciaire	4	0,75
			• 1. suite à une cyber-attaque ciblée indirecte via le sous-traitant BOD (E2)			
Prestataires infrastructures	P1	Plateforme d'hébergement	SST2. Divulgateion de données décisionnelles clients ou de données analytiques après exfiltration	Augmentation de la fiabilité cyber de l'hébergeur Cloud en optant pour un contrat de service auprès d'une société certifiée ISO/IEC 27001 et CSA STAR et toujours localisée en zone UE	2,7	2
			• 1. suite à une cyber-attaque opportuniste indirecte via l'infrastructure d'hébergement (P1)			

Index	Dépendance fonctionnelle	X	Pénétration	=	Exposition	Maturité	X	Confiance	=	Fiabilité cyber	niv. de Menace résiduel	
P1	4		4		16	4	↑	2		8	↑	2
E2	3		4		12	4	↑	4	↑	16	↑	0,75

Exposition inchangée



< 2,5
< 0,9



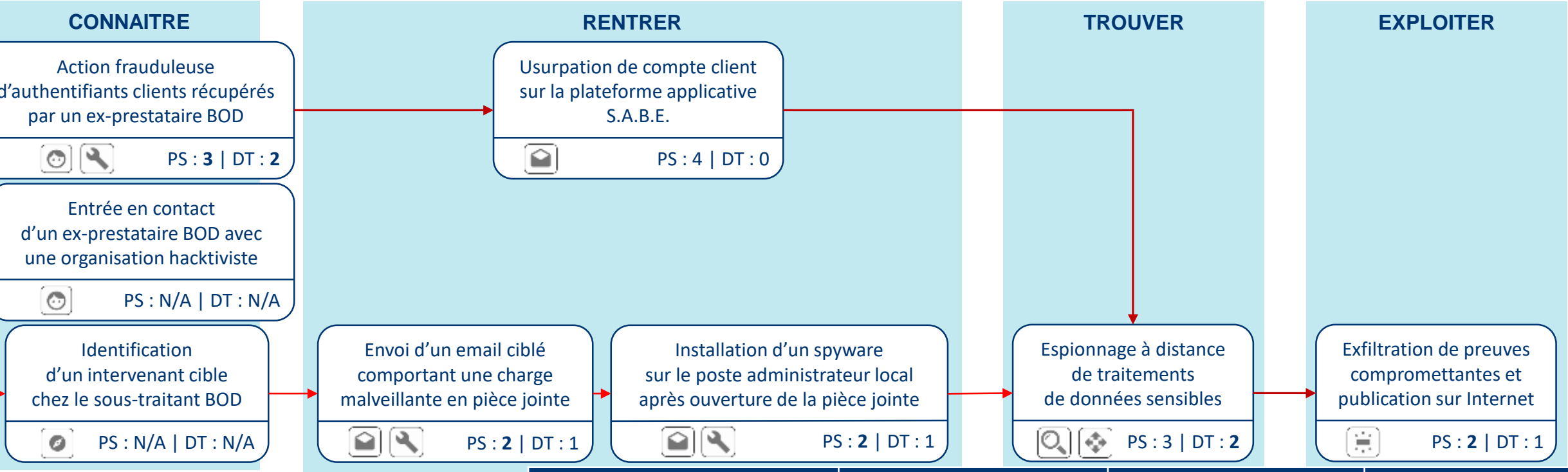
Atelier 4 : Scénarios opérationnels

ATELIER 4 - SCÉNARIOS OPÉRATIONNELS

- a. élaborer les scénarios opérationnels;
- b. évaluer leur vraisemblance.

4a. élaborer les scénarios opérationnels

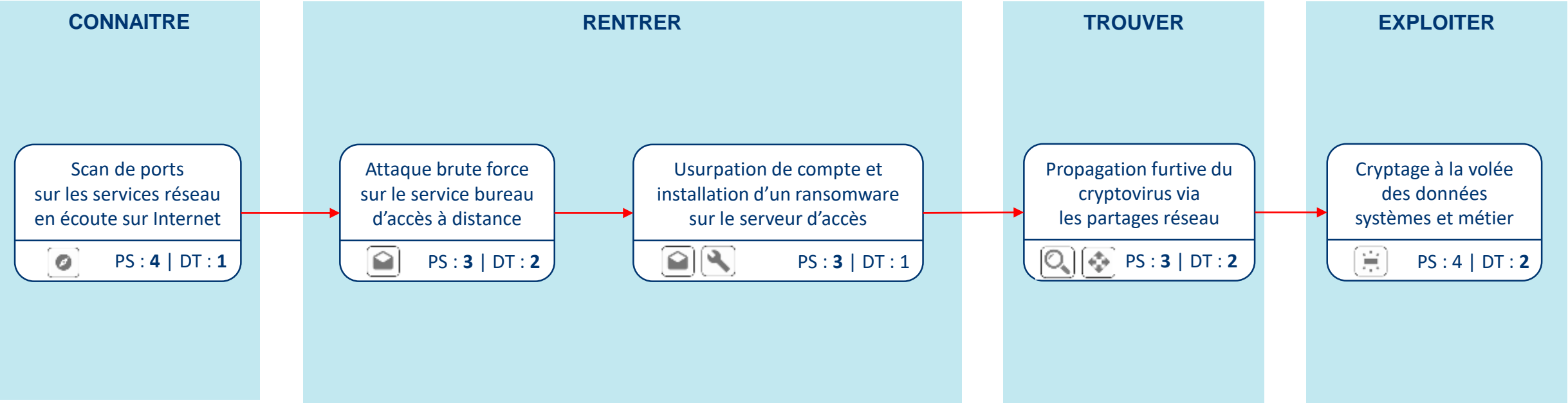
Index	Source de Risque (SR)	Objectif Visé intermédiaire (OVi)	Objectif Visé (OV)	Chemin d’Attaque Stratégique (CAS)
SST1	SR9 - Ex-partie prenante en quête de vengeance ou de profit SR5 - Organisation hacktiviste	OV5 - Divulgence de données	OV10 - Atteinte à l’image	Divulgence de données décisionnelles clients ou de données analytiques après exfiltration



Modes opératoires considérés (MO)	Probabilité de succès Min (PS)	Difficulté technique Max (DT)	Vraisemblance (V)
SST1 - MO1	3 - Très élevé	2 - Modéré	3 - Très vraisemblable
SST1 - MO2	2 - Significative	3 - Elevé	2 - Vraisemblable
Scénario global (Max)			3 - Très vraisemblable

4a. élaborer les scénarios opérationnels

Index	Source de Risque (SR)	Objectif Visé intermédiaire (OVi)	Objectif Visé (OV)	Chemin d’Attaque Stratégique (CAS)
SST2	SR4 - Organisation cybercriminelle	OV6 - Altération / Détournement de données	OV2 - Rançonnage	Entrave au fonctionnement des e-services par cryptage de données brutes clients



Modes opératoires considérés (MO)	Probabilité de succès Min (PS)	Difficulté technique Max (DT)	Vraisemblance (V)
SST2 - MO1	3 - Très élevé	2 - Modéré	3 - Très vraisemblable
Scénario global (Max)			3 - Très vraisemblable

4b. évaluer leur vraisemblance

Index	Source de Risque (SR)	Scénario Chemin d'Attaque Stratégique (CAS)	V
SST1	SR9 - Ex-partie prenante en quête de vengeance ou de profit SR5 - Organisation hacktiviste	Divulcation de données décisionnelles clients ou de données analytiques après exfiltration	3
		• 1. suite à une cyber-attaque ciblée indirecte via le sous-traitant BOD (E2)	3
		• 2. suite à une cyber-attaque ciblée directe via usurpation de comptes d'accès clients (C2 / C3)	2
SST2	SR4 - Organisation cybercriminelle	Entrave au fonctionnement des e-services par cryptage de données brutes clients	3
		• 1. suite à une cyber-attaque opportuniste indirecte via l'infrastructure d'hébergement (P1)	3



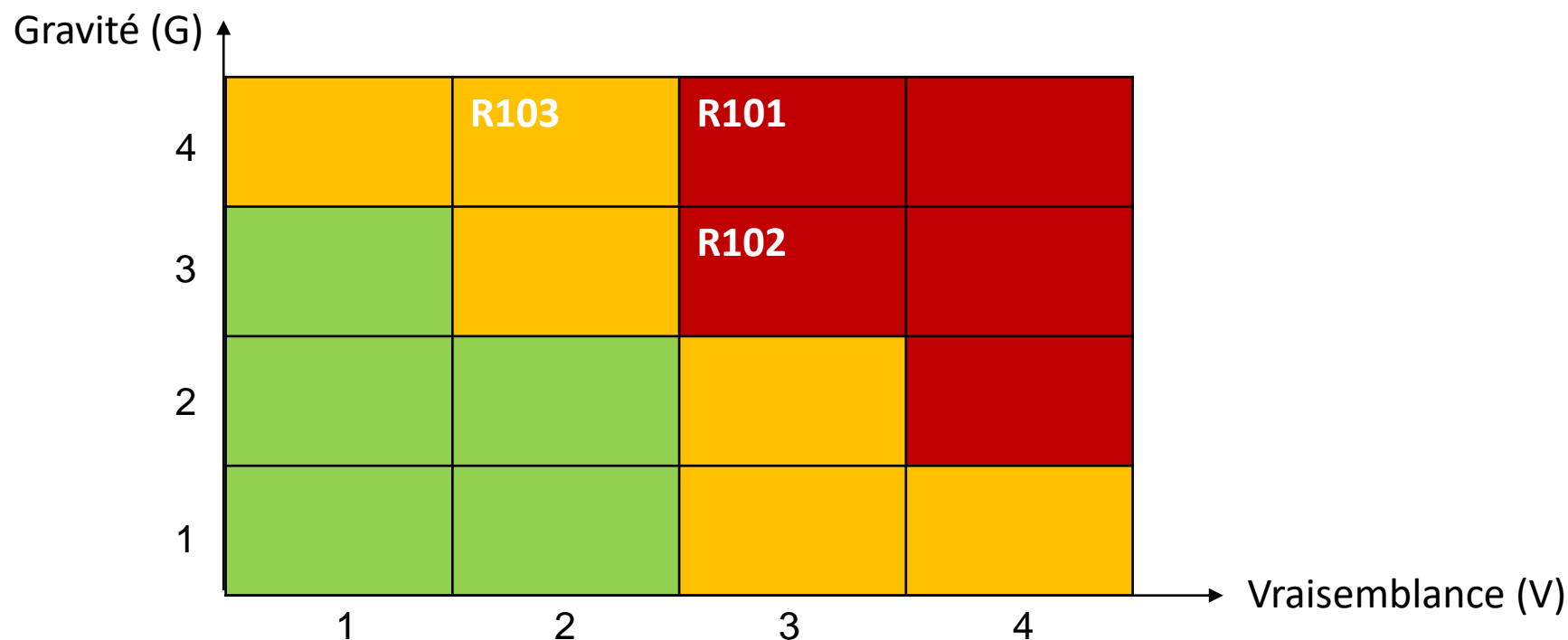
Atelier 5 : Traitement du risque

ATELIER 5 - TRAITEMENT DU RISQUE

- a. réaliser la synthèse des scénarios de risque ;
- b. définir la stratégie de traitement du risque et les mesures de sécurité ;
- c. évaluer et documenter les risques résiduels ;
- d. mettre en place le cadre de suivi des risques.

5a. réaliser la synthèse des scénarios de risque

Index	Descriptif	SST CAS	V	G	R
R101	Divulgarion de données décisionnelles clients ou de données analytiques après exfiltration suite à une cyber-attaque ciblée indirecte menée par une organisation hacktiviste en lien avec un ex-prestataire, via le sous-traitant BOD	SST1 1	3	4	4
R102	Entrave au fonctionnement des e-services par cryptage de données brutes clients suite à une cyber-attaque opportuniste indirecte menée par une organisation cybercriminelle via l'infrastructure d'hébergement	SST2 1	3	3	4
R103	Divulgarion de données décisionnelles clients ou de données analytiques après exfiltration suite à une cyber-attaque ciblée directe menée par un ex-prestataire via usurpation de comptes d'accès clients	SST1 2	2	4	3



5b. définir la stratégie de traitement du risque et les mesures de sécurité



Index	Mesure de sécurité	Scénarios de risques associés	Responsable	Freins / difficultés de mise en œuvre	Coût / Complexité	Échéance	Statut
Gouvernance							
MSG1	Choisir un contrat de service pour la sous-traitance BOD auprès d'une société localisée en zone UE. Formaliser un plan assurance sécurité précisant les règles de sécurité organisationnelles et techniques appliquées	R101, R103	DM, DPO, RSSI	Anticiper la fin de contrat avec le sous-traitant actuel	++	12 mois	A planifier
MSG2	Pour le choix de l'hébergeur Cloud, exiger la certification ISO/IEC 27001, voire CSA STAR et que les données traitées soient toujours localisées en zone UE	R101, R103	DT, RSSI, DPO	Anticiper la fin de contrat avec l'hébergeur actuel	++	9 mois	En cours
MSG3	Intégrer des clauses de sécurité dans les contrats avec l'ensemble des prestataires (auditabilité, confidentialité, incidents de sécurité, etc.)	R101, R102, R103	DM, DT, RSSI	Effectué au fil de l'eau à la renégociation des contrats	++	12 mois	A planifier
MSG4	Souscrire à un contrat de cyberassurance en cas de cyber-attaque impactant les données clients	R101, R102, R103	DG, RSSI	Faire une étude de marché pour évaluer les différentes solutions	++	6 mois	En cours
MSG5	Mise en place de CGU (Conditions Générales d'Utilisation) applicables aux utilisateurs clients et d'une charte administrateur opposables	R101, R103	DM, DT, RSSI, DPO	Faire valider la licéité du contenu auprès d'un cabinet d'avocat spécialisé	+	6 mois	En cours
MSG6	Mise en place d'une procédure de notification d'incident de sécurité vers les entreprises clientes	R101, R102, R103	DPO, RSSI	A intégrer dans la gestion des incidents de sécurité (MSG3)	++	6 mois	En cours
MSG7	Audit de sécurité organisationnel des prestataires assurant l'hébergement cloud et le BOD. Mise en place et suivi des plans d'action correctifs	R101, R102, R103	RSSI	Acceptation de la démarche par les prestataires (MSG1, MSG2 et MSG3)	+++	18 mois	A planifier

5b. définir la stratégie de traitement du risque et les mesures de sécurité

Index	Mesure de sécurité	Scénarios de risques associés	Responsable	Freins / difficultés de mise en œuvre	Coût / Complexité	Échéance	Statut
Protection							
MSP1	Chiffrer en natif les mots de passe clients stockés et lors de l'authentification	R103	DT	Gestion des clés de chiffrement	++	3 mois	Implémenté
MSP2	Définir une politique de gestion des mots de passe utilisateurs (complexité, renouvellement, ...)	R102, R103	DM, DT, RSSI	Réticence des clients	+	6 mois	A planifier
MSP3	Mettre en place une notification d'alerte (email) vers l'utilisateur légitime si une connexion est établie avec son compte depuis une nouvelle adresse P	R102	DM	Mettre en place un système de gestion des événements de sécurité (MSD2)	++	9 mois	En cours
MSP4	Mettre en place une solution de Sandboxing pour analyser préventivement les emails entrants et PJ	R101	DT	Etude de faisabilité à diligenter auprès de l'hébergeur cloud	++	6 mois	En cours
Défense							
MSD1	Souscrire à un service SOC pour la surveillance des flux par une sonde IDS, l'analyse et la corrélation des journaux d'événements par un SIEM	R101, R102, R103	DM, DT, RSSI	Etude de faisabilité à diligenter auprès de l'hébergeur cloud	+++	18 mois	A planifier
MSD2	Mettre en place un bastion d'administration avec authentification forte (OTP, certificats, ...) pour sécuriser les accès à distance	R102, R103	DT	Réticence des administrateurs	++	9 mois	A planifier
Résilience							
MSR1	Mettre en place un dispositif de sauvegarde cloisonné par rapport au réseau de production, avec tests de restauration réguliers	R102	DT	A intégrer dans le contrat d'hébergement (MSG2)	++	9 mois	En cours

5b. définir la stratégie de traitement du risque et les mesures de sécurité

R101 - Divulgarion de données décisionnelles clients ou de données analytiques après exfiltration suite à une cyber-attaque ciblée indirecte (via le sous-traitant BOD)

Description et analyse du risque résiduel :

- Sans objet

Évènements redoutés concernés :

- ER101 : Divulgarion de données décisionnelles liées au management des ressources humaines
- ER102 : Divulgarion de données techniques de paramétrage

Mesures de traitement du risques complémentaires :

- Gouvernance : MSG1, MSG2, MSG3, MSG4, MSG5, MSG6, MSG7
- Protection : MSP4
- Détection : MSD1
- Résilience : N/A

Évaluation du risque résiduel :

	Gravité	Vraisemblance	→ Niveau de risque
Initial	4	3	3
Résiduel	4	2	2

Gestion du risque résiduel :

- Sans objet

5b. définir la stratégie de traitement du risque et les mesures de sécurité

R102 - Entrave au fonctionnement des e-services par cryptage de données brutes clients suite à une cyber-attaque opportuniste indirecte (via l'infrastructure d'hébergement)

Description et analyse du risque résiduel :

- Sans objet

Évènements redoutés concernés :

- ER103 : Altération des données brutes clients liées au management des ressources humaines

Mesures de traitement du risques complémentaires :

- Gouvernance : MSG3, MSG4, MSG6, MSG7
- Protection : MSP3, MSP4
- Détection : MSD1, MSD2
- Résilience : MSR1

Évaluation du risque résiduel :

	Gravité	Vraisemblance	→ Niveau de risque
Initial	3	3	3
↓ Résiduel	2	2	1

Gestion du risque résiduel :

- Sans objet

5b. définir la stratégie de traitement du risque et les mesures de sécurité

R103 - Divulgaration de données décisionnelles clients ou de données analytiques après exfiltration suite à une cyber-attaque ciblée directe (par un ex-prestataire via usurpation de comptes d'accès clients)

Description et analyse du risque résiduel :

- Sans objet

Évènements redoutés concernés :

- ER101 : Divulgaration de données décisionnelles liées au management des ressources humaines
- ER102 : Divulgaration de données techniques de paramétrage

Mesures de traitement du risques complémentaires :

- Gouvernance : MSG1, MSG2, MSG3, MSG4, MSG5, MSG6, MSG7
- Protection : MSP1, MSP2
- Détection : MSD1, MSD2
- Résilience : N/A

Évaluation du risque résiduel :

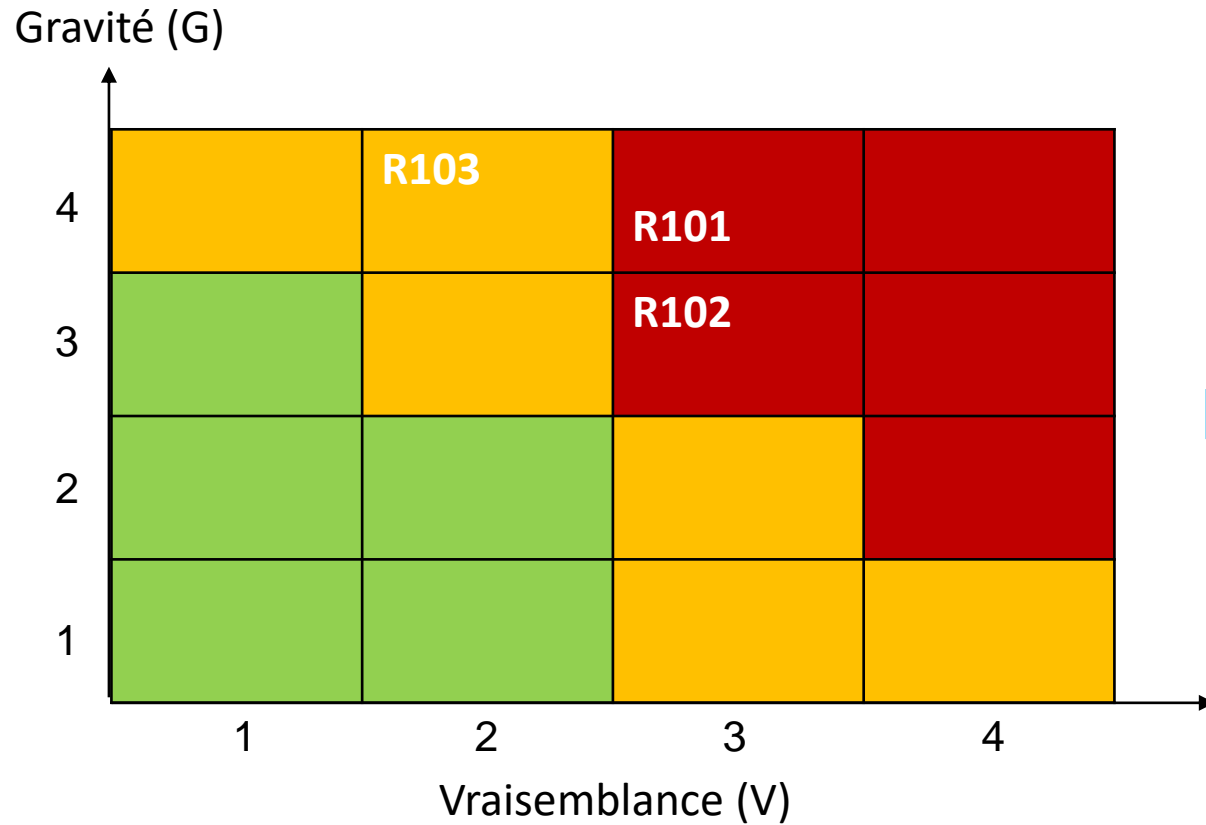
	Gravité	Vraisemblance	→ Niveau de risque
Initial	4	2	2
Résiduel	4	1	2

Gestion du risque résiduel :

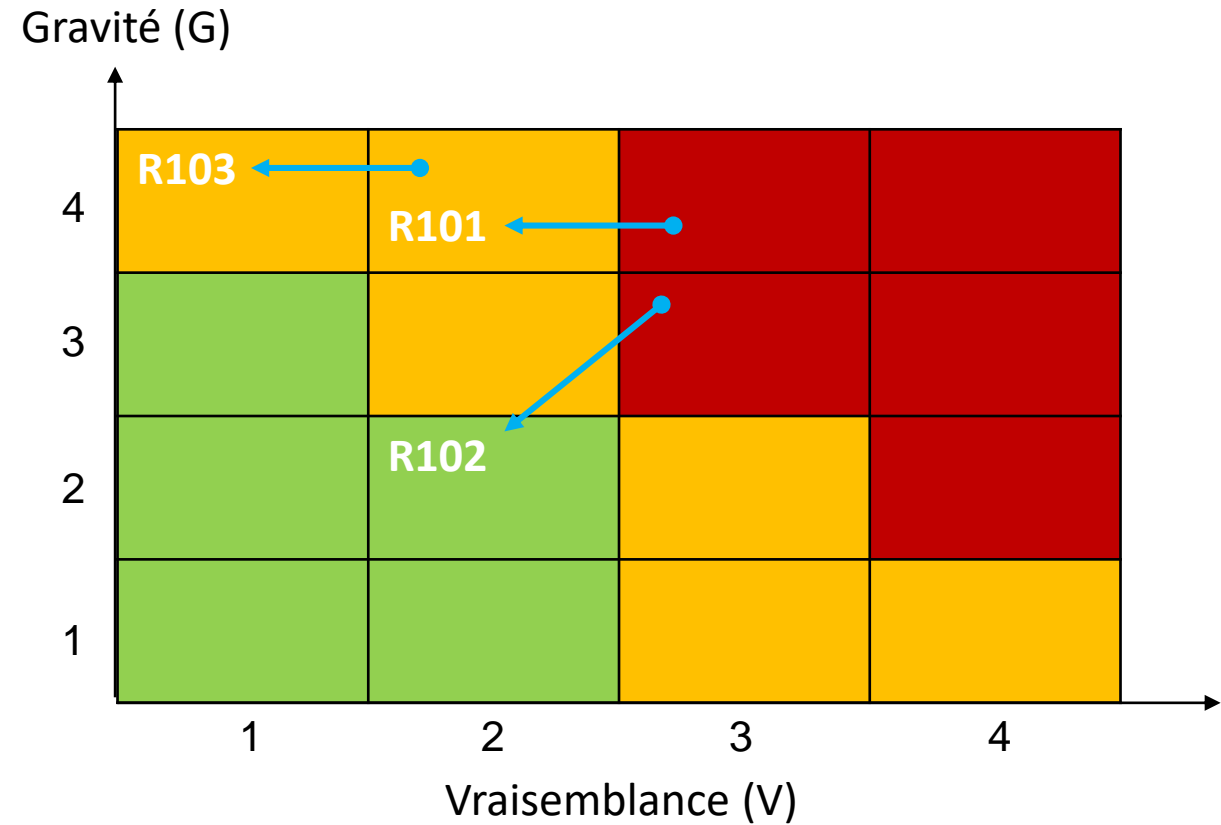
- Sans objet

5c. Évaluer et documenter les risques résiduels

Cartographie des risques nets
(avant traitement)



Cartographie des risques résiduels
(après traitement)



5d. mettre en place le cadre de suivi des risques

**Plan d'action de mise en œuvre opérationnelle (spécifications fonctionnelles)
/ Plan d'assurance des services externalisés (clauses contractuelles)**

[illegible]

5d. mettre en place le cadre de suivi des risques

Veille/Détection/Suivi de **vulnérabilités**, constats d'audit et actions de traitement correctif/palliatif

				Bases de vulnérabilités										Critères de traitement des vulnérabilités																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
Label	Intitulé	Précisions	Biens supports concernés	Editeur	CVE ID	CWE ID	OWASP VC	D	I	C	L	SM																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			
VT.2014-04-11.01	HeartBleed	Vulnérabilité logicielle	DT-NG.SABE.IN DT-NG.SABE.OUT		CVE-2014-0160	CWE-130 CWE-126	VC17				X																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																				

5d. mettre en place le cadre de suivi des risques

Détection/Notification/Suivi des **incidents** et actions de résolution

Label	Intitulé	Précisions	Biens supports impliqués	CAPEC ID	WASC ID	D	I	C	L	SRC	MEN	VUL	SM	ER	PRE	PRO	REC
INC-2017-05-23.01	Déni de service par DNS Cache Poisoning	Résolution inopér	DNS.SVC	CAPEC-142	WASC-10	X				CYB	C08.T07		SM10	ER01		X	



Annexes : Métriques et catalogues

Correspondance entre terminologies EBIOS 2010 et EBIOS RM

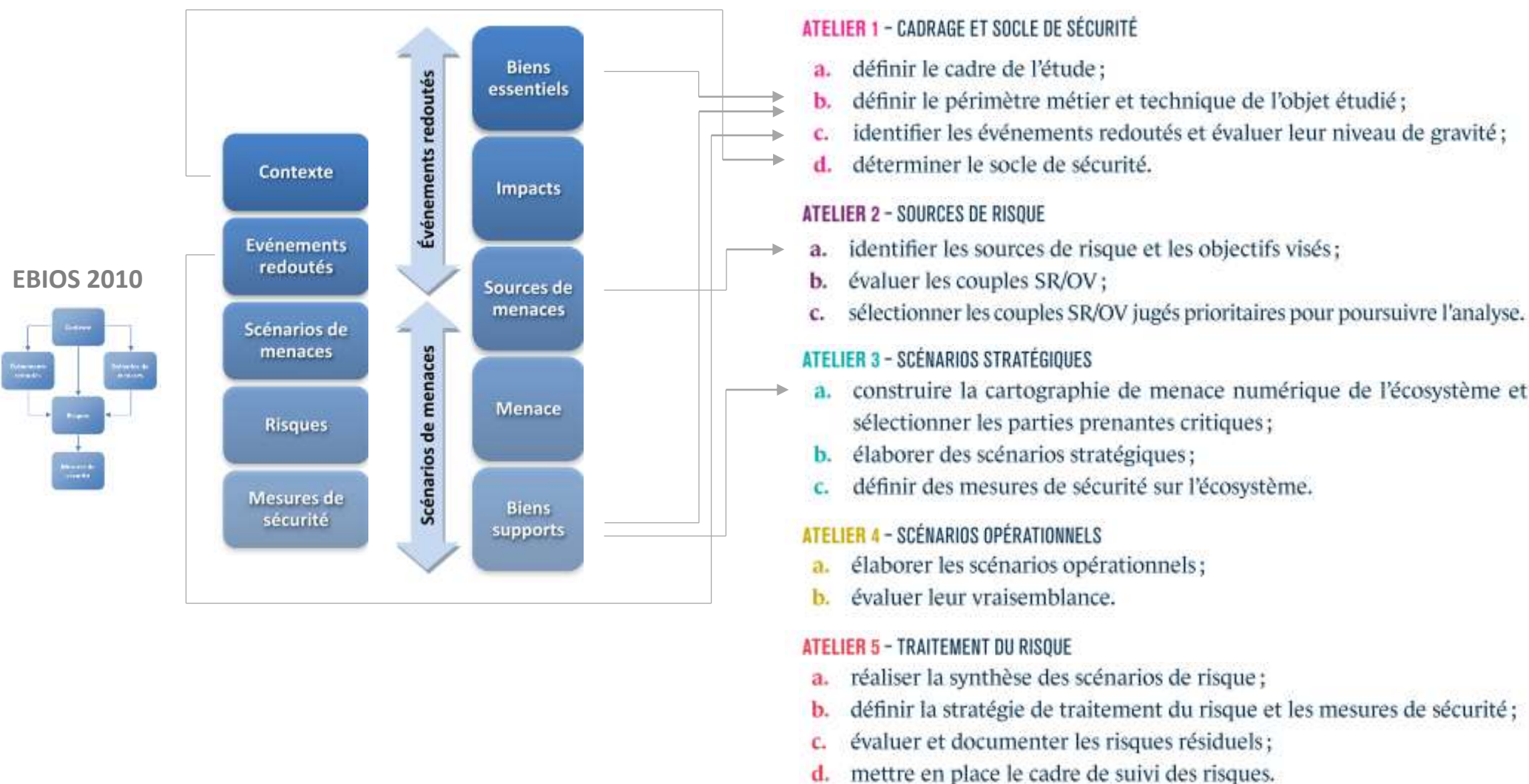
EBIOS 2010



Sigle	Terminologie EBIOS 2010	Sigle	Terminologie EBIOS RM
D, I, C, ...	Critère ou besoin de sécurité	D, I, C, ...	Critère ou besoin de sécurité
BE	Bien essentiel	VM	Valeur métier
BS	Bien support	BS	Bien support
ER	Evènement redouté	ER	Evènement redouté
G / I	Gravité des impacts	G / I	Gravité des impacts
SM	Source de menace	SR	Source de risque
		OV	Objectif visé
			Pertinence
PP	Partie prenante	PP	Partie prenante sur l'écosystème
		PPC	Partie prenante critique
		SST	Scénario stratégique
		CAS	Chemin d'attaque [stratégique]
MSx	Mesure de sécurité [générique]	MSE	Mesure de sécurité sur l'écosystème
VUL	Vulnérabilité	VUL	Vulnérabilité
SM	Scénario de menace	SOP	Scénario opérationnel
M	Menace	AE	Action élémentaire
		EI	Evènement intermédiaire
		MO	Mode opératoire
		V	Vraisemblance
R	Risque	R	Scénario de risque
MSx	Mesure de sécurité [générique]	MSx	Mesure de sécurité [sur le système]



Articulation entre la démarche EBIOS 2010 (outputs) et la démarche EBIOS RM (inputs)



Echelle de gravité des impacts

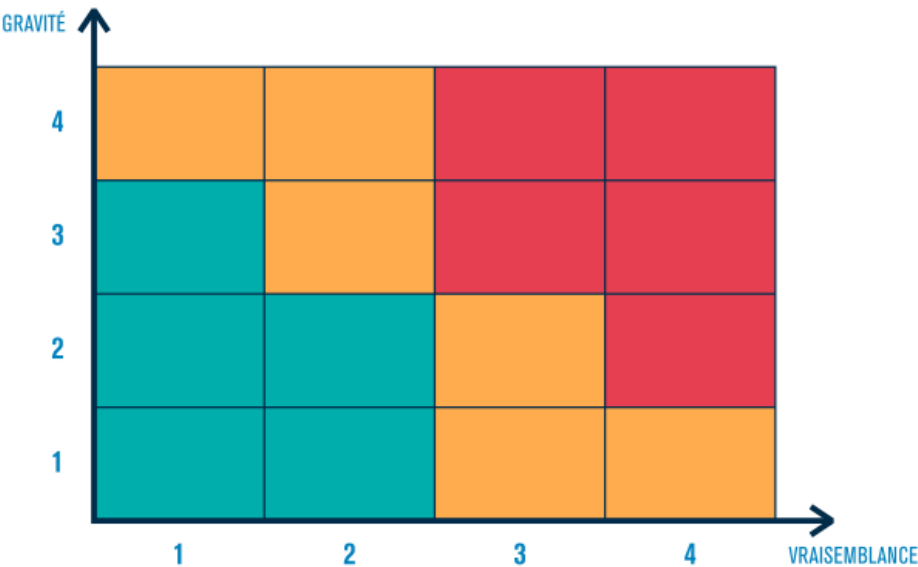
NIVEAU DE L'ÉCHELLE	DÉFINITION
G4 – CRITIQUE	<p>Conséquences désastreuses pour l'organisation avec d'éventuels impacts sur l'écosystème.</p> <p>Incapacité pour l'organisation d'assurer la totalité ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. L'organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d'activité ou étatiques dans lesquels elle opère seront susceptibles d'être légèrement impactés, sans conséquences durables.</p>
G3 – GRAVE	<p>Conséquences importantes pour l'organisation.</p> <p>Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. L'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique.</p>
G2 – SIGNIFICATIVE	<p>Conséquences significatives mais limitées pour l'organisation.</p> <p>Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. L'organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).</p>
G1 – MINEURE	<p>Conséquences négligeables pour l'organisation.</p> <p>Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. L'organisation surmontera la situation sans trop de difficultés (consommation des marges).</p>

IMPACT	EXEMPLES (LISTE NON EXHAUSTIVE)
IMPACTS SUR LES MISSIONS ET SERVICE DE L'ORGANISATION	
CONSEQUENCES DIRECTES OU INDIRECTES SUR LA RÉALISATION DES MISSIONS ET SERVICES	Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé.
IMPACTS HUMAINS, MATÉRIELS OU ENVIRONNEMENTAUX	
IMPACTS SUR LA SÉCURITÉ OU SUR LA SANTÉ DES PERSONNES CONSEQUENCES DIRECTES OU INDIRECTES SUR L'INTÉGRITÉ PHYSIQUE DE PERSONNES	Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire.
IMPACTS MATÉRIELS DÉGÂTS MATÉRIELS OU DESTRUCTION DE BIENS SUPPORTS	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels.
IMPACTS SUR L'ENVIRONNEMENT CONSEQUENCES ÉCOLOGIQUES À COURT OU LONG TERME, DIRECTES OU INDIRECTES	Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère.
IMPACTS SUR LA CAPACITÉ DE DÉVELOPPEMENT OU DE DÉCISION CONSEQUENCES DIRECTES OU INDIRECTES SUR LA LIBERTÉ DE DÉCIDER, DE DIRIGER, DE METTRE EN ŒUVRE LA STRATÉGIE DE DÉVELOPPEMENT	Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisation, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés.
IMPACTS SUR LE LIEN SOCIAL INTERNE CONSEQUENCES DIRECTES OU INDIRECTES SUR LA QUALITÉ DES LIENS SOCIAUX AU SEIN DE L'ORGANISATION	Perte de confiance des employés dans la pérennité de l'organisation, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, perte de sens des valeurs communes.
IMPACTS SUR LE PATRIMOINE INTELLECTUEL OU CULTUREL CONSEQUENCES DIRECTES OU INDIRECTES SUR LES CONNAISSANCES NON-EXPLICITES ACCUMULÉES PAR L'ORGANISATION, SUR LE SAVOIR-FAIRE, SUR LES CAPACITÉS D'INNOVATION, SUR LES RÉFÉRENCES CULTURELLES COMMUNES	Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés.
IMPACTS FINANCIERS	
CONSEQUENCES PÉCUNIAIRES, DIRECTES OU INDIRECTES	Perte de chiffre d'affaires, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées.
IMPACTS JURIDIQUES	
CONSEQUENCES SUITE À UNE NON-CONFORMITÉ LÉGALE, RÉGLEMENTAIRE, NORMATIVE OU CONTRACTUELLE	Procès, amende, condamnation d'un dirigeant, amendement de contrat.
IMPACTS SUR L'IMAGE ET LA CONFIANCE	
CONSEQUENCES DIRECTES OU INDIRECTES SUR L'IMAGE DE L'ORGANISATION, LA NOTORIÉTÉ, LA CONFIANCE DES CLIENTS	Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte de notoriété, perte de confiance d'usagers.

Echelle de vraisemblance globale de scénario opérationnel

NIVEAU DE L'ÉCHELLE	DESCRIPTION
V4 – QUASI-CERTAIN	La source de risque va très certainement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est très élevée.
V3 – TRÈS VRAISEMBLABLE	La source de risque va probablement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est élevée.
V2 – VRAISEMBLABLE	La source de risque est susceptible d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est significative.
V1 – PEU VRAISEMBLABLE	La source de risque a relativement peu de chances d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est faible.

Matrice de criticité du risque



Niveau de risque et acceptabilité du risque

NIVEAU DE RISQUE	ACCEPTABILITÉ DU RISQUE	INTITULÉ DES DÉCISIONS ET DES ACTIONS
Faible	Acceptable en l'état	Aucune action n'est à entreprendre
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme
Élevé	Inacceptable	Des mesures de réduction du risque doivent impérativement être prises à court terme. Dans le cas contraire, tout ou partie de l'activité sera refusé

BIEN SUPPORT	EXEMPLES (LISTE NON EXHAUSTIVE)
SYSTÈMES INFORMATIQUES ET DE TÉLÉPHONIE	
MATÉRIELS	
TERMINAL UTILISATEUR	Ordinateur fixe, ordinateur portable, tablette, téléphone mobile.
PÉRIPHÉRIQUE	Imprimante, scanner, clavier, souris, caméra, microphone, objet connecté.
TÉLÉPHONE	Téléphone fixe ou mobile analogique ou IP.
ÉQUIPEMENT DE STOCKAGE	Clé USB, disque dur, CD-ROM, carte mémoire.
SERVEUR	Mainframe, serveur lame, serveur rack.
MOYEN D'ADMINISTRATION	Poste d'administration, serveur outils d'administration, bastion.
ÉQUIPEMENT RÉSEAU	Commutateur, routeur, passerelles d'entrée depuis l'extérieur, borne Wi-Fi.
ÉQUIPEMENT DE SÉCURITÉ	Pare-feu, sonde (IDS/IPS), passerelle VPN.
ÉQUIPEMENT INDUSTRIEL	Automate programmable industriel, capteur, actionneur, système SCADA, système instrumenté de sécurité.
LOGICIELS	
SERVICE D'INFRASTRUCTURE	Service d'annuaire, service de gestion d'adresse IP (DHCP), service de nom de domaine (DNS), contrôleur de domaine, serveur d'impression.
APPLICATION/SERVICE APPLICATIF	Serveur web, service web, serveur d'application, serveur de courrier électronique, serveur de bases de données, progiciels (RH, relation client, ERP).
INTERGICIEL (MIDDLEWARE)	Enterprise Application Integration (EAI), Extract-Transform-Load (ETL), Open DataBase Connectivity (ODBC).
SYSTÈME D'EXPLOITATION, HYPERVISEUR	Windows, Linux, MacOS, Xen.
MICROGICIEL (FIRMWARE)	Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur.
LOGICIEL DE SÉCURITÉ	Outil de gestion d'événements Security Information and Event Management (SIEM).
RÉSEAUX/CANaux INFORMATIQUES ET DE TÉLÉPHONIE	
RÉSEAU/CANAL INFORMATIQUE	Câble réseau, fibre optique, liaison radio (Wi-Fi, Bluetooth, etc.).
RÉSEAU/CANAL TÉLÉPHONIQUE	Ligne téléphonique.

BIEN SUPPORT	EXEMPLES (LISTE NON EXHAUSTIVE)
ORGANISATIONS	
PERSONNE	Employé, stagiaire, prestataire, personnel d'entretien.
SUPPORT PAPIER	Document manuscrit ou imprimé.
ÉCHANGE VERBAL	Réunion, échange informel.
ÉLÉMENT D'INGÉNIERIE SOCIALE	Information partagée sur les réseaux sociaux.
LOCAUX ET INSTALLATIONS PHYSIQUES	
SITE/BÂTIMENT/SALLE	Siège social, usine, site de stockage, bâtiment industriel, salle de réunion, salle serveur.
SYSTÈME DE SÉCURITÉ PHYSIQUE	Système d'accès par badge, système de détection d'intrusion, système de vidéo-protection.
SYSTÈME DE SÛRETÉ DE FONCTIONNEMENT	Climatisation, sécurité incendie, alimentation électrique.

CATÉGORIES DE SOURCES DE RISQUE

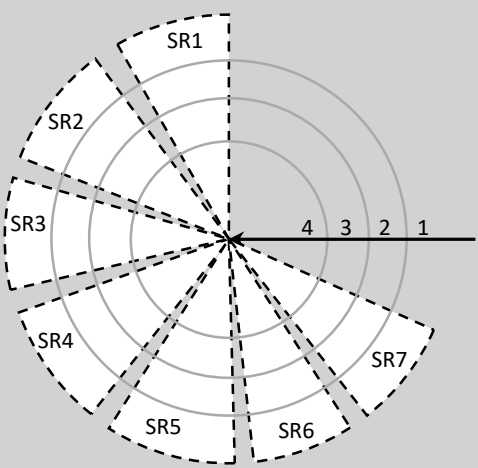
PROFILS D'ATTAQUANTS	EXEMPLES ET MODÈS OPÉRATOIRES HABITUELS
ÉTATIQUE	États, agences de renseignement. Attaques généralement conduites par des professionnels, respectant un calendrier et un mode opératoire prédéfinis. Ce profil d'attaquant se caractérise par sa capacité à réaliser une opération offensive sur un temps long (ressources stables, procédures) et à adapter ses outils et méthodes à la topologie de la cible. Par extension, ces acteurs ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day) et certains sont capables d'infiltrer des réseaux isolés et de réaliser des attaques successives pour atteindre une ou des cibles (par exemple au moyen d'une attaque visant la chaîne d'approvisionnement).
CRIME ORGANISÉ	Organisations cybercriminelles (mafias, gangs, officines). Attaque en ligne ou au président, demande de rançon ou attaque par rançongiciel, exploitation de réseaux de « machines robots » (botnet), etc. En raison notamment de la prolifération de kits d'attaques facilement accessibles en ligne, les cybercriminels mènent des opérations de plus en plus sophistiquées et organisées à des fins lucratives ou de fraude. Certains ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day).
TERRORISTE	Cyberterroristes, cybermilitants. Attaques habituellement peu sophistiquées mais menées avec détermination à des fins de destabilisation et de destruction : déni de service (visant par exemple à rendre indisponibles les services d'urgence d'un centre hospitalier, accès Internet d'un système industriel de production d'énergie), exploitation de vulnérabilités de sites Internet et de données.
ACTIVISTE IDÉOLOGIQUE	Cyberhacktivistes, groupements d'intérêt, sectes. Modèles opératoires et sophistication des attaques relativement similaires à ceux des cyberterroristes mais motivés par des intentions moins destructrices. Certains acteurs ont mené ces attaques pour véhiculer une idéologie, un message (exemple : utilisation massive des réseaux sociaux comme canal de résistance).
OFFICINE SPÉCIALISÉE	Profil de « cybermercenaire » doté de capacités informatiques généralement élevées sur le plan technique. Il est de ce fait à distinguer des script-kiddies avec qui il partage toutefois l'esprit de défi et la quête de reconnaissance mais avec un objectif lucratif. De tels groupes peuvent s'organiser en officines spécialisées proposant de véritables services de piratage. Ce type de hacker chevronné est souvent à l'origine de la conception et de la création d'outils et kits d'attaques « accessibles en ligne (éventuellement payants) » qui sont ensuite utilisables « clés en main » par d'autres groupes d'attaquants. Il n'a pas de motivations particulières autres que le gain financier.
AMATEUR	Profil du hacker « script-kiddie » ou doté de bonnes connaissances informatiques, et motivé par une quête de reconnaissance sociale, d'amusement, de défi. Attaques basiques mais capacité à utiliser les kits d'attaques accessibles en ligne.
VENGEUR	Les motivations de ce profil d'attaquant sont guidées par un esprit de vengeance aiguë ou un sentiment d'injustice (exemples : salarié licencié pour faute grave, prestataire mécontent suite au non-renouvellement d'un marché, etc.). Ce profil d'attaquant se caractérise par sa détermination et sa connaissance intime des systèmes et processus organisationnels. Cela peut le rendre redoutable et lui conférer un pouvoir de nuisance important.
MALVEILLANT PATHOLOGIQUE	Les motivations de ce profil d'attaquant sont d'ordre pathologique ou opportuniste et parfois guidées par l'appât du gain (exemples : concurrent déloyal, client mécontent, escroc, fraudeur). Ici, soit l'attaquant dispose d'un socle de connaissances en informatique qui l'amène à tenter de compromettre le SI de sa cible, soit il exploite par lui-même des kits d'attaques disponibles en ligne, soit il décide de sous-traiter l'attaque informatique en faisant appel à une officine spécialisée. Dans certains cas, l'attaquant peut porter son attention sur une source interne (salarié mécontent, prestataire peu scrupuleux) et tenter de la corrompre.

CATÉGORIES D'OBJECTIFS VISÉS

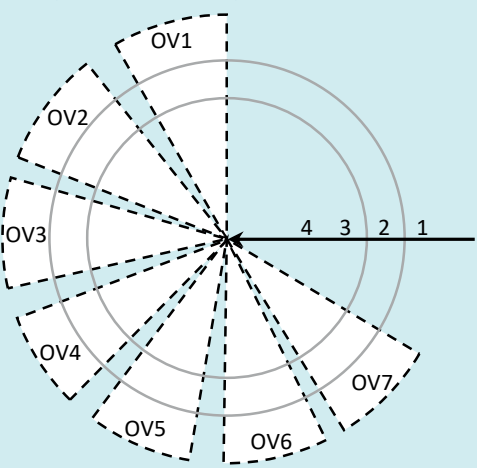
INTENTIONS POURSUIVIES	DESCRIPTION
ESPIONNAGE	Opération de renseignement (étatique, économique). Dans de nombreux cas, l'attaquant s'insère durablement dans le système d'information et en toute discrétion, l'armement, le spatial, l'aéronautique, le secteur pharmaceutique, l'énergie ou encore certaines activités de l'État (économie, finances, affaires étrangères) constituent des cibles privilégiées.
PRÉPOSITIONNEMENT STRATÉGIQUE	Prépositionnement visant généralement une attaque sur le long terme, sans que la finalité poursuivie soit clairement établie (exemples : compromission de réseaux d'opérateurs de télécommunication, infiltration de sites Internet d'information de masse pour lancer une opération d'influence politique ou économique à fort écho). La compromission soudaine et massive d'ordinateurs afin de constituer un réseau de robots peut être affiliée à cette catégorie.
INFLUENCE	Opération visant à diffuser de fausses informations ou à les adhérer, mobiliser les leaders d'opinion sur les réseaux sociaux, détruire des réputations, divulguer des informations confidentielles, dégrader l'image d'une organisation ou d'un État. La finalité est généralement la destabilisation ou la modification des perceptions.
ENTRAVE AU FONCTIONNEMENT	Opération de sabotage visant par exemple à rendre indisponible un site Internet, à provoquer une saturation informationnelle, à empêcher l'usage d'une ressource numérique, à rendre indisponible une installation physique. Les systèmes industriels peuvent être particulièrement exposés et vulnérables au travers des réseaux informatiques auxquels ils sont interconnectés (exemple : envoi de commandes afin de générer un dommage matériel ou une panne nécessitant une maintenance lourde). Les attaques en déni de service distribué (DDoS) sont des techniques largement utilisées pour neutraliser des ressources numériques.
LUCRATIF	Opérations visant un gain financier, de façon directe ou indirecte. Généralement liée au crime organisé, on peut citer : escroquerie sur Internet, blanchiment d'argent, extorsion ou détournement d'argent, manipulation de marchés financiers, falsification de documents administratifs, usurpation d'identité, etc. Il est à noter que certaines opérations à but lucratif peuvent recourir à un mode opératoire relevant des catégories ci-dessus (exemple : espionnage et vol de données, rançongiciel pour neutraliser une activité) mais l'objectif final reste financier.
DÉPL. AMUSEMENT	Opération visant à réaliser un exploit à des fins de reconnaissance sociale, de défi ou de simple amusement. Même si l'objectif est essentiellement ludique et sans volonté particulière de nuire, ce type d'opération peut avoir de lourdes conséquences pour la victime.



IDENTIFICATION		COTATION			CARACTÉRISATION				ÉVALUATION	
Source de risque (SR)	Objectif visé (OV)	Motivation	Ressources	Activité	Modèles opératoires	Sec-teurs d'activités	Arsenal d'attaque	Faits d'armes	Pertinence du couple SR/OV	Choix P1/P2

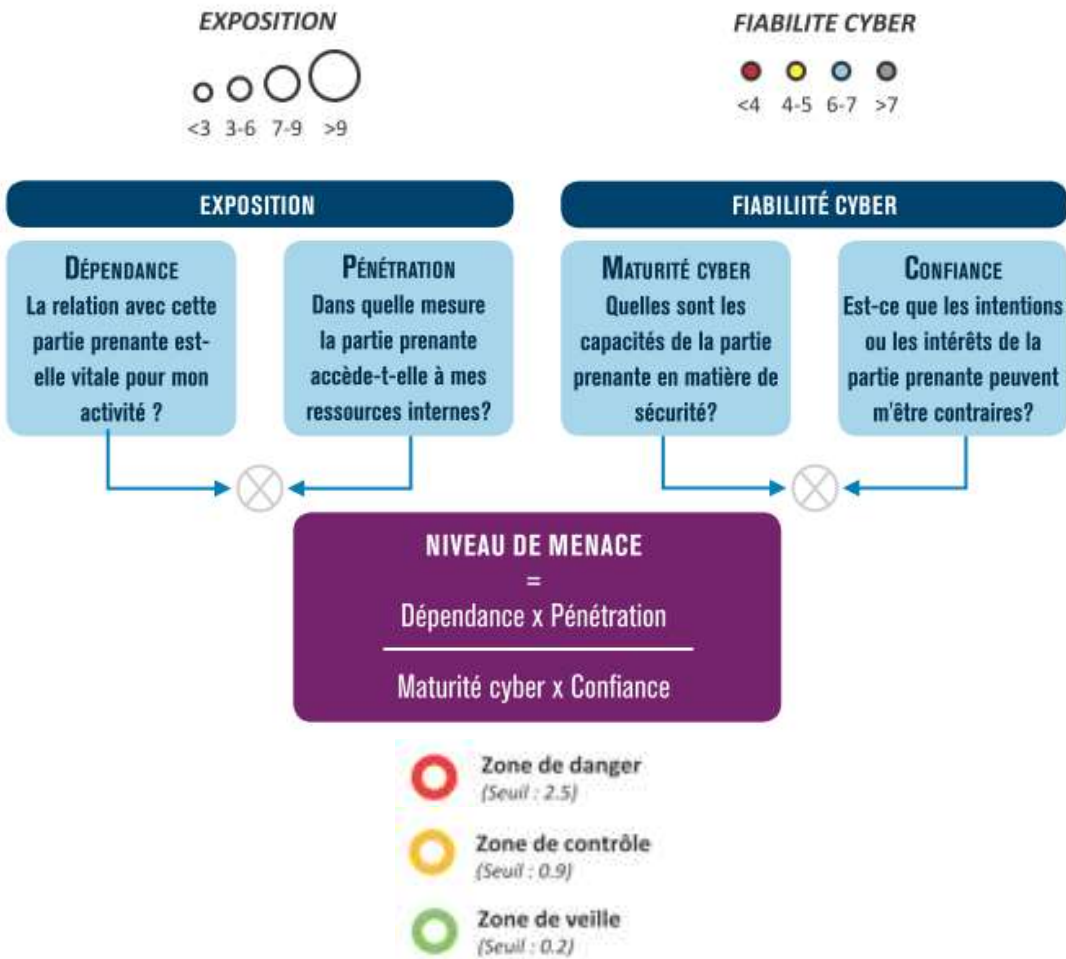
Radar de pertinence raffinée (point de vue SR)



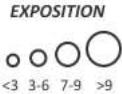
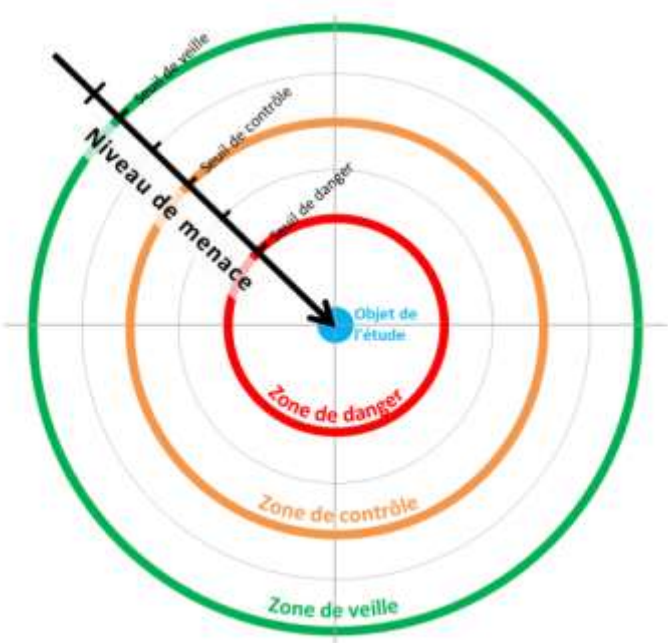
Radar de pertinence raffinée (point de vue OV)



-  Couple SR/OV retenu
-  Couple SR/OV non retenu



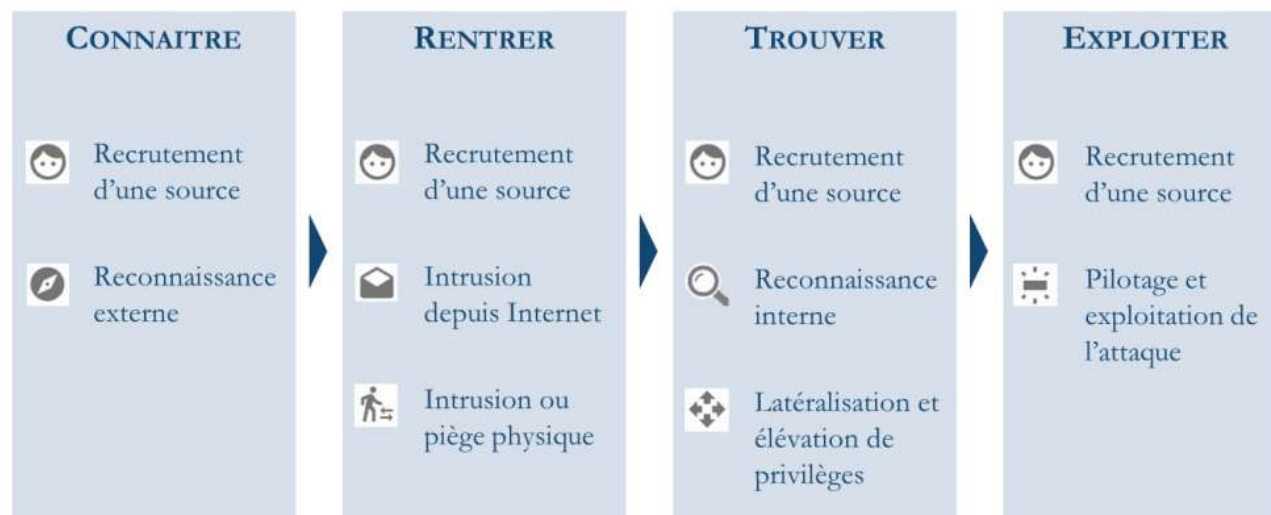
	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFIANCE
1	Relation non nécessaire aux fonctions stratégiques.	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2	Relation utile aux fonctions stratégiques	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3	Relation indispensable mais non exclusive.	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	Relation indispensable et unique (pas de substitution possible à court terme).	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisation.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.



NIVEAU DE MENACE	ACCEPTABILITÉ	RECOMMANDATIONS D'ACTIONS
 TRÈS ÉLEVÉ - ZONE DE DANGER	Inacceptable	Aucune partie prenante dans cette zone : réduction du risque, ou refus d'établir l'interaction.
 ÉLEVÉ - ZONE DE CONTRÔLE	Tolérable sous contrôle	Enrôlement de la partie prenante dans le processus de management du risque : -surveillance particulière, voire accrue, en termes de cyberdéfense ; - audit de sécurité technique et organisationnel ; -réduction/transfert du risque dans le cadre d'un plan d'amélioration continue de la sécurité.
 FAIBLE - ZONE DE VEILLE	Acceptable en l'état	Sans objet (menace résiduelle).

Modèle de séquence d'attaque type

> arbre/séquences d'attaque (« cyber kill chain »)



Catégories d'actions élémentaires (AE)

-  Recrutement d'une source, corruption de personnel
-  Reconnaissance externe de la cible
-  Intrusion depuis Internet ou des réseaux informatiques tiers
-  Intrusion ou piège physique
-  Reconnaissance interne
-  Latéralisation et élévation de privilèges
-  Pilotage et exploitation de l'attaque
-  Outils malveillants

Méthode expresse : cotation directe de la vraisemblance globale du scénario opérationnel

ÉCHELLE DE PROBABILITÉ DE SUCCÈS D'UNE ACTION ÉLÉMENTAIRE	
NIVEAU DE L'ÉCHELLE	DESCRIPTION
4 – QUASI-CERTAINE	Probabilité de succès quasi-certaine > 90%
3 – TRÈS ÉLEVÉE	Probabilité de succès très élevée > 60%
2 – SIGNIFICATIVE	Probabilité de succès significative > 20%
1 – FAIBLE	Probabilité de succès faible < 20%
0 – TRÈS FAIBLE	Probabilité de succès très faible < 3%

PROBABILITÉ DE SUCCÈS DU SCÉNARIO OPÉRATIONNEL

	DIFFICULTÉ TECHNIQUE DU SCÉNARIO OPÉRATIONNEL				
	0 – NÉGLIGEABLE	1 – FAIBLE	2 – MODÉRÉE	3 – ÉLEVÉE	4 – TRÈS ÉLEVÉE
4 – QUASI CERTAINE	4	4	3	2	1
3 – TRÈS ÉLEVÉE	4	3	3	2	1
2 – SIGNIFICATIVE	3	3	2	2	1
1 – FAIBLE	2	2	2	1	0
0 – TRÈS FAIBLE	1	1	1	0	0

ÉCHELLE DE DIFFICULTÉ TECHNIQUE D'UNE ACTION ÉLÉMENTAIRE	
NIVEAU DE L'ÉCHELLE	DESCRIPTION
4 – TRÈS ÉLEVÉE	Difficulté très élevée : l'attaquant engagera des ressources très importantes pour mener à bien son action.
3 – ÉLEVÉE	Difficulté élevée : l'attaquant engagera des ressources importantes pour mener à bien son action.
2 – MODÉRÉE	Difficulté modérée : l'attaquant engagera des ressources significatives pour mener à bien son action.
1 – FAIBLE	Difficulté faible : les ressources engagées par l'attaquant seront faibles.
0 – NÉGLIGEABLE	Difficulté négligeable, voire nulle : les ressources engagées par l'attaquant seront négligeables ou déjà disponibles.

Mesures de sécurité opérationnelles



CLUBEBIOS

Site : <https://club-ebios.org>

Twitter : @club_ebios

LinkedIn : <https://fr.linkedin.com/company/club-ebios>

