THALES

RETEX EBIOS RM au sein de THALES : augmentations et perspectives

CLUBEBIOS

Club-EBIOS - 13/05/2020

Agenda

- Constats sur la pratique d'EBIOS
- Augmentations et complements
- Conclusion : perspectives

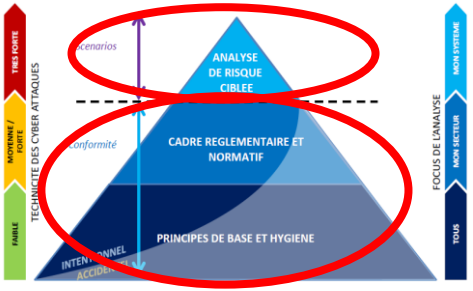
Constats sur la pratique d'EBIOS

Une adhésion sur des nouveautés structurantes

- Intérêt pour le double point de vue « attaquant » / « défenseur »
- Et pour la prise en compte de l'écosystème!

Attention à la « mise en équation »

- L'abandon de l'exhaustivité reste déroutant



Un frein « culturel » sur l'approche mixant conformité et scénarios

- Une analyse des risques peut-elle ne pas avoir de scénario associé?

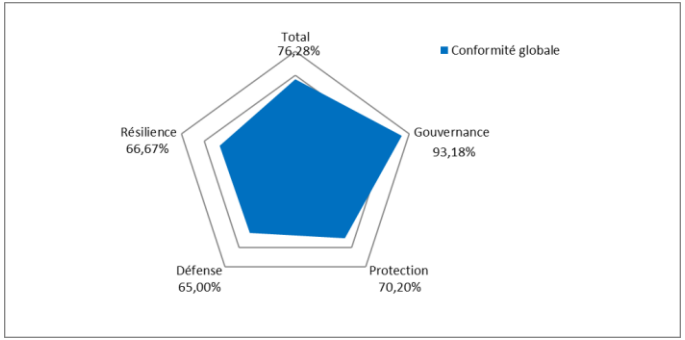
THALES

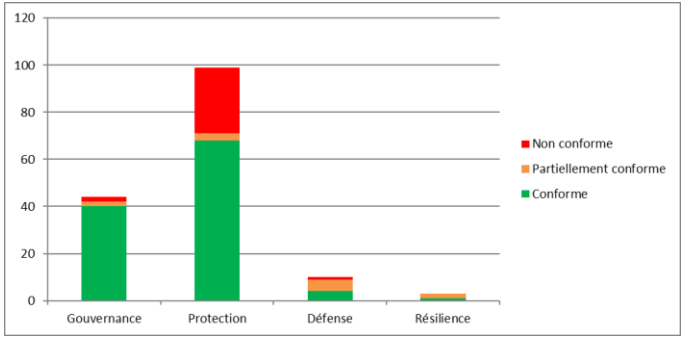
Augmentations et compléments

Atelier 1 : cadrage et socle de sécurité

Étape 1.d : socle de sécurité

- Présentée comme une phase clé
  - Exigences = résultat d'analyses de risque passées
- Structurée selon les 4 axes de la défense en profondeur
  - Gouvernance
  - Protection
  - Défense
  - Résilience
- Fait l'objet d'une analyse complète…
  - Diagrammes sur la couverture atteinte
  - Note de synthèse
  - Objectifs de sécurité à travailler
- Et présentée aux commanditaires!





THALES

Augmentations et compléments

Atelier 2 : sources de risque

- Étymologie du mot « source »
  - Officine spécialisée??
- Évaluation de la « capacité d'attaque » mobilisable
  - Approfondissement de la notion de « ressource »
  - S'appuyant sur la méthode d'évaluation des CC
    - « Expertise » mobilisable
    - « Connaissance du SI » mobilisable
    - « Budget » mobilisable
    - « Temps » mobilisable
  - En en gardant les pondérations proposées pour le « scoring »
    - Positionnement sur une échelle à 4 niveaux
- Synthèse = lien explicite ER – SR/OV

Profils de source de risque
Étatique
Crime organisé
Terroriste
Activiste idéologique
~~Officine spécialisée~~ Concurrent
Amateur
Vengeur
Malveillant pathologique

Capacité / Difficulté	Valeurs
Maximale	41 – 54
Forte	18 – 40
Significative	5– 17
Minime	0 – 4

THALES

Augmentations et compléments

Atelier 3 : scénarios stratégiques

Étape 3.a : sélection des parties prenantes critiques

- PPC = calcul d'un niveau de « criticité » (Vs. « menace »)

EXPOSITION		NIVEAU CYBER	
Dépendance	**Pénétration**	**Maturité SSI**	**Confiance**
1-Non nécessaire Relation non nécessaire aux fonctions stratégiques	**1-Niveau Utilisateur** Accès avec au mieux des privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, ordiphone, etc.).	**1-Mode Ponctuel** Des règles d'hygiène sont au mieux appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	**1-Intentions Suspectes** Les intentions de la partie prenante sont considérées comme suspectes.
2-Utile Relation utile aux fonctions stratégiques	**2-Niveau Administrateur local** Accès avec des privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.).	**2- Mode Hygiène** Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La SSI est conduite en mode réactif.	**2-Intentions Neutres** Les intentions de la partie prenante sont considérées comme neutres ou ne peuvent être évaluées.
3-Indispensable Relation indispensable mais non unique	**3-Niveau Administrateur métier** Accès avec des privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).	**3-Mode Réactif** Une politique globale est appliquée en matière de SSI. La SSI est conduite en mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	**3-Intentions Positives** Les intentions de la partie prenante sont connues et probablement positives.
4-Unique Relation indispensable et unique (pas de substitution possible à court terme)	**4-Niveau Administrateur infrastructure** Accès avec des privilèges de type administrateur à des équipements d'infrastructure (Annuaires d'entreprise, DNS, DHCP, switchs, firewall, hyperviseurs, baies de stockage, etc.)	**4-Mode Proactif** L'organisation met en œuvre une politique de management du risque. La politique est intégrée et prend pleinement en compte une dimension proactive. La partie prenante est un prestataire qualifié (cf. PAMS / PASSI / PRIS / PDIS) mature.	**4-Intentions Communes** Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

THALES

Augmentations et compléments

Atelier 4 : scénarios opérationnels

- Dissociation entre « intention » et « réalisation » de l'attaque
  - Notion d'« acteurs de la menace » (Vs. « sources de risque »)
- Évaluation de la « difficulté » des scénarios
  - Idem évaluation de la « capacité d'attaque »!
    - « Expertise » nécessaire
    - « Connaissance du SI » nécessaire
    - « Budget » nécessaire
    - « Temps » nécessaire
    - Positionnement sur la même échelle à 4 niveaux
  - Alimente l'évaluation de la « chance de succès »
    - Par confrontation entre « capacité » et « difficulté »

Type		Profils des acteurs de la menace
Humaines	1	Personne tierce
	2	Manutentionnaire
	3	Indirectement connectée
	4	Partenaire d'échange d'information
	5	Utilisateur normal
	6	Personne à portée
	7	Intrus physique
	8	Utilisateur privilégié
	9	Client du service
	10	Prestataire de service essentiel
	11	Souscripteur de service essentiel partagé
	12	Fournisseur
Non humaines	13	Code malveillant d'origine inconnue (peut être ciblé ou non-ciblé)
	14	Phénomène naturel
	15	Catastrophe naturelle ou sanitaire
	16	Activité anormale
	17	Événement interne

Ne devraient pas être nécessaires dans le cadre de l'activité d'analyse de risque par scénarios ciblés d'EBIOS RM !!

OPEN

THALES

Augmentations et compléments

Atelier 5 : traitement du risque

- Approfondissement de la notion de « Plan d'Amélioration Continue de la Sécurité »

  - Pilotage de la « performance SSI » selon 3 dimensions :
    - « Renseignement » : connaissance et anticipation
    - « Agilité » : capacité de maintien en condition
    - « Engagement » : adhésion et implication

  - Véritable journal de bord de la « maîtrise des risques »
    - Suivi des plans d'actions
    - Suivi des résultats d'audits
    - Suivi des indicateurs
    - Suivi des incidents et retex
    - Revues annuelles

THALES

Conclusion : perspectives

Premières pierres pour une révision intermédiaire de la méthode?

- Clarification d'étape de la méthode
  - Renforcement du rôle à donner à la conformité (analyse, note de synthèse, etc.)
- Clarification de vocabulaire
  - pour limiter les amalgames (cf. « menace » Vs. « criticité »)
- Clarification de notions
  - « source de risque » Vs. « acteur de la menace »
- Clarification de bases de connaissance
  - « sources de risques » & « acteurs de la menace »
  - « évaluation des PP »
- Extension d'approches méthodologiques
  - Vraisemblance : formalisation « capacité » Vs. « difficulté »

THALES

Conclusion : perspectives

Des pistes encore à explorer!

- Limite de l'approche actuelle par scénario vis-à-vis des APT = (trop) statique!
  - Pourquoi ne pas jouer un peu ? ☺
- Approfondissement de la modélisation au service de l'analyse de risque
  - Interfaçage avec les standards de la modélisation par couche (cf. MODAF/DODAF)
  - Approche quantitative?
- La « kill chain », le retour
  - Intérêt de l'UKC (« Unified Kill Chain »)?

Et une question?

- Quid de l'approche « G-P-D-R » de la directive SRI/NIS Vs. l'approche « I-P-D-R-R » du CSF du NIST et du TR ISO/IEC-27103?

Questions

Pour toute information :

Nicolas VAN CAUTER
RSSI Central adjoint,
Expert technique Thales,
Doctorant Telecom Paris.

nicolas[dot]vancauter[at]
thalesgroup[dot]com

Fin de la présentation

THALES