THALES

RETEX EBIOS-RM sur un cas IoT

RÉUNION DU CLUB EBIOS, PARIS, 10/01/2018

STÉPHANE PAUL
THALES RESEARCH & TECHNOLOGY

Introduction

Contexte

- Thales Ground Transportation Systems (GTS) compte inclure de l'IoT dans sa prochaine génération de SCADA (métro/train) → création d'un « KTD UC »

Objectifs de l'étude

- Identifier and gérer les risques liés à l'IoT
- Établir un référentiel de risques
- Définir une stratégie de migration

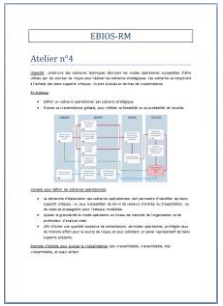
Approche / organisation

- Sessions de remue-méninges, basées sur la méthode EBIOS-RM
- 5 sessions de 2h chacune at Vélizy: 10 Sept., 12 Oct., 15 Oct., 30 Oct., 9 Nov.
- 9 invités / session, mais 4 personnes clef: 1 expert métier (GTS), 1 expert cybersécurité (GTS), 2 animateurs (TRT)

Méthodologie

En session

- Équipement
  - Posters
  - Post-its de couleur
  - Feutres de couleur
  - Fiches conseils au format A5
- Animation remue-méninges & gardien du temps
  - Collection des idées & des contributions (post-its)
  - Rappel des résultats de l'atelier précédent (5mn)


EBIOS-RM

Atelier n°4

Travail en back office

- Mise au propre des résultats
  - Conservation de la forme (e.g. position des post-its)
  - Compléter, et lever les incohérences (questions à poser lors du prochain atelier)

Avancement

Atelier n°1: Cadrage et socle de sécurité DONE

- Parties-prenantes, valeurs métiers, besoins de sécurité, cadre réglementaire(IEC 62443 SL2), biens supports

SRs and REs	SL 1	SL 2
FR 4 – Data confidentiality (DC)		
SR 4.1 – Information confidentiality	✓	✓
RE (1) Protection of confidentiality at rest or in transit via untrusted networks		✓
RE (2) Protection of confidentiality across zone boundaries		
SR 4.2 – Information persistence		✓
RE (1) Purging of shared memory resources		
SR 4.3 – Use of cryptography	✓	✓

Atelier n°2: Sources de risque DONE

- Sources et leurs objectifs

Atelier n°3: Scénarios stratégiques DONE

- Écosystème, scénarios d'attaque : 12 scénarios liés à des enjeux d'intégrité et/ou de disponibilité, 1 scénario lié à la vie privée, 1 scénario non retenu)

Atelier n°4: Scénarios opérationnels INCOMPLETE

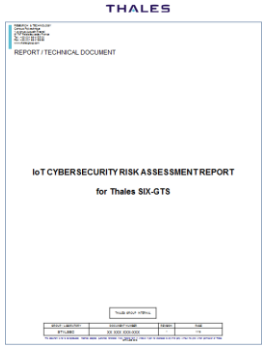
- 2 scénarios principaux, avec 1 alternative pour chaque scenario, propositions de mesures additionnelles, synthèse des risques nets

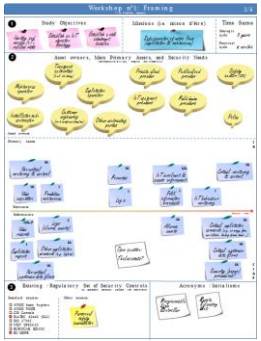
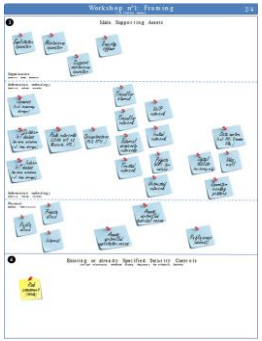
Atelier n°5: Traitement du risque

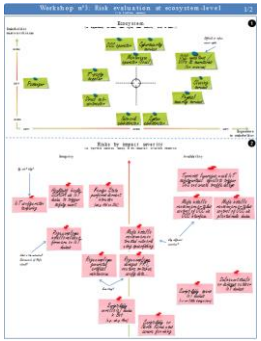
Résultats & feuille de route

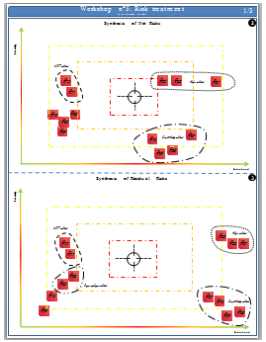
Résultats

- Génération d'un rapport (14 pages) – recyclage des posters !







- SL2 semble insuffisant pour sécuriser l'IoT: un « SL2+ » pourrait convenir

Feuille de route

- 1 atelier supplémentaire prévu le 14 janvier 2019
  - Objectifs: finaliser le jeu de mesures de sécurité, évaluer le risque résiduel

RETEX spécifique au cas d'étude

Ce qui a bien marché

- Connaissance au préalable du cadre réglementaire (IEC 62443 SL2)
  - Autorise une focalisation immédiate sur la malveillance
- Disponibilité des experts métier et cybersécurité de GTS
- Début de réflexions sur les options / mesures de traitement lors de l'atelier n°4

Ce qui a moins bien marché

- Version finale d'EBIOS-RM non encore publiée au lancement de l'étude
- Difficile d'animer les sessions et de garder des traces des digressions (souvent intéressantes)
- Pas d'étude des événements redoutés lors de l'atelier n°1 → compensé par l'atelier n°3

Ce qui n'a pas marché

- Rapport entre nombres de scénarios stratégiques et scénarios opérationnels
  - Liste des biens supports incomplète (architecture système, infrastructure, conception de l'IoT)
- Dérivation de IEC 62443 SL2: comment les contrôles sont-ils actuellement implémentés?

Source des problèmes: temps limité, confidentialité, spécifications IoT non finalisées…

RETEX générique (i.e. méthode EBIOS-RM, et 2 autres études)

Ce qui a bien marché

- Sessions de remue-méninges de 2 heures: vécues comme efficaces et amusantes
- Posters: bon passage à l'échelle, faciles à comprendre

Ce qui a moins bien marché

- Gestion des scénarios accidentels (i.e. versus malveillance & intrusion des ateliers n°2 & 4)
- Différences entre les événements redoutés des ateliers n°1 & n°3
  - Faiblesse de l'analyse des impacts métiers (ex-module 2 d'EBIOS 2010): surtout développé dans les fiches méthodes → proposition: ne gérer qu'une fois (dans atelier n°1 ou n°3)
- Travail en back office: assurer la cohérence & la complétude de l'étude → support outillé?
- Séquencement des ateliers
  - Étude des biens supports (atelier n°1), utiles seulement lors de l'atelier n°4 → 2 posters, étude séparée possible
  - L'écosystème (atelier n°3) est une expertise métier → pourrait être étudié lors de l'atelier n°1

Et maintenant…

Définir le positionnement de l'approche

- Quel champ d'application?
- Placer cette approche à base de posters dans une approche outillée plus générale
  - E.g. comment assurer la transition vers un outillage informatique?

Promouvoir l'approche en interne Thales

- Conférences, présentation…
- Utilisation dans la formation interne Thales « Cybersécurité, impact sur l'ingénierie et évaluation de risques » sur un cas IFE

Cercle des formateurs du Club EBIOS

- Mise à disposition à discuter

Merci ! Questions ?