THALES

Nouvelle EBIOS :
Pistes d'approches « Cyber Kill Chain » étudiées au sein de Thales

CLUBEBIOS

Club-EBIOS - 03/05/2018

Agenda

- La pratique d'EBIOS au sein de Thales
- Nouvelle EBIOS : nouveau contexte d'emploi
- Focus sur l'approche « Cyber Kill Chain »
- Cyber Kill Chain Vs. Attack Tree
- Cyber Kill Chain + Attack Tree
- Conclusion

THALES

La pratique d'EBIOS au sein de Thales

Le contexte Thales

www.thalesgroup.com

Le contexte Thales

Méthodologie :

- Thales utilise la méthode EBIOS :
  - Pour ses activités « Défense »
  - Pour ses besoins internes
  - Pour ses clients du Secteur Public
  - Enfin, pour ses clients civils (depuis EBIOS-2010)

TRN : xxxx-xxxxxxxxxx rev xxx - 03/05/2018
Thales Communications & Security/ Modèle : 87204467-DOC-GRP-FR-002

THALES

Le contexte Thales

Périmètres :

- Thales réalise des analyses des risques sur tous types de périmètres :

  - Au niveau « composants »
  - Au niveau « produits »
  - Au niveau « systèmes »
  - Au niveau « systèmes complexes » (systèmes de systèmes / SMSI)
  - Au niveau « Stratégies »

Le contexte Thales

Utilisations :

- Les raisons d'être des analyses des risques pratiquées par Thales :
  - Les homologations de produits / systèmes
  - Les certifications de produits

Utilisateurs :

- Une population technique, principalement d'ingénieurs, dans les domaines :
  - De l'ingénierie système
  - De l'ingénierie logicielle

THALES

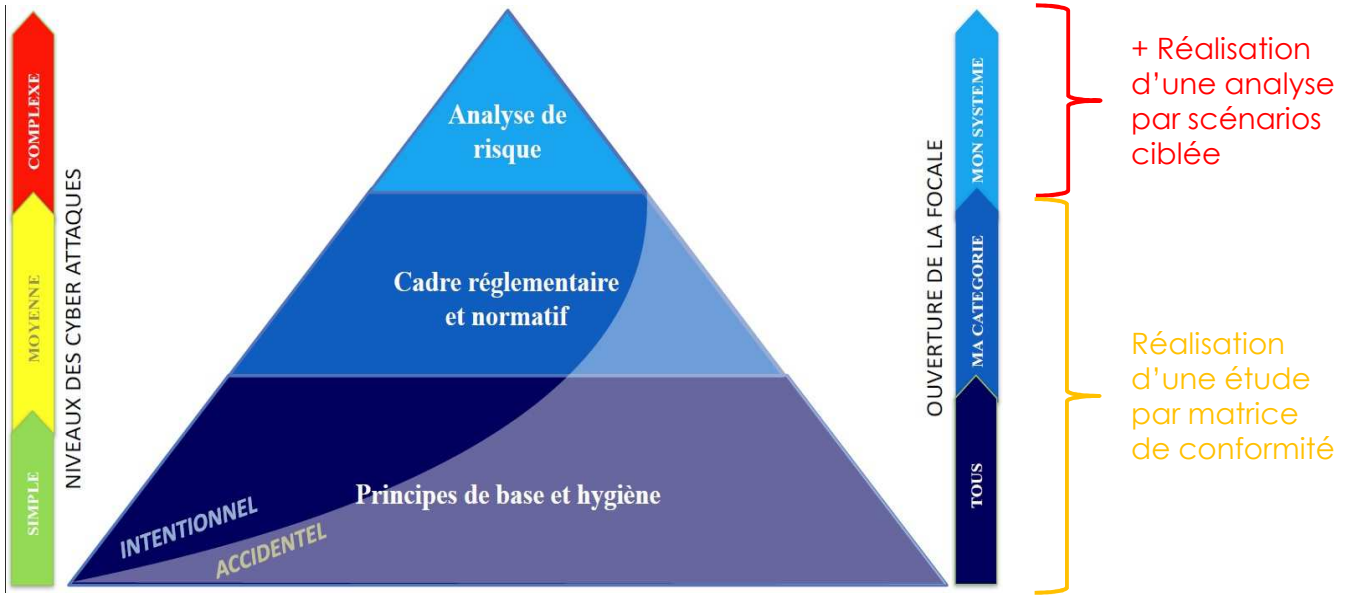
Nouvelle EBIOS : nouveau contexte d'emploi

www.thalesgroup.com

Nouvelle EBIOS : nouveau contexte d'emploi

Nouvelle approche « mixte » de l'évaluation des risques

> Abandon d'une approche de l'évaluation des risques « systématique » et « exhaustive » pour une approche « mixte » :



THALES

Nouvelle EBIOS : nouveau contexte d'emploi

Évolutions EBIOS-2010 / nouvelle EBIOS :

- Changement de paradigme :
  - EBIOS-2010 = approche inductive
  - Nouvelle EBIOS = approche déductive
- Qui amène un changement de finalité :
  - EBIOS-2010 = recherche d'exhaustivité, des scénarios simples aux scénarios complexes
    - Cependant très souvent études limitées aux scénarios "simples" / "directs"
  - Nouvelle EBIOS = focus sur les scénarios complexes représentatifs
    - Par "complexe" on entend par exemple les scénarios de type "APT" (Advanced Persistent Threat)
    - Cela oriente sur des études de scénarios d'attaque "de bout en bout"
    - L'approche "cyber kill chain" va dans ce sens

TRN : xxxx-xxxxxxxxxx rev xxx - 03/05/2018
Thales Communications & Security/ Modèle : 87204467-DOC-GRP-FR-002

THALES

THALES

Focus sur l'approche « Cyber Kill Chain »

www.thalesgroup.com

OPEN

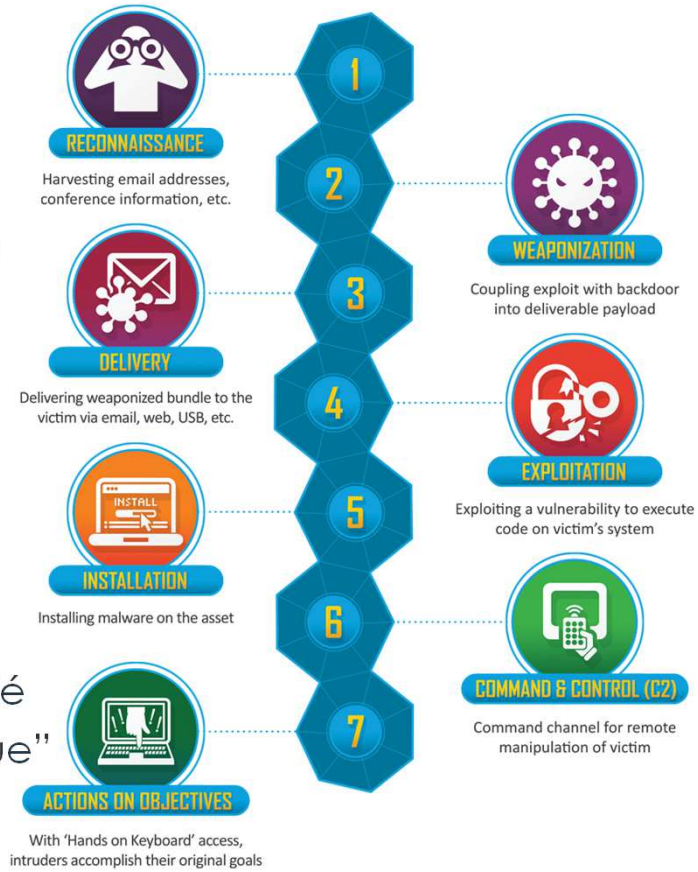
Focus sur l'approche « Cyber Kill Chain »

Origines :

- Introduite par Lockheed-Martin en 2011
  - Inspirée du modèle de "kill chain" des militaires
    - Cf. F2T2EA : find / fix / track / target / engage / assess
  - Avec le principe suivant :
    - Si la chaine est interrompue alors l'attaque échoue

Limites :

- Les principales critiques de la CKC de Lockheed-Martin :
  - Très orientée "attaque par malware"
  - Plusieurs étapes se déroulent à l'extérieur du SI ciblé
  - Ramène dans un schéma de "défense périmétrique"
  - De fait n'adresse pas bien les attaques internes



TRN : xxxx-xxxxxxxxxx rev xxx - 03/05/2018
Thales Communications & Security/ Modèle : 87204467-DOC-GRP-FR-002

OPEN

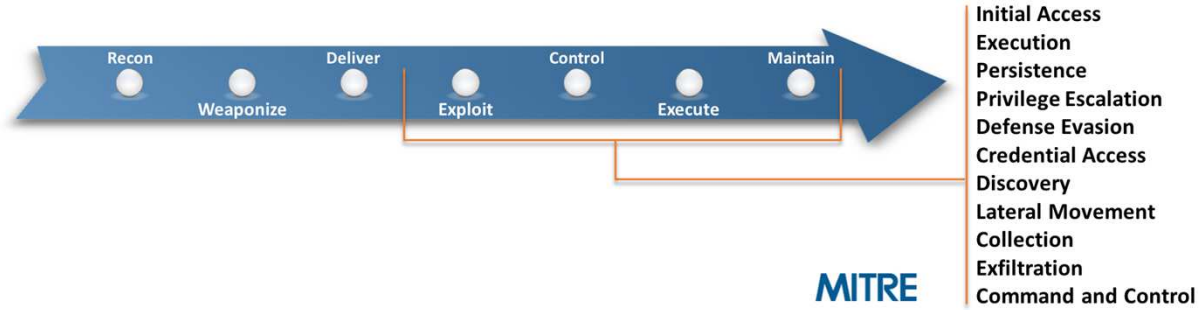
THALES

Focus sur l'approche « Cyber Kill Chain »

Variantes :

L'approche du MITRE

- L'approche "ATT&CK™" (Adversarial Tactics, Techniques, and Common Knowledge) est complémentaire de la CKC de Lockheed-Martin
- Elle introduit 11 catégories de "tactiques" pour approfondir les 4 dernières étapes de la CKC (i.e. lorsque l'attaque est effective sur le SI ciblé)



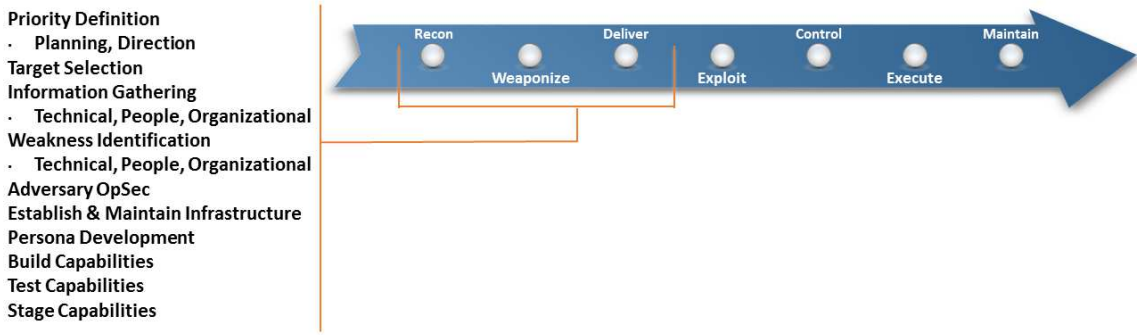
- Ces 11 "tactiques" sont ensuites déclinées en 284 "techniques" (cf. approche "TTP")
- L'équipe de Threat Intelligence de Thales s'appuie sur cette approche
- Cette granularité permet de traiter les attaques "internes"

Focus sur l'approche « Cyber Kill Chain »

Variantes (suite) :

L'approche du MITRE (suite)

- Le MITRE a également proposé une approche "pre-ATT&CK™" pour adresser les premières étapes de la CKC de Lockheed-Martin
- Elle introduit 15 catégories de "tactiques" pour approfondir les 3 premières étapes (i.e. lorsque l'attaque est en préparation hors du SI ciblé)



- Les 2 approches sont complémentaires même si différentes :
  - "ATT&CK™" est une approche plus concrète, facilement instanciable en mesures de sécurité
  - "pre-ATT&CK™" est plus abstraite et prend de l'intérêt si l'on dispose d'une réelle capacité de Threat Intelligence

THALES

Cyber Kill Chain Vs. Attack Tree

www.thalesgroup.com

OPEN

Cyber kill chain Vs. Attack tree

Similitudes :

- Aptitude à modéliser des scénarios d'attaque de bout en bout

Différences :

- Prise en charge du niveau "métier" d'un scénario d'attaque
- Prise en compte de la temporalité dans les actions d'un scénario d'attaque
- Exhaustivité des sous-scénarios d'un scénario d'attaque

Arbres d'attaque : un retour d'expérience Thales

- Danger de l'exhaustivité = la complexité de l'arbre
  - i.e. explosion combinatoire des feuilles sur un système complexe
- Danger de l'universalité = la construction de l'arbre
  - i.e. d'avoir et de gérer les différents "bons sachants"

TRN : xxxx-xxxxxxxxxx rev xxx - 03/05/2018
Thales Communications & Security/ Modèle : 87204467-DOC-GRP-FR-002

THALES

THALES

Cyber Kill Chain + Attack Tree

www.thalesgroup.com

OPEN

Cyber Kill Chain + Attack Tree

Piste Thales : approche combinée CKC-AT

- Approche "AT" pour les "scénarios stratégiques" (cf. Atelier 3)
  - L'exhaustivité en première approche est intéréressante
  - L'approche inductive peut être un facilitateur vis-à-vis des interlocuteurs visés
  - Limitation aisée de la profondeur de l'arbre
- Approche "CKC" pour les "scénarios pratiques" (cf. Atelier 4)
  - Pour gérer la temporalité des scénarios de bout en bout
  - Doit capitaliser les apports des équipes de "Threat Intelligence"
- Augmentée d'une approche "ATT&CK" pour les "actions" des "scénarios pratiques"
  - Pour une certaine exhaustivité des types de tactiques et techniques d'attaque

TRN : xxxx-xxxxxxxxxx rev xxx - 03/05/2018
Thales Communications & Security/ Modèle : 87204467-DOC-GRP-FR-002

THALES

THALES

Conclusion

Conclusion

La nouvelle EBIOS semble prometteuse :

> Pour appréhender les nouveaux enjeux des APT

- L'approche Cyber Kill Chain va dans ce sens
- Cependant il faut être prêt à prendre du recul
  - La CKC de Lockheed-Martin n'est pas la panacée
  - Le contexte du SI doit amener à contextualiser les CKC
    - » i.e. en fonction des scénarios stratégiques et des sources de menace
- Et il faut avoir de la matière pour construire des Cyber Kill Chain pertinentes
  - La contribution de la Threat Intelligence est fondamentale
  - Cependant elle n'est pas à la portée de tous les organismes
  - Se pose la question du niveau de collaboration et de partage entre acteurs de la cybersécurité?

La maîtrise de la Threat Intelligence sera un facteur clé

Pour toute information :

Nicolas VAN CAUTER
RSSI Central Adjoint,
Thales – TCS
m: +33 (0) 6 43 59 28 20
nicolas.vancauter@thalesgroup.com

OPEN

THALES