De la rondache au pavois :

Le renseignement cyber circule-t-il vraiment dans nos organisations ?

Les Lundis de la Cybersécurité · 16/11/2026

D'après une thèse de MBA Management de la Cybersécurité (2025)

François Stricher

1

Du duel… à la volée de carreaux





La rondache · le duel

Le mur de pavois · la volée de carreaux

Images : Cleveland Museum of Art (1916.1615) ; Art Institute of Chicago (106393) — domaine public

2

2

Parcours

2000-2004	2004-2014	2014-2022	2024	2024-2025	Aujourd'hui
Doctorat en biochimie	**Ingénierie de protéines**	**Direction de R&D**	**Cap sur la cybersécurité**	**MBA Management**	**CTI et investigations**
ENS Cachan, CEA	logiciels de modélisation · EMBL, CRG	industrie des biotechnologies	reconversion	de la Cybersécurité	SOC, gestion de crise cyber

On ne progresse qu'en partageant

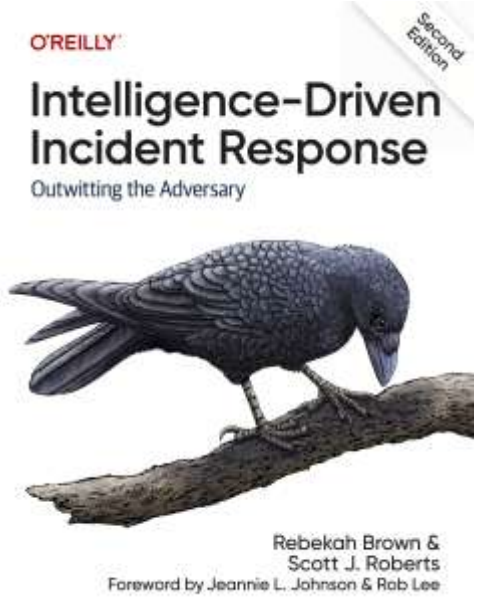
3

3

À l'origine:

« Là où la diffusion échoue, l'apprentissage s'arrête et les défenses s'amenuisent. »

F3EAD : le « D » de Disseminate



4

4

Le programme de la soirée

1	2	3	4	5
Les bases	**Le monde idéal…**	**… et le terrain**	**Un modèle**	**Un an après**
du signal au renseignement	ce qui devrait circuler	ce que disent huit entretiens	pour faire circuler le renseignement	ce qui a changé… et ce qui tient

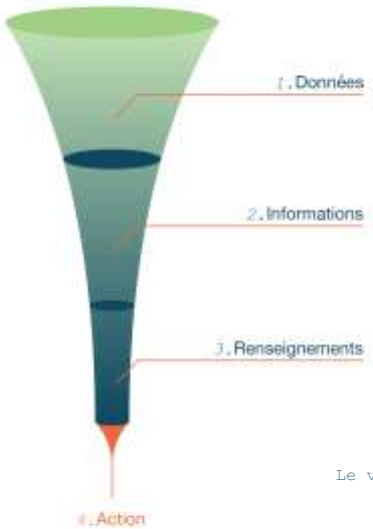
Deux sondages Zoom anonymes · une discussion pour finir · la parole si vous la demandez

Le paradoxe : la CTI est installée partout… mais à l'intérieur des organisations, les flux se grippent.

5

5

Données, Information, Renseignement



		Exemple : un serveur saturé
1. Données	le quoi · brutes, massives, bruyantes	Des milliers de lignes de logs de connexion
2. Informations	qui, quand, où, comment · structurée, contextualisée	*« Plusieurs IP surchargent le serveur en même temps »*
3. Renseignements	pourquoi, et ensuite ? · actionnable	Attaque DDoS coordonnée : activer la protection maintenant

Le volume diminue, la valeur augmente

Utile · Utilisable · Utilisé

6

6

Les sources du renseignement : les « INT »

TECHINT
matériel adverse

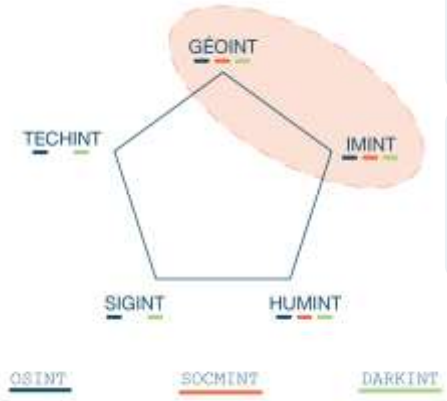
Hier l'avion abattu, aujourd'hui la rétro-ingénierie de malware

SIGINT
signaux

D'Enigma au trafic réseau : toute donnée issue d'une machine

HUMINT
sources humaines

Cyber-HUMINT : avatars sur les forums



GEOINT
géographie

Où sont les serveurs, les acteurs, les effets physiques

OSINT
sources ouvertes

La plus utilisée en CTI… à évaluer avec soin

IMINT
imagerie

Du U-2 au-dessus de Cuba (14/10/1962) à l'ampleur d'APT1

SOCMINT
réseaux sociaux

Revendications, fuites, usurpations d'identité

DARKINT
dark web

Marchés, forums, fuites de données, tarifs

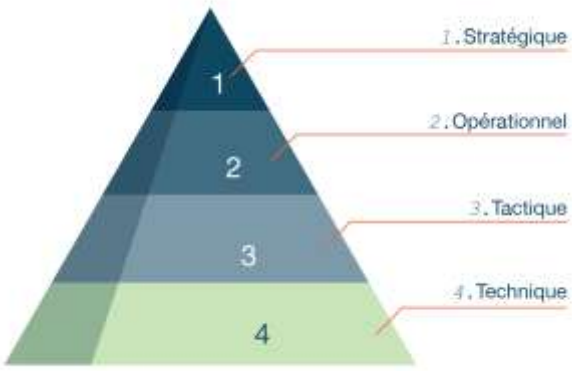
Héritées du renseignement classique

Propres au numérique

7

7

Un peu de sémantique



	Pour qui · horizon · forme
Motivations Géopolitique	**Direction, conseil, risques** Long terme · Rapports soignés, sans jargon
TTP Campagnes Capacités	**Managers SOC et DFIR, architectes** Campagnes · Rapports ; STIX en temps de guerre
TTPs IoCs	**Analystes SOC, CSIRT, DFIR** Court terme · IoCs, TTPs
Atomic IoCs	**Les machines** Heures, jours · Flux automatisés

Les différents types de CTI

8

8

Fil rouge : une vulnérabilité, quatre lectures



Stratégique Une menace nouvelle, une nouvelle victimologie ? Faut-il revoir l'architecture ou la politique de sécurité ?

Opérationnelle Quelle ampleur ? Attaque ciblée ou opportuniste ? Quelles victimes, quels objectifs ? Comment durcir le système ?

Tactique Les artefacts de post-exploitation : chercher l'adversaire (threat hunting)

Technique Les IP qui scannent, les empreintes de malwares : poussées automatiquement dans le pare-feu et l'EDR

`Le même événement, quatre renseignements, quatre publics`

9

9

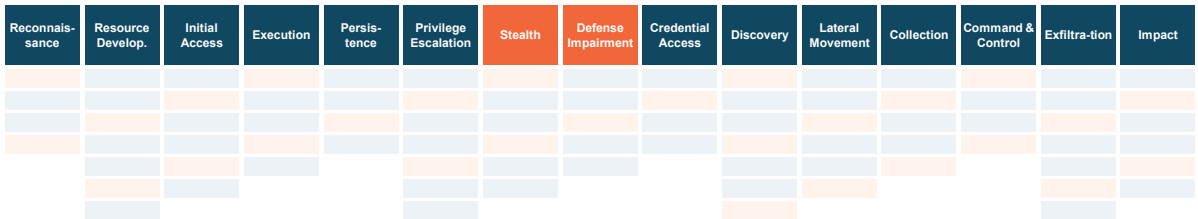
Penser comme l'attaquant

« Tous les modèles sont faux, mais certains sont utiles. » — George Box

`Cyber Kill Chain · Lockheed Martin, 2011`



`MITRE ATT&CK v20 (octobre 2026) · 15 tactiques · 227 techniques`



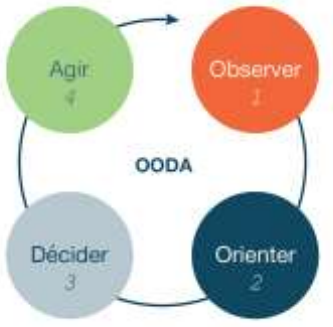
ATT&CK : l'encyclopédie des comportements adverses… et une langue commune

D3FEND : le miroir défensif d'ATT&CK — les contre-mesures

10

10

La boucle OODA



John Boyd



Le tempo
Un pilote moins bien équipé l'emporte s'il tourne sa boucle plus vite que l'adversaire.

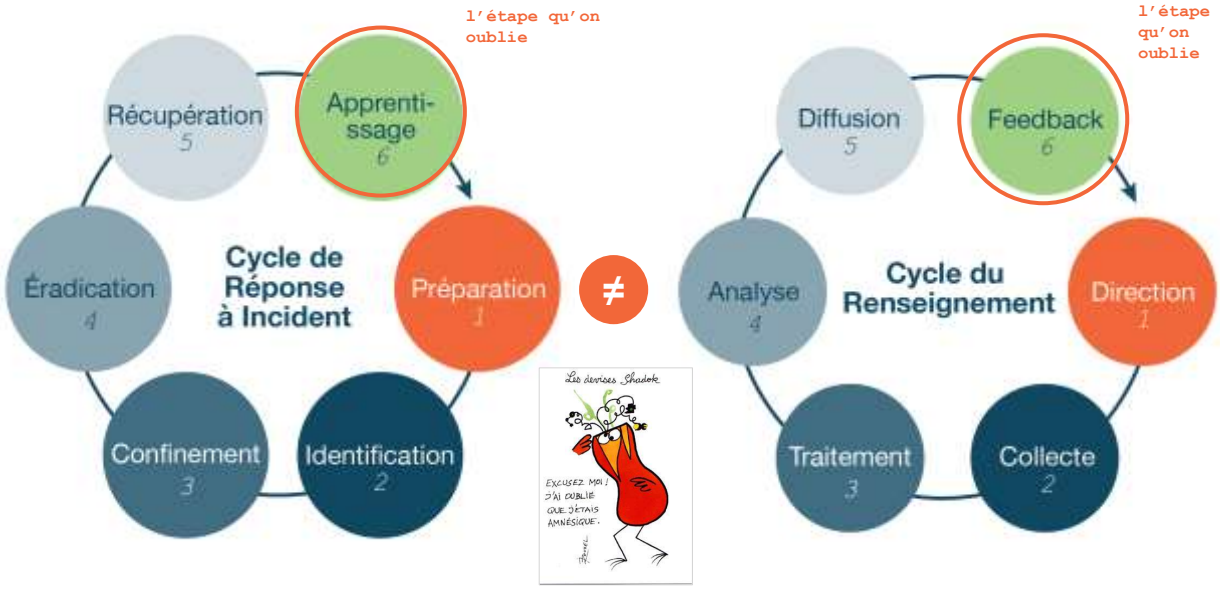
Orienter, l'étape centrale
Trier l'avalanche de données grâce à l'expérience… et malgré ses biais.

Deux boucles face à face
L'attaquant a la sienne : la bataille se joue sur la vitesse de décision.

Observer + Orienter = un cycle du renseignement

11

De deux cycles distincts…



Les Shadoks © Jacques Rouxel

12

… à un cycle mixte

Renseignement : Exploit · Analyze · Disseminate

Opérations : Find · Fix · Finish

Analyze
Quels TTPs, quelles faiblesses ?

Exploit
On collecte les artefacts

Finish
Confinement, correctif



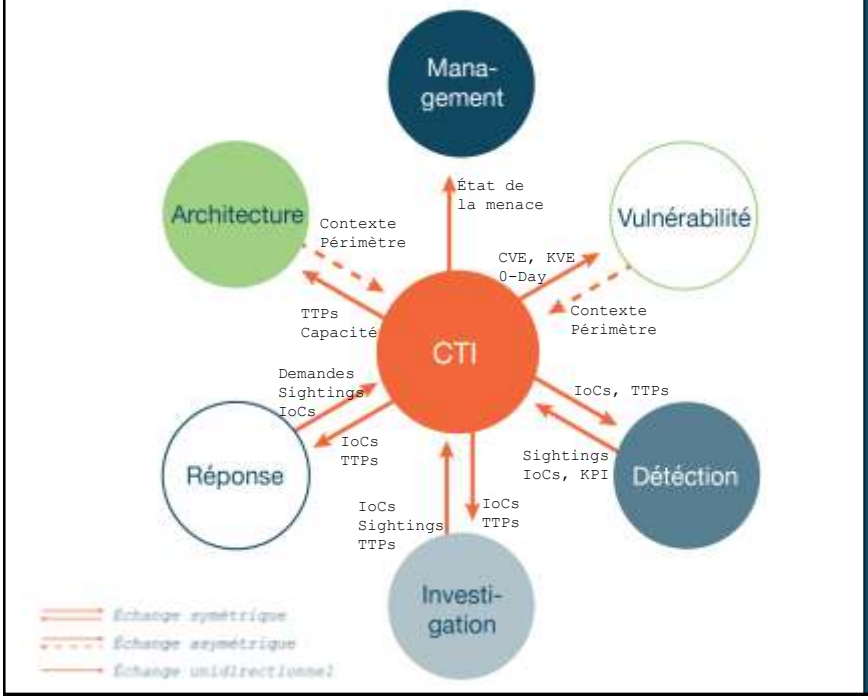
Disseminate
Vers la détection, l'architecture, la direction

Find
Une vulnérabilité exploitée est signalée

Fix
Où est l'adversaire chez nous ?

Une représentation explicite des échanges entre la fonction CTI et la fonction IR 13

13



Échanges de renseignements

Le code de diffusion :

TLP:RED | TLP:AMBER | TLP:GREEN | TLP:CLEAR

Schéma idéal…

14

14

Le voyage d'une vulnérabilité

	La CTI envoie →	← L'équipe renvoie
Vulnérabilité	CVE, exploitation active (KEV), probabilité d'exploitation (EPSS)	Ce qui n'est pas corrigé, l'exposition réelle
Détection	IoCs, règles de détection (SIGMA, YARA)	Détections qualifiées, faux positifs, télémétrie
Réponse · Investigation	Hypothèses sur l'adversaire, pivots probables	Artefacts, chronologie de l'attaque
Architecture	Évolution des techniques adverses, contre-mesures (D3FEND)	Nouvelles technologies, inventaire logiciel (SBOM)
Management	Scénarios de risque	Priorités de renseignement (PIRs)

15

15

Pas une utopie : c'est écrit dans les normes

ISO 27001:2022

Annexe A.5.7

Un processus de collecte et d'analyse du renseignement sur la menace

NIST CSF 2.0

DE.AE-07 · ID.RA

Le renseignement intégré à la détection et à l'analyse de risque

ANSSI

Qualifications PDIS · PRIS

L'amélioration continue des règles de détection par la CTI

NIS 2

Article 20

La formation obligatoire des organes de direction

Alors… pourquoi ça ne marche pas toujours ?

16

16

Problématique et Hypothèses

Quels sont les limites et les freins au partage de renseignements sur les cybermenaces (CTI) à l'intérieur d'une organisation ?

Utilisation majoritaire d'IoCs

Peu de flux inverses d'informations

Technique	Gouvernance	Culture	Ressources	Technique	Gouvernance	Culture	Ressources

17

17



À vous !

Sondage 1/2

Mode d'emploi

Le sondage s'affiche par-dessus les slides.

Réponses anonymes.

Répondez d'après les organisations que vous connaissez… ou votre intuition.

1 **Dans une organisation « type », quelle part du renseignement consommé est faite d'indicateurs techniques (IoCs) ?**

Moins de 25 % | 25 à 50 % | 50 à 75 % | Plus de 75 %

2 **Les équipes de terrain font-elles remonter ce qu'elles apprennent vers ceux qui produisent le renseignement ?**

Jamais | Parfois, de façon informelle

Systématiquement, de façon structurée | Je ne sais pas

3 **Sur 100 indicateurs qui circulent dans une organisation, combien viennent du terrain ?**

0 à 5 | 6 à 15 | 16 à 30 | 31 à 50 | Plus de 50

Répondez au sondage qui s'affiche

Levez la main pour prendre la parole

18

18

Méthodologie

8 entretiens
juin 2025 · 1 h à 2 h
4 questionnaires
24 sous-hypothèses
anonymat garanti
exploratoire · déclaratif

Entretiens Semi-Dirigés

Acteurs Internes		Acteurs Externes	
RSSI/CERT	Banque	CEO	ESN Moyenne
RSSI	Commerce	CTI	ESN Grande
RSSI	Santé	Vente	Services CTI
SOC	Hospitalité	Compte	Logiciel CTI

Analyse

Analyse Transversale

19

19

Vous aviez dit…

Vous (sondage 1)

Part d'IoCs dans la CTI consommée

majorité : ……

Indicateurs venant du terrain (sur 100)

majorité : ……

Le terrain

> 90 %

de CTI tactique ou technique

2 % / 98 %

des indicateurs remontent du terrain — et 98 % descendent du CERT

20

20

CTI Stratégique	Banque	CERT IoCs (Bidirectionnel) TTPs Vulnérabilité État de la menace
CTI Opérationnelle		Contextualisation Règles maison, Purple Team ← Santé
CTI Tactique		TIP ← Commerce
CTI Technique	Hospitalité	IoCs (automatique)



Analyse Transversale

Utilisation Majoritaire d'IoCs

Flux Inverses rares

21

21

Paroles de terrain

RSSI · santé

En quatre ans, les IoCs externes n'ont presque jamais détecté une intrusion majeure.

Les compromissions ont été trouvées par des règles maison, issues du Purple Teaming.

ESN

Beaucoup consomment de la CTI… sans même le savoir.

Elle est encapsulée dans les mises à jour de leurs équipements.

Grande ESN

L'ambition est stratégique ; l'usage, technique.

On parle chasse aux menaces et modes opératoires ; on active les IoCs poussés par les éditeurs.

Propos reformulés à partir des entretiens · organisations anonymisées

22

22

En résumé

H1 · Utilisation majoritaire d'IoCs
étayée par le terrain

> 90 %

de CTI tactique ou technique, souvent injectée directement dans les SIEM, EDR et SOAR

H2 · Peu de flux inverses
étayée par le terrain

Parcellaire

voire inexistant : le renseignement descend, il remonte rarement

Là où il existe : une gouvernance forte et une TIP

Pourquoi ?

Huit entretiens, des déclarations : une tendance nette, pas une statistique

23

23

À vous !

Sondage 2/2

Selon vous, qu'est-ce qui empêche le renseignement de circuler… et surtout de remonter ?

Choisissez les 3 freins qui vous semblent les plus importants (3 maximum)

1. Les outils ne permettent pas d'extraire les données
2. La sécurité est externalisée
3. La peur des fuites, la confidentialité
4. Pas de culture du partage ni de confiance entre les équipes
5. Personne n'est chargé de faire circuler le renseignement
6. La compétition interne
7. La CTI arrive « toute faite » dans les outils des éditeurs
8. Pas assez de temps ni de personnes
9. Pas de budget, pas de ROI démontrable

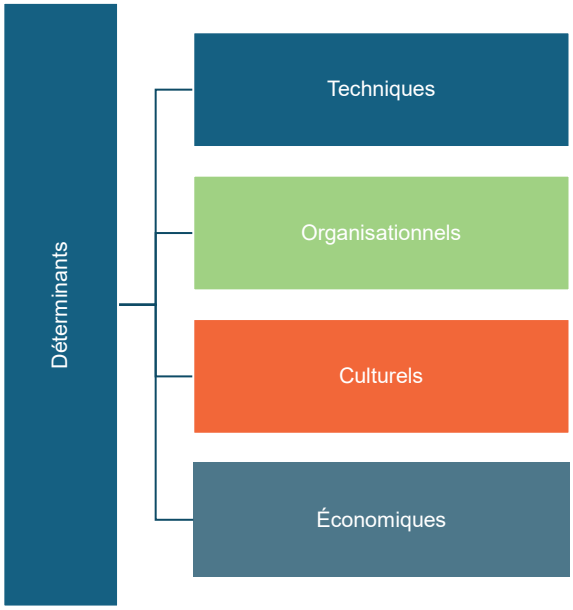
Répondez au sondage qui s'affiche

Levez la main pour prendre la parole

24

24

Analyse Transversale



- Solutions Intégrées
- Extractions
- Normalisation

- Historique
- Silos
- Complexité

- Historique
- Géographie
- Formation

- Centre de coûts
- ROI
- Incidents/Réglementation

Bilan de la thèse

techniques, organisationnels, culturels… et, dans une moindre mesure, économiques

25

25

Deux constats qui dérangent

« Trop littéraire »

Ce jugement sur la CTI stratégique revient surtout dans les pays de culture latine. L'Europe du Nord et le monde anglo-saxon adoptent plus vite la défense guidée par la connaissance de la menace.

« Je paie, donc je ne donne pas »

Beaucoup de clients voient la CTI comme une prestation descendante : puisqu'ils paient, pourquoi enrichir la base du fournisseur ? Et quand ses centres de données sont hors juridiction, partager devient délicat, voire impossible.

TLP:RED TLP:AMBER TLP:GREEN TLP:CLEAR

Le code de diffusion existe… **le frein n'est pas dans l'outil, il est dans la confiance.**

26

26

Lignes de fracture

Organisations
Un levier opérationnel, à court terme : bloquer un phishing, accélérer la réponse

Prestataires
Une vision stratégique, la mutualisation… que le client craint

Grandes organisations régulées
CERT et CTI internes : des flux structurés, même imparfaits

Organisations moyennes
Externalisation… et donc simple ingestion

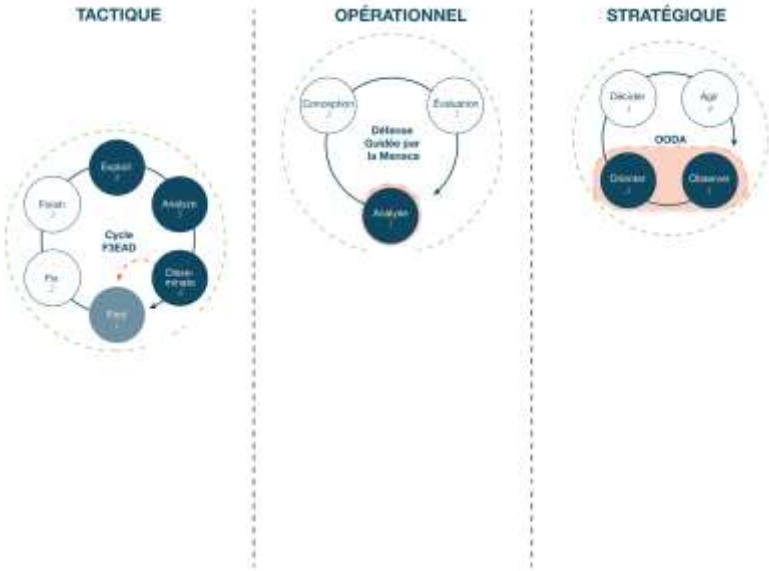


En France, l'expertise CTI est concentrée dans quelques sociétés de conseil.

Et si le problème n'était pas la maturité… mais la représentation ?

27

Trois niveaux, trois horizons, trois cycles



Tactique · court terme
Détection, réponse, investigation → CTI tactique et technique → F3EAD

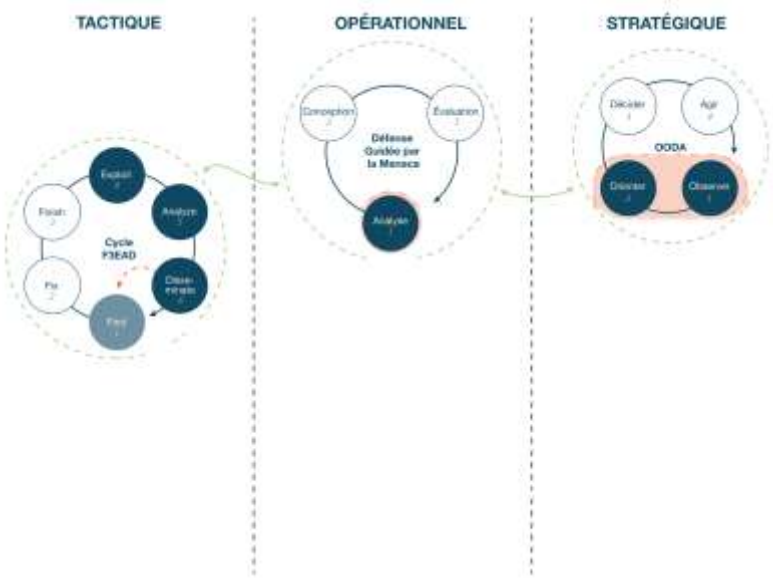
Opérationnel · moyen terme
Architecture, ingénierie, vulnérabilités → CTI opérationnelle → défense guidée par la menace

Stratégique · long terme
RSSI, direction, conseil → CTI stratégique → OODA

… mais trois îles

28

Des cycles qui s’engrènent



Find (F3EAD)
Préparer la détection et la tester pour « fixer » l’adversaire : c’est déjà un cycle TID

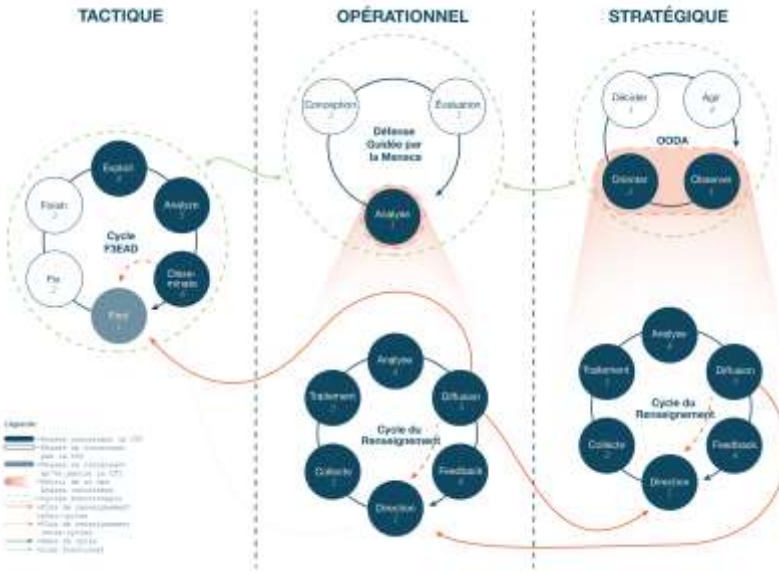
Agir (OODA)
Renforcer, étendre, modifier le système d’information : encore un cycle TID

Les roues ont enfin des dents

29

29

Le renseignement circule



Chaque cycle d’action nourrit son cycle de renseignement
Exploit (F3EAD) · résultats des tests Purple Team (TID) · conséquences de l’Agir (OODA)

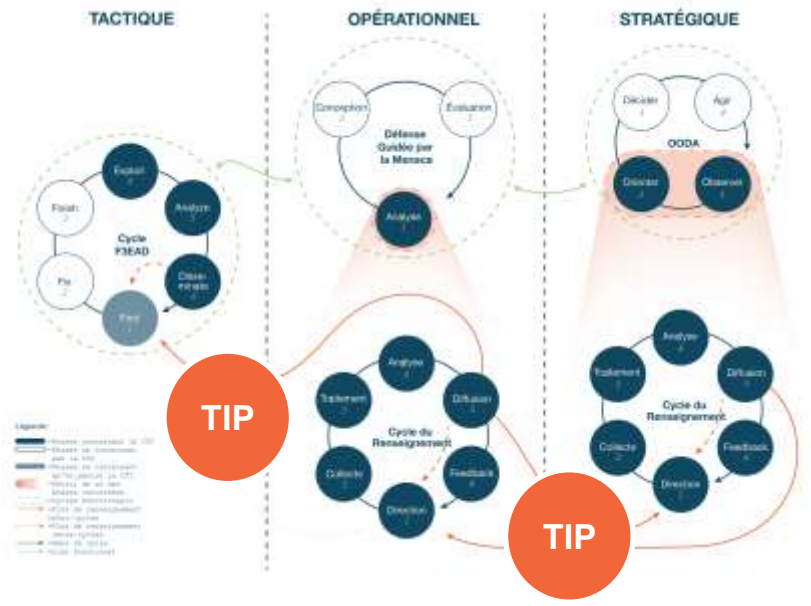
Chaque Diffusion lance une nouvelle Direction
Au même niveau ou au niveau voisin : les PIRs stratégiques orientent l’opérationnel

La remontée des équipes devient structurelle

30

30

Au centre, la TIP



Ingérer · normaliser · corréler · enrichir · redistribuer
Enrichir avec ATT&CK, redistribuer en temps réel à chaque niveau

« Source unique de vérité »
Sans elle, le volume et l'hétérogénéité rendent la continuité impossible

Nécessaire, pas suffisante
Sans quelqu'un pour la nourrir, une TIP n'est qu'un flux d'IoCs de plus

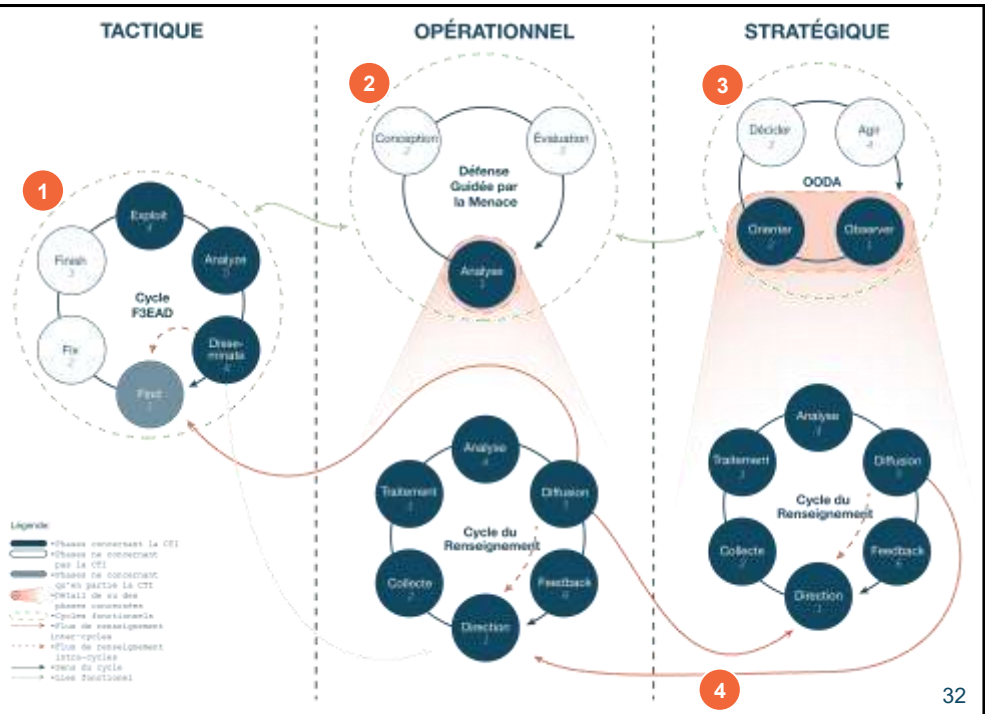
31

31

1 F3EAD : correctif, artefacts
2 TID : règle testée en Purple Team
3 OODA : la direction arbitre
4 de nouvelles PIRs redescendent

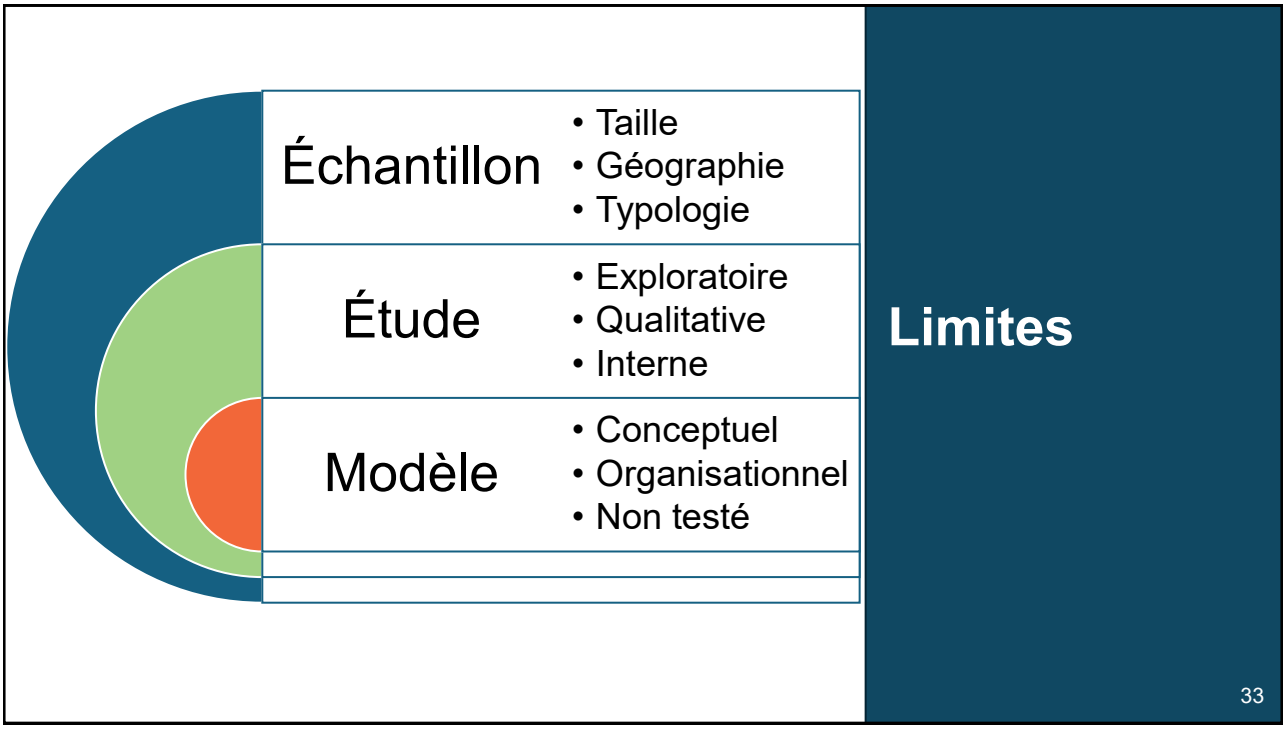
Un modèle unifié

Organisation des Renseignements Intégrés aux Opérations Numériques (ORION)

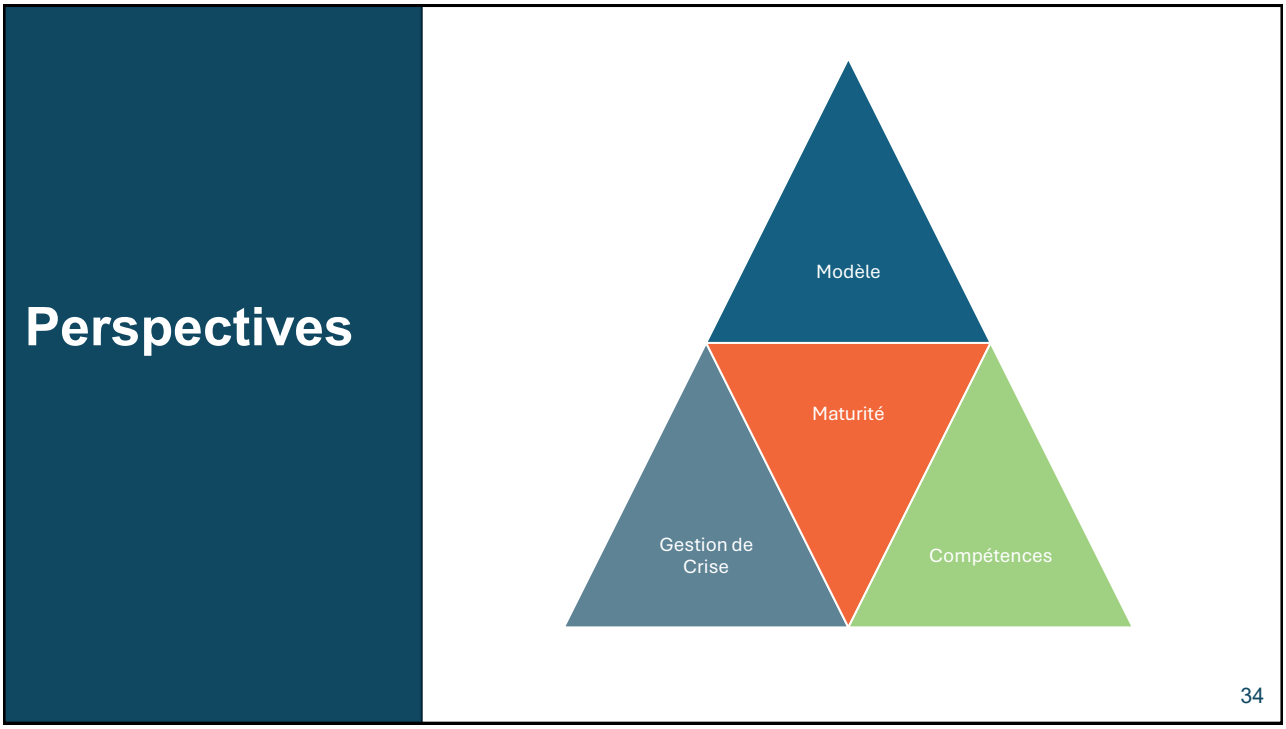


32

32


Échantillon
• Taille
• Géographie
• Typologie
Étude
• Exploratoire
• Qualitative
• Interne
Modèle
• Conceptuel
• Organisationnel
• Non testé
Limites
33

33


Perspectives
Modèle
Maturité
Gestion de Crise
Compétences
34

34

Un an après (1/2) : la menace a changé de vitesse

31 %

des accès initiaux passent par l'exploitation de vulnérabilités : 1er vecteur, une première en 19 ans

Verizon DBIR 2026 · correctif complet médian : 43 jours (contre 32)

6 sur 10

intrusions dont le vecteur est identifié passent par une vulnérabilité

ENISA Threat Landscape 2026 · 8 257 incidents (2025)

−7 jours

délai moyen d'exploitation : l'attaquant passe, en moyenne, avant le correctif

Mandiant M-Trends 2026

80 à 90 %

d'une campagne d'espionnage exécutés par une IA (GTG-1002, ~30 cibles)

Anthropic, nov. 2025 · rapport d'éditeur, contesté : aucun IoC publié

Boyd : la bataille du tempo… à la vitesse machine

35

35

Un an après (2/2) : les règles bougent



Les sources publiques se fragilisent

NVD : depuis le 15 avril 2026, l'enrichissement est réservé en priorité aux vulnérabilités exploitées (KEV) et aux logiciels critiques.

Le contexte, il faut désormais le produire chez soi



Le partage devient une obligation

CRA : les fabricants signalent sous 24 h les vulnérabilités activement exploitées.

Pour signaler en 24 h, l'information doit d'abord remonter en interne



L'IA entre au SOC… et devient une cible

Agents d'IA au sommet du « pic des attentes » (Gartner, 2026) ; ATT&CK v20 décrit les attaques contre l'IA de défense.

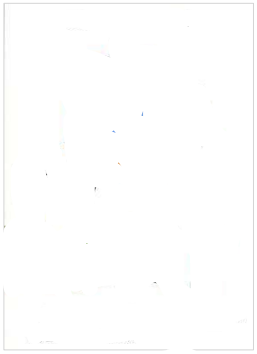
Un nouvel acteur dans la boucle, à gouverner

36

36

Le fil rouge, version 2026 : ce que l'IA a changé

	À cause de l'IA	Grâce à l'IA
Technique	L'exploitation précède souvent le correctif : les IoCs arrivent après la bataille	Moins d'enrichissement « gratuit » : la TIP et le croisement des sources deviennent indispensables
Tactique	L'exploit se fabrique en heures ; l'IA de la défense devient elle-même une cible	Des règles de détection écrites et testées plus vite (ATT&CK v20, agents de SOC)
Opérationnelle	Les mêmes techniques… à la vitesse machine et à grande échelle	L'IA lit, corrèle et résume les campagnes pour l'analyste
Stratégique	Près de 50 000 CVE publiées par an : le correctif devient le goulot	Découvrir avant l'attaquant ; prioriser selon l'exploitation réelle (KEV)

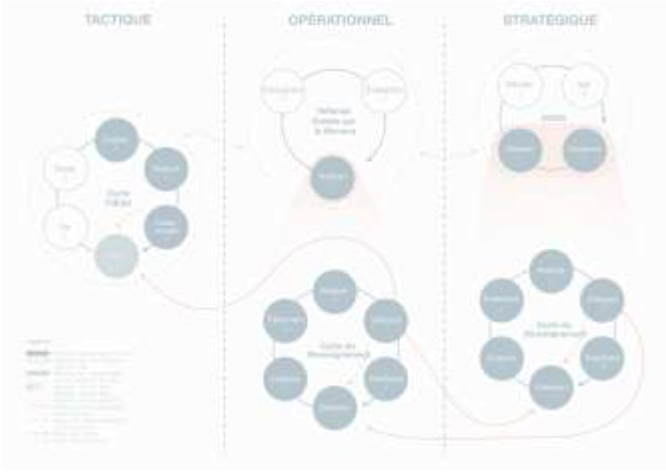


L'IA ne change pas les quatre lectures : elle change leur vitesse.

37

37

Et ORION, un an après ?



ATT&CK v20 : l'IA de défense est désormais une cible

1. **L'accélération rend-elle la circulation interne plus critique ?**
2. **L'IA sera-t-elle le moteur de la circulation… ou la consommation passive d'IoCs, à la vitesse machine ?**
3. **Un nouveau frein est-il apparu : la gouvernance des agents IA eux-mêmes ?**

À vous la parole : levez la main

38

38

De la rondache au pavois





« Passer du besoin d'en connaître au besoin de partager, pour que le renseignement soit enfin Utile, Utilisable… et Utilisé. »

39

Merci de votre attention

Avez-vous des questions?

fstricher@me.com 40

40

Annexe · Glossaire

APT Advanced Persistent Threat
ATT&CK base MITRE des tactiques et techniques adverses
BAS Breach and Attack Simulation
CERT / CSIRT équipe de réponse aux incidents
CTI Cyber Threat Intelligence, renseignement sur la menace
DFIR investigation numérique et réponse
EDR / XDR détection et réponse sur les postes / étendue
EPSS probabilité d'exploitation d'une vulnérabilité
IoC indicateur de compromission
KEV catalogue CISA des vulnérabilités exploitées
PIR besoin prioritaire en renseignement
SIEM corrélation des journaux de sécurité
SOAR orchestration et automatisation de la réponse
SOC centre des opérations de sécurité
STIX / TAXII format et transport de la CTI
TID défense guidée par la menace
TIP plateforme de renseignement sur la menace
TLP Traffic Light Protocol, code de diffusion
TTP tactiques, techniques et procédures

Annexe · Sources de la partie « un an après »

Verizon, Data Breach Investigations Report 2026 (SecurityWeek, TechTarget, mai 2026)
ENISA, Threat Landscape 2026 (22/09/2026) ; Help Net Security (24/09/2026)
Mandiant, M-Trends 2026 (cité par la Cloud Security Alliance)
Anthropic, « Disrupting the first reported AI-orchestrated cyber espionage campaign », 13/11/2025
Critiques du rapport GTG-1002 : BleepingComputer, CyberScoop, heise (novembre 2025)
ANSSI, Panorama de la cybermenace 2025 (11/03/2026) ; Le Monde Informatique
NIST, annonce NVD du 15/04/2026 (Help Net Security, CSA)
Commission européenne, CRA : obligations de signalement ; Help Net Security, lancement de la SRP (11/09/2026)
MITRE ATT&CK, Updates : octobre 2025 (v18), avril 2026 (v19), octobre 2026 (v20)
Gartner, Hype Cycle for Security Operations 2026 ; sondage sur les agents IA (T2 2026)

ORION minimal : trois gestes, sans équipe CTI



1 · Nommer

Une personne chargée de faire circuler le renseignement.

Un rôle, pas un outil



2 · Ritualiser

Après chaque incident : qu'avons-nous appris ? Qui doit le savoir ? Quelle règle change ?

Et une note régulière à la direction



3 · Questionner

La direction pose une ou deux questions prioritaires : de quoi avons-nous le plus peur ?

La question qui lance le cycle

La TIP vient ensuite : **elle accélère une circulation, elle ne la remplace pas.**

43

43