

NORME EN18031

L'arme anti-hack des objets connectés

Laurent MOULIN
Expert cybersécurité
lmoulin@spartan-conseil.fr



Qui suis-je

- Expert cybersécurité (+15ans)
- Travail avec des TPE jusqu'aux grands groupes internationaux
- Accompagne sur la sécurité IT, OT, IOT, ...



Disclaimer



Directive RED



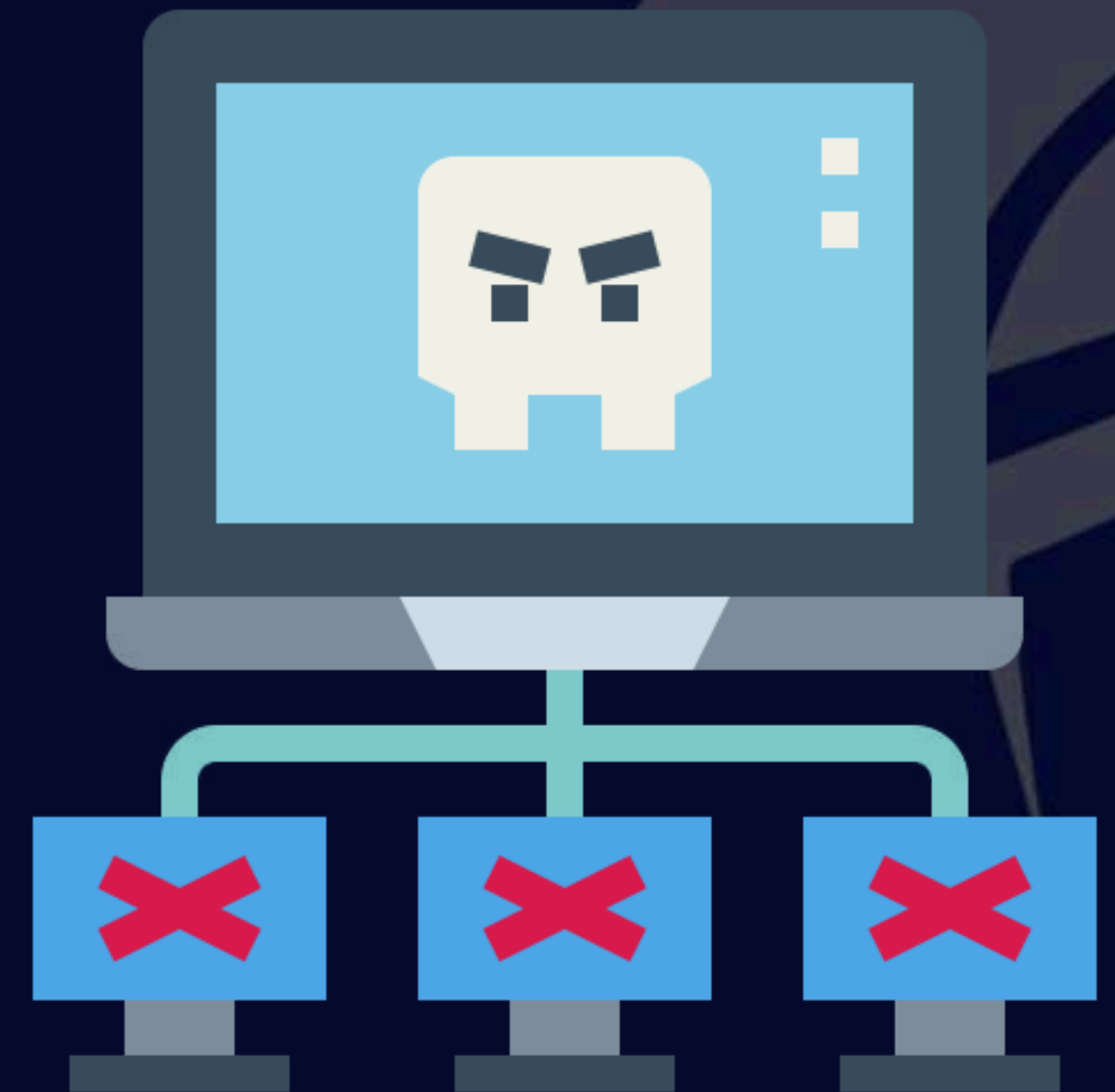
- Mise en application depuis 2016-2017 hors cyber
- Inclusion de la cyber depuis le 1er août 2025



Pourquoi est-ce pertinent ?

Botnet Mirai

- 2016
- Botnet
- 600 000 devices (routeur wifi, camera IP, ...)



Modus operandi



- Scan d'IP automatisé
- Attaque par dictionnaire sur les login/mdp par défaut
- En cas de succès, déploiement sur la cible
 - Mise à disposition de la bande passante de la victime
- Chaque bot recherche de nouvelles victimes

OVH

- Septembre 2016
- DDOS (ping, syn, ...)
- 1.0-1.2 Tb/s
 - DDOS typ. en 2016 : ~10Gb/s
- D'autres acteurs ont aussi subi des attaques moindres, mais inaccessibles.



Remédiation



- Prise de contrôle des CNC (sinkholes)
- Blacklisting des signatures de Mirai
- Emission d'alertes par les CERTs concernant les devices compromis

Qui paie ?

- Les fabricants des devices ?
- Les utilisateurs des devices ?
- Les victimes des DDOS ?
- Les différents intermédiaires de sécurité ?



[AUM-5-1] : mot de passe unique par appareil

(si c'est simple pour vous, c'est simple pour l'attaquant)



Directive RED

Directive 2014/53/eu

Articles :

- 3.d : L'équipement radio ne doit pas perturber ou affaiblir le fonctionnement du réseau auquel il est connecté.
- 3.e : L'équipement radio doit garantir la protection des données personnelles et de la vie privée des utilisateurs.
- 3.f : L'équipement radio qui permet des paiements ou des transactions électroniques doit offrir une protection contre la fraude



EN18031

- EN18031-1 : Tout ce qui possède une interface radio
- EN18031-2 : Tout ce qui traite de l'enfance, des données à caractère privé ou portable (wearable)
- EN18031-3 : tout ce qui touche à un enjeu financier



Il faut donc identifier la configuration



Harmonisée



- 30 janvier 2025
- Présomption de conformité si respecté (auto-déclaration)
- Organisme notifié

Vue générale



Assets
+
Interfaces



Requirements



Assessments

Assets



- EN18031-1 : network et security assets
- EN18031-2 : privacy et security assets
- EN18031-3 : financial and security assets

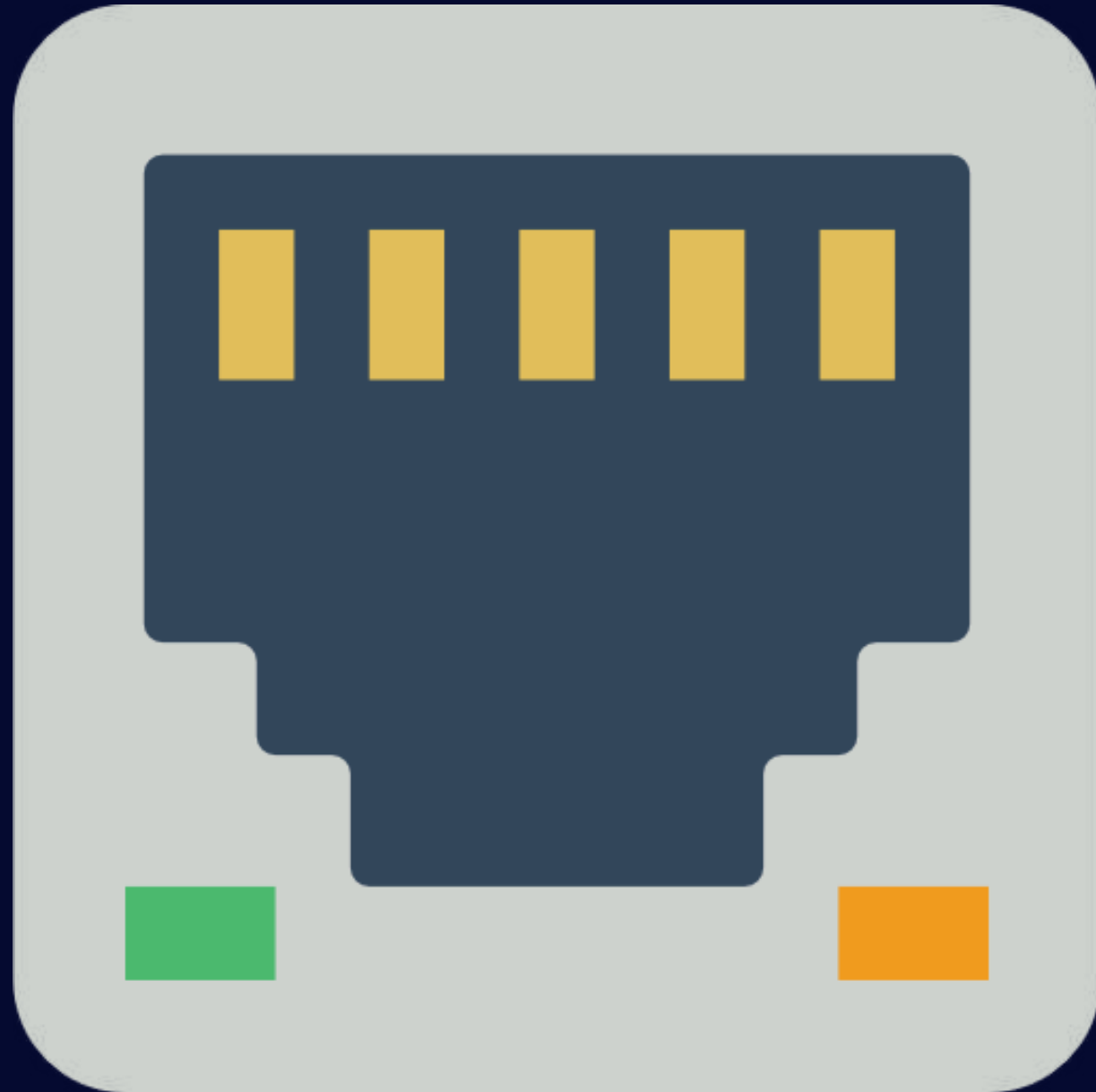
+ interfaces

Exemple d'asset

- security : mot de passe, clé privé, ...
- network : table de routage, serveur dns, serveur web pour la GUI, ...
- privacy : nom, adresse ip, coordonnées GPS, ...
- financial : numero de carte de credit, log de transaction, ...

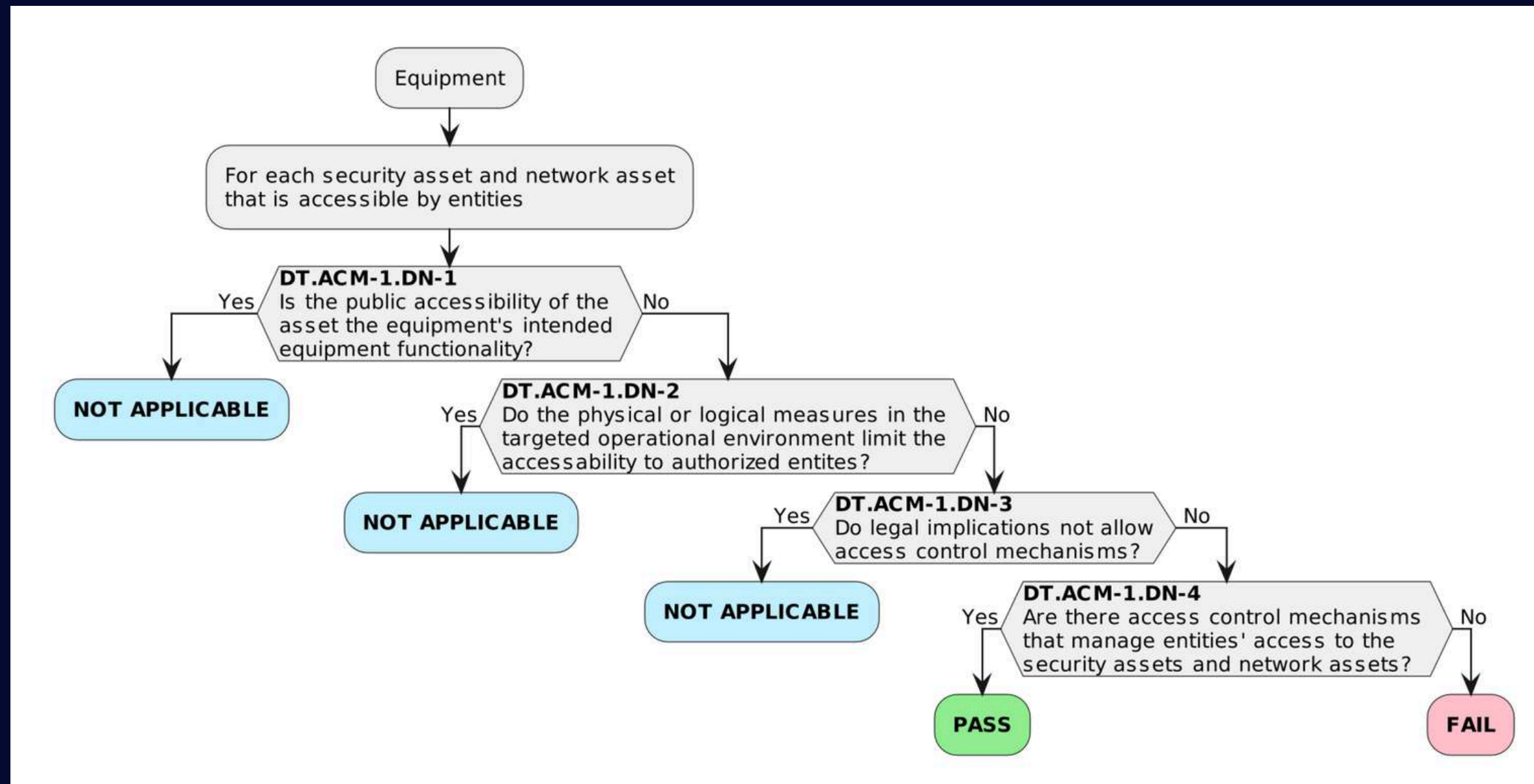


Interfaces



- user : ecran tactile, clavier, bouton,...
- machine : api rest, USB, ...
- network : lora, wifi, ethernet, ...

Requirements : decision trees



Basé sur des preuves

- Information
- Justification



Assessments



C'est la méthodologie utilisée par vous et l'auditeur

- conceptual assessment (est ce bien documenté ?)
- completeness assessment (Est-ce bien implémenté comme la documentation ?)
- sufficiency assessment (Est-ce que le protection est efficace dans le monde réel?)

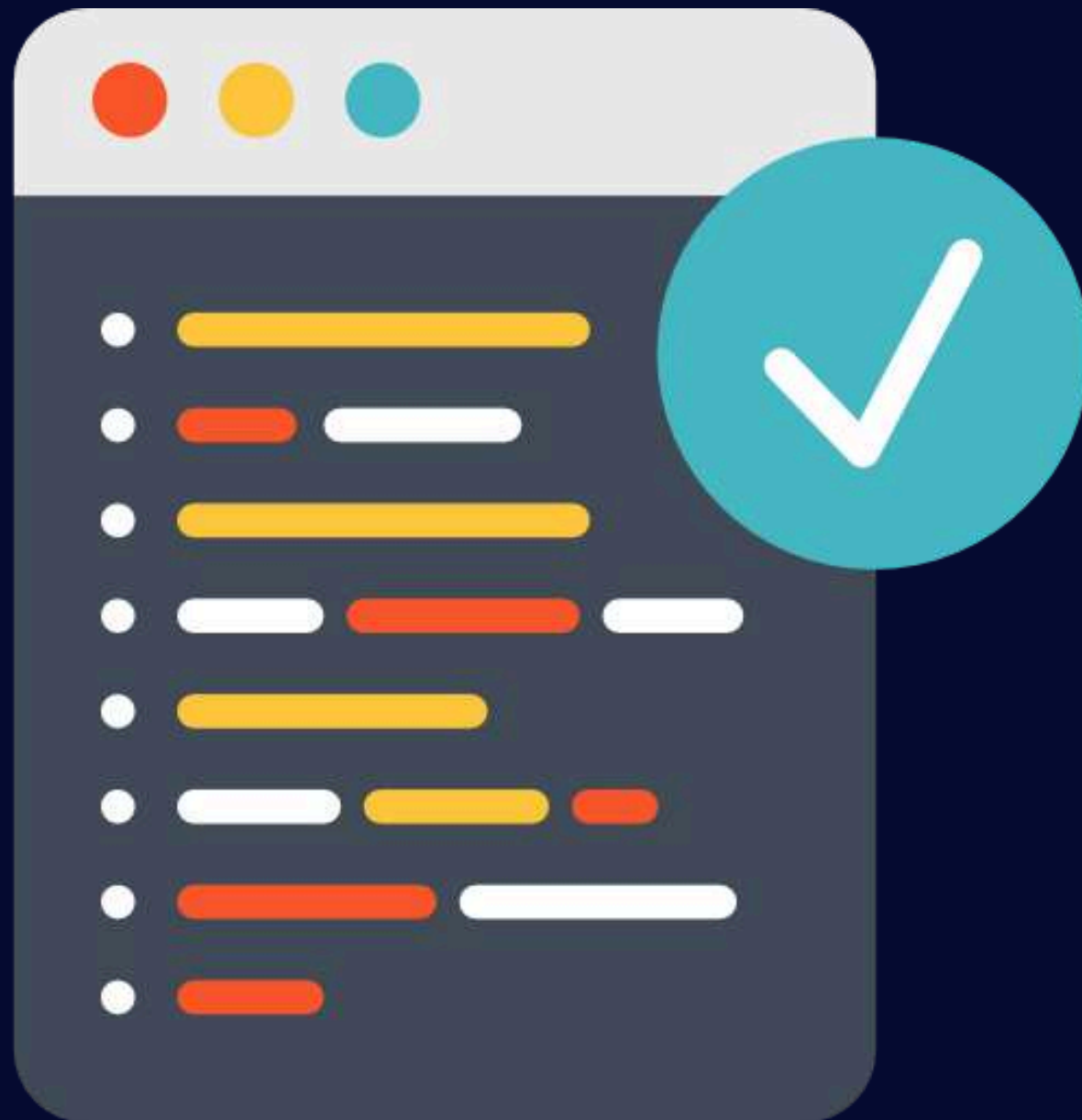
Conceptual assessment

Donne les éléments à vérifier dans la documentation créée.

Exemple : est-ce que ACM-1 documenté est bien en PASS ou non applicable, et est-ce que les informations et la justification sont valides



Completeness assessments



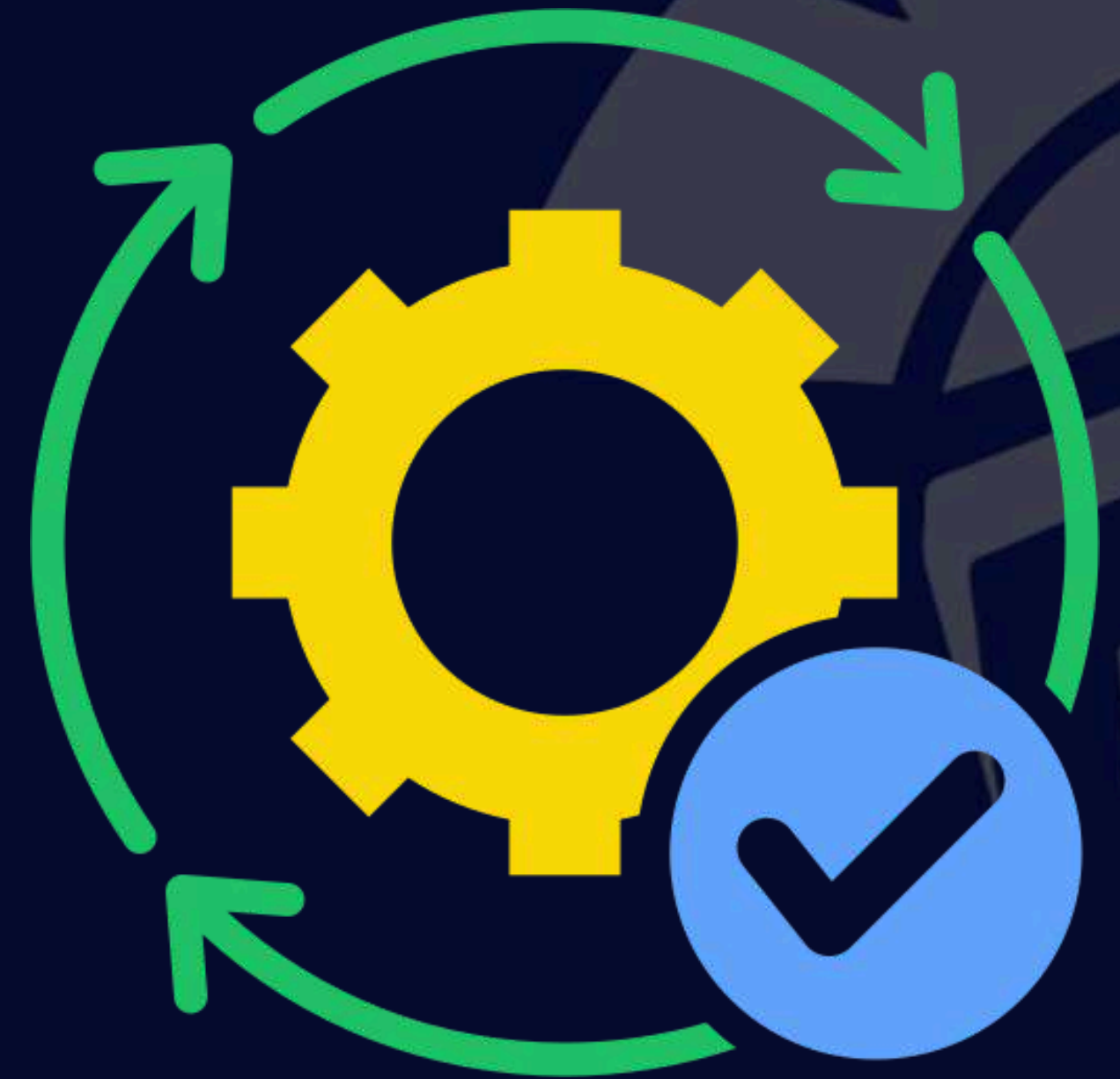
Donne les éléments à vérifier sur le produit pour vérifier que la documentation est conforme.

exemple : regarder le code montrant la gestion d'un bearer token sur une API rest.

Sufficiency assessment

Donne la méthodologie de test pour l'équipement en fonctionnement, permettant de valider le mécanisme de sécurité.

exemple : réaliser un curl sans authentification, avec un bearer invalid, fuzzing, ...



Comment réaliser la documentation ?



- Par vous même (ex nihilo)
- Par vous même avec un logiciel d'assistance
- Via un cabinet conseil / organisme notifié

Par vous même

- Prévoir une courbe d'apprentissage

"Si vous m'avez bien compris, c'est que je me suis mal exprimé" Alan Greenspan

- Fabrication des templates
- Nécessite des compétences cyber

Templates open source pouvant vous aider (zealience, github)



Assisté par logiciel



- Cout relativement abordable
- Gain de temps
- Dépendance au dit logiciel
- Nécessite des compétences cyber

exemple : <https://www.complerion.com/>

Externaliser

- Clef en main
- Coût important
- Mais moins transparent, aller-retour, questionnaire à rallonge ...
- Nécessite parfois des compétences cyber pour répondre aux questions



Merci pour votre attention

