NIST Rapport interne
NIST IR 8425 fre

Profil du noyau de base de l'IdO pour les produits IdO grand public

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffery Marron
Barbara Cuthill

Cette publication est disponible gratuitement auprès de :
https://doi.org/10.6028/NIST.IR.8425.fre

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Rapport interne
NIST IR 8425 fre

Profil du noyau de base de l'IdO pour les produits IdO grand public

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Division de la cybersécurité appliquée
Laboratoire de technologie de l'information

Cette publication est disponible gratuitement auprès de :
https://doi.org/10.6028/NIST.IR.8425.fre

septembre 2022

Département du commerce des États-Unis
Gina M. Raimondo, Secrétaire

Institut national des normes et de la technologie
Laurie E. Locascio, directrice du NIST et sous-secrétaire au commerce pour les normes et la technologie

Certaines entités commerciales, certains équipements ou matériaux peuvent être identifiés dans le présent document afin de décrire correctement une procédure ou un concept expérimental. Cette identification n'a pas pour but d'impliquer une recommandation ou une approbation par le National Institute of Standards and Technology (NIST), ni d'impliquer que les entités, les matériaux ou l'équipement sont nécessairement les meilleurs disponibles pour l'objectif visé.

Le NIST peut faire référence à d'autres publications en cours d'élaboration conformément aux responsabilités statutaires qui lui sont attribuées. Les agences fédérales peuvent utiliser les informations de cette publication, y compris les concepts et méthodologies, avant même que ces publications complémentaires ne soient finalisées.. Ainsi, jusqu'à ce que chaque publication soit achevée, les exigences, lignes directrices et procédures actuelles, lorsqu'elles existent, restent en vigueur. À des fins de planification et de transition, les agences fédérales peuvent souhaiter suivre de près l'élaboration de ces nouvelles publications par le NIST.

Le NIST invite les organisations à examiner tous les projets de publication pendant les périodes de consultation publique et à lui soumettre leurs commentaires. De nombreuses publications du NIST sur la cybersécurité, autres que celles mentionnées ci-dessus, sont disponibles à l'adresse suivante : https://csrc.nist.gov/publications.

Politiques de la série technique du NIST
Droits d'auteur, utilisation équitable et déclarations de licence
Syntaxe de l'identificateur de publication de la série technique du NIST

Historique de la publication
Approuvé par le comité de rédaction du NIST le 09/08/2022
Comment citer cette publication de la série technique du NIST :
Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425

ID ORCID des auteurs
Michael Fagan : 0000-0002-1861-2609
Katerina N. Megas : 0000-0002-2815-5448
Paul Watrobski : 0000-0002-6449-3030
Jeffrey Marron : 0000-0002-7871-683X
Barbara B. Cuthill : 0000-0002-2588-6165
Informations de contact
iotsecurity@nist.gov

Institut national des normes et de la technologie
A l'attention de : Division de la cybersécurité appliquée, Laboratoire des technologies de l'information
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

La loi sur l'accès à l'information peut entraîner la divulgation de tous les commentaires. (Freedom of Information Act, FOIA).

Rapports sur la technologie des systèmes informatiques

Le Laboratoire des technologies de l'information (ITL) du National Institute of Standards and Technology (NIST) promeut l'économie américaine et le bien-être public en assurant le leadership technique de l'infrastructure nationale de mesure et de normalisation. L'ITL développe des tests, des méthodes de test, des données de référence, des mises en œuvre de démonstration de faisabilité et des analyses techniques afin de faire progresser le développement et l'utilisation productive des technologies de l'information. Les responsabilités de l'ITL comprennent l'élaboration de normes et de lignes directrices en matière de gestion, d'administration, de technique et de physique pour une sécurité et une confidentialité rentables des informations autres que celles liées à la sécurité nationale dans les systèmes d'information fédéraux.

Résumé

Cette publication documente le profil du consommateur de la base de référence de l'Internet des objets (IdO) du NIST et identifie les capacités de cybersécurité généralement nécessaires pour le secteur de l'IdO grand public (c'est-à-dire les produits IdO destinés à un usage domestique ou personnel). Il peut également constituer un point de départ pour les entreprises lors de l'achat de produits IdO. Le NIST a développé le profil du consommateur en réponse à l'ordre exécutif 14028 et l'a initialement publié dans les *Critères recommandés pour l'étiquetage de la cybersécurité pour les produits de l'Internet des objets (IoT)*.

Le profil du consommateur formule les capacités sous forme de résultats en matière de cybersécurité, censés s'appliquer à l'ensemble du produit IdO. Ce document aborde également les fondements de l'élaboration du profil recommandé du consommateur et les considérations qui s'y rapportent. Le NIST a examiné un ensemble de documents sources pertinents pour établir le profil du consommateur et s'est engagé avec les parties prenantes dans un effort d'un an pour élaborer les recommandations.

Mots clés

Internet des objets (IdO) ; IdO grand public ; cybersécurité ; produits IdO ; vie privée ; sécurité ; produits sécurisables.

Audience

Le présent rapport s'adresse aux fabricants de produits de consommation, en particulier aux responsables de la sécurité des produits, aux détaillants, aux intégrateurs et aux sociétés d'assistance technique au service des consommateurs et des entreprises, ainsi qu'aux organismes de test et de certification désireux d'établir des normes de référence pour les capacités de cybersécurité de l'IdO.

Avis de divulgation de brevet

AVIS : L'ITL a demandé aux détenteurs de brevets dont l'utilisation peut être nécessaire pour se conformer aux orientations ou aux exigences de la présente publication de divulguer ces brevets à l'ITL. Toutefois, les détenteurs de brevets ne sont pas obligés de répondre aux appels à brevets de l'ITL et l'ITL n'a pas entrepris de recherche de brevets afin d'identifier les éventuels brevets applicables à la présente publication.

À la date de publication, suite à l'appel pour identifier les revendications de brevet nécessaires à la conformité avec les orientations ou exigences de cette publication, l'ITL n'a reçu aucune revendication de brevet.

ITL ne prétend pas que des licences ne sont pas nécessaires pour éviter la violation de brevets lors de l'utilisation de cette publication.

Table des matières

Liste des tableaux

Liste des figures

Remerciements

Les auteurs souhaitent remercier tous ceux qui ont contribué à cette publication, y compris les participants aux ateliers et autres sessions interactives, les personnes et les organisations des secteurs privé et public, y compris les fabricants de divers secteurs ainsi que plusieurs organisations professionnelles de fabricants, qui ont fait part de leurs commentaires pendant la période de réponse à l'ordre exécutif 14028 du NIST. Nous remercions tout particulièrement les membres de l'équipe "Cybersécurité pour l'IdO", Rebecca Herold, Brad Hoehn et David Lemire.

1. Introduction

Le 12 mai 2021, le président a publié le décret 14028 qui, entre autres directives, demandait au NIST de recommander des exigences pour un programme d'étiquetage de la cybersécurité des produits IoT grand public. Dans le cadre de la réponse du NIST à cette directive[1], un profil du noyau de base de l'IdO[2] pour les produits IdO grand public a été créé. Ce profil a fait partie des recommandations que le NIST a publiées en février 2022 en réponse à l'ordonnance d'urgence et qui s'intitulent *Critères recommandés pour l'étiquetage de la cybersécurité des produits de l'internet des objets (IdO) destinés aux consommateurs* [Critères EO].

Le profil s'appuie sur la série NISTIR 8259 en étendant la base de référence de l'IdO aux produits IdO grand public. Le NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [IR8259], fournit des orientations fondamentales aux fabricants d'appareils IoT concernant le développement d'appareils IoT qui peuvent être utilisés en toute sécurité par les clients. Le NISTIR 8259 ne cible aucun secteur IoT spécifique, mais examine comment les fabricants peuvent aborder la cybersécurité pour les dispositifs IoT en général. NISTIR 8259A, *IoT Device Cybersecurity Capability Core* Baseline[IR8259A] et NISTIR 8295B, *IoT Non-Technical Supporting Capability Core Baseline* [IR259B] définissent le noyau de base des capacités de cybersécurité des dispositifs IoT (également appelé noyau de base). Le référentiel de base est un point de départ que les fabricants peuvent utiliser pour identifier les capacités de cybersécurité que leurs clients peuvent attendre des dispositifs IdO qu'ils créent. Le NISTIR 8259A traite des capacités de cybersécurité des appareils, qui sont des fonctions ou des caractéristiques mises en œuvre par l'appareil au moyen de son propre matériel et de son propre logiciel. Par exemple, le NISTIR 8259A aborde des concepts tels que la protection des données, le contrôle d'accès et la mise à jour des logiciels, entre autres. Le NISTIR 8259B traite des capacités de soutien non techniques, qui sont des mesures prises par les organisations pour soutenir la cybersécurité de l'appareil. Par exemple, le NISTIR 8259B aborde des concepts tels que l'éducation et la sensibilisation, ainsi que la réception d'informations et de requêtes (par exemple, par les fabricants/développeurs).

Comme le NISTIR 8259, ces documents de référence ne sont pas spécifiques à un secteur ou à un cas d'utilisation, mais constituent un point de départ pour *tout* appareil IoT. L'adaptation des capacités de base à un secteur et/ou à un cas d'utilisation spécifique nécessite une forme de profilage. Le processus d'établissement de profils à l'aide de la série NISTIR 8259 demande au profileur de rassembler des informations spécifiques à un secteur ou à un cas d'utilisation et d'interpréter les impacts pertinents pour sélectionner les capacités de base les plus adaptées aux besoins et aux objectifs des clients dans le secteur ou le cas d'utilisation en question.

Le reste de ce document décrit les résultats de ce processus de profilage pour le secteur de la consommation et est organisé comme suit :

[1] Pour plus d'informations sur la réponse du NIST à l'appel à recommandations de l'EO 14028 concernant un label de cybersécurité pour les produits IoT grand public, consultez le site https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0

[2] Les termes « base de référence », « Base de référence de l'IdO » et « Base de référence des capacités de base des appareils IdO » font tous référence à l'ensemble des capacités présentées dans les NISTIRs 8259A et 8259B.

- La section 2 explique l'applicabilité prévue du profil du consommateur aux produits IdO grand public et définit le profil du consommateur.
- La section 3 décrit plus en détail le processus d'élaboration du profil du consommateur.
- La section 4 explore les considérations supplémentaires que les lecteurs doivent prendre en compte lorsqu'ils utilisent le profil du consommateur.

2. Profil du consommateur de la base de référence de l'IdO

Cette section s'appuie sur le livre blanc intitulé *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Critères recommandés pour l'étiquetage des produits de l'internet des objets destinés aux consommateurs)* [Critères EO]. On définit d'abord le champ d'application d'un "produit IdO", puis on présente le profil du produit IdO grand public de la base de référence de l'IdO.

2.1. Déclaration sur la portée des produits IdO

Consommateur Les produits IdO constituent souvent un ensemble de composants de système qui fonctionnent ensemble pour fournir une fonctionnalité réalisée au point final ou au composant "appareil" du produit. Le NIST décrit un dispositif IdO comme un équipement informatique doté d'au moins un transducteur (c'est-à-dire un capteur ou un actionneur) et d'au moins une interface réseau [IR8259]. Tous les produits IdO contiennent au moins un dispositif IdO et peuvent ne contenir que ce composant de produit. Dans de nombreux cas, le produit IdO peut être acheté en tant qu'équipement unique (c'est-à-dire l'appareil IdO), mais il nécessite néanmoins d'autres composants pour fonctionner, tels qu'un backend (par exemple, un serveur en nuage) ou une application utilisateur complémentaire sur un ordinateur personnel ou un smartphone.

Les produits IdO complexes peuvent contenir plusieurs dispositifs IoT physiques, d'autres types d'équipements, ou se connecter à plusieurs backends ou applications compagnons en tant que composants. Même si de nombreuses combinaisons de composants peuvent former un produit IdO, on peut utilement se concentrer sur trois types spécifiques de composants, en plus de l'appareil IdO lui-même, toujours présent dans un produit IdO :

- Un concentrateur ou autre matériel spécialisé de mise en réseau/passerelle assure la connexion des dispositifs IdO dans le système.
- Logiciel d'application compagnon (par exemple, une application mobile pour communiquer avec l'appareil IdO).
- Backends (par exemple, un service en nuage, ou plusieurs services, qui peuvent stocker et/ou traiter des données provenant de l'appareil IdO).

Certains composants du produit IdO, tels que le(s) dispositif(s) IdO (et éventuellement un matériel spécialisé de réseau/passerelle[3]) seront « dans la boîte » que le client achète.[4] D'autres composants, tels que les logiciels d'application compagnons ou les backends, existeront « en dehors de la boîte[5] », mais feront néanmoins partie du produit IdO par le soutien qu'ils apportent au fonctionnement du produit IdO. Indépendamment de ces relations, ces composants supplémentaires ont accès à l'appareil IdO et aux données qu'il crée et utilise, ce qui en fait des vecteurs d'attaque potentiels susceptibles d'avoir un impact sur l'appareil IdO, le client et d'autres personnes (par exemple, par le biais d'attaques sur les systèmes, les réseaux locaux ou l'internet en général). Étant donné que ces composants supplémentaires peuvent introduire des risques nouveaux ou uniques pour le produit IdO, l'ensemble du produit IdO, y compris les composants auxiliaires, doit pouvoir être sécurisé.

Note sur les considérations relatives à l'évaluation de la conformité des composants IdO

Ce document définit les capacités au niveau du produit IdO et présente les produits IdO comme un ensemble de composants. Lorsqu'on évalue la conformité dans ce contexte, la complexité liée à la diversité des combinaisons de composants IdO susceptibles de constituer un produit mérite d'être soulignée. En outre, certains de ces composants de produits IdO peuvent être entièrement ou partiellement *modulaires*, ce qui permet aux clients de choisir le composant et/ou la plateforme du composant. Par exemple, certains logiciels d'application compagnons fonctionneront sur des systèmes d'exploitation mobiles ou par l'intermédiaire d'un navigateur web, pour lesquels la cybersécurité va bien au-delà du rôle que le composant peut jouer dans le produit IdO. Dans ce cas, l'évaluation de la conformité de ces composants de produits IdO aux capacités de cybersécurité du profil du consommateur doit tenir compte de ce fait et utiliser autant que possible les normes et/ou les mécanismes de conformité existants dans le cadre du mécanisme de conformité des produits IdO. Par exemple, il peut exister des programmes de certification de la cybersécurité des systèmes d'exploitation ou de l'informatique en nuage qui peuvent démontrer une prise en charge partielle des capacités de cybersécurité identifiées dans le profil du consommateur, mais dans de nombreux cas, la prise en charge du produit

[3] Le client peut acheter séparément du matériel spécialisé pour les réseaux et les passerelles, mais ce matériel est néanmoins nécessaire pour que le produit IdO puisse fonctionner au-delà des fonctions de base. Dans la plupart des cas où un produit IdO nécessite un matériel réseau/passerelle spécialisé acheté séparément, ce matériel effectuera des tâches spécifiques et cohérentes dans la mise en œuvre d'un produit IdO (par exemple, la traduction de protocoles). Par exemple, certains produits IdO nécessitent des connexions réseau autres que les connexions Wi-Fi/éthernet classiques, telles que Bluetooth, Zigbee ou Z-Wave, qui nécessiteraient un *concentrateur* ou une *passerelle* pour permettre une connectivité plus large (c.-à-d. par Wi-Fi et/ou Ethernet). Ce *concentrateur* ou cette passerelle n'est pas toujours inclus dans un produit IdO et est plutôt considéré comme faisant partie de l'infrastructure réseau du client, tout comme un routeur Wi-Fi est considéré comme faisant partie des produits IdO utilisant le Wi-Fi.

[4] Les composants « dans la boîte », en particulier le(s) dispositif(s) IdO qui sert(nt) de point final au produit, peuvent être considérés comme le *visage du* produit IdO, car c'est ce que le client manipulera, gérera et utilisera physiquement. Bien que d'autres composants puissent être essentiels au fonctionnement du produit IdO (y compris la cybersécurité), le(s) dispositif(s) IdO joue(nt) un rôle central dans le produit IdO et, en général, est(sont) au centre du fonctionnement du produit IdO.

[5] Certains composants « externes » peuvent être entièrement éloignés du client, tandis que d'autres peuvent être physiquement présents dans l'environnement du client (par exemple, à l'intérieur de son domicile), mais sont néanmoins distincts du ou des dispositifs IdO.

par le composant IdO se fera à l'aide de logiciels d'application et/ou de matériel supplémentaires qui peuvent ne pas être pris en compte ou évalués par les programmes existants. L'évaluation de la cybersécurité du produit IdO peut donc accepter la certification existante et évaluer la cybersécurité du logiciel/matériel d'application supplémentaire.

Dans ce contexte, on définit un produit IdO comme un appareil IdO, ou un ensemble d'appareils IdO, accompagné de tout composant supplémentaire nécessaire à son utilisation, au-delà de ses fonctions opérationnelles de base. Par exemple, une ampoule intelligente non connectée éclaire toujours d'une couleur, mais les autres composants du produit sont nécessaires pour activer ses fonctions intelligentes, comme le changement de couleur.

2.2. Profil du consommateur

Cette section définit les capacités de cybersécurité[6] attendues des produits IdO et de leurs développeurs dans le cadre d'un profil de consommateur.

Il est recommandé d'appliquer les critères de produit à l'ensemble du produit IdO, , ainsi qu'à chaque composant individuel du produit IdO, le cas échéant. La plupart des critères concernent directement le produit IdO et le produit doit les satisfaire via des moyens logiciels et/ou matériels intégrés. Certains critères s'appliquent au développeur du produit IdO plutôt qu'au produit IdO lui-même. Le développeur doit satisfaire à ces critères par des actions, soutenues par des affirmations et des preuves, plutôt que par le produit IdO lui-même.

La figure suivante présente les capacités de haut niveau des produits IdO et les activités du développeur de produits IdO[7] développées sur la base des NISTIRs 8259A et 8259B, respectivement, qui sont discutées dans les sections ci-dessous.

[6] Le présent document utilise généralement le terme « capacité » en référence à la série NISTIR 8259, mais ces mêmes capacités ont été présentées comme des « résultats » dans la section 2.2 des *critères recommandés pour l'étiquetage de la cybersécurité des produits IoT destinés aux consommateurs*. Ces termes sont synonymes et peuvent être utilisés de manière interchangeable dans le contexte du présent document et du livre blanc.

[7] La série NISTIR 8259 mentionne les fabricants d'appareils IdO, qui peuvent être la même entité que le développeur de produits IdO évoqué ici. La nature multicomposante des produits IdO augmente toutefois le risque que l'entité qui commercialise un produit IdO n'ait pas fabriqué le ou les dispositifs physiques IdO, mais ait plutôt utilisé des dispositifs fabriqués par une autre entité pour créer un produit IdO. C'est pourquoi ce document utilise le terme « développeur de produits IdO ».

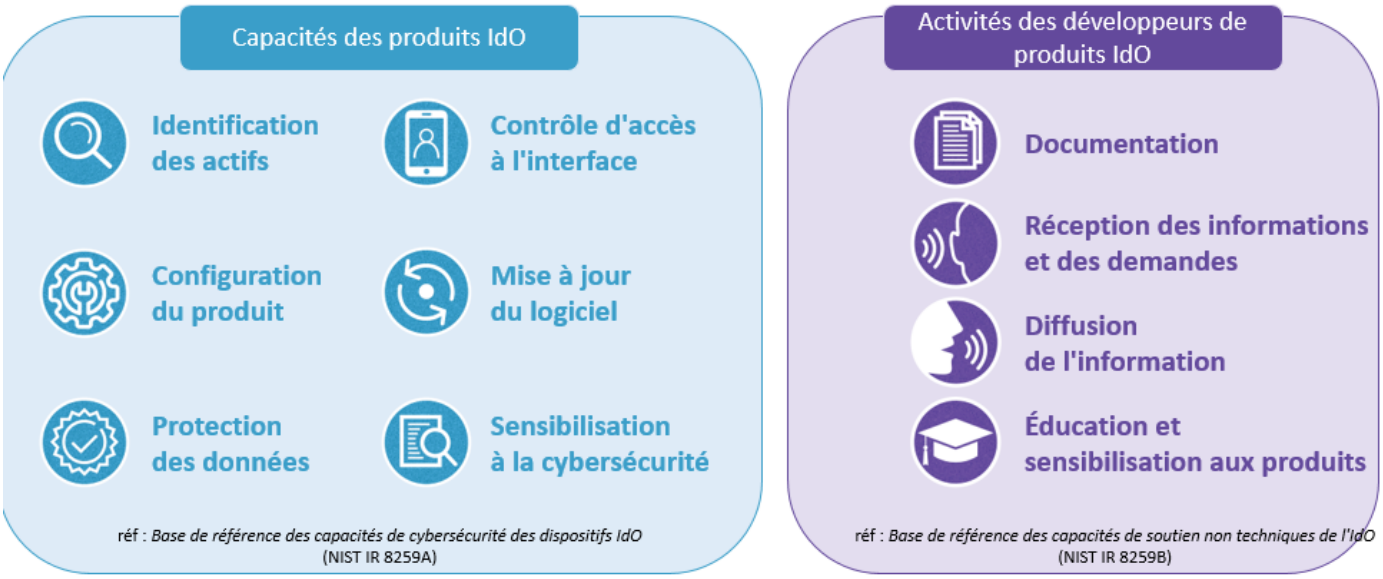

Fig. 1. Capacités identifiées pour le profil du consommateur.

Le nom et la définition de haut niveau de chaque capacité sont présentés, suivis d'une liste alphanumérique de sous-critères pour chaque capacité. Pour certains sous-critères[8], le texte normatif détaillant le résultat figure après le texte **en gras**, tandis que les explications et exemples supplémentaires, en texte informatif, suivent le texte *en italique*. Enfin, chaque capacité est accompagnée d'une brève description de l'utilité qu'elle est censée avoir en matière de cybersécurité.

[8] Les sous-critères fournissent des détails supplémentaires sur la manière dont un produit IdO peut atteindre le résultat décrit dans la définition de la capacité de haut niveau. Les sous-critères peuvent ne pas être exhaustifs de tous les soutiens possibles nécessaires pour un résultat dans tous les cas d'utilisation, et les sous-critères peuvent également ne pas s'appliquer à tous les cas d'utilisation.

2.2.1. Capacités des produits IdO

Identification des actifs

Le produit IdO est identifiable de manière unique et inventorie tous ses composants.

1. Le client et les autres entités autorisées peuvent identifier de manière unique le produit IdO.(par exemple, le développeur du produit IdO).[9]
2. Le produit IdO identifie de manière unique chaque composant du produit IdO et tient à jour un inventaire[10] des composants du produit connecté.

Service public de cybersécurité : La capacité à identifier les produits IdO et leurs composants est nécessaire pour soutenir des activités telles que la gestion des actifs pour les mises à jour, la protection des données et les capacités de criminalistique numérique pour la réponse aux incidents.

[9] Dans certains cas, un identifiant unique peut être attribué au produit IdO lui-même, indépendamment de l'identifiant du dispositif IdO. Cependant, dans de nombreux cas, l'identification du produit IdO correspond généralement à celle de l'un de ses composants. Pour garantir l'unicité de l'identifiant du produit dans toutes les instances du produit, il s'agit généralement de l'appareil IoT ou d'un autre composant "dans l'emballage", plutôt que d'un composant partagé par de nombreuses instances, comme le backend.

[10] Les inventaires peuvent résider sur un composant (par exemple, dispositif IdO, application dorsale) ou sur plusieurs composants (par exemple, l'architecture du produit IdO inventorie certains composants sur un matériel de réseau ou une passerelle spécialisée.

Configuration du produit

Les personnes, services et composants autorisés peuvent modifier la configuration du produit IdO, rétablir un réglage par défaut sécurisé, et effectuer toutes les autres modifications.

1. Les personnes autorisées (c'est-à-dire le client), les services et les autres composants du produit IdO peuvent modifier les paramètres de configuration du produit IdO par l'intermédiaire d'un ou de plusieurs composants du produit IdO.[11]
2. Les personnes autorisées (c'est-à-dire le client), les services et les autres composants du produit IdO ont la possibilité de rétablir le produit IdO dans une configuration sécurisée par défaut (c'est-à-dire non initialisée).
3. Le produit IdO applique les paramètres de configuration aux composants IoT applicables.

Service public de cybersécurité : La possibilité de modifier certains aspects du fonctionnement du produit IdO peut aider les clients à adapter les fonctionnalités du produit IdO à leurs besoins et à leurs objectifs. Les clients peuvent configurer leurs produits IdO pour éviter les menaces et les risques spécifiques dont ils ont connaissance, en fonction de leur appétence au risque.

[11] Certains composants peuvent nécessiter une configuration spécifique (par exemple, la plateforme ou l'infrastructure des backends) pertinente pour la cybersécurité, que le produit IdO et/ou le client ne gèrent pas toujours correctement. Par exemple, dans la plupart des cas, le logiciel d'application compagnon du produit IdO ne devrait pas gérer la cybersécurité du système d'exploitation sur lequel le logiciel fonctionne.

Protection des données

Le produit IdO protège les données stockées dans tous les composants du produit IdO et transmises à la fois entre les composants du produit IdO et en dehors du produit IdO contre tout accès, toute divulgation et toute modification non autorisées.

1. Chaque composant de produit IdO protège les données qu'il stocke par des moyens sécurisés.
2. Le produit IdO peut supprimer ou rendre inaccessibles les données collectées auprès du client, de son domicile, de sa famille, ou qui le concernent..
3. Lorsque des données sont transmises entre les composants d'un produit IdO ou vers l'extérieur, le produit utilise des protections pour sécuriser la transmission.[12]

Service public de cybersécurité : Le maintien de la confidentialité, de l'intégrité et de la disponibilité des données est fondamental pour la cybersécurité des produits IdO. Les clients s'attendent à ce que le produit IdO protège leurs données et que cette protection contribue à garantir sa sécurité et son bon fonctionnement.

[12] Cela peut inclure la capacité de communiquer avec des composants du produit qui ne peuvent pas mettre en œuvre la capacité de protection des données de la même manière que les autres composants (par exemple, ils ne peuvent pas prendre en charge une cryptographie adéquate). Ce type de communication, comme la transmission de données avec une protection réduite ou limitée, doit toujours être réalisé de manière à minimiser le risque. Cela peut se faire, par exemple, en utilisant un protocole de transmission à courte portée ou un réseau local (comme Zigbee ou Bluetooth) pour communiquer avec certains composants du produit dans des circonstances spécifiques, mais nécessaires.

Contrôle d'accès à l'interface

Le produit IdO limite l'accès logique aux interfaces locales et réseau - ainsi qu'aux protocoles et services utilisés par ces interfaces - aux seules personnes, services et composants du produit IdO autorisés.

1. Chaque composant de produit IdO contrôle l'accès à et depuis toutes les interfaces (par exemple, les interfaces locales, qu'elles soient accessibles de l'extérieur ou non, les interfaces réseau, les protocoles et les services) afin de limiter l'accès aux seules entités autorisées. **Au minimum, le composant du produit IdO doit :**
    a. N'utiliser et n'avoir accès qu'aux interfaces nécessaires au fonctionnement du produit IdO. Le système supprime ou sécurise tous les autres canaux et accès à ces canaux.
    b. Pour toutes les interfaces nécessaires à l'utilisation du produit IdO, des mesures de contrôle d'accès sont en place (par exemple, authentification multifactorielle basée sur un mot de passe unique, ports d'interface physiques inaccessibles depuis l'extérieur d'un composant).
    c. Pour toutes les interfaces, les privilèges d'accès et de modification sont limités.
2. Certains composants de produits IdO, mais pas nécessairement tous, disposent des moyens de protéger et de maintenir le contrôle d'accès à l'interface. **Au minimum, le produit IdO doit :**
    a. Valider que les données partagées entre les composants du produit IdO correspondent aux définitions de format et de contenu spécifiées.
    b. Empêcher les transmissions non autorisées ou l'accès à d'autres composants du produit.
    c. Maintenir un contrôle d'accès approprié lors de la connexion initiale (c'est-à-dire l'accueil) et lors du rétablissement de la connectivité après une déconnexion ou une panne.

Service public de cybersécurité : L'énumération et le contrôle de l'accès à toutes les interfaces internes et externes du produit IdO contribueront à préserver la confidentialité, l'intégrité et la disponibilité du produit IdO, de ses composants et de ses données en empêchant les accès et les modifications non autorisés.

Mise à jour du logiciel

Les personnes, services et composants autorisés peuvent mettre à jour le logiciel[13] de tous les composants des produits IdO en utilisant un mécanisme sécurisé et configurable, adapté aux besoins de chaque composant.

1. Chaque composant de produit IdO peut recevoir, vérifier et appliquer des mises à jour logicielles vérifiées.
2. Le produit IdO met en œuvre des mesures visant à maintenir à jour les logiciels installés sur les composants du produit IdO (application automatique des mises à jour ou notification cohérente au client des mises à jour disponibles via le produit IdO).

Service public de cybersécurité : Les logiciels peuvent présenter des vulnérabilités découvertes après le déploiement du produit IdO ; les capacités de mise à jour des logiciels peuvent contribuer à garantir la livraison sécurisée des correctifs de sécurité.

[13] Cela comprend le code exécutable, ainsi que les bibliothèques logicielles, les packs d'assistance et d'autres données logicielles non exécutables.

Sensibilisation à la cybersécurité

Le produit IdO permet de détecter les incidents de cybersécurité qui affectent ou sont affectés par les composants du produit IdO et les données qu'ils stockent et transmettent.

1. Le produit IdO capture et enregistre en toute sécurité des informations sur l'état de ses composants[14], permettant ainsi de détecter des incidents de cybersécurité affectant ces composants et les données qu'ils stockent et transmettent.

Service public de cybersécurité : Le produit IdO peut assurer la protection des données et son bon fonctionnement en alertant le client lorsque l'appareil fonctionne de manière inattendue. Cela peut indiquer une tentative d'accès non autorisé, le chargement d'un logiciel malveillant, la création d'un botnet, des erreurs logicielles, ou d'autres actions non initiées par l'utilisateur ou non prévues par le développeur.

[14] Les informations sur l'état des composants de l'IdO qui seraient utiles pour détecter les incidents de cybersécurité sont fortement liées au contexte du produit IdO, de ses composants et de son fonctionnement. Dans la plupart des cas, les informations temporelles telles que l'horodatage ou les données de localisation (numériques ou physiques) doivent être saisies. La version et l'état de fonctionnement du logiciel et du matériel (par exemple, les failles ou les exceptions connues) peuvent aider à détecter les vulnérabilités en matière de cybersécurité (par exemple, un logiciel ou un matériel spécifique peut présenter des vulnérabilités connues). Les informations sur l'état de la cybersécurité peuvent également contenir des enregistrements de commandes et d'actions reçues et exécutées par le produit IdO ou d'autres données significatives pour le produit IdO et son fonctionnement, et donc utiles pour détecter les incidents.

2.2.2. Capacités de soutien non technique des produits IdO

Documentation

Le développeur de produits IdO crée, rassemble et stocke[15] les informations relatives à la cybersécurité du produit IdO et de ses composants avant l'achat par le client et tout au long du développement du produit et de son cycle de vie ultérieur.

1. Tout au long du cycle de développement, le développeur de produits IdO crée ou recueille et stocke des informations relatives à la cybersécurité du produit IdO et de ses composants, **notamment** :
    a. Hypothèses formulées au cours du processus de développement et autres attentes liées au produit IdO, **notamment** :
        i. Clients attendus et cas d'utilisation.
        ii. Considérer l'utilisation et les caractéristiques physiques, notamment la sécurité de l'emplacement du produit IdO et de ses composants (par exemple, une caméra destinée à un usage intérieur avec un interrupteur d'arrêt, par opposition à une caméra de sécurité extérieure sans interrupteur d'arrêt).
        iii. Accès au réseau et exigences (par exemple, exigences en matière de largeur de bande).
        iv. Données créées et traitées par le produit IdO.
        v. Toutes les entrées et sorties de données prévues (y compris les codes d'erreur, la fréquence, le type/la forme, la plage de valeurs acceptables, etc.)
        vi. Exigences de cybersécurité présumées du développeur du produit IdO pour le produit IdO.
        vii. Toutes les lois et réglementations auxquelles le produit IdO et les activités de soutien connexes sont conformes.
        viii. Durée de vie prévue et coûts de cybersécurité anticipés liés au produit IdO (par exemple, prix de la maintenance) et durée et conditions de l'assistance.
    b. Tous les composants de l'IdO, y compris, mais sans s'y limiter, l'appareil IdO, qui font partie du produit IdO.
    c. Expliquer comment le produit IdO respecte les critères de base à travers l'ensemble de ses composants, y compris identifier les critères non respectés et justifier ce non-respect (par exemple, la capacité jugée non nécessaire après évaluation des risques).
    d. Considérations relatives à la conception du produit et à l'assistance liées au

[15] Le développeur du produit IdO tient à jour et contrôle la documentation décrite dans ce critère. Le partage de ces informations peut être approprié et limité aux techniciens autorisés et aux experts en cybersécurité qui cherchent à obtenir davantage d'informations sur le produit IdO (par exemple, pour évaluer le produit IdO en vue de son étiquetage, ou pour enquêter sur une violation), mais les informations documentées ne sont pas destinées, dans tous les cas, à être partagées directement avec les consommateurs.

produit IdO, par *exemple* :

i. Tous les composants matériels et logiciels, quelle qu'en soit la source (par exemple, source ouverte, tiers propriétaire, développement interne), utilisés pour créer le produit IdO (c'est-à-dire utilisés pour créer chaque composant du produit).
ii. Plate-forme IdO utilisée pour le développement et le fonctionnement du produit IdO, ses composants, y compris la documentation y afférente.
iii. Fiabilité et protection des éléments logiciels et matériels mis en œuvre pour créer le produit IdO et ses composants (par exemple, démarrage sécurisé, racine de confiance matérielle et enclave sécurisée).
iv. Prise en compte des risques connus liés au produit IdO et des utilisations abusives potentielles connues.
v. Utilisation de pratiques sécurisées en matière de développement de logiciels et de chaîne d'approvisionnement.
vi. Résultats d'accréditation, de certification et/ou d'évaluation des pratiques liées à la cybersécurité.
vii. La facilité d'installation et d'entretien du produit IdO par un client (c'est-à-dire la facilité d'utilisation du produit [ISO9241]).

e. Exigences en matière de maintenance pour le produit IdO, *par exemple* :
   i. Les attentes en matière de maintenance de la cybersécurité et les instructions ou procédures associées (par exemple, le plan de gestion des vulnérabilités et des correctifs).
   ii. Comment le développeur de produits IdO identifie les parties auxiliaires autorisées qui peuvent effectuer des activités de maintenance (par exemple, les centres de réparation agréés).
   iii. Les considérations relatives à la cybersécurité du processus de maintenance (par exemple, comment les données des clients non liées au processus de maintenance restent confidentielles, même de la part des responsables de la maintenance).
f. Les politiques et processus du cycle de vie du système sécurisé associés au produit IdO, **y compris :**
   i. Mesures prises au cours du développement pour s'assurer que le produit IdO et ses composants sont exempts de toute vulnérabilité connue et exploitable.
   ii. Le processus de collaboration avec les fournisseurs de composants et les vendeurs tiers pour garantir la sécurité du produit IdO et de ses composants pendant toute la durée de son cycle de vie.
   iii. Toute considération postérieure à la fin du support, telle que la découverte d'une vulnérabilité qui aurait un impact significatif sur la sécurité, la confidentialité ou la sûreté des clients qui continuent d'utiliser le produit IdO et ses composants.

g. Les politiques et processus de gestion des vulnérabilités associés au produit IdO, **y compris** :
    i. Méthodes de réception des rapports sur les vulnérabilités (voir la section « Réception des informations et des demandes » ci-dessous).
    ii. Procédures d'enregistrement des vulnérabilités signalées.
    iii. Politique de réponse aux vulnérabilités signalées, y compris le processus de coordination des activités de réponse aux vulnérabilités parmi les fournisseurs de composants et les vendeurs tiers.
    iv. Politique de divulgation des vulnérabilités signalées.
    v. Procédures de réception des notifications des fournisseurs de composants et des vendeurs tiers concernant tout changement d'état des composants qu'ils fournissent, comme la fin de la production, la fin du support, l'état déprécié (par exemple, le produit n'est plus recommandé), ou les insécurités connues.

Service public de cybersécurité : La production, la saisie et le stockage d'informations importantes sur le produit IdO et son développement (par exemple, l'évaluation du produit IdO et des pratiques de développement utilisées pour le créer et le maintenir) peuvent contribuer à informer le développeur du produit IdO sur la situation réelle du produit en matière de cybersécurité.

Réception des informations et des demandes

Le développeur de produits IdO a la capacité de recevoir des informations relatives à la cybersécurité et de répondre aux demandes du client et d'autres personnes concernant des informations relatives à la cybersécurité.

1. Le développeur du produit IdO peut recevoir des informations relatives à la cybersécurité du produit IdO et de ses composants et peut répondre à des demandes relatives à la cybersécurité du produit IdO et de ses composants émanant de clients et d'autres personnes, **y compris** :
    a. La capacité du développeur de produits IdO à désigner un point de contact pour recevoir des informations sur la maintenance et les vulnérabilités (par exemple, des capacités de signalement de bogues et des programmes de chasse aux bogues) de la part des clients et d'autres acteurs de l'écosystème des produits IdO (par exemple, un technicien de réparation agissant pour le compte du client).
    b. La capacité du développeur du produit IdO à recevoir des demandes de renseignements de la part des clients et d'autres acteurs de l'écosystème du produit IdO concernant la cybersécurité du produit IdO et/ou de ses composants, et à y répondre.

Service public de cybersécurité : À mesure que les clients utilisent les produits IdO, ils peuvent poser des questions ou signaler des problèmes, contribuant ainsi à améliorer la cybersécurité du produit au fil du temps.

Diffusion de l'information

Le développeur de produits IdO diffuse (par exemple, au public) et distribue (par exemple, au client ou à d'autres acteurs de l'écosystème des produits IdO) des informations relatives à la cybersécurité.

1. Le développeur du produit IdO peut diffuser des informations à un grand nombre d'entités ou à toutes via un canal (par exemple, un message sur un canal public, des courriels envoyés à toutes les adresses enregistrées des clients concernés) afin d'alerter le public et les clients du produit IdO sur les informations et les événements relatifs à la cybersécurité tout au long du cycle de vie de l'assistance. **Ces informations comprennent au minimum**
    a. Conditions d'assistance actualisées (par exemple, fréquence des mises à jour et mécanisme(s) d'application) et notification de la disponibilité et/ou de l'application des mises à jour du logiciel.
    b. Fin de la période d'assistance ou de la fonctionnalité du produit IdO.
    c. Opérations de maintenance nécessaires.
    d. Les nouvelles vulnérabilités des appareils IoT, les détails associés et les mesures d'atténuation requises de la part du client.
    e. Découverte d'une brèche liée à un produit IdO et à ses composants utilisés par les clients, détails associés et mesures d'atténuation requises de la part du client (le cas échéant).
2. Le développeur du produit IdO peut diffuser des informations relatives à la cybersécurité du produit IdO et de ses composants pour alerter les entités appropriées de l'écosystème (par exemple, les fabricants de composants du produit IdO et/ou les entités de soutien, les autorités communes de suivi des vulnérabilités, les accréditeurs et les certificateurs, les organisations tierces d'assistance et de maintenance) au sujet des informations relatives à la cybersécurité, par *exemple* :
    a. Documentation applicable saisie lors de la conception et du développement du produit IdO et de ses composants.[16]
    b. Alertes sur la cybersécurité et les vulnérabilités et informations sur la résolution des vulnérabilités.
    c. Une vue d'ensemble des pratiques de sécurité de l'information et des mesures de protection utilisées par le développeur de produits IdO.
    d. Les résultats de l'accréditation, de la certification et/ou de l'évaluation des pratiques du développeur de produits IdO en matière de cybersécurité.

[16] Ce sous-critère vise à indiquer que les informations saisies dans le cadre de la capacité de documentation peuvent devoir être communiquées à des entités spécifiques (par exemple, les fabricants de composants de produits IdO et/ou les entités de soutien, les autorités communes de suivi des vulnérabilités, les accréditeurs et les certificateurs, les organisations tierces d'assistance et de maintenance). Dans la plupart des cas, ce type de documentation ne sera partagé qu'avec les parties intéressées qui ont un objectif spécifique pour l'information (par exemple, l'évaluation de la conformité) et ne sera généralement pas partagé publiquement ou même avec les clients du secteur de la consommation.

e. Un rapport d'évaluation des risques ou un résumé de la situation des risques liés à l'environnement commercial du développeur de produits IdO.

Service public de cybersécurité : À mesure que le produit IdO, ses composants, les menaces et les mesures d'atténuation évoluent, les clients devront être informés de la manière d'utiliser le produit IdO en toute sécurité.

Éducation et sensibilisation aux produits

Le développeur de produits IdO sensibilise et forme les clients et les autres acteurs de l'écosystème des produits IdO aux informations relatives à la cybersécurité (par exemple, considérations, caractéristiques) liées au produit IdO et à ses composants.[17]

1. Le développeur de produits IdO sensibilise et forme les clients aux informations relatives à la cybersécurité du produit IdO et de ses composants, **notamment :**
    a. La présence et l'utilisation de capacités de cybersécurité pour les produits IdO, **comprenant au minimum** :
        i. Comment modifier les paramètres de configuration et, le cas échéant, les conséquences de cette modification sur la cybersécurité.
        ii. Comment configurer et utiliser les fonctionnalités de contrôle d'accès (par exemple, définir et modifier des mots de passe).
        iii. La manière dont les mises à jour logicielles sont appliquées et toutes les instructions nécessaires au client pour utiliser la fonctionnalité de mise à jour logicielle.
        iv. Comment gérer les données de l'appareil, y compris la création, la mise à jour et la suppression des données sur le produit IdO.
    b. Comment assurer la maintenance du produit IdO et de ses composants pendant toute sa durée de vie, y compris après la période d'assistance en matière de sécurité (par exemple, la fourniture de mises à jour et de correctifs logiciels) par le développeur du produit IdO.
    c. Déterminer comment réapprovisionner ou éliminer en toute sécurité un produit IdO et ses composants.
    d. Proposer aux clients des options de gestion des vulnérabilités pour le produit IdO ou ses composants, telles que la gestion de la configuration, l'application de correctifs, et la lutte contre les logiciels malveillants.
    e. Informations supplémentaires que les clients peuvent utiliser pour prendre des décisions d'achat éclairées concernant la sécurité du produit IdO (par exemple, la durée et l'étendue de l'assistance produit par le biais de mises à jour logicielles et de correctifs).

Service public de cybersécurité : Les clients devront être informés sur la manière d'utiliser l'appareil en toute sécurité afin d'obtenir les meilleurs résultats en matière de cybersécurité pour les clients et le marché des produits IdO grand public.

[17] Les informations et l'expertise nécessaires à la mise en place d'une éducation et d'une sensibilisation efficaces concernant un produit IdO peuvent se trouver chez le développeur ou le fabricant des composants du produit IdO. Il est recommandé de mettre en place un écosystème d'éducation et de sensibilisation qui partage des informations sur la cybersécurité de l'IdO, même avant le déploiement d'un produit IdO, car cela facilitera la mise en œuvre de ces capacités de cybersécurité et d'autres.

3. Considérations sur le secteur de la consommation utilisées pour créer le profil

Le NIST a utilisé les concepts de profilage de la base de référence des capacités de cybersécurité des dispositifs IoT pour élaborer le profil du consommateur. La première étape a consisté à recueillir des sources et d'autres informations sur la cybersécurité des produits IdO grand public. Ensuite, le NIST a utilisé ces informations pour créer le profil du consommateur à l'aide des sources, des informations, des conclusions et des idées qui en résultent.

3.1. Collecte d'informations sur la cybersécurité des produits IdO grand public

Le profil du consommateur découle de la réponse du NIST à l'EO 14028, qui a demandé au NIST de développer des recommandations pour un programme de label de cybersécurité pour les produits IdO grand public. Les recommandations étaient plus larges que l'élaboration d'un profil du consommateur de la base de référence de l'IdO, mais le profil était un élément clé de cette tâche. Le NIST a donc pu recueillir des sources et engager des discussions avec des parties prenantes externes sur les besoins et les objectifs des clients des produits IdO grand public. Au cours d'une année d'événements, de réunions et d'autres engagements, les participants ont recueilli des centaines de commentaires sur l'étiquetage de la cybersécurité des produits IdO grand public. Un grand nombre de ces retours ont contribué à établir le profil du référentiel de base pour ce secteur.

Le NIST a également examiné le domaine public pour identifier les vulnérabilités applicables au secteur des produits IdO grand public. Ces informations sont importantes pour déterminer une vue transversale des vulnérabilités des produits IdO grand public, qui peut servir de base pour déterminer les menaces et les vulnérabilités. Ces menaces et vulnérabilités influencent le processus d'établissement des profils, en particulier les aspects relatifs à la sécurité minimale. Tableau 1, reproduit du document *Consumer Cybersecurity Labeling for IoT Products : Discussion Draft on the Path Forward* Whitepaper [Chemin d'accès] énumère un certain nombre de vulnérabilités applicables et bien documentées, les catégories d'attaques du cadre MITRE ATT&CK[ATT_CK] qui leur sont associées, ainsi que les capacités profilées qui peuvent aider à remédier à la vulnérabilité.[18]

Tableau 1. Exemple de vulnérabilités de l'IdO du consommateur et des capacités pertinentes du profil du consommateur.

Vulnérabilité	Capacités liées au profil du consommateur
Attaques de variantes de logiciels malveillants Mirai - Utilisation d'une authentification faible pour permettre le chargement de logiciels malveillants sur l'appareil et l'utilisation de cet appareil dans des attaques DDOS et autres.	

[18] Les capacités identifiées ne sont pas exhaustives mais sont incluses pour démontrer que les capacités de soutien à la cybersécurité telles que celles détaillées dans le profil du consommateur peuvent contribuer à atténuer ou à prévenir les vulnérabilités identifiées. Par exemple, une capacité de contrôle d'accès à l'interface aurait pu empêcher l'accès non autorisé à un appareil IdO.

Vulnérabilité	Capacités liées au profil du consommateur
Accès non autorisé à l'appareil IdO	Identification des actifs Contrôle d'accès à l'interface Diffusion de l'information Éducation et sensibilisation
Un code malveillant peut être chargé sur l'appareil IdO	Mise à jour du logiciel Sensibilisation à la cybersécurité Éducation et sensibilisation
Les commandes peuvent être lancées à l'aide de l'appareil	Contrôle d'accès à l'interface Documentation
Publication non autorisée des données d'un tracker de fitness - Le tracker de fitness du personnel militaire a rendu publiques des données de localisation, même si le produit était configuré pour protéger la vie privée.	
Vulnérabilités des applications web	Configuration du produit Sensibilisation à la cybersécurité Documentation Diffusion de l'information
Vulnérabilités des applications mobiles	Configuration du produit Sensibilisation à la cybersécurité Documentation Diffusion de l'information
Possibilité de réidentifier les données dépersonnalisées	Configuration du produit Protection des données Documentation
Accès non autorisé aux données des caméras de sécurité domestiques - L'accès non autorisé aux données et aux images de l'intérieur et de l'extérieur des bâtiments s'est produit avec plusieurs marques de caméras de sécurité.	
Authentification faible	Contrôle d'accès à l'interface
Partage de données non autorisé	Protection des données Documentation Diffusion de l'information

Vulnérabilité	Capacités liées au profil du consommateur
Absence de réponse aux questions et aux plaintes adressées aux développeurs	Réception des informations et des demandes
Manque de capacités et de procédures de contrôle	Identification des actifs Configuration du produit Documentation
Absence de contrôles de l'enregistrement et de la collecte des données	Identification des actifs Configuration du produit Documentation Diffusion de l'information Éducation et sensibilisation

Le NIST a également examiné les normes existantes, la conformité et l'écosystème d'étiquetage pour les appareils et les produits IdO afin de comprendre où d'autres avaient pris en compte les considérations relatives aux produits IdO grand public. Les participants ont examiné une trentaine de documents sources, incluant des lois sur la cybersécurité de l'IdO, des catalogues de capacités de cybersécurité, des ensembles de capacités de base et des schémas de hiérarchisation.[19] Tous ont abordé spécifiquement l'appareil IdO lui-même, mais plusieurs ont inclus le nuage, l'application mobile, le concentrateur ou d'autres composants externes dans leurs considérations comme faisant partie d'un produit IdO. Tout au long des consultations publiques et des discussions avec les parties prenantes, le NIST a constaté un large consensus en faveur d'une approche plus large, incluant tous les composants d'un produit IdO plutôt que de se limiter à l'appareil IdO. Ce consensus soutenait l'inclusion de tous les composants dans le champ d'application des capacités de cybersécurité.

3.2. Évaluer les sources de cybersécurité des produits IdO grand public

Les documents sources peuvent être comparés plus directement aux capacités de soutien techniques et non techniques établies dans les NISTIR 8259A et 8259B. Sur les 30 documents sources collectés, un sous-échantillon de 8 était le plus directement lié aux produits IdO grand public. Les participants ont comparé ce sous-échantillon aux capacités décrites dans le NISTIR 8259A/B et ont constaté un large alignement sur les capacités techniques. Ils ont également utilisé certaines capacités techniques communes, absentes du NISTIR 8259A, pour adapter la base de référence au profil du consommateur. Toutefois, peu de documents sources traitent des capacités non techniques développées sur la base du NISTIR 8259B. Comme les utilisateurs prévus des dispositifs IoT grand public ne sont généralement pas des experts en cybersécurité,

[19] Le décret 14028 a demandé au NIST d'envisager des niveaux pour les recommandations relatives à l'étiquetage de l'IdO à l'intention des consommateurs, mais les recherches du NIST et le retour d'information qui en a découlé n'ont pas permis d'établir un ensemble ou un cadre clair et efficace pour l'élaboration de ces niveaux. Les sources existantes qui traitent des niveaux ne le font pas de manière consensuelle. En outre, le NIST a entendu des commentaires selon lesquels les niveaux devraient refléter des niveaux de risque croissants liés aux produits IdO grand public, mais la variété des cas d'utilisation de l'IdO grand public fait du regroupement de ces cas d'utilisation sur la base du risque, une condition préalable à leur hiérarchisation, une tâche qui ne pouvait pas être achevée dans le délai d'un an prévu pour la réponse au décret 14028.

ces capacités de soutien non techniques sont essentielles pour garantir un fonctionnement sécurisé.

Les commentaires du public et les réactions verbales tout au long des travaux sur la réponse à l'OE ont confirmé cela. Le NIST s'est appuyé sur ces retours pour établir le profil du consommateur. Grâce à ces sources, le NIST a également entendu parler d'un certain nombre d'autres façons dont le secteur de la consommation peut être différent du cas général ou d'autres secteurs. Par exemple, la gestion des risques de cybersécurité des entreprises clientes est généralement plus structurée et formalisée que l'approche de gestion des risques de cybersécurité utilisée par les clients du secteur de la consommation. En outre, les entreprises ont généralement un meilleur accès à l'expertise en matière de cybersécurité que les consommateurs ordinaires. Ces différences et d'autres éléments ont des répercussions sur la manière dont les capacités de cybersécurité doivent être abordées et mises en œuvre. Le tableau 2 présente les principales données utilisées pour élaborer le profil de l'IdO des consommateurs.

Tableau 2. Aperçu et principales conclusions du processus de profilage de l'IdO des consommateurs.

Point de vue mis en exergue	Principaux enseignements
Les perspectives de cybersécurité pour le secteur de la consommation, basées sur les risques et les vulnérabilités, sont similaires à celles du scénario de base général. (Par exemple, ceux énumérés dans le tableau 1)	La plupart des capacités reposent sur des concepts de cybersécurité similaires
Les lignes directrices en matière de cybersécurité au niveau des appareils seraient insuffisantes au regard des besoins et des objectifs des clients dans ce secteur, notamment en raison de l'absence de distinction entre l'appareil IdO et les composants qui l'accompagnent.	Le produit est le niveau privilégié pour les lignes directrices relatives à la cybersécurité de l'IdO des consommateurs.
La confidentialité et la sécurité sont des préoccupations majeures pour les produits IdO grand public, au même titre que la cybersécurité.	Les capacités de cybersécurité doivent être conçues de manière à ne pas créer de risques dans ces domaines et à soutenir les approches générales en matière d'atténuation des risques liés à la vie privée et à la sécurité.

Point de vue mis en exergue	Principaux enseignements
Aucun ensemble clair et universel de besoins et d'objectifs des consommateurs en matière de cybersécurité n'existe dans le secteur de la consommation. Le NIST a toutefois identifié plusieurs approches pour répondre aux attentes des clients à partir des documents sources analysés dans l'étude du paysage.	Les capacités doivent être fondées sur des fonctions de cybersécurité universellement acceptées et généralement applicables.
Les besoins et les objectifs des clients de ce secteur varient. Les clients peuvent avoir des connaissances et des capacités limitées en ce qui concerne les technologies IdO/TI et les fonctions de cybersécurité.	Les facteurs humains liés aux capacités de cybersécurité sont primordiaux pour atténuer les risques de cybersécurité.

Ces observations et les conclusions qui en découlent ont conduit le NIST à formuler les considérations suivantes concernant le profil de l'IdO du consommateur :

1. De nombreux appareils IoT grand public dépendent clairement de composants supplémentaires, comme un back-end ou une application mobile, qui sont essentiels à leur utilisation, au point que l'appareil ne peut pas fonctionner de manière significative sans eux.
2. En outre, les consommateurs à domicile n'ont souvent que peu de contrôle sur ces éléments supplémentaires. Par conséquent, pour déterminer comment l'approche centrée sur l'appareil s'appliquera au secteur de la consommation, le concept doit s'étendre au-delà de l'appareil pour englober le produit dans son intégralité. Ce champ d'application peut inclure des composants supplémentaires faisant partie d'un produit IdO, y compris ceux avec lesquels le consommateur n'interagit qu'indirectement (par exemple, le backend).
3. Le profil du consommateur doit être mis en œuvre dans le contexte des principales perceptions et considérations du secteur en matière de protection de la vie privée et de sécurité. Les considérations relatives à la sécurité et à la protection de la vie privée sont dynamiques pour les produits IdO grand public, car même dans ce secteur spécifique, les cas d'utilisation des produits IdO peuvent varier de manière significative. Un produit et son fonctionnement peuvent avoir des implications claires en matière de sécurité, mais ce n'est pas toujours le cas. Cela s'applique également à la protection de la vie privée. Cette situation s'aggrave lorsque différents cas d'utilisation partagent des considérations générales de sécurité et de respect de la vie privée, mais que les spécificités de leurs impacts et leurs mesures d'atténuation varient considérablement. Cela signifie que les capacités de cybersécurité du profil du consommateur doivent prendre en charge un grand nombre de cas d'utilisation tout en veillant à ne pas entraver ces domaines.
4. Les pratiques de cybersécurité des clients (c'est-à-dire des particuliers) qui gèrent les produits IdO grand public varieront en termes de définition et de maturité. La nature

imprévisible et ponctuelle de l'atténuation du risque client pour les produits IdO grand public souligne la nécessité de refléter dans le profil des pratiques de cybersécurité largement utiles et généralement recommandées.

5. En outre, un besoin important de ce secteur en matière de cybersécurité est de disposer de capacités de cybersécurité utilisables qui soient mises en œuvre de manière à nécessiter une configuration et une interaction minimales/efficaces de la part des clients, étant donné que ces derniers n'auront pas de connaissances approfondies ou de ressources à exploiter si les capacités ne sont pas utilisables pour eux.
6. Enfin, des normes, des solutions, des mises en œuvre ou des mesures d'atténuation spécifiques doivent être choisies en fonction de la fonctionnalité et du cas d'utilisation d'un produit IdO. Cela signifie qu'aucun ensemble unique d'exigences spécifiques ne peut s'appliquer à tous les produits IdO grand public. Par conséquent, le profil du consommateur décrit les lignes directrices en matière de cybersécurité au niveau des produits IdO en termes de résultats à atteindre et à soutenir par le produit dans son ensemble, mais il peut ne pas s'appliquer de la même manière à tous les composants des produits IdO. Certains composants peuvent ne pas être en mesure de répondre ou ne pas devoir répondre à tous les critères.[20] Ces résultats fournissent des orientations pour une variété de technologies et de cas d'utilisation, mais permettent une certaine souplesse dans l'application du profil du consommateur à des produits IdO spécifiques.[21]

Le NIST a appliqué ces considérations aux capacités de base 8259A/B des NISTIR afin d'adapter l'approche générale de l'IdO au secteur de la consommation. Le profil du consommateur qui en résulte, bien qu'il soit plus directement adapté au secteur, est toujours destiné à couvrir un large éventail de technologies IdO, de cas d'utilisation et de considérations relatives à l'atténuation des risques. Par conséquent, l'application du profil du consommateur à un produit, un type de produit ou un composant de produit IdO spécifique peut nécessiter une adaptation supplémentaire, mais similaire, par la collecte et l'examen des informations décrites dans la présente section.

[20] Comme indiqué dans les *Critères recommandés pour l'étiquetage des produits de l'internet des objets (IdO) destinés aux consommateurs en matière de cybersécurité*, toutes les capacités ou tous les sous-critères ne s'appliquent pas nécessairement à tous les composants des produits IdO ou ne sont pas pris en charge de la même manière par ces derniers. Cela peut être dû à des considérations liées au risque du produit, au développement du produit (par exemple, les tâches de cybersécurité sont déléguées par le biais de contrats et de la chaîne d'approvisionnement), à la nature des composants qui constituent le produit (par exemple, les backends peuvent être hautement distribués) ou aux limites des composants IdO (par exemple, les appareils peuvent être limités, les applications logicielles compagnons peuvent avoir un accès et des fonctionnalités limités). Prendre en compte cet aspect lors de l'application des capacités et des sous-critères à des produits réels, par exemple via un mécanisme d'évaluation de la conformité, est essentiel pour créer un marché et un écosystème de cybersécurité robustes, capables de répondre à des besoins et contextes variés.

[21] Le NIST invite les personnes disposant de conseils, de normes ou de programmes qui, selon eux, soutiennent ou sont liés à tout ou partie des résultats reflétés dans ce profil, à consulter le catalogue de référence informative en ligne du NIST (OLIR) pour obtenir de plus amples informations sur la manière de soumettre des correspondances publiques entre leur travail et le profil du consommateur.

Références

[ATT_CK] The MITRE Corporation (2013) Adversarial Tactics, Techniques, and Common Knowledge. (The MITRE Corporation, Bedford, MA). https://attack.mitre.org/

[EO_Criteria] National Institute of Standards and Technology (2022) Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. (National Institute of Standards and Technology, Gaithersburg, MD), Livre blanc du NIST sur la cybersécurité. https://doi.org/10.6028/NIST.CSWP.24

[IR8259] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[IR8259A] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[IR8259B] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[ISO9241] International Organization for Standardization/International Electrotechnical Commission (2018) ISO 9241-11:2018 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts (ISO Geneva, Switzerland). Disponible à l'adresse suivante : https://www.iso.org/standard/63500.html

[Path_Forward] National Institute of Standards and Technology (2021) Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward. (National Institute of Standards and Technology, Gaithersburg, MD). Disponible à l'adresse suivante : https://www.nist.gov/document/draft-paper-consumer-cybersecurity-labeling-iot-products-discussion-draft-path-forward

Appendix A. Glossaire

produit IdO grand public
Produits IdO destinés à un usage personnel, familial ou domestique.

base de référence
Ensemble de capacités de cybersécurité des dispositifs et de capacités de soutien non techniques nécessaires pour soutenir les contrôles de cybersécurité communs qui protègent les dispositifs et les données des dispositifs, les systèmes et les écosystèmes du client.

capacité de cybersécurité des produits
Les caractéristiques ou fonctions de cybersécurité que les dispositifs informatiques fournissent par leurs propres moyens techniques (c'est-à-dire le matériel et les logiciels des dispositifs). [IR8259]

> *Remarque :* Ce terme est synonyme de capacités de cybersécurité des *appareils* , telles que définies dans le document NISTIR 8259, mais il s'applique à un produit IdO tel que défini dans le présent document, et non pas uniquement à l'appareil IdO.

Dispositif IdO
Appareils dotés d'au moins un transducteur (capteur ou actionneur) pour interagir directement avec le monde physique et d'au moins une interface réseau (par exemple, Ethernet, Wi-Fi, Bluetooth) pour interagir avec le monde numérique.

Produit IdO
Un ou plusieurs dispositifs IdO ( ) et tout composant de produit supplémentaire (par exemple, backend, application mobile) nécessaire pour utiliser le dispositif IdO au-delà des fonctions opérationnelles de base.

Composant de produit IdO
Un appareil IdO ou un autre équipement ou service numérique (par exemple, backend, application mobile) utilisé pour créer des produits IdO.

capacité de soutien non technique
Les capacités de soutien non techniques sont des actions qu'une organisation met en œuvre pour soutenir la cybersécurité d'un dispositif IdO.