Fiche d'information

Produits électroniques de sécurité incendie et de sûreté dans le cadre des produits importants et critiques définis par la loi sur la cyber-résilience (CRA)

Introduction

La loi sur la cyber-résilience (CRA, Cyber Resilience Act, (UE) 2024/2847) a été publiée au Journal officiel de l'Union européenne (JOUE) en novembre 2024. Elle établit des exigences horizontales en matière de cybersécurité pour les produits traitant et transmettant des données numériques, ainsi que pour leurs solutions de traitement des données à distance, le cas échéant. Le Règlement s'appliquera à partir du 11 décembre 2027. Toutefois, les dispositions relatives aux obligations de communication des fabricants (article 14) entrent en vigueur dès le 11 septembre 2026 et celles concernant la notification des organismes d'évaluation de la conformité, dès le 11 juin 2026.

Les exigences essentielles applicables aux produits relevant du champ d'application du CRA, ainsi qu'au processus de gestion des vulnérabilités mis en place par le fabricant, sont définies à l'article 6 et détaillées à l'annexe I. Ces exigences sont identiques pour l'ensemble des produits concernés.

Des catégories spécifiques de produits importants et critiques sont définies aux articles 7 et 8, puis listées aux annexes III et IV du CRA. Leur description technique a été précisée par le Règlement d'exécution (UE) 2025/2392, publié au Journal officiel de l'Union européenne (JOUE) en décembre 2025. L'objectif de cette classification est de soumettre ces produits à des procédures d'évaluation de la conformité plus strictes que celles applicables aux produits « par défaut », c'est-à-dire ceux qui ne sont ni importants ni critiques.

Il est donc essentiel de bien comprendre ces catégories afin de se conformer aux exigences du Règlement. Cette fiche d'information a pour objectif d'expliquer comment les procédures d'évaluation de la conformité sont attribuées aux différentes catégories de produits, et d'identifier les produits électroniques de sécurité incendie et de sûreté concernés.

Certains types de produits font l'objet de commentaires explicites à titre d'exemples illustratifs. Cette fiche n'est pas exhaustive : d'autres produits de sécurité incendie ou de sûreté non mentionnés ici (comme les caméras vidéo) pourraient également relever d'une catégorie spécifique et être intégrés dans une version ultérieure du document.

Procédures d'évaluation de la conformité

La procédure d'évaluation de la conformité applicable à un produit est définie à l'article 32 du CRA.

- Pour les produits « par défaut », l'auto-évaluation et l'autodéclaration de conformité (module A) sont autorisées, que la norme technique utilisée pour les essais soit ou non citée au JOUE. Toutefois, seuls les produits conformes à une norme harmonisée citée au JOUE bénéficient de la présomption de conformité (article 27). Pour les produits électroniques de sécurité incendie et les produits de sécurité physique relevant de cette catégorie, la conformité peut être démontrée, par exemple, à l'aide des normes verticales générales EN 62443-4-x (issues de la série IEC 62443 et couvrant l'ensemble des exigences essentielles du CRA), en cours d'élaboration au sein du CLC/TC 65X, ou des normes horizontales EN 40000-x en cours d'élaboration au sein du CEN/CLC/JTC 13.
- Pour les produits classés « importants – classe I », l'auto-évaluation et la déclaration de conformité (module A) ne sont possibles que si la norme technique utilisée est citée au JOUE. À défaut, ou si cette norme n'est

pas entièrement appliquée, le produit doit être soumis à un organisme notifié (examen UE de type, module B) et le fabricant doit mettre en œuvre un contrôle interne de la production (module C).

- Pour les produits classés « importants – classe II », l'auto-évaluation et l'autodéclaration de conformité ne sont pas autorisées. Le produit doit obligatoirement être évalué par un organisme notifié (module B), puis faire l'objet d'un contrôle interne de la production (module C).
- Pour les produits classés « critiques », la procédure dépend de l'existence d'un acte délégué applicable à la catégorie concernée. La Commission européenne peut en effet attribuer, par acte délégué, un système européen de certification en cybersécurité (élaboré par l'ENISA en vertu du règlement sur la cybersécurité, comme l'EUCC fondé sur les critères communs). En présence d'un tel acte, le fabricant doit appliquer le système de certification désigné. À ce jour, aucun acte délégué de ce type n'a été adopté. En l'absence de celui-ci, le produit doit être évalué par un organisme notifié (module B) et soumis à un contrôle interne de la production (module C).

Catégories de produits importants et critiques

Introduction

L'annexe III du CRA recense 19 catégories de produits importants de classe I et 4 catégories de produits importants de classe II.

<table>
<tr><th colspan="2">Classe I</th></tr>
<tr><td>

Systèmes de gestion des identités et logiciels et dispositifs de gestion des accès privilégiés, dont lecteurs d'authentification et de contrôle d'accès et lecteurs biométriques
Navigateurs autonomes ou intégrés
Gestionnaires de mots de passe
Logiciels qui recherchent, suppriment ou mettent en quarantaine des logiciels malveillants
Produits comportant des éléments numériques avec la fonction de réseau privé virtuel (VPN)
Systèmes de gestion de réseau
Systèmes de gestion des informations et des événements de sécurité (SIEM)
Gestionnaires de démarrage
Infrastructures à clé publique et logiciels d'émission de certificats numériques
Interfaces réseau physiques ou virtuelles
Systèmes d'exploitation
Routeurs, modems destinés à la connexion à Internet et commutateurs
Microprocesseurs dotés de fonctionnalités liées à la sécurité

</td><td>
<ol start="14">
Microcontroleurs dotés de fonctionnalités liées à la sécurité
Circuits intégrés spécifiques à l'application (ASIC) et réseaux de portes programmables (FPGA) dotés de fonctionnalités liées à la sécurité
Assistants virtuels polyvalents pour maison intelligente
Produits domestiques intelligents dotés de fonctionnalités de sécurité, notamment serrures, caméras de sécurité, systèmes de surveillance pour bébé et systèmes d'alarme
Jouets connectés couverts par la directive 2009/48/CE du Parlement européen et du Conseil, qui présentent des caractéristiques sociales interactives (par exemple, parler ou filmer) ou qui possèdent des fonctions de localisation
Produits portables personnels destinés à être portés ou mis sur un corps humain à des fins de surveillance de la santé (suivi par exemple), et auxquels le règlement (UE) 2017/745 ou (UE) 2017/746 du Parlement européen et du Conseil ne s'applique pas, ou produits portables personnels destinés à être utilisés par ou pour les enfants

</td></tr>
<tr><th colspan="2">Classe II</th></tr>
<tr><td>

Hyperviseurs et systèmes d'exécution de conteneurs prenant en charge l'exécution virtualisée de systèmes d'exploitation et d'environnements similaires
Pare-feu, systèmes de détection et de prévention des intrusions

</td><td>
<ol start="3">
Microprocesseurs résistants aux manipulations
Microcontrôleurs résistants aux manipulations

</td></tr>
</table>

L'annexe IV énumère trois catégories de produits critiques :

1. **Dispositifs matériels avec boîtiers de sécurité.**
2. «Passerelles pour compteur intelligent» au sein des systèmes intelligents de mesure tels que définis à l'article 2, point 23), de la directive (UE) 2019/944 du Parlement européen et du Conseil (1) et autres dispositifs à des fins de sécurité avancées, y compris pour un traitement cryptographique sécurisé
3. Cartes à puce ou dispositifs similaires, y compris éléments sécurisés

Conformément aux articles 7 et 8 du CRA, et comme précisé dans la FAQ publiée par la Commission européenne, un produit est considéré comme important ou critique lorsque sa **fonctionnalité** principale correspond à celle décrite dans le Règlement d'exécution (UE) 2025/2392. Il convient de souligner qu'un produit intégrant une fonctionnalité qualifiée d'importante ou de critique ne devient pas automatiquement un produit important ou critique si sa fonctionnalité principale ne relève pas de cette classification.

Par exemple, un microcontrôleur doté de fonctionnalités de sécurité et commercialisé comme tel sur le marché de l'Union européenne doit être classé comme un produit important de classe I. En revanche, un équipement de contrôle et sz signalisation (ECS) destiné à la détection d'incendie dans un environnement commercial ou industriel intègre un microcontrôleur, mais sa fonction principale est de traiter les signaux provenant des détecteurs d'incendie et de déclencher une alarme. Cette fonctionnalité n'étant pas considérée comme importante ou critique, cet ECS relève donc de la catégorie « par défaut ».

Trois catégories présentent des similitudes avec les produits du secteur de la sécurité incendie et de la sûreté électroniques. Elles sont mises en évidence en caractères gras dans les tableaux ci-dessus et feront l'objet de commentaires dans les sections suivantes.

Produits domestiques intelligents dotés de fonctionnalités de sécurité

Cette catégorie 17 des produits importants de classe I est décrite dans le Règlement d'exécution comme suit :

> *Les produits comportant des éléments numériques qui protègent la sécurité physique des consommateurs dans un environnement résidentiel et qui peuvent être contrôlés ou gérés à distance à partir d'autres systèmes, ainsi que le matériel et les logiciels qui contrôlent ces produits de manière centralisée.*
>
> *Cette catégorie comprend, sans s'y limiter, les dispositifs intelligents de verrouillage des portes, les systèmes de surveillance des bébés, les systèmes d'alarme et les caméras de sécurité à domicile.*

Pour qu'un produit relève de cette catégorie, quatre critères doivent être réunis :

- « protéger la sécurité physique » : la fonctionnalité principale du produit doit viser à garantir la sécurité physique, notamment contre les agressions, les intrusions, les incendies, les gaz toxiques ou inflammables ;
- « des consommateurs » : le produit doit être destiné, dans son usage prévu, à protéger des consommateurs ;
- « dans un environnement résidentiel » : le produit doit être conçu pour fonctionner dans un environnement résidentiel, même s'il peut également être utilisé dans des contextes commerciaux ou industriels ;
- « peuvent être contrôlés ou gérés à distance à partir d'autres systèmes » : le produit doit être conçu pour être contrôlé ou géré à distance, généralement via le cloud. Le contrôle ou la gestion à partir d'un ECS situé dans les mêmes locaux n'entre pas dans ce cadre.

Le tableau ci-dessous présente quelques exemples et précise pourquoi ces produits relèvent, ou non, de cette catégorie.

Description de l'exemple	Dans le champ d'application du CRA	Appartient à la catégorie « Important » de classe I n° 17
Centrale de détection intrusion pour environnement résidentiel	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	La fonctionnalité principale consiste à assurer la sécurité physique des consommateurs dans un environnement résidentiel (même s'il est également destiné à des environnements commerciaux ou industriels)
— dotée de fonctionnalités d'accès à distance		**OUI,** il peut être contrôlé ou géré via une infrastructure d'accès à distance
— équipée d'un émetteur-récepteur pour la transmission d'alarmes via le protocole IP et sans fonctionnalités d'accès à distance		**NON** (appartient à la catégorie par défaut), il ne peut pas être contrôlé ou géré via une infrastructure d'accès à distance et la transmission d'alarmes en soi ne constitue pas un moyen de contrôle ou de gestion du produit
Clavier permettant l'interaction de l'utilisateur avec une centrale de détection intrusion pour environnement résidentiel	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	La fonctionnalité principale est d'assurer la sécurité physique des consommateurs dans un environnement résidentiel (même s'il est également destiné à des environnements commerciaux ou industriels)
— permettant l'envoi et la réception de messages numériques, uniquement via une connexion locale vers et depuis la centrale d'alarme		**NON** (appartient à la catégorie par défaut), il ne peut pas être contrôlé ou géré via une infrastructure d'accès à distance
— doté de fonctionnalités permettant la réception de commandes de contrôle ou de gestion depuis Internet		**OUI,** il peut être contrôlé ou géré via une infrastructure d'accès à distance
Détecteur d'intrusion destiné à un environnement résidentiel		La fonctionnalité principale est d'assurer la sécurité physique des consommateurs dans un environnement résidentiel (même s'il est également destiné à des environnements commerciaux ou industriels)
— signalant ses états à l'ECS uniquement via des signaux OUVERT/FERMÉ	**NON,** il ne dispose pas d'une connexion de données numériques avec un autre appareil ou réseau	**NON,** ce produit n'entre pas dans le champ d'application du CRA
— envoyant et recevant des messages numériques uniquement via une connexion locale vers ou depuis l'ECS	**OUI,** il dispose d'une connexion de données numériques avec un autre appareil ou réseau	**NON** (appartient à la catégorie par défaut), il ne peut pas être contrôlé ou géré via une infrastructure d'accès à distance (l'ECS peut être contrôlé à distance, mais le détecteur est contrôlé par l'ECS)
— avec des fonctionnalités permettant de recevoir des commandes de	**OUI,** il dispose d'une connexion de données numériques	**OUI,** il peut être contrôlé ou géré via une infrastructure d'accès à distance

contrôle ou de gestion depuis Internet	avec un autre appareil ou réseau	
ECS pour la détection incendie dans un environnement commercial ou industriel avec des fonctionnalités d'accès à distance	**OUI,** il intègre une connexion de données numériques avec un autre appareil ou un réseau	**NON** (appartient à la catégorie par défaut), la fonctionnalité principale est de protéger la sécurité physique des consommateurs dans un environnement non résidentiel
Dispositif d'alarme de fumée ou de monoxyde de carbone		Sa fonctionnalité principale consiste à assurer la sécurité physique des consommateurs dans un environnement résidentiel.
— sans interconnexion	**NON,** il ne dispose pas d'une connexion de données numériques avec un autre appareil ou réseau	**NON,** ce produit n'entre pas dans le champ d'application du CRA.
— avec interconnexion locale vers un autre dispositif d'alarme ou vers une centrale locale	**OUI,** s'il dispose d'une connexion de données numériques avec un autre appareil ou réseau	**NON,** il ne peut être contrôlé ni géré via une infrastructure d'accès à distance (il appartient à la catégorie par défaut).
— doté de fonctionnalités permettant de recevoir des commandes de contrôle ou de gestion depuis Internet	**OUI,** il dispose d'une connexion de données numériques avec un autre appareil ou réseau	**OUI,** il peut être contrôlé ou géré via une infrastructure d'accès à distance.
Logiciel mis sur le marché de l'UE, destiné à être déployé dans le cloud et permettant de gérer l'accès à distance à un système d'alarme dans un environnement résidentiel	**OUI,** il dispose d'une connexion de données numériques avec un autre appareil ou réseau	**OUI,** sa fonctionnalité principale consiste à assurer la sécurité physique des consommateurs dans un environnement résidentiel et il contrôle de manière centralisée les ECS.
Logiciel mis sur le marché de l'UE, destiné à être déployé dans le cloud et permettant de gérer la transmission des alarmes générées dans un environnement résidentiel	**OUI,** il dispose d'une connexion de données numériques avec un autre appareil ou réseau	**OUI,** sa fonctionnalité principale est d'assurer la sécurité physique des consommateurs dans un environnement résidentiel et il contrôle de manière centralisée la transmission des alarmes.

Cette catégorie de produits est destinée à être couverte par la future norme harmonisée EN 304 632, actuellement en cours d'élaboration par le comité technique ETSI TC CYBER.

Systèmes de gestion des identités et logiciels et dispositifs de gestion des accès privilégiés

Cette catégorie n° 1 de produits importants de classe I est décrite comme suit dans le Règlement d'exécution :

> *Les systèmes de gestion de l'identité sont des produits comportant des éléments numériques qui prévoient des mécanismes d'authentification ou d'autorisation et qui peuvent également prévoir des mécanismes de gestion tout au long du cycle de vie des identifiants des personnes physiques, des personnes morales, des dispositifs ou des systèmes, tels que l'enregistrement de l'identité, la fourniture, la maintenance et la radiation de l'identité. Ces systèmes comprennent les systèmes de gestion des accès*

qui contrôlent l'accès des personnes physiques, des personnes morales, des dispositifs ou des systèmes aux ressources numériques ou aux lieux physiques.

Le logiciel de gestion des accès privilégiés est un système de gestion des accès qui contrôle et surveille les droits d'accès aux systèmes informatiques ou opérationnels et aux informations sensibles au sein d'une organisation, y compris les systèmes appliquant des politiques de contrôle d'accès différenciées pour les utilisateurs privilégiés.

Cette catégorie comprend, sans s'y limiter, les lecteurs d'authentification et de contrôle d'accès, les lecteurs biométriques, les logiciels d'authentification unique, les logiciels de gestion des identités fédérés, les logiciels de mot de passe à usage unique, les dispositifs d'authentification matériels tels que les générateurs de numéros d'authentification de transaction (TAN), les logiciels d'authentification et les logiciels d'authentification multifactorielle.

Cette catégorie couvre les dispositifs et systèmes de contrôle d'accès, qu'il s'agisse de ressources numériques (accès logique) ou de sites physiques (accès physique). S'agissant de l'accès physique, les éléments suivants doivent être pris en compte :

- La solution de contrôle d'accès physique est considérée comme un système de technologie opérationnelle (OT) et elle est pilotée par un logiciel de gestion des accès. Sa finalité est d'appliquer des politiques de contrôle d'accès pour les utilisateurs disposant de privilèges leur permettant d'accéder aux sites physiques d'un bâtiment.
- Le fonctionnement de cette solution repose sur son interaction avec des lecteurs de contrôle d'accès de tous formats, ainsi qu'avec des applications mobiles (identifiants mobiles).
- Le système de contrôle d'accès physique est lié à de la gestion des identités et aux logiciels associés : une base de données d'utilisateurs (identifiants), chaque identifiant étant rattaché à une identité (utilisateur) disposant ou non de droits d'accès.

Le tableau ci-dessous présente quelques exemples et précise si ces produits relèvent ou non de cette catégorie.

Description de l'exemple	Dans le champ d'application du CRA	Appartient à la catégorie « Important » de classe I n° 1
ECS d'un système électronique de contrôle d'accès destiné à contrôler l'accès physique des personnes à un bâtiment ou à une zone	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	**OUI,** sa fonctionnalité principale consiste à gérer les accès en fonction des privilèges liés à l'identité; il stocke les identités associées aux identifiants et aux droits d'accès
Logiciel de contrôle d'accès fonctionnant sur un serveur distant	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	**OUI,** sa fonctionnalité principale consiste à gérer les accès en fonction des privilèges liés à l'identité; il stocke les identités associées aux identifiants et aux droits d'accès
Lecteur de contrôle d'accès (par exemple, lecteur biométrique, lecteur de badges) d'un système électronique de contrôle d'accès destiné à contrôler l'accès physique des personnes à un bâtiment ou à une zone	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	

— ne gérant pas lui-même l'identité des utilisateurs		**NON** (appartient soit à la catégorie par défaut, soit à la catégorie n° 17) : — ce lecteur de badges ne gère pas lui-même les identités des utilisateurs (celles-ci ne sont pas stockées sur le lecteur) — même si le lecteur de badges peut intégrer un logiciel de gestion des accès privilégiés, il s'agit d'un produit matériel
— gérant lui-même l'identité des utilisateurs		**OUI,** sa fonctionnalité principale est la gestion des identités (les identités sont stockées sur le lecteur)
Identifiant de contrôle d'accès (par exemple, badge physique)	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	**NON** (appartient soit à la catégorie par défaut, soit à la cat. n° 17) : sa fonction principale est de contenir des données d'identification, mais il est statique et ne gère pas les identités
ECS pour la détection incendie ou la détection intrusion	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	**NON** (appartient soit à la catégorie par défaut, soit à la cat. n° 17) : bien que le CIE intègre un logiciel gérant l'accès privilégié à ses ressources (gestion des niveaux d'accès), sa fonctionnalité principale n'est ni la gestion des identités ni la gestion des accès privilégiés

Example description	In scope of CRA	Belongs to category Important Class I #1
Lecteur biométrique d'un système de détection intrusion, mis sur le marché de l'UE séparément de l'ECS	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	
— ne gérant pas lui-même l'identité des utilisateurs		**NON** (appartient soit à la catégorie par défaut, soit à la cat. n° 17): — ce lecteur biométrique ne gère pas lui-même les identités des utilisateurs (les identités ne sont pas stockées sur le lecteur) — même si le lecteur biométrique peut intégrer un logiciel de gestion des accès privilégiés, il s'agit d'un produit matériel
— gérant lui-même l'identité des utilisateurs		**OUI,** sa fonctionnalité principale est la gestion des identités (les identités sont stockées sur le lecteur)
Lecteur de badges permettant de désactiver un système d'alarme intrusion, mis sur le marché de l'UE séparément de l'ECS	**OUI,** il permet la connexion numérique avec un autre appareil ou un réseau	
— ne gérant pas lui-même l'identité des utilisateurs		**NON** (appartient soit à la catégorie par défaut, soit à la cat. n° 17): — ce lecteur de badges ne gère pas lui-même les identités des utilisateurs (les identités ne sont pas stockées sur le lecteur) — même si le lecteur de badges peut intégrer un logiciel de gestion des accès privilégiés, il s'agit d'un produit matériel

— gérant lui-même l'identité des utilisateurs		**OUI,** sa fonctionnalité principale est la gestion des identités (les identités sont stockées sur le lecteur)

Cette catégorie de produits est destinée à être couverte par une future norme harmonisée actuellement en cours d'élaboration par le CEN/TC 224.

Dispositifs matériels avec boîtiers de sécurité

Cette catégorie n° 1 de produits critiques est décrite comme suit dans le règlement d'exécution :

> *Les produits matériels comportant des éléments numériques qui stockent, traitent ou gèrent des données sensibles en toute sécurité ou effectuent des opérations cryptographiques, et qui consistent en plusieurs composants discrets, comprenant une enveloppe physique matérielle fournissant en cas de manipulation des preuves, une résistance ou une réaction, contre-mesures face aux attaques physiques.*
>
> *Cette catégorie comprend, sans s'y limiter, les terminaux de paiement physiques, les modules de sécurité matériels qui génèrent et gèrent des éléments cryptographiques et les tachygraphes qui répondent à la description ci-dessus.*

Les produits de détection intrusion ainsi que les dispositifs de contrôle d'accès électronique réalisent des opérations cryptographiques — notamment pour répondre aux exigences essentielles du CRA — et présentent des mécanismes de résistance aux tentatives de manipulation ainsi que des capacités de réaction. Toutefois, ces fonctions ne constituent pas leur fonctionnalité principale. En conséquence, ces produits ne relèvent pas de cette catégorie de produits critiques.

Cette catégorie est appelée à être couverte par une future norme harmonisée, actuellement en cours d'élaboration au sein du CEN/TC 224.

Conclusion

Les exigences essentielles prévues par le CRA sont identiques pour tous les produits concernés, quelle que soit leur classification.

Le règlement distingue deux catégories de produits : « importants » et « critiques ». Celles-ci déterminent la procédure d'évaluation de la conformité que le fabricant doit suivre avant de mettre ses produits sur le marché de l'Union européenne. Il appartient donc au fabricant de classer correctement ses produits et d'appliquer les dispositions correspondantes.

Au vu des informations disponibles (Règlement CRA, Règlement d'exécution et FAQ), un nombre limité de produits électroniques de sécurité ainsi que certains dispositifs de détection intrusion relèvent de la catégorie des « produits domestiques intelligents dotés de fonctionnalités de sécurité » de classe I. Par ailleurs, certains produits électroniques de contrôle d'accès sont classés dans la catégorie des produits importants de classe I « systèmes de gestion des identités et logiciels et dispositifs de gestion des accès privilégiés ». Pour ces produits, l'application complète d'une norme harmonisée publiée au Journal officiel de l'Union européenne (JOUE) est nécessaire pour bénéficier de l'auto-évaluation et de la présomption de conformité.

Aucun produit de sécurité incendie ou de sécurité physique n'a été identifié dans la catégorie des produits critiques « dispositifs matériels avec boîtiers de sécurité ». En conséquence, la majorité des produits électroniques de sécurité incendie et de sécurité physique relèvent de la catégorie « par défaut ». Leur conformité aux exigences essentielles du CRA peut être démontrée à l'aide de toute norme couvrant l'ensemble de ces exigences, comme la

norme EN 62443-4-x en cours d'élaboration au sein du CLC/TC 65X, ou les normes horizontales en préparation au sein du CEN/CLC/JTC 13.

Zoug, le 10 février 2026

À propos d'Euralarm

Euralarm représente le secteur de la sécurité incendie et de la sûreté, en apportant leadership et expertise à l'industrie, au marché, aux décideurs politiques et aux organismes de normalisation. Ses membres contribuent à renforcer la sécurité de la société grâce à des systèmes et services de détection et d'extinction d'incendie, de détection d'intrusion, de contrôle d'accès, de vidéosurveillance, de transmission d'alarmes et de centres de réception d'alarmes. Fondée en 1970, Euralarm représente plus de 5 000 entreprises du secteur, pour une valeur estimée à 67 milliards d'euros. Ses membres sont composés d'associations nationales et d'entreprises individuelles à travers l'Europe.

Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

AVERTISSEMENT

Note: The English version of this document is the approved Euralarm reference document.