BAROMÈTRE ETI
SÛRETÉ - SÉCURITÉ

FAIRE FACE
AUX PROBLÈMES DE SÉCURITÉ
EN ENTREPRISE

FRENCHSHIELD

CYBERSÉCURITÉ

SÉCURITÉ DES BÂTIMENTS

E-RÉPUTATION

SÛRETÉ HUMAINE

2015-2019

TABLE DES MATIÈRES

FRENCHSHIELD
LA SURETÉ 360°

INTRODUCTION

Infographie réalisée par 4 consultants juniors en Analyse Stratégique et Intelligence Économique de l'École Internationale des Sciences du Traitement de l'Information.

8 mois de recensement des incidents de sûreté-sécurité survenus depuis 2015.

206 incidents survenus dans des entreprises de taille intermédiaire (ETI) françaises.

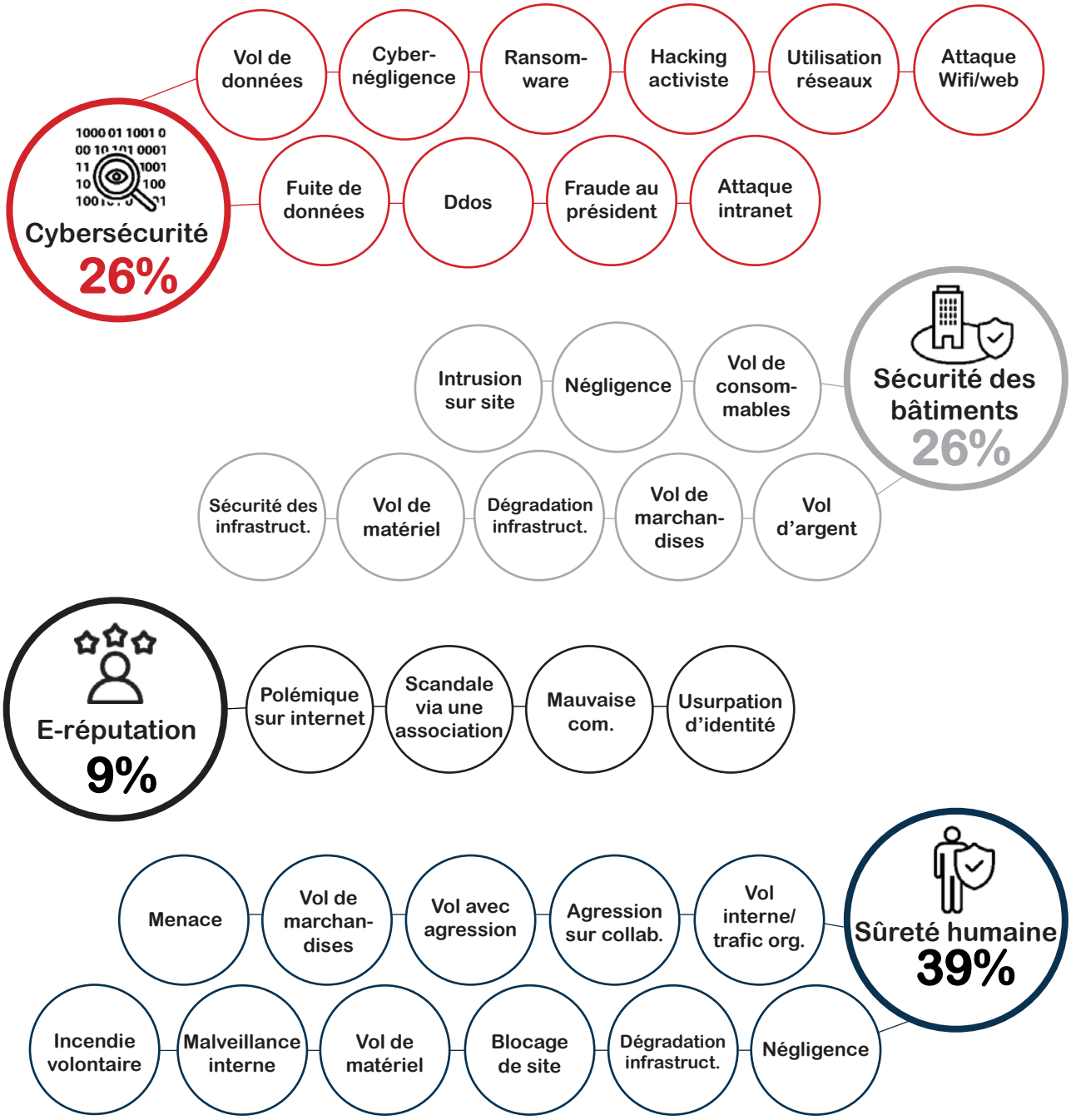
4 catégories d'incidents : e-réputation, cybersécurité, sûreté humaine et sécurité des bâtiments.

Des résultats qui prévoient une **augmentation significative des incidents** de sûreté-sécurité dans les années à venir.

FRENCHSHIELD
LA SURETÉ 360°

TYPOLOGIE DES INCIDENTS

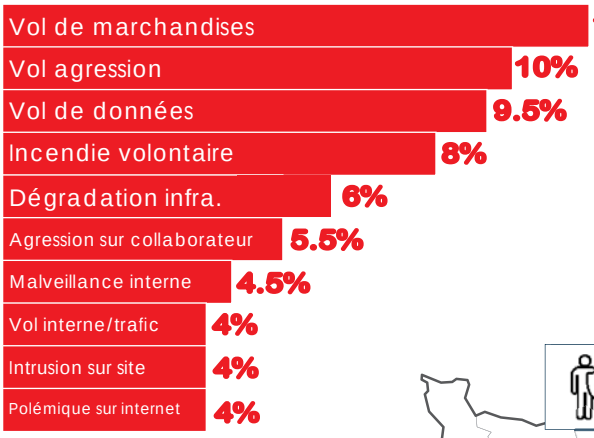
Les 206 incidents recensés ont été catégorisés en 4 piliers : cybersécurité, sécurité des bâtiments, e-réputation, sûreté humaine. 33 types d'incidents sont répartis dans ces piliers.



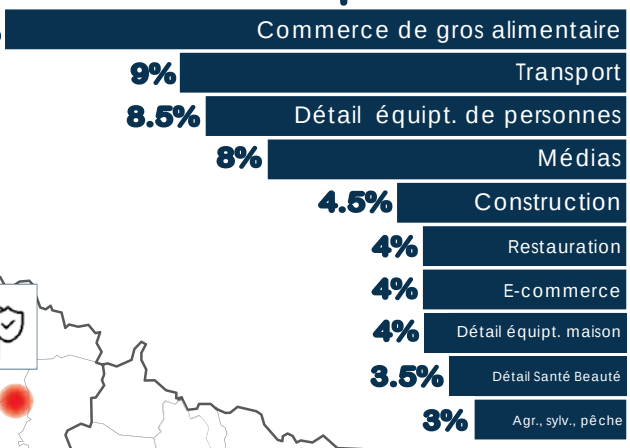
Un glossaire, en fin de document, apporte plus de précisions sur la nature des incidents mentionnés.

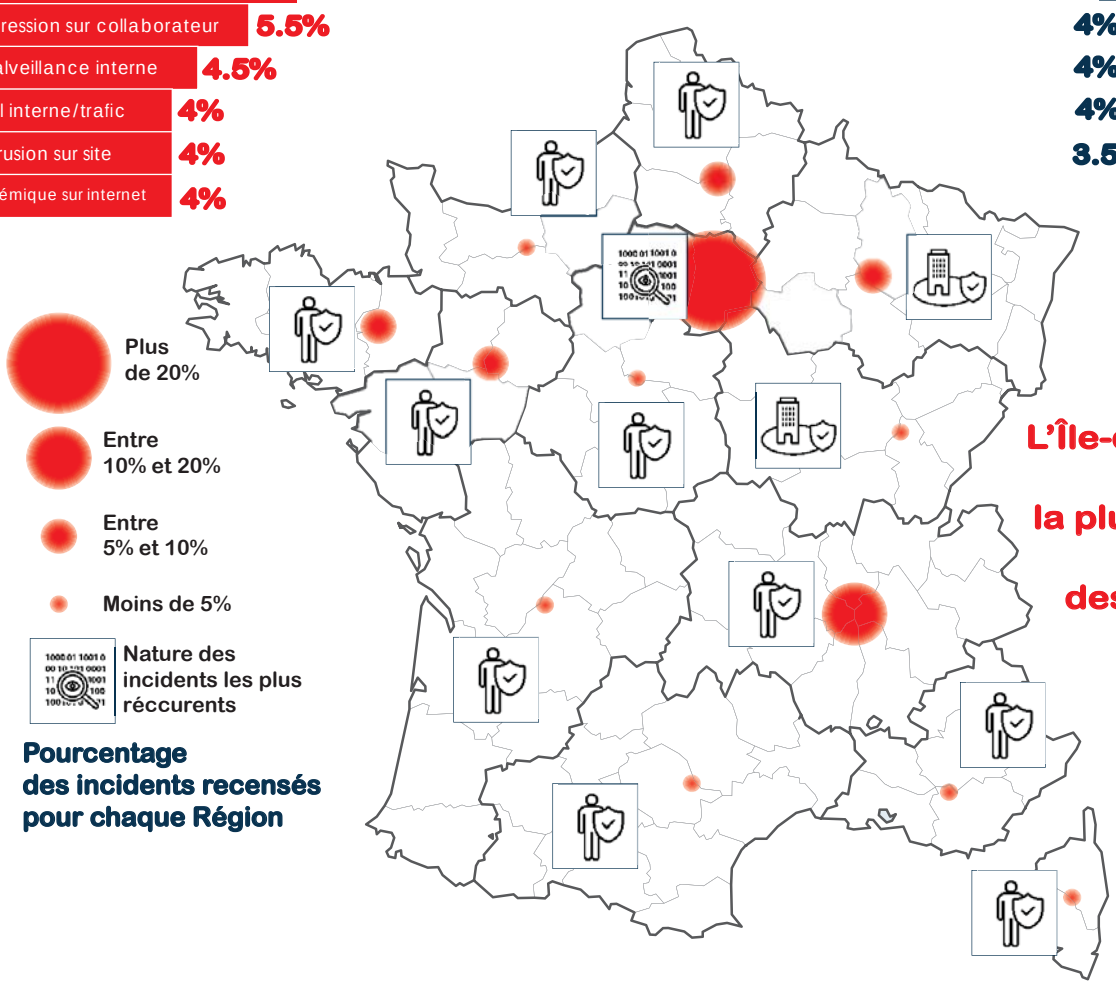
TENDANCES

Les incidents les plus fréquents



Les secteurs les plus touchés

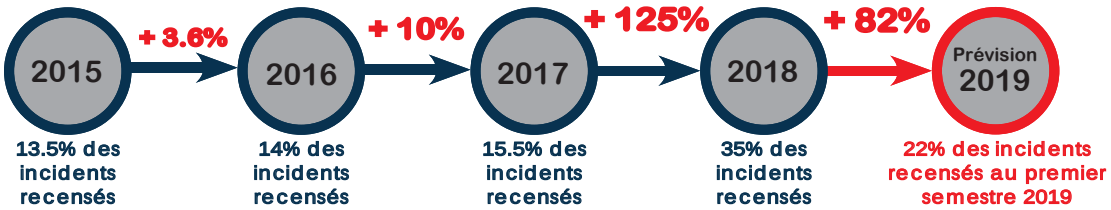




Pourcentage des incidents recensés pour chaque Région

L'Île-de-France, Région la plus touchée avec 33% des incidents recensés

Des incidents de plus en plus réccurents

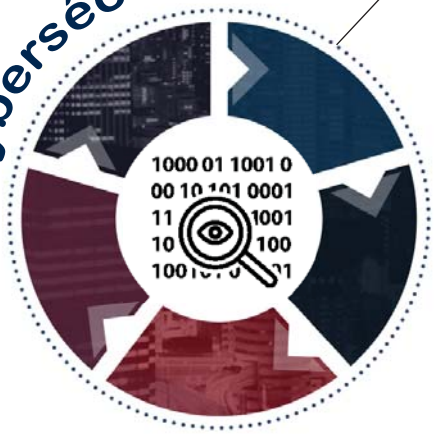


- 2015 : 13.5% des incidents recensés
- 2016 : 14% des incidents recensés
- 2017 : 15.5% des incidents recensés
- 2018 : 35% des incidents recensés
- Prévision 2019 : 22% des incidents recensés au premier semestre 2019

35% des ETI touchées réalisent un chiffre d'affaire compris entre 50M et 150M d'euros

INCIDENTS

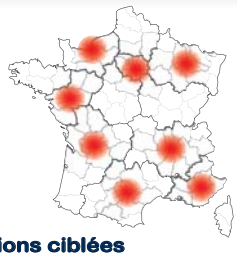
Cybersécurité



26% des incidents recensés

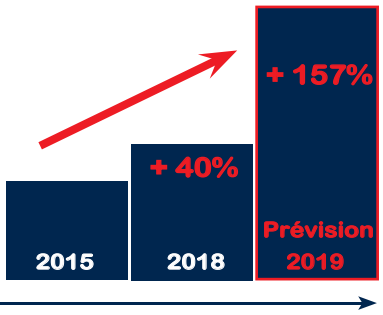
INCIDENTS LES PLUS FRÉQUENTS :

1. Vol de données **36%**
2. Fraude au président **13%**
3. Fuite de données **11%**
4. Cybernégligence **11%**



Régions ciblées

ÉVOLUTION DU NOMBRE D'INCIDENTS de 2015 à 2018 :



SECTEURS LES PLUS TOUCHÉS :

Médias

E-commerce

Services web/cloud

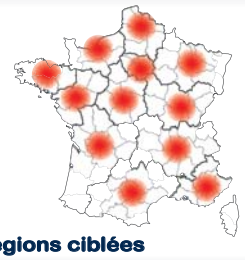
42% des ETI touchées réalisent un chiffre d'affaire compris entre 50M et 150M d'euros

Sécurité des bâtiments

26% des incidents recensés

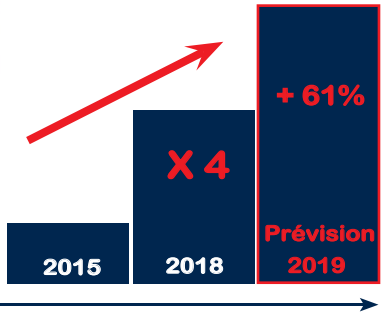
INCIDENTS LES PLUS FRÉQUENTS :

1. Vol de marchandises **43%**
2. Intrusion sur site **15%**
3. Négligence **11%**
4. Vol de matériel **9%**



Régions ciblées

ÉVOLUTION DU NOMBRE D'INCIDENTS de 2015 à 2018 :



SECTEURS LES PLUS TOUCHÉS :

Commerce de gros

Détail équipement maison

Construction

32% des ETI touchées réalisent un chiffre d'affaire compris entre 50M et 150M d'euros

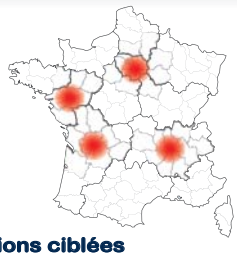
INCIDENTS

E-réputation

9% des incidents recensés

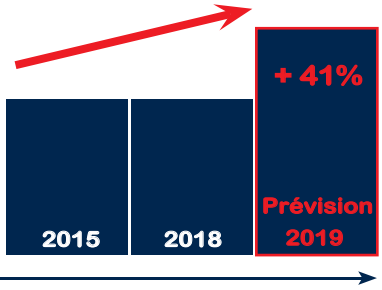
INCIDENTS LES PLUS FRÉQUENTS :

1. Polémique relayée sur internet **40%**
2. Scandale venant d'associations **30%**
3. Usurpation d'identité numérique **15%**
4. Mauvaise communication **15%**



Régions ciblées

ÉVOLUTION DU NOMBRE D'INCIDENTS de 2015 à 2018 :



SECTEURS LES PLUS TOUCHÉS :

Commerce de gros — Santé — Restauration

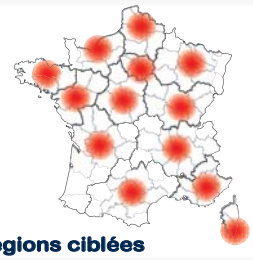
35% des ETI touchées réalisent un chiffre d'affaire compris entre 50M et 150M d'euros

Sûreté humaine

39% des incidents recensés

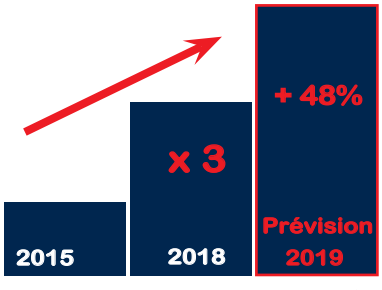
INCIDENTS LES PLUS FRÉQUENTS :

1. Vol avec agression **25%**
2. Incendie volontaire **20%**
3. Dégradation des infrastructures **14%**
4. Agression sur collaborateur **14%**



Régions ciblées

ÉVOLUTION DU NOMBRE D'INCIDENTS de 2015 à 2018 :



SECTEURS LES PLUS TOUCHÉS :

Transport — Détail équipement personnes — Médias

33% des ETI touchées réalisent un chiffre d'affaire compris entre 50M et 150M d'euros

GLOSSAIRE

Piliers d'analyse :

Incidents de sécurité des bâtiments :

- Incident relatif à une intrusion ou à un vol par effraction dans un bâtiment (entrepôt/site de production). L'incident n'a pas donné lieu à l'agression d'un collaborateur.
- Incident faisant suite à une négligence sur un lieu de production ou d'activité de l'entreprise et ayant porté atteinte à la sécurité des travailleurs.

Incidents de sûreté humaine :

- En interne : incident relatif à un acte de malveillance, de sabotage, de vol ou de trafic interne.
- En externe : vol de marchandises, d'argent ou de consommables avec agression sur un collaborateur.
- Violence sur un collaborateur, qu'elle provienne de l'intérieur ou de l'extérieur de l'entreprise.

Incidents de cybersécurité :

- Incident faisant suite à une intrusion dans le système informatique de l'entreprise pouvant donner lieu à un vol d'informations, une extorsion d'argent (ransomware) ou une interruption de l'activité des systèmes/services de l'entreprise.
- Fuite de données dont la cause n'a pas été établie.
- Négligence en matière de cybersécurité aboutissant en la mise en danger des données de l'entreprise ou de celles de ses clients/partenaires.
- Pratiques de fraudes au virement numérique.

Incidents d'e-réputation :

- Incident relayé sur internet portant atteinte à l'image de l'entreprise.
- Polémique créée par une association et relayée massivement sur internet.
- Communication corporate ou personnelle inopportune, critiquée et portant atteinte à la réputation numérique de l'entreprise.

Incidents :

Agression sur collaborateur : attaque physique à l'encontre d'un salarié ou d'un cadre de l'entreprise.

Attaque sur le réseau Wifi/internet de l'entreprise : accès non autorisé au réseau internet de l'entreprise par une personne tierce et donnant lieu en l'arrêt des services proposés par l'entreprise.

Blocage de site : interruption d'activité liée au blocage des entrées de l'entreprise visant à empêcher les salariés à rejoindre leur poste de travail.

Cybernégligence : mauvaise pratique d'un membre de l'entreprise, de manière non intentionnelle, mettant en jeu la sécurité du réseau et du système d'information de l'entreprise (divulgation de mots de passe, ouverture d'un mail frauduleux, etc.).

GLOSSAIRE

Ddos : attaque visant à mettre le réseau ou le système d'information de l'entreprise temporairement hors service.

Dégradation sur infrastructures : acte de malveillance visant à saboter l'appareil de production de l'entreprise ou à causer des dégâts matériels sur ses actifs (locaux, entrepôts, bureaux).

Fuite de données : accès à des données de l'entreprise par des personnes tierces sans raison déterminée, contrairement au vol de données, dont la cause est déterminée.

Fraude au Président et assimilés : arnaque élaborée grâce à l'ingénierie sociale ayant pour objectif de soutirer des sommes d'argent à l'entreprise par virement bancaire.

Hacking activiste : piratage informatique motivé par des pensées idéologiques, politiques, etc.

Incendie volontaire : acte de malveillance consistant à provoquer un incendie de façon délibérée.

Intrusion sur site : accès non autorisé de la part d'une personne sur un site appartenant à l'entreprise.

Malveillance interne : acte perpétré par un membre de l'entreprise visant à nuire au bon fonctionnement de la structure.

Mauvaise communication (e-réputation) :
- Action de communication/publicité inopportune de l'entreprise générant de vives critiques de la part du public.
- Communication personnelle d'un cadre ou d'un salarié de l'entreprise qui donne lieu à des critiques de la part du public.

Menace : menace perpétrée à l'encontre d'un membre de l'entreprise par une personne tierce.

Négligence : mauvaise pratique d'un membre de l'entreprise/erreur opérationnelle, de manière non intentionnelle, mettant en danger la sécurité de l'environnement de l'entreprise et/ou de ses salariés.

Polémique relayée sur internet : scandale portant atteinte à l'image de l'entreprise "viralement" partagé sur les réseaux sociaux par des communautés d'internautes et/ou de consommateurs.

Ransomware : attaque informatique accompagnée d'une demande de rançon.

Sécurité des infrastructures : défaut d'une structure entraînant la mise en cause de l'intégrité physique d'un client ou d'une personne tierce.

Scandale alimenté par une association : scandale faisant suite à une vidéo ou une polémique générée par une association qui défend des intérêts particuliers (L214, Greenpeace).

Utilisation des réseaux : intrusion d'une personne dans un réseau informatique dans le but d'accéder aux données internes de l'entreprise ou à une connexion internet.

Usurpation d'identité numérique : atteinte à la réputation de l'entreprise par la copie des éléments constituant son identité numérique : site internet, logo, slogan…. Action malveillante dont le but est d'arnaquer des clients, porter atteinte à la réputation de l'entreprise, etc.

Vol avec agression : vol accompagné de violence sur une personne de l'entreprise.

Vol d'argent : appropriation illégale de monnaie fiduciaire aux dépens de l'entreprise (caisses, convoyeurs de fonds).

Vol de consommables : appropriation de produits consommables (carburants, fournitures de bureau) de manière illégale.

GLOSSAIRE

Vol de données : capture des données de l'entreprise par une personne extérieure, de façon délibérée.

Vol de marchandises : appropriation illégale par une personne extérieure à l'entreprise de marchandises produites par l'entreprise.

Vol de matériel : appropriation d'outils/de matières premières servant à la production par une une personne extérieure à l'entreprise (ex : matériel de construction, support aux transport).

Vol interne/ trafic organisé : vol ou trafic résultant d'actions perpétrées en collaboration avec les salariés de l'entreprise.

Secteurs d'activité :

Commerce de gros alimentaire : activité de vente de produits alimentaire et BFRS aux détaillants et surfaces de grande distribution (Ex : Panzani, Pierre Martinet, Petit Navire).

Construction : activités de commerce de gros/de vente au détail en magasin de matériaux de construction et activités de construction de bâtiments (hors promotion immobilière).

Détail de santé/beauté : détaillants de produits de beauté (Ex: Séphora, Nocibé) ou de produits avec prescription médicale (Ex : Afflelou, Optic 2000,...).

Détail équipement de maison : vente au détail de meubles, de décoration d'intérieur, d'équipements pour l'extérieur (Ex: Gamm vert, Maisons du monde, Lapeyre).

Détail équipement de personnes : vente au détail en magasin d'habits, de chaussures, de maroquinerie (Ex : Zara, Lacoste).

E-commerce : vente en ligne effectuée par des pure players avec peu voire aucune infrastructure physique (Ex : Leboncoin).

Médias : presse écrite, télévision, radio et autres médias (Ex : Le Figaro, France Bleu, France Info).

Restauration : activités de restauration rapide (Ex : Quick), restauration collective et activités de restauration spécialisée (Ex : Newrest).

Santé : laboratoires d'analyses, laboratoires médicaux (Ex: Eurofin Biomnis, CEVA santé animale).

Transports : activité de fret et de livraison express (Ex: DHL France, Easydis, Relais Colis). Les activités de stockage et logistique sont intégrées à une autre section ("Stockage").