Enova
Guide d'hygiène sécurité pour l'usine connectée

Sylvain Castillo
Senior Manager, Cyber Risk & Security

15/09/2016

CYBER RISK & SECURITY

Scope: ICS CS activities

Depuis près de 5 ans, Beijaflore sécurise les systèmes de contrôle industriels (ICS) d'Europe, d'Asie et d'Amérique

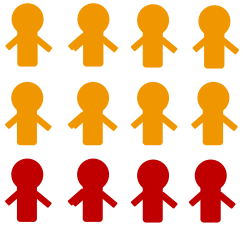
CREATION EN

2000

COLLABORATEURS

800

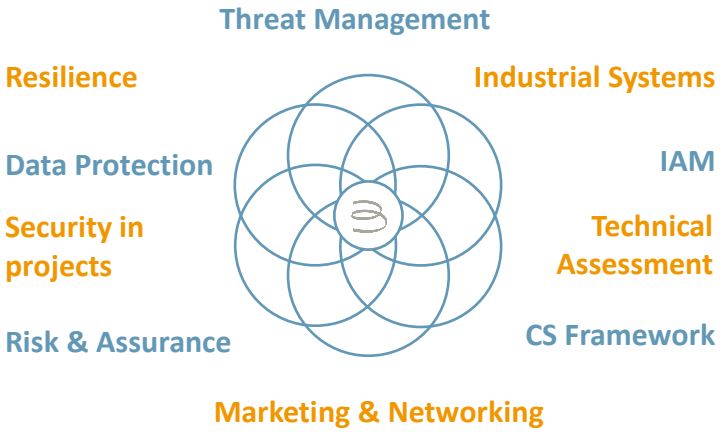
Dont **100** experts cyber sécurité



CHIFFRE D'AFFAIRES

75 **M€**

EXPERTISES CYBER SECURITE



SECURITE DES SYSTEMES INDUSTRIELS

- Analyse de risques en phase d'ingénierie
- Design d'infrastructures sécurisées
- Durcissement d'usines existantes
- Formation des responsables opérationnels
- Audits (FAT/SAT, commissioning)

L'évolution des ICS soulève de nouveaux enjeux de cyber sécurité

Les besoins des opérationnels ont évolué, et continuent d'évoluer

- La convergence avec les ERP entraine des interconnexions avec l'informatique de gestion
- Les coûts sont en permanence optimisés :
  - La maintenance à distance se démocratise
  - Les technologies sont standardisées, abandonnant peu à peu les protocoles propriétaires

Les usines connectées sont peu préparées aux cyber menaces

- Elles se retrouvent exposées à des malwares génériques
- Elles sont vulnérables à des attaques sophistiquées qui peuvent avoir des conséquences dramatiques

La maturité cyber sécurité est encore faible

- Les automaticiens sont peu sensibilisés aux risques d'une usine connectée
- Il s'agit d'un périmètre de responsabilité souvent mal établi
- Un état des lieux similaire à celui de l'informatique d'il y a 20 ans

L'industrie doit faire face à plusieurs nouveaux risques

Incidents de sûreté

Impacts humains dus à des :

- Expositions à des substances nocives
- Collisions avec le matériel (ex : AGV)
- Incidents liés aux atmosphères explosives (ATEX) et aux liquides inflammables

Défauts qualité

Déviation des bonnes pratiques de fabrication :

- Contamination des produits (ex. mauvais dosage)
- Mauvais étiquetage, emballage ou stockage (confusion entre les produits)

Arrêts de production

Dysfonctionnements majeurs :

- Des systèmes en goulot d'étranglement du processus (ex. wrapper)
- Des serveurs applicatifs industriels (ex : MES)

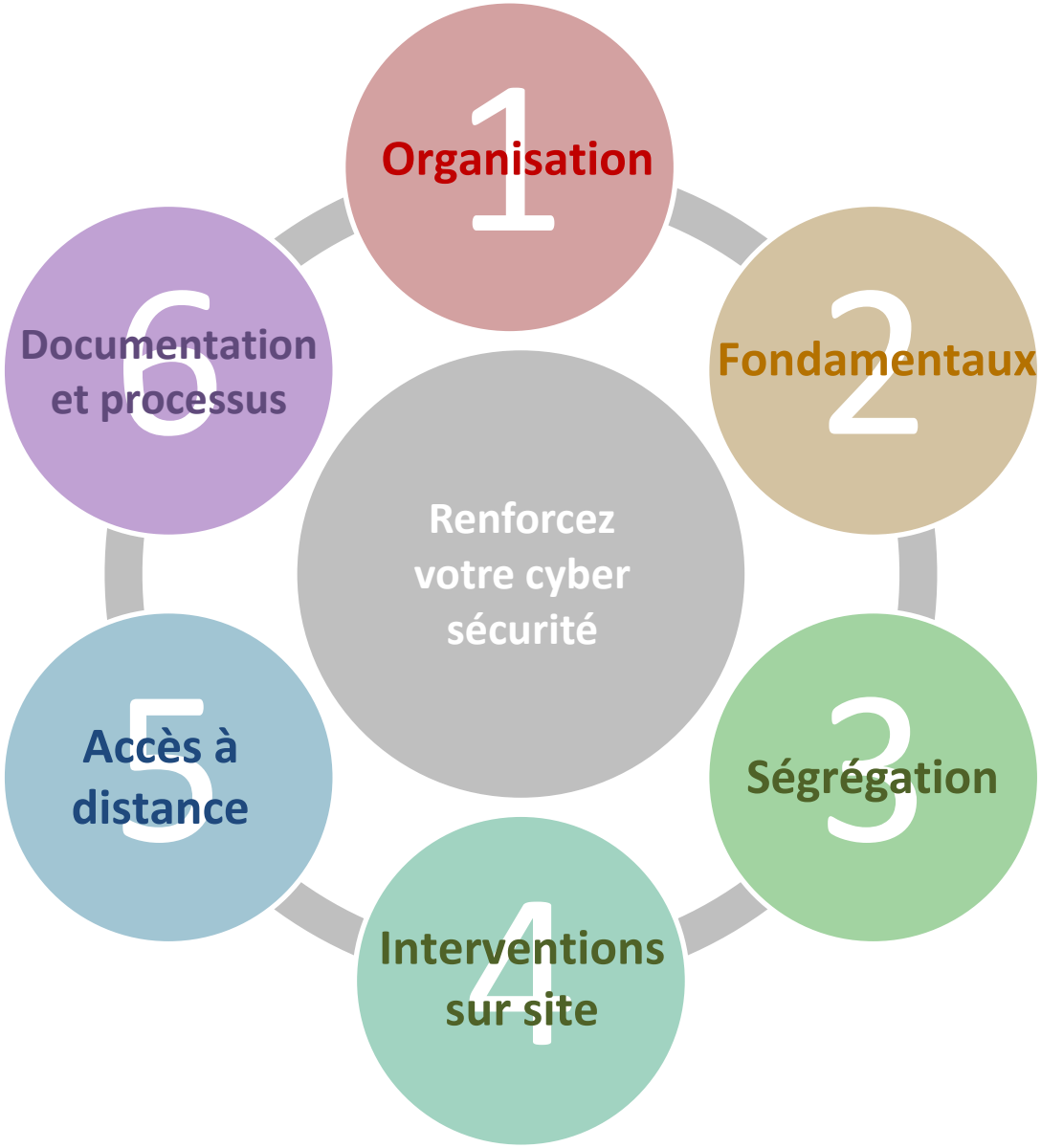
Conséquences potentielles

 Blessures & décès

 Perte d'homologation

 Perte de chiffre d'affaires

6 piliers pour sécuriser vos actifs industriels



Pilier #1 – Mettre en place une organisation pour la sécurité des usines

Le sponsorship du management

Le projet est piloté en central par la direction industrielle / des opérations, avec le soutien de la DSI Groupe

Une sensibilisation à la cyber sécurité :

- Au niveau du comité exécutif
- Au niveau des responsable d'usines

Un relai en usine est en charge de l'application locale de la politique de cyber sécurité

Points d'attention

Etablissement d'un corpus documentaire

Définition d'une politique de cyber sécurité industrielle

Identification d'un plan pluriannuel de sécurisation des usines

Formalisation de la gouvernance cyber sécurité industrielle

Pilier #2 – S'assurer que les fondamentaux sont correctement mis en œuvre

Par où commencer?

- Antivirus pour protéger des malwares génériques
- Politique stricte de gestion des mots de passe
- Blocage USB, la première source de malware
- Sauvegardes des systèmes et des automates
- Gestion tactique des correctifs de sécurité

Points d'attention

Sécurisation des automates

- Authentification pour la programmation
- Switch physique de lecture seule (sûreté)
- Surveillance des changements sur les fichiers projets
- Application des correctifs uniquement en maintenance

Pilier #3 – Séparer les réseaux en zones de sécurité

Boite à outils pour la ségrégation

Une ségrégation logique (VLANs) suffit dans l'essentiel des cas

Les pare-feux séparent les différentes zones

Les IPS peuvent bloquer toute communication suspicieuse mais sont sujets à des faux positifs

Les diodes assurent un trafic unidirectionnel mais amènent des contraintes opérationnelles

Points d'attention

Règles pour la ségrégation

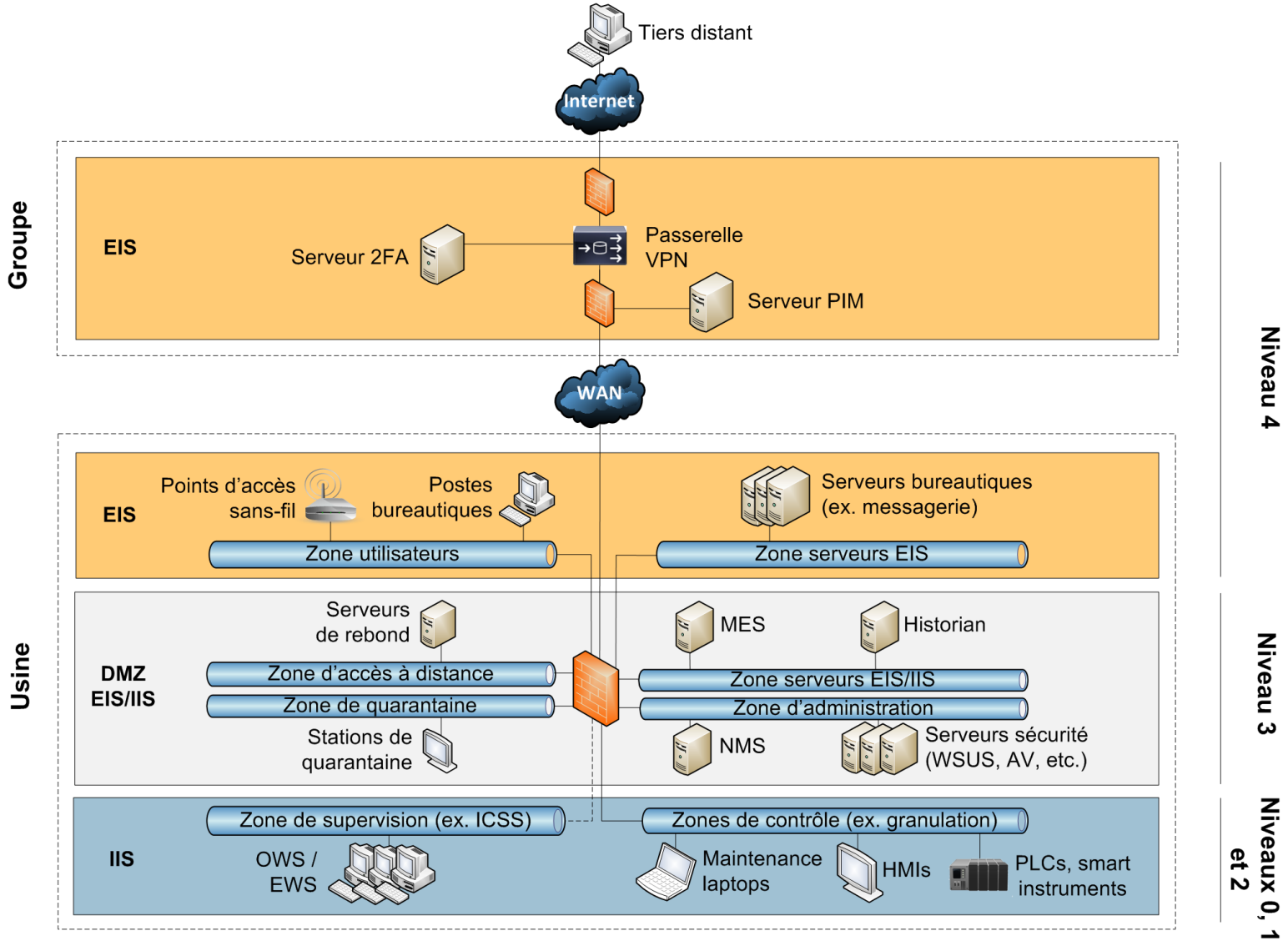
Séparer le SI bureautique du SI industriel

Placer tous les composants intermédiaires en DMZ

Séparer les réseaux de procédé de ceux de sûreté

Pour aller plus loin, identifier les zones et conduits (IEC 62443)

Pilier #3 – Exemple (simplifié) d'architecture sécurisée



Pilier #4 – Cadrer les interventions sur site

Quels sont les risques ?

Propagation de malware à partir d'ordinateurs portables et de clés USB

Installation de logiciels de fournisseurs non testés

Solutions

Scanner les ordinateurs portables et les clés USB

Sensibiliser les tiers à la sécurité, des contrats jusqu'à l'induction de sûreté

Tendances

Vérifier la propreté des supports amovibles avant de les utiliser avec des stations de quarantaine

Exploiter l'arrivée de la virtualisation en usines pour créer des environnements de staging

Favoriser les interventions à distance

Pilier #5 – Renforcer la sécurité des accès distants aux usines

Quels sont les risques ?

Points d'entrée obsolètes toujours en usage (ex. modems)

L'accès à distance est généralement imposé contractuellement

Solutions

Utilisation d'une passerelle VPN centrale

Authentification forte

Durcissement de tous les composants liés à cet accès

Tendances

Limiter l'accès distant des tiers à des serveurs de rebond, particulièrement durcis (ex. application whitelisting)

Privileged Identity Management (PIM) assure une traçabilité détaillée sur les actions réalisées au cours d'une session à distance

Pilier #6 – Maintenir localement une documentation et des processus performants

Connaître son environnement

Maintenir la documentation de l'infrastructure

Cartographier ses actifs et identifier les plus sensibles

Maintenir en conditions de sécurité

Définir une procédure de référence pour gérer les changements

Mettre en place localement des processus de sécurité opérationnels

Points d'attention

Sécurité opérationnelle

Gestion des incidents de sécurité

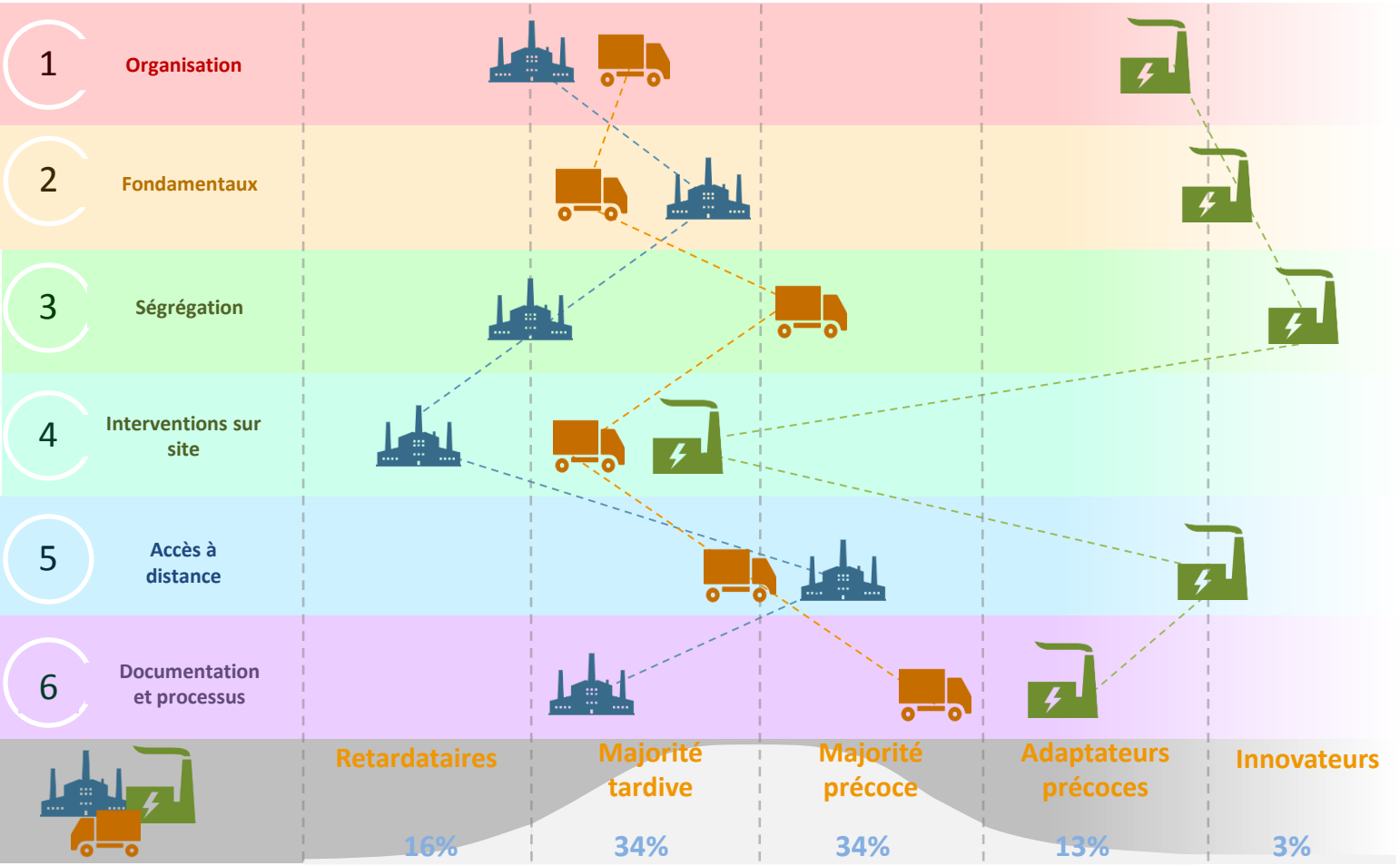
Gestion des correctifs

Gestion des identités et des accès

Gestion des visiteurs

Définition d'indicateurs de suivi par processus

La maturité cyber sécurité des systèmes industriels



Transport

Energie

Manufacturing

La cyber sécurité doit tenir compte des évolutions futures

Virtualisation

- Les attaques de type « **VM escape** » sont rarissimes
- Toutefois, l'étendue des **droits administrateurs** amène souvent à séparer les systèmes critiques
- Cela amène également des **opportunités** de sécurisation (notamment en termes de **résilience**)

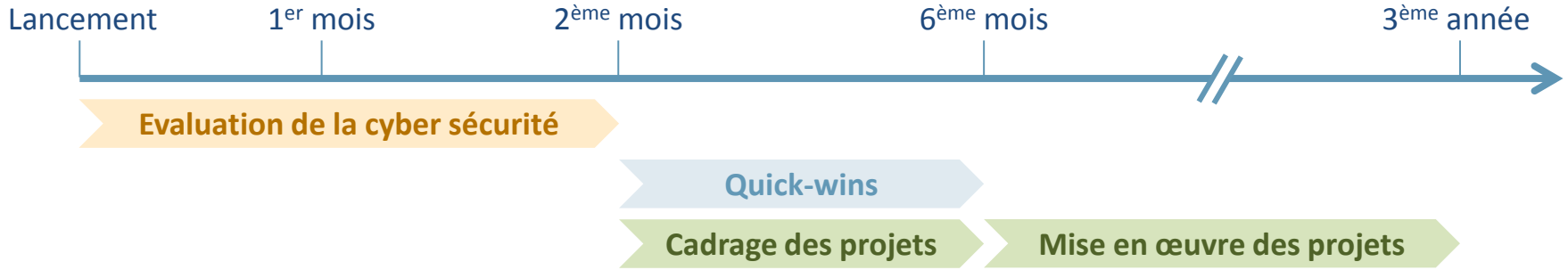
Cloud

- Les enjeux du cloud en sécurité : maîtriser les actifs informatiques **sans savoir les localiser**
- Les clouds, même publics, ne sont **pas incompatibles avec la sécurité**. Ils nécessitent simplement la mise en place de **mesures spécifiques**

Industrial IoT

- Les industrial IoT augmentent l'**exposition** des systèmes industriels
- L'objet lui-même doit être sécurisé (intégrité du firmware, chiffrement des données stockées)
- Mais également **ses interfaces** (portails d'administration, API, flux réseaux, etc.)

Elaborez un plan d'action pour durcir vos biens industriels



Evaluation de la cyber sécurité

Audits de cyber sécurité
Conformité aux normes
Conformité à la politique de sécurité
Recommandations

Mise en œuvre des quicks-wins

Efforts de mise en œuvre limités
Bénéfices sécurité à court terme
Réutilisation des actifs existants
Fondamentaux

Lancement des projets

Investissements soutenus
Projets à long terme
Refontes de l'infrastructure
Actions stratégiques

Et vous, où vous situez-vous ?

Contact

Sylvain Castillo

Senior Manager

+33(0) 6 01 39 51 77
scastillo150@beijaflore.com

Pavillon Bourdan
11-13, avenue du Recteur Poincaré
75016 Paris