Présentation
CHRU DE NANCY

Laurent DERTIN
Christophe JAQUET

Le 05/06/2026

123CS
MANAGE DATA, SECURE THE FUTURE

123CS, un acteur de référence dans la Cybersécurité et le management des données de Santé

Sommaire

1. Présentation et rappel du contexte
2. Et le secteur des établissements de Santé ?
3. Notre savoir faire chez 123CS: Cybersécurité, HDS, Infogérance, DPO, Cot'Optim
4. Focus Cyber : Le Mod@block

Constats en France de la cybercriminalité

- Chiffres clés :

- **3ème** secteur le plus ciblé, **+ 30%** en 2024 : la Santé
- **80%** des attaques proviennent de négligences humaines
- **90%** des cyberattaques démarrent par un e-mail de phishing
- **62 %** sous forme de ransomware, ou logiciel d'extorsion avec prise d'otage des données
- **100 000 €** Impact financier moyen d'une attaque pour une petite entreprise (- 50 pers, ≤ 7,5 M €) jusqu'à **plusieurs M€** pour un hôpital.

La vraie menace, ce n'est plus la cyberattaque…
…c'est de ne pas être prêt quand elle arrivera !

Santé – Cyber & HDS - Obligations et Recommandations

1. Conformité au RGPD (UE 2016/679).

Le directeur est responsable des données collectées (nom, numéro de sécurité sociale…). Il se doit de :

- Tenir un registre des traitements et Informer les personnes concernées.
- Mettre en place de mesures techniques et organisationnelles de sécurité.
- Notifier à la CNIL en cas de violation de données dans les 72 heures.

2. Sécurité des Systèmes d'Information (SSI)

Recommandations de l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) :

- Pare-feu, antivirus, mises à jour régulières. Sauvegardes régulières, avec copie hors ligne.
- Authentification forte : mot de passe complexe, double authentification si possible.
- Chiffrement des données sensibles. Principe du moindre privilège.
- Personnel : restriction des accès, formation.

3. Référentiel MSSanté et DMP

- Utilisation obligatoire d'outils compatibles MSSanté (Messagerie Sécurisée de Santé).
- L'établissement doit pouvoir alimenter le Dossier Médical Partagé (DMP) et respecter la confidentialité.

4. Network and Information Security Directive 2 (NIS2)

- Mesures techniques et organisationnelles (Analyse politique de sécurité, gestion incidents, cryptage, PRA, PCA…)
- Notification des incidents (sous 24 heures à ANSSI).
- Responsabilité personnelle de la direction (17/10/2024)

Santé – Cyber & HDS - Obligations et Recommandations

1. Obligation légale depuis 2018

Toute donnée de santé à caractère personnel **hébergée en dehors des locaux** (cloud, serveur externalisé) **doit l'être chez un hébergeur certifié HDS pour être en conformité avec la loi**. (Cadre juridique : Article L1111-8 du Code de la santé publique).

2. Obligations spécifiques liées au SI de santé

Si l'établissement est intégré à un système d'information régional de santé (ex. via des GHT ou échanges avec les hôpitaux), d'autres obligations peuvent s'appliquer :

- Respect des référentiels de l'**ANS (Agence du Numérique en Santé)**.
- Participation à des programmes nationaux comme **SUN-ES** (Ségur numérique en santé).

3. La société 123CS appartient à la liste des hébergeurs certifiés

La liste : 👉 https://dsih.fr/annuaire/20/softandem/184/123cs

123 CS en quelques mots

Société de cybersécurité française créée en 2020 s'adressant à tous les acteurs de la Santé: privés, publics, industriels.

Créée par un **DSI de CHU** et un **entrepreneur visionnaire**.

Propose une offre complète de services en France et en Europe visant à :

- **Garantir la sécurité** des établissements de Santé face aux cyberattaques
- **Héberger les Données de Santé - HDS -** après recueil et sécurisation
- **Une utilisation intelligente** de ces informations au bénéfice de tous

Une
Société à taille humaine

Des
Experts à vos côtés

Une
Approche partenariale

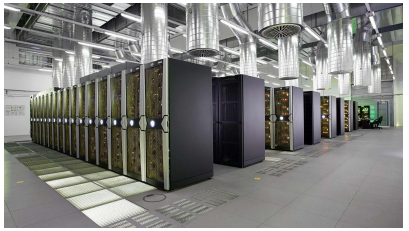
Nos Produits & Services

Cybersécurité

Suivi personnalisé Cybersécurité

Boite Noire, Grise, Blanche

Phishing



Hébergement des données de santé

- **Editeurs : RIS , PACS, VNA**
- **BOX**

Support Infrastructure
Data Expertise
By your side

Création de SIDE :

Schéma Directeur SI

Infogérance

Equipement informatique

Gamme Mod@ :

- **Mod@block**
- **Mod@Scan**

Délégué à la protection des données

Délégué à la protection des données :

Externe

Création de TIGER DATA, société spécialisée dans l'utilisation secondaire des données :

- **Cot'Optim**
- **Valorisation des données d'imagerie**

SECURISATION MODALITES : MOD@BLOCK

Principes élémentaires de notre Sécurisation :

1. Détection attaques (Crypto, Ransomware, ….)

2. Isolation immédiate de la modalité, du Lan (ou Vlan) de l'établissement attaqué.
   - Eviter toute propagation d'attaque

3. Fonctionnement en autonomie de la modalité.

Schéma de principe des SI au sein des établissements de Santé

➔ Quand tout va bien…

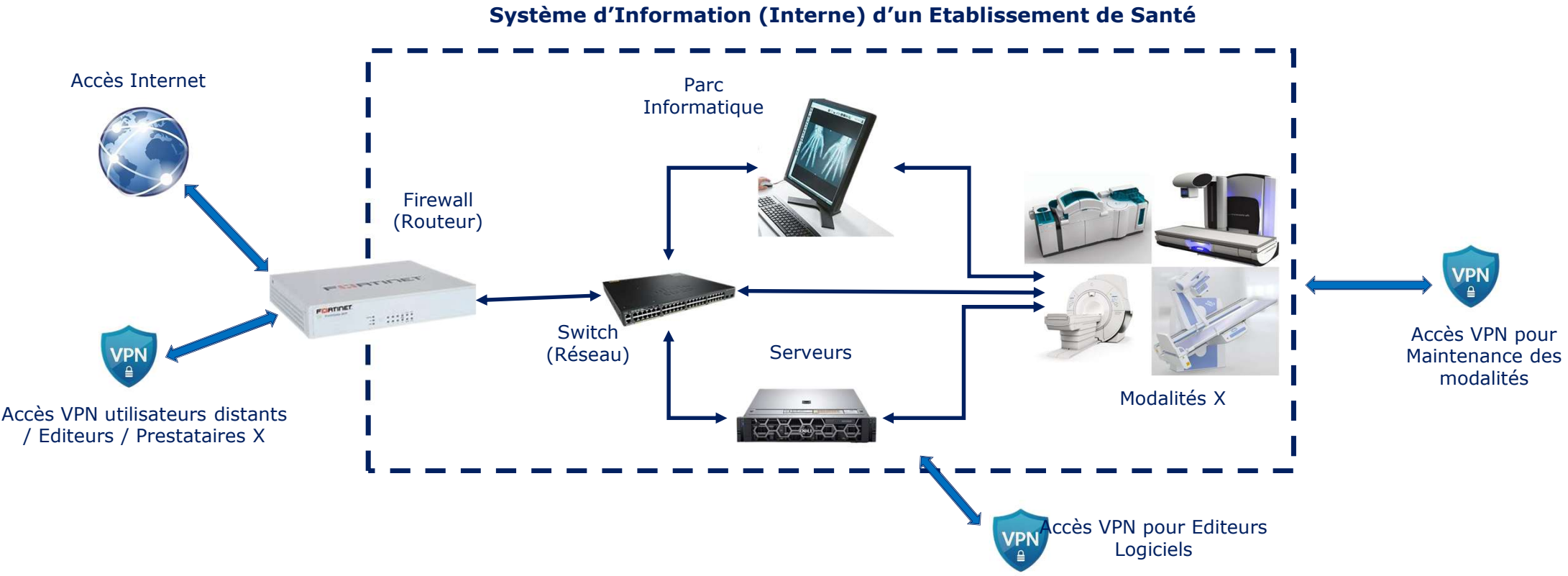


Schéma de principe des Cyberattaques

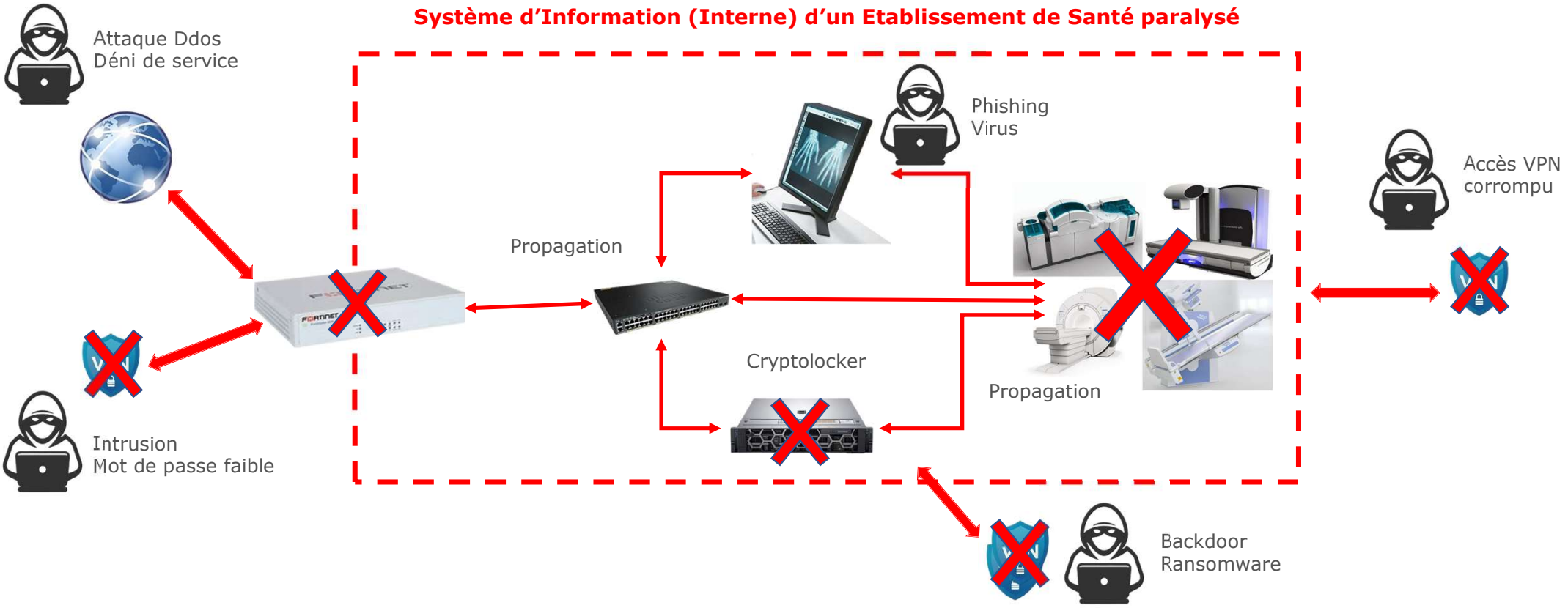


Schéma de principe des SI au sein des établissements de Santé

➔ **La solution : l'isolement en cas de Cyber Attaque**

Système d'Information (Interne) d'un Etablissement de Santé

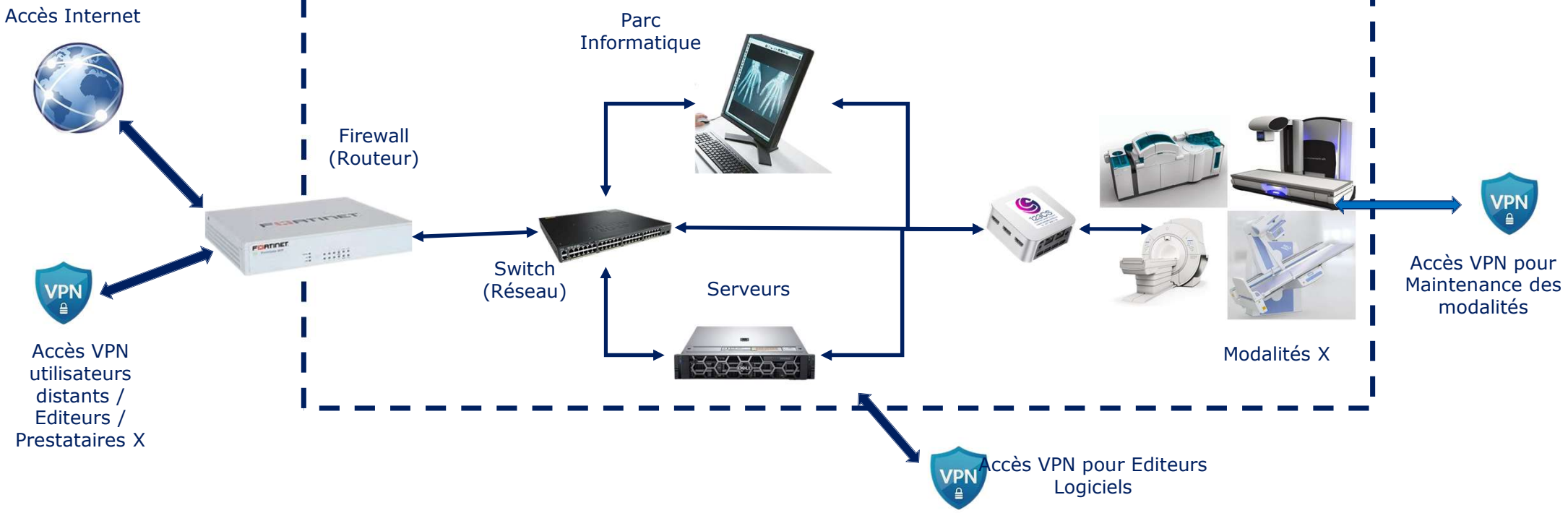
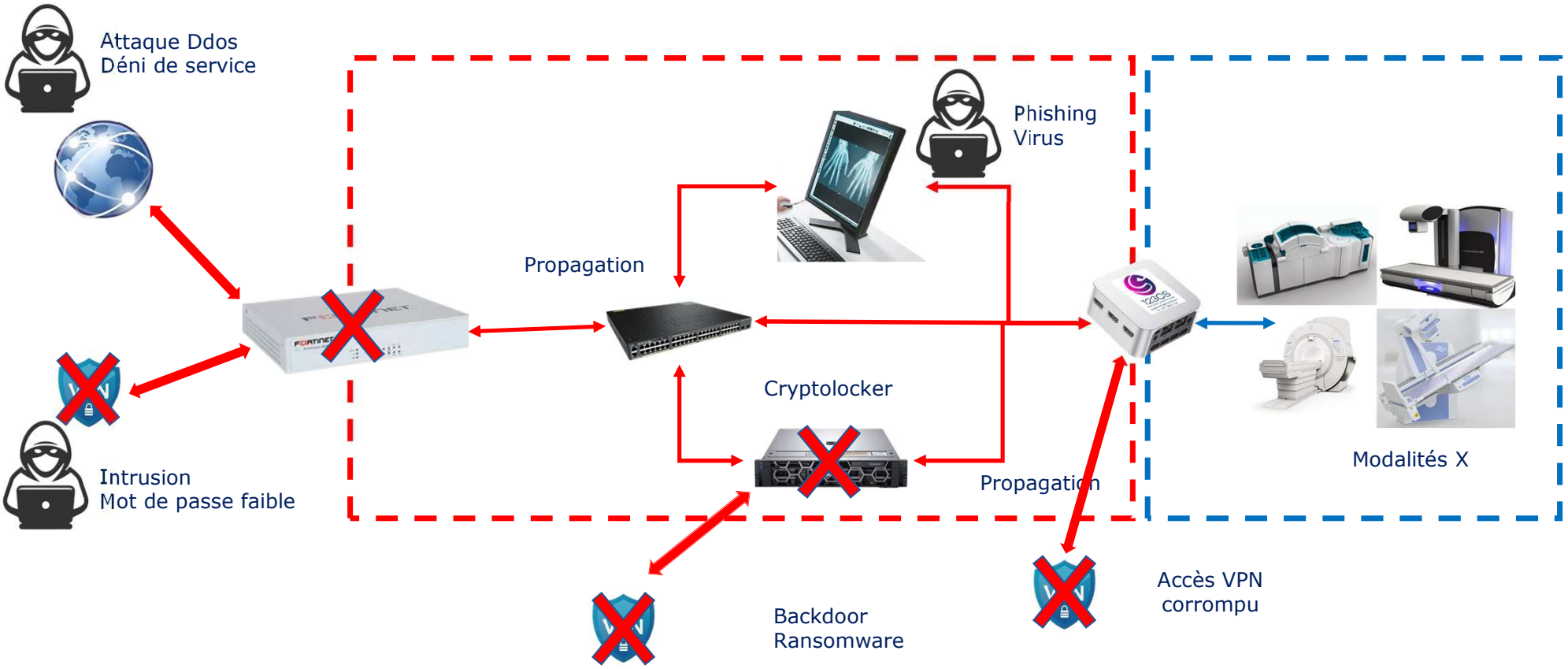


Schéma de principe des Cyber Attaques : avec isolement Mod@Block



Solution Boitier Sécurisation, en cas de Cyberattaque :

1. La Mod@block, détecte l'attaque (Crypto, chiffrement, virus, ….),

2. Isolement de la modalité, en aval du boitier, du reste du réseau,
   - Déconnexion Logique et Physique pour isoler l'équipement à protéger

3. Remontées d'informations au « Cockpit Datacenter»,
   - Visualisation de la typologie de l'attaque par notre équipe d'ingénieurs en Cybersécurité
   - Remontées d'alertes pour l'établissement Client et/ou notre Partenaire Industriel

4. Intervention (si possible) à distance pour contrer ou repousser l'attaque (hors Boitier)

Mise en service :

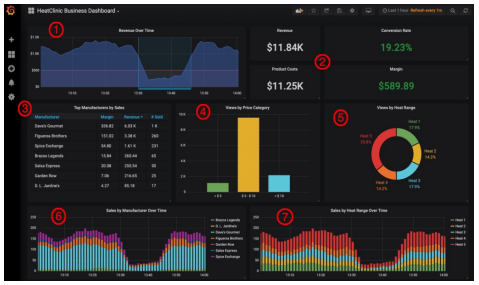
Intégration du boitier en amont de la modalité, sur le site client,

- Pas de limitation de débit,
- Supervision des taux de flux, si besoin,
- Paramétrage Réseau / VLAN

Notre abonnement :

1. Supervision 24/7, par nos équipes de Cyber Experts(Cybersécurité, Réseau & Systèmes)

2. Alertes pour différents points :
   - Attaques,
   - Pertes de connexion,
   - Volumes en transit (débits),
   - …



Remise en service :

Intervention post- attaque pour remettre en fonctionnement le Mod@block

Les avantages de notre solution :

- Sécurisation renforcée par le boitier Mod@block
- Suppression des contraintes d'obsolescence des systèmes CEM (Windows 7, ..)
- Suppression des interactions négatives entre les directions informatiques et biomédicales des clients
- Déconnexion immédiate des liens lors d'attaques (en entrée ou en sortie)

NOS CERTIFICATS ET LABELS / CYBER et HDS

- ✓ Membre actif de l'ACN : Alliance pour la Confiance Numérique
- ✓ Certifié Cybersécurité Made In Europe
- ✓ Certifié ISO 27 001
- ✓ Certifié HDS
- ✓ Certification France Cybersecurity
- ✓ Professionnel Référencé pour la Cyber
- ✓ Certifié Expert CYBER
- ✓ Membre de l'APSSIS
- ✓ SECNUMEDU (ANSSI)
- ✓ SGDSN
- ✓ Certification PASSI RGS (ANSSI) – *En cours*
- ✓ SECNUMCLOUD (ANSSI) – *En cours*

Merci pour votre attention!

123CS

MANAGE DATA, SECURE THE FUTURE

Votre Contact :

Christophe JAQUET
Directeur Commercial
+33 6 20 22 36 62
cjaquet@123cs.fr

18 Allée d'Orléans - 33 000 Bordeaux – France / +33 5 35 54 11 08 / https://123cs.fr/