GIMELEC
Nous décuplons les énergies

Sensibilisation à la Cyber-OT dans les hôpitaux

Etude sectorielle du Club Cyber OT du GIMELEC

Novembre 2022

GIMELEC CYBER OT
le club des offreurs pour la cybersécurité industrielle

Que trouver dans ce guide ?

1. Différencier les cybersécurités IT et OT
2. Identifier les Systèmes Techniques Hospitaliers
3. Trouver les documents de référence
4. Découvrir les risques métiers, les architectures, les bonnes pratiques associés aux systèmes OT critiques
    1. Système de Sécurité Incendie (SSI)
    2. Gestion Technique de Bâtiment (GTB)
    3. Gestion Technique Electrique (GTE)
    4. Equipements Biomédicaux
5. Connaitre le top 10 des mauvaises pratiques !

A qui s'adresse ce guide ?

Aux professionnels du monde hospitalier qui souhaitent se sensibiliser ou sensibiliser leurs directions aux enjeux de la cybersécurité des systèmes industriels hospitaliers. Ces systèmes sont critiques et doivent être protégés

Introduction

Qu'est-ce que le Club Cyber-OT du GIMELEC ?

- Le **GIMELEC** est une association professionnelle, **porte parole des industriels de l'électronumérique et de l'automatisme**. Ses 212 membres développent des solutions pour les **transitions énergétiques, industrielles et numériques sur le marché français**, avec plus de 16 milliards de chiffre d'affaires.

- Le **Club Cyber-OT du GIMELEC** est un Club regroupant un collectif d'entreprises et d'organismes de recherches, actifs dans le domaine de la **cybersécurité des systèmes industriels et urbains**, communément appelée **Cyber OT**. Le collectif vise une action en faveur des solutions sécurisées et participent à une maitrise de la souveraineté numérique française et européenne.

- Créé en 2020, successeur du Cluster ECC4iU, **le Club rassemble désormais une trentaine d'entreprises phare du secteur,** couvrant l'ensemble des offres du secteurs : conseil et audit, matériels, installation et maintenance.

- **L'action du Club est structurée sur 5 axes fondamentaux au service du développement de la Cyber-OT :**

Accompagner la prise de maturité du secteur

en communicant sur l'importance de la cyber pour accompagner les gains de compétitivité du digital.

Développer des partenariats

pour co-construire les pratiques de cyber-OT dans tous les secteurs concernés, avec les acteurs métier déjà en place.

Appuyer le développement des offres de formations nécessaires

en sensibilisant sur les besoins de formation croisée entre cybersécurité et connaissance du monde industriel.

Coconstruire le cadre règlementaire, normatif et de certification

en facilitant les échanges et l'émergence de consensus au niveau français puis européen.

Suivre la conjoncture du marché

en permettant aux membres de croiser leur vision des dynamiques et des caractéristiques du marchés et des enjeux associés.

Méthodologie employée

- Nous remercions les experts du secteur de la **cybersécurité** dans les hôpitaux qui ont contribué par leurs échanges à enrichir cette publication :
  - **Charles Blanc Rolin** – **GCS e-santé Pays de la Loire**
  - **Sandrine Roussel** – **AFIB CHU de Besançon**
  - **Pascal Sabatier** – **RSSI / DPD CHU Aix-en-Provence**
  - **Stéphane Pasquier** – Ancien **FSSI / Ministère de la Transition écologique**

- Cette étude a été menée avec quelques entreprises du Club particulièrement actives sur le marché de la santé :

SIEMENS · STORMSHIELD · Advens Security for the greater good · automatique & industrie · SAUTER Pour l'environnement durable. · seclab -cybersecurity- · Schneider Electric

Etat des lieux Cyber dans les Hôpitaux

2020

Plus de **80 organismes** de santé touchés par rançongiciel

2021

733 incidents de sécurité dont **environ une centaine d'attaques informatiques** ont été répertoriées dans **582 hôpitaux**.

2021-2022

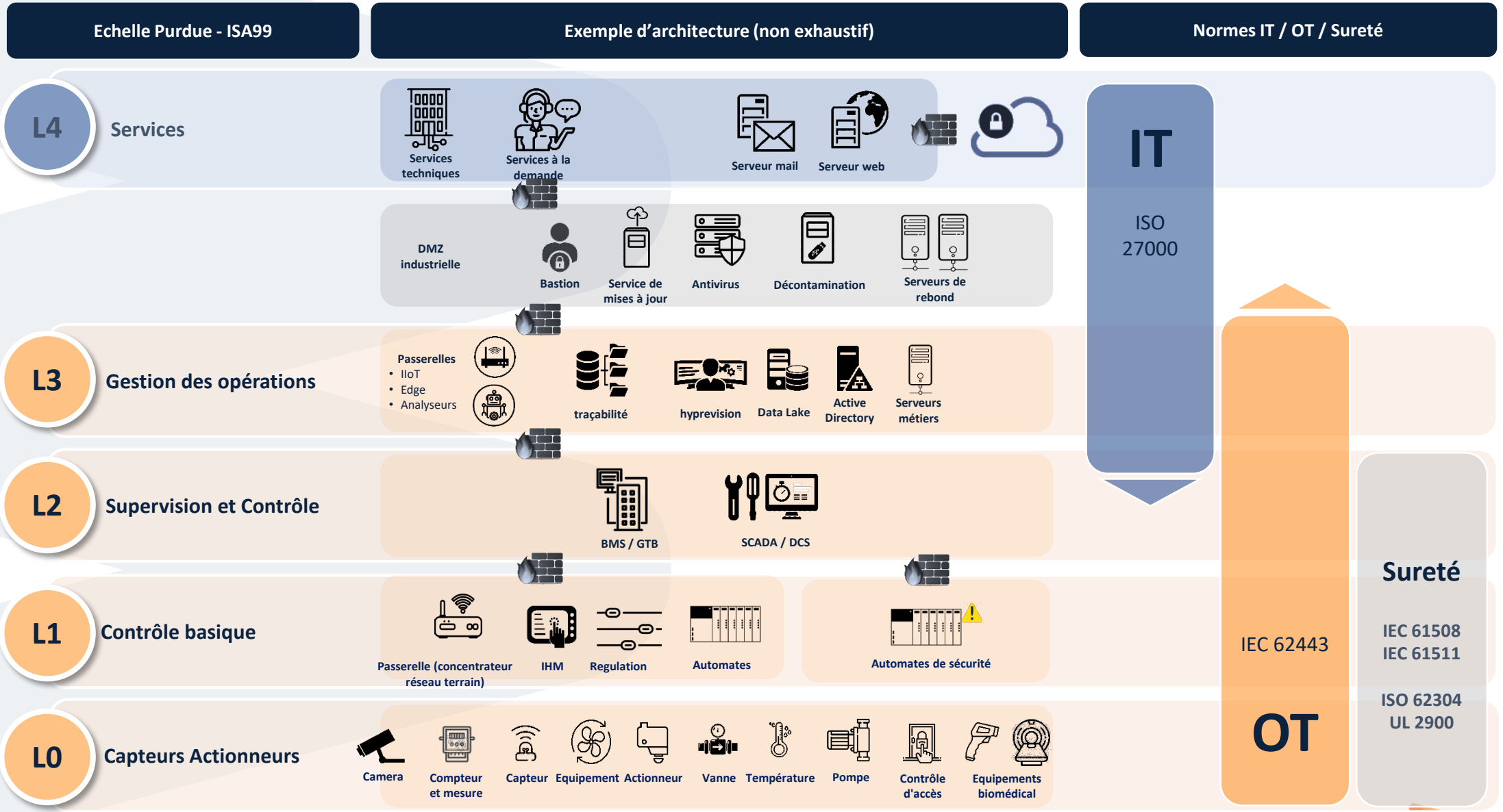
18 millions d’euros pour les hôpitaux avec le plan **France Relance**
20 millions d’euros supplémentaires suite à une cyberattaque en Ile de France

GIMELEC
Nous décuplons les énergies

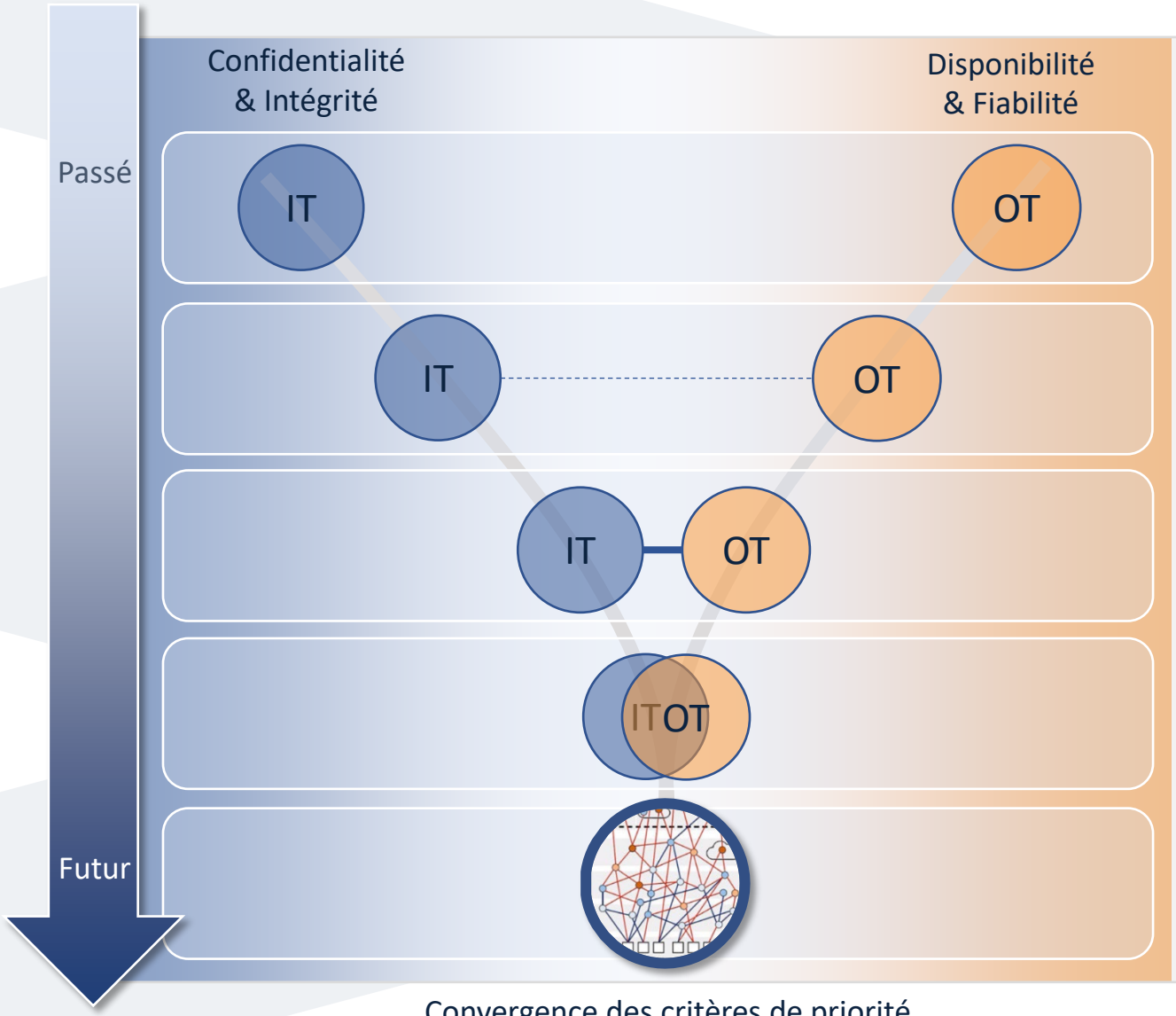
1

Différencier les cybersécurités IT et OT

Les différentes couches IT et OT dans un bâtiment hospitalier



Une tendance à la convergence IT – OT, mais qui ne gomme pas les spécificités métier des systèmes d'informations techniques



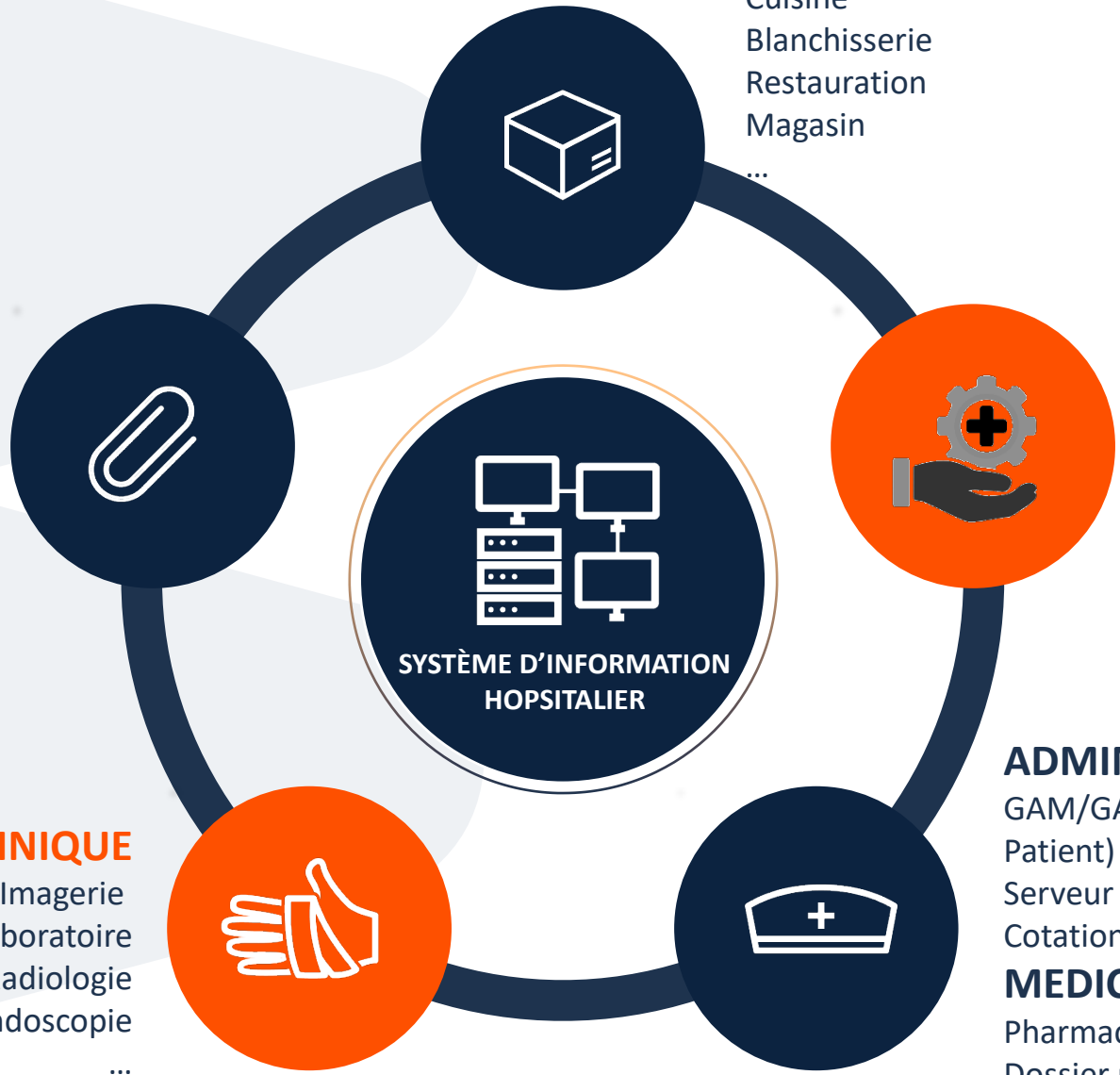
Evolutions Technologiques	Evolutions de la Gouvernance
Réseaux séparés Technologies et cycles de vie différents	Gouvernance distincte Equipes métiers dédiées
Connexion des équipements industriels à Internet Interconnexion de l'OT avec l'infrastructure IT	Premières prises de conscience de façon indépendante
Adoption et installation de systèmes IT dans le périmètre OT Industrialisation de matériels IT	Sensibilisation des équipes, échanges entre les instances IT et OT, voire instances communes Convergence sur les objets communs
Industrie du Futur, jumeaux numériques, cyber physical systems, sécurité by design	Gouvernance partagée Formation croisée des équipes IT/OT Intégration forte entre les processus portés par IT et OT
Plateforme technologique intégrée	Gouvernance commune/intégrée

Convergence des critères de priorité

2

Identifier les Systèmes Techniques Hospitaliers

Système d'Information Hospitalier



LOGISTIQUE
Cuisine
Blanchisserie
Restauration
Magasin
…

ADMINISTRATIF
Ressources humaines
Comptabilité
GEF (Gestion Economique et Financière)

SITH | SYSTÈME D'INFORMATION TECHNIQUE HOSPITALIER
Courant fort
Courant faible
Chauffage Ventilation Climatisation
Contrôle de Salles Blanches
…

MEDICO-TECHNIQUE
Imagerie
Laboratoire
Radiologie
Endoscopie
…

ADMINISTRATIF MEDICAL
GAM/GAP (Gestion Administrative Médicale ou du Patient)
Serveur d'identité
Cotation des actes (PMSI)

MEDICAL
Pharmacie
Dossier médical (SI médecins)
Dossier de soin (SI infirmiers)

SITH - Système d'Information Technique Hospitalier

UTILITES

ELECTRICITE

Monitoring hautes et basses tensions
Délestage
Reconfiguration de boucle

AIR /EAU

Gestion de la ventilation
Production et distribution EC, EF, ECS – qualité de l'eau et de l'air

CONFORT

Terminaux, éclairage et stores

EQUIPEMENTS TECHNIQUES

ALARMES

Fluides médicaux
Mobilité (monte charge, ascenseur…)
Bon de travaux

TRAITEMENT DES DECHETS MEDICAUX

Déchets médicaux : DASRI
Traitement des effluents radioactifs

FROID

Surveillance des enceintes et chambres froides

MANUTENTION

Transport de prélèvement
Produits pharmaceutiques, robots, stockeurs rotatifs, AGV, « tortues »), linges, déchets…

RESSOURCES

Géolocalisation des équipements mobiles
Gestion des ressources salariés (véhicules, clés, casiers..)

SUPPORT

ENERGIE

Comptabilisation et analyse des énergies : air, eau, gaz

PATRIMOINE

Gestion et centralisation de la documentation

MAINTENANCE

Gestion de la maintenance des équipements : inventaire, ordre de travaux, prévisionnel…

SECURITE | SURETE

SURETE

Vidéosurveillance
Contrôle d'accès

SECURITE

Incendie | Remontée d'alerte & centrale incendie

COMMUNICATION

PATIENT

Appel malade

TOUS PUBLIC

Téléphonie pour communication interne et externe

SERVICES D'URGENCE

SAMU, SMUR, centre antipoison…

MOBILITE

INTERIEURE

Monte charge, ascenseurs…
Gestion des accès véhicules : accès parking, reconnaissance immatriculation…
Rechargement de véhicules électriques

EQUIPEMENTS BIOMEDICAUX

DIAGNOSTIC

Equipements de diagnostique IRM, scanner, IoT médical,
Dispositifs médicaux portables et surveillance à distance des patients

3

Trouver les documents de référence

Documentation de référence

Le guide des mesures détaillées de l'ANSSI reste la référence pour retrouver l'ensemble des mesures à mettre en œuvre, y compris dans les hôpitaux. Ces mesures sont classées par grandes catégories métiers.

ANSSI
Mesures détaillées
La cybersécurité pour les systèmes industriels

MESURES DE SECURITE ORGANISATIONNELLES

Connaissance du système industriel	Maitrise des intervenants	Intégration de la cybersécurité dans le cycle de vie du système industriel	Sécurité physique et contrôle d'accès aux locaux	Réaction en cas d'incident
Chaines de responsabilités	Gestion des intervenants	Exigences dans les contrats et cahiers des charges	Accès aux locaux	PRA & PCA
Cartographie	Sensibilisation et formation	Intégration de la cyber en phases de spécification et de conception	Accès aux équipements et câblages	Mode dégradé
Analyse de risque	Gestion des interventions	Audits et tests de cybersécurité		Gestion de crise
Gestion des sauvegardes		Transfert en exploitation		
Gestion de la documentation		Gestion des modifications et évolutions		
		Processus de veille		
		Gestion de l'obsolescence		

Documentation de référence

Les mesures, techniques comme organisationnelles, peuvent être appréhendées de manière pragmatique pour commencer à sécuriser les points les plus vulnérables avant de maitriser l'ensemble des axes d'actions.

MESURES DE SECURITE TECHNIQUES

Authentification des intervenants : contrôle d'accès logique	Sécurisation de l'architecture du système industriel	Sécurisation des équipements	Surveillance du système industriel
Gestion de comptes	Cloisonnement des systèmes industriels	Durcissement des configurations	Accès aux locaux
Gestion de l'authentification	Interconnexion avec l'IT	Gestion des vulnérabilités	Accès aux équipements et câblages
	Accès Internet et interconnexions entre sites distants	Interfaces de connexion	
	Accès distants	Equipements mobiles	
	Systèmes industriels distribués	Sécurité des postes	
	Communications sans fil	Développement sécurisé	
	Sécurité des protocoles		

4

Découvrir les risques métiers, les architectures, les bonnes pratiques associés aux systèmes OT critiques

Focus sur 4 sous-systèmes

4.1

Système de Sécurité Incendie

Risques associés à la gestion du système de sécurité incendie

Prise de contrôle du système du système de sécurité incendie

RISQUES

Indisponibilité du Système Incendie liée à l'arrêt de la centrale technique

Absence de visibilité sur la supervision

Fermeture des issues par déclenchement des portes coupe-feu

Activation du désenfumage et des sirènes, modification des messages transmis par les haut-parleurs ou activation de l'alarme.

Déclenchement des sprinklers déclenchant des dégâts des eaux

QUELQUES IMPACTS METIER

- **Risque de propagation d'un incendie ou de non détection d'un incendie existant**
- **Désorganisation de la prise en charge des patients**
- **Mouvement de panique et atteinte à l'intégrité physique des patients**
- **Déclenchement injustifiée de l'évacuation de l'hôpital**
- **Dégâts des eaux et dommages aux matériels hospitaliers**

Système de Sécurité Incendie : architecture et composants

Supervision qui centralise toutes les alarmes et états des sous-systèmes de GTB et notamment le SSI

SUPERVISION GTC/GTB
Vision globale

Local technique ou bureau

Remontée d'informations d'activités et d'état des fonctions du SSI

BATIMENT A | BATIMENT B | BATIMENT C

Détection
Extinction
SYSTÈME DE SECURITE INCENDIE

Intervenants :
- **ASI – Agent de sécurité Incendie**
- **Mainteneur interne/externe**
- **Intégrateur**
- **Expert système de sécurité incendie interne/externe**
- **Responsable GTB**

Détection
Extinction
SYSTÈME DE SECURITE INCENDIE
Local technique

DIA | Détecteur automatique d'incendie
DM | Déclencheurs manuels



Bouteille de gaz, gicleur, alarme sonore, chemin lumineux, …

Couloirs, chambres, salles…

Capteurs et actionneurs dédiés à la détection d'incendie et à la mise en sécurité des lieux

Prise en main à distance et ordre de commande vers le SSI

Remontée d'alarme du SSI

Poste permettant de visualiser graphiquement et contrôler les informations données par la ou les centrales et de les piloter

UAE | UNITE D'AIDE A L'EXPLOITATION
Pilotage centralisé du ou des SSI

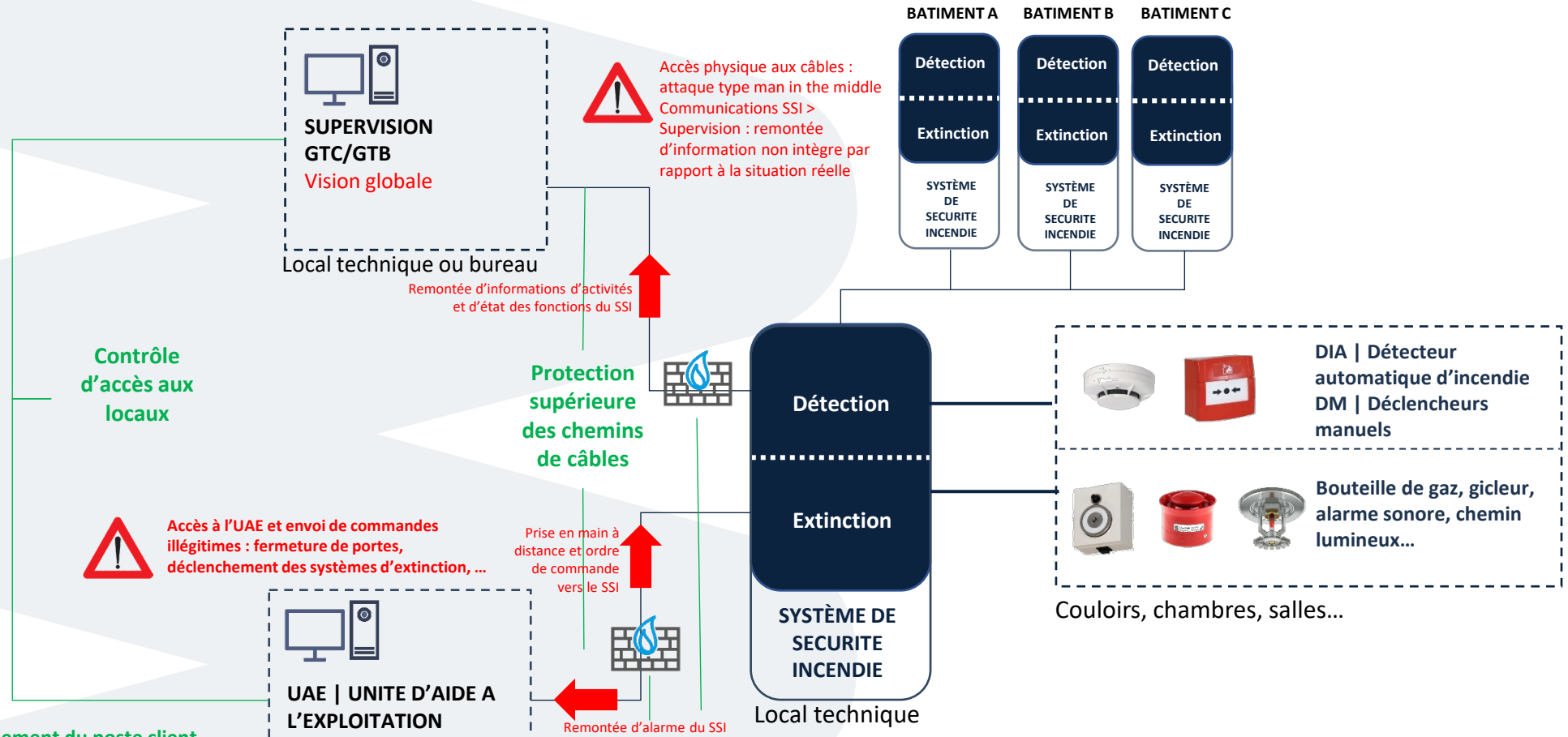
Local sécurisé | VTP

Acquittement alarme
Réarmement des zones
Ouverture clapet désenfumage
Fermeture de l'aspiration

Centrale de contrôle-commande des fonctions de sécurité incendie.

Permet de piloter localement et manuellement la détection/extinction

Système de Sécurité Incendie : mesures de sécurité



Durcissement du poste client ou du serveur :

- logiciel EDR
- anti-virus
- authentification des utilisateurs et gestion des droits (profile, rôle, droit d'accès, …)
- gestion des supports amovibles
- mise à jour des OS et logiciels métier
- sécurisation des accès (scellé de sécurité, câble antivol, …)

Sécurisation des flux de communication :

- Pare-feu avec analyse protocolaire (Modbus…)

Renforcement des mécanismes de sécurité :

- Authentification et intégrité

4.2 Gestion Technique du Bâtiment

Risques associés à la gestion technique du bâtiment (GTB)

Prise de contrôle du système de gestion du bâtiment et modification des paramétrages

RISQUES

Modification de la gestion de la qualité de l'air au sein des services critiques (bloc opératoire, service grands brûlés…)

Blocage des ascenseurs, reprogrammation des **accès physiques**

Modification des différentiels de pressions dans les pièces sensibles de type laboratoires ou salles d'opérations

Coupure ou augmentation du chauffage, dans tous le bâtiment ou juste certaines zones sensibles

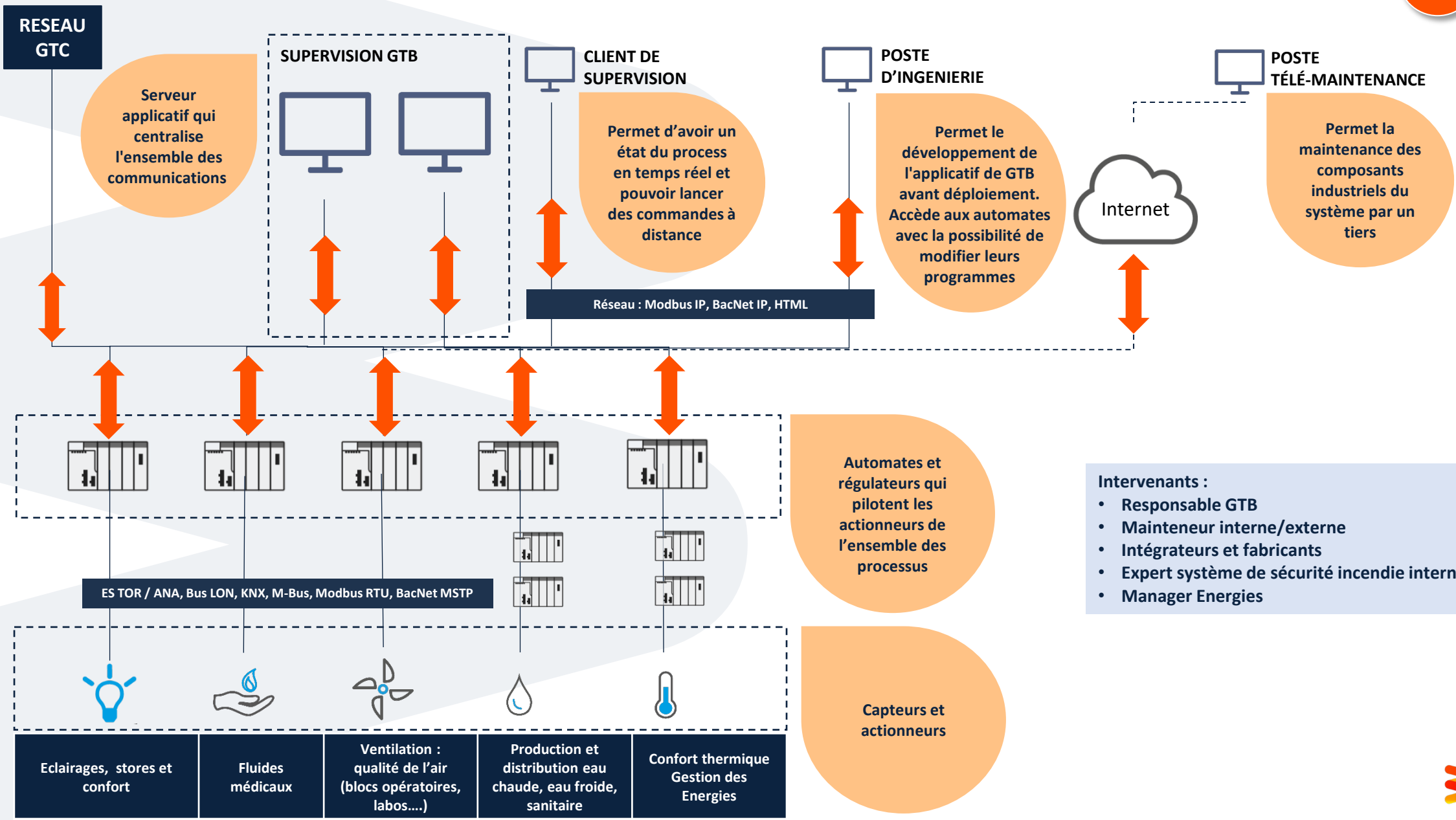
Dégradation de la **traçabilité des chaines du froid pour des s**tockage de prélèvements, Suivi environnement zones sensibles ...

Modification de la gestion de la température de l'eau chaude sanitaire

QUELQUES IMPACTS METIER

- **Propagation de micro-organismes et toxines pathogènes (MOT)**
- **Propagation d'infection ou de bactéries comme les légionelloses**
- **Impossibilité de transférer des patients d'un étage à l'autre**
- **Déclanchement d'un Plan Blanc**

GTB : architecture et composants

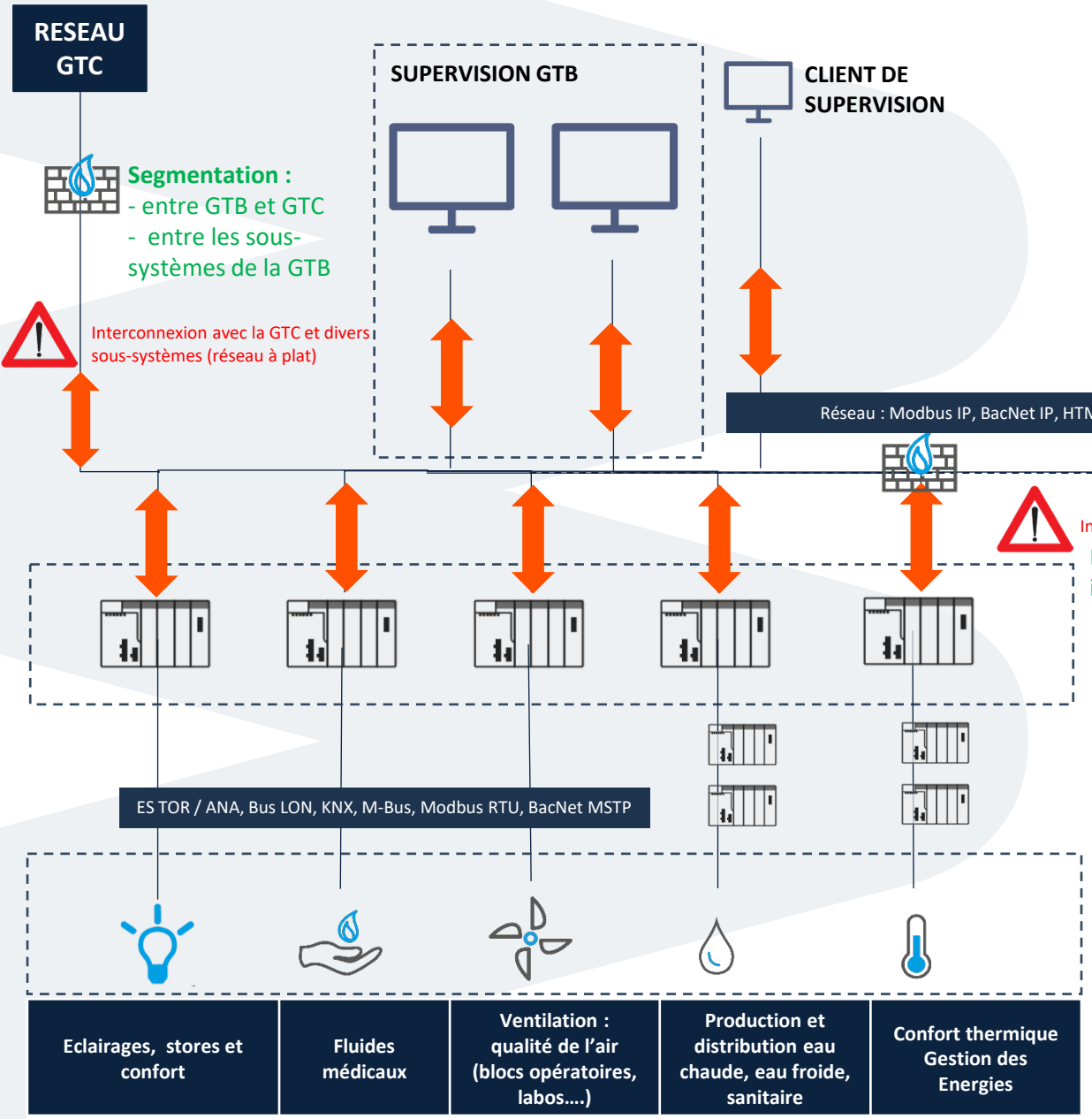


Intervenants :

- Responsable GTB
- Mainteneur interne/externe
- Intégrateurs et fabricants
- Expert système de sécurité incendie interne/externe
- Manager Energies

GIMELEC
Nous décuplons les énergies

GTB : architecture et composants



Droits et privilèges d'accès aux postes de la GTB (Supervision, poste d'ingénierie, poste de maintenance…)

- logiciel EDR
- anti-virus
- authentification des utilisateurs (profile, rôle, …)
- gestion des supports amovibles
- mise à jour des OS et logiciels
- sécurisation des accès (scellé de sécurité, câble antivol, …)

GIMELEC
Nous décuplons les énergies

4.3 Gestion Technique Électrique

Risques associés à la gestion technique de l'électricité (GTE)

Prise de contrôle du système de gestion électrique

RISQUES

Déclenchement d'un incident électrique avec risque incendie

Coupure de courant généralisé, blocage du démarrage des groupes secours

Arrêt de l'éclairage, à part les dispositifs de sorties de secours autonomes

Interruption de la **distribution d'eau** dans les étages

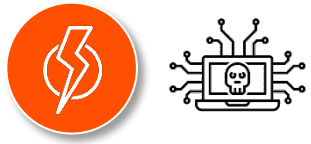
Arrêt des **ascenseurs**

Arrêt de la **distribution des fluides médicaux** et des systèmes de vide

QUELQUES IMPACTS METIER

- **Interruption imprévue des actes chirurgicaux**
- **Evacuation totale de l'hôpital sans ascenseurs, déclenchement du Plan Blanc**
- **Arrêt des systèmes de soins et d'équipements bio médicaux**
- **Mouvements de panique**
- **Pertes de données, arrêt des systèmes informatiques**

GTE : architecture et composants



Intervenants :
- Responsable GTE
- Mainteneur interne/externe
- Intégrateurs et fabricants
- …

Réseau électrique
Réseau de communication

Supervision et contrôle local
Interface Homme-Machine
Serveur Applications
Passerelle vers GTB/TC

ACCÈS TÉLÉ-MAINTENANCE

Réseau technique du site
Switch L3

Moyenne tension (HTA)
Reconfiguration de boucle, délestage

Poste de transformation 1 à X repartis dans les zones et bâtiments de l'hôpital

Poste de livraison connecté au réseau EDF. Redistribue l'alimentation aux postes répartis dans l'hôpital

HSR IEC61850

Poste 1
Automate
Détecteur de défaut

Poste 2
Automate
Détecteur de défaut

Poste de livraison
Automates
Relais de protection (IED)

Groupes électrogènes

Distribution de l'énergie dans le bâtiment prévoit un TGBT. Des disjoncteurs sont connectés pour la surveillance des tableaux. Les automates remontent l'état des disjoncteurs

En secours de l'arrivée EDF. Gestion de la séquence de démarrage des groupes par de l'automatisme.

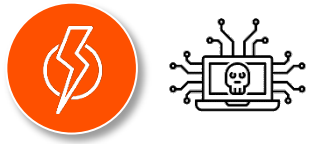
Basse tension

RSTP, IEC61850, MODBUS & ION

Disjoncteur connecté
Automates programmables
Passerelle
Compteurs d'énergie

Disjoncteur connecté
Passerelle
Compteurs d'énergie

GTE : architecture et composants



Intervenants :
- Responsable GTE
- Mainteneur interne/externe
- Intégrateurs et fabricants
- …

Accès à l'IHM et envoi de commandes illégitimes

Durcissement du poste client ou du serveur :
- logiciel EDR
- anti-virus
- authentification des utilisateurs et gestion des droits (profile, rôle, droit d'accès, …)
- gestion des supports amovibles
- mise à jour des OS et logiciels métier
- sécurisation des accès (scellé de sécurité, câble antivol, …)

Supervision et contrôle local

Interface Homme-Machine

Serveur Applications

Passerelle vers GTB/TC

ACCÈS TÉLÉ-MAINTENANCE

Accès télé-maintenance par réseau tiers distant non maitrisé

Chiffrement des flux de communication
Authentification des utilisateurs
Gestion des sessions d'accès distant
Traçabilité des opérations de maintenance

Réseau technique du site

Switch L3

Réseau électrique
Réseau de communication

Moyenne tension (HTA)
Reconfiguration de boucle, délestage

HSR IEC61850

Poste 1
Automate
Détecteur de défaut

Poste 2
Automate
Détecteur de défaut

Poste de livraison
Automates
Relais de protection (IED)

Groupes électrogènes

Pas de segmentation des communications
Segmentation des flux (routage, VLAN, …)
Système de détection d'intrusion

Modification des programmes automates
Sécurisation des flux process
Pas de contrôle de l'intégrité des versions

Contrôle d'intégrité et d'authenticité des firmwares.
Sécurisation des communications à travers une analyse protocolaire
Gestion des autorisations RBAC
Gestion des versions

Basse tension

RSTP, IEC61850, MODBUS & ION

Disjoncteur connecté
Automates programmables
Passerelle
Compteurs d'énergie
Disjoncteur connecté
Passerelle
Compteurs d'énergie

4.4 Dispositifs biomédicaux

Les risques numériques du domaine biomédical

Qu’est-ce qu’un dispositif biomédical ?

- Un dispositif biomédical est un équipement, un instrument, un appareil, un logiciel ou un autre article utilisé seul ou en association, à des fins de prévention, diagnostic, contrôle, traitement et thérapie, maintien des fonctions vitales ou d'analyse. Lorsqu’il est connecté, on parle de dispositif médical connecté (DMC).
- Les objets connectés de santé (OCS) sont des équipements destinés au bien être des patients (montres connectées, balances connectées, T-Shirt de cardiologie, …), il ne s’agit pas de dispositifs biomédicaux mais la frontière peut parfois paraître floue.

Pourquoi sont-ils porteurs de risques ?

- L’utilisation des technologies numériques au sein des dispositifs biomédicaux et l’introduction des objets connectés de santé permettent d’améliorer la qualité du soin et la prise en charge des patients (précision du diagnostic, optimisation du traitement, automatisation de tâches récurrentes, …).
- Mais ces dispositifs ouverts et connectés peuvent contenir des vulnérabilités. Leur introduction dans l’enceinte des hôpitaux, sans l’analyse des risques associés, augmente la surface d’attaque. L’usage de ces dispositifs connectés pourrait être détourné et générer une perte de chance voire le décès d’un patient.

Risques associés à la gestion des équipements biomédicaux

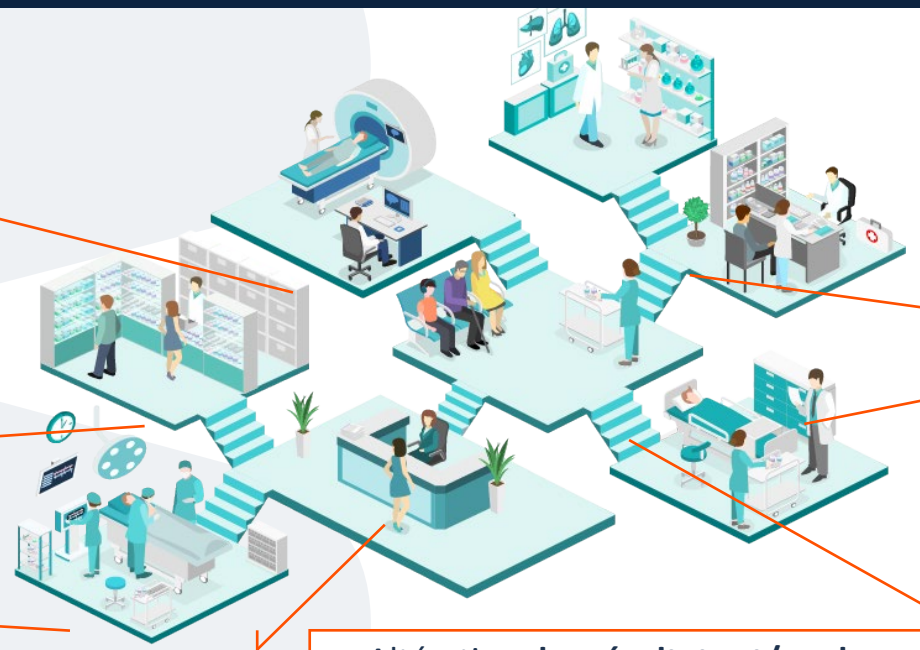
Prise de contrôle des équipements biomédicaux et Dispositifs Médicaux Connectés (DMC)

RISQUES

Altération des paramétrages ou blocage des équipements de diagnostic (rayonnement, modification des unités de mesure…)

Arrêt ou compromission **des automates de pharmacie et de distribution de médicaments**

Arrêt ou prise de main distante des **équipements de chirurgie**



Altération **des résultats et/ou des données d'identification** des patients

Altération des paramétrages des **équipements dans les laboratoires** (extracteurs ADN, ensemenceurs automatiques, métrologie…)

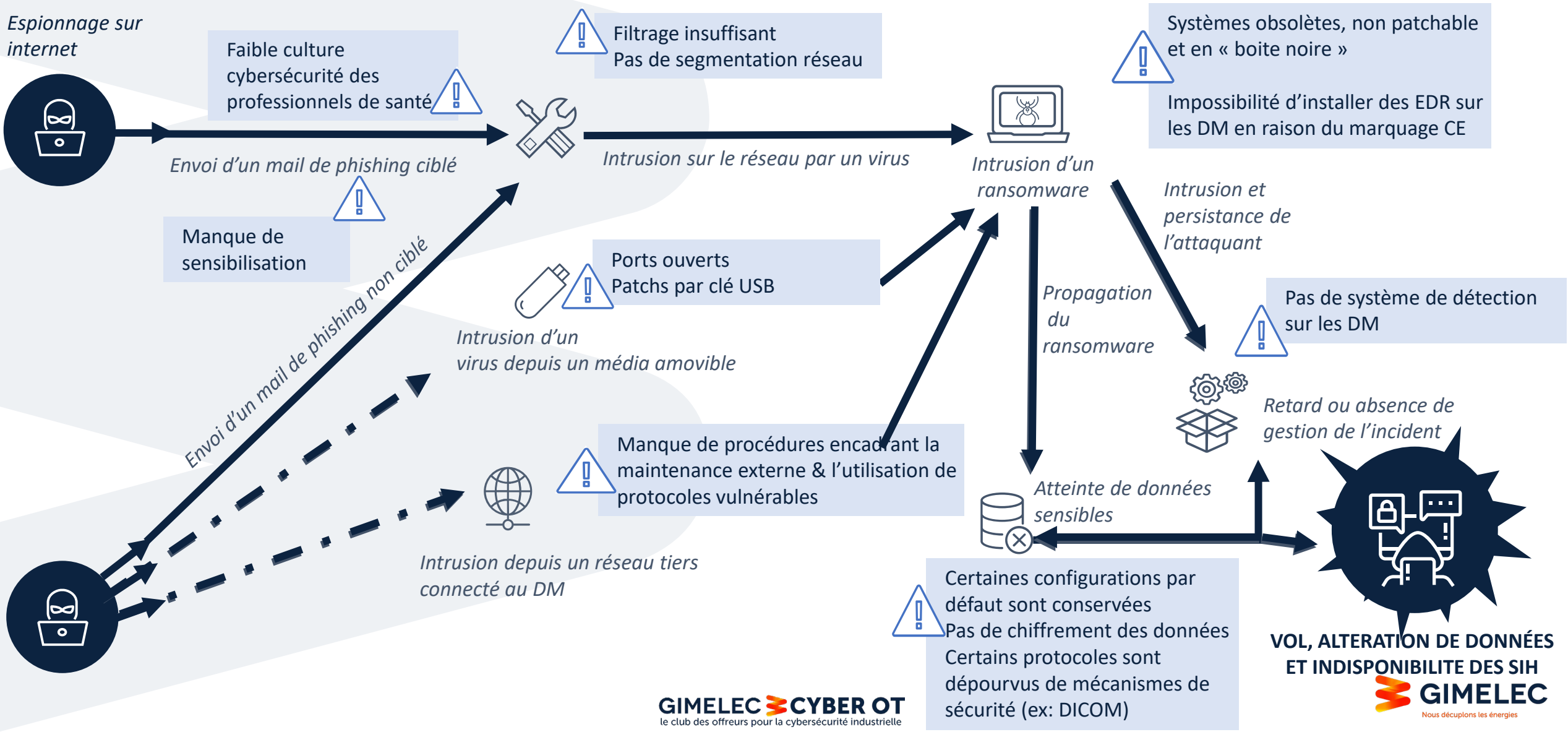
Altération des unités de mesures ou des paramétrages des **dispositif médicaux des services de soins** (pousses-seringues, respirateurs, …)

Accès aux données des équipements biomédicaux

QUELQUES IMPACTS METIER

- **Perte de chance voire décès du patient**
- **Divulgation de données de santé portant atteinte à la vie privée des patients**
- **La désorganisation des établissements de santé conduisant à l'altération de la prise en charge et du soin apporté aux patients**
- **Atteinte à la santé publique dans le cas d'une attaque de grande ampleur**

Schéma d'attaques ciblant des équipements biomédicaux



GIMELEC CYBER OT
le club des offreurs pour la cybersécurité industrielle

GIMELEC
Nous décuplons les énergies

Mesures de sécurité pour la gestion des équipements biomédicaux

Espionnage sur internet

Sensibiliser les professionnels sur les risques liés à leurs usages des SI (mails, dispositifs biomed..)

Mettre en place une segmentation entre différentes zones de confiance avec un filtrage inter VLAN

Envoi d'un mail de phishing ciblé

Intrusion sur le réseau par un virus

Intrusion d'un ransomware

Développer des règles de corrélation spécifiques dans un SOC pour détecter les intrusions

Cartographier des équipements et des flux

Analyser ponctuellement des postes avec un antivirus installé sur clé USB

Intrusion et persistance de l'attaquant

Envoi d'un mail de phishing non ciblé

Fermeture des ports non essentiels opérationnellement ;
Mise en place d'une station blanche pour tester les clés USB

Intrusion d'un virus depuis un média amovible

Propagation du ransomware

Formaliser des fiches réflexes à destination des ingénieurs biomédicaux

Retard ou absence de gestion de l'incident

Faire signer un Plan d'Assurance Sécurité aux fournisseurs ;
Durcir les accès externes via un bastion d'administration.

Intrusion depuis un réseau tiers connecté au DM

Atteinte de données sensibles

Durcir les équipements en lien avec les éditeurs ;
Surveiller l'accès aux données
Sauvegarder les données et les configurations hors réseau.

VOL, ALTERATION DE DONNÉES ET INDISPONIBILITE DES SIH

GIMELEC CYBER OT
le club des offreurs pour la cybersécurité industrielle

GIMELEC
Nous décuplons les énergies

5

Connaitre le top 10 des mauvaises pratiques !

Le top 10 des vulnérabilités et mauvaises pratiques cyber OT

Gouvernance	1 - **Manque de dialogue et de compréhension** entre la DSI et les métiers - pas ou peu d'analyse de risque en commun SI/OT 2 - **Manque de clarté sur l'affectation des budgets** liés à la sécurisation des SITH et des équipements biomédicaux
Architecture	3 – **Manque de cloisonnement et de filtrage** entre les sous systèmes du SITH et les SI critiques pour l'hôpital (Dossier Patient Personnalisé, Centre 15 SAMU…)
Fournisseurs	4 - **Les accès par la télémaintenance sont mal maîtrisés** et ne permettent pas une authentification individuelle et forte 5 – Dans le domaine du bio-médical, **les fournisseurs sont en position de force** et **imposent leurs méthodes** alors qu'ils peuvent manquer de maturité au niveau cybersécurité et la RSSI manque parfois de maîtrise des exigences de sécurité dans la phase d'acquisition 6 - **Peu d'équipements biomédicaux et d'automatismes intègrent historiquement la cybersécurité depuis le design** du produit 7 - **Le marquage CE accentue le problème d'obsolescence des équipements bio-médicaux**, il rend coûteux et chronophage leur mise à jour et ne permet pas de pouvoir installer des solutions de sécurité
Continuité de service	8 - **La cartographie du parc des équipements est rarement disponible** 9 - **Manque de formation du personnel,** qui n'a pas les compétences pour réagir à un incident de cybersécurité 10 - **Manque de moyens de détection et de protection des attaques** ou la difficulté de les intégrer **sur les différentes briques du SITH** rend difficile la gestion des incidents de sécurité

Un collectif d'entreprises complémentaires et spécialisées dans la **Cyber-OT**

Retrouvez nos services et systèmes !

- Sensibilisation du management via la communication des équipes, des autorités et des associations
- Prise de conscience suite à des attaques de concurrents ou partenaires
- Echanges entre équipes IT et OT sur la stratégie cybersécurité
- Rédaction d'un avant projet et d'un cahier des charges pour un premier accompagnement

- Etablir une cartographie initiale du système industriel
- Réaliser un audit organisationnel et technique
- Mener une analyse de risque pour caractériser les ratios Risques / Vulnérabilités
- Faire réaliser des tests d'intrusions sur l'OT
- Réaliser des POC Cyber-OT
- Mettre en place une stratégie cybersécurité industrielle globale et priorisée.
- Planifier son implémentation
- Faire évoluer l'organisation IT/OT sur la gouvernance cyber

- Déployer une campagne de sensibilisation, de formation et de conduite du changement sur les processus IT/OT
- Durcir les systèmes OT :
  - *Mise à jour ou isolement des systèmes obsolètes*
  - *Segmentation réseaux OT*
  - *Sécurisation des accès et des droits utilisateurs*
  - *Gestion et durcissement de tous les périphériques*
  - *Rédaction des procédures*
  - *Gestion des sauvegardes*
  - *Paramétrage sécurité, …*
- Durcir la sécurité physique des sites industriels
- Tests, Commissioning

- Réaliser des Audits réguliers du niveau de sécurité des sites OT
- Veille sur les vulnérabilités et le niveau de menace
- Coordination entre maintenance prédictive et gestion des patchs pour optimiser la disponibilité
- Maintien des cartographies à jour sur les systèmes OT
- Surveillance des installations, planification et remédiation (*Management des logs, analyse du trafic réseau et des données opérationnelles, …*)
- Valorisation des données collectées et de la sécurisation pour optimiser les performances opérationnelles

- Préparation du plan de continuité de l'activité
- Tests de reprise après incidents
- Sécuriser une capacité ponctuelle de réponse à incidents, de gestion et de résolution de crise
- Entretien des canaux avec les partenaires cybersécurité (ANSSI, SOC, CSIRT)
- Supervision des mesures de sécurité

Certification ISO et IEC

Merci !

GIMELEC CYBER OT

le club des offreurs pour la cybersécurité industrielle