Retour d'expérience de l'exercice « Cyber Rage 2017 »

27 janvier – 3 février 2017

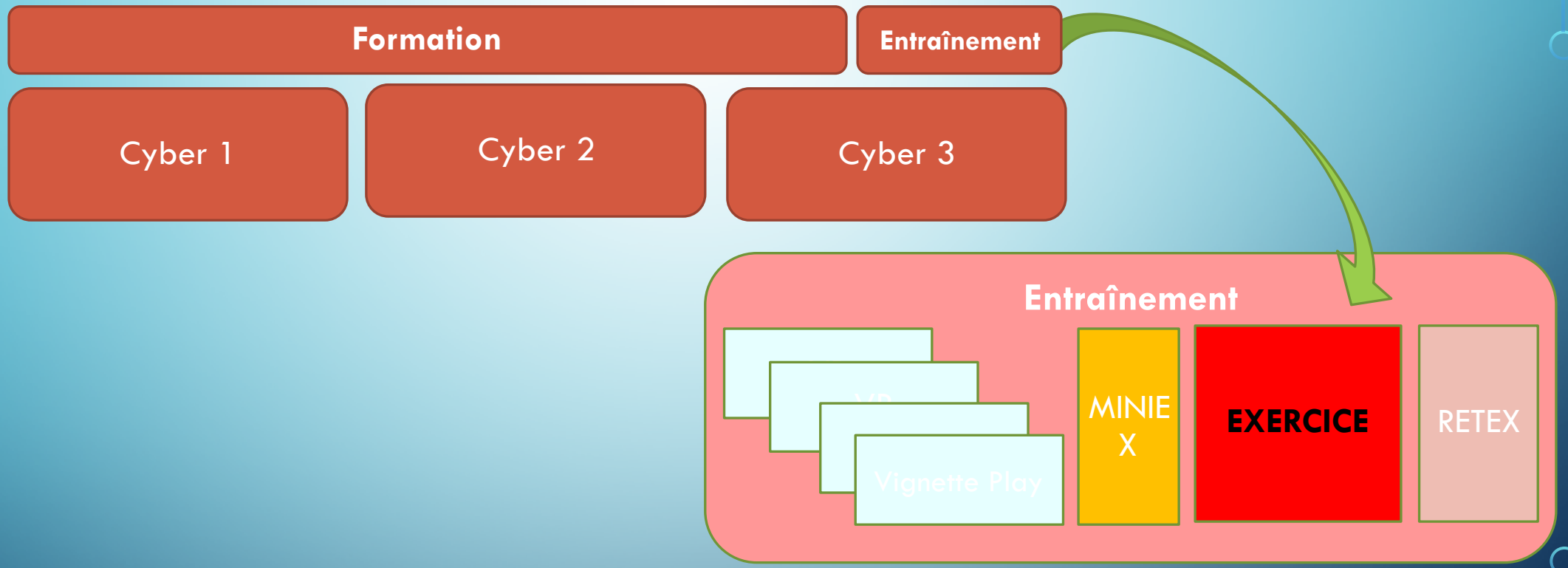
Guillaume CHOUQUET, directeur formation en cyberdéfense
Xavier de PONTBRIAND, directeur d'exercice et responsable de développement

Cyber Rage 2017

SOMMAIRE

1. **L'exercice dans le cursus de la formation cyberdéfense**
2. Le scénario (vidéo)
3. Une construction conjointe
   - Comment avons-nous procédé ?
   - Le référentiel de l'hôpital – la production des joueurs
4. Les bénéfices réciproques
   - Pour le GHBS
   - Pour les apprentis

L'exercice d'entraînement dans le cursus ingénieur



Formation = Compétences théoriques et pratiques sur une discipline (Forensic, sécurité des réseaux…)

Entraînement = Intégration des compétences dans une équipe pour des actions collectives de cyberdéfense dynamique d'un OIV.

3

Scénario opérationnel d'exercice

Le **scénario opérationnel** exprime une attaque du système d'information d'un établissement hospitalier d'importance régionale. La direction de PennOspital est confrontée à des faits redoutés techniques et des incidents d'environnement.

Le **scénario opérationnel** est mis en œuvre par l'animation de l'exercice (Red team, HICON-LOCON, White cell)

La **Cyberdéfense de l'OIV** est assurée par la « Technical blue team » et la « Management blue team »

PennOspital

Cyber Rage 2017

Scénario

UIMM
PÔLE FORMATION
LA FABRIQUE DE L'AVENIR

Cyber Rage 2017

Il était une fois un hôpital…

UIMM
PÔLE FORMATION
LA FABRIQUE DE L'AVENIR


PENNOSPITAL
Nolwenn
Infirmière


DIRECT
Natacha Guegen
L'hopital PennOspital : début de tension

PennOspital

Cyber Rage 2017

Jour 1
Début des attaques

UIMM
PÔLE FORMATION
LA FABRIQUE DE L'AVENIR


RÉPUBLIQUE FRANÇAISE
CARTE NATIONALE D'IDENTITÉ
Nationalité Française
COURVITE
YANN
IDFRGCURVITE<<<<<<<<<<<<<<<<<<<<56MO12
0812560O1235YANN<<<<<<<<<<<<8705305M5

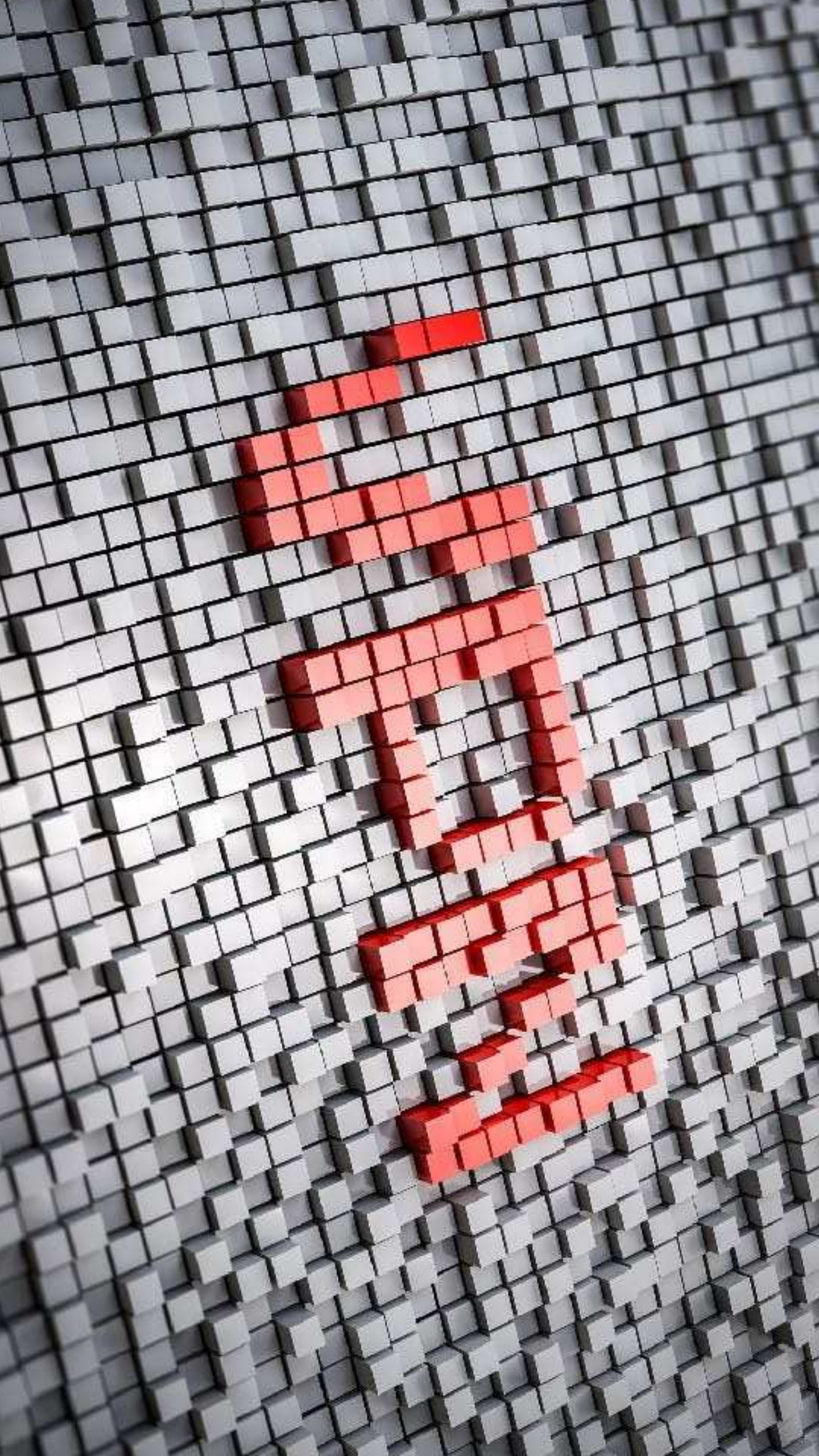

RUE DU STADE
PRÉFECTURE DE VANNES


carte d'assurance maladie
vitale
YANN


hacked-compressor.jpg
www.pennosipital.fr
YOU HAVE BEEN
HACKED !

Cyber Rage 2017

Jour 2
On pousse le curseur



CENTRE HOSPITALIER PENNOSPITAL (CHP)

1 Avenue Emile Jamais
30250 An Orian

01.06.80.91.70
04.66.80.35.10

Certificat médical d'inaptitude à la pratique de l'éducation physique et sportive

(décret n°88-977 du 11 octobre 1988)

Je soussigné, Dr LACROIX, docteur en médecine exerçant au centre médical de Sommières, certifie avoir examiné l'élève :

Jean DUPUIS né(e) le 17/07/1988

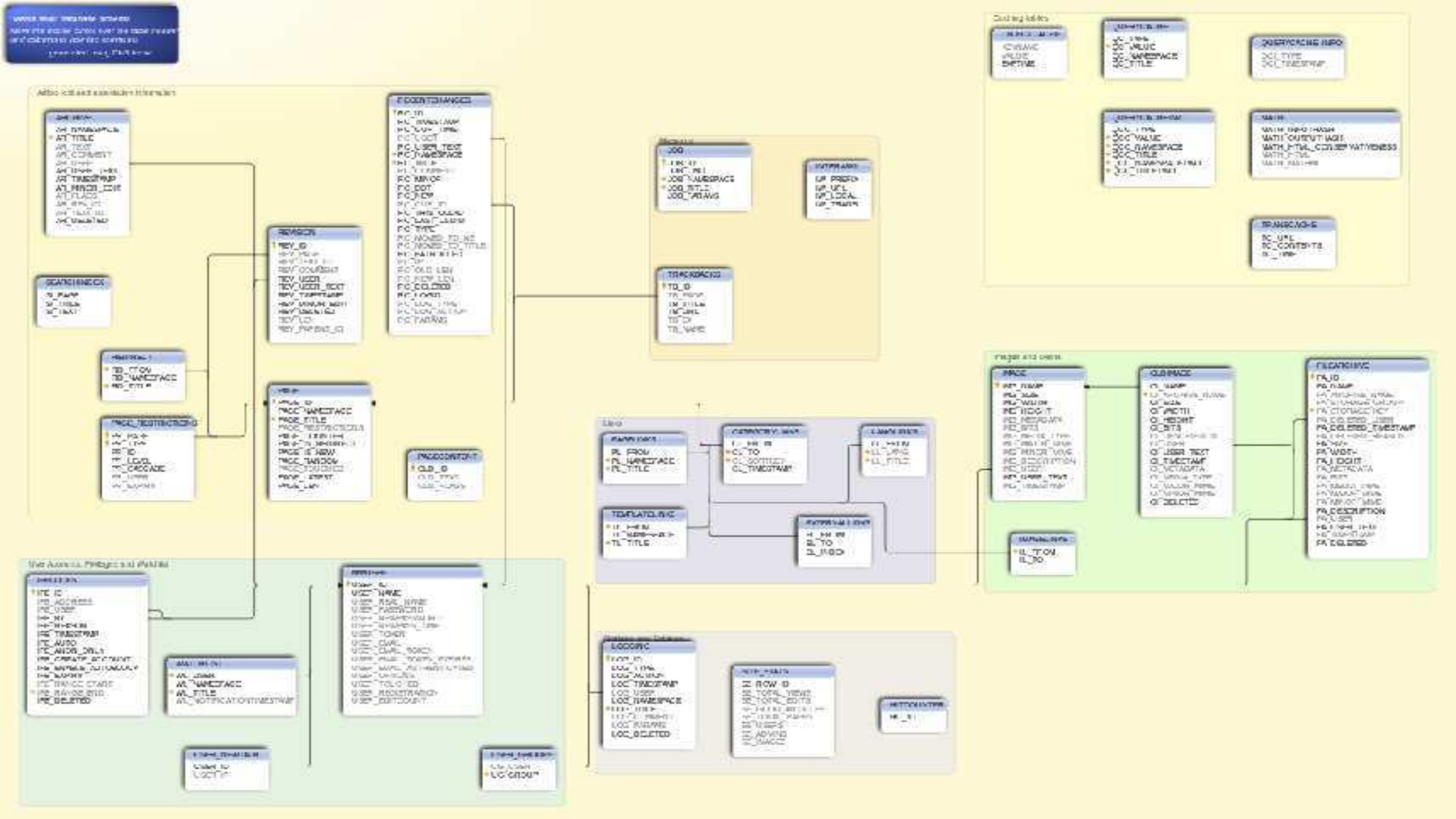
et constaté, ce jour que sa condition physique entraine une inaptitude partielle de la pratique de l'EPS

du 01/01/2016 au 20/06/2016*

Afin d'adapter l'enseignement sportif aux possibilités de l'élève, il peut être utile de considérer les détails suivants :

fracture au niveau du premier métacarpe

22/01/2017, Signature :



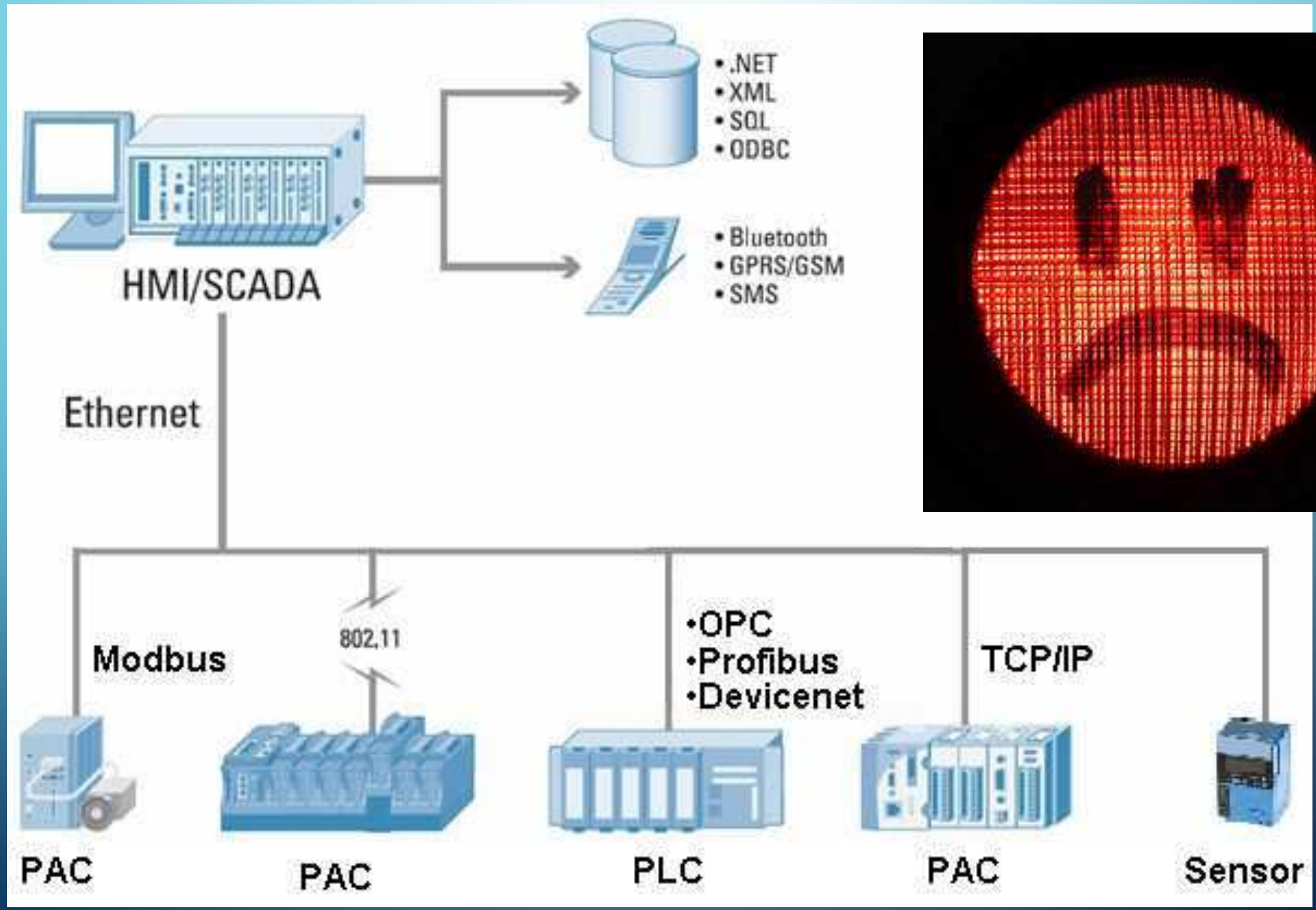
Jour 3
La crise approche


The page cannot be displa
The page you are looking for is curren
unavailable.
The Web site might be experien
difficulties, or you may need
your browser settings.
Cannot find server
Try again

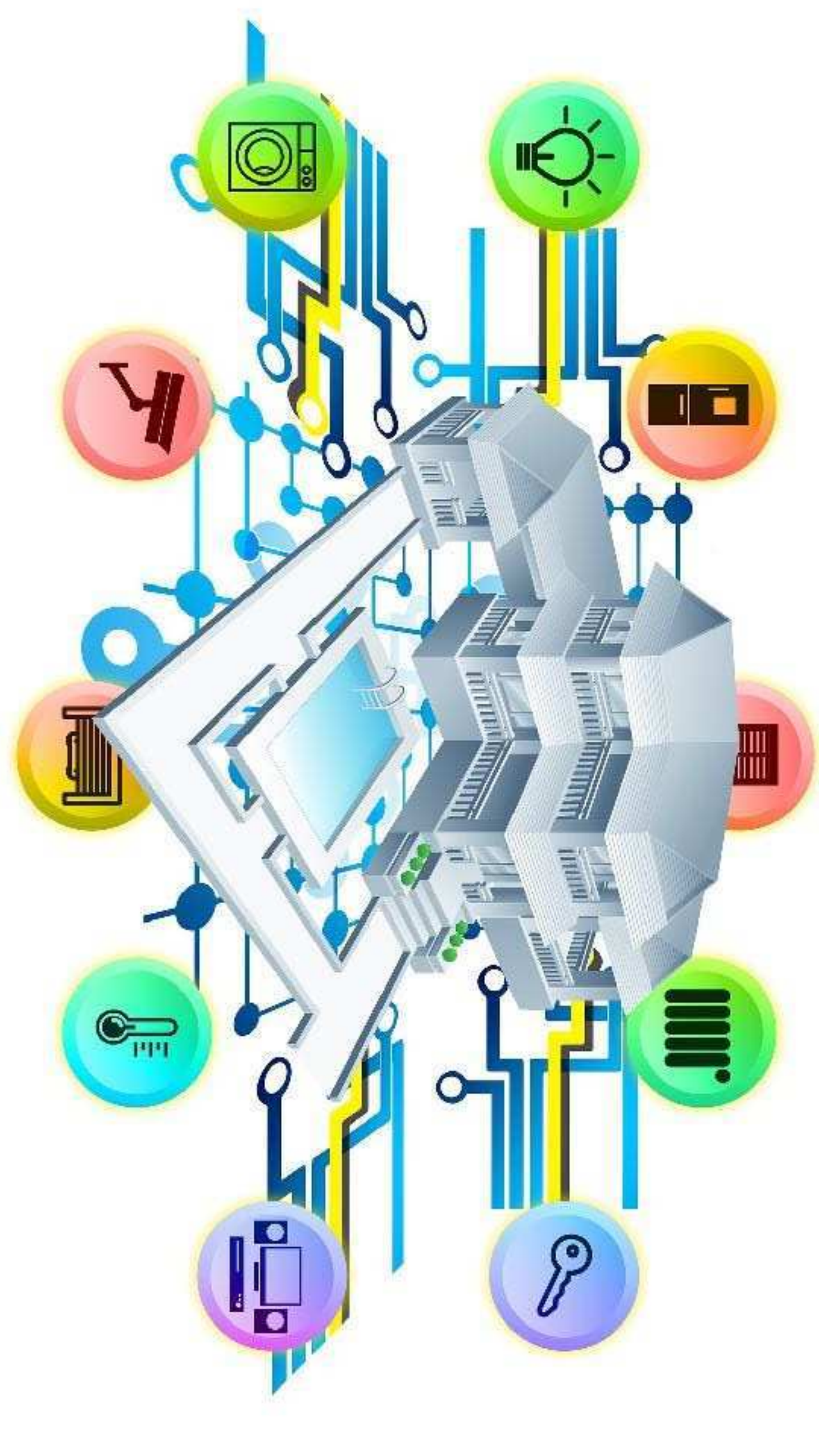

I
PDF

Cyber Rage 2017

Jour 4
Le jeudi noir


•.NET
•XML
•SQL
•ODBC
•Bluetooth
•GPRS/GSM
•SMS
HMI/SCADA
Ethernet
Modbus
802.11
•OPC
•Profibus
•Devicenet
TCP/IP
PAC
PAC
PLC
PAC
Sensor

Cyber Rage 2017




problem
analysis
solution

Cyber Rage 2017

Jour 5
Sortir de crise

SOMMAIRE

1. Le cadre de l'exercice 2017 : un grand centre hospitalier
   - Contexte – le SI du GHBS – intérêt de l'exercice
2. Le scénario (vidéo)
3. **Une construction conjointe**
   - Comment avons-nous procédé ?
   - Le référentiel de l'hôpital – la production des joueurs
4. Les bénéfices réciproques
   - Pour le GHBS
   - Pour les apprentis

Une construction conjointe

Comment avons-nous construit l'exercice ?

- Pourquoi le GHBS ?
- Les échanges : comment avons-nous procédé ?
  - Les faits redoutés et expériences des équipes DSI du GHBS
  - Un fait initiateur
  - Un fait déclencheur : passage de gestion d'incidents à gestion de crise :
    - Pic de crise au bout de 3 jours : imposer un passage en crise
    - Désescalade pour appliquer un PRA.

EXEMPLES D'INCIDENTS CYBER RAGE 2017

GDH	Incident	Réaction attendue	Réaction obtenue	Production éventuelle
Mardi 31 janvier				
Mardi 16h45	Changement des ID patients (666 partout).	Détecter, vérifier, déclencher une sauvegarde. Passage en crise attendu, car danger pour la santé.	Non vu et ignoré jusqu'à ce qu'un patient ne reçoive pas les bons soins. BLUE s'est basé sur la technique et moins sur la mission première de l'hôpital qui est de soigner. Difficulté de mesurer les conséquences des actions menées par RED TEAM.	Pas de CR. Plan de sauvegarde
Mercredi 1er février				
9h	Suppression (drop) des ID (IPP)	Passage en crise (2e motif). Remettre les sauvegardes. Trouver une solution pour constituer les dossiers des nouveaux patients.	Mode dégradé et passage en crise à 14h15, enfin ! L'accueil de l'hôpital a constitué les dossiers des 881 nouveaux patients sous pdf (DIRANI) à 10h45.	Echec dans la conversion des pdf en données patients.
10h	Ransomware	Isoler les postes contaminés + rechercher les sauvegardes.	Aucune. Rémi a joué l'intervenant extérieur sans succès.	Pas de CR. Mail à ALL de ne pas cliquer. MAJ de PCA chiffrement des Postes de Travail.
Jeudi 2 février				
15h	Chiffrement de PC (au lieu de téléphones) et Ransomware	Sauvegardes sur les PC	Refus de paiement de rançon = bonne réaction Mise en œuvre des PCA-PRA = excellente réaction	PRA Ransomware

RÉACTION FACE AUX INCIDENTS

- Incidents → réactions des joueurs
- Un exemple : GTB
- 50 incidents → 50 réponses techniques ou organisationnelles
- Réponse incident GTB : Prévenir le prestataire

Production

PRODUCTION

CONTRIBUTION GHBS

1. Plaquette présentation expurgée
2. Organigramme GHBS anonyme
3. PLAN BLANC PENNOSPITAL
4. PSSI
5. PRA
6. Référencement des Procédures Dégradées
7. Cartographie Fonctionnelle Applicative
8. Charte informatique
9. GHBS activité 2013
10. Eléments chronologiques d'un incident expurgés
11. Fiche incident SI
12. Fiche de signalement d'incident indésirable PENNOSPITAL

LIVRABLES JOUEURS

1. Politique de sécurité
   a. Guide de bonnes pratiques
   b. PSSI (modèle GHBS)
2. Analyse de risque
3. Plan de communication de crise
4. Matrice des flux
5. Passage en gestion de crise
6. Plans de continuité d'activité (PCA)
7. Plans de rétablissement de l'activité (PRA)
8. Plan de défense
9. Plan de sauvegarde

Passage en gestion de crise

Gestion d'incidents et gestion de crise

Un incident, c'est une situation prévisible qui peut être gérée par des procédures (prévues dans un PCA) et éventuellement un Plan de Reprise d'Activité.

Une Crise, c'est une situation dont la maîtrise est rendue difficile, voire impossible, qui demande la mise en œuvre immédiate de procédures et de moyens exceptionnels.

Les PCA sont insuffisants ou inexistants.
Les PRA sont dépassés ou non concernés par la situation.

Passer en crise

1. Critères et classification par niveau de crise
2. Déclenchement (qui, quand, comment)
3. Constitution d'une cellule de crise
4. Convocation de la cellule de crise.

Piloter la crise

1. Suivre les événements par logs
2. Confier (et transférer) le lead de l'action à l'acteur majeur
3. Assurer la coordination entre acteurs
4. Gérer les ressources humaines, techniques, logistiques

Clôturer la crise

1. Discerner les facteurs favorables dans le dernier CR de crise
2. Organiser une réunion de clôture (premier bilan à chaud).
3. Ordonner les actions post-crise et orientations pour bilan à froid.
4. Adresser un message de fin de crise (formaté).

Bénéfices réciproques

GHBS

1. Apport en planification
2. Test de procédures en « temps masqué » sur un SOC d'exercice
3. Regard opérationnel sur la cybersécurité
4. Montée en compétence des collaborateurs
5. Leviers de communication interne et externe

APPRENTIS

1. Réalisme et intérêt pour une gestion de crise :
   - Sensibilité du secteur
   - Faits redoutés tirés sur le vif,
   - Scénario construit ensemble,
   - Participation de la direction de l'hôpital à l'animation
2. Productions préparatoire, en cours d'exercice, et postérieure

Questions ?