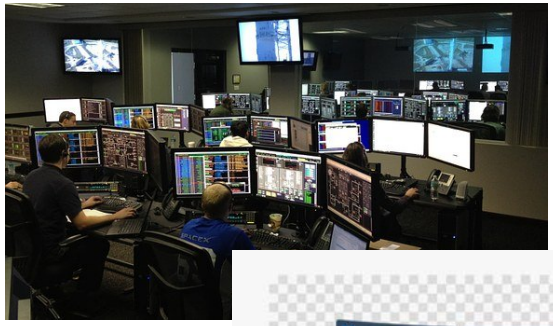
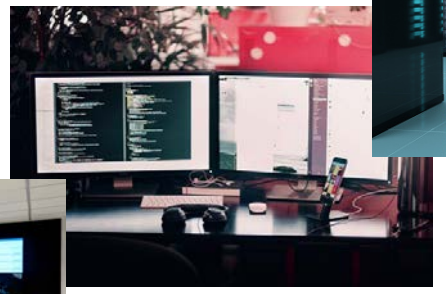
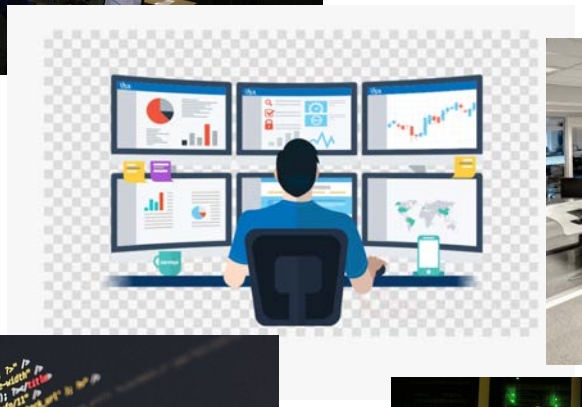
CYBER SECURITY MANAGEMENT

MANAGED SERVICES

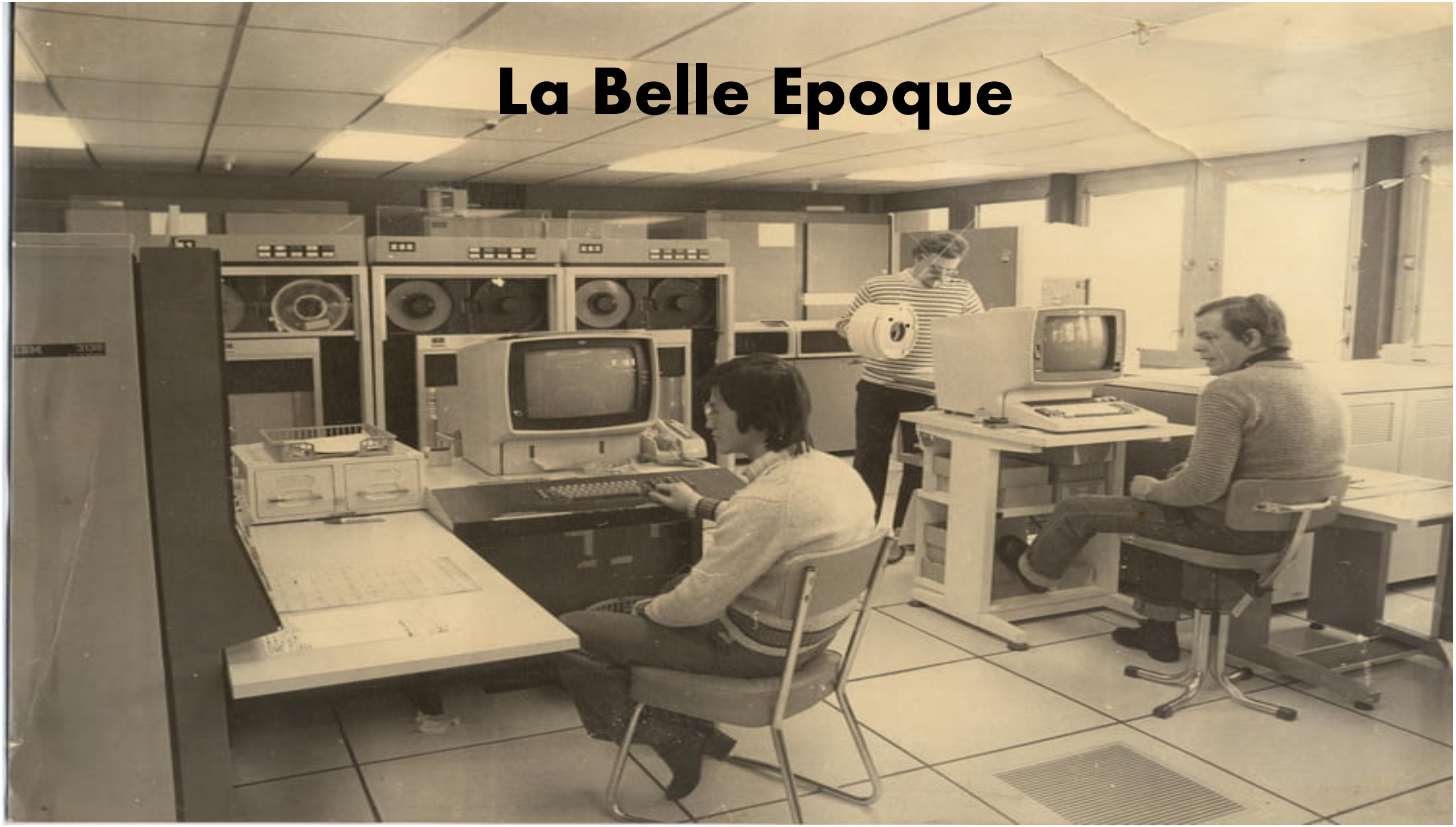


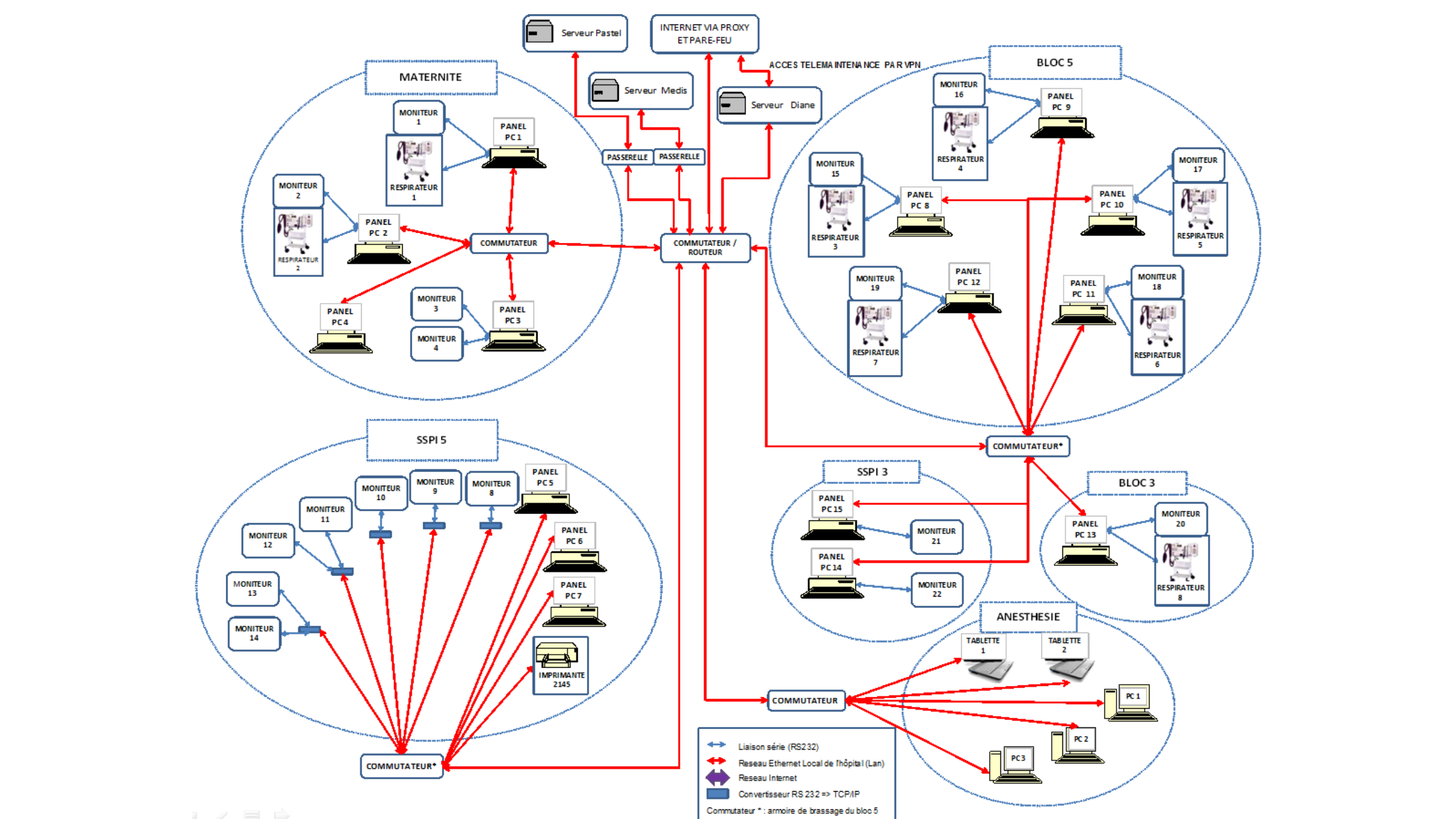




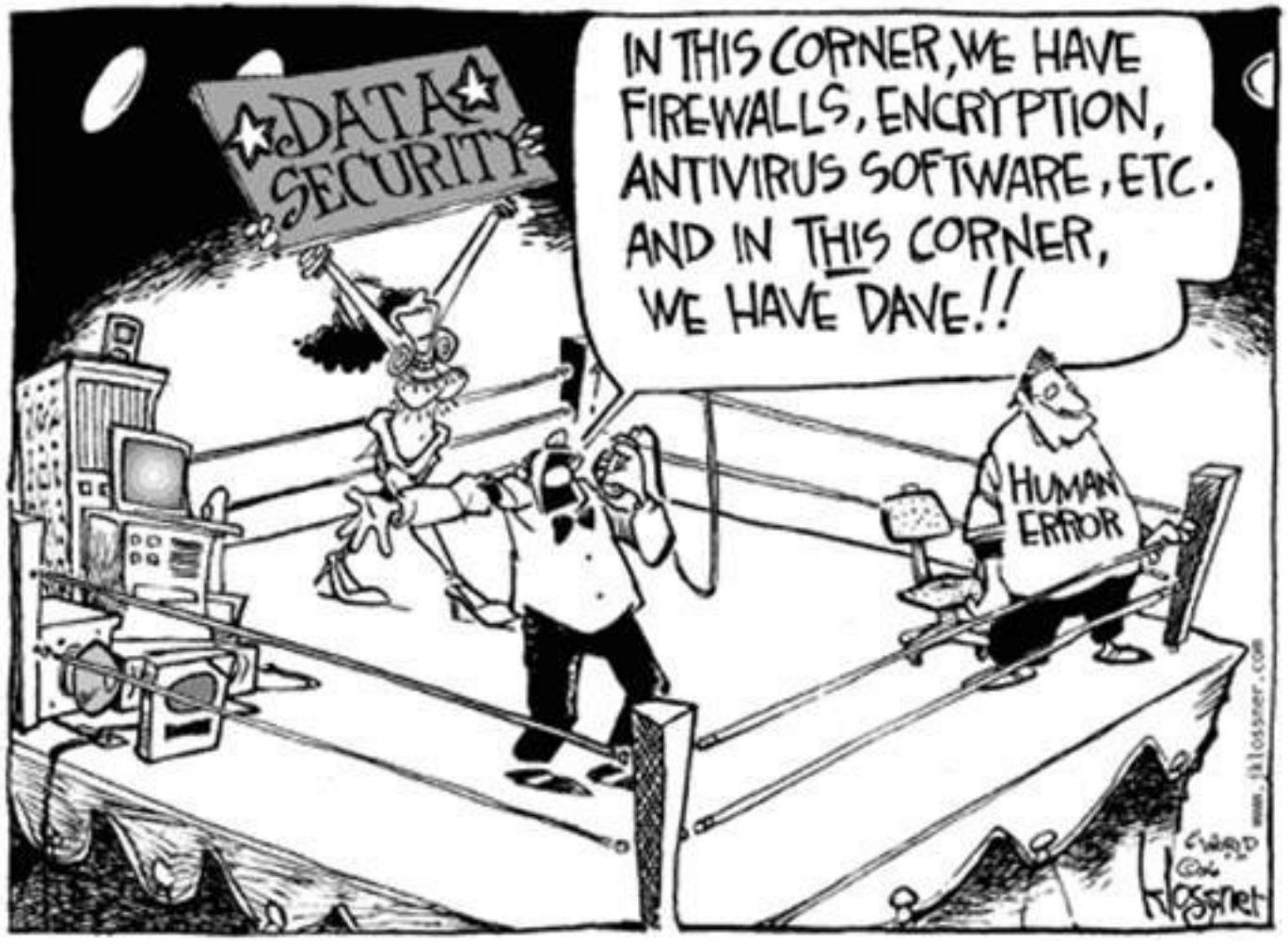

The Centre for Cyber secur
Disconnect
Vision
Faire de la Belgique l'un des pays les moins cybervulnérables d'Europe d'ici fin 2023
CENTRE FOR CYBER SECURITY BELGIUM

La Belle Epoque




Serveur Pastel
INTERNET VIA PROXY ET PARE-FEU
ACCES TELEMAINTENANCE PAR VPN
Serveur Medis
Serveur Diane
PASSERELLE
PASSERELLE
MATERNITE
MONITEUR 1
RESPIRATEUR 1
PANEL PC 1
MONITEUR 2
RESPIRATEUR 2
PANEL PC 2
COMMUTATEUR
PANEL PC 4
MONITEUR 3
MONITEUR 4
PANEL PC 3
COMMUTATEUR / ROUTEUR
BLOC 5
MONITEUR 16
RESPIRATEUR 4
PANEL PC 9
MONITEUR 15
RESPIRATEUR 3
PANEL PC 8
PANEL PC 10
MONITEUR 17
RESPIRATEUR 5
MONITEUR 19
RESPIRATEUR 7
PANEL PC 12
PANEL PC 11
MONITEUR 18
RESPIRATEUR 6
COMMUTATEUR*
SSPI 5
MONITEUR 10
MONITEUR 9
MONITEUR 8
PANEL PC 5
MONITEUR 11
MONITEUR 12
PANEL PC 6
MONITEUR 13
MONITEUR 14
PANEL PC 7
IMPRIMANTE 2145
COMMUTATEUR*
SSPI 3
PANEL PC 15
MONITEUR 21
PANEL PC 14
MONITEUR 22
BLOC 3
PANEL PC 13
MONITEUR 20
RESPIRATEUR 8
ANESTHESIE
TABLETTE 1
TABLETTE 2
COMMUTATEUR
PC 1
PC 2
PC3
Liaison série (RS232)
Reseau Ethernet Local de l'hôpital (Lan)
Reseau Internet
Convertisseur RS 232 => TCP/IP
Commutateur * : armoire de brassage du bloc 5

Quels sont challenges?



#1 - La menace est en augmentation régulière et durable.

Nippon Telegraph & Telephone (NTT) hacked: Japan defense, client & employees data leaked

One of the biggest European banks leaking sensitive data on their website | CyberNews

Hackers str… sovereign wealth fund | CyberNews

t Month as #COVID19

#2- Les ressourc… s et précieuses

Organizations struggle with patching endpoints against critical vulnerabilities

helpnetsecurity.com

Ransomware Attack on Europe's Largest Private Hospital Operator

infosecurity-magazine.com • 2 min read

#3 - Les solutions de sécurité sont complexes et segmentées

#4 - L'augmentation systématique des moyens n'est pas une fin en

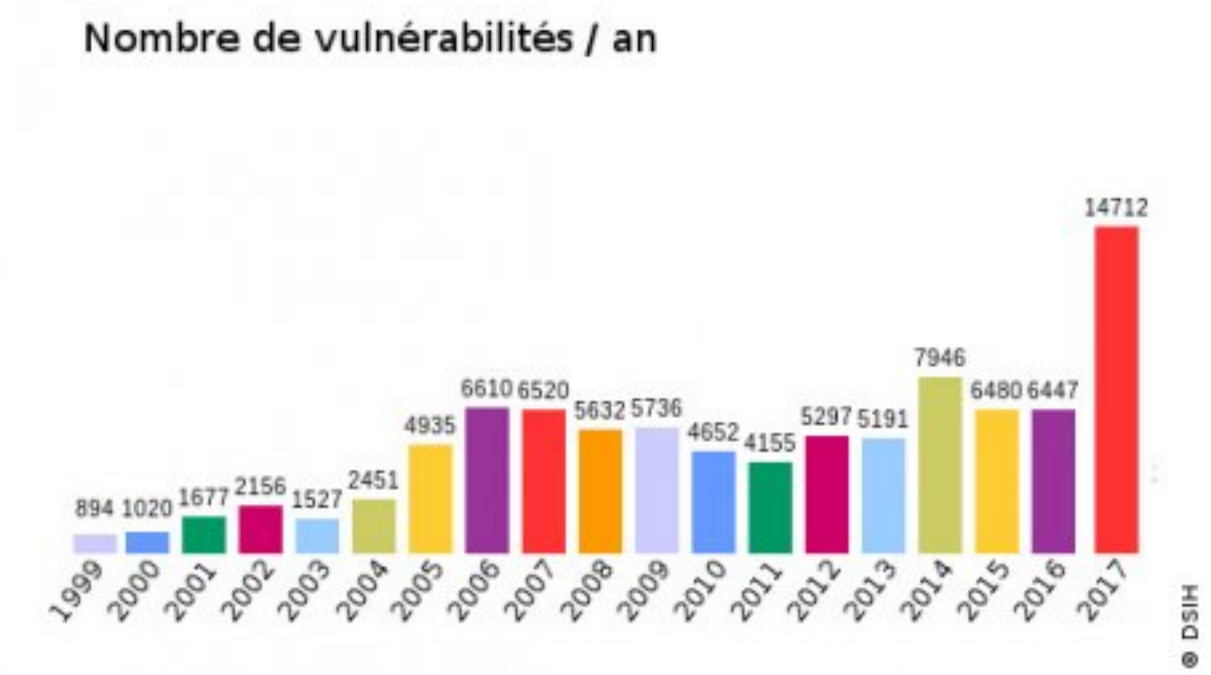
UNE NOUVELLE APPROCHE

Le SECaas ou Sécurité as a service : Définition

Le SECaas, un moyen de mutualiser des ressources trop rares

Quels sont les solutions SECaas appropriées aux menaces?

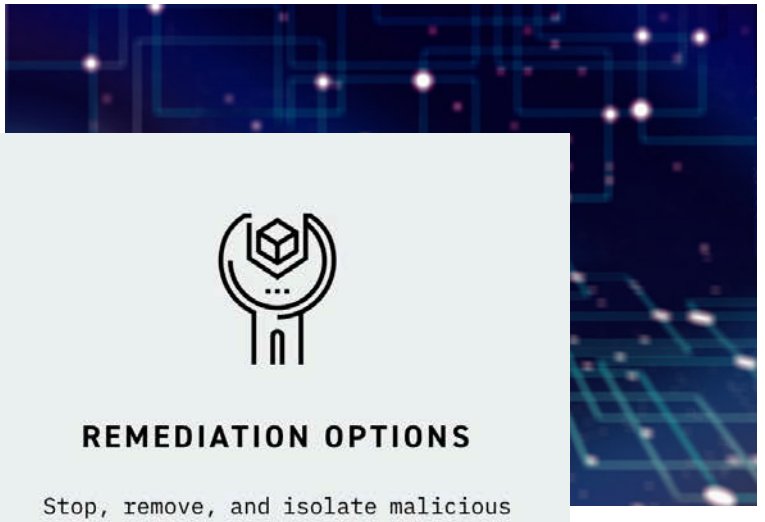
Scan de Vulnérabilités Managé



Je corrige ce qui pourrait impacter mon business en priorité VS je corrige toutes les vulnérabilités dont le score CVSS > 8

EDR Managé

End-Point Detection & Respons



ACTIONABLE THREAT DETECTION

Get actionable, detailed threat detection without the noise.

CUSTOM DETECTION RULES

Build detection rules across platforms for Windows, macOS, and Linux.

REMEDIATION OPTIONS

Stop, remove, and isolate malicious operations with a single click.

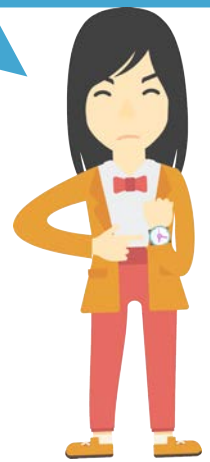
cybereason

EDR as a Service

Temps de propagation et règle du 1-10-60

- Le temps de propagation se décompose en trois éléments qui permettent d'évaluer les moyens de défense de l'entreprise :
  - Le délai nécessaire pour détecter une intrusion ;
  - Le délai nécessaire pour enquêter sur un incident, comprendre la gravité et l'étendue de l'attaque, et définir les contre-mesures requises ;
  - Le délai nécessaire pour réagir à l'intrusion, éliminer l'adversaire et prendre les mesures appropriées pour éviter tout préjudice.
- Un EDR managé de nouvelle génération : Une très grande vélocité qui leur permet de :
  - Détecter une intrusion en moins d'une minute (1),
  - Effectuer une enquête complète en moins de dix minutes (10)
  - Expulser un ennemi du système en moins d'une heure (60).
- Objectif : Agir plus vite que l'adversaire ! La règle du 1-10-60 et le « temps de propagation » constituent deux repères qui mesurent clairement la capacité d'une entreprise à résister à des cybermenaces grandissantes.

Il est temps d'adopter une **approche immunitaire !**
La question n'est plus de savoir si vous allez être attaqués… mais de se préparer à l'être et de disposer des bons outils et experts pour réagir.



Les antivirus classiques, déjà difficiles à gérer, ne détectent plus que **23% des attaques.**

Vos équipes informatiques n'ont **pas le temps** de gérer ces technologies, ni les incidents qu'elles laissent passer !
… encore moins en **24/7** !

cybereason

SOC as a Service

AVANTAGES NOMBREUX

- Simple, agile et accessible à tous
- Sécurité contrôlée et optimisée en continu
- Coûts maîtrisés et économies substantielles
  Accompagnement et proximité d'experts Disponibilité de vos ressources

UN MODÈLE DE *DELIVERY* …

- People, Technologies & Process inside
- = Security Process Outsourcing
- SOCs, MSSPs, Saas

CONCLUSION


USERNAME:: [usa
PASSWORD:: [
PASSWORD:: [
PASSWORD:: [
iStock
by Getty Images

CONCLUSION

- L'approche Security-as-a-Service est aussi un outil de visibilité et de maitrise des coûts. Il est toujours difficile d'évaluer un ROI (Return On Investment) dans le domaine de la cybersécurité.
- Pour atteindre un niveau de sécurité comparable, celles-ci devraient recruter beaucoup plus de personnes (notamment pour travailler en 24/7) ou de se doter d’expertises plus rares.
- Il est facile de démontrer le ROI du service, en s’appuyant sur les KPI et les SLA que doit contenir le contrat.
- L’externalisation est une réponse possible pour optimiser les dépenses Cyber.


IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

QUESTIONS ?