CYBERWEEK 2024

LA CYBERSÉCURITÉ DANS LE SECTEUR HOSPITALIER

16 OCTOBRE 2024

MONS

Agence du Numérique

Cyberwal by digital wallonia

UNESSA

santhea

CYBER SECURITY COALITION.be

Wallonie Relance

Programme

8:30 : Accueil café.
9:00 : Welcome by Agence du Numérique & CSC FG chair.
9:15 : SOC/CSIRT - Maxime Lamarche, Easi.
10:00 : Retour d'expériences - Stéphane Odent, CHU Saint Pierre.
10:45 : Pause-café.
11:00 : Budgets/Fonds/aides disponibles - Ellen Stassart, CCB.
12:00 : Networking Lunch. Animation HackingLab, Cresco.
13:00 : NIS2 Awareness et approche. Panel discussion moderator Sabrina Cristofano. Panelists : Christophe Hohl CSM, Kurt Gielen ZOL, Alexandru Pelin (CISO) Approche NIS2 aux Cliniques Universitaires Saint Luc, Bastien Ducarme CHRSM.
14:00 : OT/IOT PAM par CSM et la Flux OT/IT - Easi.
14 :45 : Pause-café.
15:00 : CRT Regional - Jeremy Grandclaudon, Agence du Numérique.
15:30 : Groupes de travail (30min).
Groupe 1 : NIS 2 resp : CSM Christophe Hohl.
Groupe 2 : Recrutement : resp : AdN + EEcampus.
Groupe 3 : Assets Management : ZOL Kurt Gielen.
17:00 : Networking drink.

Cyberwal
by digital
wallonia

Agence du Numérique

CYBER SECURITY COALITION

Welcome !

Cyberwal by digital wallonia

Maxime Lamarche

Easi

Cyberwal
by digital
wallonia

Beyond a Security Breach

Navigating the recovery post Cyber Incident

easi

Agenda

1. Introduction
2. True cost of a breach
3. Human Impact
4. Operational Disruption
5. Regulatory & Legal Aftermath
6. Rebuilding Trust
7. Financial Recovery
8. Strengthening Security
9. Communication with Stakeholders
10. Recovery Timeline: How long does it take?

01

Introduction

Statistics in Health Care*

Context

35% experienced at least one **ransomware attack** in the past year

90% reported experiencing **phishing attempts**

Average cost of a data breach reached approximately **$10.9 million** in 2023

Only 58% felt fully prepared to meet new **regulatory cybersecurity requirements** introduced in 2023

*

https://www.getastra.com/blog/security-audit/phishing-attack-statistics/
https://www.healthcaredive.com/news/healthcare-data-breach-costs-2024-ibm-ponemon-institute/722958/
https://www.devx.com/news/organizations-feel-unprepared-for-new-cybersecurity-regulations/

Objectives

1. Understand the ***challenges*** and ***complexities***
a business faces **during** and **after** a **cyber incident**

2. Focus on the ***non-technical aspects***

3. Define the ***recovery steps***

02

True cost of a Breach

Costs

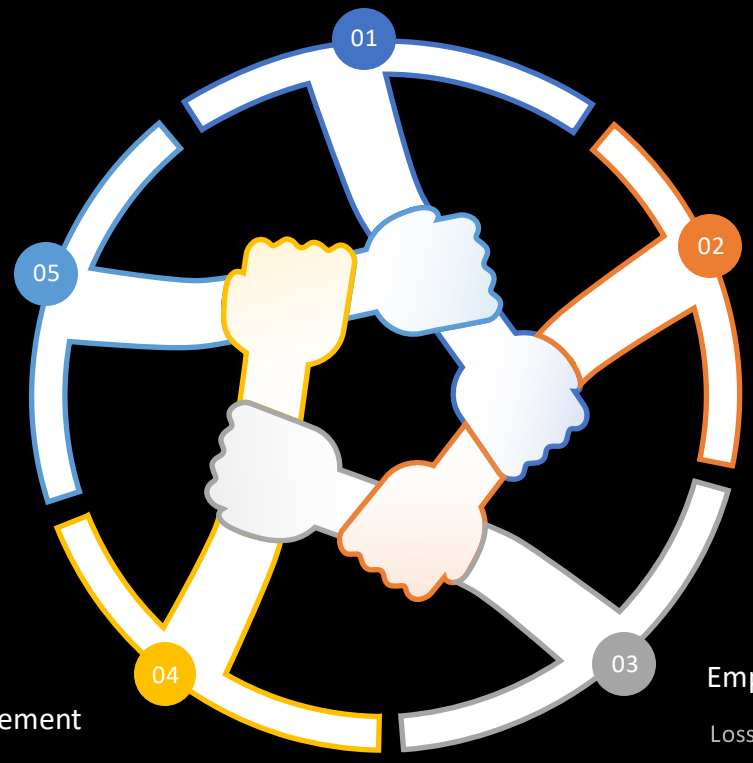

Direct
• Legal Violation (GDPR, NIS 2…)
• Lost revenue during Downtime
• Compensation & Settlements
Indirect
• Customer's Trust/Reputation
• Increased Insurance Premiums
• Future Business Loss
Cyber Incident

03

Human Impact

Employees

Increased Workload/Stress



Employees

Potential Layoffs

Job Insecurity

Employees

Loss of trust

Executive/Management

Credibility's Loss with stakeholders

Executive/Management

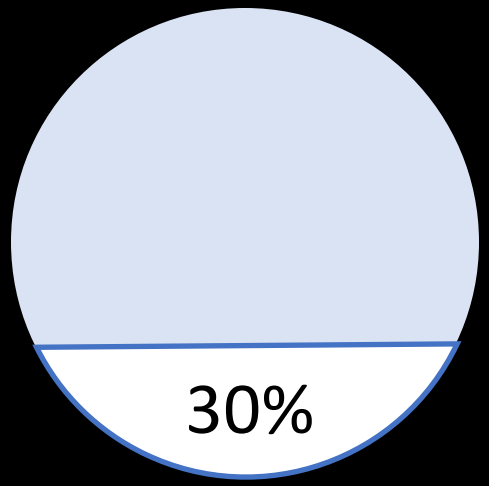
Investor Dissatisfaction

/!\The Need for Mental Health Support -> PTSD /!

04

Operational Disruption

Can we operate in degraded mode?

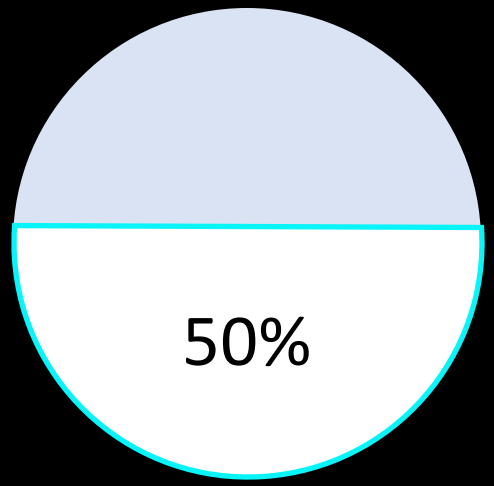


Business Operation

Can be stopped during several hours/days/weeks

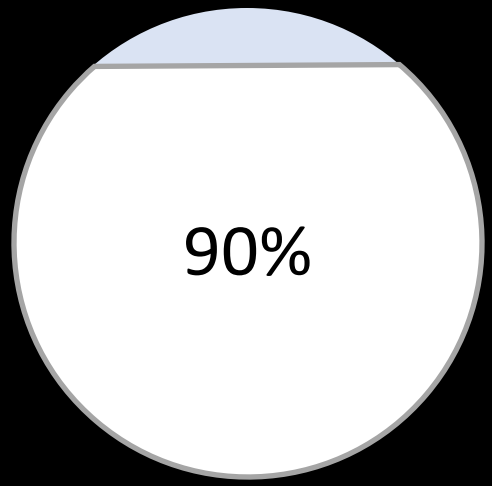
Containment & Eradication

Short-term



Supply Chain

Impact and delays can be encountered

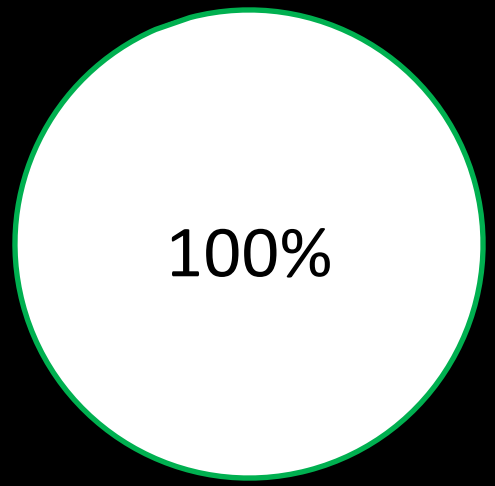


Business as usual

Can be difficult to reach

Full Operational Recovery

Pre-breach Levels



Business more resilient

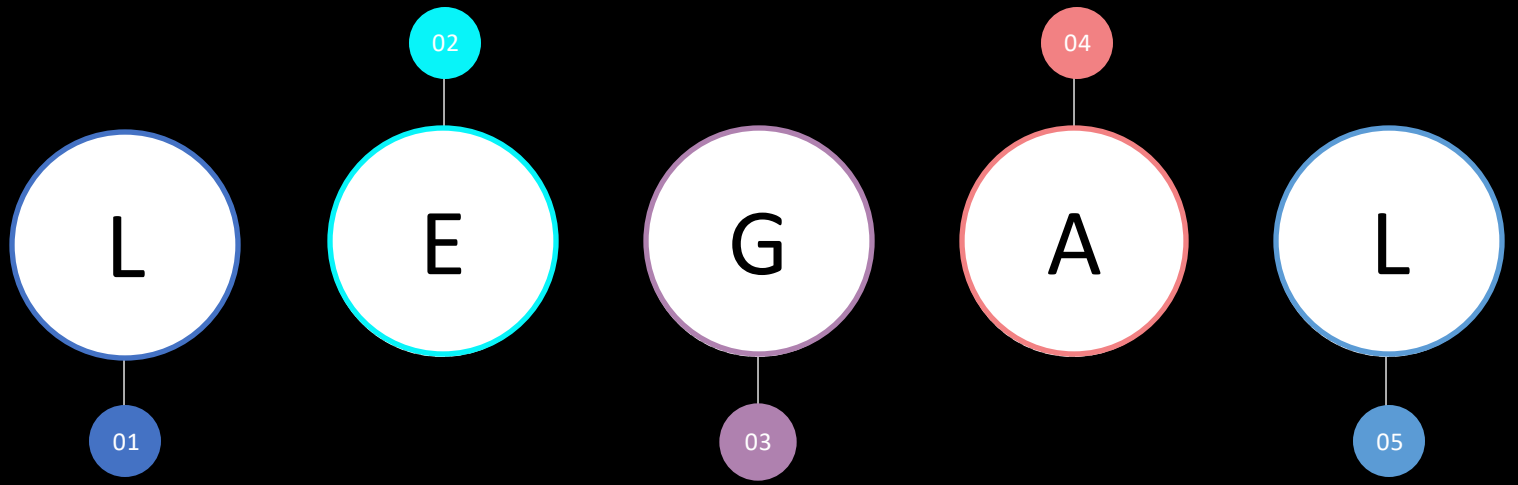
Improved Processes

Long-term Optimization

Strengthen security

05

Regulatory & Legal Aftermath



Investigations

By regulatory bodies

Fines could be given

Audits

Ensure post-breach compliance

Improve/recover reputation

Lawsuits

From affected customers/providers

Costs

Lawyers & Settlements

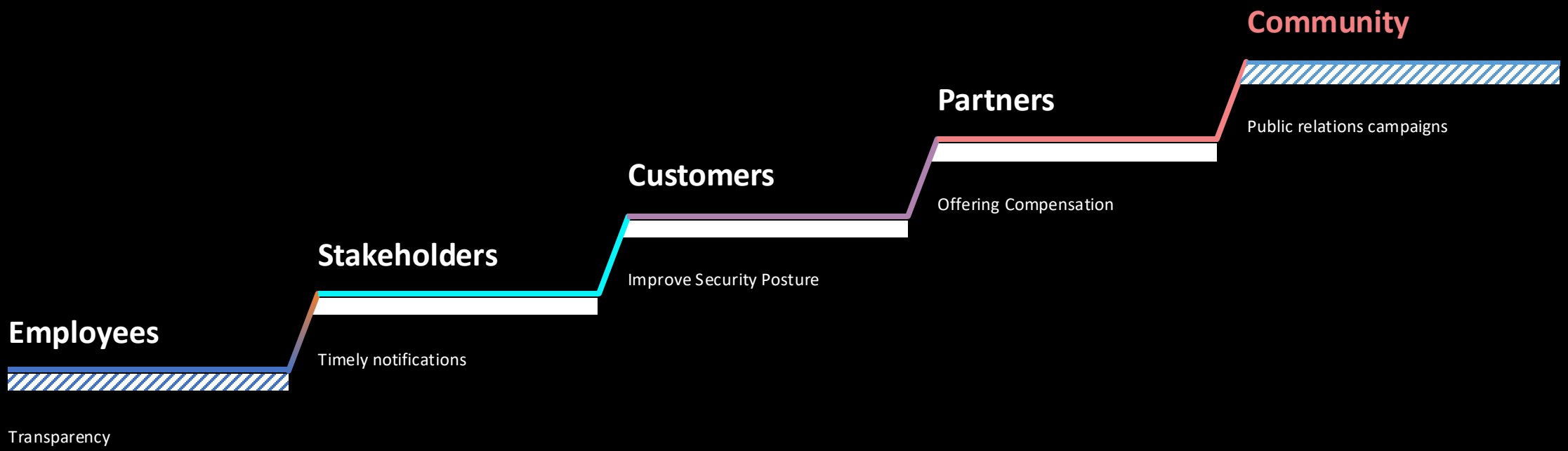
Board Liability

If negligence is proven

/!\Legal team should be involved throughout the incident/!

06

Rebuilding Trust



/!\All these elements are valid for each audience /!

07

Financial Recovery

Costs Estimation

Short-term Vs Long-term Impact

Recovery Budget (IT, Reputation, Legal…)

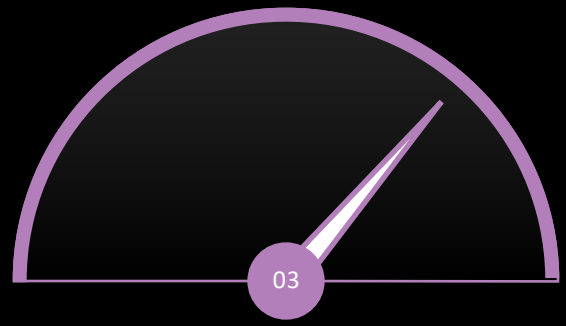
Cyber Insurance

Do you have one?

What does it cover?

Are you still eligible?

Resilience



Allocating budget for:

- Future Incidents
- Post-Incident Recovery

/!\ Security is an investment, not a cost /!

08

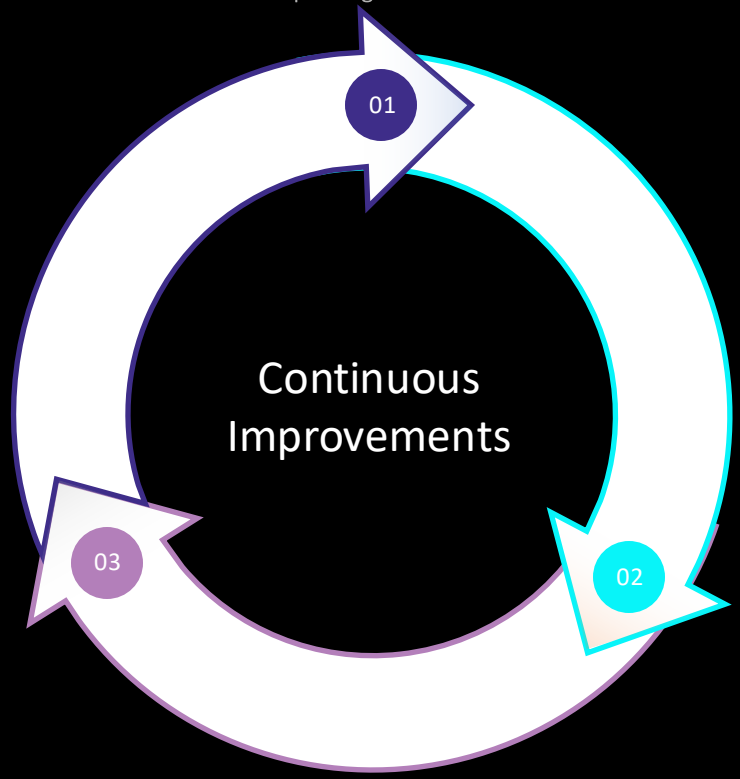
Strengthening Security

Lessons Learned

Root Cause Analysis

Enhancing Cybersecurity measures

Updating Policies



Audits

Governance

Penetration Test

Security Assessments

Investments

Security Operation Center

User Awareness Training

Collaboration with experts

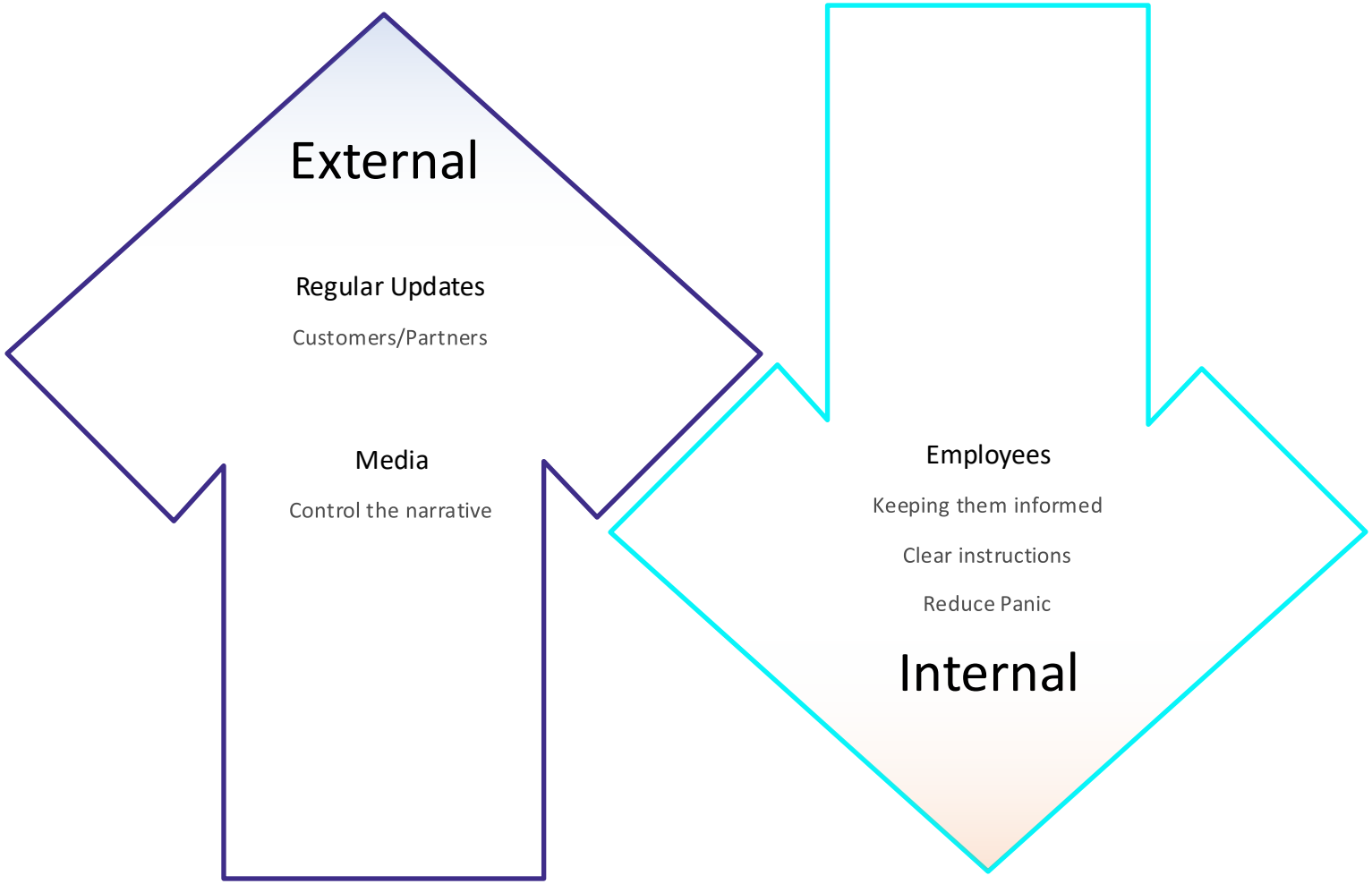
/!\ Security is an ongoing process/!

09

Communication with Stakeholders

Communication Plan

Prepare for the next potential breach



10

Recovery Timeline: How long does it take?

Critical Recovery

A dedicated order should be defined based on the incident date in month

J+1

Short-Term

Internal Structure

Regaining full operational capacity

J+30

Mid-Term

External Assets

- Reputation
- Legal Settlements
- Financial Recalibration

J+120

Long-Term

Strengthening

Security is not a sprint, it is a marathon

J+360

Improvements

Beyond a Security Breach

Navigating the recovery post Cyber Incident

easi

Conclusion

A cybersecurity incident impacted **the whole company**

Successful recovery requires a **long-term, strategic approach**

Your **board** should be **responsible** of it

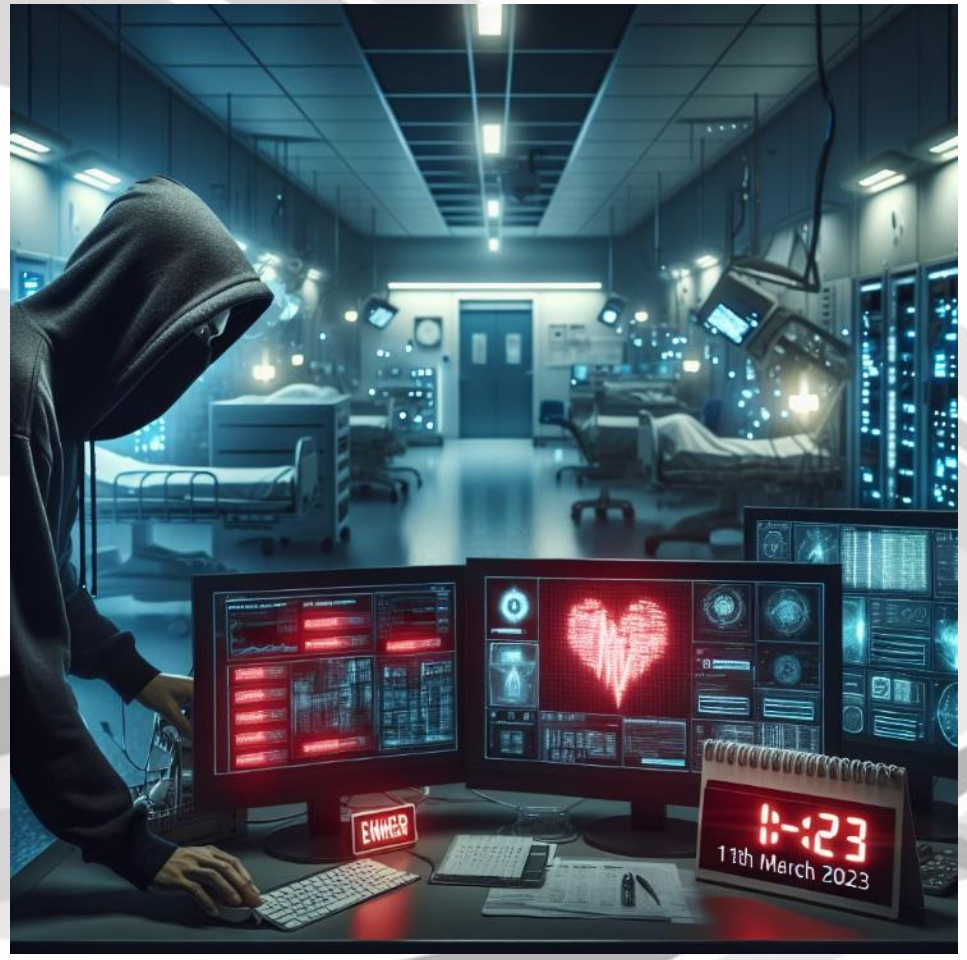
You can never start too early ;)

CHU Saint-Pierre
UMC Sint-Pieter

Stéphane Odent

CHU Saint Pierre

Cyberwal
by digital
wallonia



Source : Copilot

Cyberweek 2024 : la cybersécurité dans le secteur hospitalier
Mons | 16 Octobre 2024

Cyberattaque du 11 mars 2023
Retour d'expérience

Stéphane Odent | CIO

Respect | Innovation | Engagement | Solidarité | Qualité

Présentation

Stéphane Odent

Je suis…

- CIO au CHU Saint-Pierre depuis septembre 2020
- citoyen belge, Bruxellois, né Wallon, de parents Flamands
- ingénieur civil diplômé de l'Ecole Royale Militaire
- informaticien diplômé de la VUB
- ex-militaire officier
- manager
- directeur
- collègue
- entrepreneur
- homme
- papa
- fils
- mari
- sportif
- voyageur
- cuisinier
- photographe
- patient
- …

Officier | Manager/Directeur IT | Consultant | Directeur IT

1990 1998 2015 2020

Le CHU Saint-Pierre C’est…

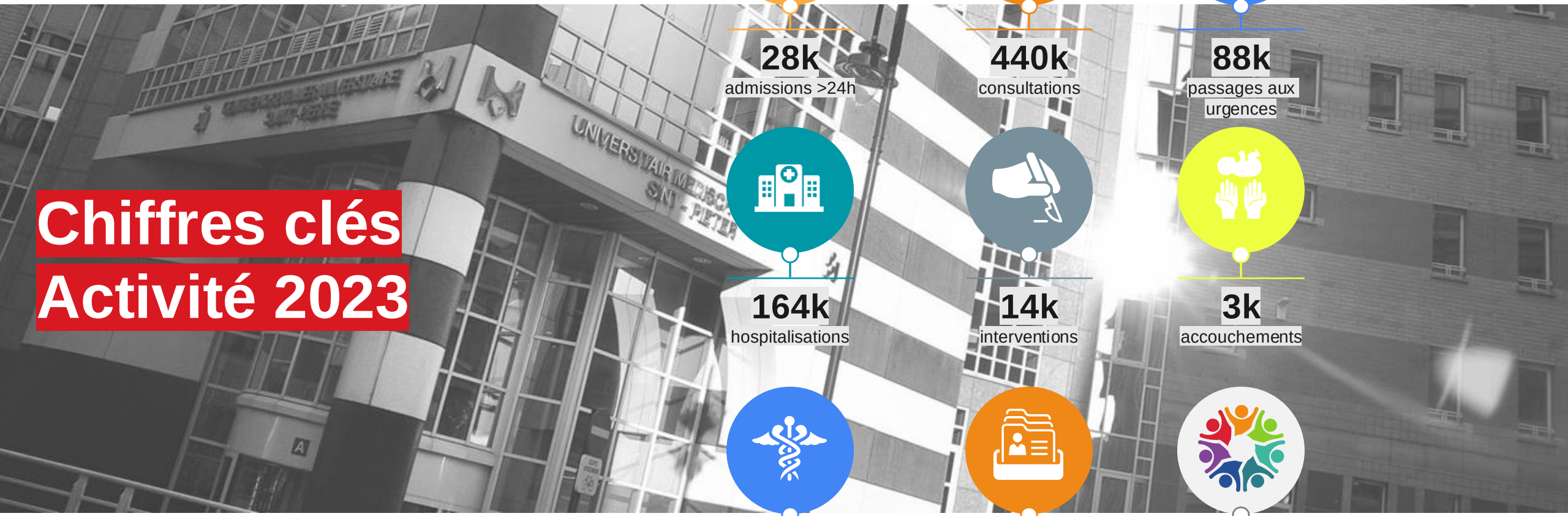
Un hospital public Au coeur de Bruxelles

300
millions €

587
Lits agrées
2 sites

2,500
Collaborateurs

Chiffres clés Activité 2023



28k
admissions >24h

440k
consultations

88k
passages aux urgences

164k
hospitalisations

14k
interventions

3k
accouchements

40
services médicaux

120
métiers

> 80
nationalités & origines

Etat des lieux de la cybersécurité

Contexte

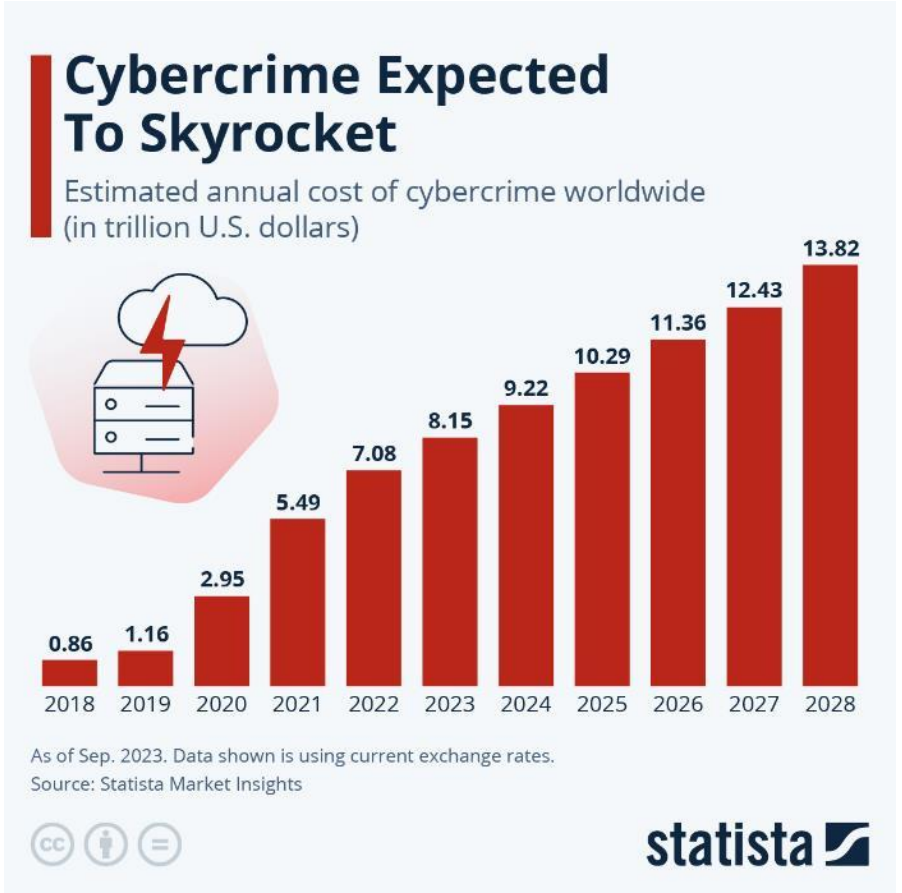
- Evolution de la menace (social engineering, BEC/Business Email Compromise)
- Situation géopolitique
- Digitalisation et connectivité
- IOMT
- Intelligence Artificielle
- Pénurie de personnel
- Contraintes budgétaires

DEFENCE
Cyber Command
19/10/2022

Quelques dates

- 2004 ENISA (agence européenne de cybersécurité) a 20 ans
- 2014 CCB (centre de cybersécurité belge) a 10 ans
- 2016 NIS1 -> be 2019
- **2022 NIS2 -> be loi 26/04/2024, AR 9/06/2024, entrée en vigueur le 18/10/2024**
- 2022 CER (Critical Entities Resilience directive)

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY 20 years!



Malgré les mesures prises depuis 20 ans, la menace continue d'augmenter.
Ça ne va pas s'arrêter ni diminuer…

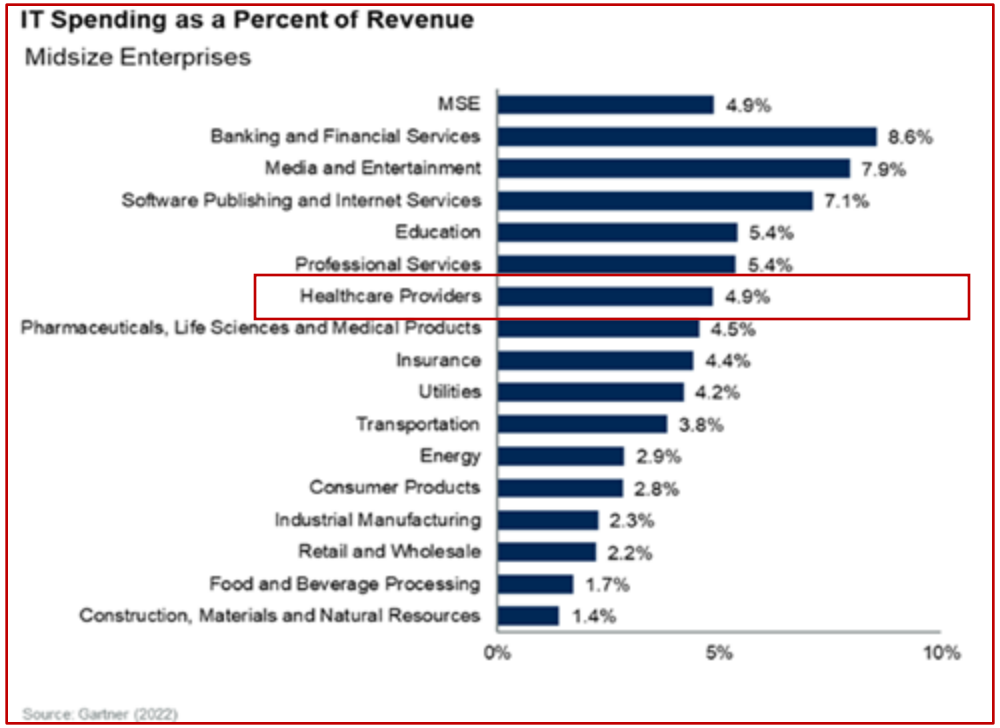
Exemple : lundi 7 octobre 2024

Ces attaques, revendiquées et annoncées à l'avance par un **groupe d'hacktivistes pro-russes**, s'inscrivent dans une campagne plus large ciblant des entités européennes et liées à l'OTAN.
Les cibles privilégiées incluent les agences gouvernementales, les médias et les entreprises privées.

Maturité de la cybersecurité?

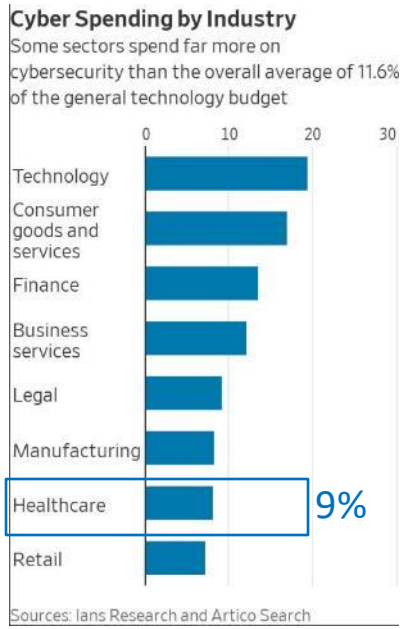
Et vous?

Budget IT = ~5% du chiffre d'affaires

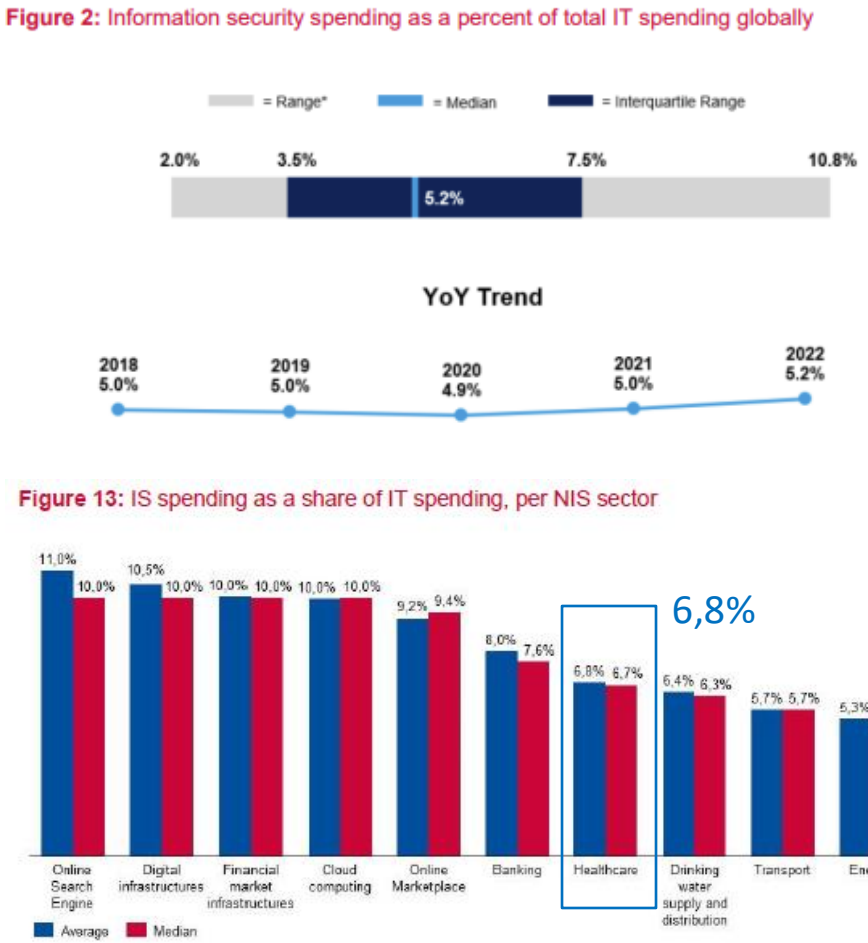


IT/CA 5%

Budget cybersécurité = ~7-20% du budget IT



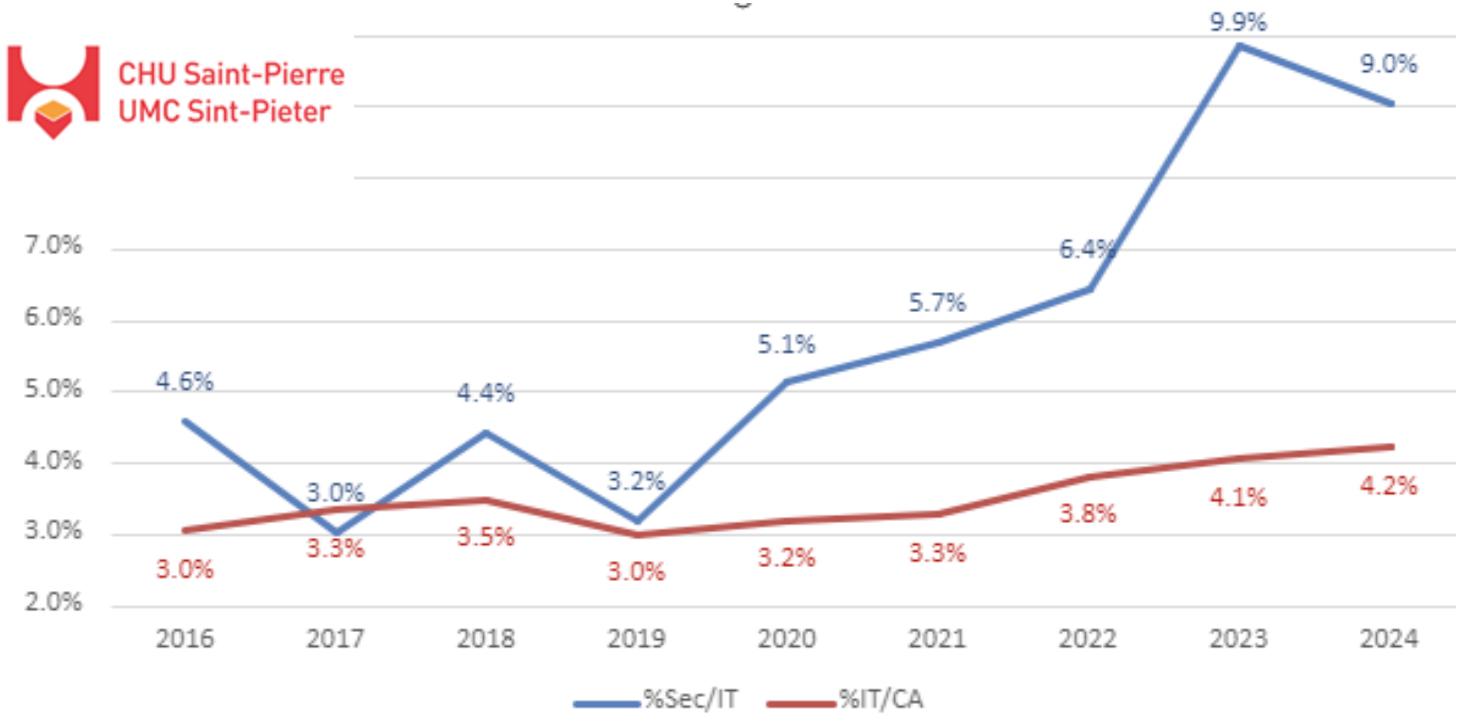
Cyber/IT 7-20%



Source: ENISA NIS Investments November 2023

Evolution au CHU Saint-Pierre

Le **budget IT** du CHU Saint-Pierre a quasi **doublé en 5 ans**
Le **budget cybersécurité** a été **quintuplé en 5 ans**



Cyber/IT
7-20%

Benchmarks

IT/CA
5%

Financement fédéral de la cybersécurité en 2022: **€20 millions** = ~30% du budget cybersécurité
2024: **€15 millions**, dont €12 millions pour les hôpitaux, €2,25 millions « collectif » et €750.000 « contributeur »
<10% du budget cybersécurité

SHIELD vzw

Analyse SWOT de la cybersecurité au CHU Saint-Pierre

FORCES

- IT infrastructure team
- Bonne gestion du réseau et des systèmes
- Réplication de data center
- Roadmap cybersécurité depuis 2020
- Email dans le cloud

FAIBLESSES

- Les utilisateurs
- Hôpitaux belges pas désignés OSE (Opérateurs de Services Essentiels) – loi NIS1
- Niveau de maturité faible
- Obsolescence des systèmes
- Gestion des identités et des accès
- Moyens limités

OPPORTUNITES

- Sensibilisation et financement SPF Santé
- Normes Minimales (NMN)
- NIS 2 (18/10/2024)
- Cyberfundamentals Framework CCB
- Collaborations
- IA

MENACES

- Complexité de notre environnement IT
- Fournisseurs
- Télétravail
- Augmentation de la cybercriminalité
- Risques liés aux conséquences d'une cyberattaque
- Difficulté du recrutement/pénurie de personnel IT
- IOMT
- IA

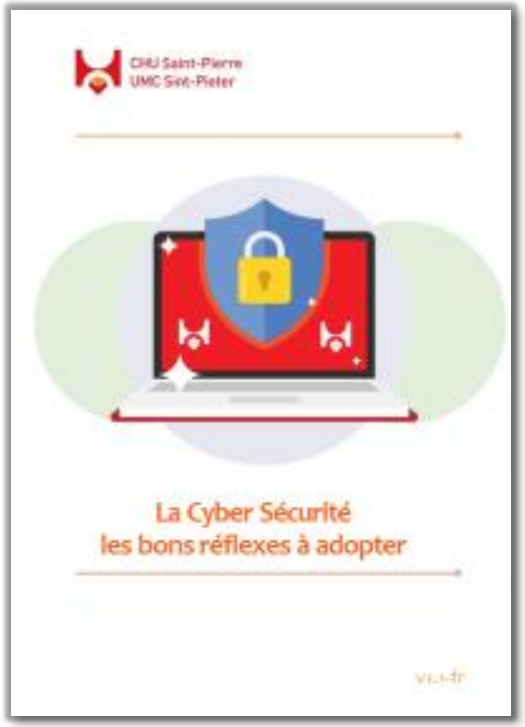
Utilisateur = maillon faible

Chaque utilisateur est une cible pour les cybercriminels!

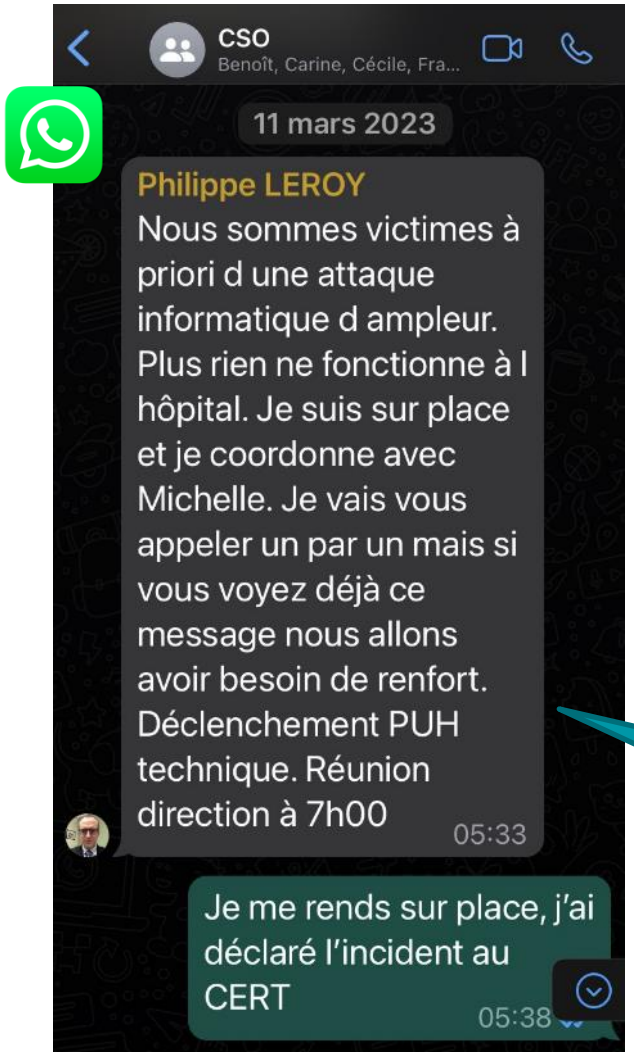
Chaque utilisateur est la première ligne de défense!

Test de phishing => **>60%** ont cliqué sur le lien
Cas rapporté de **fraude par « BEC »** (Business Email Compromise)

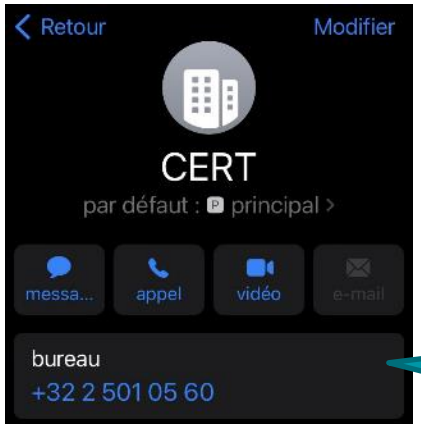
Importance de la sensibilisation



Cyberattack incident & crisis management



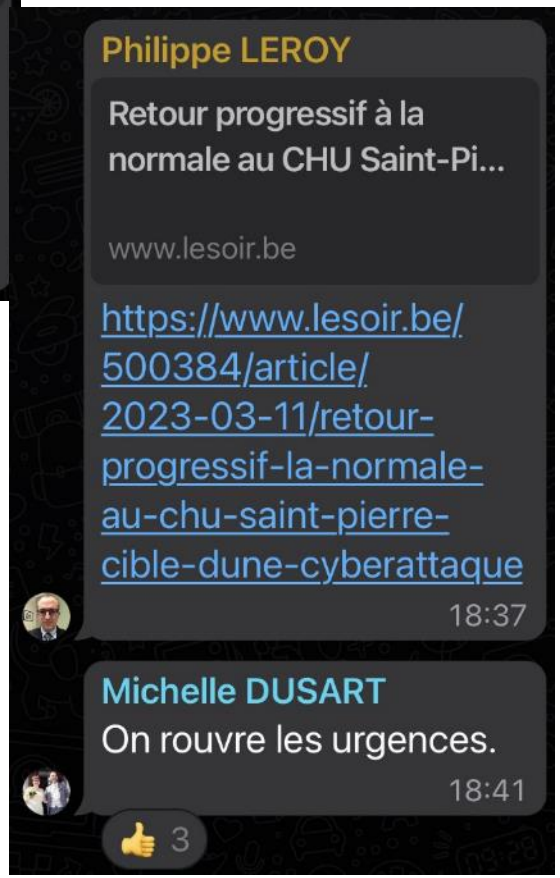
CERT.be
The Federal Cyber Emergency Team

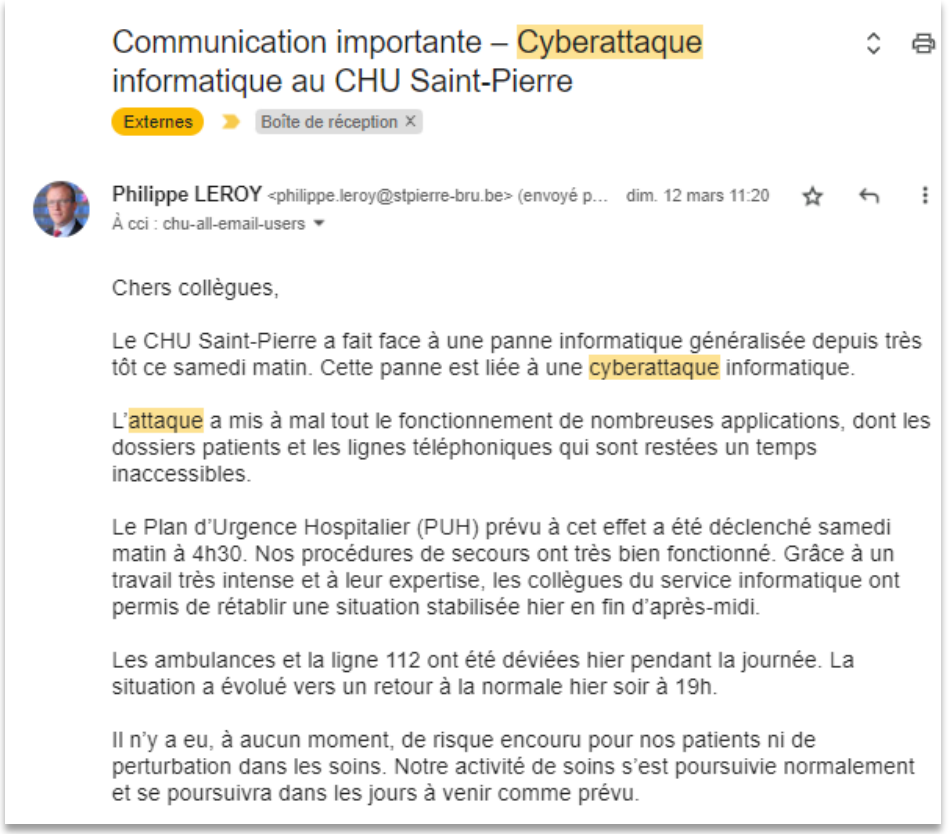


Savoir qui contacter

Cyber response plan

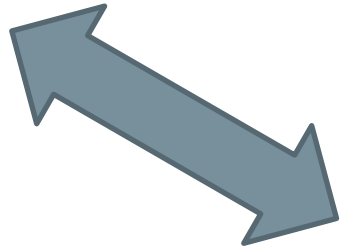
Communication externe & interne

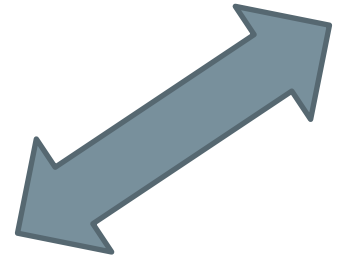




4 cellules de gestion de crise et de communication

Comité PUH (Direction)





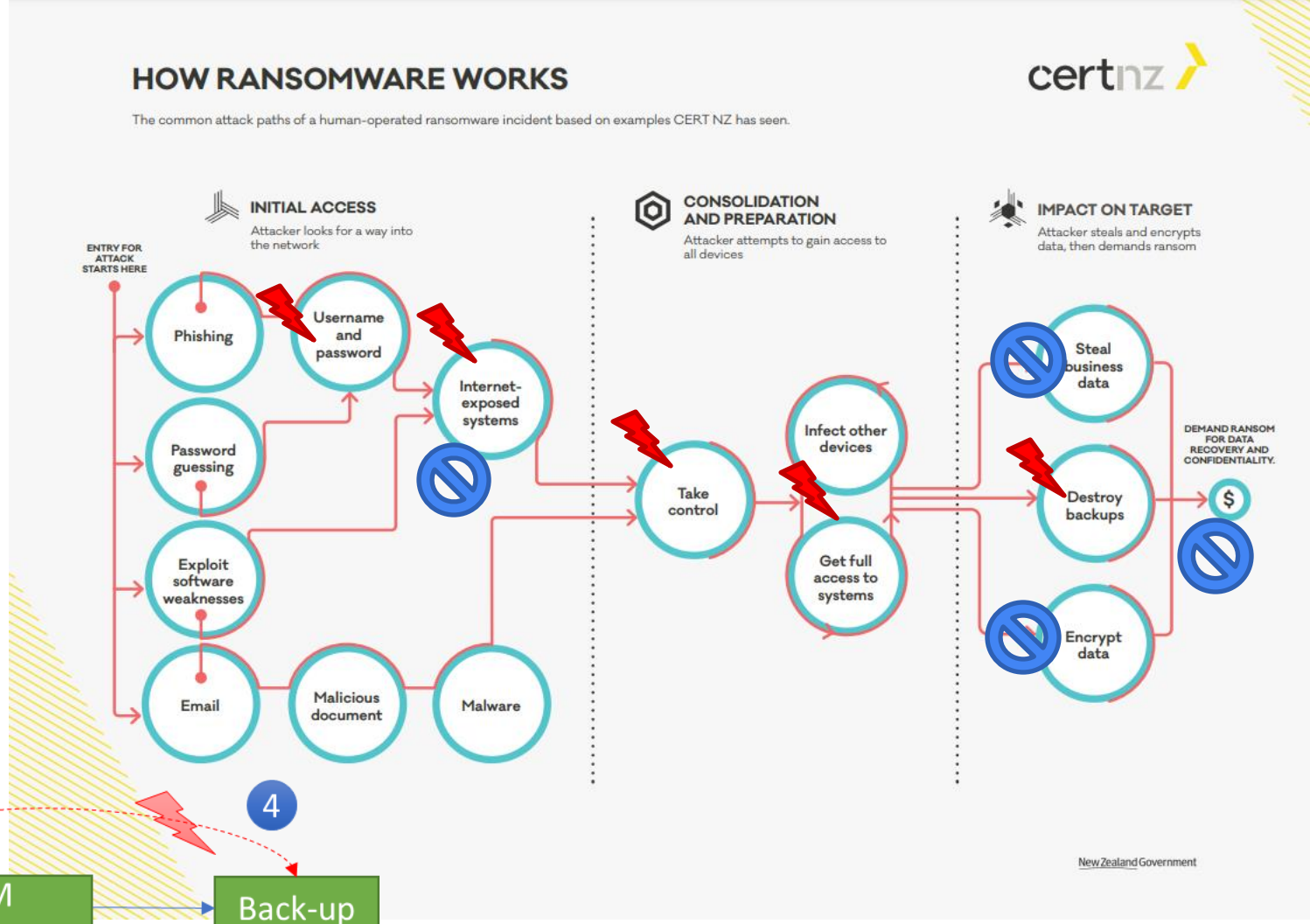
Equipe IT

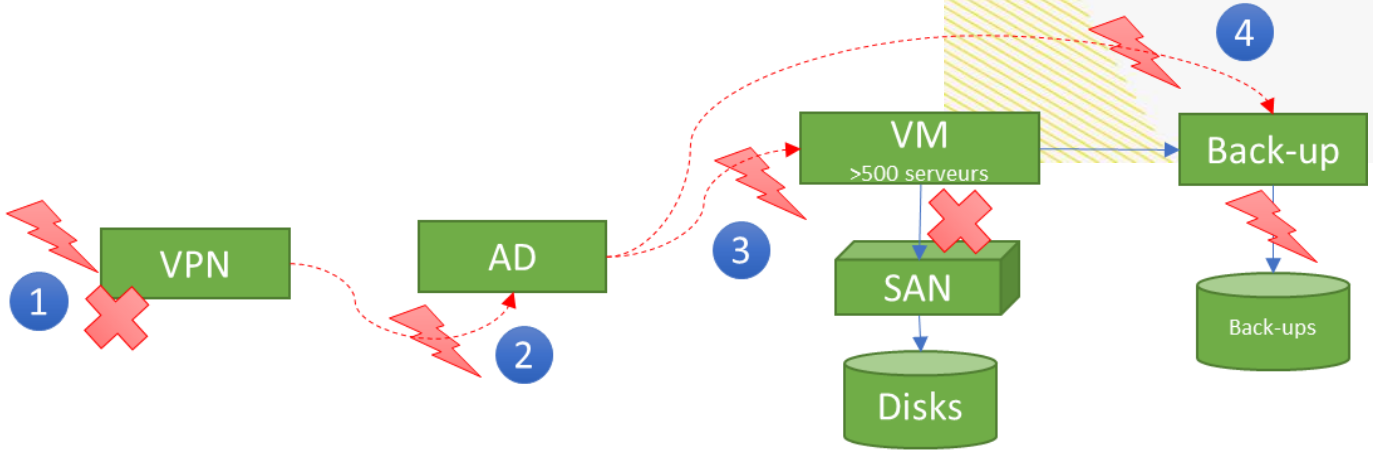
CIOs réseau

Scenario de la cyberattaque

48h

Première connexion 8/3 ~22h
Dernière connexion 11/3 ~1h





Actions immédiates

1. **Coupure** de la connexion internet et des connexions avec les hôpitaux partenaires.

2. **Plan d'urgence** enclenché rapidement et suivi de façon efficace.

3. **Vecteur d'attaque arrêté** rapidement et **plainte** déposée à la police de Bruxelles

→ Intervention efficace de la cellule de crise fédérale dédiée à la cybersécurité (**CERT** – Cybersecurity Emergency & Response Team).

→ Très bonne **solidarité et collaboration** entre les services informatiques du réseau CHU Saint-Pierre, CHU Brugmann, HIS, Erasme, LHUB

Conséquences

- Impact sur l'activité du CHU Saint-Pierre limité :
  Tous les systèmes de l'hôpital **opérationnels en moins de 24h**

- Impact sur les **partenaires déconnectés :**
  Fonctionnement en mode dégradé du LHUB et des Cuisines Bruxelloises pendant une semaine.

- **Pas de perte de données des patients**

- **AD corrompu**

- **Accélération** de la roadmap sécurité (**69 recommandations** du CERT)

« Il ne faut jamais gaspiller l'opportunité d'une crise »

Conséquences pour le CHU Brugmann

- Prélèvements, Tri, hémato, biologie, chimie, BDS
  Tout est passé en papier (sortie des analyseurs)
- Processus manuel activé pour la commande des repas
- Outil Anapath à l'arrêt 3 jours
- Processus de gestion de paie et planification difficile

Mesures - Acceleration de la roadmap

5 Password manager

6 AD Reconstruction

Password change
Password policy

2

VPN

AD

VM
>500 serveurs

Back-up

4 Reconstruction des back-ups

SAN

Disks

Back-ups

3 MFA

1 EDR, EPP

9 IAM

10 Cloud back-up

11 Sensibilisation

8 NTA

7 SOC

Lessons learned

1. **Priorités en matière de cybersécurité :**
   - Gestion des identités et des accès, password policy, MFA
   - Backup immuable
   - « Whitelisting » versus « blacklisting »
   - Visibilité sur les événement de sécurité

→ réseau = maillon faible : détecter et couper la source du vecteur d'attaque (pour éviter de tout couper)

2. **« Get the basics right » : IT Service Management/Asset Management (Identify)**
   - Inventaires des applications, connexions, flux des données
   - Points de contact pour des applications (pour tester, décider, etc.)
3. **Assurer la continuité des opérations**
   - Documents critiques accessibles offline – mode dégradé (connaissance et documentation des processus)
   - Moyens alternatifs de communication : numéros de téléphones, WhatsApp, 4G, imprimantes déconnectées
4. **Plan de reprise des activités :** définir une stratégie et les priorités pour la reprise des activités

5. **Communication** interne et externe

6. **Facteur humain**


Philippe LEROY
Merci
20:31
Un dîner typique à l'informatique
20:33
4
Gaëtan Bonny
Vous avez besoin de ravitaillement? Si oui dis-moi quoi peu importe l'heure!
20:34

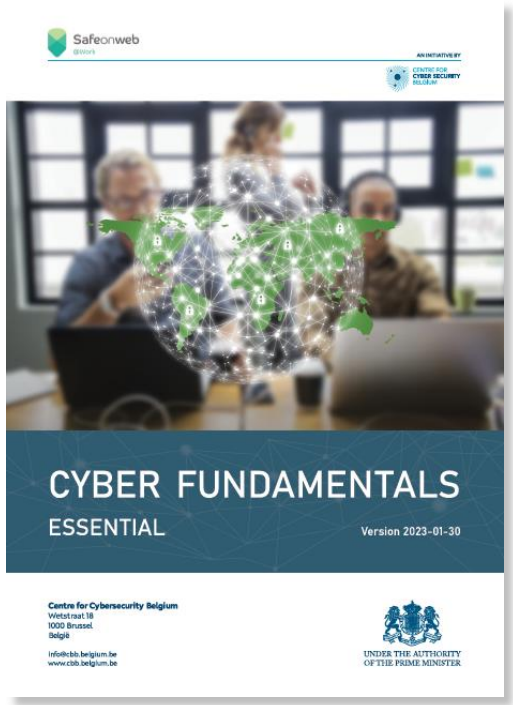

KEEP
CALM
IT'S NOT A SPRINT
IT'S A
MARATHON

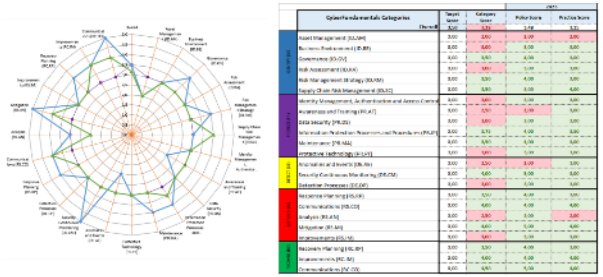
Cybersecurity program : « Vigilare »

NIS2

.be 18/10/2024

30 mois





- Lot 1 – Business Environment
- Lot 2 – Continuity Management
- Lot 3 – Backup Strategy
- Lot 4 – Security Governance
- Lot 5 – Security Awareness
- Lot 6 – Risk Management
- Lot 7 – Data Management
- Lot 8 – Vulnerability Management
- Lot 9 – M365 Security
- Lot 10 – Physical Access Management
- Lot 11 – Remote Access Management
- Lot 12 – Network Protection
- Lot 13 – Central Log Management
- Lot 14 – Device Management
- Lot 15 – Supply Chain Management

18 AVRIL 2027


S’unir pour sécuriser!
Merci pour votre attention

Les conférences reprendront dans 15 minutes.

Cyberwal
by digital
wallonia

CENTRE FOR
CYBERSECURITY
BELGIUM

Ellen Stassart

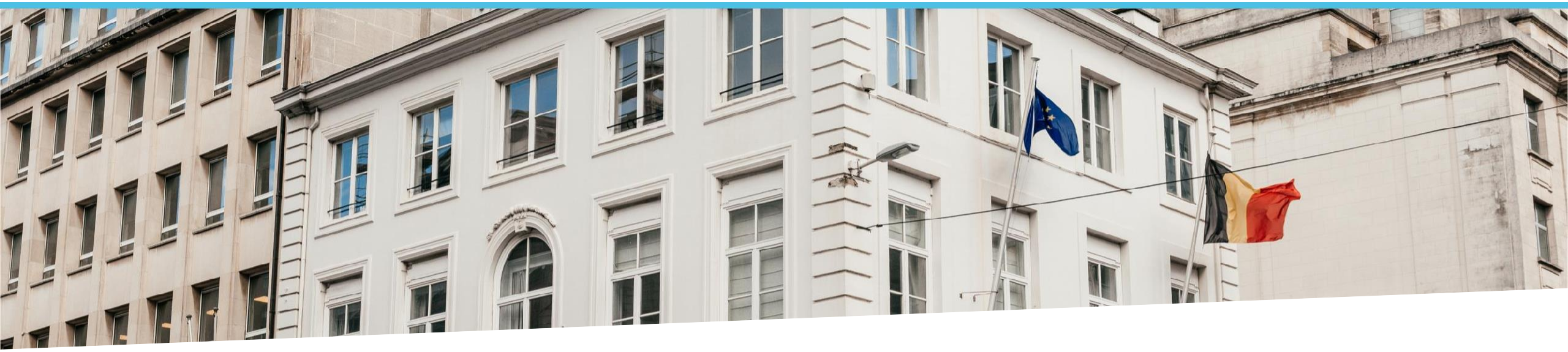
Centre for Cybersecurity Belgium (CCB)

Cyberwal
by digital
wallonia

CENTRE FOR CYBERSECURITY BELGIUM

NCC-BE
BELGIUM CYBERSECURITY COORDINATION CENTRE

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister



Cybersécurité: Un enjeu vital pour les hôpitaux belges

Profitez des fonds européens pour protéger vos infrastructures et garantir la sécurité des soins de santé

16 Octobre 2024 - Ellen STASSART (Directrice CCB & Head of the NCC-BE)

Agenda

1. Qu’est-ce que le CCB?
2. Introduction de l’ECCC et du NCC-BE
3. Sources de financement disponibles
4. Que pouvez-vous tirer du NCC-BE?
5. Points à retenir et prochaines étapes
6. Questions et réponses

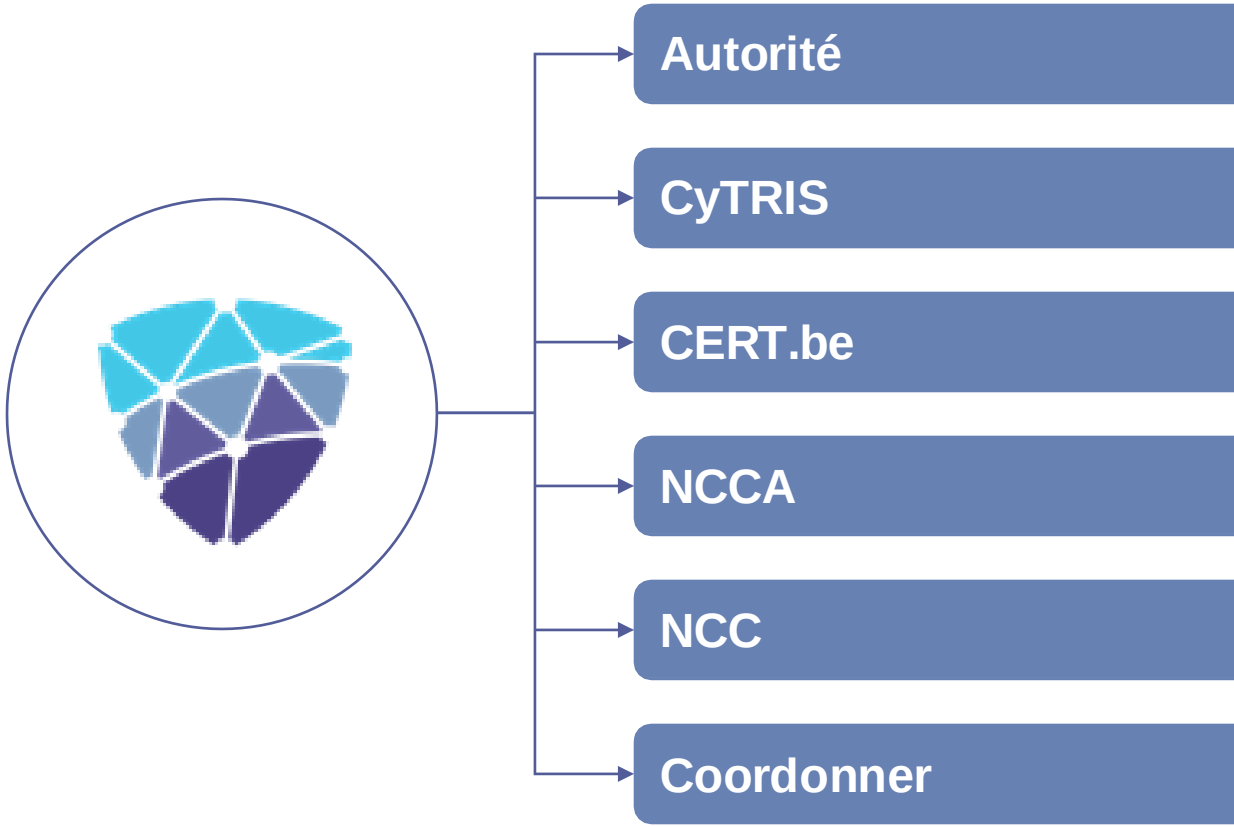
Le Centre pour la Cybersécurité Belgique (CCB) est l’autorité nationale en charge de la cybersécurité en Belgique

Créé par l’Arrêté Royal du 10 octobre 2014

Le CCB supervise, coordonne et contrôle l'application de la stratégie belge en matière de cybersécurité

CENTRE FOR CYBERSECURITY BELGIUM

Grâce à un **échange d'informations optimal**, les entreprises, les pouvoirs publics, les prestataires de services essentiels et la population peuvent **se protéger de manière appropriée**.



Le CCB en tant qu'autorité nationale

CENTRE FOR CYBERSECURITY BELGIUM

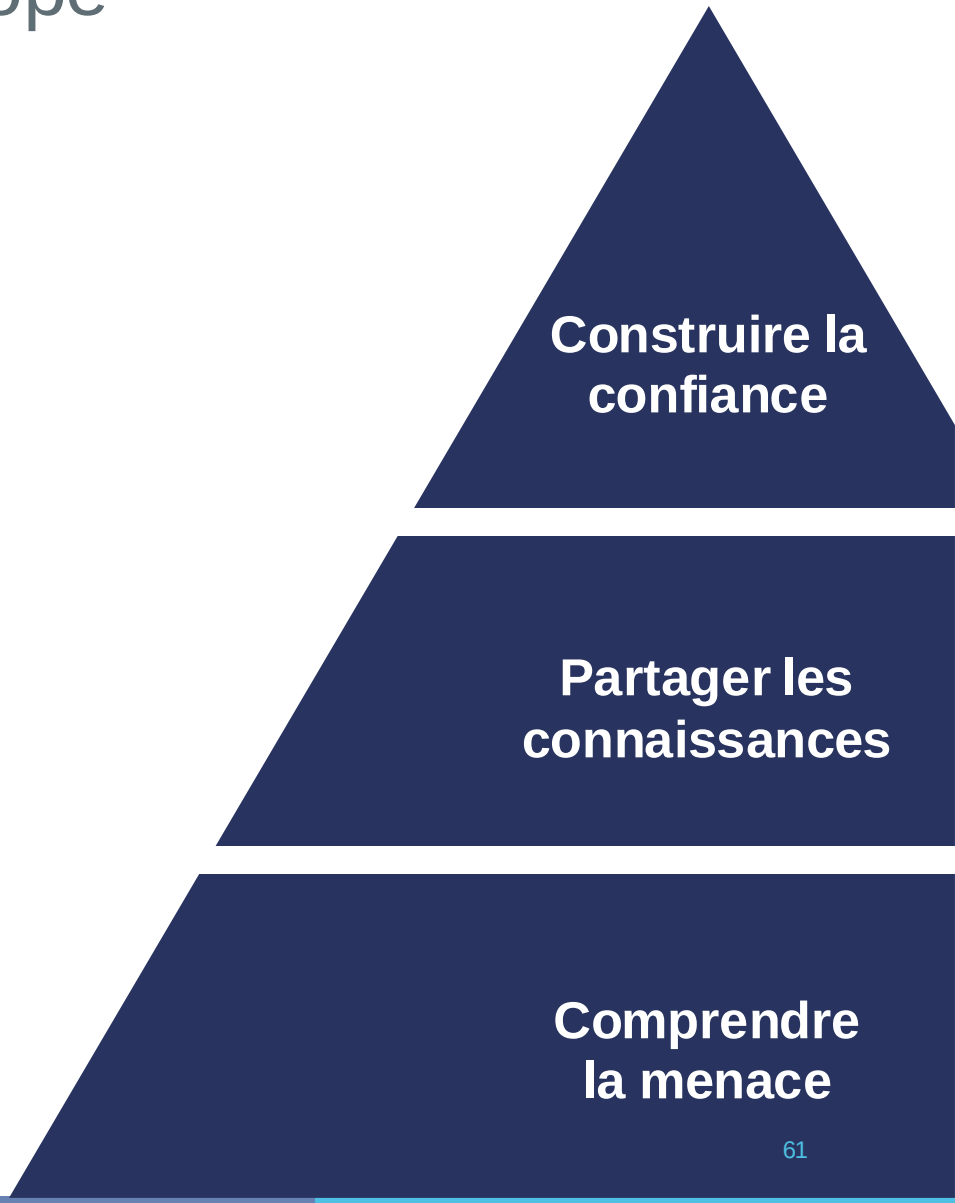
1. Mise en œuvre de la stratégie et de la politique belges en matière de cybersécurité
2. Assurer la coordination
3. Adapter le cadre réglementaire
4. Assurer la gestion des crises
5. Mise en œuvre de normes, de lignes directrices et de normes de sécurité pour les institutions publiques
6. Représentation de la Belgique dans les forums internationaux sur la cybersécurité
7. Évaluation et certification de la sécurité
8. Informer et sensibiliser

Notre mission est de faire de la Belgique l'un des pays les moins vulnérables d'Europe

Ceci est fait grâce

› A la stratégie nationale du CCB

› L'approche de **cyber protection active** (ACP)



Introduction de l’ECCC

L'ECCC est le moteur de la mise en œuvre de la stratégie européenne en matière de recherche, d'innovation et de politique industrielle dans le domaine de la cybersécurité.

Officiellement fondé en 2021. Sa création repose sur le Règlement (UE) 2021/887, adopté par le Parlement européen et le Conseil le 20 mai 2021.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Sources de financement européen (2021-2027)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Digital Europe Programme

Horizon Europe

European Cybersecurity Competence Center

Réseau de centres de coordination nationaux (NCC)

Projets de renforcement des capacités

Projets de R&D collaboratifs

Co-investissement par l'industrie sur une base projet

Co-investissement par les États membres (volontaire)


et s'appuyant sur des programmes européens

En 2022, le CCB a été désigné comme le centre national de coordination pour la Belgique (NCC-BE)

CENTRE FOR CYBERSECURITY BELGIUM

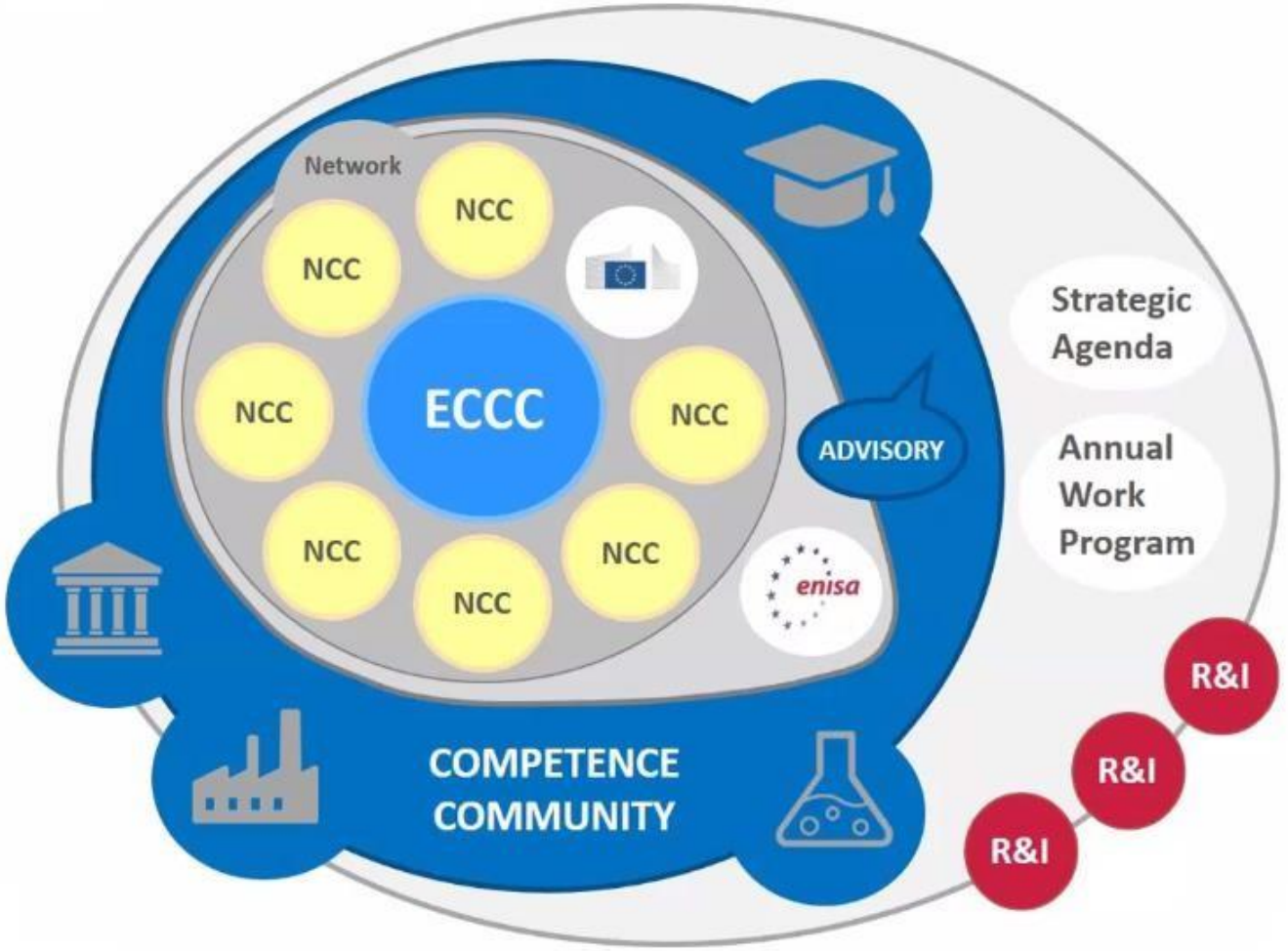
Ses missions légales sont les suivantes :

1. Coordonner **les investissements de l'UE** (DEP et HE) – y compris le FSTP ;
2. Soutenir **les missions stratégiques du Centre de compétence européen** – renforcement des capacités nationales ;
3. Agir en tant que **point de contact national** pour le cadre de l'ECCC.

NCC-BE
BELGIUM CYBERSECURITY COORDINATION CENTRE

De plus, le NCC-BE devrait servir de **plateforme pour la coordination et la collaboration entre les parties prenantes belges** des secteurs industriel, académique et de la recherche, ainsi que les citoyens, le secteur public et les autorités dans le cadre de la NIS.

Un nouveau cadre européen



Source: ENISA

Objectifs du nouveau cadre européen

Renforcer le ‘leadership’ global de l’UE en matière de cybersécurité et **son autonomie stratégique**

Préserver et développer **les capacités technologiques et industrielles** dans le domaine de la recherche sur la cybersécurité

Renforcer la **compétitivité de l'industrie** de la cybersécurité

Faire de la cybersécurité **un avantage concurrentiel** pour les autres secteurs

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Les possibilités de financement sont multiples

Soutien Financier aux Tiers (FSTP)

… et il y en aura certainement d'avantage dans un futur proche

« Nous devons également faire davantage **pour protéger la sécurité de nos systèmes de santé**, qui sont de plus en plus la cible d'attaques par cybersécurité et de rançongiciels. Pour améliorer la détection des menaces, la préparation et la réponse aux crises, je proposerai un **plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé** dans les **100 premiers jours du mandat**. »

Source : LIGNES DIRECTRICES POLITIQUES POUR LA PROCHAINE COMMISSION EUROPÉENNE 2024−2029.

Quels sont les avantages pour vous?

CENTRE FOR CYBERSECURITY BELGIUM

1

Faites entendre votre voix sur la scène européenne

Rejoignez la Communauté de Compétence en Cybersécurité belge !

2

Soyez au courant des possibilités de financement de l'UE en avant-première

Participez à nos événements de networking !

3

Recevez du soutien pour la mise en œuvre du CRA

Inscrivez-vous à notre newsletter

Principaux points à retenir et prochaines étapes

1. Le CCB est le **NCC de la Belgique**
2. Le NCC-BE sert de plaque tournante pour la **coordination et la collaboration entre tous les acteurs belges** à tous les niveaux de gouvernement
3. Le NCC-BE est là pour **soutenir le secteur hospitalier belge** dans ses efforts pour se conformer aux nouvelles règles de cybersécurité

Rejoignez notre groupe LinkedIn pour rester informés de toutes les dernières nouvelles du NCC-BE

Avez-vous des questions?

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

NCC-BE
BELGIUM CYBERSECURITY
COORDINATION CENTRE

Les conférences reprendront à 13h.

Cyberwal by digital wallonia

NIS2 Awareness et approche
Panel discussion

Christophe Hohl (CSM), Kurt Gielen (ZOL), Alexandru Pelin (CISO), Bastien Ducarme (CHRSM)

Cyberwal
by digital
wallonia

CYBER SECURITY MANAGEMENT

PAM

Privilege Access Management

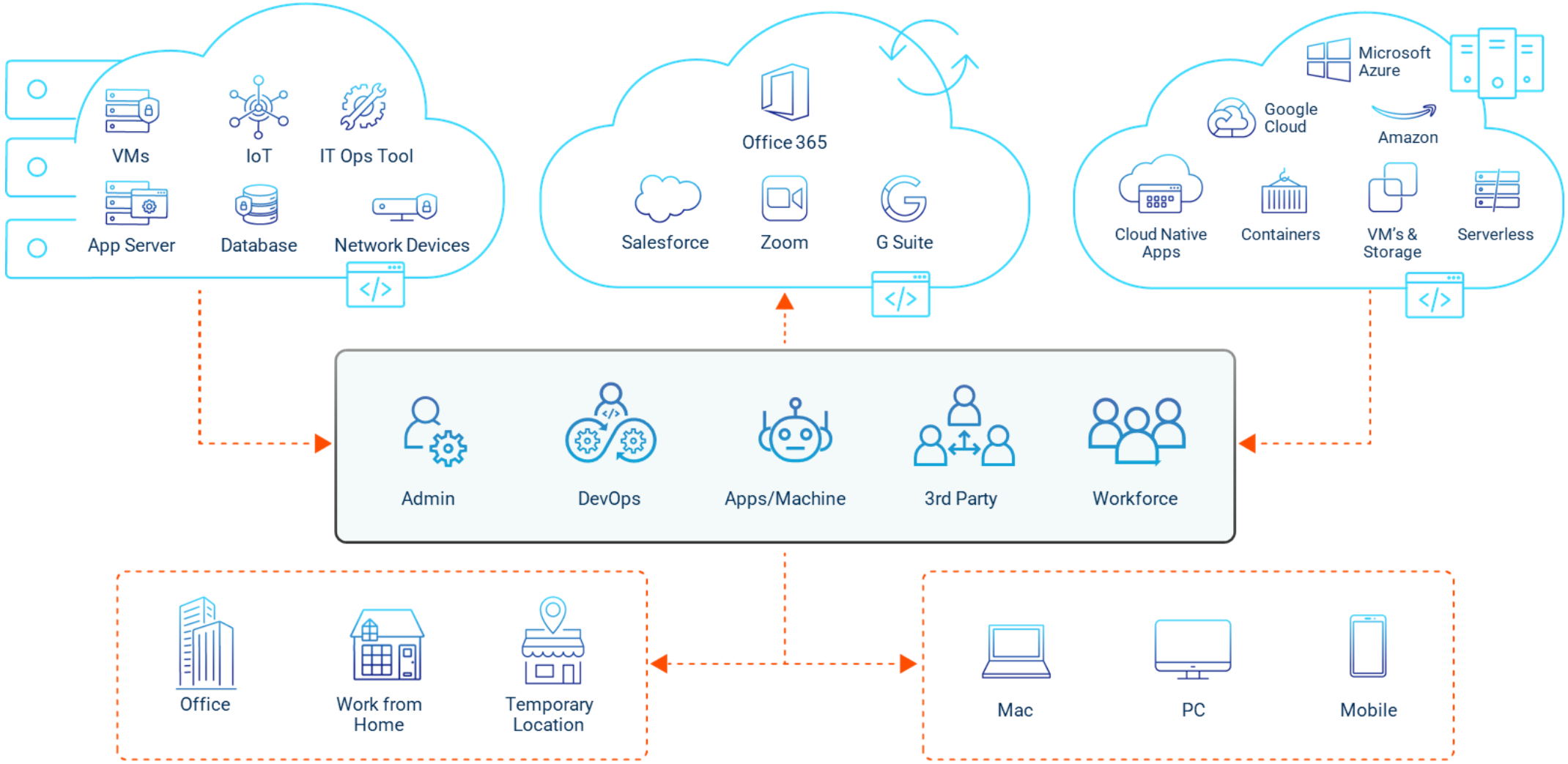
Introduction

What is a privileged account?

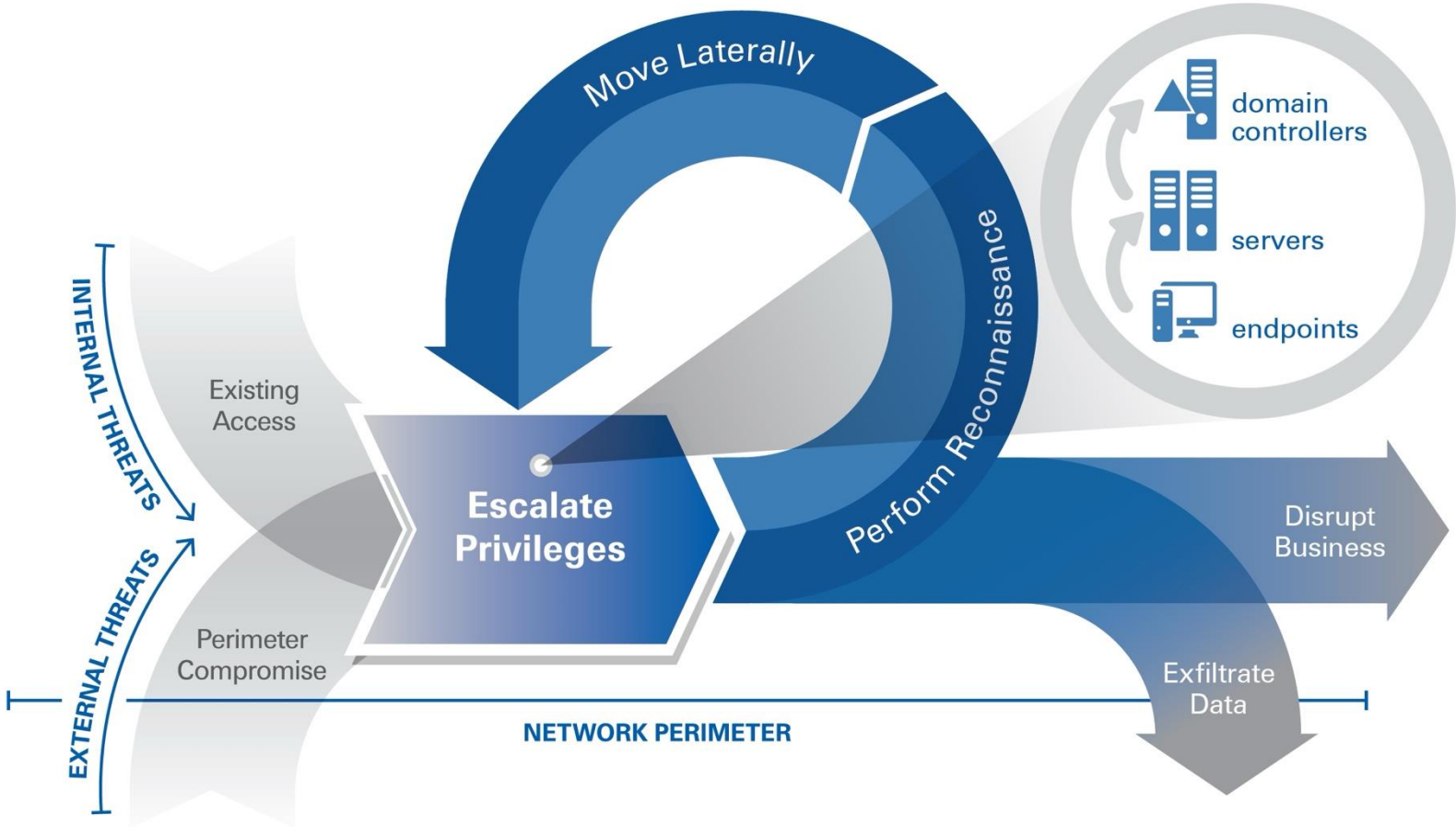
- A privileged account is a user account with higher privileges than regular user accounts and that allows for more operational actions.
- Privileged accounts exist in many forms in the enterprise environment

- Local admin accounts
- Domain admin accounts
- Breaking glass accounts
- Service accounts
- Application accounts
- Database accounts
- …..

Privileged accounts are everywhere!



Risk of privileged accounts:
They are at the heart of the attack cycle



PAM COMPLIANCE

DIRECT LINK WITH SOME ISO 27K POINTS

ACCESS CONTROLS

Section	Subject	Objective/Control	Role of PAM in the Control Execution
A.9.2.1	User registration and de-registration	Control: A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	A PAM solution facilitates user registration and de-registration to provide high visibility over access rights and active privileged users.
A.9.2.2	User access provisioning	Control: A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	The PAM solution provides a centralized management interface to grant or revoke privileged access rights to critical systems.
A.9.2.3	Management of privileged access rights	Control: The allocation and use of privileged access rights shall be restricted and controlled.	The PAM solution restricts and controls privileged access rights.
A.9.2.5	Review of user access rights	Control: Asset owners shall review users' access rights at regular times.	Asset owners can specify privileged usage rights to the PAM system manager, who then implements the policies to ensure that only administrators approved by the asset owners are allowed privileged access. All access rights can also be managed in a centralized platform directly built in the PAM solution.
A.9.2.6	Removal or adjustment of access rights	Control: The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	The PAM solution allows super admins to smoothly modify their privileged of users or groups of users, thereby facilitating the termination or reduction of employee rights.

PAM COMPLIANCE

DIRECT LINK WITH SOME ISO 27K POINTS

OPERATIONS SECURITY

Section	Subject	Objective/Control	Role of PAM in the Control Execution
A.12.1.2	Change management	Control: Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	PAM's session and activity tracing and recording should be used as a tool to monitor all change management work carried out to help troubleshoot issues that may show up after the change management. PAM also carries access validation workflows to ensure the control of processes.
A.12.1.3	Capacity management	Control: The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	A PAM solution provides a clear and concise view of targetuses along with information regarding the storage status and the number of concurrent connections.
A.12.4.1	Event logging	Control: Event logs recording user activities, exceptions, faults and information security events shall be produced, kept, and regularly reviewed.	A PAM solution traces and records all privileged users' activity to give administrators complete visibility over the actions that occur on their systems and equipment.
A.12.4.2	Protection of log information	Control: Logging facilities and log information shall be protected against tampering and unauthorized access.	All accesses should be logged into the system including unauthorized access. A PAM solution should differentiate the system administrator from the root user to protect against tampering. The WALLIX Bastion separates the administrator from the system's root user, thereby making the root user the only one able to access to logs files, protecting them against tampering. All access logs are also closely monitored.
A.12.4.3	Administrator and operator logs	Control: System administrator and system operator activities shall be logged and the logs protected regularly.	All operations realized by administrators should be logged through a syslog system. This includes information such as administrator connection, user creation by the administrator, password modification etc.

PAM COMPLIANCE

NIS 2

NIS2 Article 21 Security Area Corresponding ISO27001 Annex A:	
NIS2 Article 21 Security	ISO 27001 Annex A Controls
Incident handling and reporting	A.16: Information Security incident management
Business continuity	A.17: Information security aspects of business continuity
Supply chain security	A.15: Supplier Relationship
Systems acquisition, development, and maintenance security	A.14: System acquisition, development, and maintenance
Cryptography and encryption technologies	A.10: Cryptography
Human resources security	A.7 Human resource security
Access control polices	A.9: Access control and A.5: Information security policies
Asset management	A.8: Asset management
Authentication Solutions / MFA	A.9: Access control

CYBER SECURITY MANAGEMENT

PAM
Features

Components and Features

Password Vault

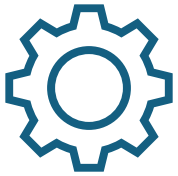
- Storage/locking of privileged accounts & SSH keys
- Encryption according to national, European or international standards
- Separation of roles using an authorization matrix

Session Manager

- Define session properties and workflow based on defined policies
- Session hardening
- Restrict user-initiated processes
- Restrict network bounces

Password Manager

- Change passwords according to defined policies
- Visualize passwords
- Password checkin/checkout process



Components and Features

Interfaces

- User interface
- Bastion and other components administration
- Connect to target or recover password
- Using standard tools: RoyalTS, Putty, MobaXterm

External Acces

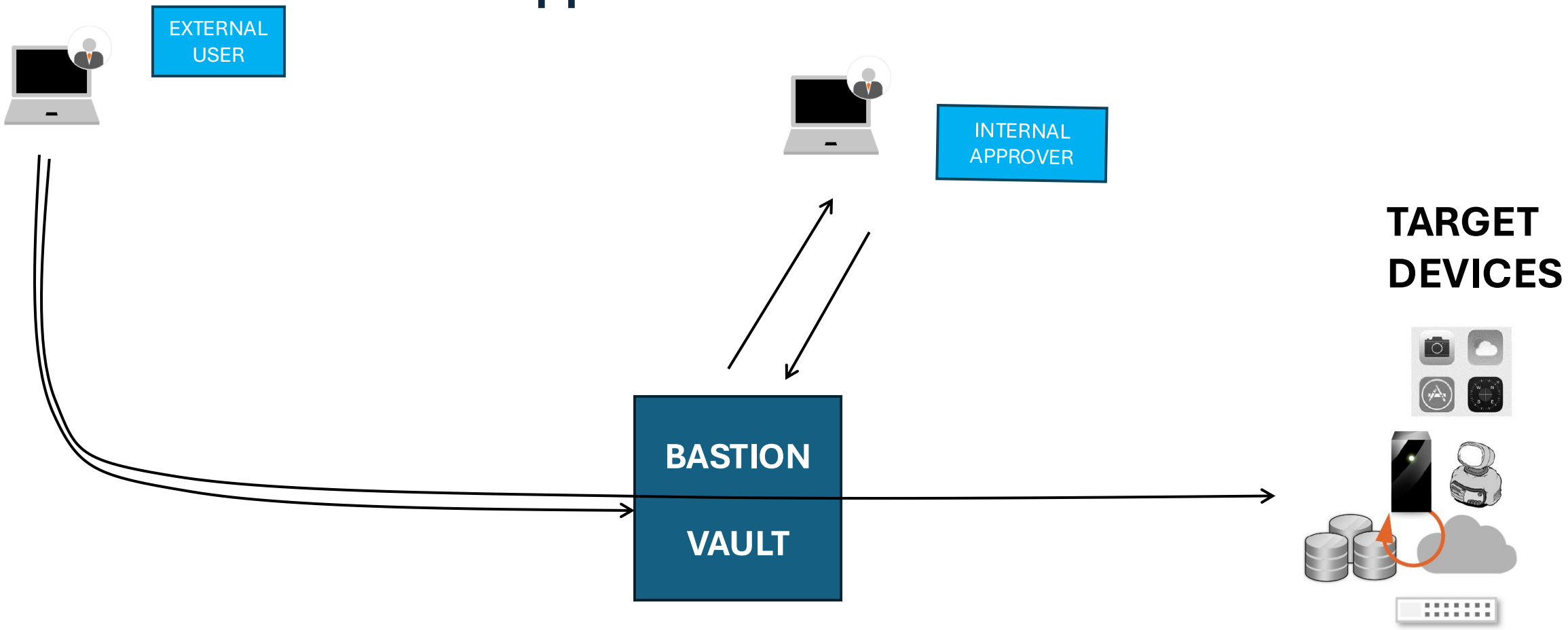
- HTML5 WEB Gateway
- Accessible only via HTTP/HTTPS
- Interconnected to Bastion
- Connect to targets from Bastion

Audit

- Viewing recordings and session logs
- Real-time monitoring
- Remote control
- Access to user keyboard entries, metadata, processes in log files
- SIEM integration

Components and Features

Approval workflow

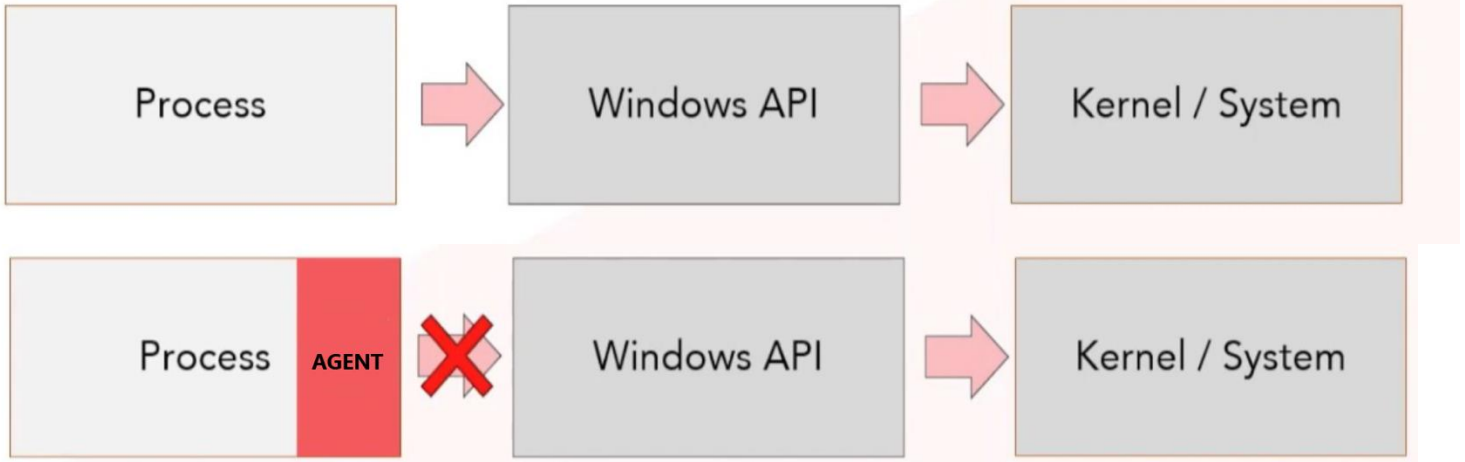


Components and Features

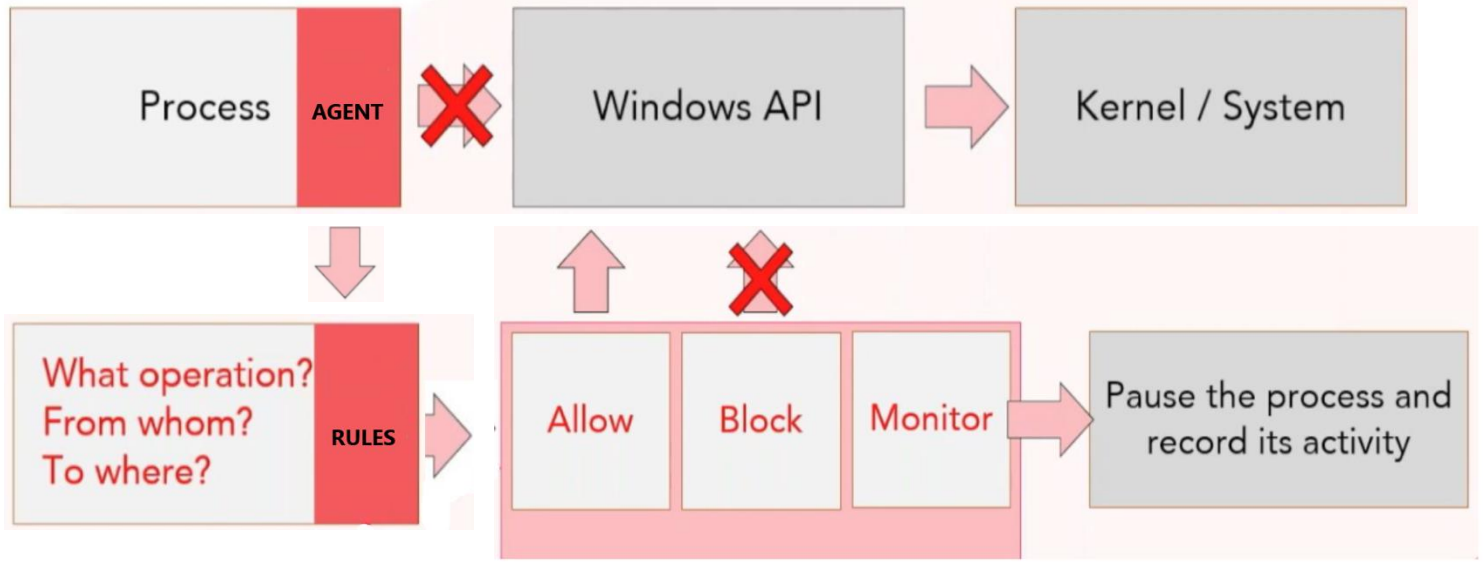
POLP – Principe Of Least Privilege
An admin is not an admin anymore

(Concept of Zero Trust)

WITHOUT POLP



WITH POLP



Components and Features

Zero Trust

Former Forrester analyst John Kindervag developed the concept of Zero Trust security in 2010.
A Zero Trust architecture follows the maxim
“never trust, always verify”

Zero Trust is a cybersecurity strategy based on the principle of least privilege and strict user authentication, not implicit trust.

Zero Trust is a security policy in which no one – regardless of their role or responsibility – is inherently considered “safe.”

It consists of granting only the rights strictly necessary to the user.

Components and Features

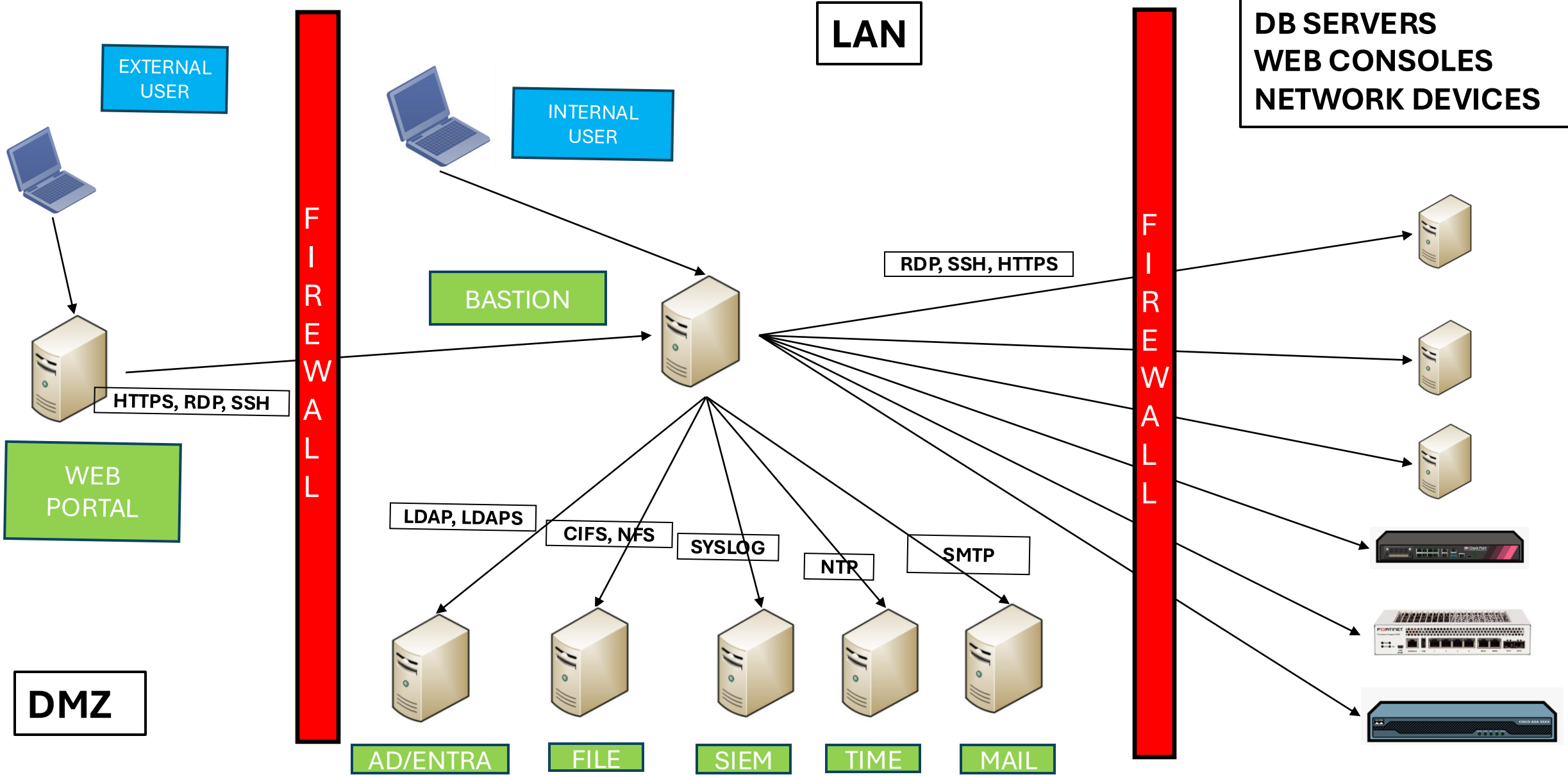
Breaking Glass

Procedure for restoring privileged accounts in the event of PAM unavailability

CYBER SECURITY MANAGEMENT

Architecture

VLAN SECURE
WIN & LINUX
SERVERS
DB SERVERS
WEB CONSOLES
NETWORK DEVICES



PAM OT

Today OT ?

Today, OT increasingly relies on IT technologies.

Multiple, uncontrolled and unmonitored remote accesses drastically increase the attack surface of OT environments with major consequences in terms of production costs, data leakage or human impacts (biomedical context for example).

Some service providers have their own tools to connect to the PLCs, with their own configuration and their own habits. It is therefore essential to secure their connection directly from their workstation to the target to guarantee operational efficiency.

PAM OT

According to the latest Microsoft Digital Defense Report, 25% of OT devices use unsupported Operating Systems !

The state of IoT and OT security continued

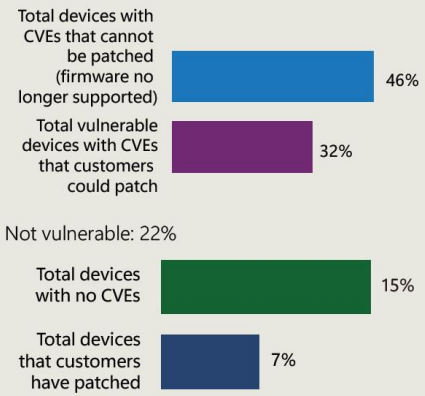
Vulnerable devices susceptible to compromise

OT and industrial control system devices are frequently left unpatched and exposed, making them easy targets for hackers. Patching these systems can be challenging for organizations, as updates may need to be postponed to avoid disrupting operations.

Additionally, some OT devices lack patches for vulnerabilities, often due to discontinued support. Hackers can exploit vulnerable OT devices by using internet search tools to find ports used for remote management and gain unauthorized access, often using default credentials.

It is vitally important to know the status of your devices and to take steps to protect them from potential attacks.

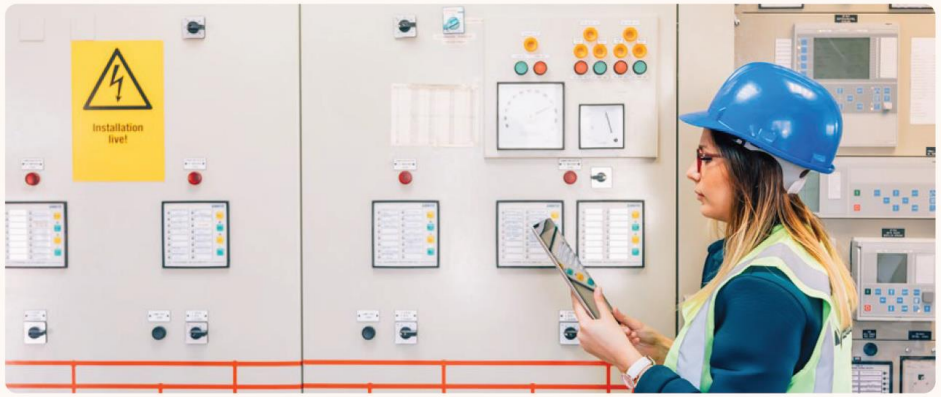
Device vulnerabilities in industrial control networks



Source: Microsoft Defender for IoT sensors

25%

of OT devices on customer networks use unsupported operating systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats.



Microsoft Defender for IoT actively monitors critical infrastructure device security to stay ahead of emerging threats. However, recent data reveals that 78% of devices on customer networks have known vulnerabilities that threat actors can exploit, and 46% of these devices cannot be patched.

Some OT devices still use unsupported operating systems, such as Windows 2000, which are no longer receiving security patches from Microsoft. Twenty-five percent of OT devices on customer networks use unsupported systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats. This allows threat actors to exploit known vulnerabilities in unsupported OT devices, posing significant risks to critical infrastructure and industrial processes.

Pr Cybersecurity Tech Accord principles mapping index **page 124**

Actionable insights

1. Gain deeper visibility into IoT/OT devices and prioritize them based on their risk to the enterprise if compromised.
2. Reduce the attack surface by eliminating unnecessary internet connections, open ports, and restricting remote access using VPN services.
3. Ensure devices are robust by applying patches, changing default passwords, and modifying default SSH ports.

PAM OT

Killware

Killware is a type of cyberattack deployed with the aim of creating real risks to human life through the manipulation of operating technology (OT).

In 2020, the University Hospital of Düsseldorf was hit by a ransomware attack that led to a collapse of the digital infrastructure.

A 78-year-old woman in dire need of medical attention died after emergency workers were forced to redirect her to another hospital 20 miles away.

PAM OT

Killware

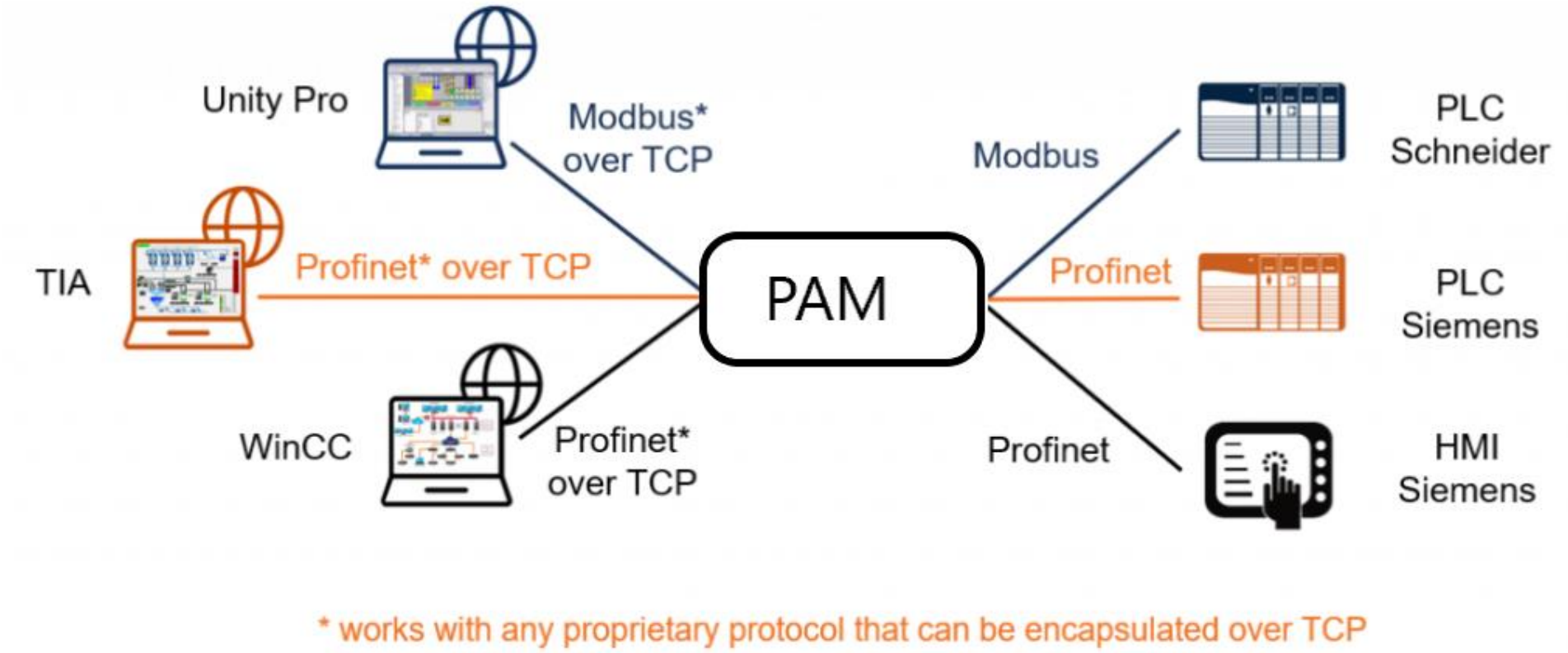
Another killware incident occurred in early 2021, when hackers gained access to the controls of a water treatment plant in Oldsmar, Florida. The hackers increased sodium hydroxide concentrations in the water to dangerously high levels (11,100 parts per million instead of 100 parts per million) just days before the Super Bowl was scheduled to take place.

Fortunately, operators responded quickly and were able to regain control of the systems within minutes. As a result, no injuries or health incidents were reported. Employees at the company had shared their remote access credentials with each other, which allowed the hackers to gain access to the facility's network.

PAM OT

Some PAM publishers offer solutions for OT, such as TCP/IP tunneling (SSH) between the operator station and the medical device, PLC, and this regardless of the OS used by the target device.

The TCP/IP session will be recorded in a PCAP file and can therefore be analyzed a posteriori with Wireshark.



PAM OT

Some tips to increase your OT protection level

- Adopt an OT Cybersecurity Framework
- Adopt a Defense-in-Depth Approach to Security
- Implement an Asset Management Solution
- Deeply Isolate the OT Network
- Ensure OT User Accounts are Separated from IT User Accounts
- Secure OT Privileged Access
- Secure Privileged Access for Vendors and Contractors
- Secure Access for Remote Employee Access
- Monitor and Remediate OT Security Vulnerabilities
- Remove Hard-Coded OT Credentials from Applications and Scripts
- Establish a Security-First Culture
- Perform Penetration Testing on Your OT Devices

PAM OT – CYBER SECURITY STANDARD ISA/IEC 62443

ISA/IEC 62443 Series of Standards

The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards

The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). These standards set best practices for security and provide a way to assess the level of security performance. Their approach to the cybersecurity challenge is a holistic one, bridging the gap between operations and information technology as well as between process safety and cybersecurity.

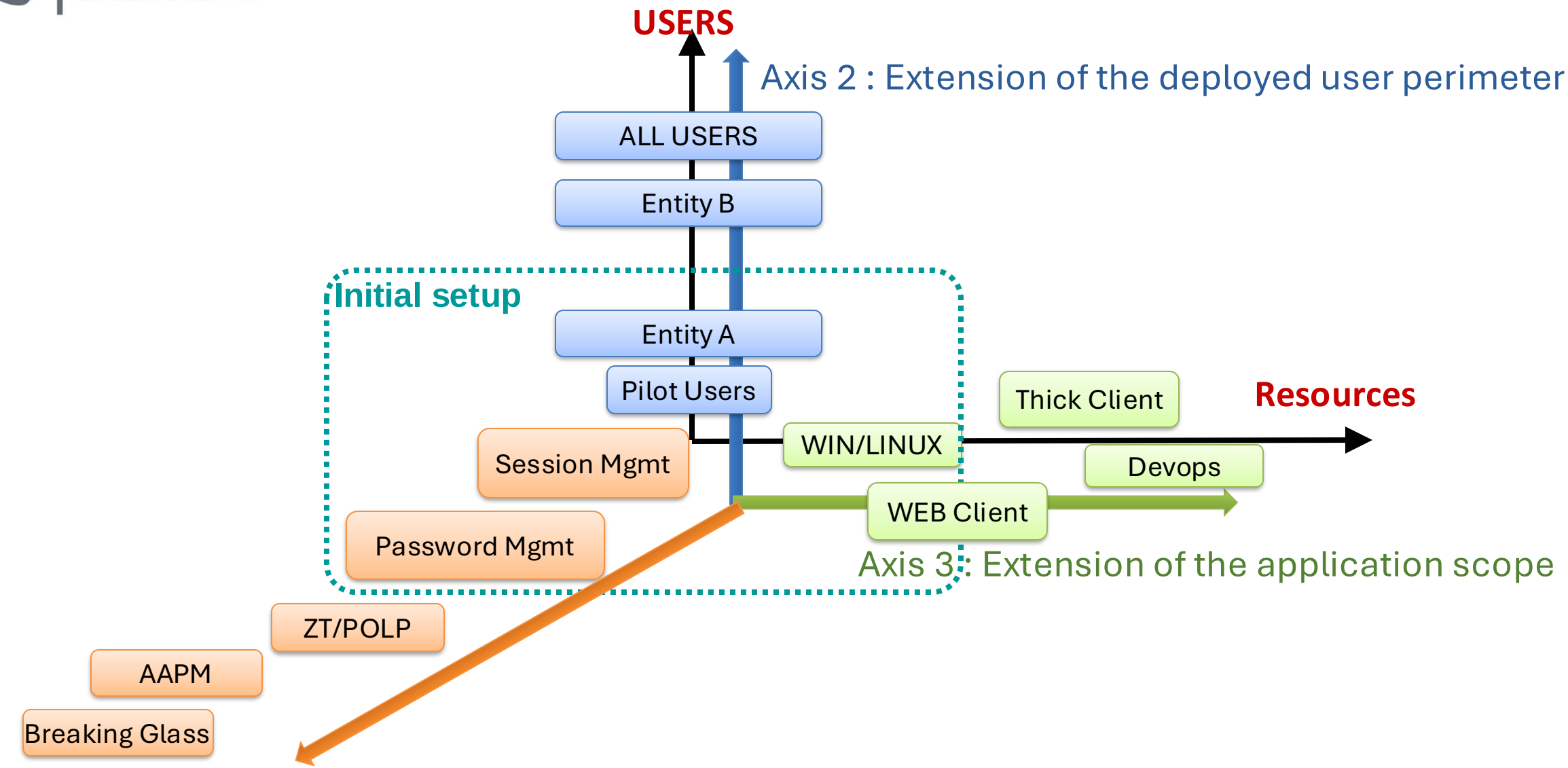
PAM OT – FRAMEWORK NIST

NIST Publishes Guide to Operational Technology (OT) Security

The impact of cybersecurity breaches on infrastructure control system owners/operators is more significant and visible than ever before. Whether you work for an infrastructure owner/operator or are a consumer of an infrastructure service, the events of the past few months/years have made it clear that cybersecurity is a critical factor in ensuring the safe and reliable delivery of goods and services. For infrastructure control system owners/operators, it can be challenging to address the range of cybersecurity threats, vulnerabilities, and risks that can negatively impact their operations, especially with limited resources.

Credit: Smart Connected Systems Division, NIST

Setup and Integration



Thank you for your attention

Easi

Cyberwal
by digital
wallonia

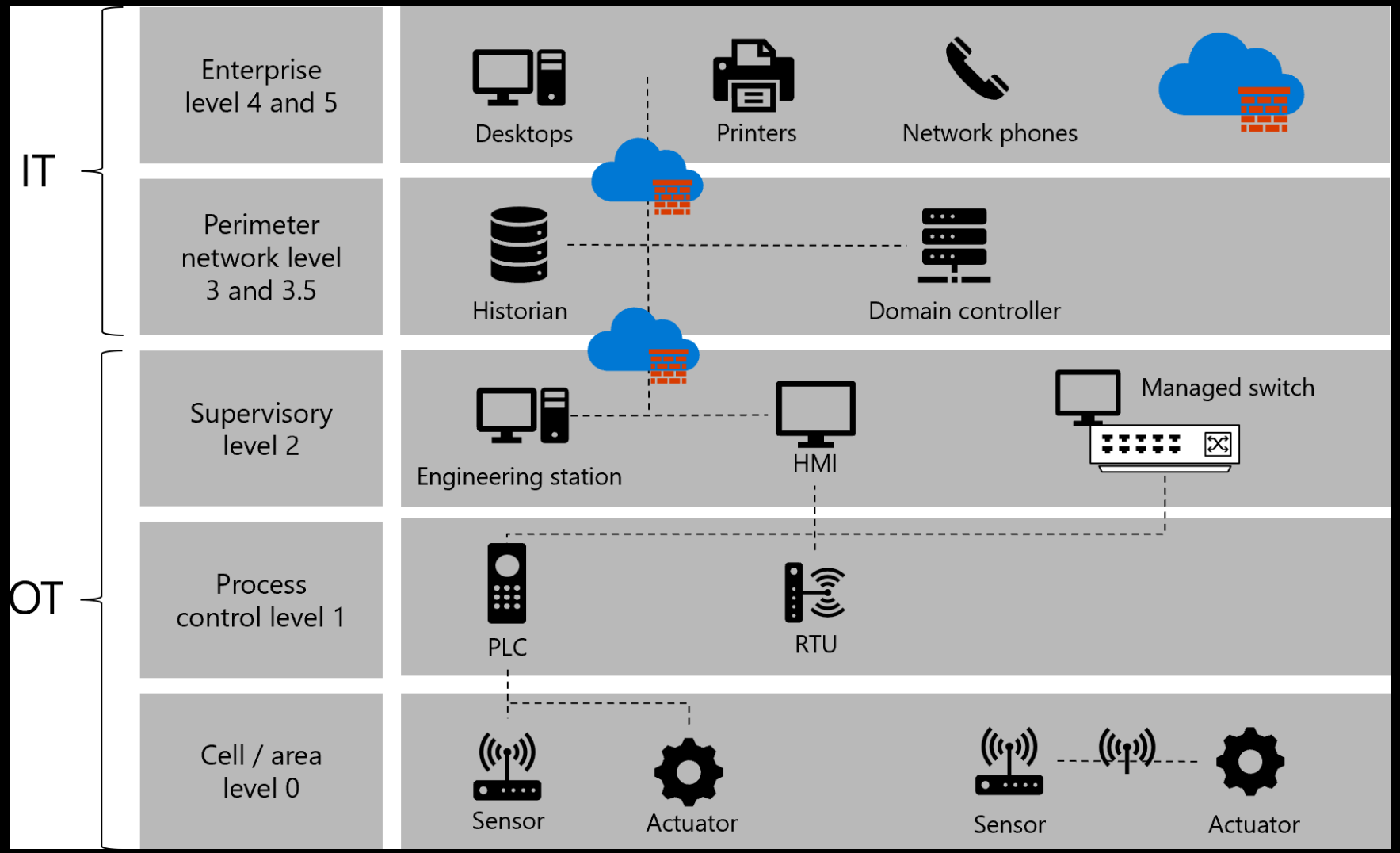
IT Vs OT

System’s Battle at the hearth of Digital Transformation

Different worlds, different people involved, different priorities,… but one common goal

	IT	OT
People	Business Analyst CIO IT Architect	Plant Manager Control Engineer COO
Business Priority	Confidentiality	Availability
Major Focus	Data integrity	Control processes -> No Downtime
Protection Targets	Computers, Servers	Industrial (legacy) devices, PLC, SCADA, HMI, MES, EWS
Environmental Conditions	Air-conditioned	Harsh environments such as extreme temperatures, vibrations, shocks
Standards	ISO27001	IEC 62443/NIST SP 800-82
Focus	Productivity	Safety
Cost	Hardware & SAAS (renewal every 3-5y)	Hardware & maintenance (up to +30y)
Threats	Ransomware/Malware -> Users cannot work	Ransomware/Malware -> Production is down
Patch Management	Challenging, but doable	Challenging, even sometimes impossible
Models/framework	OSI Model	Purdue Model

Network Flows



IT -> OT

- Only allow it via PAM (privilege access management tools)

OT -> IT

- Can be allowed
- Unidirectional flows with Data Diodes, Unidirectional gateways
- Multiple firewalls between environments

Conclusion

The **distinction** OT/IT is **significant**

Their **convergence is essential** for modern industrial operations

By **bridging the gap**, organizations can

- Enhance operational **efficiency**
- Improve **security**
- Foster **innovation**

Les ateliers débuteront dans 15 minutes.

Cyberwal by digital wallonia

Agence
du Numérique

Jeremy Grandclaudon

Agence du Numérique

Cyberwal
by digital
wallonia

Cyberwal
by digital
wallonia

Cyberweek – 16/10/2024

La cybersécurité dans le secteur hospitalier

Jeremy Grandclaudon

Nina Hasratyan

Agence
du Numérique


QUATRE
PILIERS

USAGES

COMPETENCES

RECHERCHE

RAYONNEMENT

Cyberwal by Digital Wallonia : des actions dédiées au secteur hospitalier

Cyberwal
by digital
wallonia

Campagne de sensibilisation spécifique

Mobiliser & Accompagner

Objectifs :

- Rappeler l'importance de veiller à la sécurité des données des patients, résidents, pensionnaires

Cyberwal by digital wallonia

Campagne de sensibilisation spécifique

Livre blanc :

Les défis et les meilleures pratiques de la cybersécurité dans le secteur de la santé

Mobiliser & Accompagner

- Présenter de manière concrète les **défis et les bonnes pratiques de cybersécurité** dans le secteur de la santé
- Faire prendre consciences des **risques associés aux nouvelles technologies** dans le domaine de la santé
- Proposer une **stratégie globale pour renforcer les défenses** en cybersécurité des établissements de santé

Simulateur numérique

Mobiliser & Accompagner

- **Objectif :** offrir une **démonstration pratique et concrète** des effets et conséquences d'une cyberattaque, afin de rendre la problématique de la **cybersécurité plus tangible** pour les participants.

Cyberwal by digital wallonia

- Un **environnement virtuel** offrant différents **scénarios de cyberattaques**.
- Des scénarios avec une variété de processus, de cibles, de vulnérabilités et de conséquences.
- Disponible de manière itinérante **à partir de 2025**.
- Propose **3 niveaux de complexité** dans les scénarios d'attaque

- **Pour qui ?**
  - Preneurs de décision.
  - Tout type de public, technique ou non.
  - Utilisé lors d’événements et de conférences pour les publics cibles.

Cyber Response Team (CRT) Wallonne

Accompagner & Soutenir

- **Objectif :** offrir un **support** aux demandes d'assistance des acteurs du secteur public ou privé en les **accompagnant dans les premières démarches** pendant ou après un incident et en les mettant en relation avec des partenaires pertinents.

- Constituée après **consultation et accord du CCB et du CERT.be**.
- Déploiement à partir de **2025**.
- **Intervention sur place** pour endiguer les cyberattaques.
- Contribue en amont à préparer et gérer les incidents cyber.
- Fait le **lien avec les initiatives internationales** (bonnes pratiques, retours d'expérience, ...).
- **Pour qui ?**
  - Services publics.
  - Secteur de la santé.
  - Ecoles.

Cyberwal by digital wallonia

DIGITAL WALLONIA
www.digitalwallonia.be
info@digitalwallonia.be
@digitalwallonia

AGENCE DU NUMERIQUE
Av. Prince de Liège, 133
5100 Jambes
+32 (0)81 778080
www.adn.be

STÉPHANE VINCE
Directeur,
Pôle Technologie et
Administration Numérique
Stephane.vince@adn.be

JEREMY GRANDCLAUDON
Jeremy.grandclaudon@adn.be

NINA HASRATYAN
Nina.Hasratyan@adn.be

WE LOVE DIGITAL

WE KNOW DIGITAL

WE MAKE DIGITAL

Wallonie Relance

AdN

Boot Camp cyber : de la formation au recrutement,
présentation d’un projet pilote

Les rôles de l’Ee-Campus

Former

Être acteur

Sensibiliser

La genèse du projet

WAPI 2040
animation territoriale
de la Wallonie picarde

Le groupe de travail e-santé : la rencontre entre les acteurs de soin de santé et le monde de la formation

Le secteur IT hospitalier un triple constat :

1. Manque d’attractivité sociale
2. Manque d’attractivité pécuniaire
3. Problème d’acculturation

Le « club des 5 » entre en scène (avec le soutien de Cybewall)

Le Boot Camp : principes de base

1. Une formation courte mais intense
2. Une présentation globale de la cybersécurité dans les hôpitaux
3. Une mise en contact directe avec les acteurs de soin de santé
4. Une réplication sur tout le territoire en mode « upskilling »

Le Boot Camp : les modules

1. Introduction aux systèmes hospitaliers
2. Introduction à la cybersécurité
3. Cybersécurité défensive (Blue Team)
4. Cybersécurité offensive (Red Team)
5. Gouvernance des systèmes d’information
6. Soft Skills

Introduction aux systèmes hospitaliers

- 5 jours
- Avoir une solide compréhension des réseaux hospitaliers, des systèmes d'information de santé, et des dispositifs médicaux connectés.

Introduction à la cybersécurité

- 3 jours
- connaître les bases de la cybersécurité d'un point de vue d'une personne chargée de mettre en œuvre la cybersécurité dans son organisation

Cybersécurité défensive (Blue Team)

- 7 jours
- installer et configurer des dispositifs médicaux, intégrant les systèmes d'information (IT), en respectant les normes de sécurité informatique et physique et savoir identifier, évaluer, et répondre efficacement aux incidents de sécurité.

Cybersécurité offensive (Red Team)

- 5 jours
- Acquérir les compétences pour planifier, exécuter, et rapporter des tests d'intrusion,
- maîtriser les techniques d'exploitation pour évaluer la sécurité d'un système
- Développer une compréhension approfondie des vulnérabilités avec une forte emphase sur l'éthique professionnelle.

Gouvernance des systèmes d’information

- 3 jours
- Comprendre et appliquer les principes fondamentaux de la gouvernance en cybersécurité
- Analyser et gérer efficacement les risques liés à la cybersécurité en utilisant des méthodologies éprouvées comme Artemis et EBIOS.
- Naviguer parmi les différents frameworks et normes de la cybersécurité (ISO 27001/27002, NIST, CCB, …), et comprendre leur application pratique pour la conformité et l'amélioration continue.

Softs skills

1. 2 jours
2. Développer les soft skills pour améliorer l'intégration au sein des équipes, améliorer la communication et favoriser la collaboration.

Premiers enseignement

Points positifs

- 9 inscrits
- Groupe très motivé
- Taux de satisfaction très élevé
- 1 premier recrutement à la clef

Points à améliorer

- Beaucoup de « fausses inscriptions » (16 inscrits à une semaine de la formation)
- Articulation module Blue Team /Red Team
- « outboarding »

Place à l’upskilling (à Charleroi)

1. Introduction à la cybersécurité. 15 novembre
2. Red Team 25 novembre
3. Gouvernance 9 décembre

Merci de votre attention !

Me contacter ?

069/49.02.04

Hubert.deschamps@ee-campus.be

Campus Numérique – Bâtiment 4
Rue du progrès, 24 – 7503 Tournai

www.ee-campus.be

Plus d’infos sur

digitalwallonia.be/cyber

Cyberwal by digital wallonia

Wallonie Relance