MINALOGIC
Auvergne-Rhône-Alpes

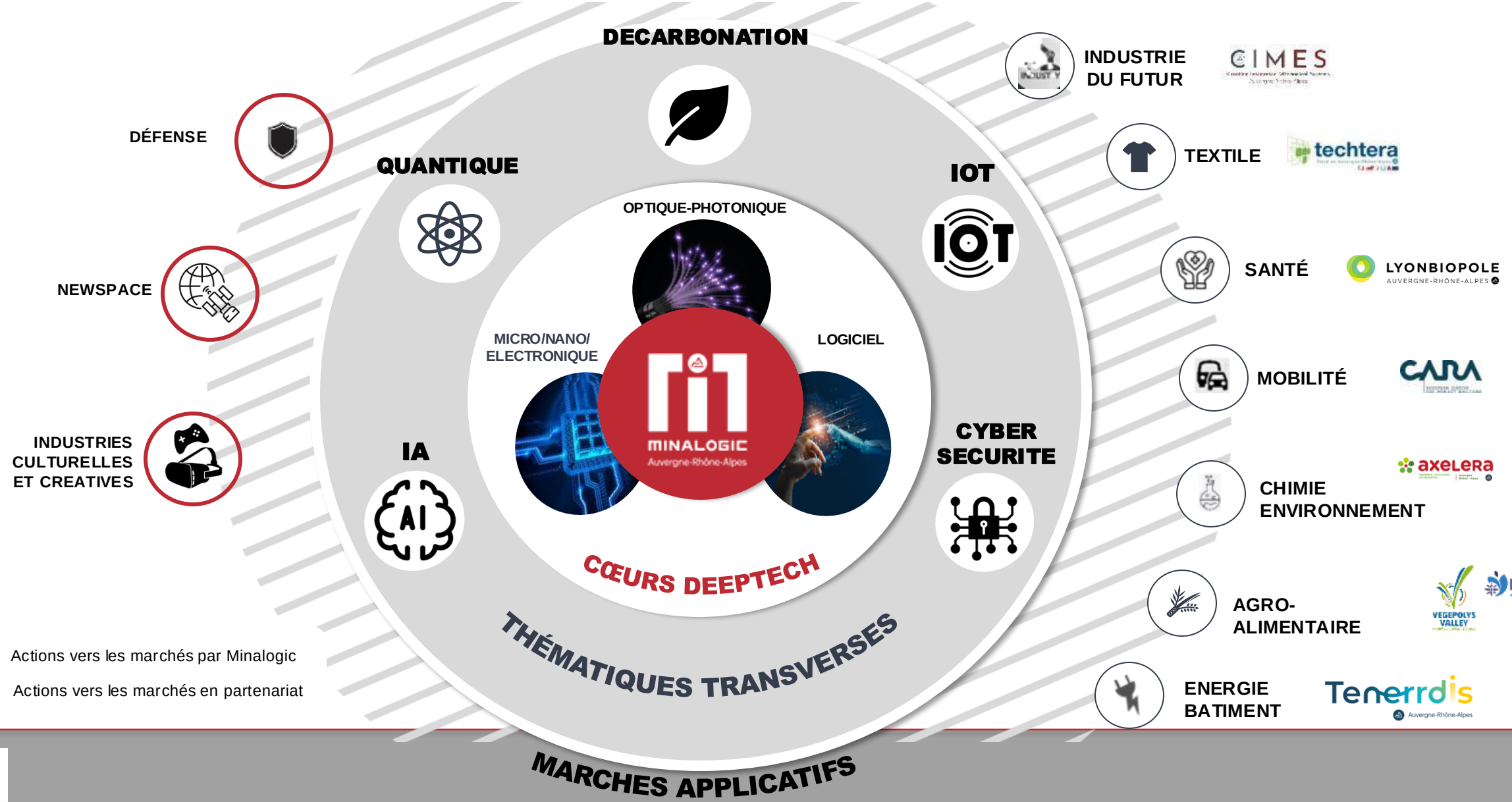
Sécurité des Systèmes Energétiques

Tenerrdis
Auvergne-Rhône-Alpes

AuRA
Digital Solaire

mine smart
Auvergne-Rhône-Alpes

Moteur numérique des industries de demain



mind smart
Auvergne-Rhône-Alpes

PME, ETI, OSP

Les entreprises d'Auvergne Rhône Alpes qui travaillent dans les filières industrielles fortes présentes dans la région se verront proposer un accompagnement sur mesure et complet pour faire de la cybersécurité et de l'intelligence artificielle un levier de performance et d'innovation

Textile **Agri Agro** **Santé** **Industrie** **Chimie et environnement** **Energie**

Un pré diagnostic est effectué avec la structure intéressée afin de qualifier son besoin. Après avoir fait une demande en ligne, un conseiller prendra rdv avec vous

13 partenaires régionaux

axelera · CIMES Auvergne-Rhône-Alpes · cea · Digital League Auvergne-Rhône-Alpes · ENE entreprises & numerique · Inria · Innov'Alliance · Medicalps · Minalogic Auvergne-Rhône-Alpes · SWARM Innovation & transformation center · Techtera · Tenerrdis Auvergne-Rhône-Alpes · Vegepolys Valley

Cofinancé par l'Union Européenne

SECURISER ET RÉVÉLER LE POTENTIEL DE VOS DONNÉES !

15 parcours sur 3 Piliers stratégiques

Cybersécurité **Intelligence Artificielle** **Calcul Intensif**

DIAGNOSTIC
Diagnostic des besoins et construction d'un plan d'actions

PROTOTYPAGE
Accompagnement pour la réalisation de POC et tests de solutions

COMPETENCES
Montée en compétences et formation

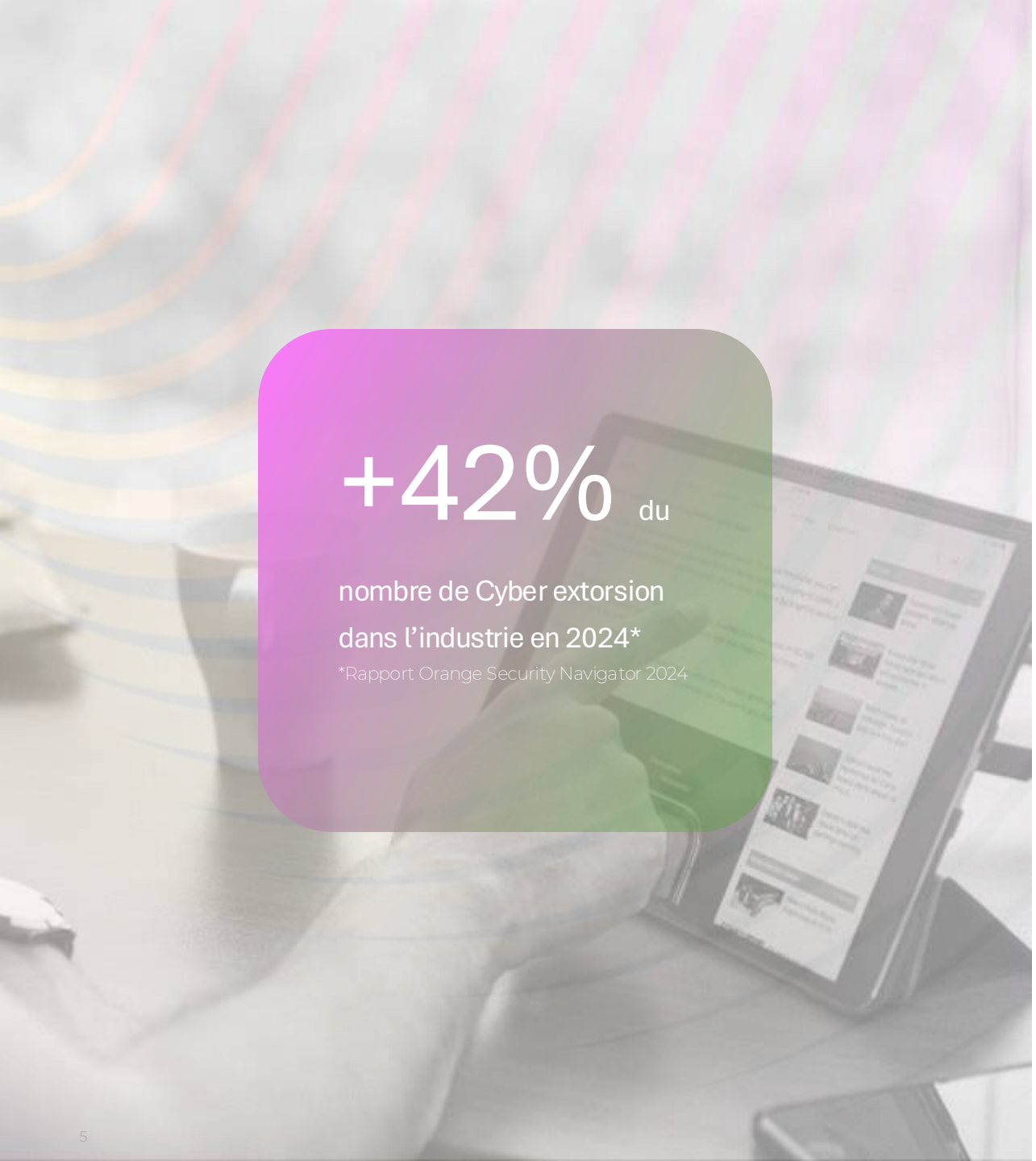
FINANCEMENT
Aide à la recherche de financement et gestion du projet

LES ENJEUX DE LA CYBERSECURITE

Pour les PME-ETI

mine smart Auvergne-Rhône-Alpes

Cofinancé par l'Union européenne



Attaques toujours en augmentation

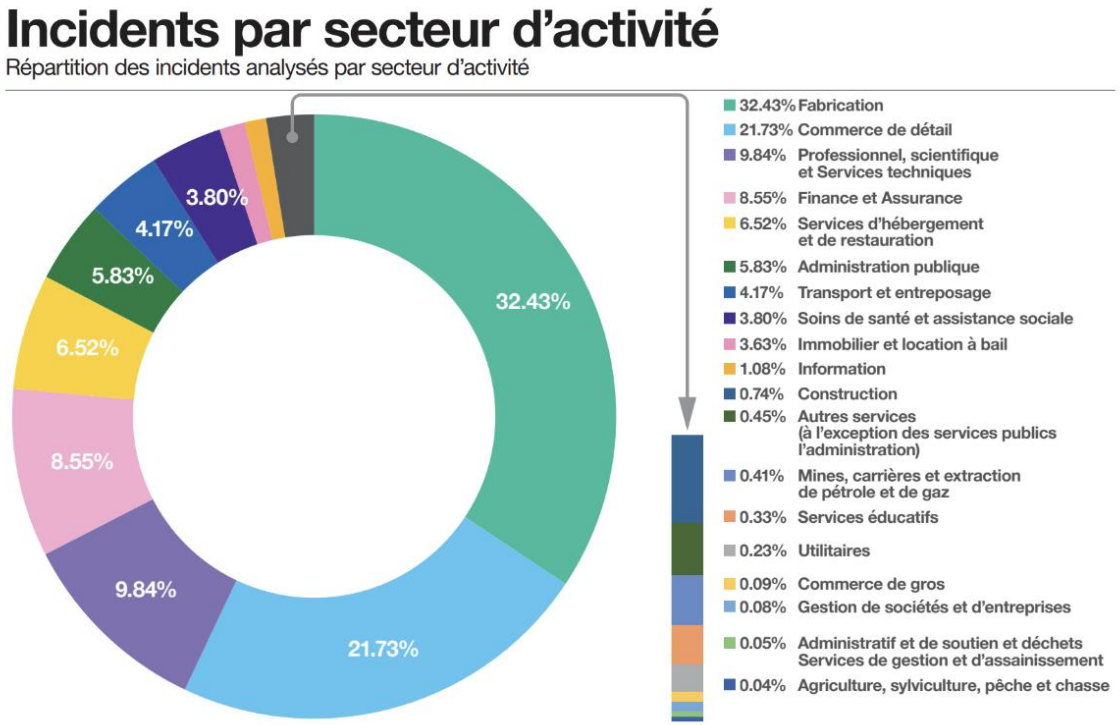
La cybercriminalité est en forte augmentation en France sur tous les secteurs d’activités :

+42% dans l’industrie
+52% dans le service aux entreprises
+62% dans la santé
+115% dans l’éducation
+106% dans la finance
+22% dans l’administration
+33% dans le BTP

Le seul secteur en baisse face à la cybermenace est la vente au détail (**-22%**) qui reste un secteur très fortement touché.

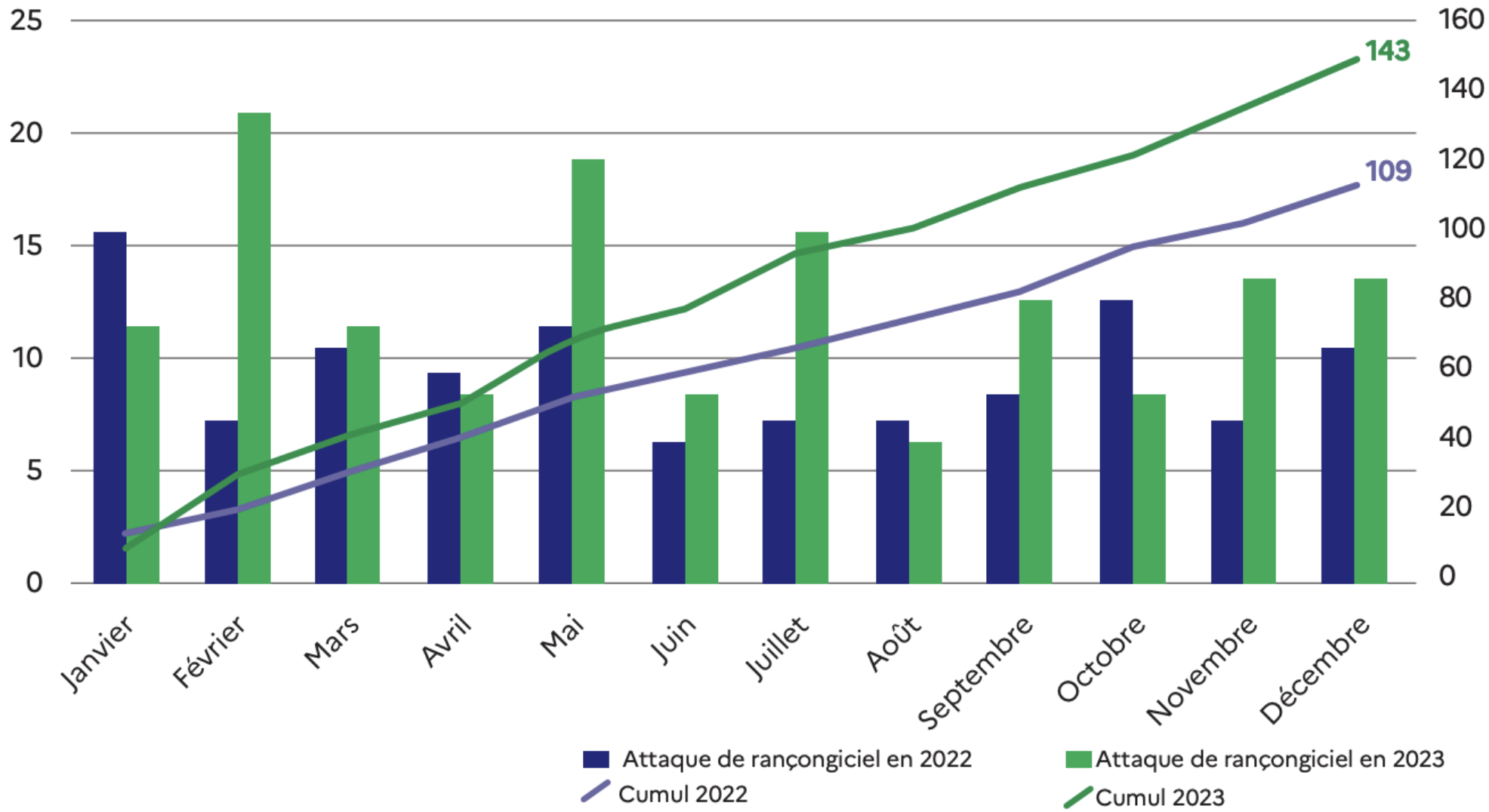
L’industrie et le commerce de détail représentent à eux seuls +50% des incidents reportés en France en 2024.

L’industrie et le commerce de détail à la fête



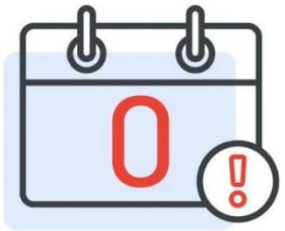
*Rapport Orange Security Navigator 2024

→ **Comparaison des signalements d'attaques par rançongiciel en 2022 et 2023**



Des attaques de plus en plus rapides

TOUJOURS rester en mouvement



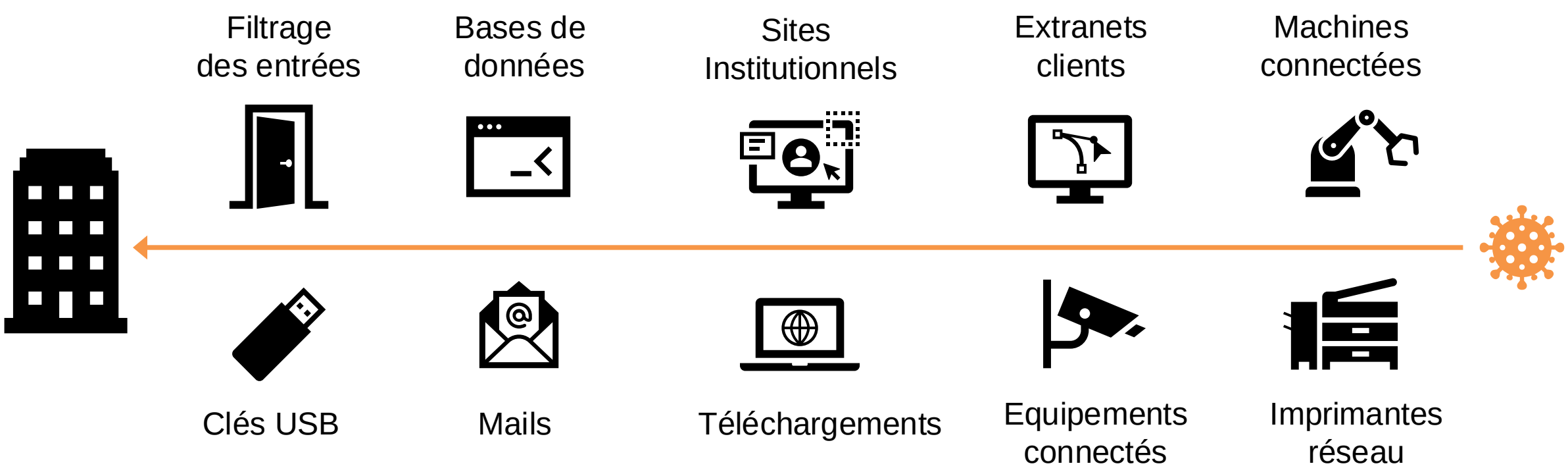
70% des vulnérabilités exploitées dans les attaques de 2023 sont des zero days

2021 & 2022

2023

Le temps moyen d'exploitation des failles est passé de 32 jours à 5 jours

Les points d'entrée des cyber-attaques



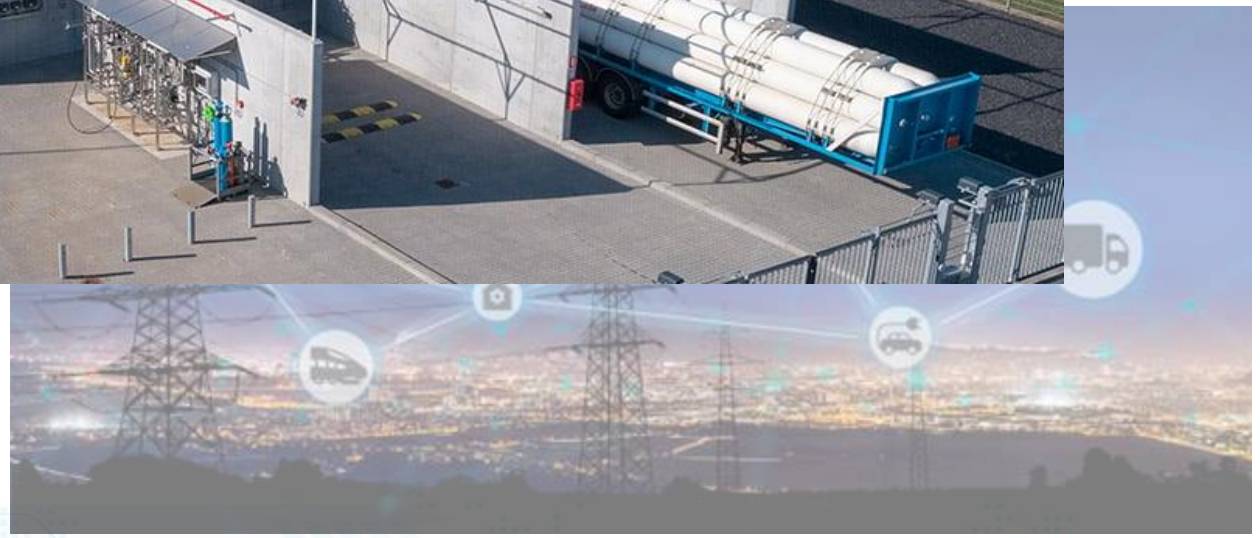
mine smart Auvergne-Rhône-Alpes
Cofinancé par l'Union européenne

mine smart Auvergne-Rhône-Alpes

Cofinancé par l'Union européenne

mine smart
Auvergne-Rhône-Alpes

Cofinancé par
l'Union européenne



mine smart
Auvergne-Rhône-Alpes

Cofinancé par
l'Union européenne

mine smart
Auvergne-Rhône-Alpes

Cofinancé par
l'Union européenne

mine smart
Auvergne-Rhône-Alpes

Cofinancé par
l'Union européenne

Quelles actions démarrer dès maintenant ?

Se préparer

Evaluer le niveau de maturité cyber de ses sous-traitants

- Est-ce que chaque tiers a été évalué en termes de cybersécurité ?
- Est-ce l'Entités Régulées dispose d'un moyen pour vérifier ce niveau de maturité (clause d'audit) ?
- Est-ce que le processus d'achat est centralisé et permet d'avoir une vision exhaustive sur les tiers ?

Quelles actions démarrer dès maintenant ?

Se préparer

Identifier ses activités et SI prioritaires en prenant en compte l'ensemble des règlementations applicables

- Liste de ses principales activités (les joyaux de la couronne)
- Liste des éléments techniques sur lesquelles elles reposent
- Liste des évènements redoutés : Indisponibilité (temporaire ou définitive), fuite de données, perte d'intégrité

Cartographier vos assets IT-OT et Bâtir un plan d'amélioration continue

Se préparer

Définir le point de départ

1. Etat des lieux VS référentiel ANSSI
2. Inventorier & Cartographier les équipements et logiciels
3. Cartographier les accès tiers
4. Audit architecture & configuration des serveurs industriels

Mettre en place les fondations

5. Système de management de la sécurité*
6. « Durcissement » des équipements et des sauvegardes
7. Urbanisation des accès tiers
8. Interconnexion IT/OT (DMZ)
9. Architecture : Zones et conduits

Améliorer

10. Sécurité Physique OT (accès et resilience)
11. Architecture des serveurs industriels
12. Sécuriser le Cloud / MultiCloud
13. Visibilité OT avec detection de Malware
14. Analyse de risque*
15. Processus de gestion des vulnérabilités*

mine smart Auvergne-Rhône-Alpes
Cofinancé par l'Union européenne

Quelles actions démarrer dès maintenant ?

Se préparer

Inventaire de vos services exposés sur internet (email, pares-feux, VPN, applications SaaS, sites internet…)

- ➔ Utilisez d'un service de gestionnaire de mot de passe
- ➔ Ciblez les systèmes d'authentification forte
- ➔ Se préparer à se déclarer auprès de l'ANSSI, en indiquant les points de contacts
- ➔ Procédurer la déclaration d'incident de sécurit

Formalisez Le plan de gestion de crise inclut-il les crises d'origine cyber ?
Les collaborateurs opérationnels sont-ils formés sur les procédures de continuité ?

20%

3

1

Vous appuyer sur vos FORCES

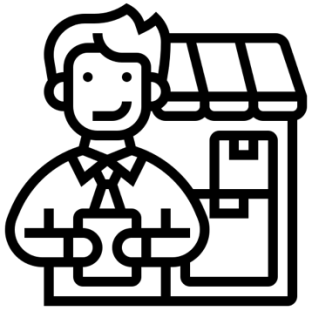
Direction

DSI

Collaborateurs

2

Identifiez vos MARGES DE MANOEUVRE



Fournisseurs

Outil de production

Finance

3

Trouvez des SOLUTIONS

SIMPLES PRAGMATIQUES UTILES

LE PRINCIPAL N’EST PAS LA VITESSE MAIS LE MOUVEMENT

MINALOGIC
Auvergne-Rhône-Alpes

Label et parcours Cyber

mind smart
Auvergne-Rhône-Alpes

Tenerrdis
Auvergne-Rhône-Alpes

DGA
DIRECTION GÉNÉRALE DE L'ARMEMENT

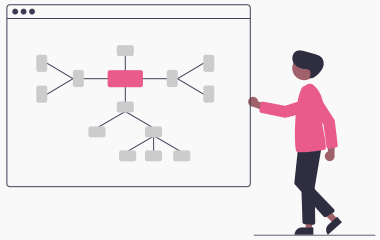
EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Cyber Pilot

La première plateforme de diagnostic et pilotage en Cybersécurité pensée et développée pour les PME-ETI.

Pensée par des RSSI pour des DSI 💔

Un diagnostic 360°



Gouvernance

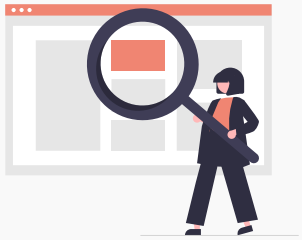
Disponible dans tous les packs

Audit de 166 points de contrôle basé sur :

ISO 27001 : 2022

ANSSI / NIS-2

DGA Fondamental



Externe

Disponible dans tous les packs

Analyse de surface d'exposition externe.

Nos consultants testent votre exposition sur le web au travers de plusieurs tests de surface d'attaque.

M365

Disponible dans le pack pro

Analyse Microsoft 365

Nos algorithmes analysent la configuration de vos solutions Microsoft 365 et vous remonte le niveau de sécurité de votre tenant.

Interne

Disponible dans le pack pro

Pentest interne sur votre infrastructure informatique.

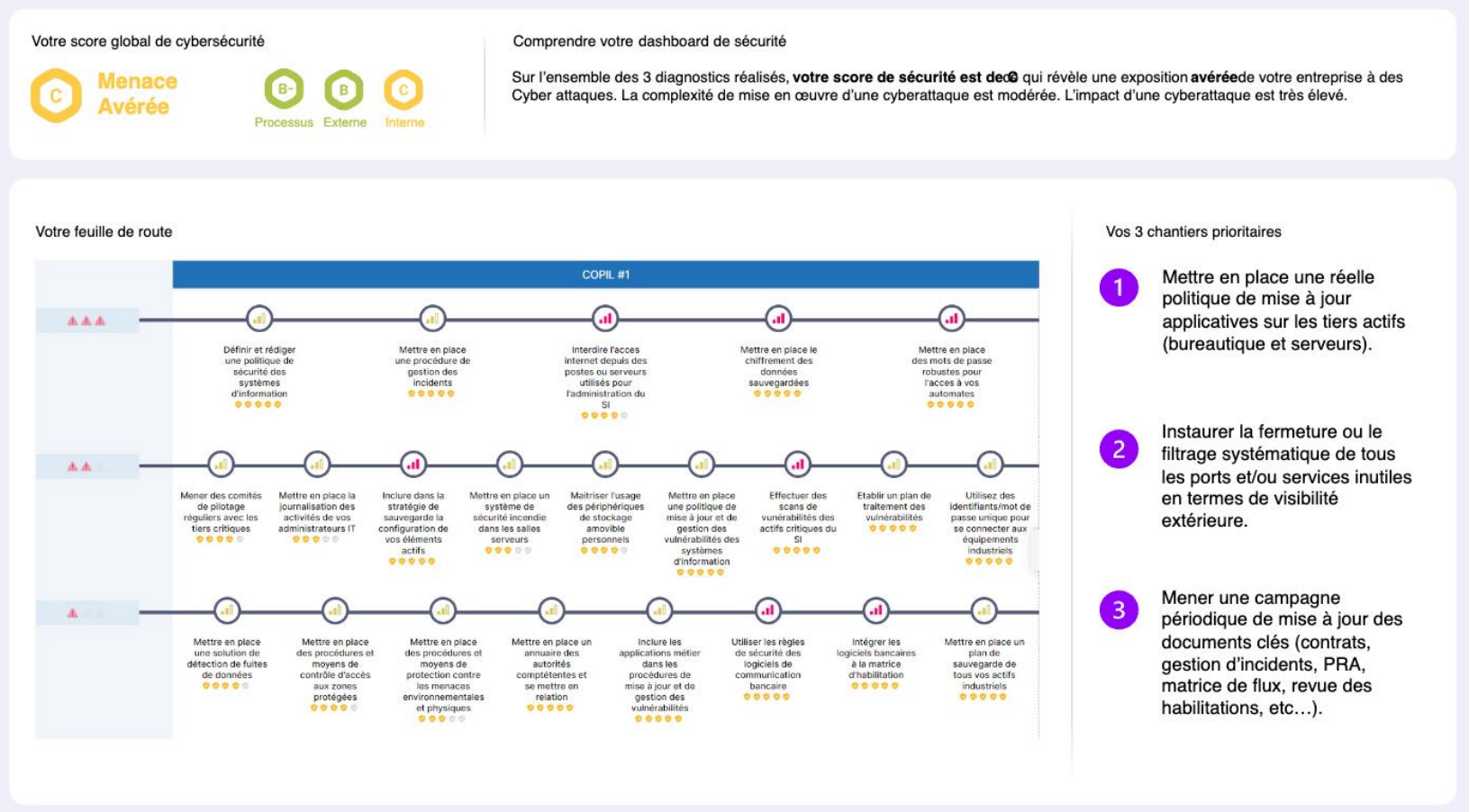
Nos pentesteurs simulent des centaines de scénarios d'attaques pour un test grandeur nature d'une Cyber attaque.

Résumé pour la direction

Un résumé du diagnostic adapté pour les directions générales

Nous avons modélisé des vues dédiées aux directions générales afin de comprendre les menaces, les expositions et les risques qui pèsent sur l'entreprise.

Cela aide nos clients DSI / RSI à mettre en avant les besoins et les budgets nécessaires à la résolution des vulnérabilités les plus critiques.

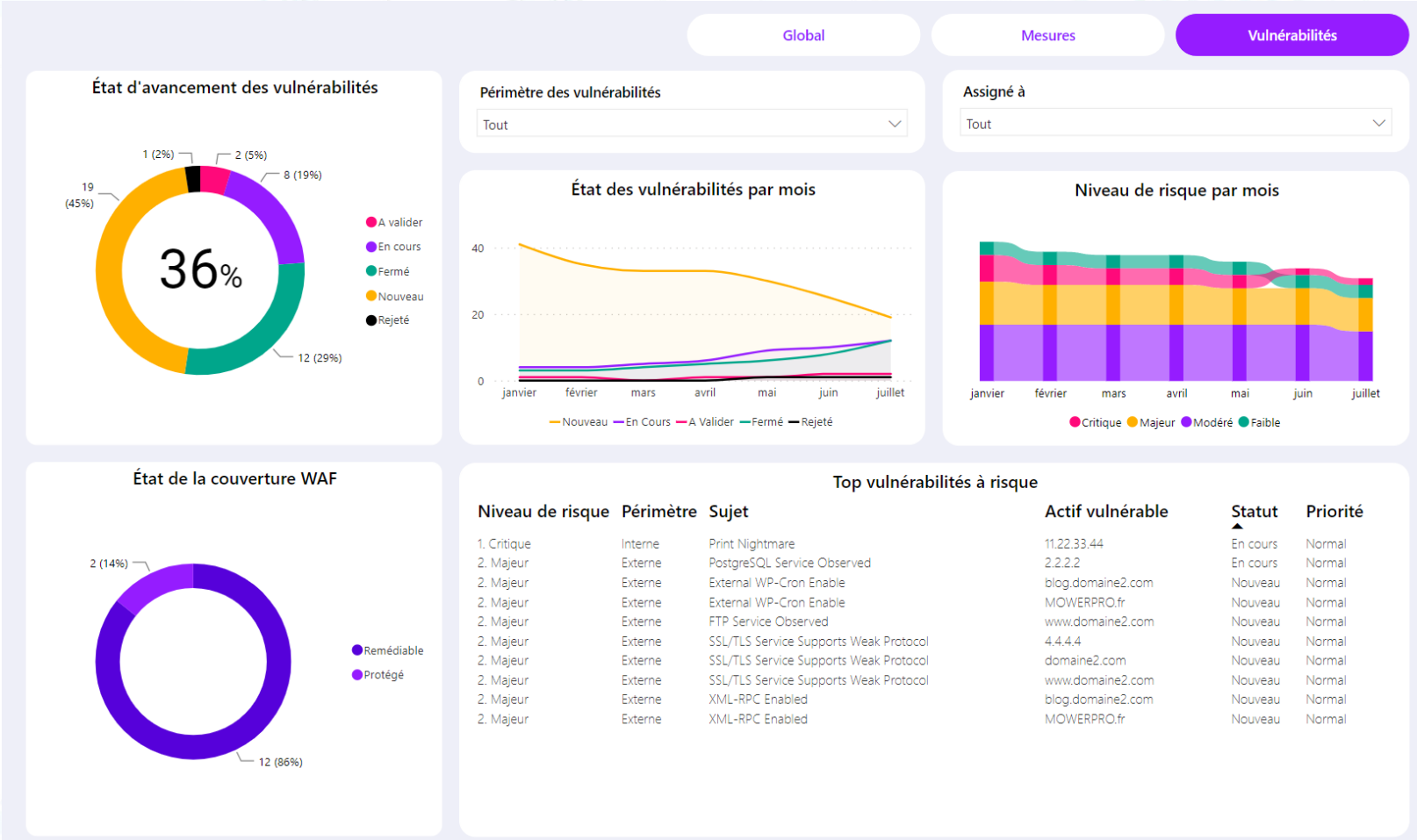


Pilotez votre niveau de sécurité

Des indicateurs clairs :

Pilotez votre plan de remédiation grâce à des indicateurs clairs et dynamiques :

- Vos scores évoluent en fonction de vos actions
- Définissez 3 chantiers prioritaires
- Objectivez les actions à mener pour améliorer votre sécurité



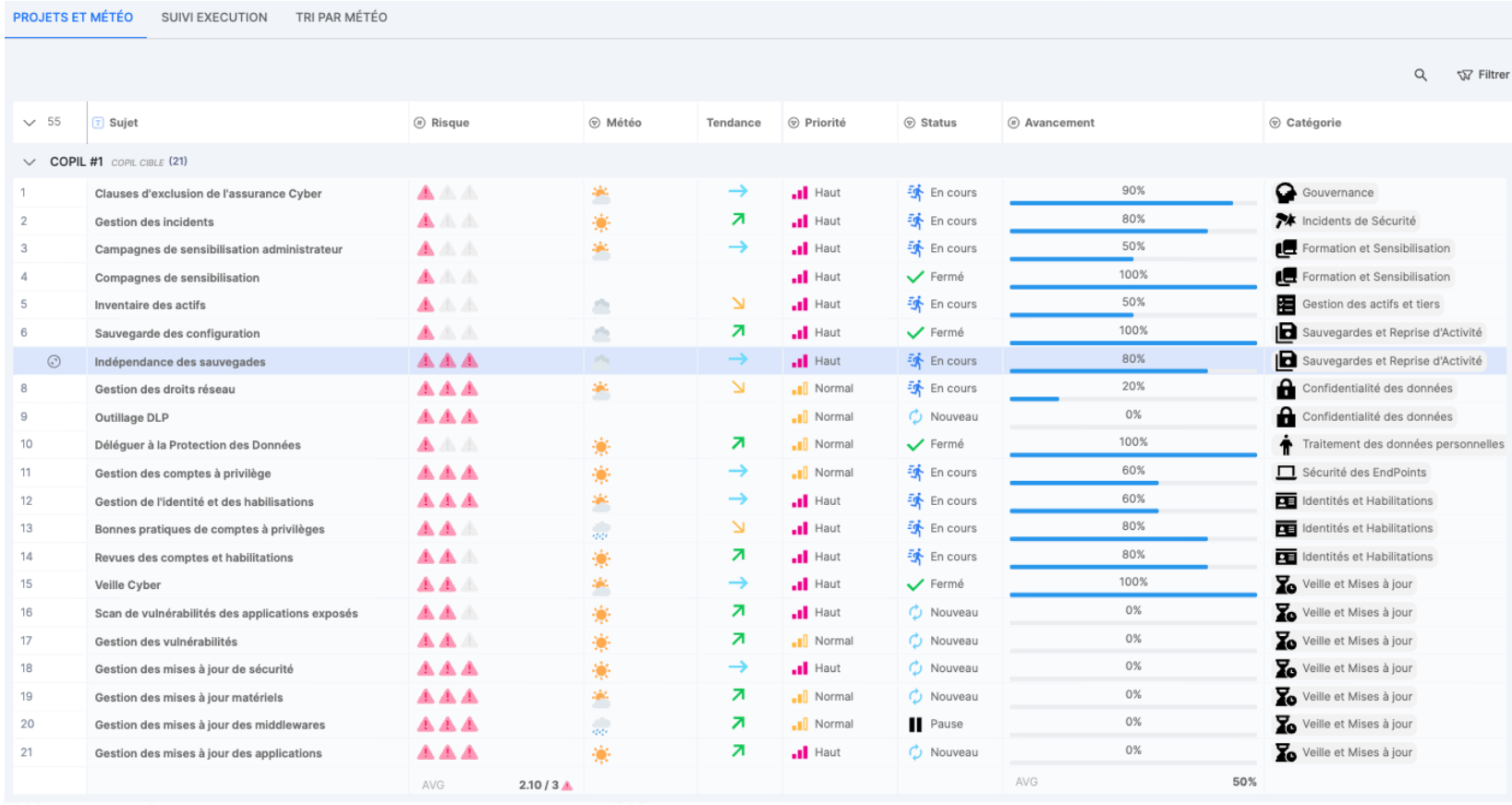
Pilotez votre niveau de sécurité

Gestion de projet intégrée

Notre plateforme comporte des modules dédiés à la gestion de projet SSI avec différentes options de tri :

- Météo
- Criticité
- Risque
- Avancement
- Priorité
- Catégories

Et la possibilité de modifier les status des recommandations pour faire avancer le plan de remédiation.



Tarifs diagnostic Cyber Pilot

4 500€

Abonnement annuel

- Score externe
- Score gouvernance
- Guides pratiques
- Plateforme de pilotage
- Diagnostic annuel

Standard

6 000€

Abonnement annuel

- Score Microsoft 365 *
- Score interne
- Score externe
- Score gouvernance
- Guides pratiques
- Plateforme de pilotage
- Diagnostic annuel

Professional

*Early adoption octobre 2025

Cofinancé par l'Union européenne

Les outils de financement du parcours Cyber

Start-up et PME défense

DGA
DIRECTION GÉNÉRALE DE L'ARMEMENT

bpifrance
DIAG CYBERSÉCURITÉ

50% de prise en charge

Start-up et PME industrielles

OSEZ INDUSTRIE DU FUTUR
La Région Auvergne-Rhône-Alpes
ene

50% de prise en charge

Start-up et PME

mind smart
Auvergne-Rhône-Alpes

50% de prise en charge

Pour plus d'informations

Antoine CAMUS – MINALOGIC

06 71 83 66 06

antoine.camus@minalogic.com

mine smart Auvergne-Rhône-Alpes

Cofinancé par l'Union européenne

Inria Academy

SUPERVIZ

mines smart
Auvergne-Rhône-Alpes

Cybersécurité des systèmes énergétiques

Stéphane Mocanu
Inria/LIG, team CTRL-A
stephane.mocanu@inria.fr

PLAN

- Motivation
- Systèmes industriels et énergétiques
- Les bases de la cybersécurité
- Les évènements fondateurs
- Le déploiement de la sécurité des systèmes d'information

Motivation

- **Attaques et conséquences**
  - Ukraine 2015 (BlackEnergy 3) : 30 postes électriques arrêtés, 230000 personnes affectées
  - Ukraine 2017 (Industroyer) : blackout d'une heure d'un cinquième de la ville de Kiev
  - ……
  - 2020 : blackout de la ville de Mumbai pendant 10h. 20 millions de personnes affectées. Rançongiciel.
  - 2021 : Centrais Eletricas Brasileiras (Eletrobras) and Companhia Paranaense de Energia (Copel) victimes de rançongiciels
  - 2021: attaques massives contre le réseau électrique indien
  - 2021 : Volue (Norvège) attaque rançongiciel (Ryuk). Arrêt des systèmes d'approvisionnement en eau de 200 villes. 85% de la population norvégienne affectée.
  - 2023 : Campagne d'attaques sur les automates Unitronics
  - 2024 : Plusieurs tentatives d'attaques contre des barrages hydroélectriques en France
  - Bilan sûreté RTE 2019 : 10000 attaques et 200 virus par mois en 2018 (deux fois plus par rapport à 2017)

Systèmes industriels et énergétiques

SYSTÈMES INDUSTRIELS (SCADA)

Systèmes Cyberphysiques

IT

OT
Operational Technology

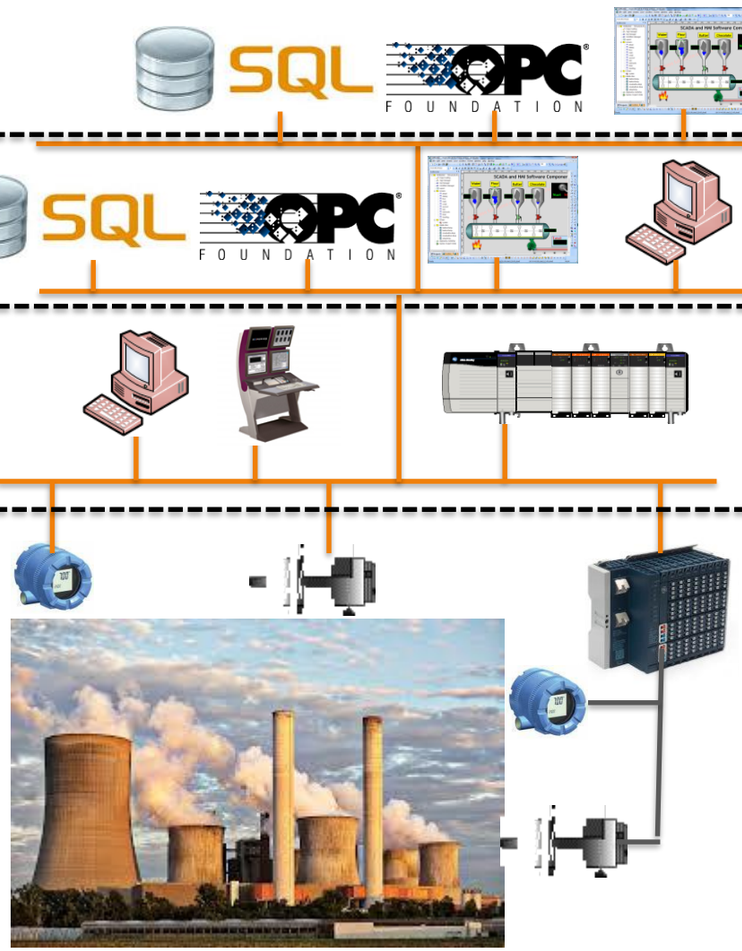
Connexions distante

Supervision
Pas de temps réel

Contrôleurs
Temps-réel souple

Capteurs/actionneurs
Temps-réel stricte

Processus physique



Contrôleur cellule

Contrôleur poste

Contrôleur charge

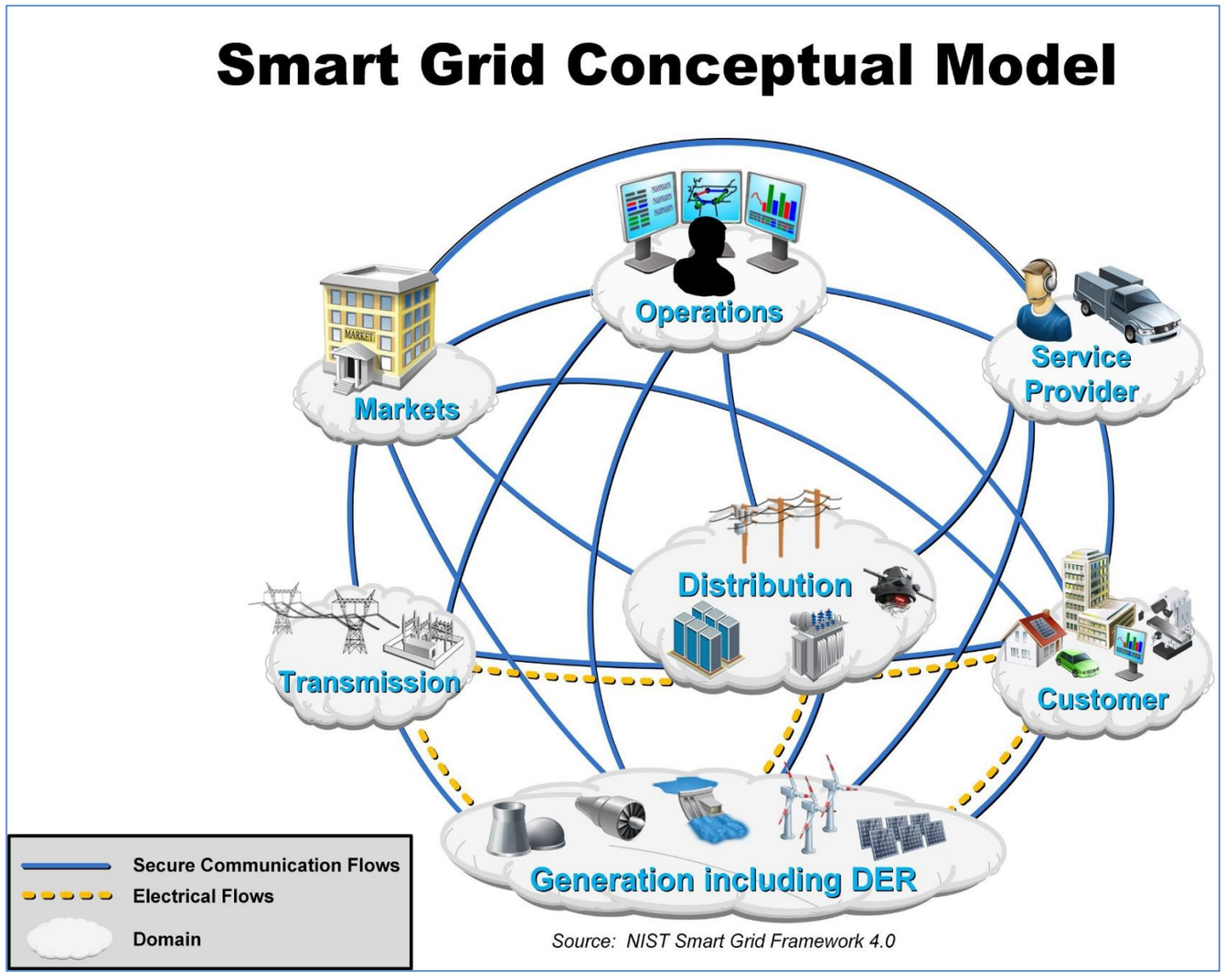
Relais protection

Parc PV

Convertisseur

Poste électrique

SMARTGRIDS ET RÉSEAUX INFORMATIQUES

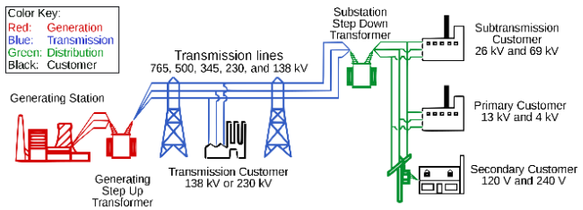


- **Un « double » réseau : électrique et informatique**
- **Plusieurs acteurs interconnectés**
  - **Producteurs**
  - **Exploitants**
  - **Consommateurs**
  - **Marchés**
  - **Sous-traitants**
- **Une exposition importante**

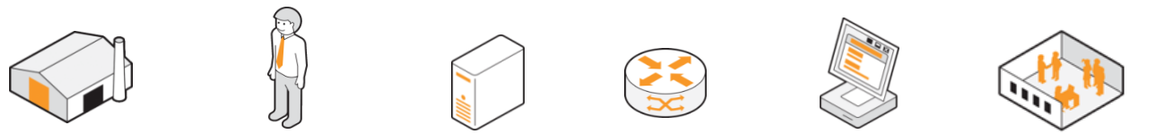
Les bases de la cybersécurité

Cybersécurité, les bases: système d'information

Actifs primordiaux



Actifs supports

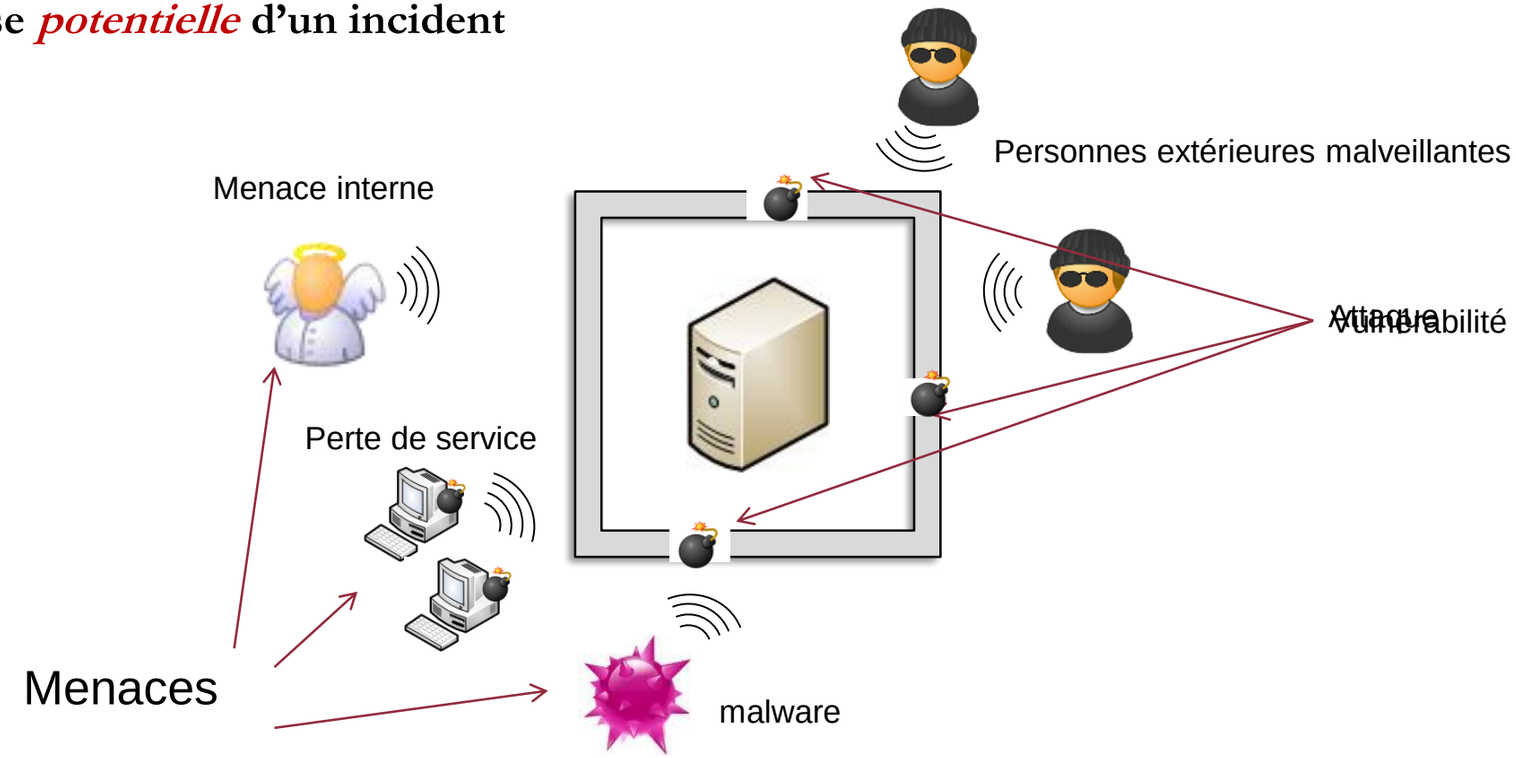


ISO/IEC 27005:2008 et mallette CyberEdu

La sécurité du S.I. concerne
la sécurité de l'ensemble de ces biens

Cybersécurité les bases : vulnérabilité/menace/attaque

- **Vulnérabilité : faiblesse d'un bien**
  - ▶ « bug » logiciel, mauvaise configuration, mauvais usage, non-respect des procédures
- **Menace : cause *potentielle* d'un incident**



- **Attaque : action malveillante qui porte atteinte à la sécurité d'un bien. Concrétisation de la menace.**
  - ▶ **L'attaque nécessite l'exploitation d'une vulnérabilité.**

Vulnérabilités courantes dans le

- **Exemples de vulnérabilités courantes d**
  - Accès aux automates sans mots de p
  - Absence de chiffrement (tout les traf
  - Absence de contrôle d'accès (un aut
  - Absence des rôles (même identité ut
  - Absence de log (de sécurité) sur les
  - Equipements connectés à Internet

TOTAL RESULTS

4

TOP CITIES

Courdimanche	1
Limoges	1
Lisses	1
Paris	1

TOP PORTS

1883	3
10000	1

TOP ORGANIZATIONS

Bouygues Telecom SA	1
Free SAS	1
Hurricane Electric LLC	1
Orange S.A.	1

View Report | View on Map | Advanced Search

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

[redacted]

2024-11-27T05:40:05.284003

doors.huapi.net.ar
Hurricane Electric LLC
France, Paris

```
MQTT Connection Code: 0

Topics:
$SYS/broker/version
$SYS/broker/connection/doors.limbo/state
$SYS/broker/uptime
$SYS/broker/load/messages/received/1min
$SYS/broker/load/messages/received/5min
$SYS/broker/load/messages/received/15min
$SYS/broker/load/messages/sent/1min
$SYS/broker/load/messages/s...
```

[redacted]

2024-11-22T21:32:07.686282

lfbn-poi-1-412-11 1.w86-239.abo.wanadoo.fr
Orange S.A.
France, Limoges

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "2118880824"
Last-Modified: Fri, 09 Mar 2018 12:34:56 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Length: 40879
Date: Fri, 22 Nov 2024 21:32:18 GMT
Server: webserver

<!DOCTY...
```

[redacted]

2024-11-22T17:58:51.926077

82-65-181-109.subs.proxad.net
Free SAS
France, Lisses

```
MQTT Connection Code: 0

Topics:
$SYS/broker/version
$SYS/broker/uptime
$SYS/broker/load/messages/received/1min
$SYS/broker/load/messages/received/5min
$SYS/broker/load/messages/received/15min
$SYS/broker/load/messages/sent/1min
$SYS/broker/load/messages/sent/5min
$SYS/broker/load/messages/sent/1...
```

[redacted]

2024-11-17T14:42:25.832370

4va54-h02-176-189-64-86.dsl.sta.abo.bbox.fr
Bouygues Telecom SA
France, Courdimanche

```
MQTT Connection Code: 0

Topics:
$SYS/broker/version
$SYS/broker/uptime
$SYS/broker/clients/total
$SYS/broker/clients/maximum
$SYS/broker/clients/inactive
$SYS/broker/clients/disconnected
$SYS/broker/clients/active
$SYS/broker/clients/connected
$SYS/broker/clients/expired
$SYS/broker/load/message...
```

Objectifs de sécurité – CIA triad

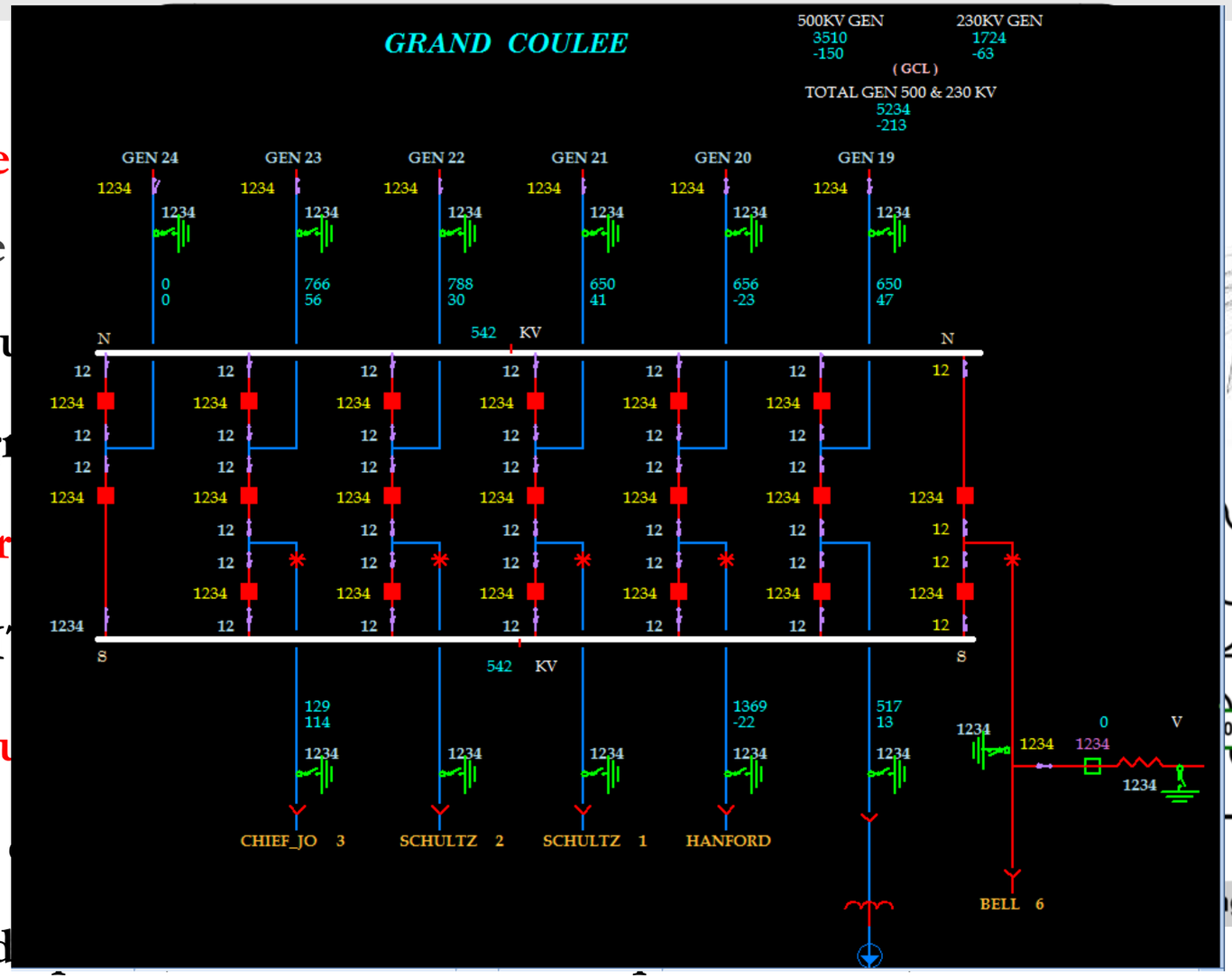
- **Confidentialité : Propriété des biens et informations de n'être accessibles qu'aux personnes autorisées**
- **Intégrité : Propriété d'exactitude et de complétude des biens et informations**
- **Disponibilité : Propriété d'accessibilité au moment voulu des biens par les personnes autorisées**
- **Preuve : Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe :**
  - **traçabilité des actions menées**
  - **authentification des utilisateurs**
  - **imputabilité du responsable de l'action effectuée**

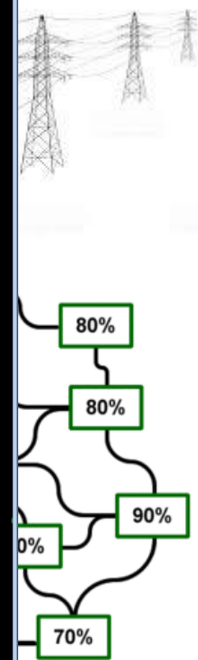
► **Habituellement évalués sur quatre niveaux selon le niveau de la menace.**

Les évènements fondateurs

BLACKOUT ETATS-UNIS 2003

- **Fausses mesures de**
  - ► Fausse image de
- **Arrêt d'un générateu**
- **Surcharge d'une ligr**
- **Vulnérabilité : un ar**
- **Perte d'une ligné H**
- **Vulnérabilité : un bu**
- **Le réseau s'écroule**





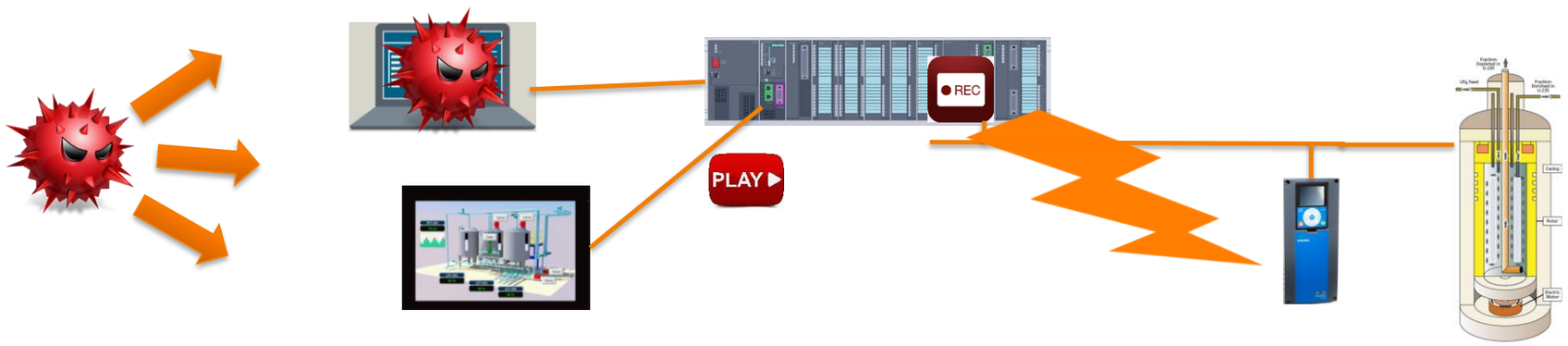
wikipedia

6 milliards de dollars d personnes affectées, 100 morts

BLACKOUT 2003

- Evènement initial : fausses valeurs des capteurs (erreur de maintenance)
- Exploite des vulnérabilités physiques et cyber
- Déni de vue
- Déni du contrôle
- Endommagement du système physique
- Pas de violation de la syntaxe ou sémantique des protocoles de communication

STUXNET



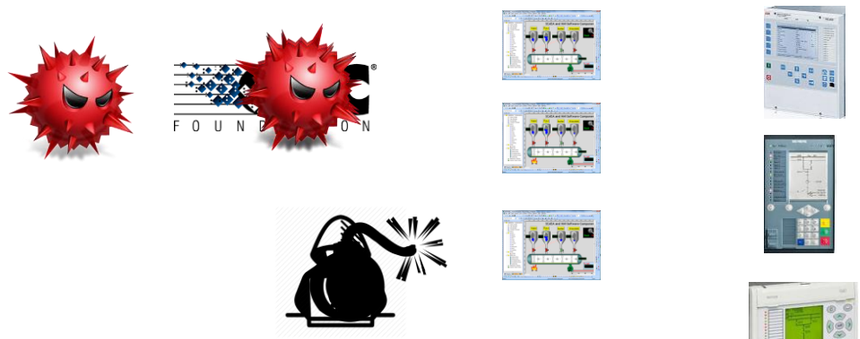
- Recherche de stations d'ingénierie Step 7
- Corruption de la bibliothèque de communication
- Chargement du code malveillant dans l'automate S7-300
- Recherche des variateurs de vitesse sur Profibus
- Enregistrement des valeurs normales des capteurs
- Exécution des séquences malveillantes de commandes des variateurs et rejeu des séquences normales

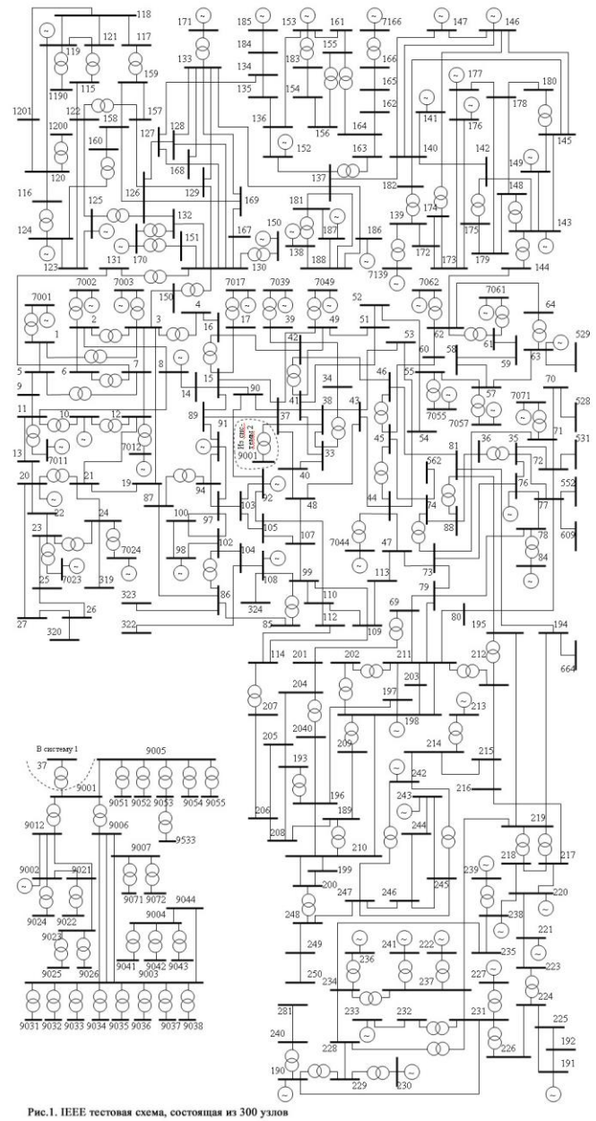
- Connaissance préalable du système (attaque informatique et contrôle/commande)
- Pas de violation de la syntaxe ou de la sémantiques des protocoles de communication
- Déni de vue
- Déni du contrôle
- Endommagement du systèmes physique

15

INDUSTROYER/CRASHOVERRIDE

- **Réseaux électrique**
  - Fonctions de protection et automatisme connues
  - Etat et distribution de charges inconnues (par l'attaquant)





- ✦ Compromission d'un serveur OPC
- ✦ Cartographie du système
- ✦ Ouverture des backdoors sur des IHM
- ✦ Actions distantes
- ✦ Commandes malveillantes envoyées aux relais de protection

INDUSTROYER/CRASHOVERRIDE

- Reconnaissance du système physique via un serveur OPC
- Pas de violation de la syntaxe ou de la sémantiques des protocoles de communication
- Déni de vue
- Déni du contrôle
- Endommagement du systèmes physique
- Perte de protection
- Perte de Productivité et de Chiffre d'Affaires

Les consequences des attaques: Mitre ATT&CK ICS

https://attack.mitre.org/matrices/ics/

- **Vol d'informations opérationnelles : Vol de propriété intellectuelle industrielle**
-
- **Manipulation de vue : Modifier les données envoyées à la supervision (salle de contrôle)**
- **Déni de vue : Désactivation temporaire de l'affichage de l'état du processus**
- **Perte de vue : Désactivation permanente de l'affichage de l'état du processus**
-
- **Manipulation de la commande : Modification des consigne ou des paramètres**
- **Déni du contrôle : Interdiction temporaire d'accès aux commandes**
- **Perte du contrôle : Interdiction permanente d'accès aux commandes**
-
- **Perte de disponibilité : Perturbation de certains composants (contrôleurs ou IHM)**
- **Perte de protection : Perturber des fonctions qui agissent en cas de panne (réseaux électriques)**
- **Perte de sécurité : Perturbation des fonctions protégeant l'opérateur et l'intégrité du système (arrêt d'urgence, portiques de protection)**
-
- **Perte de Productivité et de Chiffre d'Affaires : perturber partiellement ou totalement les chaînes de production**
- **Dommages matériels : endommager ou détruire les infrastructures, les équipements et l'environnement**

Principales voies d'infiltration dans les systèmes industriels

Les 10 principales tactiques d'accès initial dans les systèmes industriels	Tendance depuis 2019	Tendance depuis 2016
Virus sur clé USB ou disque externe	→	↗
Virus propagé par Internet ou Intranet	↑	↗
Erreur Humaine et Sabotage	→	↑
Extranet ou Cloud	→	↑
Ingénierie Sociale et Hameçonnage	→	↘
(D)Déni de Service	↗	↑
Equipements de Contrôle Commande connectés à Internet	↗	→
Intrusion par Access Distant	↗	→
Défaillance Technique et Force Majeure	→	↘
Vulnérabilités dans le supply-chain	↑	
Smartphones Compromis en Environnement Professionnel		→

Source BSI-CS005E Top 10 Threats and Countermeasures 2022

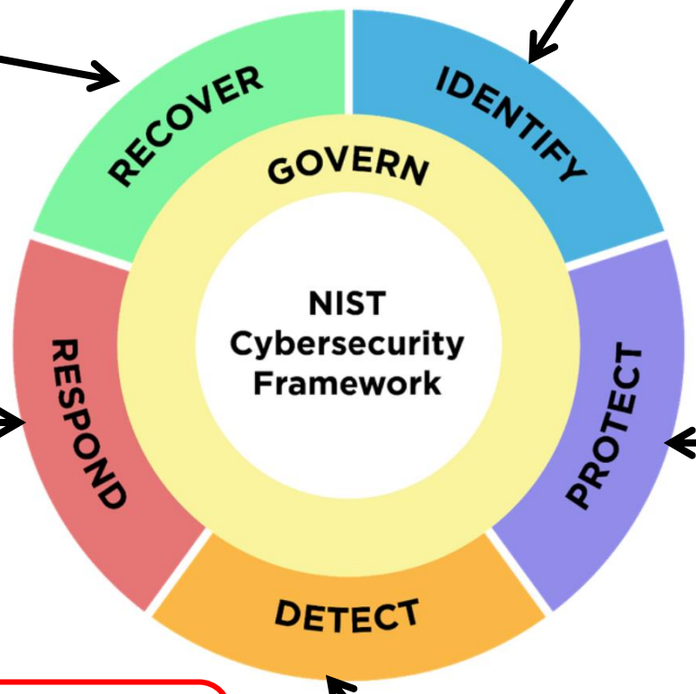
Le déploiement de la sécurité des systèmes d'information

NIST cybersecurity framework

https://www.nist.gov/cyberframework/

Evaluation des risques cyber

Restaures le système et reprendre l'activité



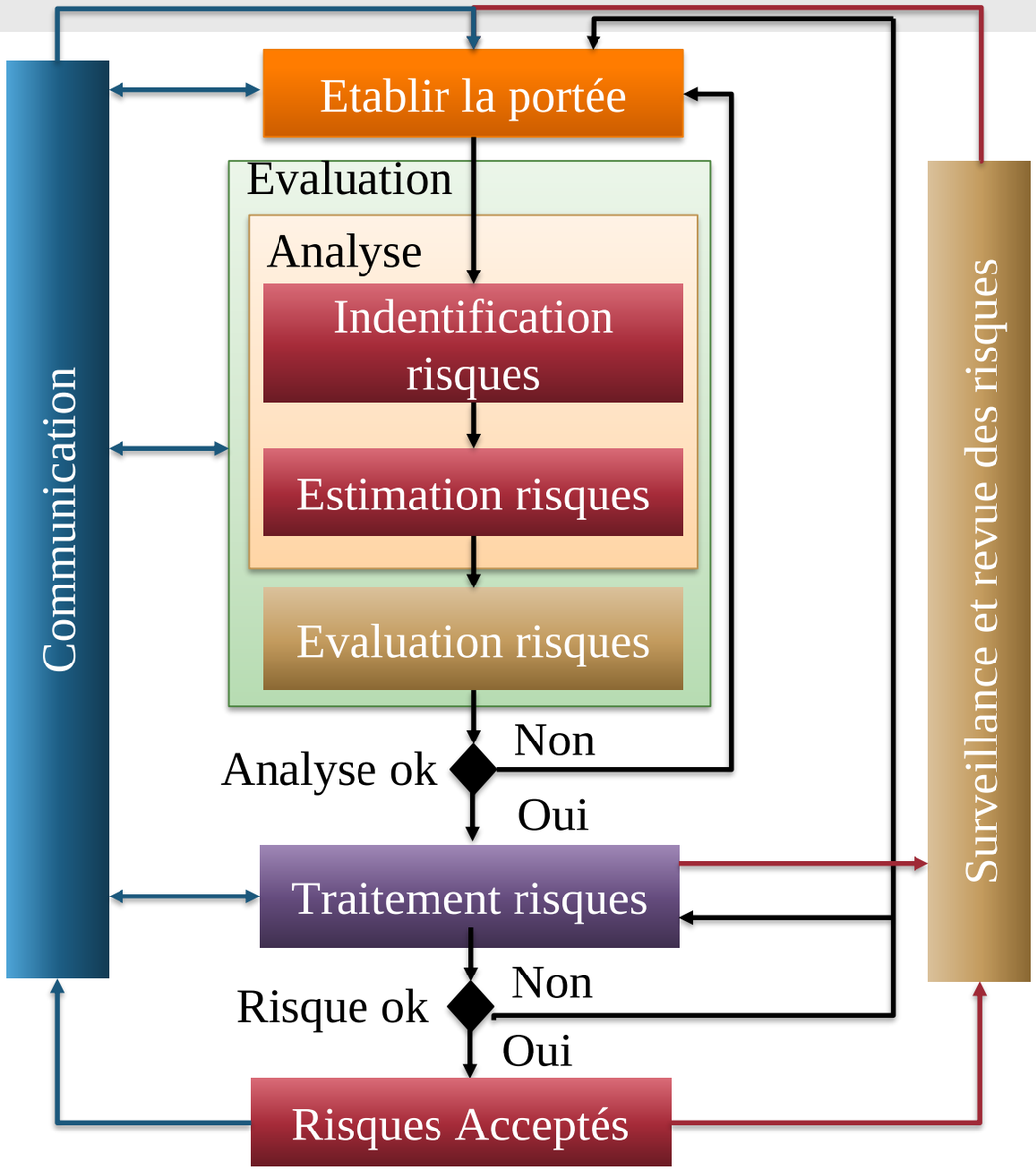
Traiter les incidents

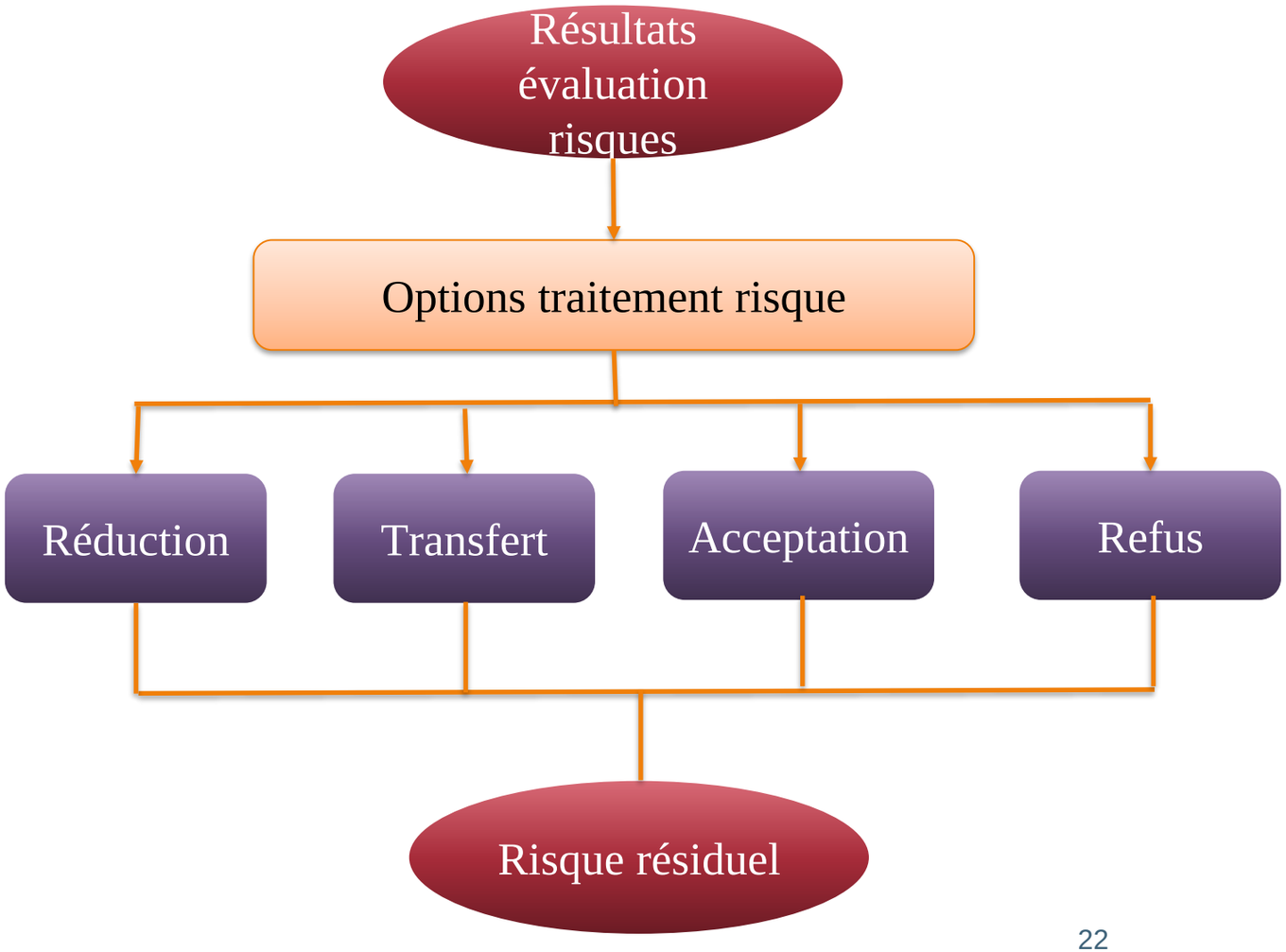
Déploiement des mesures

Gouverner : Etablir la stratégie les politiques et les objectifs

Détecter et analyser les attaques

PROCESSUS DE GESTION DE RISQUE (IEC 31010 ET ISO 27005)





22

Un dernier mot

- **Processus continu : la maintenance de la sécurité est la clé**
- **Le rôle du management est fondamental**
  - Etablir la politique de sécurité
  - Allouer les moyens
  - Evaluer les risques (coût des mesures versus coût des pertes)
  - Mesures organisationnelles
  - Revue du processus
  - Clauses partenariales
  - Communication

Merci de votre attention !