Reconnue d'utilité normande

BIENVENUE À

LA PLACE DE L'INNO

Plongez au cœur de la performance

14 OCT 2025 | Houlgate Centre Sportif de Normandie 9h à 17h

Cofinancé par l'Union européenne

RÉGION NORMANDIE

NORMANDIE AGENCE DE DÉVELOPPEMENT

LES ENJEUX DE LA CYBERSÉCURITÉ INDUSTRIELLE

Pascal VANDEPUTTE
Référent Sécurité Systèmes d'Information

SMÉDAR

Frédéric BLIN
Responsable Développement Réseaux & cybersécurité industriels

REXEL FRANCE

Le SMÉDAR

Syndicat Mixte d'élimination des déchets

160 communes, 615.000 habitants

Réduction des déchets (sensibilisation)

Plateformes de Compostage

Centre de Tri : 100-130 t/j

Unité de Valorisation Énergétique

- Incinération : ~1000 t/j, déchets médicaux pour le 76
- Production réseau de chaleur (>10.000 logements)
- Production électrique (autoconsommation, revente)

REXEL INDUSTRIE : Qui sommes-nous ?

VOUS ACCOMPAGNER DANS VOTRE COMPETITIVITE VIA UN OUTIL DE PRODUCTION MODERNE, DECARBONE ET DES INFRASTRUCTURES PERENNES.

Des ressources spécialisées, des compétences expertes, des solutions innovantes et adaptées aux besoins spécifiques de chaque industrie :

130 itinérants

Portent **l'ensemble** de **l'offre** Rexel sur la clientèle industrielle :

- Clients finaux
- OEM
- Installateurs industriels
- Tableautiers industriels

80 experts

dédiés à l'outil de production

- Réseaux industriels
- Cybersécurité
- Automatisme
- Mécatronique
- Robotique / Cobotique
- Digitalisation
- Vision industrielle

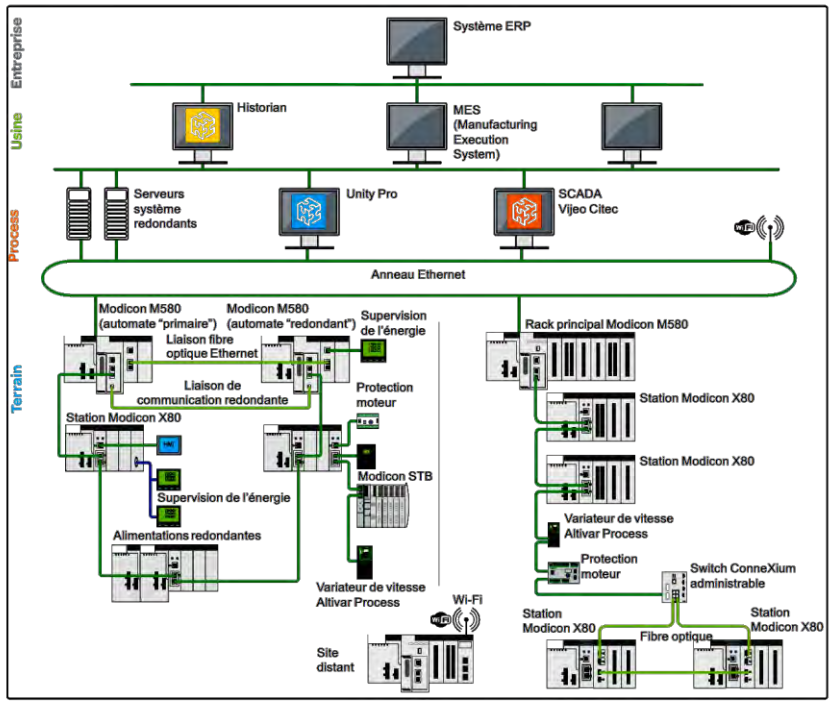
Certifiés :

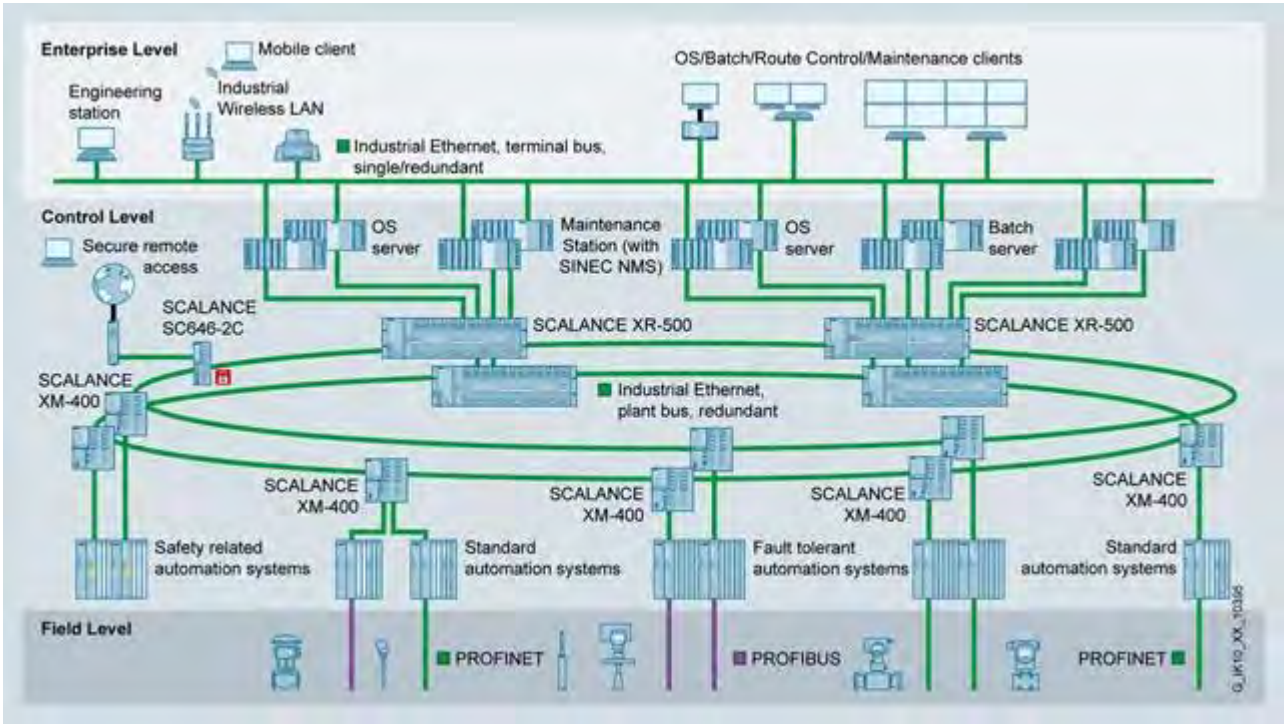
REXEL INDUSTRIE : Pourquoi nous choisir pour vos problématiques de cybersécurité ?

REXEL INDUSTRIE : Pourquoi nous choisir pour vos problématiques de cybersécurité ?

Expertise du réseau OT

➔ Expérience des automatismes, des réseaux industriels et des contraintes associées





Alliance Certified Industrial Automation Distributor

Schneider Electric

OMRON

Approved Partner

SIEMENS

Rexel

REXEL INDUSTRIE : Pourquoi nous choisir pour vos problématiques de cybersécurité ?

Expertise du réseau OT

➔ Expérience des automatismes, des réseaux industriels et des contraintes associées

Accompagnement sur mesure, avec nos partenaires

➔ Une démarche pas à pas, de l'état des lieux jusqu'à la mise en œuvre des solutions adaptées à votre site

REXEL INDUSTRIE : Pourquoi nous choisir pour vos problématiques de cybersécurité ?

Expertise du réseau OT

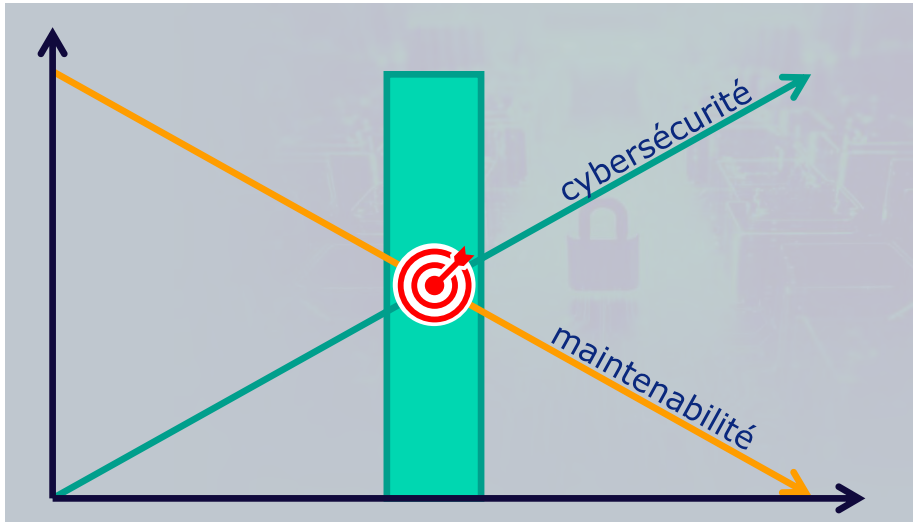
➔ Expérience des automatismes, des réseaux industriels et des contraintes associées

Accompagnement sur mesure, avec nos partenaires

➔ Une démarche pas à pas, de l'état des lieux jusqu'à la mise en œuvre des solutions adaptées à votre site

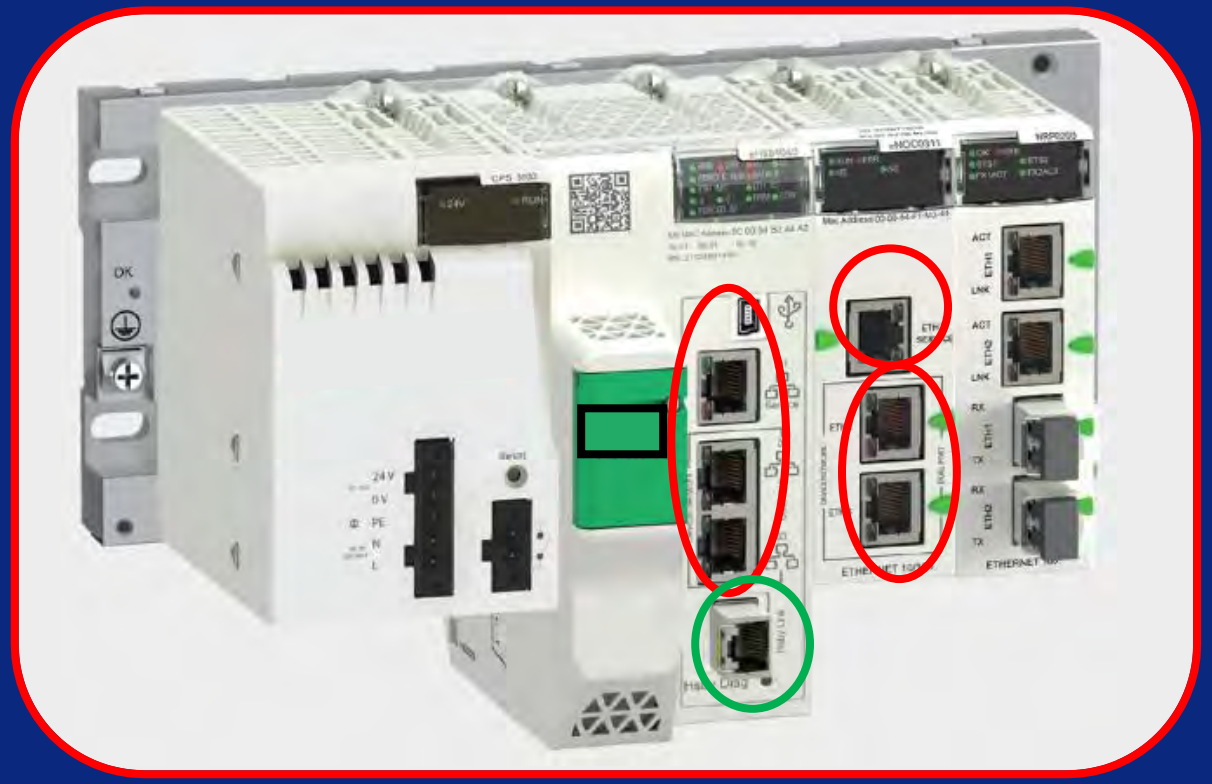
Une approche pragmatique

➔ Pour trouver selon vos contraintes le juste équilibre entre sécurité et maintenabilité



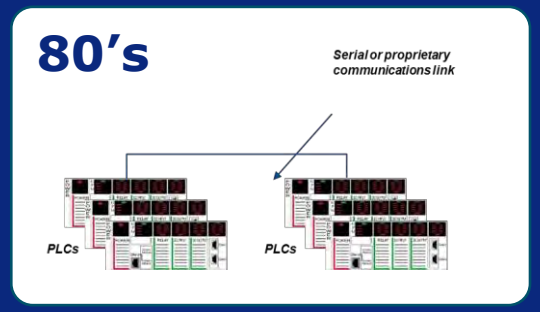
Qu’est-ce que l’OT ? (Operational Technology)

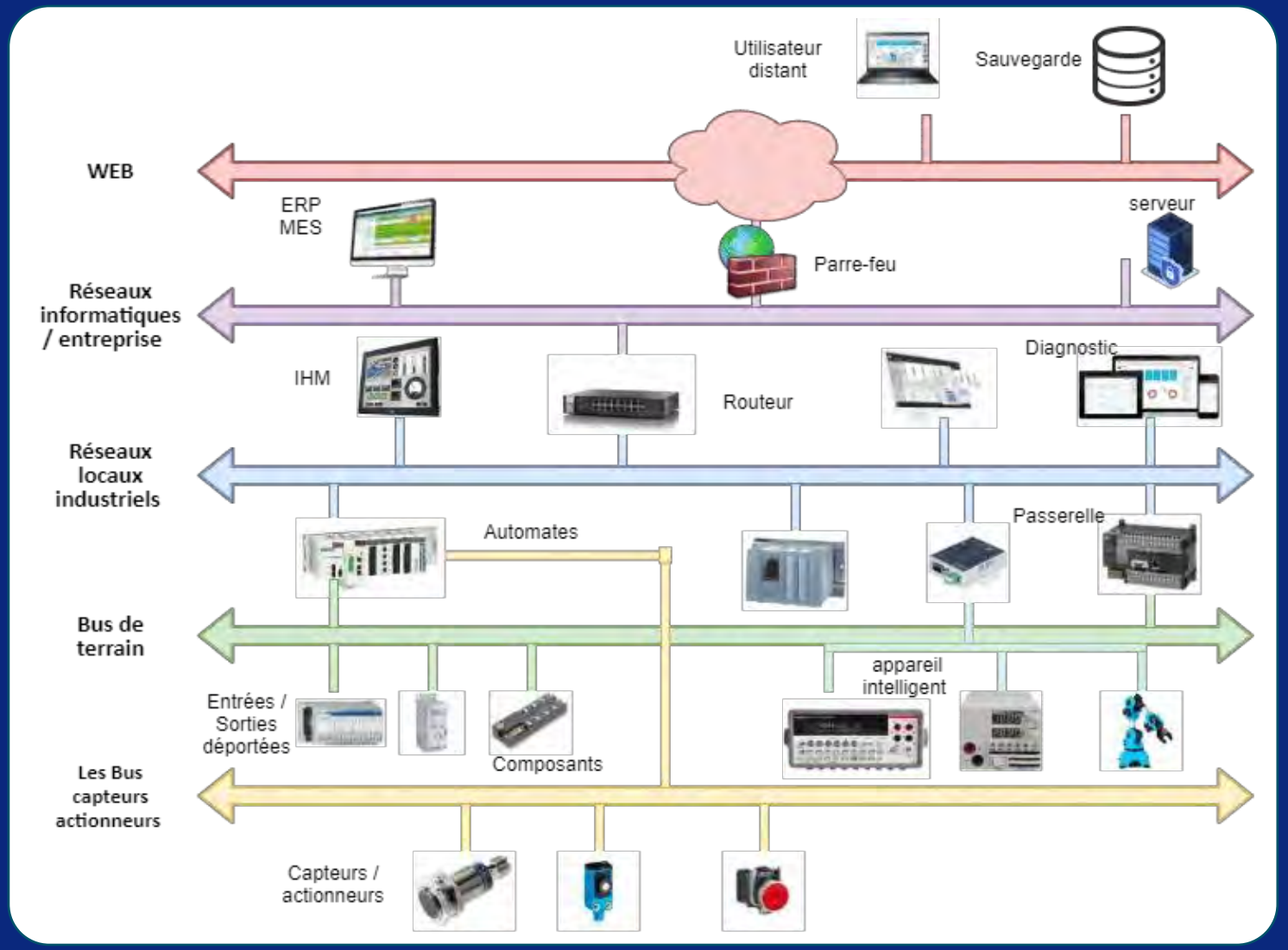
Les matériels utilisés sont tous des systèmes informatiques



Les produits utilisés dans vos process industriels sont des organes communicants qui possèdent un firmware et qui peuvent présenter des failles de sécurité

Qu'est-ce qu'un réseau OT aujourd'hui?





Sources de menace : Mais qui s’en prendrait à nous ?

Menace étatique ?

Cyberattaque

Un groupe de hackeurs russes se vante d’attaquer un barrage français mais frappe en réalité un ancien moulin à eau

Cybercriminel ?

Un automate industriel des stations d'épuration d'Oloron Sainte-Marie a été visé par une cyberattaque avec ransomware à la clé. Un renforcement de la sécurité est en cours pour éviter d'autres incidents.

Hacktivisme ?

Des hackers iraniens provoquent une panne d’eau en Irlande en soutien à la Palestine

Un logiciel facilement piratable

Vengeance interne ?

En Floride, une usine d'approvisionnement en eau potable piratée par un hacker

Révélation sur la cyberattaque d’Oldsmar : le pirate était un employé

La Cybersécurité : Les impacts sur votre entreprise

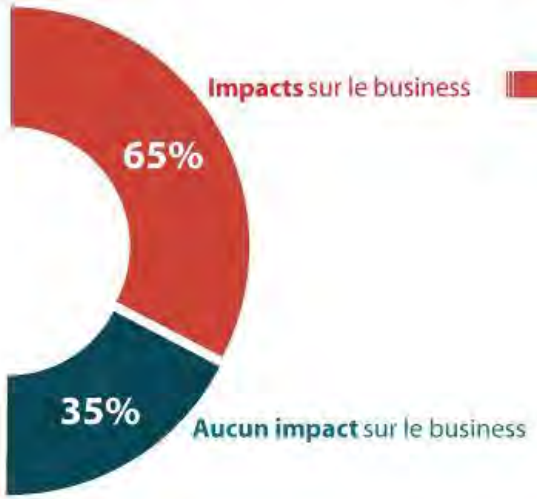
L'impact des cyberattaques sur le business reste stable cette année : 2/3 le subissent. Si la perturbation de la production est toujours la conséquence la plus mentionnée, l'indisponibilité du site web pendant une période significative recule.

351 personnes

Q7. Quel a été l'impact des cyberattaques sur votre business ?

Base : ont constaté une attaque et / ou une cause d'incidents de sécurité - Plusieurs réponses possibles

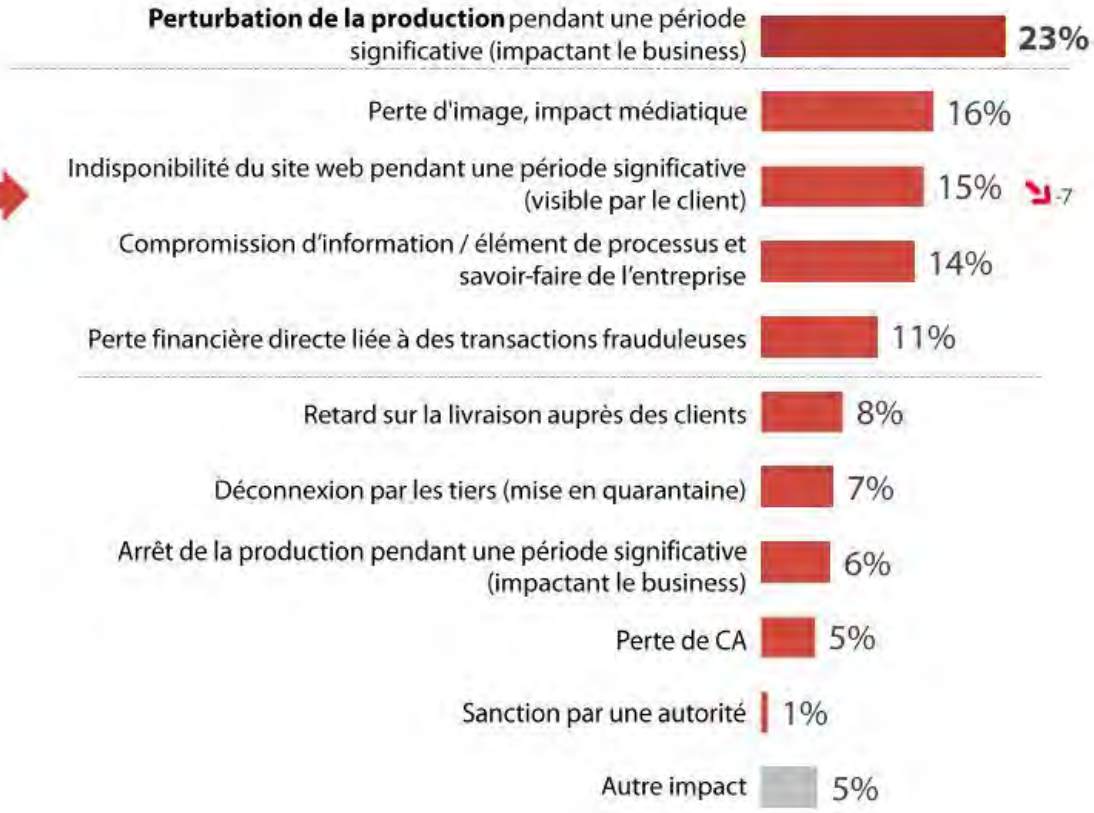
Rappel Vague 9 : 65%



Impacts sur le business

Aucun impact sur le business

Rappel Vague 9 : 35%



NIS2 : Préparer les entreprises aux risques de cybercriminalité

Qui est concerné ?

En France, NIS 2 s'appliquera aux entités essentielles (EE) et à des milliers d'entités importantes (EI) réparties dans 18 secteurs

TAILLE ENTITE	NOMBRE D'EMPLOYÉS	CHIFFRE D'AFFAIRES (MILLIONS D'EUROS)	BILAN ANNUEL (MILLIONS D'EUROS)	ANNEXE 1	ANNEXE 2
INTERMÉDIAIRE ET GRANDE	x ≥ 250	y ≥ 50	z ≥ 43	ENTITES ESSENTIELLES	ENTITES IMPORTANTES
MOYENNE	50 ≥ x ≥ 250	10 ≥ y > 50	10 ≥ z > 43	ENTITES IMPORTANTES	ENTITES IMPORTANTES
MICRO ET PETITE	x < 50	y < 10	z < 10	*Non concernées*	*Non concernées*

** Sauf lien avec une EE ou EI*

Annexe	Secteur
1	01. Énergie
1	02. Transports
1	03. Secteur bancaire
1	04. Infrastructures des marchés financiers
1	05. Santé
1	06. Eau potable
1	07. Eaux usées
1	08. Infrastructure numérique
1	09. Gestion des services TIC
1	10. Administration publique
1	11. Espace
2	01. Services postaux et d'expédition
2	02. Gestion des déchets
2	03. Fabrication, production et distribution de produits chimiques
2	04. Production, transformation et distribution des denrées alimentaires
2	05. Fabrication
2	06. Fournisseurs numériques
2	07. Recherche

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MonEspaceNIS2

Mon entité est-elle concernée ?

Réalisez un test pour déterminer si votre entité est régulée par la directive NIS 2 et à quelle catégorie elle appartient.

Pourquoi les réseaux OT méritent-ils notre attention ?

Assurer la disponibilité du réseau et le superviser

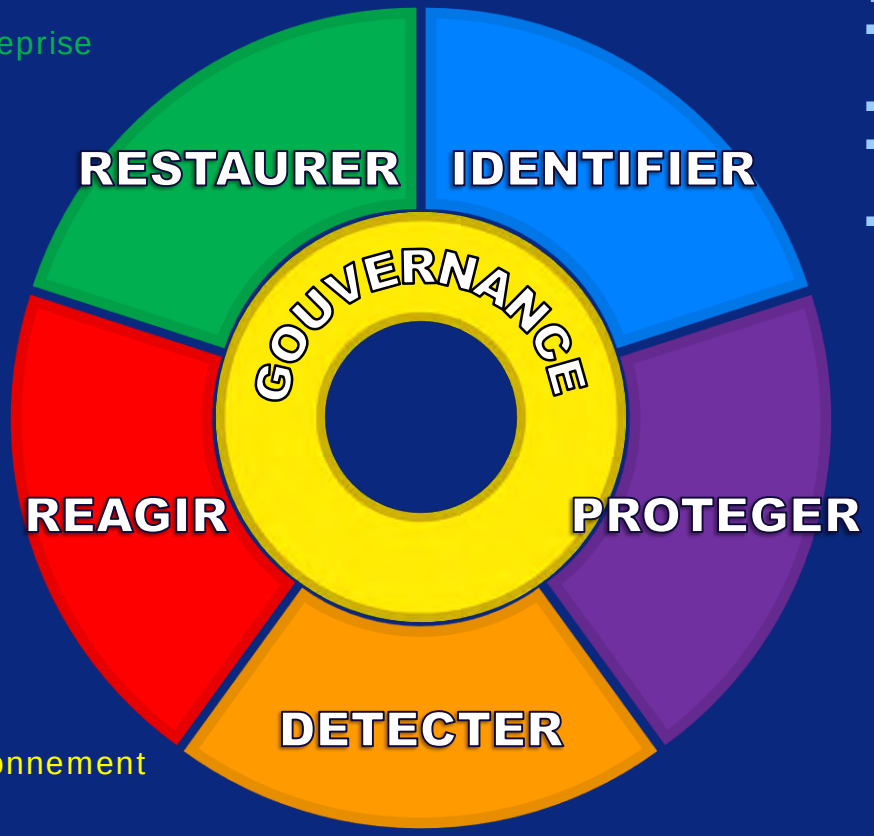
Assurer la cybersécurité d'un réseau industriel

Accéder à distance à vos automatismes, en toute sécurité

Mise en place d’une démarche cyber

RESUME DE LA DEMARCHE (Le Framework NIST v2.0) :

RESTAURER:
- Rétablissement des opérations (Plan Reprise d’Activité)
- Communication



IDENTIFIER:
- Inventaire des équipements matériels, logiciels
- Cartographie flux de données
- Évaluation du risque : Exposition, criticité, menaces
- Suivi des modifications

REAGIR :
> **contenir les effets de l’incident**

- Gestion des incidents
- Analyse des incidents
- Rapports et communication sur les interventions

PROTEGER:
- Formation, sensibilisation
- Authentification, droits, (passwords)
- Gestion des sauvegardes, résilience des infrastructures
- Application des correctifs (Vulnérabilités)
- Durcissement réseau, segmentation, isolement
- Accès distant
- Priorisation des actions

GOUVERNANCE :
- Contexte organisationnel
- Stratégie de gestion du risque
- Gestion des risques de la chaîne d'approvisionnement
- Rôles, responsabilités et autorités
- Politiques, processus et procédures
- Contrôle

DETECTER:
- Les activités suspectes, flux, menaces,
- Alerter

Collaboration étroite entre les équipes IT et OT pour une cybersécurité robuste

Quelques d'un RSSI OT (& IT)

→ Comme pour l'IT : Gouvernance, Hygiène, Conformité, Gestion des Risques

→ Règles d'hygiène :

- Guide mesures industrielles ANSSI
- Guide du CLUSIF

→ Objectif de sécurité n°1 = disponibilité

→ Faire une analyse de risques

→ La Conformité : le futur proche… NIS2

N'attendez pas le décret d'application !

→ **La cybersécurité n'est pas que du ressort des responsables IT ou OT**

COMEX, élus, décideurs… saisissez-vous du sujet !

SMÉDAR

Merci

RETROUVEZ LES EXPOSANTS AU VILLAGE DE L'INNOVATION TOUT AU LONG DE LA JOURNÉE

Cofinancé par l'Union européenne