C3 CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

CLUB ETI NOUVELLE-AQUITAINE
ENTREPRISES DE TAILLE INTERMÉDIAIRE

« Penser global, agir local »

3

Une ambition

faire de la Nouvelle-Aquitaine un territoire de confiance numérique

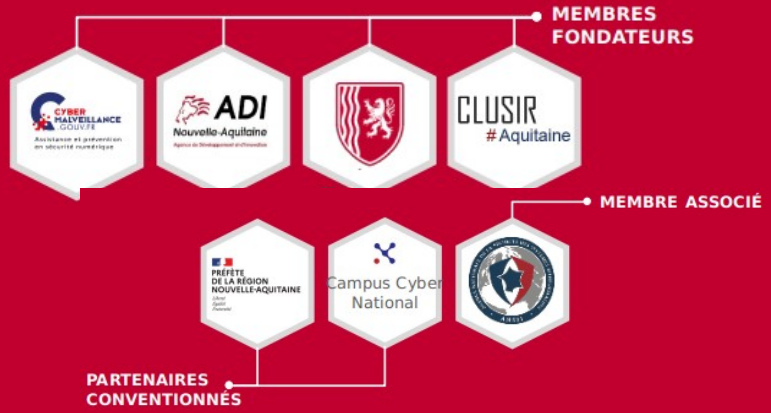
En renforçant la résilience des organisations publiques et privées de la région

En accompagnant la montée en compétence des ESN et la coordination des actions sur le territoire

3

1 lieu Totem au sein du parc Ampéris, regroupant 20 000 m² dédiés à la filière

1 outil : une association cofondée par des acteurs engagés



1 principe fort : temps de travail que les membres actifs consacrent aux travaux collaboratifs du Campus C3

1 %

4 piliers

Opération	Formation	Innovation	Mobilisation
Anticipation (alerte)	Sensibilisation	Projets collaboratifs	Développement de l'écosystème
Détection	Référentiels	Démonstrateurs	Rencontres
Réponse à incident	Contenus pédagogiques	Partenariats	Echanges
Capitalisation			

Des relais locaux

CRC Nord Nouvelle-Aquitaine
Université de Poitiers (IRIAF), CLUSIR, SOLURIS, pôle assurantiel niortais, collectivités territoriales…

CRC Châtellerault
Agglo

CRC Limoges
Limoges Métropole, Université de Limoges (Cryptis), SILPC, Aliptic, Orange, Legrand, Enedis

CRC Angoulême
En construction

CAMPUS
Région + Entreprises + Académiques + Centres R&D

CRC Périgueux
En construction

CRC Mont De Marsan
Agglomération, Université de Pau et des Pays de l'Adour, CEAM et ESIOC (BA118), Département des Landes, ALPI, ENSC

CRC Agen
Département + Université

CRC Pau
En construction

CAMPUS CYBER PAYS BASQUE (Espagne)

Un ancrage

Territorial, relayé par les centres de ressources en cybersécurité

National, en tant que (futur) Campus Cyber Territorial

Européen, par ses coopérations avec ses partenaires

AGENDA

2022 ____ 2023 ____ 2024

Opération

- Détection
- Réponse à incident / Kit PRA
- Recherche de compromission
- Anticipation

Formation

- Réf. Expert Cyber
- Labellisation Expert Cyber
- Gestion de crise
- Entraînement
- Diagnostic de maturité

Innovation

- Outil analyse C&C (Police judiciaire)
- Démonstrateurs

Mobilisation

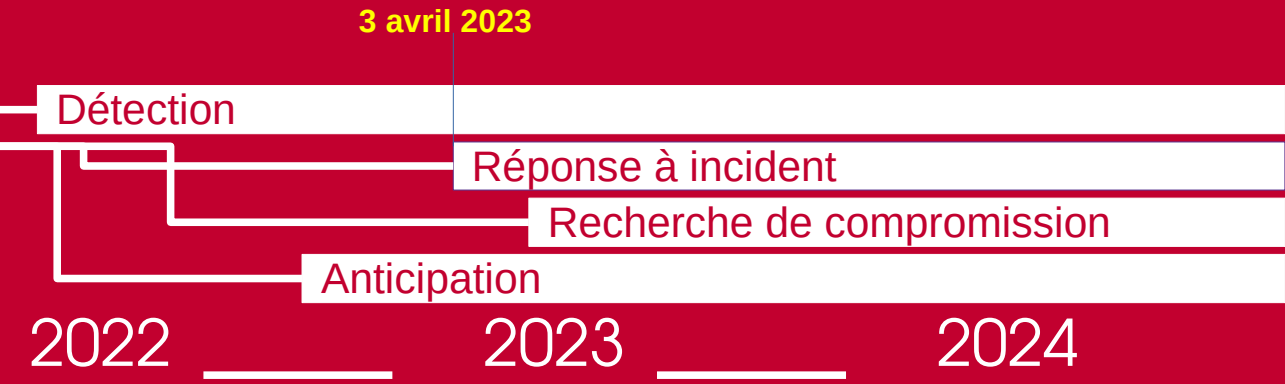
- Cyber Cafés
- Événements (CMCS, FIC , Hack It N, Mars@Hack, FIC Lille, Sthack
- Préparation « Cyber resilience act »

Une mise en place progressive

Opération

- Anticipation (alerte)
- Détection
- Réponse à incident
- Capitalisation

Mes vulnérabilités.
Suis-je attaqué/attaquant ?
Un accompagnement dans la réponse à incident
Capitalisation et partage
…..



Campus Cyber Nouvelle Aquitaine

Analyse du *Cyber Resilience Act*

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

Table ronde – 16/02/2023

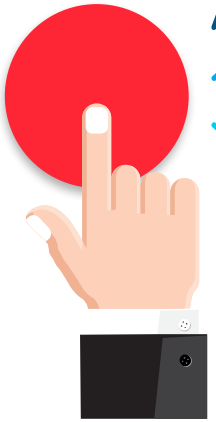
CYBER ICS formind KYRON SERMA SAFETY & SECURITY TrustnGo Plug & Play Security v6Protect Web Application Security

Sommaire

C3NA
Les équipes impliquées

Cyber Resilience Act
Les objectifs

Cyber Resilience Act
Les produits et entreprises concernées



Cyber Resilience Act
Les exigences à appliquer

Cyber Resilience Act
Les sanctions applicables

Cyber Resilience Act
Les prochaines étapes

Les entreprises au côté du C3NA

CYBER ICS

KYRON

TrustnGo
Plug & Play Security

formind

SERMA
SAFETY & SECURITY

v6Protect
Web Application Security

Les services proposés

Conseil	R&D sur mesure	Audits techniques	Audits en milieu industriel	Sûreté électronique	Sûreté des biens et des personnes	Gouvernance & Risques
Evaluation	Solutions technologiques	Conformité	Cyber-résilience	Sécurité du Cloud	Audits spécifiques (PASSI RGS, PASSI LPM)	Formation

Les constats

- La banalisation des cyber-attaques visant les produits matériels ou logiciels entraîne des surcoûts estimés à 5,5 milliards d'euros (en 2021)
- Deux problèmes majeurs identifiés :
  - Faible niveau de sécurité des produits vendus se traduisant par des vulnérabilités généralisées et des processus de mise à jour insuffisants voire incohérents, et
  - Des utilisateurs mal informés, dans l'incapacité de choisir de manière éclairée des produits sécurisés et de les utiliser correctement.
- En Europe, aucun cadre, uniformisé et cohérent, n'existe en matière d'obligations légales en ce qui concerne les équipements connectés.

Les objectifs du Cyber Resilience Act

1. Améliorer la sécurité des produits commercialisés, depuis leur conception jusqu'à leur mise au rebut.
2. Faciliter le respect des règles pour les producteurs de matériels et logiciels en mettant en place un cadre cohérent et unique.
3. Rendre plus transparentes les propriétés de sécurité des produits comportant des éléments numériques.
4. Permettre aux utilisateurs d'utiliser ces produits de manière sécurisée, tout au long de leur cycle de vie.

Le Cyber Resilience Act : Qui est concerné ?

- « Tous les équipements dont l'utilisation implique une connexion directe ou indirecte, physique ou logicielle à un réseau ou un autre appareil. »
- Concrètement : **tous les produits électroniques connectés** ainsi que leurs logiciels compagnons, à l'exception :
  - Des produits déjà couverts par une législation européenne.
    - par exemple les dispositifs médicaux.
  - Des produits militaires et de défense classifiés.
  - Des logiciels open source développés et fournis en dehors d'un cadre commercial.

Les produits concernés et leurs classes

Classe	Niveau de risque (CA)	Types de produit	Obligations
Non-classé	Faible	Produits *consumer* à petite / moyenne échelle (90% du marché)	Self-assessment et maintenance pendant le cycle de vie
Classe I	Moyen	Navigateur, gestionnaire de mots de passe, MCU, FPGA, IoT industriel, VPN, etc.	Conformité à un standard ou évaluation tierce partie
Classe II	Elevé	OS, Hyperviseur, PKI, Routeurs, modems, firewalls industriels, CPU, Robots, Smart meters, équipements concernés par NIS 2, etc.	Évaluation tierce partie

Source : Annexe III du Cyber Resilience Act

Le Cyber Resilience Act : Les exigences à appliquer

- En plus de l’obligation d’effectuer une analyse de risques, le Cyber Resilience Act définit deux types d’exigences essentielles de cybersécurité

1. Un ensemble d’exigences techniques de sécurité concernant la conception et l’implémentation du produit
2. Un ensemble d’exigences organisationnelles visant à diminuer le risque pendant le cycle de vie du produit

Le Cyber Resilience Act : Les exigences techniques de sécurité

1. Être conçu, développé et produit avec un niveau de cybersécurité approprié
2. Être livré sans vulnérabilité connue
3. Être sécurisé par défaut
4. Être protégé contre les accès non autorisés
5. Protéger la confidentialité des données manipulées
6. Protéger l'intégrité des données stockées, transmises et manipulées
7. Minimiser la collecte des données au strict nécessaire
8. Prévenir les dénis de services des fonctions et services essentiels
9. Réduire les probabilités de DDoS sur d'autres produits
10. Limiter la surface d'attaque
11. Réduire l'impact et l'exploitabilité des incidents cyber
12. Enregistrer les événements de sécurité
13. Corriger les vulnérabilités au moyen de mises à jour, de préférence automatiques en notifiant l'utilisateur

Le Cyber Resilience Act : Les exigences organisationnelles

1. Avoir une SBOM (*Software Bill of Material*)
2. Documenter les vulnérabilités
3. Corriger les vulnérabilités sans délai
4. Faire des tests et des revues de sécurité régulièrement
5. Publier publiquement au sujet des vulnérabilités corrigées
   - Pour les produits classe I et II, l'ENISA doit être prévenue dans les 24h.
6. Créer et appliquer des politiques de divulgation coordonnée des vulnérabilités
7. Faciliter le partage d'information concernant les vulnérabilités et fournir un point de contact pour le reporting
8. Fournir des mécanismes sécurisés de distribution des mises à jour
9. Distribuer rapidement et gratuitement les mises à jour de sécurité en expliquant aux utilisateurs leur rôle exact (pendant 5 ans)

Le Cyber Resilience Act : Les sanctions applicables

1. Jusqu’à 15 millions d’euros ou 2,5% du CA **en cas de non conformité avec les exigences de sécurité** (Annexe I, Article 10 et 11).

2. Jusqu’à 10 millions d’euros ou 2% du CA **pour non conformité avec les autres exigences**.

3. Jusqu’à 5 millions d’euros ou 1% du CA **en cas de fourniture d’informations incorrectes, incomplètes ou trompeuses** aux autorités compétentes.

Le Cyber Resilience Act : La mise en application

- Le CRA est en cours d’adoption par l’Union Européenne.
- Une fois le texte final adopté et ratifié (2023/2024), **la mise en application est immédiate**.
- Les fabricants auront **un an** pour se mettre en conformité vis-à-vis de la **remontée des incidents à l’ENISA**.
- Les fabricants auront **deux ans** pour se mettre en conformité avec les **autres exigences**.

Prochaines étapes des travaux du C3NA

- **Kit de sensibilisation à destination des entreprises**
  - Guide de compréhension du Cyber Resilience Act
  - Kit de sensibilisation : vidéos, affiches

- **Kit de mise en conformité pour les produits Class-less**
  - Modèles de documents
  - Checklist de commercialisation
  - Checklist de préparation d’audit de contrôle

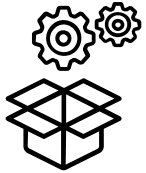
Merci pour votre attention !

Présentation de CYBER ICS

- CYBER ICS est une société à forte valeur ajoutée, dotés d'experts multicartes en sécurité et sûreté
- Organisation autour de 3 secteurs d'activité :

Cybersecurity Audit & Advisory

- Cybersécurité IT & OT
- Expertise en cybersécurité industrielle (oil & gas, energy)
- Audit et conseil
- Mise en place des [illegible]



Training & Procurement

- Fourniture de matériel technique
- Création de formations
- Sensibilisations et formations cyber
- Développements sur mesure

Incident Response & TSCM

- Gestion de crise sécurité et cyber
- Accompagnement à la mise en place organisatoinnelle : PCA, PRA, PRI
- Audit et test de SOC
- Opérations TSCM (*« bug sweeping »*)

Présentation KYRON

- KYRON est une société dotée d’ une forte expertise en Cybersécurité des environnements industriels (OT) et IT
- Organisation autour de 4 secteurs d’activité :

Audit

- Cybersécurité OT & IT
- Analyse de risques (nucléaire, agro-alimentaire, transports, santé…)
- Audit organisationnel
- Audit d’ architecture et

Conseil

- Gouvernance
- Définir et implémenter un système de Management de la sécurité des environnements Industriels ou du SI
- Assistance à maîtrise ouvrage
- Accompagnement à homologation

Sécurisation & Intégration

- Sécurisation des systèmes industriels et des SI
- Mettre en œuvre ou faire évoluer une architecture sécurisée
- Durcir la configuration

Formation

- Former et certifier les équipes opérationnelles à la sécurité industrielle
- Sensibiliser les dirigeants et collaborateurs aux risques cyber
- Identifier et

KYRON

Présentation de TRUSTNGO

- TrustnGo est une jeune société spécialisée dans le durcissement des systèmes embarqués.

TrustnGo
Plug & Play Security