# DEF 1b

## Stratégie d'accompagnement au Renforcement des capacités

## Cybersécurité - Introduction

# SOMMAIRE

1

# Digital Energy Facility

# RAPPELS SUR LA DEF ET SES QUATRE COMPOSANTES

Digital Energy FACILITY

RTEi

1 Digitalisation des opérateurs énergétiques
**6,7M€**

2 Financement de l'innovation
**7,2M€**

3 Création d'une communauté d'acteurs
**1,8M€**

4 Capital amorçage pour des solutions innovantes destinées aux entreprises d'accès à l'énergie
**4,8M€ (prêts d'amorçage)**

Financé par l'Union européenne et mis en œuvre par l'Agence française de développement (AFD), ce programme soutient la digitalisation et la modernisation du secteur de l'énergie.

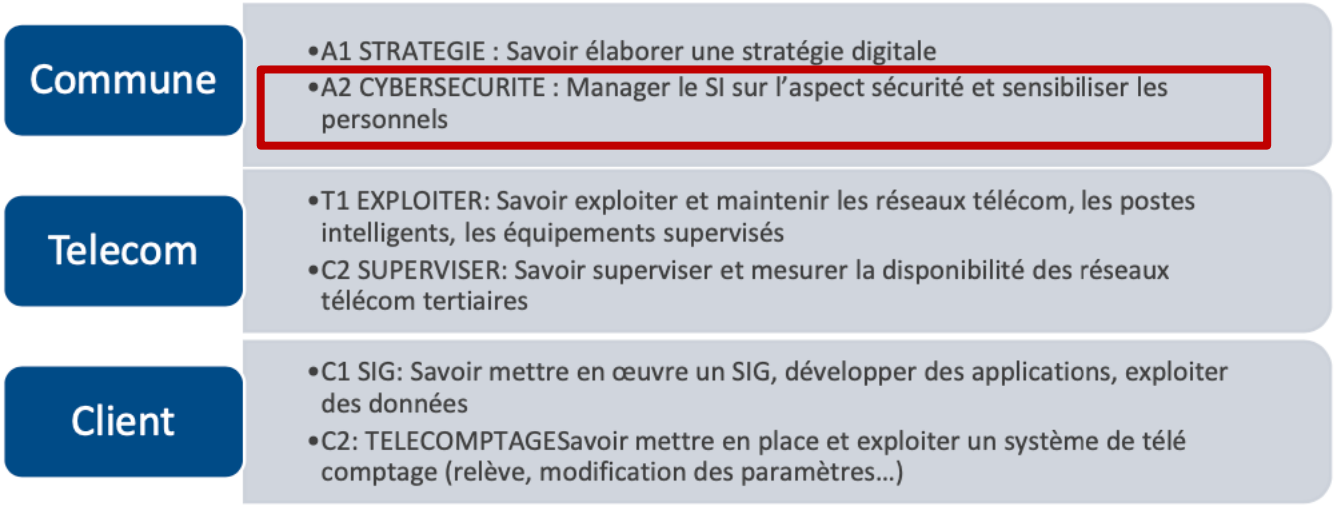
# COMPOSANTE 1B DE LA DEF

Objectif : Accompagner le renforcement des capacités des opérateurs

Actions financées : webinaires, ateliers, séminaires, échanges entre pairs, mise en réseau, formations…

# LES DOMAINES RETENUS

7 thématiques prioritaires initialement retenues et regroupées en 3 groupes de travail




S1 – Outils collaboratifs pris en compte tout au long du projet

2

# Introduction à la cybersécurité

# ACTUALITÉ 2022 : CYBERATTAQUE CONTRE LE RÉSEAU ÉLECTRIQUE UKRAINIEN

- ***Date:*** 13 avril 2022
- ***Gouvernement ukrainien*** : un piratage du réseau électrique du pays a été évité
- ***Modalités de la cyberattaque :*** Les hackers russes ont pris pour cible l'une des principales entreprises énergétiques du pays, et tenté de désactiver des postes.
- ***En cas de succès***, plus de deux millions de personnes auraient été plongées dans le noir.

# INTRODUCTION À LA CYBERSÉCURITÉ

## Définition

Le mot cybersécurité est un néologisme désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger **les personnes et les actifs informatiques matériels et immatériels** (connectés directement ou indirectement à un réseau) des États et **des organisations** (avec un objectif de **disponibilité, intégrité et authenticité, confidentialité**, preuve et non-répudiation).

# INTRODUCTION À LA CYBERSÉCURITÉ

## Enjeux & Objectifs

La sécurité des Système d'Informations vise à garantir:

- La disponibilité des données
- L'intégrité des données
- La confidentialité des données

# INTRODUCTION À LA CYBERSÉCURITÉ

## Enjeux & Objectifs

La sécurité des Système d'Informations vise à protéger la « valeur » d'une entreprise:

SÉCURITÉ DES PERSONNES

SÉCURITÉ PHYSIQUE (actifs)

SÉCURITÉ DE L'INFORMATION

On perçoit ici une spécificité des entreprises du secteur énergétique (et plus largement des entreprises industrielles) avec des actifs physiques et informationnels qui se recoupent.

# INTRODUCTION À LA CYBERSÉCURITÉ

## Impacts des cyber attaques

Les risques cyber peuvent conduire à des impacts divers :

- Perte financière
- Risque réputationnel
- Dommages matériels / corporels
- Responsabilité civile / pénale
- **Perte de disponibilité du système**

3

# Panorama des menaces

# PANORAMA DES MENACES

## Classification des menaces

| | |
|---|---|
| Impact des menaces | •Confidentialité<br>•Integrité<br>•Disponibilité |
| Sources et agents des menaces | •Délibéré<br>•Accidentel<br>•Environnemental |
| Actions de menace | •Taxonomies (ENSIA, ISO/IEC, etc.) |
| Cibles des menaces | •MITRE ATT&CK Matrix<br>•Kill Chain |

# PANORAMA DES MENACES

## Acteurs & Motivations

| | |
|---|---|
| ETATS / NATIONS | GEOPOLITIQUE |
| CYBER TERRORISTES | PROFIT |
| CYBERCRIMINELS | IDEOLOGIE |
| HACKTIVISTES | IDEOLOGIE |
| SCRIPT KIDDIES | SATISFACTION |
| INSIDER THREATS | MECONTENTEMENT |

# PANORAMA DES MENACES

## ENISA Threat Landscape 2022

**Figure 1:** ENISA Threat Landscape 2022 - Prime threats


**https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022**

enisa THE EU CYBERSECURITY AGENCY

# PANORAMA DES MENACES

## ENISA Threat Landscape 2022

L'ENISA a classé les menaces en 8 groupes. La fréquence et l'impact déterminent l'importance de ces menaces.

1. Ransomware : 60 % des organisations touchées pourraient avoir payé des demandes de rançon.
2. Logiciels malveillants : 66 divulgations de vulnérabilités de type "zero-day" observées en 2021
3. Ingénierie sociale : Le phishing reste une technique populaire, mais de nouvelles formes de phishing apparaissent, telles que le spear-phishing, le whaling, le smishing et le vishing.
4. Menaces contre les données :Augmentation proportionnelle au total des données produites
5. Menaces contre la disponibilité :
    1. La plus grande attaque par déni de service (DDoS) jamais réalisée a été lancée en Europe en juillet 2022 ;
    2. Internet : destruction d'infrastructures, pannes et réacheminement du trafic Internet.
6. Désinformation - désinformation : Escalade de la désinformation basée sur l'IA, des deepfakes et de la désinformation en tant que service.
7. Ciblage de la chaîne d'approvisionnement : Les incidents impliquant des tiers représentent 17 % des intrusions en 2021, contre moins de 1 % en 2020.

# PANORAMA DES MENACES

## ENISA Threat Landscape 2022

Principales tendances :

- **Les Vulnérabilité zero-day »** sont la nouvelle ressource utilisée par les acteurs astucieux de la menace.
- Une nouvelle vague d'hacktivisme a été observée depuis la guerre entre la Russie et l'Ukraine.
- **Les attaques DDoS** deviennent plus importantes et plus complexes et sont utilisées dans la cyberguerre (elles se déplacent vers les réseaux mobiles et l'IoT).
- **La désinformation basée sur l'IA et les "deepfakes",** qui inondent les agences gouvernementales de faux contenus, peuvent facilement perturber le processus d'élaboration des règles et l'interaction avec la communauté.
- Les groupes de menace ont accru leur intérêt et leurs capacités en matière d'attaques contre **la chaîne d'approvisionnement et les fournisseurs de services gérés (MSP).**

# PANORAMA DES MENACES

## ENISA Threat Taxonomy

- Attaque physique (délibérée/ intentionnelle)
- Dommages/pertes involontaires d'informations ou de biens informatiques
- Catastrophe (naturelle, environnementale)
- Défaillances / dysfonctionnements
- Pannes
- Écoute clandestine/interception/ détournement
- Activité malveillante/ Abus
- Juridique

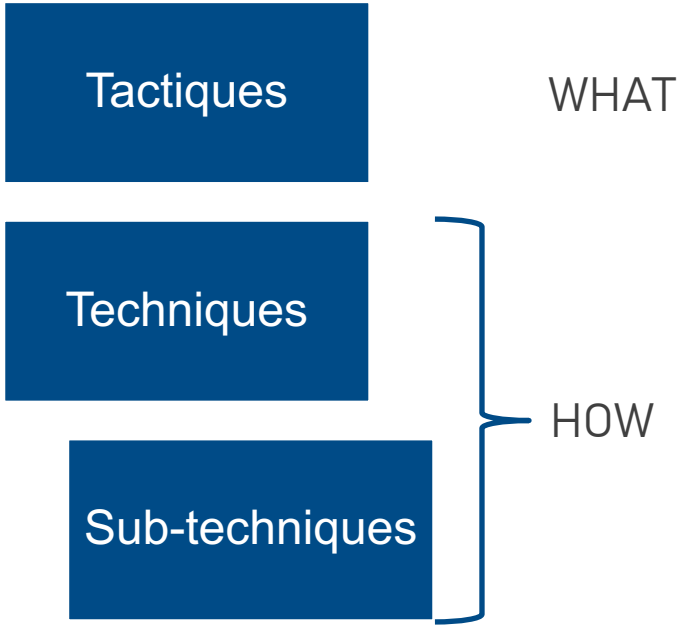
https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

# PANORAMA DES MENACES

## Cibles de menaces – Framework MITRE ATT&CK

- MITRE ATT&CK (pour Adversarial Tactics, Techniques, and Common Knowledge) est une base de connaissance aidant à modeler les tactiques et techniques utilisées par les cyberadversaires, ainsi qu'à comprendre comment les détecter et les stopper.
- Cette base de connaissance classifie et décrit les cyberattaques et les intrusions. Elle est créée et publiée par la société à but non lucratif MITRE en 2013.

https://attack.mitre.org/

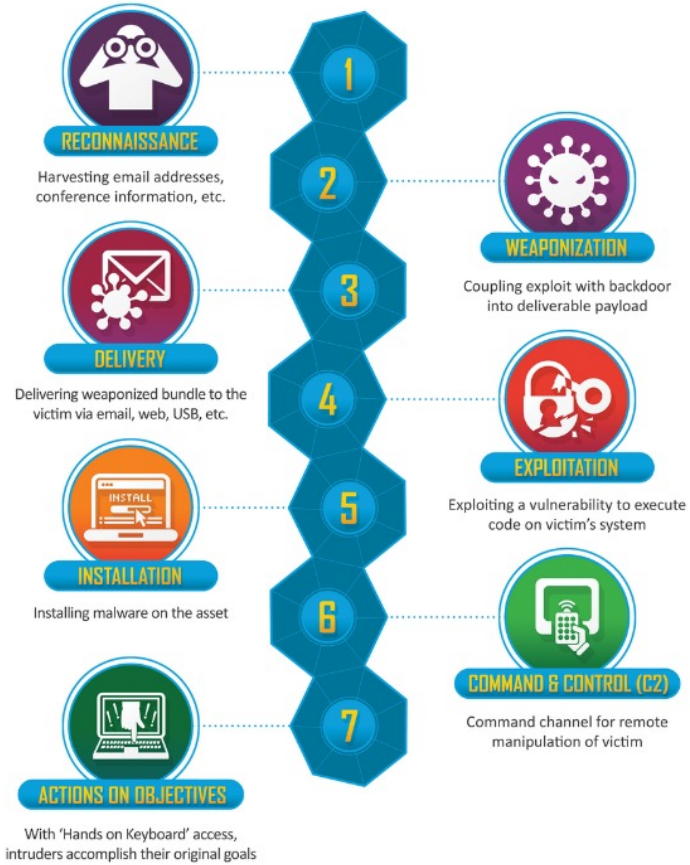


# PANORAMA DES MENACES

## Cibles de menaces – Cyber Kill chain

- Lockheed Martin a décrit en 2011 un nouveau cadre ou modèle de «kill chain» pour défendre les réseaux informatiques. Selon ce modèle, les attaques peuvent être découpées en phases et peuvent être perturbées grâce à des contrôles établis à chaque étape.
- Depuis, le modèle de «cyber kill chain» a été adopté par les organisations de sécurité des données pour définir les phases des cyberattaques.

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



4

# Quelques spécificités du secteur

# SPÉCIFITÉS DU SECTEUR

## Les menaces pour le domaine OT

Récemment, des virus avec la capacité de prendre le contrôle sur des industrial control systems (ICS) ont été découverts :

1. Stuxnet ,
2. Havex ,
3. Blackenergy2 ,
4. Crashoverride or industroyer ,
5. Trisis or triton

De nouveaux groupes (Kostovite, Petrovite et Erythrite) ayant l'intention ou la capacité de cibler les réseaux OT ont été identifiés (sur un total de 18).

Https://industrialcyber.Co/threats-attacks/dragos-estimates-that-chernovites-pipedream-malware-targets-ics-networks/

# SPÉCIFITÉS DU SECTEUR

## Les menaces pour le domaine de l'énergie

L'ENISA a identifié certaines tendances pour 2030, qui concernent en particulier le secteur de l'énergie :

- EC5 Increasing reliance on automation and connectivity of sustainable energy production
- EC7 Increasing danger of resource bottlenecks of critical raw materials for strategic technologies and sectors in the EU
- EN1 The increased usage of new technologies in remote maintenance
- EN7 The emerging use of distributed and alternative energy resources
- EN8 The increasing energy consumption of digital infrastructure

https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

5

# Evaluation des vulnérabilités

# EVALUATIONS DES VULNÉRABILITÉS

## Vulnérabilité - définition

**A security vulnerability is a weakness an adversary could take advantage of to compromise the confidentiality, availability, or integrity of a resource.**

***Une faille de sécurité est une faiblesse dont un adversaire pourrait tirer parti pour compromettre la confidentialité, la disponibilité ou l'intégrité d'une ressource.***

*ENISA*

# EVALUATIONS DES VULNÉRABILITÉS

## Vulnérabilité – Référentiel CVE

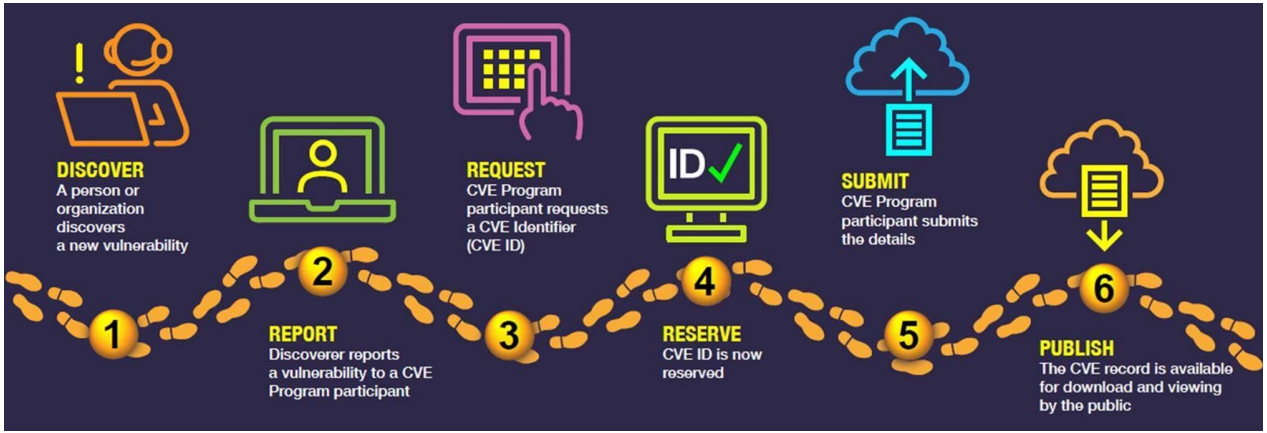
Common Vulnerabilities and Exposures (« Vulnérabilités et expositions communes ») ou CVE est un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE, soutenu par le département de la Sécurité intérieure des États-Unis.
*https://cve.mitre.org/*

En lien avec le dictionnaire CVE, il existe deux autres ressources MITRE :

- NVD - La National Vulnerability Database (NVD) est une base de données, maintenue par le NIST, qui est entièrement synchronisée avec la liste CVE de MITRE.
- CVSS - Le Common Vulnerability Scoring System (CVSS) est un système largement utilisé dans les programmes de gestion des vulnérabilités. CVSS indique la gravité d'une vulnérabilité en matière de sécurité de l'information et fait partie intégrante de nombreux outils d'analyse des vulnérabilités.

# EVALUATIONS DES VULNÉRABILITÉS

## CVE Reporting Process



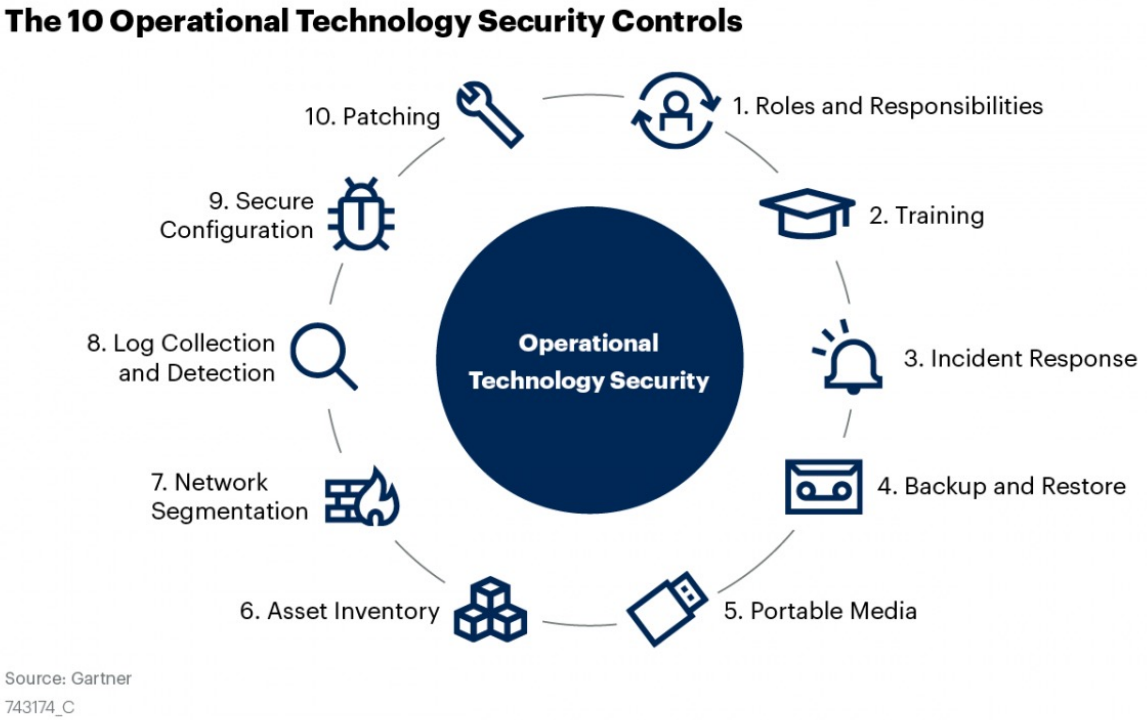

Pour se prémunir de ces vulnérabilités (voir menaces zero-day), les développeurs peuvent se munir d'outils comme mend.io
*https://www.mend.io/vulnerability-database/*

6

# Contremesures et meilleures pratiques

# CONTRE MESURES & MEILLEURES PRATIQUES

## Top 10 moyens



7

# Contexte réglementaire et normatif

# CONTEXTE RÉGLEMENTAIRE

## Obligations légales

Obligations nationales :

- Loi de programmation militaire

Obligations européennes :

- NIS
- NIS 2
- NCCS – spécifique réseaux électriques

Normes internationales :

- ISO
- IEC

8

# L’exemple de RTE

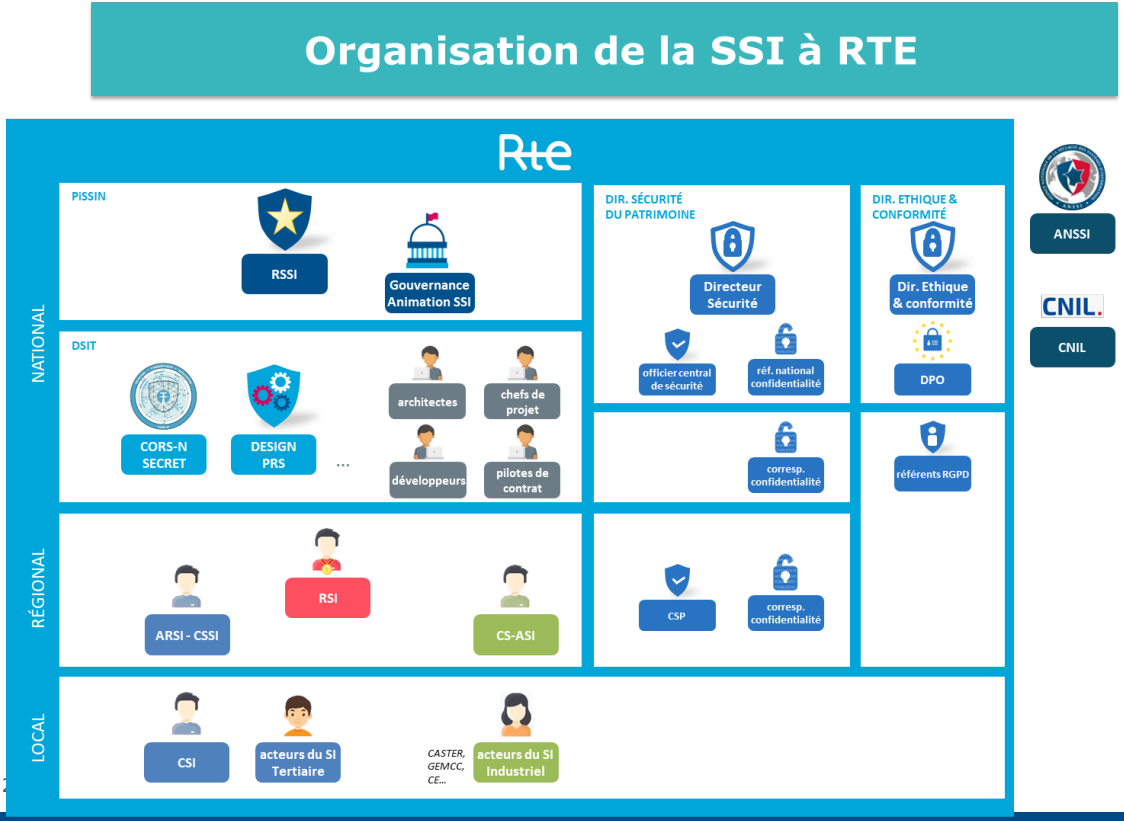
# EXEMPLE DE RTE

## Exemple de RTE

- Témoignage de Xavier Carton, RSSI RTE

# EXEMPLE DE RTE

## Organisation de la SSI chez RTE



# RÔLE DU RSSI

## Missions du RSSI

- Définir et faire évoluer la PSSI
- S'assurer de la mise en œuvre de la PSSI, sur délégation de la Direction de RTE
- Informer, conseiller et alerter la Direction Générale et les fonctions sur les enjeux de la sécurité du SI
- Décliner la Loi de Programmation Militaire (LPM)
- Réaliser les veilles technologique et réglementaire
- Piloter les audits et contrôles
- Piloter les cellules de crises cyber
- S'assurer de la sensibilisation et de la formation des collaborateurs de RTE aux enjeux de sécurité du SI