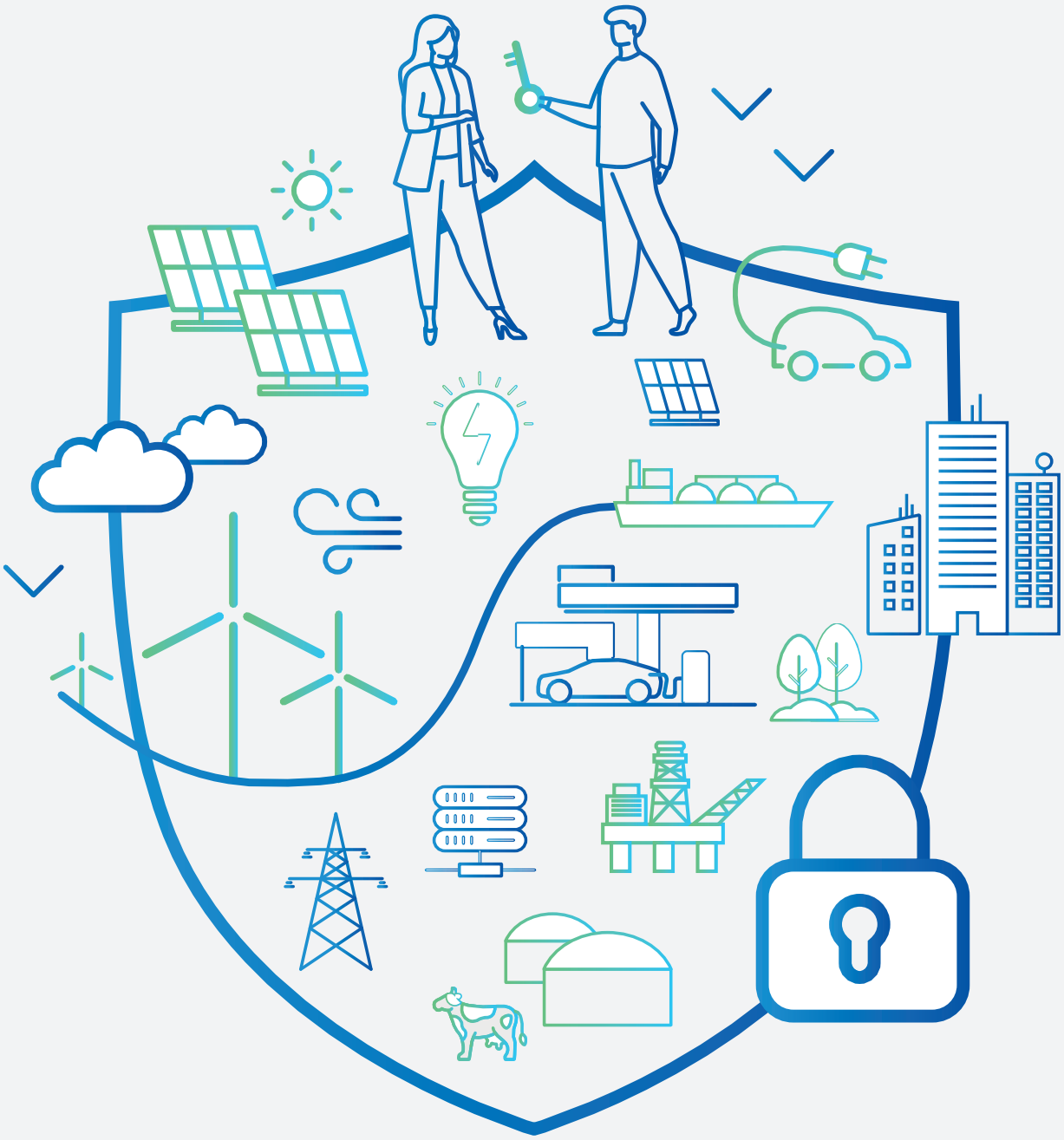


Notre approche **cybersécurité**

Nous faisons de la cybersécurité une priorité. Élément clé de la confiance de nos clients et de nos partenaires, elle participe aussi à la pérennité de nos activités.

TotalEnergies

AVERTISSEMENT

Les termes “ TotalEnergies ”, “ compagnie TotalEnergies ” et “ Compagnie ” qui figurent dans ce document sont utilisés pour désigner TotalEnergies SE et les entités comprises dans le périmètre de consolidation. De même, les termes “ nous ”, “ nos ”, “ notre ” peuvent également être utilisés pour faire référence à ces entités ou à leurs collaborateurs. Il ne peut être déduit de la simple utilisation de ces expressions une quelconque implication de TotalEnergies SE ni d’aucune de ses filiales dans les affaires ou la gestion d’une autre société de la compagnie TotalEnergies. Ce document peut contenir des informations et déclarations prospectives. Elles peuvent s’avérer inexactes dans le futur et sont dépendantes de facteurs de risques. Des informations supplémentaires concernant les facteurs, risques et incertitudes susceptibles d’avoir un effet sur les résultats financiers ou les activités de la Compagnie sont par ailleurs disponibles dans les versions les plus actualisées du document d’enregistrement universel déposé par la société auprès de l’Autorité des marchés financiers et du Form 20-F déposé par la société auprès de la *United States Securities and Exchange Commission* (SEC).

Brochure éditée en juillet 2023.
Remerciements à l’ensemble des contributeurs.

Crédit photo
Michel Labelle

Conception et réalisation
Inetum

“La menace cyber persistera et se transformera. TotalEnergies a mis en place des moyens de protection, de défense et de résilience pour s’adapter en continu à la réalité de la menace. Ce dispositif nous permet d’assurer nos missions essentielles quel que soit le contexte cyber.”

Jean-Dominique Nollet
Chief Information Security Officer **(CISO)**
TotalEnergies

Les fondamentaux de notre approche cybersécurité

- L’ensemble de notre Compagnie fait de la cybersécurité une priorité au quotidien.
- Nos systèmes d’information (SI) sont protégés de manière homogène et adaptée en fonction du profil de risque.
- Notre Compagnie détecte les attaques, y réagit vite et sait reconstruire ses applications ou systèmes les plus critiques.
- Tous nos SI sont intégrés dans une gouvernance cybersécurité efficace permettant de déployer les mesures de sécurité.

SOMMAIRE

Nous vous proposons de découvrir, dans cette brochure, notre approche cybersécurité s'inspirant du *NIST Cybersecurity Framework. Elle présente notre gouvernance, notre organisation, nos activités de protection, de maintien en condition de sécurité, de détection et de réaction et notre résilience.**

La **maîtrise des risques** liés à la cybersécurité constitue un **enjeu majeur et prioritaire pour notre Compagnie.** C'est pourquoi nous avons déployé un ensemble de **mesures** pour atteindre et maintenir **un état de cybersécurité élevé et en adéquation avec la menace.**

Notre approche cybersécurité repose sur **la gestion des risque**s et **la conformité** aux réglementations mondiales et s'illustre par :

- **une gouvernance cybersécurité centralisée** pilotée par le *Chief Information Security Officer* (CISO) de notre Compagnie ;
- **une organisation claire** avec une répartition des rôles et responsabilités en 3 lignes de défense ;
- **des audits et contrôles récurrents** pour **éprouver notre modèle.**

Un **socle de bonnes pratiques** est également en place pour garantir un haut niveau de sécurité des appareils, des réseaux et des données avec :

- un **référentiel de cybersécurité** décliné à l'ensemble de la Compagnie, composé de grands principes et exigences applicables aux personnes, aux processus et aux technologies ;
- des ***Golden Rules*** destinées au management métier et à l'IT ;
- un ***Cyber Pass*** pour former régulièrement nos collaborateurs de la filière cybersécurité ;
- un **programme de sensibilisation** pour l'ensemble des collaborateurs.

De plus, notre Compagnie veut s'assurer que nos fournisseurs ont un niveau d'exigence cybersécurité suffisant pour protéger les informations et nos biens et garantir la continuité des services qui nous sont rendus.

Des partenariats technologiques avec les fournisseurs cloud **Microsoft et Amazon renforcent nos capacités à sécuriser** nos usages de leurs plateformes.

Enfin, ces mesures de protection sont complétées de **mesures de défense et de résilience pour une réponse adaptée et maîtrisée par des équipes expertes** en cas de cyberattaques. En effet, notre Compagnie est dotée :

- d'un ***Security Operations Center*** **(SOC)** pour superviser nos systèmes d'information et détecter les incidents de sécurité ;
- d'un ***Computer Emergency Response Team*** **(CERT),** membre du FIRST**, composé d'experts capables de réagir à toute cyberattaque et connectés aux autres CERT des grandes entreprises pour partager de l'information sur la menace.

** Le framework cybersecurité du National Institute of Standards and Technology (agence fédérale américaine) définit un cadre méthodologique de gestion de la cybersécurité. Ce framework aide à gérer et réduire les risques cybersécurité des systèmes d'information.*
*** Forum of Incident Response and Security Teams*

TotalEnergies,
une compagnie cyberactive

Des moyens de télécommunication sécurisés relient nos navires et nos sites industriels localisés en mer

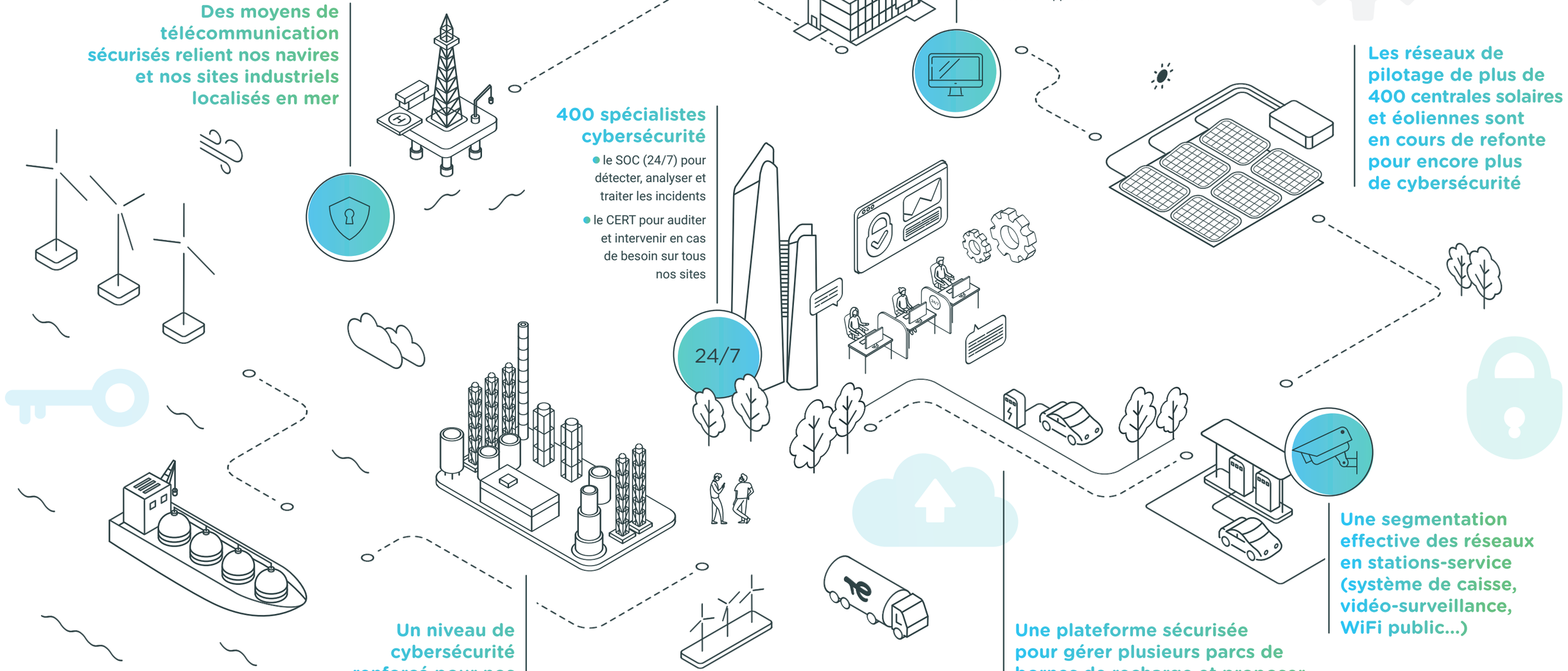
Des postes de travail sécurisés

Nous utilisons une authentification moderne sans mot de passe pour les sessions utilisateurs et l'accès aux applications.

400 spécialistes cybersécurité

- le SOC (24/7) pour détecter, analyser et traiter les incidents
- le CERT pour auditer et intervenir en cas de besoin sur tous nos sites

Les réseaux de pilotage de plus de 400 centrales solaires et éoliennes sont en cours de refonte pour encore plus de cybersécurité



Une segmentation effective des réseaux en stations-service (système de caisse, vidéo-surveillance, WiFi public...)

Un niveau de cybersécurité renforcé pour nos sites industriels

Une plateforme sécurisée pour gérer plusieurs parcs de bornes de recharge et proposer des services à nos clients

130 pays

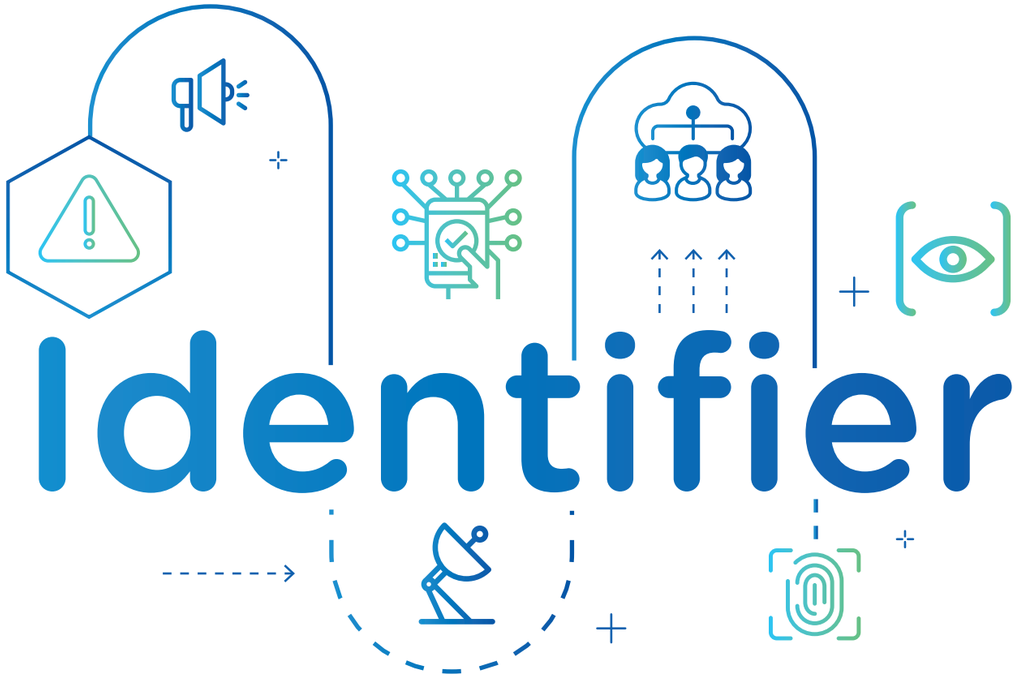
+100 000 postes de travail

+200 000 adresses IP publiques

3 900 applications centrales

14 000 serveurs

+37 600 térabytes de données



Gouvernance de la cybersécurité

Notre gouvernance de la cybersécurité définit, d'une part, les principes de mise en œuvre de la stratégie cybersécurité de notre Compagnie et de ses filiales et, d'autre part, les rôles et les responsabilités. Elle s'appuie sur la gestion des risques cybersécurité pour se concentrer sur les risques numériques majeurs et prendre des décisions éclairées lors des réexamens des risques.

Elle s'organise autour de comités

Le **Comité exécutif** de notre Compagnie valide la stratégie, les directives en matière de cybersécurité.

Le **Comité de direction cybersécurité** est composé du *Chief Information Officer* (CIO), du *Chief Information Security Officer* (CISO) de notre Compagnie et du directeur de la Sûreté. Le **Comité de direction cybersécurité industrielle** intégre en plus les secrétaires généraux des activités industrielles, le directeur technique* et le directeur HSE**. Ces deux comités s'assurent de la bonne application de la stratégie, définissent les évolutions de celle-ci et prennent les décisions stratégiques sur leur périmètre respectif.

Le **Comité des CISO** regroupe autour du CISO Compagnie l'ensemble des CISO des différentes activités. Il décline la stratégie dans un programme cybersécurité pluriannuel fixant les priorités cybersécurité de notre Compagnie et prend les décisions opérationnelles.

**En charge de l'ingénierie et de la R&D des activités industrielles de notre Compagnie **HSE : Hygiène Sécurité Environnement*

Référentiel de cybersécurité commun

Nos deux directives cybersécurité sont partagées avec tous nos collaborateurs. Elles sont déclinées en exigences à respecter pour être en conformité avec le niveau de cybersécurité attendu par notre Compagnie.

Elles encadrent les usages numériques professionnels.

La directive Cybersécurité est à destination exclusive des professionnels de l'IT impliqués dans la construction ou les opérations des systèmes d'information répartis dans le monde.

La directive sur l'usage des systèmes d'information, à destination de nos collaborateurs, décrit les usages numériques attendus et les comportements à proscrire.

Périmètre d'application du référentiel

Le référentiel s'applique à TotalEnergies SE ainsi qu'à toute société dans laquelle TotalEnergies SE détient, directement ou indirectement, la majorité des droits de vote et toute structure, autre que des sociétés, constitué en association avec des tiers et contrôlé par une société de la Compagnie (dont joint-ventures, GIE, partenariats…) dans le respect de leurs règles de décision respectives et sous réserve des dispositions légales et réglementaires applicables localement.

S'agissant des sociétés et des structures non contrôlées par notre Compagnie (c'est-à-dire qui ne sont contrôlées ni par TotalEnergies SE ni par l'une de ses filiales), les représentants de TotalEnergies SE ou de sa filiale au sein de ces sociétés ou structures, s'efforcent de promouvoir ce référentiel auprès de ces dernières.

Contenu du référentiel

5
2 directives
3 règles

17
principes directeurs

172
exigences

Une réponse adaptée à chaque niveau de risque

Les activités de la Compagnie dépendent fortement de la fiabilité et de la sécurité des systèmes d'information. Chaque système d'information présente un risque différent, selon les menaces auxquelles il est exposé, de leur vraisemblance et des conséquences en cas d'une cyberattaque. Les conséquences d'une cyberattaque peuvent être extrêmement dommageables : elles peuvent avoir une incidence sur la sécurité de nos collaborateurs et de nos installations, dégrader nos finances, révéler les données personnelles de nos clients ou même nuire à notre réputation, et de fait porter atteinte à nos valeurs et notre ambition.

Une approche par les risques permet une classification des systèmes d'information entreprise et industriel selon un profil de sécurité. Cette classification induit une mise en œuvre différenciée des exigences de cybersécurité. Des audits de cybersécurité permettent de s'assurer du respect de ces exigences et d'évaluer la vraisemblance des cyberattaques pour ensuite définir les plans d'action associés pour le traitement des risques et leur contrôle.

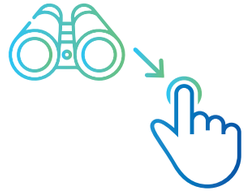
3 lignes de défense complémentaires pour 3 niveaux de protection

La ligne 1
OPÉRER

La ligne 1 est constituée de nos équipes en charge de la bonne exécution opérationnelle des mesures de cybersécurité, du maintien en condition de sécurité des systèmes et de l'intégration de la cybersécurité dans les projets, en premier lieu *via* les analyses de risques.

La ligne 1 intervient également dans le **traitement des incidents cybersécurité** de leur périmètre respectif sous le contrôle du SOC ou du CERT* selon la gravité.

La ligne 2
DÉFINIR et RÉAGIR



La ligne 2 définit les directives et règles qui constituent notre référentiel cybersécurité et contrôle leur application.

Elle gère les risques métiers et projets et pilote la gestion de crise cyber.

Elle est également en charge de l'activité de détection et de réaction aux incidents.

La ligne 3
CONTRÔLER

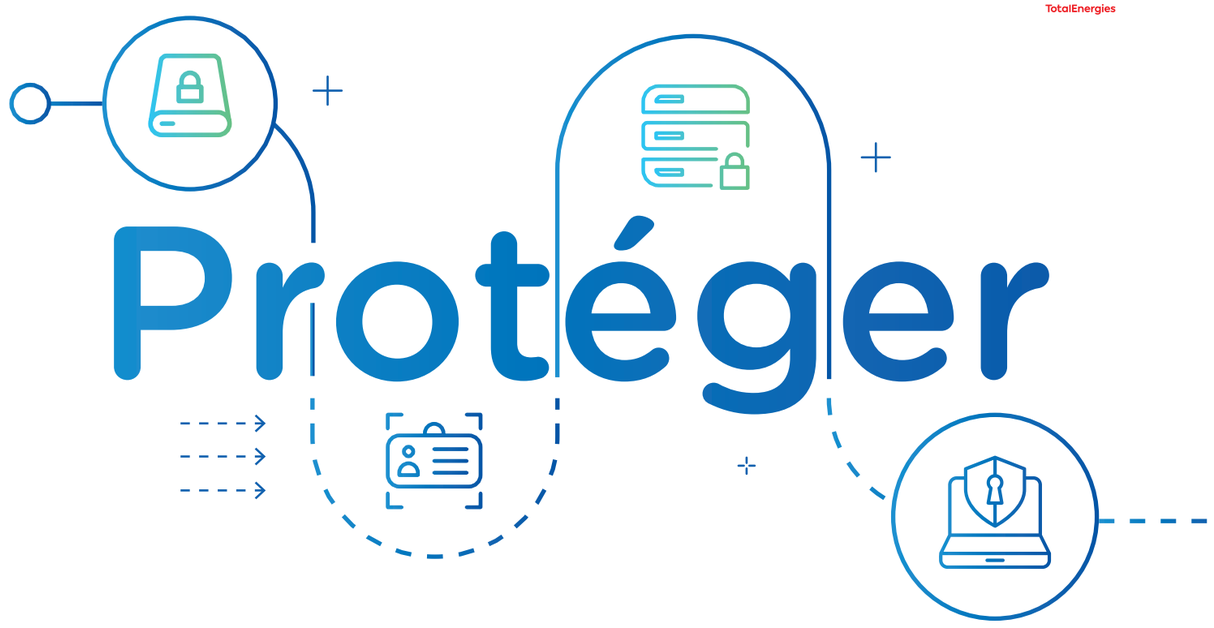
La ligne 3 s'assure que la stratégie est bien appliquée et qu'il n'y a pas de failles dans les systèmes de protection, détection et remédiation.

La direction de la Sûreté de notre Compagnie évalue, de façon indépendante, l'efficacité des mesures cybersécurité mises en place. Pour cela, elle réalise des tests en conditions réelles.

La direction de l'Audit et du Contrôle interne réalise les audits de conformité y compris sur la gouvernance cybersécurité.

La ligne 3 remonte au Comité exécutif les non-conformités critiques ou majeures.

** SOC : Security Operations Center*
CERT : Computer Emergency Response Team



La protection des données : 3 politiques de protection de l'information et une fonction dédiée

Nous protégeons nos données, celles de nos clients et partenaires, et imposons à nos fournisseurs qu'ils s'alignent sur notre niveau d'exigence. Pour cela, nous avons initié une démarche cohérente de protection en continu de l'information.

Au sein de notre Compagnie, **3 politiques** constituent le socle permettant de protéger les données détenues ou échangées. Elles permettent de protéger les systèmes d'information entreprise et industriel. Elles s'appliquent à l'ensemble de nos activités, sièges et filiales.

Le programme de protection des données personnelles (PDP) définit la gouvernance et précise les solutions disponibles au sein de notre Compagnie pour satisfaire aux exigences du règlement général sur la protection des données (RGPD), ainsi qu'aux réglementations locales.

La politique de sûreté du patrimoine informationnel (PSPI) vise à définir et faire appliquer les exigences relatives à la protection de la confidentialité, de l'intégrité, de la disponibilité de l'information détenue et échangée au sein de notre Compagnie.

Enfin, **la politique de conservation des documents (PCD)** vise à définir et à faire appliquer les exigences relatives à la conservation des documents.

Une équipe dédiée et rattachée au CISO Compagnie est responsable de la démarche de protection de l'information, du pilotage des correspondants dans les entités de notre Compagnie chargés de la mise en œuvre et du contrôle.

Le règlement général sur la protection des données (RGPD) est entré en application le 25 mai 2018. Le RGPD harmonise les règles dans l'Union européenne (UE) en offrant un cadre juridique unique aux professionnels et permet de développer leurs activités numériques en se fondant sur la confiance des utilisateurs. Cependant, les législations locales peuvent prévoir des dispositions particulières ou spéciales, qu'il convient de prendre en compte.
La Compagnie a mis en place des règles internes d'entreprise (*Binding Corporate Rules* ou BCR) approuvées par les autorités européennes de protection des données. Elles permettent d'assurer un niveau de protection homogène à travers notre Compagnie, lorsque les données sont transférées par des entités situées au sein de l'UE vers des entités de la Compagnie établies hors de l'Espace économique européen. Ces BCR établissent la gouvernance de notre Compagnie en matière de protection des données personnelles par la constitution d'un corpus de règles internes auquel chaque entité signataire est tenue de se conformer.

Des mesures de protection adaptées aux systèmes d'information industriel et entreprise

Nous cloisonnons notre système d'information industriel (SII), qui pilote nos processus de production, de notre système d'information entreprise (SIE) qui regroupe les processus de gestion, serveurs, applications indispensables à nos collaborateurs pour assurer le fonctionnement de notre Compagnie. Des mesures spécifiques de protection s'appliquent à chaque système en fonction des besoins de sécurité.

Cloisonner, différencier et détecter : nos 3 actions clés pour protéger notre SII

Notre SII interagit fortement avec notre environnement physique à travers des équipements tels que moteurs, vannes, capteurs et pompes. Cette connexion avec l'outil industriel rend la cybersécurité essentielle au regard des conséquences humaines ou environnementales que pourrait avoir un acte malveillant sur notre système d'information industriel.

CLOISONNER

pour éviter la propagation

La séparation physique des SII et SIE est la première réponse que nous apportons à leur protection. Ainsi, en cas d'une cyberattaque, ils peuvent être isolés, ce qui limite le risque de propagation. Cette séparation est assurée par un ensemble de pare-feux déployés au sein de nos sites industriels, limitant et sécurisant les échanges d'informations entre les deux systèmes d'information. Les accès des administrateurs et des fournisseurs passent par des bastions, assurant le bon déroulé de nos activités de production.

DIFFÉRENCIER

pour des réponses adaptées

Notre SII est classifié en niveaux selon la criticité des installations industrielles qu'il pilote et les risques HSE associés. Cette classification nous permet d'attribuer à chaque système d'information un niveau de sécurité attendu ou profil de sécurité. En particulier, les systèmes qui assurent la protection des personnes et des installations industrielles ont le niveau de sécurité le plus élevé, avec les mécanismes de protection les plus forts.

AUGMENTER LA DÉTECTION

pour sécuriser le processus industriel

Afin de réagir au plus vite en cas d'une cyberattaque, nous améliorons constamment notre capacité de détection notamment avec l'appui de technologies émergentes. Nous travaillons sur le déploiement d'un *Endpoint Detection and Response* (EDR) sur le périmètre industriel.

Pour assurer la protection de notre SII, nous avons développé notre suite de solutions de cybersécurité : SAFIIS*. Cette suite de solutions est déployée sur tous nos sites industriels critiques ; elle est exploitée par une équipe dédiée et le traitement des logs est intégré à notre SOC. Parmi les services de sécurité devant être implémentés, un bastion sécurise les accès à distance sur notre SII.**

** SAFIIS : Safer Architecture For Industrial Information System*
*** SOC : Security Operations Center*

Énergies renouvelables : nouvelle protection *via* le cloud

Nos équipes cybersécurité accompagnent la transformation de notre Compagnie vers les énergies renouvelables. Nos installations, telles que les éoliennes, les panneaux solaires et les bornes de recharge électrique sont implantées sur des territoires beaucoup plus vastes que nos sites industriels pétroliers. Les systèmes d'information de ces activités sont largement basés sur des solutions cloud pour accroître notre capacité de traitement des données. Nous avons adapté nos principes cybersécurité aux plateformes cloud en nous appuyant sur les nouvelles technologies de sécurité. Nous avons également modifié notre approche d'intégration de la sécurité dans les projets Agile et dans le process CI/CD (Intégration continue/ Développement continu).

La sécurité du système d'information entreprise : cloud, DevSecOps et suite XDR

UNE STRATÉGIE CLOUD

ambitieuse intégrant la sécurité et la conformité

Pour accompagner notre passage vers le cloud, nous avons conclu **deux accords stratégiques** avec les fournisseurs **Amazon** et **Microsoft**. Ces accords reposent sur des partenariats technologiques forts afin de mettre en place une **redondance de nos données**, leur assurer **une disponibilité permanente** ainsi qu'un **haut niveau de sécurité**.

Les projets développés dans le cloud suivent la méthodologie de notre Compagnie et intègrent la cybersécurité dans chacune de leurs phases. Des contrôles sont effectués pour assurer la conformité de nos plateformes à nos exigences cybersécurité.

DÉMARCHE

DevSecOps

Pour intégrer la sécurité des données tout au long du cycle d'un projet, nous nous inscrivons dans une démarche DevSecOps qui se traduit par :

- une **revue de code applicatif** portant sur la sécurité et la qualité avec la solution leader du marché ;
- une **revue des vulnérabilités des *frameworks* et des dépendances applicatives** ;
- une **méthodologie d'accompagnement des projets de développement** par des coachs spécialisés dans la cybersécurité applicative.

SUITE EXTENDED DETECTION & RESPONSE (XDR)

pour prévenir les menaces et réduire le temps de réponse

La suite XDR est un ensemble de solutions de détection et de réponses installées sur nos SI (aux sièges et dans les filiales). Ces solutions couvrent tous les *endpoints* (postes de travail, serveurs et mobiles), la messagerie, les annuaires et les clouds.

Cette suite fournit des informations corrélées aux équipes cybersécurité centrales, qui disposent ainsi d'une vision la plus exhaustive des vulnérabilités et menaces sur le périmètre couvert.

Le SOC et le CERT* *(voir pages 16-17)* disposent ainsi de moyens d'investigation avancés et de capacités de réponses rapides et efficaces pour limiter les impacts.

L'ensemble de ces solutions nous permettent d'être réactifs face aux menaces, et de bénéficier d'améliorations régulières des fonctionnalités de protection, de détection et de réaction.

Le déploiement de ces solutions assure au SOC une supervision sur une console unique. La facilité de déploiement de ces solutions et leur capacité d'extension permettent à tout nouveau périmètre de bénéficier rapidement des services opérationnels cybersécurité centralisés.

** SOC : Security Operations Center*
CERT : Computer Emergency Response Team

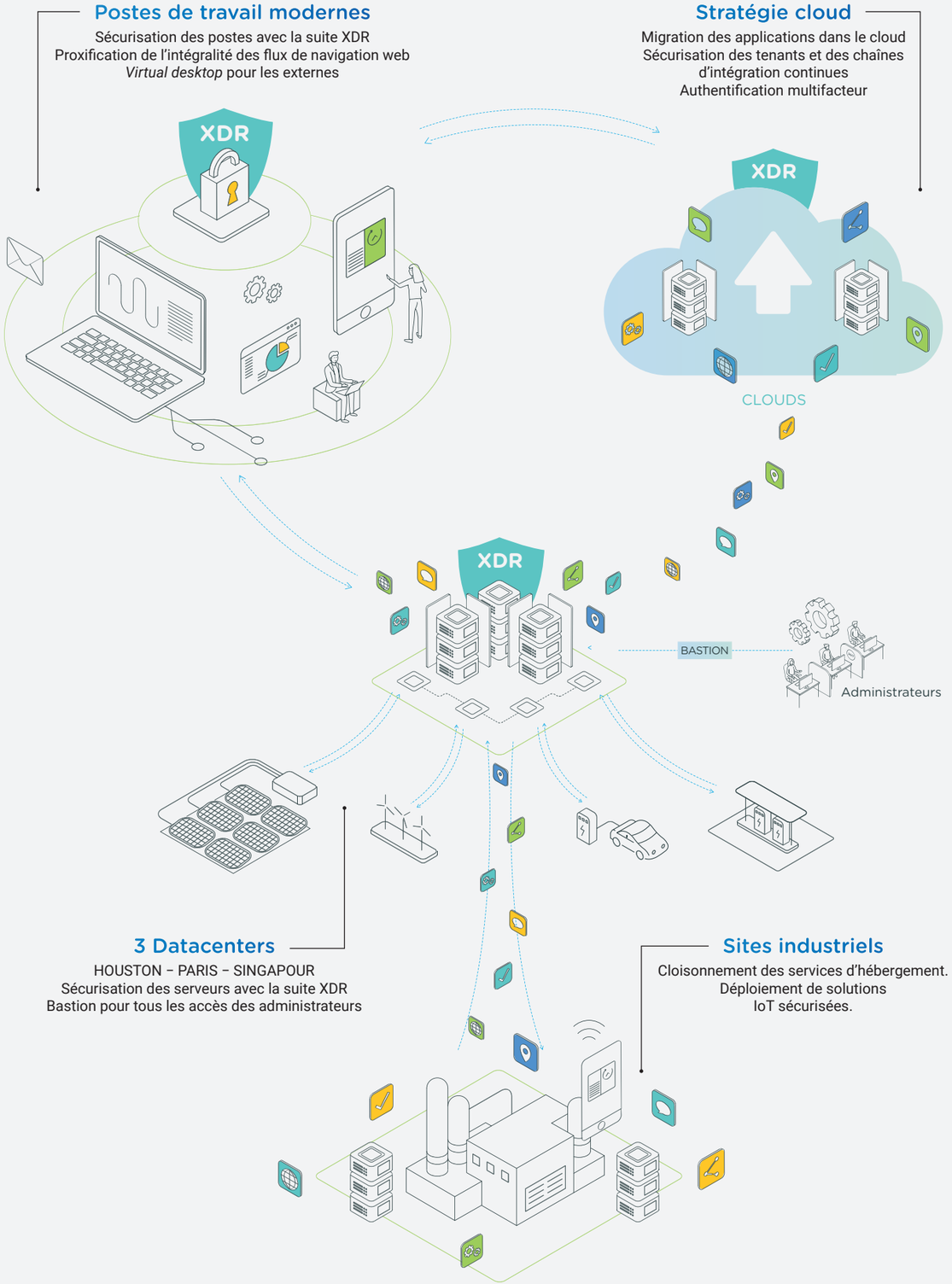
Un plan d'assurance sécurité s'impose à nos fournisseurs

Pour les prestations de service, nos partenaires décrivent dans le plan d'assurance sécurité (PAS) les mesures et contrôles qu'ils vont mettre en place pour garantir le niveau d'exigence de cybersécurité requis par notre Compagnie tout au long de la durée de leur prestation. Ces engagements font l'objet de **contrôles** et de **suivis** lors des comités opérationnels et de gouvernance planifiés.

Deux clauses contractuelles sont insérées dans les contrats avec nos fournisseurs :

- **une clause relative à la cybersécurité** définit le niveau de conformité et de sécurité attendu : certifications, traçabilité, audits externes, mais aussi formation des parties prenantes, et clauses de confidentialité ou de responsabilité ;
- **une clause relative au règlement général sur la protection des données (RGPD)** encadre le traitement et les transferts des données personnelles.

Un écosystème
moderne et monitoré



Sensibilisation et formation de nos collaborateurs : la cybersécurité est l'affaire de tous

Face à la cybermenace, les outils et solutions techniques ne peuvent pas tout. Nos collaborateurs, aussi, ont un rôle essentiel à jouer. Parce qu'ils sont les premiers maillons de notre chaîne de cyberdéfense, nous déployons un plan de formation et de sensibilisation pour les impliquer et les aider à adopter les bons réflexes.

Développer une cyberculture passe d'abord par le management

Nous avons défini des *Golden Rules,* dont 3 sont destinées aux managers métiers et 10 aux managers IT. Garants du bon respect de ces règles, les managers participent activement à leur diffusion et s'assurent de leur application au sein de leurs équipes. Il s'agit d'exigences simples, mais indispensables, comme "*Revoir annuellement les droits d'accès aux données et applications*" ou "*Organiser un exercice de crise cybersécurité annuel*" sur l'entité managée. Ces *Golden Rules* sont déployées au sein de la Compagnie dans une démarche "*Tone of the top*" *via* les comités directeurs d'entités.

Par ailleurs, à des fins d'acculturation sur la base d'exemples concrets, certains incidents font l'objet d'une diffusion large auprès de tous les collaborateurs, sous forme de fiche incident comme pour HSE, en partant du top management.

Formations dédiées et Mois de la Cybersécurité

En parallèle, nous avons développé de nombreuses formations cybersécurité accessibles depuis notre plateforme d'e-learning. Les formations se font aussi en présentiel, dans nos locaux ou au sein d'organismes que nous avons soigneusement sélectionnés. Notre Compagnie développe désormais des parcours certifiants basés sur ces formations et adaptés aux profils multiples de nos utilisateurs : manager métier, collaborateur IT, correspondant cybersécurité par exemple.

Tout au long de l'année, nous diffusons des newsletters pédagogiques et menons des actions de sensibilisation. Des actualités et bonnes pratiques cybersécurité sont diffusées *via* l'intranet et des messages de sensibilisation sont émis notamment sur les écrans de verrouillage des postes de travail.
Nous réalisons également des campagnes de *phishing* globales ou ciblées sur un site, une filiale ou un pays spécifique.

Chaque année, en octobre, nous organisons notre Mois de la Cybersécurité durant lequel nos quelque 100 000 collaborateurs sont invités à participer à des événements et à des ateliers construits sur mesure pour notre Compagnie.

À travers des vidéos, des cas pratiques, des webinars mais aussi des démonstrations de piratage, par exemple sur des systèmes d'information industriels ou des exercices en *live* d'attaque de *phishing*, ils apprennent à reconnaître les menaces et à y faire face.

L'édition 2022 a rassemblé plus de 15 000 participants à ces activités.

Le *Security Operations Center* (SOC) : une équipe dédiée à la surveillance et à l'analyse des événements de cybersécurité

Chaque seconde, et partout dans le monde, le SOC (*Security Operations Center*) analyse les informations des applications et des infrastructures SI utilisées par nos métiers. Sa mission est de détecter tous les signaux ou comportements anormaux qui pourraient être le signe d'un incident de cybersécurité. Le SOC travaille également sur la résolution des incidents de sécurité et lorsque ceux-ci deviennent complexes, il travaille en synergie avec le CERT (*Computer Emergency Response Team*).

Le SOC est une équipe interne, composée d'experts cybersécurité passionnés. Cette équipe s'appuie sur un centre de service externalisé pour assurer la supervision 24/7. Le SOC améliore en continu sa capacité de détection en fonction des évolutions des cybermenaces et du système d'information de notre Compagnie.

Le SOC rappelle si nécessaire aux collaborateurs le respect des bonnes pratiques. Il capitalise sur les traitements des incidents et propose des améliorations sur les composants des SI pour éviter que ces incidents se reproduisent.

Le *Computer Emergency Response Team* (CERT) : une équipe dédiée à la réponse aux incidents

Le CERT TotalEnergies est l'équipe en charge de mener la réponse à incident et les audits de cybersécurité au sein de toutes les entités et filiales de notre Compagnie.

Le CERT intervient **en première ligne lors d'une crise cybersécurité :** l'équipe réalise les analyses techniques et décide en conséquence et en autonomie des mesures à prendre pour résoudre un incident, comme par exemple, isoler une partie du système d'information (SI) pour contenir une menace, après validation du CISO Compagnie.
Le CERT assure également **une mission d'anticipation de la menace,** à la fois *via* une **veille sur les nouvelles vulnérabilités ou moyens d'attaques** qui émergent (*Threat Intelligence*) mais également en surveillant en permanence l'exposition publique de notre Compagnie.

Il réalise des dizaines **d'audits de cybersécurité** (organisationnel, test d'intrusion…) chaque année et suit les plans d'action qui en découlent, mettant ainsi à profit son expérience en sécurité opérationnelle pour contribuer à notre amélioration continue.

Pour mener à bien ses missions et être résilient en cas d'attaques de grande ampleur, le CERT maintient une infrastructure en propre, totalement isolée du SI de la Compagnie. Elle contient toutes les applications et outils nécessaires au bon déroulement de ses activités.

Enfin, le CERT **participe à de nombreux groupes de coopération** sur la cybersécurité comme le FIRST*, l'InterCERT France** ou l'*Oil and Gas Information Sharing Forum* (OGISF).
Cette coopération entre pairs, à l'échelle mondiale, renforce notre capacité de veille, nous permet d'être mieux informés des nouveaux modes opératoires des assaillants et d'identifier de nouvelles menaces au plut tôt.

** Forum of Incident Response and Security Teams (cf. www.first.org).*
*** L'InterCERT France est une association loi 1901. Elle constitue la première communauté de CERT en France.*

Audits et tests d'intrusion : un programme rigoureux

Nous organisons régulièrement des audits pour dresser un état des lieux de la sécurité de nos systèmes d'information à un instant donné avec pour objectif de mettre en évidence les éventuelles vulnérabilités et y remédier.

Le mode opératoire de chaque test est adapté aux types d'actifs audités (tests d'intrusion, audit organisationnel, audit d'architecture, revue de configuration). Un rapport est émis à l'issue de chaque audit. Le plan d'action qui en découle fait l'objet d'un suivi renforcé avec demande de preuves. La périodicité des audits réalisés sur un actif dépend du niveau de criticité de celui-ci.

Notre politique de divulgation responsable : un levier supplémentaire pour identifier des failles

Nous avons mis en place une politique de divulgation responsable (*Responsible Disclosure Policy*). Elle permet à toute personne découvrant une ou plusieurs vulnérabilités dans nos systèmes et réseaux informatiques (sites web, applications mobiles, etc.) de nous alerter. Elle définit et décrit précisément le cadre et les procédures de signalement : adresse mail de contact, formulaire de déclaration, respect de l'anonymat de l'informateur, protection de ses données personnelles, confidentialité des échanges…

Télétravailler en toute sécurité

Les travaux de sécurisation du système d'information en amont de la crise sanitaire, et ceux menés de façon continue durant celle-ci, ont permis au plus grand nombre de nos collaborateurs de poursuivre leurs activités en télétravail pendant les confinements et aux équipes cybersécurité de renforcer la maturité de notre Compagnie en matière de sécurité numérique.
À travers des campagnes de sensibilisation et des formations renforcées dédiées aux experts, il a également été rappelé à l'ensemble des utilisateurs la nécessité d'appliquer les bons gestes et comportements exigés dans la règle "principes d'utilisation des systèmes d'information et des ressources".

Et en cas de crise ?

Notre Compagnie a **intégré la cybersécurité à son dispositif de gestion de crise** pour se préparer et pouvoir se défendre face à une crise majeure provoquée par une cyberattaque. Notre processus de gestion de crise cybersécurité est structuré et organisé comme celui d'une crise industrielle ou environnementale, avec le même niveau d'exigences et de moyens.

La cellule de management de crise (CMC) dirige les aspects stratégiques de la situation de crise, tels que la gestion de certaines parties prenantes, la communication, les aspects juridiques et financiers, la prise en compte en anticipation des impacts potentiels de la crise en cours et la continuité d'activité. ***L'Incident Management Team*** **(IMT) dirige la réponse tactique.**

Des exercices de gestion de crise cyber, basés sur des scénarios de risques spécifiques, sont organisés chaque année. Ils permettent d'entraîner l'ensemble des parties prenantes.

Reconstruction de notre système d'information : des tests en grandeur réelle pour mesurer notre capacité à repartir de zéro

La seule solution face à un *blackout* numérique est de se préparer à en diminuer son impact et à réduire au maximum le temps d'indisponibilité des systèmes. C'est en partant de ce constat que nous avons initié un programme pluriannuel d'exercices de reconstruction de nos systèmes d'information.

UN TEST À GRANDE ÉCHELLE

Les exercices de simulation sont menés en conditions opérationnelles et à échelle réelle. En 2022, 200 personnes ont été mobilisées pendant 40 jours dans 8 pays : les équipes de production informatique, les prestataires externes chargés de la maintenance applicative, de l'infogérance et un certain nombre de fournisseurs. La simulation a porté sur 12 périmètres SI et métiers prioritaires, 8 applications qui supportent les processus critiques de notre Compagnie mais aussi les services d'infrastructure essentiels (Active Directory, orchestrateur, hyperviseur…) : au final 300 serveurs, 15 bases de données, 100 téraoctets de sauvegardes ont été testés.

TESTER NOS SYSTÈMES JUSQU'À LEURS LIMITES

Après un arrêt total de nos systèmes, les scénarios prévoient de repartir de zéro, en reconstruisant progressivement leurs différentes strates, depuis la couche basse des infrastructures jusqu'aux applications qui supportent les processus métiers de notre Compagnie. Cette démarche, inédite et innovante par son ampleur et son réalisme, présente de nombreux avantages. Sur le plan humain d'abord, elle nous permet d'évaluer notre organisation mais aussi la résilience des équipes et leurs capacités à mener des actions coordonnées en situation de crise. D'un point de vue technique ensuite, c'est l'opportunité d'éprouver aux limites nos procédures de reconstruction, la sécurisation et la robustesse de nos infrastructures et la performance de nos systèmes de sauvegarde de données. Enfin, nous associons à ces exercices nos fournisseurs de maintenance et nos prestataires pour évaluer leurs capacités et rapidité d'intervention. C'est l'occasion également de croiser nos expériences et nos fonctionnements.

Toutes les informations recueillies pendant ces phases de tests sont compilées, analysées et partagées. Leur analyse aboutit à l'identification de nouveaux leviers de sécurisation et à la définition de plans d'optimisation qui seront déployés puis de nouveau testés. Des exercices se dérouleront sur des périmètres de plus en plus larges, dans un cercle vertueux tester-apprendre-corriger-améliorer qui favorise aussi la sérendipité.

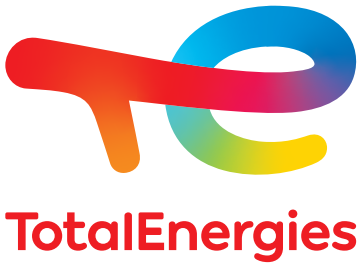
EN CHIFFRES

200
personnes mobilisées

40
jours de tests

8
équipes de maintenance impliquées

> **Par son ampleur et son réalisme, cet exercice alliant simulation d'une cyberattaque, reconstruction à partir de sauvegardes et remédiation des vulnérabilités est une première. C'est une démarche pionnière parmi les grandes entreprises industrielles similaires à la nôtre.**



TotalEnergies SE

Siège social :
2, place Jean Millier – La Défense 6
92400 Courbevoie – France

Standard :
+33 (0)1 47 44 45 46

Capital social :
6 225 655 060,00 euros
542 051 180 RCS Nanterre

totalenergies.com