Cigref
RÉUSSIR
LE NUMÉRIQUE

Anticiper les cyberattaques

De la surveillance à la gestion de crise

Mars 2024

Cigref

Anticiper les cyberattaques

De la surveillance à la gestion de crise

Mars 2024

ÉDITO

L'accélération de la transformation digitale, impulsée par les crises de ces dernières années, a conduit le RSSI à se réorganiser, à optimiser ses moyens et ressources, à rechercher à travers l'innovation comment couvrir plus efficacement son risque. L'écosystème de l'entreprise, souvent perfectible, s'est en parallèle développé accentuant ainsi les flux d'information, indispensables aux métiers, mais qui exposent chaque jour un peu plus aux cyberattaques violentes et en augmentation. Pour atténuer ces risques et garantir une meilleure sécurité, il est essentiel de mettre en place des processus solides.

C'est dans ce contexte qu'avec les membres du Cigref, nommés ci-dessous et que nous remercions, nous avons travaillé sur cette nécessité qu'est l'anticipation des cyberattaques, en identifiant les domaines prioritaires à adresser et leurs bonnes pratiques associées.

Thierry AUGER, DSI adjoint et RSSI, chez LAGARDERE
Julien LEROUX, Manager du CERT Groupe, chez EDF

SYNTHÈSE

Dans un monde de plus en plus connecté, les entreprises, grandes ou petites, se retrouvent désormais exposées à des cyberattaques de toutes sortes. La numérisation rapide des organisations a considérablement étendu leur surface d'attaque, créant ainsi un défi majeur pour préserver leur intégrité numérique.

Pourtant, cette lutte inégale se déroule dans un contexte où les moyens cyber ne sont pas répartis de manière équitable. Certaines entreprises disposent de ressources considérables pour se protéger, tandis que d'autres doivent jongler avec des budgets limités. Cette disparité crée un écart croissant entre les prédateurs cyber et leurs proies potentielles.

C'est dans ce contexte que l'anticipation des cyberattaques devient essentielle. Comprendre la menace cyber est la première étape pour prioriser les chantiers de cybersécurité. La *Cyber Threat Intelligence* (CTI) offre un éclairage précieux, permettant aux organisations de mieux appréhender les menaces qui les entourent.

Mais connaître la menace, c'est appréhender seulement la moitié du champ de bataille. Il est tout aussi crucial de connaître sa propre surface d'attaque, qui s'étend désormais au-delà des frontières physiques de l'entreprise. La migration vers le cloud, la multiplication des tiers et l'intégration croissante des systèmes industriels compliquent davantage la tâche. C'est là que le *Security Operations Center* (SOC) entre en jeu, surveillant sans relâche les systèmes d'information pour détecter toute activité suspecte.

Pourtant, la cybersécurité ne se limite pas à la protection des frontières numériques. Les attaques ont des implications bien réelles, et il est essentiel de prévoir la gestion de crise en cas de cyberattaque. Une gouvernance solide, une communication efficace et la limitation de la propagation de l'attaque sont autant de piliers essentiels pour apporter une réponse appropriée.

Aujourd'hui, anticiper les cyberattaques est devenu une nécessité incontournable pour toute organisation cherchant à prospérer dans cet environnement numérique complexe. La surveillance constante, la compréhension des menaces et la préparation à la gestion de crise sont les clés de la résilience face à cette menace omniprésente. La cybersécurité ne peut plus être reléguée au second plan, elle doit être intégrée dans le cœur même de chaque entreprise, préservant ainsi son avenir dans un monde de plus en plus interconnecté.

REMERCIEMENTS

Nos remerciements vont à **Thierry AUGER**, DSI Corporate et Directeur Cybersécurité Groupe, chez **Lagardère**, et **Julien LEROUX**, responsable cybersécurité opérationnelle du Groupe, chez **EDF**, qui ont piloté ce travail, ainsi qu'à toutes les personnes qui ont participé et contribué à ce groupe de travail Cigref (par ordre alphabétique) :

Patrick ARMUSIEAUX – MSA

Gönül BASODA – HARMONIE MUTUELLE

Véronique BARDET – LABORATOIRES PIERRE FABRE

Robert BREEDSTRAET – AMADEUS

Téodor CHABIN – TRANSDEV

Jean-Paul CHAVANT – EGIS GROUP

Jean-Marc DO LIVRAMENTO – ENEDIS

Christophe FLOCH – DASSAULT AVIATION

Benoit HERMENT – VINCI

Saïd KHALDOUNE – AUCHAN

Bruno LAURENT – AXA

Marc LEYMONERIE – AIR FRANCE KLM

Racim LOUCIF – CONFORAMA

Pascal MARY – HAGER GROUP

Gino MEUL – AVRIL

Nacira SALVAN – MINISTERE DE L'INTERIEUR

Philippe NETZER-JOLY – ARKEMA

Jean-Michel RAULOT – GROUPE ADP

Jean-Yves ROSSI – SNCF

Sébastien RUFFIER – MINISTERES SOCIAUX

Margot THIAM – ICADE

Grégoire TURCAT – GROUPE SAVENCIA

Sylvie VIALLET – PLASTIC OMNIUM

Nous remercions également vivement tous les intervenants qui ont nourri la réflexion de notre groupe de travail :

- Mickaël AUDIBERT, Responsable CSIRT, chez DASSAULT AVIATION
- Thierry AUGER, DSI Corporate et Directeur Cybersécurité Groupe, chez LAGARDERE
- Véronique BARDET, Directrice Cybersécurité, chez LABORATOIRES PIERRE FABRE
- Bertrand BLOND, Directeur des Systèmes d'Information de Cyberdéfense, chez MINISTERE DES ARMEES
- Sébastien CRESPIN, Account Executive chez WIZ
- Christophe FLOCH, RSSI, chez DASSAULT AVIATION
- Estelle JOLY, Chief Operating Officer, chez CYBERVADIS
- Julien JURIE, Regional Sales Director, chez CYBERVADIS
- Bruno LAURENT, Head of Cyber Defense, chez AXA GROUP
- Julien LEROUX, responsable cybersécurité opérationnelle du Groupe, chez EDF
- Vincent NADAL, RSSI de la Direction Data&IA, chez ORANGE INNOVATION
- Philippe NETZER-JOLY, Groupe Cyber Security Officer, chez ARKEMA
- Julia OSSELAND, Director of Product Marketing, chez CYBELANGEL
- Cyril SULTAN, Sales Director, chez WIZ
- Antoine YERAMIAN, Cloud Security Solutions Engineer, chez WIZ

Ce document a été construit et rédigé par Aurélie CHOTARD, chargée de mission au Cigref.

Nous avons utilisé pour la couverture une illustration originale de **Vincent Roland**, initialement réalisée pour notre Rapport d'orientation stratégique, publié en 2022. (https://deusexmuraena.com/).

TABLE DES MATIÈRES

TABLE DES ILLUSTRATIONS

TABLE DES ENCARTS

1 INTRODUCTION : UNE SURFACE D'ATTAQUE GRANDISSANTE POUR DES MOYENS LIMITÉS

À l'ère numérique actuelle, les organisations sont de plus en plus exposées à une menace omniprésente et insidieuse : les cyberattaques. Qu'il s'agisse de gouvernements, d'entreprises, d'institutions financières ou même de simples particuliers, personne n'est à l'abri de ces assauts virtuels qui peuvent causer des dommages considérables tant sur le plan financier que sur celui de la réputation.

La problématique qui se pose est donc la suivante : comment, dans ce contexte de menace croissante, s'organiser pour anticiper au mieux les cyberattaques ? L'enjeu dépasse largement la simple protection des systèmes informatiques, il s'agit de préserver l'intégrité, la confidentialité et la disponibilité des données, tout en maintenant la confiance des parties prenantes.

C'est dans cette optique que ce rapport a été élaboré. Notre objectif principal est de construire un processus d'anticipation face aux cyberattaques en abordant deux volets d'action essentiels :

1. **Prévenir les attaques par l'anticipation** : il est impératif de mettre en place des mécanismes de détection précoce et de prévention afin de refouler les attaquants potentiels. Cette première étape vise à renforcer la résilience des systèmes informatiques et à réduire la vulnérabilité face aux menaces cybernétiques.

2. **Anticiper la réaction à une cyberattaque réussie** : malgré toutes les précautions prises, aucune organisation n'est à l'abri d'une cyberattaque réussie. Dans ce contexte, il est essentiel de se préparer à réagir de manière efficace et efficiente en cas d'incident. Cette seconde étape consiste à développer des stratégies de gestion de crise pour minimiser les conséquences d'une attaque et garantir une reprise rapide des opérations normales.

Pour atteindre ces objectifs, nous allons étudier ces deux volets à travers les partages et les retours d'expérience des participants au groupe de travail. Cette démarche nous permettra de mettre en lumière des bonnes pratiques et de formuler des recommandations concrètes pour anticiper au mieux les cyberattaques.

Ainsi, ce rapport se veut être un guide précieux pour toutes les entités soucieuses de renforcer leur posture de sécurité dans un environnement numérique de plus en plus complexe et dangereux. La sécurité informatique ne doit plus être considérée comme une simple préoccupation technique, mais comme une composante stratégique essentielle à la pérennité et à la compétitivité des organisations.

1.1 LES ENTREPRISES SONT DE PLUS EN PLUS EXPOSÉES AUX CYBERATTAQUES

Du fait de l'interconnexion des systèmes numériques, la surface d'attaque d'une organisation s'étend de plus en plus, alors que les moyens pour la protéger ne sont pas toujours adéquats.

1.1.1 UNE SURFACE D'ATTAQUE ÉTENDUE

L'ère numérique, caractérisée par l'adoption généralisée de nouveaux outils numériques et de pratiques innovantes, a considérablement élargi la surface d'attaque des entreprises et des administrations. Cette expansion des frontières numériques a engendré une série de défis majeurs en matière de cybersécurité.

Durant la crise sanitaire, la situation s'est exacerbée. L'accélération de la transformation numérique, motivée par la nécessité de maintenir les opérations à distance, a ouvert la porte à de multiples vulnérabilités. En conséquence, le nombre de cyberattaques a connu une croissance exponentielle, impactant gravement l'activité des entreprises et des administrations. Cette situation a mis en évidence le fait que les compétences des cybercriminels évoluent bien plus rapidement que les capacités de défense des organisations. Un élément préoccupant est la montée en puissance de la cybercriminalité organisée, désormais structurée et professionnelle. Les entreprises, en particulier les PME/TPE, se trouvent souvent en position de vulnérabilité face à ces groupes d'attaquants mieux organisés.

Devant cette réalité, la question essentielle qui se pose est la suivante : **quelles technologies et quels processus doivent être mis en place pour faire face à cette menace grandissante ?** La réponse réside dans la nécessité de s'appuyer sur des bonnes pratiques éprouvées, d'agréger les ressources existantes et de développer une approche globale de la cybersécurité, d'autant que la surface d'attaque continue de s'étendre. L'adoption généralisée du *cloud computing* et le développement de l'Internet des Objets (IoT) contribuent significativement à cette augmentation. Ces nouvelles technologies apportent indéniablement des avantages en termes de flexibilité et d'efficacité, mais elles introduisent également de nouvelles vulnérabilités potentielles. De plus, le volume des données collectées, stockées et traitées par les organisations ne cesse de croître, renforçant la complexité de l'environnement numérique. Cette profusion de données offre aux cybercriminels un terrain propice à l'exploration et à l'exploitation qui nécessite une vigilance constante et des stratégies de protection adaptées.

Ainsi, dans ce contexte de surface d'attaque étendue, il devient impératif de repenser notre approche de la cybersécurité et d'adopter des mesures proactives pour anticiper les cyberattaques malgré des moyens limités.

1.1.2 DES DISPARITÉS EN TERMES DE MOYENS CYBER

Face à la montée en puissance des cyberattaques, l'Union Européenne a pris des mesures pour renforcer la cybersécurité sur le continent. La révision de la directive NIS, visant à établir un niveau commun élevé de cybersécurité au sein de l'Union, connue sous le nom de « directive NIS 2 », en est un exemple notable. Cette initiative vise à harmoniser les normes de sécurité numérique, unifiant ainsi les efforts des pays membres pour faire face aux menaces cybernétiques.

Plus récemment, le *Cyber Resilience Act* a proposé un règlement qui pourrait révolutionner l'industrie du numérique en imposant des exigences minimales de sécurité sur les produits et services numériques. Cela constituerait un pas important pour mettre fin à l'absence de normes de sécurité

claires dans ce secteur en constante évolution. Ces initiatives européennes reflètent une prise de conscience de l'importance cruciale de la cybersécurité dans l'économie numérique actuelle.

Toutefois, malgré ces efforts au niveau réglementaire, de nombreuses organisations se heurtent à des difficultés importantes. L'une des principales réside dans la pénurie de ressources humaines qualifiées en cybersécurité. Le recrutement de talents spécialisés est devenu une tâche ardue, car la demande dépasse largement l'offre, et les compétences nécessaires sont rares et précieuses.

De plus, la complexité en termes de coûts constitue un autre obstacle majeur. La mise en place de mesures de sécurité robustes peut engendrer des coûts considérables, notamment pour les petites et moyennes entreprises, qui ont souvent des budgets limités pour la cybersécurité.

Enfin, **le déploiement technologique nécessaire pour renforcer la cybersécurité est entravé par des limitations financières et technologiques**. Même si une organisation parvient à résoudre les problèmes budgétaires, elle peut encore se heurter à des défis liés aux ressources techniques et à la configuration souvent complexe de ses infrastructures informatiques. De plus, les vulnérabilités ne sont pas uniquement liées à l'organisation elle-même, mais peuvent également découler des acteurs de son écosystème.

1.2 LES PRINCIPAUX OBJECTIFS DE L'ANTICIPATION

L'anticipation des cyberattaques est au cœur de toute stratégie de cybersécurité efficace. Les principaux objectifs de cette anticipation visent à prévenir et à répondre de manière proactive aux menaces numériques, afin de minimiser les risques et les impacts sur les organisations. Voici les objectifs clés de cette démarche anticipative :

1. **Connaissance des attaques potentielles** : comprendre les types d'attaques auxquelles une organisation est susceptible d'être confrontée est un objectif clé. Cette connaissance est essentielle pour orienter les efforts de prévention et de protection vers les vulnérabilités spécifiques et les schémas d'attaques qui sont les plus pertinents.
2. **Prévention des attaques** : la prévention constitue la première ligne de défense contre les actes de malveillance. Il s'agit de mettre en place des mécanismes, des politiques et des technologies visant à empêcher les attaques de réussir. Cela implique de sécuriser les infrastructures, les processus, les données, les clients et d'autres actifs critiques.
3. **Priorisation des menaces** : étant donné que les ressources en cybersécurité sont limitées, il est essentiel de hiérarchiser les menaces en fonction de leur probabilité de survenance et de leur impact potentiel. Cette approche permet de concentrer les efforts là où ils sont le plus nécessaires et d'optimiser l'allocation des ressources.
4. **Adaptation en fonction des menaces** : l'organisation doit être en mesure de s'adapter en fonction de l'évolution des menaces. Par exemple, la réponse à une attaque en cours variera en fonction de la durée pendant laquelle l'attaquant est présent dans le système d'information. Pour les attaques de longue durée, il est nécessaire d'améliorer les capacités de détection, de blocage et de réponse en temps réel pour minimiser les dégâts.
5. **Réaction face aux attaques** : en dépit des mesures de prévention, certaines attaques peuvent réussir. Par conséquent, la capacité à réagir rapidement et efficacement en cas d'incident est

un objectif essentiel. Cela inclut la gestion de crise, l'isolement des menaces, la récupération des systèmes et des données, ainsi que la collaboration avec les parties prenantes internes et externes, y compris les partenaires commerciaux.

En somme, l'anticipation des cyberattaques vise à créer un environnement numérique plus sûr en identifiant, en prévenant et en gérant les menaces de manière proactive. En comprenant les différentes dimensions des attaques potentielles et en s'organisant en conséquence, les organisations peuvent renforcer leur posture de sécurité et minimiser les risques liés à un paysage cybernétique en constante évolution.

Les moyens mis en place par EDF

EDF a mis en place plusieurs moyens opérationnels pour anticiper les cyberattaques et protéger ses infrastructures critiques. Ces initiatives visent à renforcer la posture de sécurité d'EDF dans un contexte où la cybersécurité est devenue une préoccupation majeure pour son secteur.

Dans ce cadre, EDF a constitué des équipes dédiées au sein du groupe, comprenant un CERT (*Computer Emergency Response Team*), un VOC (*Vulnerability Coordination*) et un SOC (*Security Operations Center*) avec un pilotage opérationnel commun. Le CERT est chargé d'analyser la menace et de réagir rapidement en cas d'incident, le VOC centralise les vulnérabilités identifiées suite aux scans du groupe et accompagne les filiales dans leurs processus de remédiation, tandis que le SOC, réinternalisé depuis 2021, joue un rôle crucial dans la surveillance et la détection des menaces.

La réinternalisation du SOC a été motivée par la recherche constante d'une qualité de prestation optimale. Le *turnover* élevé au sein des managers et agents du prestataire externe impactait la continuité des activités d'EDF. Bien que la réinternalisation ait été un succès, il est important de noter que garder les collaborateurs au niveau 1 du SOC s'avère souvent difficile, car ils aspirent à évoluer rapidement. En conséquence, une partie de cette activité demeure externalisée, tandis que les niveaux 2 et 3 sont totalement internalisés. Cela nécessite un vivier de compétences important et un développement de parcours professionnels pour les collaborateurs d'EDF. Ces équipes (CERT, SOC, VOC) sont réparties sur les villes de Nanterre, Lyon, Nancy et Rennes pour une meilleure capacité de recrutement.

La surface d'attaque d'EDF est étendue en raison de ses nombreux filiales, fournisseurs et partenaires, chacun avec des niveaux d'interconnexion variables. Cette surface d'attaque continue de s'agrandir et de se diversifier, ce qui renforce la nécessité d'anticipation. Une des priorités d'EDF est de protéger ses moyens de production, en particulier dans le contexte actuel de crise énergétique. La protection des données personnelles est également un enjeu fort pour le groupe.

L'un des principaux enjeux techniques auquel EDF est confronté est la détection des menaces dans ses systèmes industriels. Pour y faire face, EDF doit innover en identifiant les moyens de détection répondant aux spécificités des SI industriels. La veille effectuée par les experts de niveau 3 du SOC[1] et de la recherche et développement du groupe EDF sur des nouvelles approches de détection telles que les « *ndr* »[2], et la « *deception*[3] » permettent de répondre à cet enjeu.

EDF a également intégré une procédure de levée de doute cyber quasiment systématique au début de chaque incident IT. Tout dysfonctionnement amène à envisager une éventuelle origine cybernétique.

Le CERT d'EDF joue un rôle crucial en ayant le mandat de couper le lien du système d'information avec un partenaire en cas de nécessité. En cas d'attaque visant un partenaire interconnecté à EDF, c'est souvent la première étape de la réponse d'EDF. En parallèle, EDF a lancé plusieurs

> projets visant à renforcer sa résilience, notamment la sécurisation de ses sauvegardes, la capacité de reconstruction en cas d'incident majeur, et la mise en place d'exercices de gestion de crise pour éprouver sa capacité de gestion de crise cyber au sein de l'organisation
>
> **Julien LEROUX**, Responsable cybersécurité opérationnelle du groupe EDF

1.3 LES DIFFÉRENTES ÉTAPES D'UNE ANTICIPATION RÉUSSIE

Une anticipation réussie des cyberattaques repose sur une série d'étapes essentielles, de la connaissance des menaces à la mise en place de processus de réponse en cas d'incident. La première étape consiste à connaître les menaces potentielles auxquelles l'organisation est susceptible d'être confrontée. Cela comprend l'identification des attaquants probables et une analyse approfondie de la menace, souvent réalisée grâce à un processus de *Cyber Threat Intelligence* (CTI). Cette analyse oriente les moyens de détection en fonction des priorités.

Cette connaissance des menaces repose sur plusieurs prérequis :

1. **Veille sur les vulnérabilités** : maintenir une veille constante sur les vulnérabilités est essentiel. Cela implique de surveiller les bulletins d'alerte pour le groupe, de les affecter directement aux services concernés et d'actualiser régulièrement la liste des vulnérabilités connues.
2. **Maintenir un référentiel de cybersécurité** : un guide d'hygiène du cyber peut être utilisé comme base pour la sécurité, pour valider les architectures et les relations partenariales. Les équipes Système d'information et Cybersécurité, doivent s'assurer d'un référentiel exhaustif et à jour incluant toutes les cartographies nécessaires (systèmes, postes de travails, réseaux, applications et leurs interfaces, partenaires, tiers, matrice des flux…).
3. **Maîtrise de la surface d'attaque** : pour contrôler sa surface d'attaque, plusieurs mesures peuvent être mises en place. Une équipe de *Red Team* peut surveiller de manière agressive la surface d'attaque pour identifier les vulnérabilités. Une gestion des accès maitrisée et complétée par la mise en place de l'authentification multi-facteurs ainsi qu'une gestion des autorisations conditionnées aux postes uniquement autorisés et la surveillance des flux

[1] Un SOC (*Security Operations Center*), dont le rôle est de surveiller, analyser et préserver la sécurité des informations d'une entreprise, regroupe des équipes d'analystes réparties en 3 niveaux distincts :

- Analyste en sécurité de niveau 1 – Tri : il classe et priorise les alertes, et fait remonter les incidents aux analystes de niveau 2 ;
- Analyste en sécurité de niveau 2 – Intervention sur incident : il examine et corrige les incidents qui lui ont été remontés, identifie les systèmes touchés et l'étendue de la cyberattaque, et utilise la cyberveille pour débusquer les cyberadversaires ;
- Analyste en sécurité de niveau 3 – *Threat Hunting* : il recherche proactivement les comportements suspects et teste et évalue la sécurité du réseau afin de détecter les menaces avancées et d'identifier les points vulnérables ou les ressources qui ne sont pas assez protégées.

Source : Qu'est-ce qu'un SOC (*security operations center*) ?, Crowdstrike, consulté le 04/09/2023

[2] Le NDR (*Network detection and response*) est une catégorie de produits de sécurité réseau détectant les comportements anormaux du système en analysant en permanence le trafic réseau. – *Network detection and response*, Wikipédia, consulté le 15 février 2024.

[3] La technologie de déception est une catégorie de solutions de cybersécurité qui permet de détecter rapidement les menaces avec un faible taux de faux positifs. Cette technologie déploie des leurres réalistes (par exemple, des domaines, des bases de données, des répertoires, des serveurs, des applications, des fichiers, des informations d'identification, des fils d'Ariane) dans un réseau, aux côtés d'actifs réels, qui agissent comme des appâts. – Qu'est-ce que la technologie de tromperie ?, Zscaler, consulté le 15 février 2024.

renforcent également la sécurité. Des audits, des contrôles et des tests d'intrusion (*pentests*) sont réalisés pour évaluer la résilience de l'infrastructure.

4. **Détection et blocage** : la détection et le blocage des menaces en temps réel sont essentiels pour contrer les attaques, il faut de la technologie pour cela, les équipes cherchent à optimiser et à innover en remplaçant, dès que cela est pertinent, un outil installé par une solution plus efficace et moins lourde à gérer. Un *Security Operations Center* (SOC) est mis en place pour qualifier les alertes et lancer des actions en cas de besoin. Le *Threat Hunting* consiste à traquer les attaquants déjà présents dans le système d'information. Les indicateurs de compromission (IOC) connus sur Internet sont intégrés aux moyens de détection, ils sont partagés au sein des communautés sectorielles dès que cela est possible du fait de l'efficacité que cela apporte.
5. **Réagir en cas d'incident** : préparer des processus de réponse à incident est crucial pour réagir rapidement en cas de cyberattaque réussie. Des fiches réflexes avec des étapes d'action claires sont élaborées, permettant d'agir à distance. Ces processus sont adaptés à certaines menaces spécifiques. Réagir en cas d'incident c'est aussi avoir, en amont, sécurisé les contenus nécessaires à cela, et bien entendu garantir un jeu de données protégé.
6. **Amélioration de la cybersécurité** : plusieurs moyens peuvent être utilisés pour améliorer la cybersécurité, notamment la mise en place d'un SOC, la standardisation de l'infrastructure, la réalisation d'audits, la mise en place d'outils de surveillance et de protection (EDR, proxy, firewall…), la sensibilisation des décideurs, la mise en place de la double authentification (MFA), l'évaluation des fournisseurs et la contractualisation avec des exigences minimales de sécurité, etc.
7. **Priorisation des processus de sécurité** : pour allouer efficacement les ressources, il est important de prioriser les processus de sécurité. Cela peut être fait en utilisant une matrice de risques (impact/probabilité) pour adapter les mesures de sécurité aux risques identifiés. La communication avec les métiers est essentielle pour comprendre les risques principaux. Il est également conseillé de suivre les orientations des institutions spécialisées et de se conformer aux exigences contractuelles.
8. **Mise à jour de la priorisation** : les données issues de la surveillance doivent être régulièrement mises à jour pour refléter l'évolution des menaces. Il est crucial de garantir la disponibilité et la fonctionnalité des sauvegardes pour pouvoir récupérer les données de l'entreprise après une attaque.

En suivant ces étapes, une organisation peut renforcer sa capacité à anticiper, détecter et réagir efficacement face aux cybermenaces, tout en s'adaptant à un paysage de cybersécurité en constante évolution.

2 CONNAITRE LA MENACE POUR PRIORISER SES CHANTIERS CYBER

La compréhension de la menace cyber est désormais au cœur de la sécurité de toute organisation. Dans ce contexte, la *Cyber Threat Intelligence* (CTI) joue un rôle crucial. Cette partie explore les fondements de la CTI et la façon dont elle permet aux entreprises de mieux anticiper, comprendre et réagir face aux menaces cyber. La CTI devient un atout stratégique pour assurer la sécurité des activités et des données, en s'appuyant sur des pratiques avancées de collecte, d'analyse et d'intégration des informations sur la menace cyber.

2.1 LE PROCESSUS DE *CYBER THREAT INTELLIGENCE* (CTI)

Un processus de *Cyber Threat Intelligence* (CTI) est essentiel pour appréhender la menace cyber et prioriser les efforts de cybersécurité. Le premier objectif de la CTI est d'**identifier les menaces majeures** auxquelles l'entreprise est confrontée. Ces menaces peuvent prendre différentes formes, notamment :

- Menaces avancées (APT) : ces attaques sont particulièrement sophistiquées et ciblent généralement des organisations de manière soutenue et persistante. Elles sont difficiles à détecter et à contrer.
- Fraudes via ingénierie sociale : il s'agit de tactiques visant à tromper les employés, par exemple, en utilisant de fausses factures ou des techniques de manipulation psychologique.
- Vol d'informations/Fuites de données sensibles : les cybercriminels cherchent à accéder et à divulguer des informations confidentielles de l'entreprise.
- Actions par des ex-salariés : certaines menaces peuvent provenir d'anciens employés motivés par une volonté de nuire ou de se venger.
- Attaques par déni de service (DDoS) : ces attaques visent à rendre les services de l'entreprise indisponibles en submergeant ses serveurs de trafic malveillant.
- Exploitation d'une vulnérabilité sur un logiciel ou équipement largement répandu : dans ce cas, la menace s'exprime de manière opportuniste, sans viser de populations en particulier.
- Menaces ciblant le secteur d'activité/zone géographique : les attaques peuvent également être spécifiques à un secteur d'activité ou à une région géographique.

En fonction des menaces identifiées, il est essentiel de **structurer la réponse en cybersécurité**. Par exemple, si les menaces APT sont les plus probables, il faut concentrer les ressources et les mesures de sécurité sur cette catégorie.

Pour identifier ces menaces, la CTI **collecte des informations** provenant de différentes sources, notamment :

- Sources d'informations institutionnelles, telles que le CERT-FR, l'ANSSI, Inter-Cert, etc.
- Informations en interne issues du SOC de l'entreprise.

- Informations issues des partenaires : la collaboration avec d'autres entreprises et organisations, typiquement au sein d'une communauté sectorielle, pour partager des informations sur les menaces.
- Informations en sources ouvertes (OSINT) : la surveillance d'Internet et du *Dark Net* à l'aide de mots-clés liés à l'entreprise mais aussi de marqueurs uniques qui vont aider à qualifier directement un incident, une intrusion.
- Informations provenant de sociétés Cyber spécialisées adaptant leur recherche aux spécificités des entreprises (fournitures de mots clés par exemple).
- Retours d'expérience suite à un incident : l'analyse des incidents passés pour tirer des enseignements.

Les informations collectées en CTI comprennent les Indicateurs de Compromission (IoC) tels que les domaines suspects, les URL malveillantes, les adresses IP associées à des activités malveillantes, etc. Les tactiques, techniques et procédures (TTP) des attaquants sont également examinées, ainsi que les groupes d'attaquants et leurs modes opératoires. Ces informations sont ensuite traitées par les équipes du CERT (*Computer Emergency Response Team*) et du CSIRT (*Computer Security Incident Response Team*) de l'entreprise pour mieux comprendre les menaces et adapter les mécanismes de défense.

2.2 LES PRINCIPALES SOURCES D'INFORMATION À DISPOSITION DES ORGANISATIONS

Pour renforcer leur posture en matière de cybersécurité et anticiper les menaces, les organisations ont accès à une multitude de sources d'informations essentielles. Voici les principales sources auxquelles elles peuvent se fier :

1. **CERT-FR** : accessible au grand public, le CERT-FR joue un rôle central en fournissant des alertes de sécurité et en informant sur les menaces majeures. Il constitue une référence en matière de cybersécurité en France.
2. **US-CERT** : le CERT américain fournit des informations pertinentes sur les menaces cyber et les vulnérabilités. Ses rapports sont largement suivis à l'échelle internationale.
3. **CSIRT régionaux** : ces équipes régionales relaient les informations provenant du CERT-FR. Leurs activités sont principalement axées sur la réponse aux incidents, ce qui les rend précieuses pour les organisations locales.
4. **CERT sectoriels** : certains secteurs d'activité spécifiques disposent de leur propre CERT, comme le M-CERT pour le secteur maritime et le CERT-Aviation pour l'aviation. Ces organismes sectoriels se concentrent sur les menaces pertinentes pour leur domaine.
5. **Sources ouvertes** : plusieurs ressources en ligne fournissent des informations cruciales pour la CTI, notamment :
    a. MITRE ATT&CK : base de données classifiant les tactiques, techniques et procédures (TTP) des attaquants.
    b. MalwareBazaar : base de données de malwares qui permet d'identifier les menaces actuelles.

c. ABUSE.CH : source d'informations sur les domaines malveillants et les botnets.
d. AlienVault : plateforme de sécurité qui collecte et partage des informations sur les menaces.

6. **Sources privées** : des spécialistes français et étrangers de la CTI proposent des informations de qualité, facilement intégrables dans les outils de sécurité de l'entreprise. Les flux des opérateurs SOC (*Security Operations Center*) peuvent également constituer une source très intéressante, bien que l'extraction des données soit nécessaire.
7. **Communautés** : les communautés cyber, qu'elles soient composées de CERT, CSIRT, ou d'experts en sécurité, jouent un rôle important dans le partage d'informations et d'expertise. Les discussions sur les réseaux sociaux, notamment sur Twitter, peuvent également fournir des indications précieuses.
8. **Incidents internes** : les propres incidents de l'organisation sont une source cruciale d'informations. Ils doivent être analysés en profondeur pour en tirer des enseignements et renforcer la posture de cybersécurité.

Pour faciliter la collecte, l'organisation et le partage des Indicateurs de Compromission (IoC) et d'autres informations de CTI, différentes solutions sont disponibles :

- MISP (*Malware Information Sharing Platform & Threat Sharing*) : cet outil mature permet de collecter, organiser et partager les IoC avec les partenaires de manière efficace.
- OpenCTI : il s'agit d'un outil plus récent, proposé par l'ANSSI, orienté vers le traitement d'informations de haut niveau en CTI.
- Des outils commerciaux : des solutions commerciales telles que ThreatQuotient et Anomali offrent des fonctionnalités avancées pour la gestion des informations de CTI.

En combinant judicieusement ces sources d'information et en utilisant des outils adaptés, les organisations peuvent renforcer leur capacité à anticiper les menaces cyber et à prendre des mesures proactives pour se protéger contre les cyberattaques.

2.3 TRAITEMENT DES INFORMATIONS ISSUES DE LA CTI ET INTÉGRATION AUX PROCESSUS CYBER

L'intégration efficace des informations provenant de la *Cyber Threat Intelligence* (CTI) dans les processus cyber est cruciale pour renforcer la posture de sécurité d'une organisation. Les informations de CTI, telles que les indicateurs de compromission (IoC) et les tactiques, techniques et procédures (TTPs) des attaquants, sont identifiées et classifiées. Par exemple, si l'adresse IP d'un attaquant est connue et déjà identifiée, cela permet de déterminer la nature de l'attaquant et les méthodes potentielles de l'attaque. Ces informations sont ensuite intégrées dans les processus opérationnels, notamment au sein du *Security Operations Center* (SOC). Par exemple, les IoC et les TTPs sont utilisés pour :

- **Prioriser les corrections de vulnérabilités** : si des vulnérabilités sont activement exploitées par des attaquants, elles sont traitées en priorité pour minimiser les risques.
- **Enrichir les schémas de détection** : les schémas de détection sont régulièrement mis à jour en fonction des tendances dans le mode opératoire des attaquants. Par exemple, en cas

d'évolution rapide de la menace, les règles de détection peuvent être modifiées rapidement pour s'adapter.

- **Partager avec la communauté** : les informations de la CTI sont souvent partagées au sein d'une communauté d'intérêts communs, ce qui permet aux organisations de collaborer pour se protéger mutuellement.
- **Enrichir des outils de protection et de détection** : Les IoC sont intégrés aux outils de sécurité pour renforcer leur efficacité. Cette fonction peut être automatisée pour une réponse rapide.

Au-delà des activités opérationnelles, **la CTI joue un rôle clé dans l'élaboration de la stratégie globale de l'entreprise en matière de cybersécurité**. Elle fournit des informations de qualité qui facilitent la prise de décisions au plus haut niveau de l'organisation, notamment par le Comité Exécutif (COMEX). Ces informations peuvent influencer les arbitrages budgétaires en fonction de l'état de la menace. En effet, la CTI contribue à la mise à jour des analyses de risques de référence de l'entreprise, en fournissant des informations sur les menaces actuelles et émergentes. Des sociétés spécialisées peuvent également intervenir pour analyser le contexte géopolitique et contribuer à la définition de la stratégie cyber.

De manière globale, il existe trois niveaux de traitement de l'information en CTI, en fonction de la quantité d'informations et du degré d'automatisation :

- Niveau basique : ce niveau implique une collecte manuelle d'informations en réponse à des alertes, par exemple en provenance de l'ANSSI ou d'autres sources. Les informations sont traitées au cas par cas, souvent de manière rudimentaire, sans outils de CTI. Cela permet de mener des activités opérationnelles de base, mais sans enrichir les outils de sécurité avec les IoCs.
- Niveau maîtrisé : à ce niveau, la collecte d'informations est semi-automatisée, avec une analyse, une consolidation et une organisation plus approfondies. Les informations sont stockées dans des outils de CTI et utilisées pour des activités tactiques ou stratégiques. Certaines tâches d'enrichissement des outils de sécurité sont automatisées.
- Niveau optimisé : ce niveau implique une automatisation avancée, avec la mise en place de processus de scoring sur les informations de CTI. L'enrichissement des outils de sécurité est automatisé en fonction du scoring et de la période de validité des informations.

Pour résumer, le traitement et l'intégration des informations de CTI dans les processus cyber sont essentiels pour anticiper les menaces, améliorer la réactivité et renforcer la stratégie globale de cybersécurité de l'organisation. Plus l'intégration est avancée, plus l'entreprise est en mesure de se protéger contre les cyberattaques efficacement.

Création d'un CSIRT chez DASSAULT AVIATION

Dassault Aviation, soucieux de gérer les menaces cyber actuelles et d'anticiper les risques futurs, a pris des mesures importantes pour renforcer sa posture de sécurité.

Un besoin de comprendre l'environnement cyber extérieur

L'une des motivations clés de la création du CSIRT (*Computer Security Incident Response Team*) chez Dassault Aviation était la nécessité de mieux comprendre l'environnement cyber extérieur. Il était essentiel de mesurer la capacité de l'entreprise à résister aux cyberattaques et à les anticiper. Cette démarche s'est développée progressivement sur plusieurs années :

- Mars 2019 : préparation d'une convention cyber entre les industriels de défense et le ministère des Armées.
- Septembre 2019 : décision interne à Dassault Aviation de mettre en place son propre CSIRT, à partir d'une équipe issue d'un SOC de niveau 3.
- Novembre 2019 : signature de la convention cyber avec le ministère des Armées, accompagnée par un groupe de travail sur le partage de l'information et l'évolution des modes de gouvernance.
- Février 2020 : recrutement d'un RSSI adjoint, avec une expertise reconnue dans la création de centres opérationnels de cyberdéfense.
- Mai 2020 : début du renforcement de l'équipe de sécurité opérationnelle. Avant la création du CSIRT, l'entreprise comptait deux analystes SOC de niveau 3. Actuellement, le CSIRT est constitué de 6 personnes.
- Novembre 2020 : début du parcours d'incubation avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).
- Mars 2021 : entrée du CSIRT Dassault Aviation à l'InterCERT FR, réseau national de réponse à incidents de sécurité informatique.
- Octobre 2022 : lancement de la communauté de défense au sein de l'InterCERT FR.

Communication et partage d'informations avec le COMEX

Pour évaluer en permanence l'état de la menace et informer les instances décisionnelles, Dassault Aviation utilise une trame d'information cohérente. Une note mensuelle est transmise au Comité Exécutif (COMEX), et la fréquence de communication peut être augmentée en cas d'événements graves.

Cette note comprend les éléments suivants :

- Description de la menace : une analyse détaillée des menaces cyber actuelles et potentielles.
- Incidents partenaires : les incidents de sécurité informatique survenus chez des partenaires ou dans le secteur de l'aérospatiale et de la défense.

- Autres actualités cyber : les informations pertinentes sur les tendances et les évolutions dans le domaine de la cybersécurité.

En annexe, la note inclut des informations sur les menaces étatiques et la cybercriminalité, ainsi qu'une liste des incidents partenaires. Cette approche proactive permet au COMEX d'être informé rapidement en cas d'événements graves, prévenant ainsi les répercussions potentielles.

Mickaël AUDIBERT, Responsable CSIRT, chez DASSAULT AVIATION

Christophe FLOCH, RSSI, chez DASSAULT AVIATION

3 CONNAITRE SA SURFACE D'ATTAQUE POUR SURVEILLER L'ENSEMBLE DE SES SYSTÈMES D'INFORMATION

Au-delà de la connaissance de la menace, l'appréhension en interne de sa surface d'attaque est un facteur clé pour anticiper une cyberattaque, surtout quand celle-ci s'étend à l'occasion d'une migration dans le cloud, ou du fait de la multiplication des tiers.

3.1 MIGRATION VERS LE CLOUD ET EXTENSION DE LA SURFACE D'ATTAQUE

La migration vers le cloud représente une étape majeure pour de nombreuses entreprises, mais elle ne vient pas sans son lot de défis en matière de cybersécurité. **L'un des problèmes majeurs rencontrés réside dans la complexité inhérente au cloud**. Si le cloud public offre une gamme diversifiée de services pour la construction d'applications, il diffère considérablement des pratiques précédentes en local (*on-premises*). Lorsque les entreprises cherchent à sécuriser entièrement leur environnement cloud, elles peuvent être confrontées à des problèmes de gestion de l'identité. En effet, le cloud offre de nombreuses options pour gérer les identités et les accès, ce qui est à la fois facteur de flexibilité et de complexité.

Le cloud a également apporté de nouveaux services et technologies, ce qui constitue un défi supplémentaire en termes de compréhension des risques associés à ces services émergents. Les entreprises doivent être en mesure de suivre ces évolutions technologiques pour s'assurer qu'elles restent protégées contre les menaces actuelles et futures. Il est nécessaire dans ce cas de s'assurer que les ressources intègrent bien les bons profils qui sauront garantir une configuration à l'état de l'art.

La complexité des opérations de sécurité augmente également avec la migration vers le cloud. Souvent, les équipes de développement et les équipes de sécurité travaillent de manière séparée, ce qui peut entraîner des lacunes en matière de sécurité. Il est essentiel d'impliquer les équipes de développement dans la sécurisation des projets cloud et de leur fournir un contexte global sur les outils de sécurité.

De plus, les solutions de sécurité cloud génèrent de nombreuses alertes, ce qui peut entraîner un bruit excessif. Il peut être difficile de déterminer quelles alertes sont les plus critiques et nécessitent une intervention immédiate.

Les menaces récentes ciblant le cloud incluent des attaques sur les APIs, qui sont devenues courantes. Une mauvaise configuration des authentifications d'une API peut permettre des fuites massives de données. De plus, les équipes informatiques manquent souvent d'une vision d'ensemble des APIs utilisées dans l'entreprise, ce qui rend difficile la gestion de ces points d'entrée potentiels pour les attaquants. Les attaques de type « Lapsus » visent à exploiter les erreurs humaines, souvent en ciblant les employés pour accéder à leurs données et aux ressources de l'entreprise. Une mauvaise gestion de l'accès initial dans le cloud peut faciliter ces attaques. Enfin, l'exposition de données sensibles est un risque constant. Les mauvaises configurations des serveurs de bases de données peuvent les rendre

accessibles depuis Internet, permettant ainsi l'accès non autorisé aux données. Identifier et protéger ces données sensibles est essentiel pour éviter des fuites de données coûteuses.

Pour faire face à ces nouveaux risques, **l'approche aujourd'hui la plus efficace va consister à faire appel à de la technologie spécialisée (comme les scanners de vulnérabilités, les plateformes de gestion de la conformité cloud ou les outils de cartographie de l'infrastructure)** afin de surveiller l'ensemble des solutions exploitées sur le Cloud et ainsi de pouvoir remonter au SOC, les erreurs de configuration, les vulnérabilités, les mauvaises pratiques ou tout simplement une cartographie exhaustive, premier besoin vital.

La sécurité du cloud avec WIZ

Wiz, société présente sur le marché depuis trois ans, propose une solution de sécurité du cloud qui a déjà séduit de nombreuses entreprises françaises. Son approche vise à garantir la protection des données et des ressources cloud. La solution de Wiz offre une couverture complète, prenant en charge tous les principaux fournisseurs de services cloud. Elle fonctionne grâce à des scans qui permettent d'identifier les vulnérabilités, les *malwares*, les secrets, les données sensibles, les mauvaises configurations ainsi que les problèmes liés aux identités et aux permissions. La solution se distingue par la suite en développant des contextes autour de ces différents problèmes de sorte à aider les équipes de sécurité afin qu'elles se concentrent sur les quelques contextes importants plutôt que d'essayer de tout résoudre.

Un contexte critique (également appelé combinaison toxique), selon Wiz, découle de différents facteurs : la gravité de la faille, la facilité pour un attaquant de profiter de celle-ci et finalement l'étendue des dégâts ou le mouvement latéral qui peut en découler. Cette approche ciblée permet aux équipes de sécurité de se concentrer sur les problèmes les plus importants et de réduire le bruit des alertes inutiles.

En complément de cette approche, Wiz propose plusieurs fonctionnalités essentielles, notamment :

- Un inventaire de toutes les technologies (software, librairie, etc.) déployées dans le cloud.
- Une cartographie de toutes les données sensibles.
- Une détection en temps réel des tentatives d'attaque ainsi que des comportements suspects qui permet de prévenir les attaques potentielles.
- Une vérification de la conformité aux recommandations des principaux fournisseurs et entreprises de cybersécurité, ainsi qu'aux différentes certifications, assurant ainsi que les meilleures pratiques sont suivies.
- L'intégration dans les pipelines CI/CD des développeurs, de sorte à corriger en amont, avant de déployer en production.

Finalement, Wiz permet aux équipes projet d'accéder à la plateforme pour obtenir des informations sur leurs propres projets cloud. Cela facilite l'intégration des préoccupations de sécurité dès le début du processus de développement.

REX de la Direction Data&IA d'Orange Innovation

Lors de la migration vers le cloud de leur direction, la Direction Data&IA d'Orange Innovation a rapidement ressenti le besoin d'une solution offrant une visibilité maximale sur leur environnement cloud. La solution Wiz s'est avérée idéale, car elle ne nécessite pas l'installation d'un agent sur les postes de travail et permet d'obtenir rapidement une vue complète de tous les projets cloud. Cette solution se concentre sur les risques réels plutôt que de se limiter à la simple conformité aux normes.

Wiz assure également un environnement de confiance en effectuant tous les scans sur site, ne transmettant que les métadonnées à l'entreprise. Cette approche renforce la sécurité tout en garantissant la confidentialité des données.

Enfin, l'interaction avec l'équipe de Wiz s'est avérée fluide, permettant ainsi d'adapter la solution aux besoins changeants de l'entreprise au fil du temps. La flexibilité et la réactivité de Wiz ont été des atouts majeurs pour garantir une cybersécurité efficace dans le cloud.

Sébastien CRESPIN, Account Executive chez WIZ

Cyril SULTAN, Sales Director chez WIZ

Antoine YERAMIAN, Cloud Security Solutions Engineer, chez WIZ

Vincent NADAL, RSSI de la Direction Data&IA, chez ORANGE INNOVATION

3.2 L'ORGANISATION DE LA CYBERSÉCURITÉ À L'ÉCHELLE D'UN SECTEUR D'ACTIVITÉ

L'organisation de la cybersécurité à l'échelle d'un secteur constitue un défi majeur à une époque où les menaces numériques se multiplient. Dans un contexte où de nombreuses entreprises et organisations opèrent au sein d'un même secteur d'activité, il est essentiel de **mettre en place des mécanismes de collaboration et de partage d'information pour renforcer la résilience collective face aux cyberattaques**. Cette approche sectorielle vise à mutualiser les ressources, les bonnes pratiques et les connaissances en matière de cybersécurité afin de mieux anticiper, prévenir et répondre aux menaces qui pèsent sur l'ensemble du secteur. Elle repose sur la coopération entre les acteurs du secteur, la définition de normes et de standards communs, ainsi que sur une vigilance constante pour protéger les infrastructures critiques et les données sensibles.

Le cas de l'industrie de la défense

Créé en 2017, le Commandement de la Cyberdéfense (COMCYBER) assure la planification et la conduite dans le cyberespace des opérations de type défensives, offensives, et informationnelles.

La naissance d'une convention entre les 8 principaux maîtres d'œuvres industriels et le ministère des armées découle d'un constat flagrant, fait en 2018, de l'augmentation forte des attaques cyber passant par la *supply chain*. La numérisation grandissante des systèmes d'armes apporte de nouvelles fonctionnalités opérationnelles nécessaires aux forces armées mais elle implique une augmentation forte du risque cyber associé, nécessitant la mise en place de mesures de protections et de détection mais également d'une politique de sécurité importante afin de gérer l'obsolescence de certains composants. L'innovation dans le domaine de la défense favorise donc l'existence d'un terrain de jeu pour les attaquants qui s'étend des systèmes de communication IT traditionnels, aux systèmes d'armes ainsi qu'aux systèmes industriels, créant ainsi un spectre global dont les conditions de protection et de défense doivent être collectivement travaillées État/industrie.

À la suite de nombreuses attaques médiatisées dès 2017, la chaine de sous-traitance PME/TPE/ETI est donc apparue comme un maillon faible, et plus facile d'accès par rapport aux « gros » industriels qui ont globalement, depuis plusieurs années, renforcé leur niveau de cybersécurité. Ainsi, l'idée d'instaurer une démarche commune pour élever collectivement le niveau de sécurité a émergé, considérant que la cybersécurité doit nécessairement devenir une véritable performance et non plus uniquement une contrainte.

En 2019, la ministre des Armées, Florence Parly, fait une annonce officielle au Forum International de la Cybersécurité (FIC) et propose aux huit maîtres d'œuvres industriels de s'unir collectivement avec le MINARM et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour définir un plan d'action réaliste visant à limiter ce risque de la *supply chain attak*. Une convention est alors signée le 14 novembre 2019, le pilotage de ces travaux sera confié au COMCYBER et à la DGA.

Les objectifs de la convention

En positionnant la cybersécurité comme une performance, l'idée était bien de co-construire, Minarm/industrie, les conditions de montée en sécurité sur les programmes d'armement et de ne pas uniquement rentrer dans une logique de coûts contractuels. La valorisation de ces travaux, notamment dans le cadre d'export de matériel à l'international était une cible privilégiée dès le départ, prenant en compte le fait que certains marchés imposent déjà des contraintes cyber (cf référentiel CMMC US). Il s'agissait donc de permettre aux industriels de valoriser leur engagement et de leur permettre d'en faire notamment un véritable argument de performance face à d'autres compétiteurs étrangers.

Les travaux se sont déroulés sur 36 mois et ont été organisés en 12 groupes de travail co-pilotés par l'État et l'industrie autour de trois thématiques : la sécurisation des systèmes d'armes,

l'anticipation et évaluation de la menace, et la réponse à incident (simplification de la chaîne de réponse à incident pour la rendre plus efficace).

Avec une implication très forte de l'ensemble des acteurs, les travaux réalisés durant ces trois ans ont permis d'atteindre les objectifs fixés initialement et sont considérés collectivement État/industrie comme une réussite. La création d'une véritable communauté d'échange et de partage d'information appelée « ***le cercle de confiance cyber*** » a permis de déployer la première communauté française des CSIRT du secteur défense, visant à échanger collectivement et en temps réel sur la menace pour pouvoir s'en prémunir ensemble.

Enfin, l'année 2022 a permis de tester les livrables sur 12 programmes pilotes, et la généralisation des résultats des travaux à la totalité des programmes d'armement est en cours depuis début 2023. La réalisation d'un exercice cyber commun annuel de grande ampleur (DEFNET/ORION) permet de s'entrainer collectivement sur les processus de gestion de crise État/industrie mis en place dans le cadre de cette convention.

Les enseignements collectifs et les réalisations très pragmatiques de ces travaux, permettent aujourd'hui d'imaginer leur extension à d'autres industriels de la défense sur le même modèle.

Bertrand BLOND, Directeur des Systèmes d'Information de Cyberdéfense au MINISTÈRE DES ARMÉES

3.3 LA MULTIPLICATION DES TIERS COMME NOUVELLE SOURCE DE VULNÉRABILITÉS

À mesure que les organisations élargissent leur écosystème de fournisseurs et de partenaires, la cybersécurité devient une préoccupation croissante. Les tiers, qu'ils soient fournisseurs, partenaires commerciaux ou sous-traitants, sont devenus une source incontournable de vulnérabilités potentielles. Cette multiplicité des tiers est devenue un enjeu majeur en matière de sécurité. Pourtant, les métiers ne tiennent pas toujours compte du risque cyber lorsqu'ils choisissent leurs partenaires, créant ainsi des failles potentielles dans la chaîne de sécurité. La mauvaise visibilité sur les composants des solutions fournies par les tiers, le manque de moyens pour gérer les incidents cyber, les contractualisations sans exigence cyber, et la complexité de la gestion des accès aux tiers sont autant de problèmes qui se posent. Pour réduire ces risques et garantir une meilleure sécurité, il est essentiel de mettre en place des processus d'évaluation cyber solides, et de partager les responsabilités avec les tiers. Dans cette section, nous explorerons plus en détail les enjeux liés à la multiplication des tiers en tant que nouvelle source de vulnérabilités et les stratégies pour limiter les risques.

3.3.1 LES TIERS COMME VECTEURS DE CYBERATTAQUES

Lorsqu'on envisage la question des tiers dans le contexte de la cybersécurité, plusieurs défis se posent. En effet, les métiers au sein des organisations ne tiennent pas toujours compte du risque cyber

lorsqu'ils choisissent leurs tiers. Il est donc impératif de les **sensibiliser à l'impact cyber des tiers, même de petite taille, afin de mieux évaluer et gérer ce risque**. La solution la plus adaptée étant la mise en place d'un processus de gestion des tiers, centralisé et partagé par tous les métiers concernés. Il permettra dans ce cadre à l'équipe Cybersécurité de mettre en place les évaluations et qualifications.

Une des premières difficultés est d'obtenir une liste exhaustive des fournisseurs de l'organisation. Une autre question réside dans le manque de visibilité sur les composants des solutions fournies par les tiers, qui rend difficile l'évaluation correcte de la sécurité de ces solutions. Par ailleurs, les tiers ont souvent moins de ressources pour gérer les incidents cyber, et de nombreuses contractualisations avec eux se font sans aucune exigence spécifique en matière de cybersécurité, ce qui laisse un vide potentiellement dangereux. La gestion des accès accordés aux tiers est également complexe et peut devenir un point de vulnérabilité.

Pour résoudre ces problèmes et uniformiser l'évaluation du niveau de maturité cyber des tiers, il serait nécessaire de développer un standard européen d'évaluation. Mais pour l'instant, la seule option est d'intégrer des exigences cyber dans le cadre des contrats et des relations avec les tiers. **La gestion des tiers doit en effet commencer dès la contractualisation, en incluant des exigences spécifiques en matière de cybersécurité.**

En cas de cyberattaque chez un tiers, il est essentiel d'adopter une approche proactive. Cela peut impliquer la suspension immédiate des échanges avec l'entreprise concernée, ce qui permet d'identifier le secteur impacté. Pour les partenaires critiques, il est crucial d'établir des contacts avec leurs responsables de la sécurité de l'information (RSSI) en amont, de manière à réagir efficacement en cas d'incident et à minimiser les risques pour l'ensemble de l'organisation.

3.3.2 LE PARTAGE DE RESPONSABILITÉ AVEC LES TIERS

La gestion de la cybersécurité implique souvent un partage de responsabilité entre les différentes parties prenantes que sont les achats/*end users*, les responsables de la sécurité de l'information, et les tiers.

Le rôle des achats/*end users* tout d'abord, consiste à identifier les tiers à évaluer en fonction des besoins et des exigences de l'organisation. Ils disposent également d'outils permettant de faciliter le processus d'évaluation et peuvent accéder à tout moment aux recommandations de l'InfoSec (sécurité de l'information).

De leur côté, **les responsables de la sécurité de l'information** ont pour mission de définir les critères de sélection des tiers, de mettre en place un outil ou un processus d'évaluation rigoureux, d'analyser les résultats de ces évaluations et de détecter les fournisseurs présentant un risque potentiel. Ils partagent ensuite leurs recommandations en interne pour contribuer à la prise de décision et à la gestion des risques. De plus, ils collaborent activement avec les fournisseurs pour les aider à améliorer leur posture en matière de cybersécurité.

Quant aux **tiers**, ils jouent également un rôle essentiel dans ce processus. Ils obtiennent les résultats de leur évaluation, ainsi qu'un plan de remédiation collaboratif s'ils présentent des vulnérabilités ou des faiblesses en cybersécurité. Ils ont également la possibilité de mutualiser leurs efforts en partageant les résultats de leurs évaluations avec d'autres organisations, favorisant ainsi la

transparence et la confiance dans l'écosystème des fournisseurs. En fin de compte, les tiers peuvent faire de la cybersécurité un avantage compétitif en démontrant leur engagement envers la sécurité et en inspirant confiance à leurs clients.

Mutualiser les questionnaires de sécurité avec CYBERVADIS

CyberVadis est une plateforme dédiée à l'évaluation de la cybersécurité des fournisseurs qui répond à des objectifs essentiels pour renforcer la sécurité dans l'écosystème des tiers.

Son approche vise tout d'abord à identifier tous les tiers susceptibles de mettre en risque l'organisation. Ensuite, ces tiers sont évalués en utilisant une méthodologie adaptée et régulièrement mise à jour pour refléter les évolutions des menaces. L'équipe de sécurité collabore activement avec les fournisseurs à risque pour les aider à améliorer leur posture en matière de cybersécurité et elle émet des recommandations.

L'implication de tous les membres de l'organisation pouvant contractualiser avec un tiers est primordiale afin qu'ils intègrent les recommandations de l'InfoSec dans leurs processus de décision. Les grandes entreprises, confrontées à une augmentation des incidents liés aux tiers, ressentent la pression réglementaire et doivent déployer de nombreuses solutions malgré des ressources limitées.

D'un autre côté, les fournisseurs sont souvent submergés par des questionnaires de sécurité disparates et disposent de ressources limitées pour se consacrer à la cybersécurité. La mutualisation des évaluations cyber offre une solution pour « monter à l'échelle » des deux côtés, en remplaçant les tâches redondantes sans valeur ajoutée par un temps mieux investi dans la détection des menaces et la réaction à celles-ci.

Pour la réussite d'un tel programme, cinq facteurs clés sont à prendre en compte : définir précisément le périmètre à couvrir, clarifier les rôles et responsabilités en interne, développer une stratégie de communication pour impliquer toutes les parties prenantes, simplifier au maximum les processus et les outils, et enfin, s'assurer que les informations sont accessibles à ceux qui en ont besoin, notamment les acheteurs.

Plusieurs entreprises clientes de CyberVadis opérant dans le même secteur peuvent mutualiser leurs évaluations, ce qui facilite l'identification de fournisseurs déjà évalués. CyberVadis respecte la confidentialité des informations des fournisseurs et ne partage pas leurs données sans leur consentement. Le modèle de mutualisation est particulièrement bénéfique pour les entreprises d'un même secteur, car il permet de tirer parti des évaluations existantes pour renforcer la cybersécurité de l'ensemble de l'écosystème des fournisseurs.

Estelle JOLY, Chief Operating Officer, chez CYBERVADIS

Julien JURIE, Regional Sales Director, chez CYBERVADIS

3.4 LE RÔLE DU SOC DANS LA SURVEILLANCE DES SI

Le *Security Operations Center* (SOC) joue un rôle central dans la surveillance, la détection et la réponse aux menaces cyber qui planent sur les systèmes d'information des organisations. Dans cette section, nous explorerons en détail le fonctionnement du SOC, son évolution et ses diverses responsabilités.

3.4.1 L'ORGANISATION D'UN SOC

Le Centre des Opérations de Sécurité, ou SOC, constitue l'épine dorsale de toute organisation moderne pour anticiper et répondre aux menaces cyber. Traditionnellement, les SOC[4] sont structurés en trois niveaux opérationnels, mais ils doivent évoluer pour relever les défis à venir.

Pour optimiser son fonctionnement**, le SOC doit être doté d'une gouvernance rigoureuse**. Une feuille de route détaillée avec des priorités claires devra être construite, tandis qu'un comité de gouvernance arbitrera toutes les décisions de priorisation. Les informations seront ensuite partagées au sein de la communauté de gestion des risques du groupe.

Un enjeu majeur pour tout SOC réside dans la gestion des faux positifs. L'automatisation joue ici un rôle essentiel. Plus l'automatisation est efficace, plus les alertes d'importance seront rapidement traitées. Une question centrale est de savoir comment intégrer au mieux le SOC dans l'écosystème informatique global de l'entreprise.

Pour favoriser la transparence et la collaboration, un portail peut être créé. Chaque composante d'un groupe pourrait y consulter l'ensemble des incidents, évaluer son niveau de sécurité par rapport aux normes MITRE ATT&CK, et suivre l'évolution de la menace grâce aux données de la CTI.

Aujourd'hui, **un nouveau défi se pose pour l'organisation des SOC avec l'évolution de l'intelligence artificielle qui représente à la fois une menace potentielle et une opportunité**. Par exemple, Microsoft a fait des démonstrations d'une IA générative développée spécifiquement pour les CERT, dans l'objectif de les accompagner en cas d'attaque, notamment dans les opérations de *forensic*[5].

[4] Un SOC (*Security Operations Center*), dont le rôle est de surveiller, analyser et préserver la sécurité des informations d'une entreprise, regroupe des équipes d'analystes réparties en 3 niveaux distincts :

- Analyste en sécurité de niveau 1 – Tri : il classe et priorise les alertes, et fait remonter les incidents aux analystes de niveau 2 ;
- Analyste en sécurité de niveau 2 – Intervention sur incident : il examine et corrige les incidents qui lui ont été remontés, identifie les systèmes touchés et l'étendue de la cyberattaque, et utilise la cyberveille pour débusquer les cyberadversaires ;
- Analyste en sécurité de niveau 3 – Threat Hunting : il recherche proactivement les comportements suspects et teste et évalue la sécurité du réseau afin de détecter les menaces avancées et d'identifier les points vulnérables ou les ressources qui ne sont pas assez protégées.

Source : Qu'est-ce qu'un SOC (*security operations center*) ?, Crowdstrike, consulté le 04/09/2023

[5] L'analyse forensique (plus fréquemment appelée « forensic ») consiste à investiguer un système d'information après une cyberattaque. Les analystes vont collecter l'ensemble des données brutes (fichiers effacés, disques durs, sauvegardes, journaux des systèmes…), les étudier pour comprendre ce qu'il s'est passé et établir des conclusions. – Forensic, Tehris, consulté le 15/02/2024.

Modernisation du SOC d'AXA : passage au cloud public

Le SOC (*Security Operation Centre*) est un service centralisé utilisé pour supporter la sécurité du groupe AXA pour l'ensemble de ses sociétés. Cette centralisation engendre des défis importants. On peut citer, par exemple, la répartition géographique des systèmes d'information à surveiller qui sont dispersés à travers le monde, mais aussi le volume et la variété des données à traiter.

Des investissements majeurs dans la protection du SI ont permis de renforcer la sécurité : AXA a lancé il y a quatre ans un vaste projet pour moderniser et renforcer les capacités de son SOC et donc sa capacité de détection en bénéficiant notamment de sa stratégie de migration vers le cloud public.

Pourquoi le choix du cloud public ? En termes de gestion des données, le cloud public offre des performances et des capacités de scalabilité extrêmement élevées. Il élimine les projets de renouvellement d'infrastructure et permet de gérer la croissance des volumes aisément. Les différents types de stockage et la flexibilité de la puissance de calcul permettent d'adapter les technologies aux besoins. Cette souplesse est essentielle dans un environnement réglementé comme celui des assurances où le besoin de performance sur les données récentes doit coexister avec le besoin réglementaire, soit d'historisation des données (qui peut être de plusieurs années), soit de suppression de celles-ci. La transition vers le cloud public permet aux équipes de sécurité de se concentrer uniquement sur la sécurité, plutôt que de gérer des projets d'infrastructure lourds et à faible valeur ajoutée.

Pour maintenir une défense en profondeur et une plus grande indépendance, AXA a choisi de ne pas s'appuyer exclusivement sur un seul fournisseur de cloud. L'outil de détection et de réponse aux incidents (EDR) a été déployé sur un autre cloud, ce qui permet au SOC d'AXA de bénéficier de deux fournisseurs distincts.

Cependant, le passage au cloud public n'a pas été exempt de défis. La collecte des données, la récupération des historiques et la réécriture des logiques de sécurité à partir d'un environnement traditionnel vers le cloud public ont nécessité un programme IT majeur avec une gouvernance incluant des représentants IT, sécurité et risque. La gestion des coûts variables du cloud est également un enjeu majeur. La maitrise des coûts via un modèle Finops devient essentiel pour maîtriser les dépenses avec le passage à un mode de paiement à la consommation. Les nouvelles manières de travailler doivent être aussi adressées : formation des équipes sur le cloud public, passage des fonctions de gestionnaires d'infrastructures à gestionnaires de services cloud, création de la fonction Finops …

Du point de vue de l'organisation, le choix d'AXA a été de maintenir une expertise 24/7 pour la gestion des incidents de sécurité en interne. Pour d'autres services comme la *cyber threat intelligence* (CTI) un modèle hybride de *sourcing* a été choisi, permettant de bénéficier d'une expertise externe dans un environnement de menace qui évolue très vite, tout en étant capable

> d'interpréter celle-ci dans l'environnement interne de la société. Les fonctions à faible valeur ajoutée et répétitives sont traitées à l'extérieur.
>
> **Bruno LAURENT**, Head of Cyber Defense, chez AXA GROUP

3.4.2 OBJECTIF DU SOC : COUVRIR L'ENSEMBLE DES RISQUES CYBER RELATIFS AU SI DE L'ORGANISATION

Le rôle essentiel d'un *Security Operations Center* (SOC) au sein d'une organisation est d'anticiper les menaces cyber, de réagir rapidement aux incidents de sécurité, et de garantir la protection des actifs informatiques. Pour atteindre cet objectif essentiel, plusieurs axes de travail sont mis en place :

- **Anticipation des menaces** : le SOC doit être proactif en matière de cybersécurité. Il ne se contente pas de réagir aux incidents, mais cherche à anticiper les menaces émergentes. Cela implique de surveiller en permanence les tendances de la cybercriminalité, les vulnérabilités potentielles et les indicateurs avancés de compromission (IAC).
- **Réactivité optimale** : en cas d'incident, le SOC doit réagir rapidement pour minimiser les dommages potentiels. Cela nécessite une organisation efficace, des procédures bien définies et une coordination sans faille entre les membres de l'équipe.
- **Couverture globale** : le périmètre du SOC ne se limite pas uniquement au système d'information (SI) interne de l'organisation. Il s'étend également aux partenaires, aux sous-traitants et aux fournisseurs, car les menaces peuvent émerger de l'extérieur du SI.
- **Surveillance continue** : la surveillance continue du SI est essentielle. Le SOC doit être opérationnel 24 heures sur 24, 7 jours sur 7 pour détecter les menaces dès qu'elles se manifestent. Cette vigilance constante permet d'identifier rapidement les comportements suspects.
- **Automatisation des processus** : pour gérer efficacement le flux constant d'alertes et d'incidents, le SOC automatise autant que possible les processus de détection, d'analyse et de réponse. Cela inclut l'automatisation de la collecte de données, de l'analyse comportementale et de la réponse aux incidents.
- **Collaboration intégrée** : le SOC collabore étroitement avec d'autres services de l'organisation, tels que les équipes informatiques, les responsables de la conformité et les métiers. Cette collaboration permet de mieux comprendre les enjeux métiers et de prioriser la sécurité en fonction des besoins spécifiques.
- **Utilisation de la *Cyber Threat Intelligence* (CTI)** : le SOC s'appuie sur les informations de CTI pour mieux comprendre les menaces en évolution et pour adapter sa stratégie de sécurité en conséquence.
- **Amélioration continue** : enfin, le SOC cherche constamment à s'améliorer. Il analyse les incidents passés pour identifier les points faibles, ajuste les procédures en conséquence et reste à l'affût des nouvelles technologies et des meilleures pratiques en matière de cybersécurité.

Collaborer pour s'améliorer chez SNCF

Pour s'adapter à la vie du SI et aux schémas d'attaque, les règles de détection du SOC sont nécessairement en perpétuelle évolution, tant sur le maintien en condition de l'existant et l'ajustement de seuils que sur l'implémentation de nouvelles règles, en fonction de la feuille de route du SOC et de la stratégie de détection.

La mise en œuvre de structures Blue Team (CERT et SOC) et Purple Team (CERT, SOC Red Team) chez SNCF, sont des dispositifs de collaboration efficaces pour évaluer la pertinence des règles et leurs améliorations potentielles.

La Blue Team recherche en continu des améliorations potentielles en s'appuyant sur ses connaissances du SI de l'entreprise.

Au jeu du chat et de la souris, la Red Team (équipe interne pour SNCF) tente d'exploiter discrètement (… ou non) les vulnérabilités identifiées, là où SOC et CERT tentent de détecter et de contrecarrer.

La collaboration entre ces 3 équipes s'articule autour du partage des schémas d'attaques détaillés et des impacts associés (source : Red Team), du constat de détection ou non, et de la protection éventuelle. Un travail commun permet d'envisager l'évolution des règles existantes - ou la mise en œuvre de nouvelles – pour obtenir le blocage effectif de la menace, soit à court terme soit définitif. Suite à l'application de ces règles, un rejeu du même scénario sera réalisé quelques temps après par la Red Team pour s'assurer de la bonne efficacité opérationnelle.

Outre l'amélioration globale de la couverture des vulnérabilités, les structures Blue Team et Purple Team favorisent un échange mutuel entre équipes d'experts et créent les conditions nécessaires au rapprochement, à l'engagement et à la solidarité, des éléments précieux et indispensables dans le cadre de la gestion de crise Cyber.

Jean-Yves ROSSI, Sécurité Opérationnelle (CERT / SOC), chez SNCF

La surveillance des réseaux parallèles avec CYBELANGEL

Cybelangel est une société présente depuis une décennie sur le marché de la cybersécurité qui a étendu son expertise bien au-delà de la France pour servir des clients internationaux, notamment aux États-Unis, au Moyen-Orient et en Asie. Son approche est résolument orientée vers la protection des entreprises de tous les secteurs d'activité contre les menaces du monde numérique.

L'approche de Cybelangel, unique sur le marché, repose sur sa capacité à opérer en dehors du périmètre informatique traditionnel de ses clients. L'entreprise se spécialise dans la détection de divers risques cyber, notamment :

1. Recherche de fuites de données sur le *Dark Web* : Cybelangel surveille activement le *Dark Web* pour identifier les données sensibles de ses clients qui pourraient y être exposées. Cette surveillance vise à anticiper les fuites de données et à agir en conséquence.
2. Détection des risques de *phishing* : en scrutant les noms de domaines dormants et les comportements suspects en ligne, Cybelangel identifie les menaces de *phishing* potentielles qui pourraient viser ses clients.
3. Gestion des informations d'identification (*credentials)* : l'entreprise traque ces informations, telles que les adresses e-mail, les mots de passe et les clés API, qui ont pu être compromises et sont en circulation sur des forums clandestins.
4. Identification du *shadow IT* : Cybelangel détecte les éléments inconnus du système d'information de l'entreprise, offrant ainsi une visibilité sur les éventuelles failles de sécurité.
5. Prévention des fuites de données par tiers : l'entreprise surveille également les tiers, fournisseurs et partenaires des clients, pour identifier toute fuite de données potentielle susceptible de les affecter.

Lorsqu'un incident est détecté, Cybelangel fournit des rapports d'incident détaillés et contextualisés. La détection repose sur des mots-clés convenus avec le client, et la société propose des recommandations pour résoudre rapidement l'incident et prévenir de futures occurrences.

En moins de 24 heures, à la suite du déploiement de Cybelangel, une menace peut être détectée et des mesures de remédiation immédiatement proposées. L'entreprise joue un rôle actif dans la sélection des mots-clés pertinents pour maximiser la précision de la détection.

Les résultats sont significatifs. En utilisant la solution de Cybelangel, Lagardère a reçu, chaque année, plus de 300 alertes, ce qui a permis de prévenir des crises potentielles et de gérer les incidents, alors qu'il en était encore temps, avec une efficacité accrue. Ces alertes peuvent être variées, allant d'une fuite de données sur un espace ouvert du cloud ou un système de stockage mal protégé, d'une *backdoor* détectée en Chine à la diffusion non autorisée d'informations

> sensibles sur les installations électriques, en passant par des fuites causées par des tiers ou des employés.
>
> **Julia OSSELAND**, Director of Product Marketing, chez CYBELANGEL
>
> **Thierry AUGER**, DSI Corporate et Directeur Cybersécurité Groupe, chez LAGARDERE

3.5 UN CAS SPÉCIFIQUE : LA SÉCURITÉ DES SYSTÈMES INDUSTRIELS

Les systèmes industriels s'interconnectent de plus en plus avec les systèmes informatiques traditionnels de l'entreprise, mais sans répondre aux mêmes standards de sécurité. Côté industriel, la perception du risque n'est pas la même et les métiers hésitent à ajouter des couches de sécurité car cela engendre des effets sur leurs opérations, d'autant que les solutions cyber ne sont pas forcément adaptées au contexte industriel. Par ailleurs, la DSI reprend de plus en plus la main sur ces environnements qui échappaient auparavant à son contrôle.

Quel est l'impact de la convergence IT/OT sur l'augmentation des menaces cyber ?

3.5.1 LES DIFFÉRENCES ENTRE LA GESTION DES RISQUES IT ET DES RISQUES OT

La gestion des risques liés aux technologies de l'information (IT) et aux technologies industrielles (OT) présente des particularités significatives. **Les usines et les entrepôts font face à une complexité accrue, avec des systèmes intelligents embarqués provenant d'une multitude de fournisseurs**. De plus, la longévité des équipements industriels, en moyenne de 10 ans, ne cadre pas toujours avec la rapidité requise pour gérer les vulnérabilités en informatique traditionnelle (IT).

À l'horizon des 5 prochaines années, de nouveaux défis se profilent dans le domaine de la sécurité des systèmes industriels. L'intelligence embarquée dans les automates s'intègre de plus en plus au cloud et au SI global, nécessitant une interconnexion IT/OT agile pour soutenir les flux de bout en bout, des fournisseurs jusqu'aux clients.

La gestion des risques dans le secteur industriel vise principalement à identifier les vulnérabilités majeures et à mettre en place un processus opérationnel de cybersécurité, y compris une supervision des tiers.

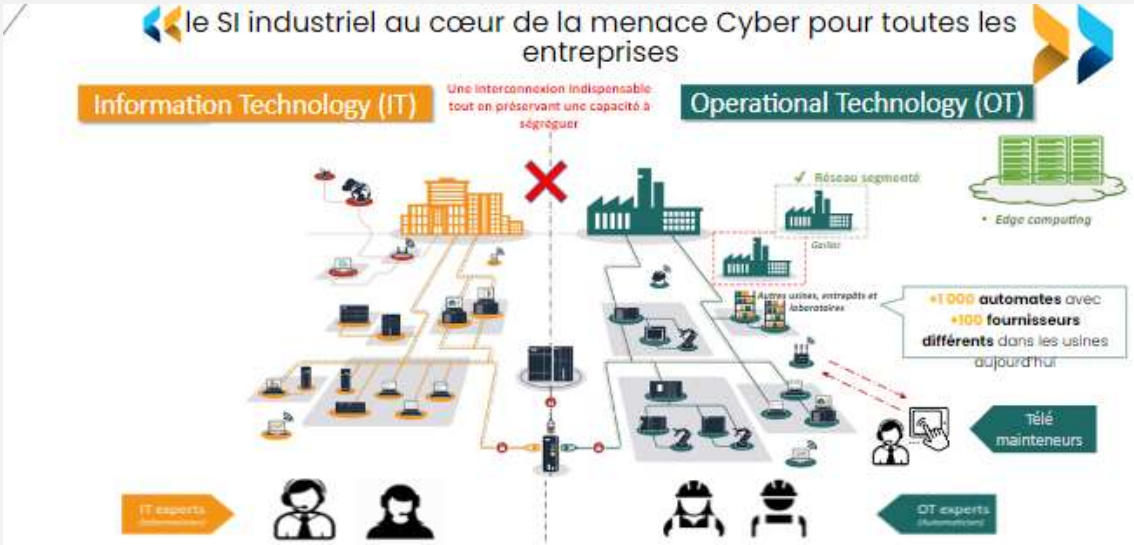
Pour atteindre ces objectifs, diverses bonnes pratiques sont recommandées, notamment :

- L'instauration de processus de sécurisation dès la conception des nouveaux systèmes industriels ;
- La définition d'éléments de cybersécurité essentiels pour l'environnement industriel ;
- L'élaboration de clauses spécifiques pour les partenaires industriels ;
- La sensibilisation des équipes industrielles aux enjeux cyber ;
- L'isolement initial du périmètre industriel ;
- La présence d'équipes de sécurité dédiées au sein de l'environnement industriel ;

- L'accent mis sur la sécurisation de l'IT dans les opérations industrielles ;
- La réalisation d'audits et de tests de pénétration pour évaluer le niveau de maturité de la cybersécurité, notamment par bâtiment.

L'amélioration de la sécurité du SI industriel chez LABORATOIRES PIERRE FABRE

Les Laboratoires Pierre Fabre opèrent, dans le secteur pharmaceutique, **18 sites logistiques**, créant un environnement complexe. Toutefois, l'un des défis majeurs réside dans la perception des métiers industriels quant à leur implication dans le domaine de l'informatique. De nombreux aspects de la maîtrise des actifs, de la proactivité et de la capacité de réaction, propres à l'informatique traditionnelle (IT), sont transposés à la sphère industrielle.



Le SI industriel au cœur de la menace cyber pour toutes les entreprises.

Source : Laboratoires Pierre Fabre

L'interconnexion croissante entre l'IT et les usines accentue la complexité, avec un système d'alertes intensifié, car l'IT est de plus en plus connecté aux usines et aux sites de production. Bien que la frontière entre ces deux environnements subsiste, elle devient de plus en plus souple et perméable. Chaque usine présente des caractéristiques uniques, et leur niveau de connectivité varie.

Les défis dans le SI industriel incluent la gestion de plus de 1000 automates, des centaines de fournisseurs peu sensibilisés à la cybersécurité (souvent sans clauses de notification en cas d'attaque) et des prestataires de maintenance à distance. Actuellement, les équipes en charge de la cybersécurité mettent en place une gestion des vulnérabilités potentielles et la détection d'attaques.

Pour faire face à ces enjeux actuels et futurs, cinq besoins fondamentaux ont été identifiés : distinguer tous les composants IT des automates et assurer leur maintien en condition de sécurité, faciliter les communications sécurisées entre le SI industriel, le cloud et le SI de gestion, mettre en place une surveillance des réseaux industriels pour détecter les vulnérabilités et les attaques, réagir à des événements atypiques potentiellement malveillants, et permettre la reconstruction des systèmes en cas de dysfonctionnement.

> Les risques associés au SI industriel peuvent avoir un impact significatif sur le SI de gestion, notamment la propagation d'une attaque cyber, l'altération des données due à des droits octroyés de manière non maîtrisée, une longue indisponibilité du SI industriel suite à une incapacité de reconstruction, l'obsolescence non maîtrisée exposant le SI à des vulnérabilités, et le risque de prise de contrôle du système industriel.
>
> **Véronique BARDET**, Directrice Cybersécurité, chez LABORATOIRES PIERRE FABRE

3.5.2 LA PROPRIÉTÉ INTELLECTUELLE COMME LEVIER DE CYBERSÉCURITÉ DANS L'ENVIRONNEMENT INDUSTRIEL

La cybersécurité dans le secteur industriel exige une réflexion approfondie sur la protection de la propriété intellectuelle. Il est crucial de reconnaître que de nombreux incidents de sécurité récents ont résulté de problématiques liées à la fuite de données industrielles sensibles telles que des plans d'usines, qui ont été involontairement exposés sur Internet. La complexité réside dans le fait que, pour maintenir leurs opérations, les entreprises industrielles doivent fréquemment partager ces informations avec des sous-traitants dont la maturité en matière de cybersécurité est souvent faible.

Parmi les données les plus sensibles pour une entreprise industrielle figurent également les procédés industriels. Cette réalité constitue un point d'ancrage essentiel pour sensibiliser les responsables des sites industriels à l'importance de la cybersécurité. La question cruciale devient alors : comment protéger les données liées aux procédés industriels, partagées avec des tiers, afin de maintenir leur intégrité et leur confidentialité ?

Protéger le patrimoine intellectuel de l'entreprise chez ARKEMA

Arkema est une société de chimie française qui opère principalement dans le secteur du BtoB (business-to-business). Bien que générant environ un tiers de son chiffre d'affaires en Europe, l'entreprise exerce son activité dans le monde entier, avec une présence dans 55 pays. En 2022, Arkema a déposé 250 brevets dans divers domaines tels que la découverte de nouvelles molécules ou les procédés industriels. Cette diversité géographique et technologique nécessite une approche globale de la sécurité de l'environnement industriel.

L'industrie chimique étant fortement axée sur l'innovation, la protection du patrimoine intellectuel de l'entreprise est cruciale. Cela inclut la sauvegarde des découvertes de molécules, des procédés de fabrication et d'autres informations confidentielles qui représentent un atout essentiel pour l'entreprise.

L'expansion rapide de la technologie numérique, en particulier en Chine, où le renouvellement des équipements industriels se fait plus rapidement, ajoute une dimension supplémentaire à la question de la sécurité. Les entreprises doivent non seulement protéger leurs innovations, mais aussi s'adapter à l'évolution constante de l'environnement technologique.

En termes d'organisation, Arkema s'appuie sur des CISO (*Chief Information Security Officer*) régionaux, des experts en sécurité de l'information qui sont responsables de la sécurité au niveau local. De plus, la supervision au niveau mondial de la sécurité est assurée par un CISO industriel qui veille à ce que les pratiques de cybersécurité soient cohérentes dans toutes les régions. Cette approche garantit que la sécurité de l'information est gérée de manière efficace à l'échelle de l'entreprise, tout en prenant en compte les spécificités locales.

La gestion de la cybersécurité dans le secteur industriel est souvent similaire à celle de l'informatique, bien que les environnements industriels puissent présenter des défis particuliers. Il est essentiel d'harmoniser les processus de gestion des données et des incidents pour garantir une approche globale de la sécurité de l'entreprise.

La protection du patrimoine intellectuel de l'entreprise est un objectif fondamental pour Arkema, et cela nécessite une collaboration étroite entre les équipes de cybersécurité, les responsables régionaux et mondiaux, ainsi que l'ensemble de l'organisation. En fin de compte, cette approche globale contribue à assurer la sécurité des données sensibles et à préserver la capacité d'innovation d'Arkema dans un environnement concurrentiel mondial.

Philippe NETZER-JOLY, Groupe Cyber Security Officer, chez ARKEMA

4 ANTICIPER SA GESTION DE CRISE EN CAS DE CYBERATTAQUE

Un rapport dédié à la gestion de crise cyber a été publié par le Cigref en février 2023. Cette dernière partie vient le compléter en présentant les aspects d'anticipation à la crise qui sont nécessaires pour réagir au moment de sa survenue.

4.1 PRÉVOIR LA GOUVERNANCE DE LA GESTION DE CRISE

La gestion d'une crise cyber nécessite une coordination soigneuse entre différentes équipes, chacune ayant des responsabilités techniques et stratégiques. Ces équipes doivent travailler de concert pour gérer les impacts de la crise, tout en veillant à rétablir le bon fonctionnement du système touché.

Sur le plan décisionnel, il est essentiel d'intégrer la Direction des Systèmes d'Information (DSI) ou le Responsable de la Sécurité des Systèmes d'Information (RSSI) dans un système de gestion de crise bien établi. La présence de ces experts en sécurité de l'information permet d'informer rapidement les décideurs sur la situation actuelle de l'attaque et de fournir les informations nécessaires pour adapter et coordonner les actions correctives.

En parallèle, une autre équipe, souvent désignée comme la **« cellule de crise opérationnelle »**, est chargée d'analyser la situation technique en profondeur et de proposer des mesures concrètes pour rétablir l'activité normale. Cette cellule s'appuie sur une expertise technique pointue pour évaluer les dégâts, identifier les vulnérabilités et élaborer des plans de rétablissement.

L'organisation de la cellule de crise ne doit pas être improvisée au moment de la crise elle-même. Elle doit être planifiée en amont, en se basant sur des cadres préexistants. L'anticipation est cruciale, car elle permet de prendre en compte les différentes manifestations potentielles de la crise et de définir les modes d'organisation appropriés.

Il est essentiel que chaque membre de la cellule de crise comprenne parfaitement son rôle et ses responsabilités, ainsi que la manière dont il doit communiquer avec les autres membres de l'équipe. Une coordination efficace est la clé pour gérer avec succès une crise cyber, minimiser les dommages potentiels et rétablir rapidement la sécurité et la stabilité du système.

4.2 ANTICIPER LES CONSÉQUENCES DE LA CRISE EN TERMES DE COMMUNICATION ET DE GESTION DES ÉQUIPES

La communication joue un rôle essentiel lors de la gestion d'une crise cyber. La coopération de toutes les parties prenantes est cruciale pour bien réagir, et la communication doit être constante, quelles que soient les circonstances. L'une des leçons les plus importantes à retenir est que les partenaires et les parties prenantes ne blâmeront pas l'entreprise pour avoir été victime d'une cyberattaque, mais ils la critiqueront sévèrement si elle ne communique pas de manière adéquate.

Même si l'organisation reconnaît qu'elle aurait pu mieux protéger son système d'information, il est généralement conseillé de ne pas dissimuler d'informations. Au contraire, il faut s'efforcer de fournir

à tous les points de contact les informations nécessaires pour faire face à la crise. Cela inclut les collaborateurs, les métiers, toutes les filiales, et surtout les instances de décision stratégique comme le COMEX (Comité Exécutif), qui doivent disposer de tableaux de bord pour suivre la gestion de la crise.

La communication de crise est complexe, car elle doit s'adapter aux besoins de différentes parties prenantes, notamment :

1. Au sein de l'entreprise : il est essentiel de communiquer avec les collaborateurs, les différentes équipes métiers et les filiales. Le COMEX doit être informé en temps réel de l'avancée de la gestion de crise grâce à des tableaux de bord dédiés.
2. Vers l'écosystème (clients, fournisseurs, partenaires) : les partenaires commerciaux attendent des garanties concernant les données exfiltrées. Il est donc impératif de leur fournir un maximum d'informations sur la situation en cours.
3. Vers les médias : les médias ont des approches variées, certains étant très factuels tandis que d'autres peuvent adopter une orientation sensationnaliste. La communication avec les médias doit être soigneusement gérée pour minimiser les risques de mauvaise interprétation ou de divulgation non autorisée d'informations sensibles.

Lorsqu'une crise cyber s'installe sur le long terme, les équipes de la DSI sont mobilisées sur des plages horaires étendues et parfois indéfinies. **Il est essentiel de prendre des mesures pour ménager les collaborateurs**, notamment en ouvrant des locaux à des horaires inhabituels et en organisant la restauration et au besoin les transports. Cette dimension logistique est souvent négligée mais revêt une importance capitale pour maintenir l'efficacité des équipes.

Outre les équipes de la DSI, les équipes métiers sont également impactées, soit en raison du chômage technique, soit parce que leur charge de travail est considérablement alourdie. Informer ces équipes de l'évolution de la gestion de crise est nécessaire pour éviter les tensions internes et les impliquer dans l'effort collectif. La collaboration avec la Direction des Ressources Humaines est essentielle pour gérer au mieux les équipes.

En termes d'actions opérationnelles, il est recommandé de ne pas faire en sorte que les équipes opérationnelles gèrent directement les communications avec les cellules de crise, car cela peut perturber leur concentration sur leurs tâches. Multiplier les signes de reconnaissance, favoriser la communication interne, privilégier le travail avec les équipes internes plutôt qu'avec des consultants externes, et segmenter les équipes en fonction de leurs objectifs sont autant de mesures qui peuvent contribuer à la gestion efficace des équipes en période de crise.

Il est également essentiel de mobiliser le médecin du travail pour s'assurer du bien-être des collaborateurs. Pour résumer, la communication, la gestion des équipes et le souci du bien-être des collaborateurs sont des facteurs cruciaux pour réussir la gestion d'une crise cyber de manière efficace et collaborative.

4.3 PRINCIPALES MESURES POUR LIMITER UNE PROPAGATION RAPIDE DE L'ATTAQUE

Lorsqu'une entreprise est victime d'une cyberattaque, il est essentiel de prendre des mesures opérationnelles rapides pour diagnostiquer l'incident de sécurité informatique et limiter sa propagation. Le but est d'identifier les premières conséquences de l'incident afin de pouvoir y répondre de manière efficace. Voici quelques-unes des actions que la Direction des Systèmes d'Information (DSI) peut entreprendre pour diagnostiquer un incident informatique et son « client zéro » ou l'origine d'une intrusion ce qui permettra d'optimiser les investigations :

1. **Consulter l'EDR (*Endpoint Detection and Response*)** : l'EDR est un outil de détection avancée des menaces installé en complément de l'antivirus. Il détecte les menaces en temps réel et agit immédiatement pour les neutraliser.
2. **Constater et identifier l'incident avec l'aide des collaborateurs** : les membres de l'équipe informatique peuvent travailler ensemble pour identifier la nature de l'incident et ses conséquences.
3. **Analyser les fichiers logs dans le SIEM (*Security Information and Event Management*)** : le SIEM est un outil qui gère les événements de sécurité du système d'information. Il permet d'analyser les journaux d'événements pour détecter des anomalies.
4. **Consulter le nombre de tickets d'incidents/alertes du SOC (*Security Operations Center*)** : L'équipe SOC est chargée de surveiller la sécurité du SI et remonte des alertes en cas de menaces. Le nombre de tickets d'incidents peut donner des indications sur l'ampleur de l'incident.
5. **Contacter l'équipe d'exploitation IT** : l'équipe d'exploitation IT peut aider à réaliser un diagnostic des serveurs et des systèmes informatiques.
6. **Analyser le volume et les destinataires du trafic Internet** : examiner le trafic Internet peut fournir des informations sur les activités suspectes.

Ce premier diagnostic repose principalement sur l'utilisation d'outils de supervision et sur la collaboration des membres de l'équipe informatique. L'objectif initial est de qualifier le périmètre de l'incident. La nature et l'étendue de l'incident détecté déterminent les premières mesures à prendre sur le SI. À ce stade, l'objectif principal est d'arrêter la propagation de l'incident et de le contenir dans son périmètre initial. Voici les principales actions à entreprendre :

1. **Isoler les systèmes impactés** : les serveurs, serveurs de fichiers, postes de travail vulnérables doivent être isolés pour empêcher la propagation de l'attaque. Cette isolation peut être réalisée depuis la console de l'EDR, ce qui est généralement le moyen le plus pertinent.
2. **Faire intervenir une équipe de réponse aux incidents de sécurit**é : une équipe dédiée aux réponses aux incidents doit être mobilisée pour gérer la situation de manière professionnelle.
3. **Désactiver la plupart des comptes administrateurs** : les comptes administrateurs doivent être désactivés, car les cyberattaquants cherchent souvent à obtenir un accès administrateur pour contrôler l'ensemble des systèmes.
4. **Identifier et sécuriser la dernière sauvegarde saine** : il est essentiel de trouver la dernière sauvegarde saine des données et de la sécuriser pour éviter toute altération.

Si le périmètre de la cyberattaque est trop étendu ou mal défini, il peut être nécessaire de prendre des mesures plus drastiques, comme l'arrêt complet ou le confinement des systèmes, pour permettre des investigations plus approfondies et éviter une propagation incontrôlée de l'incident.

5 CONCLUSION

Face à une menace cyber en constante évolution, les organisations doivent non seulement adopter des mesures de sécurité proactives, mais aussi développer des capacités de réponse rapides pour réagir efficacement aux incidents. La surveillance continue du système d'information (SI) s'impose comme un premier rempart essentiel pour détecter les menaces à un stade précoce. Cependant, la véritable résilience réside dans la capacité à anticiper, à se préparer et à réagir adéquatement en cas d'incident majeur. Les équipes de sécurité, notamment les *Security Operations Centers* (SOC), jouent un rôle central dans cette surveillance en utilisant des processus d'analyse de la menace avancés tels que la *Cyber Threat Intelligence* (CTI). En investissant dans la CTI, les organisations peuvent anticiper les menaces émergentes, identifier les vulnérabilités et se préparer de manière proactive. Cela leur permet d'adopter une posture de défense plus robuste, en identifiant les indicateurs de compromission (IoC) et les tactiques, techniques et procédures (TTP) des cybercriminels.

Aujourd'hui la cybersécurité ne peut plus être traitée comme un enjeu mineur. Les organisations doivent adopter une approche proactive, et surtout, inscrire la cybersécurité au cœur de leur culture d'entreprise. En suivant les bonnes pratiques énoncées dans ce rapport, elles seront mieux armées pour anticiper, détecter les cyberattaques et y répondre, contribuant ainsi à assurer un avenir plus sûr et plus résilient pour leurs activités. La vigilance et la préparation sont les clés pour faire face à la menace de manière efficace et efficiente.

À PROPOS DU CIGREF

Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

Appartenance
Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

Intelligence
Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

Influence
Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

NOUS CONTACTER

www.Cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
Cigref@Cigref.fr


Cigref
RÉUSSIR
LE NUMÉRIQUE