

WAVESTONE



# Livre blanc

## Supply Chain x Cybersécurité

Février 2022

Dans un contexte où l'on assiste à de fortes variations de l'offre et de la demande, la **Supply Chain** doit se transformer pour devenir **agile** et **résiliente**. Elle devient alors de plus en plus **intégrée** et **digitale** pour réaliser ses activités. Un risque accru : le **risque digital** qui peut avoir des conséquences désastreuses pour la Supply Chain comme l'arrêt total des livraisons de produits sur une zone géographique ou l'arrêt d'une usine. La **Cybersécurité** devient donc un **enjeu majeur pour la Supply Chain** et pas uniquement pour les Responsables de la Sécurité des Systèmes d'Informations (RSSI).

Ce livre blanc a pour objectif de présenter ce **risque cyber** sur les activités de la **Supply Chain** avec la digitalisation des opérations et l'Industrie 4.0.

Ce risque est déjà présent et concerne **toutes les entreprises**, des multinationales aux PME et Startups et **tous les secteurs d'activités**.

Les **responsables industriels et Supply Chain** jouent un rôle clef dans la prévention de ce risque au même titre que les **RSSI**. Ce livre blanc expose les conséquences concrètes de ce risque et propose des pistes pour s'en prémunir.



La question n'est plus de savoir **si** votre Supply Chain va se faire attaquer mais **quand** va-t-elle se faire attaquer ?





# 01

## Vers une Supply Chain 100% numérique vulnérable au risque cyber

# Une Supply Chain de plus en plus intégrée et connectée

AVEC LA GLOBALISATION DE L'ÉCONOMIE, LA SUPPLY CHAIN EST DEVENUE DE PLUS EN PLUS COMPLEXE À PILOTER. CETTE COMPLEXITÉ S'EXPLIQUE PAR L'ÉVOLUTION DES ATTENTES DES CLIENTS.



## L'ÉVOLUTION DES ATTENTES CLIENTS ...

Les clients B to C et B to B sont de plus en plus exigeants avec des attentes **très spécifiques sur les produits et le service** qui les accompagne.

La **diversité des produits augmente** avec **de plus en plus de références à gérer** au niveau des chaînes d'approvisionnement.

L'offre de service se construit avec des **modes et points de livraison multiples** ainsi que des **délais de la commande à la livraison de plus en plus courts**.

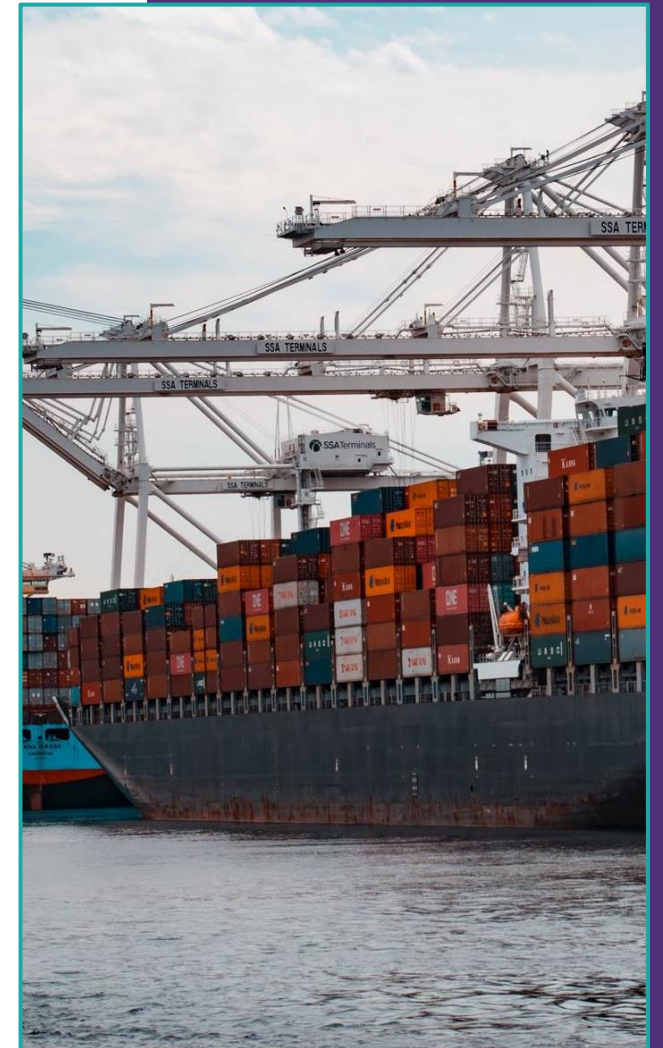


## ... TRANSFORME LA SUPPLY CHAIN ET SON PILOTAGE

La **Supply Chain est internationalisée** pour **optimiser le coût complet produit** et **servir au mieux les clients** avec des **zones de sourcing et de production souvent éloignées** des clients.

De plus en plus de Supply Chains sont construites sur la base d'un **nombre important de rangs de fournisseurs** (rang 1, 2, 3 ...) et ont **recours à des prestataires de service** pour le transport, le stockage, la douane, voire les Systèmes d'Informations.

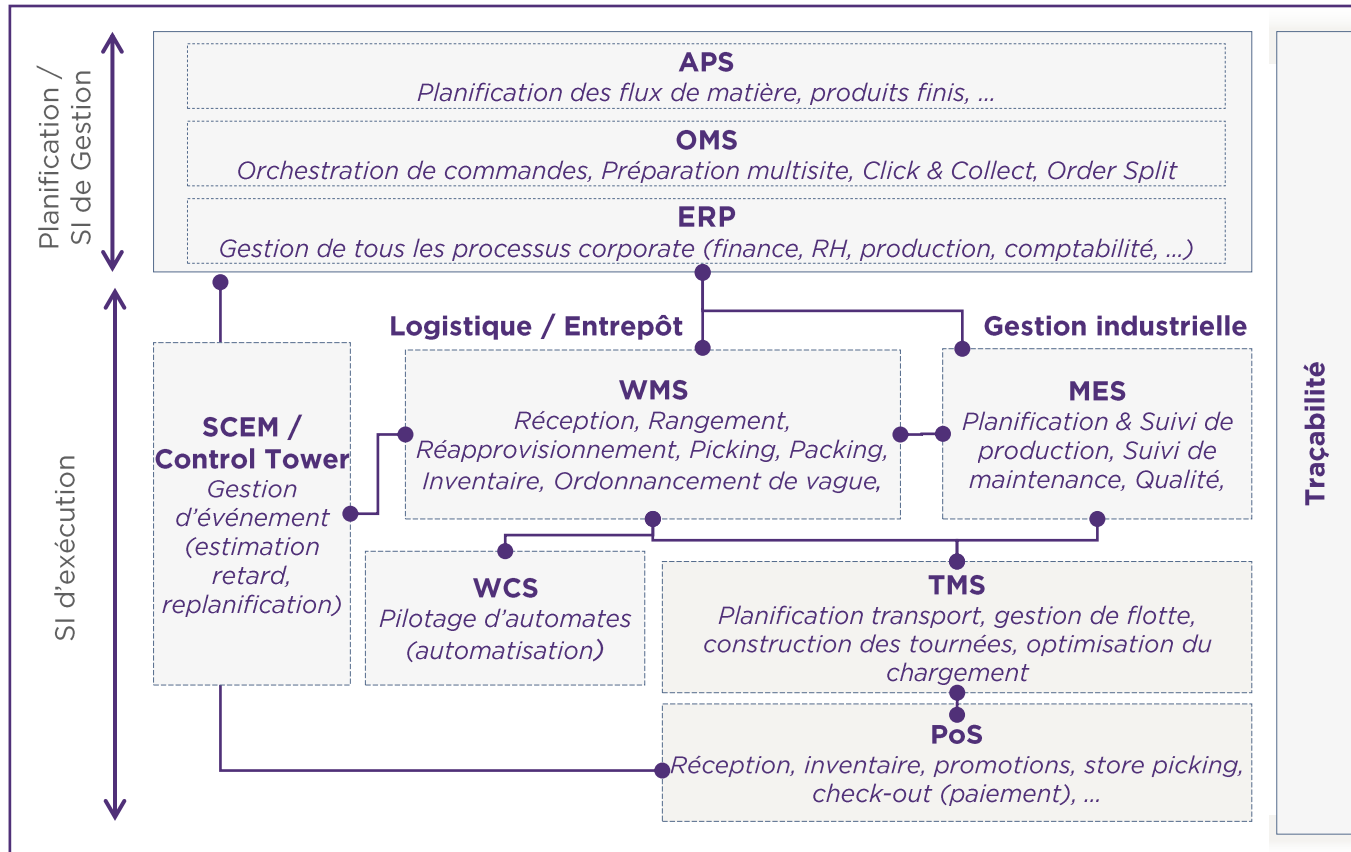
La structuration de la chaîne d'approvisionnement devient de plus en plus complexe et nécessite un **pilotage en temps réel** afin de pouvoir réagir à la moindre alerte.



# La Supply Chain intégrée et connectée nécessite un Système d'Information complexe

LE SYSTÈME D'INFORMATION SUPPLY CHAIN DES SOCIÉTÉS S'APPUIE SUR DE NOMBREUSES SOLUTIONS TECHNOLOGIQUES QUI SONT INTERFACÉES ENTRE ELLES ET VERS LES SOLUTIONS DES CLIENTS, FOURNISSEURS ET PRESTATAIRES DE SERVICE.

## Un exemple de Système d'Information Supply Chain pour illustrer sa complexité




- **APS** : Advanced Planning System (gestion des prévisions et planification)
- **OMS** : Order Management System (gestion des commandes de bout en bout)
- **WMS** : Warehouse Management System (gestion des stocks en entrepôt ou en usine)
- **MES** : Manufacturing Execution System (gestion de la production en usine)
- **TMS** : Transport Management System (gestion du transport)
- **WCS** : Warehouse Control System (pilotage des systèmes automatisés)
- **SCEM** : Supply Chain Event Manager (gestion temps réel des événements)
- **PoS** : Point of Sales (pilotage du point de vente : boutique physique, internet ...)

# La complexité du système d'information augmente sa vulnérabilité face à des attaques cybers

LA VULNÉRABILITÉ DU SYSTÈME D'INFORMATION PROVIENT DU NOMBRE DE PORTES D'ENTRÉE ET DE LA CAPACITÉ DES DSI SUPPLY CHAIN À IDENTIFIER L'EMPLACEMENT DE CES PORTES D'ENTRÉE.

## Illustration de la vulnérabilité du Système d'information



Certaines briques technologiques ont été conçues à des époques où le risque cyber n'existait pas. Il fallait par exemple être présent physiquement pour avoir accès au système là où il est maintenant possible d'y avoir accès en ligne n'importe où dans le monde.



L'essor des accès distants avec par exemple le télétravail, la télémaintenance et le pilotage à distance de la Supply Chain sont autant de nouvelles pratiques que des portes d'entrée pour accéder au système d'information.



Le développement de plateformes cloud avec du SaaS (Software as a Service), des serveurs globalisés ou sous-traités, de la gestion déléguée des infrastructures IT pour réduire les coûts peuvent faire perdre en contrôle sur la sécurité.

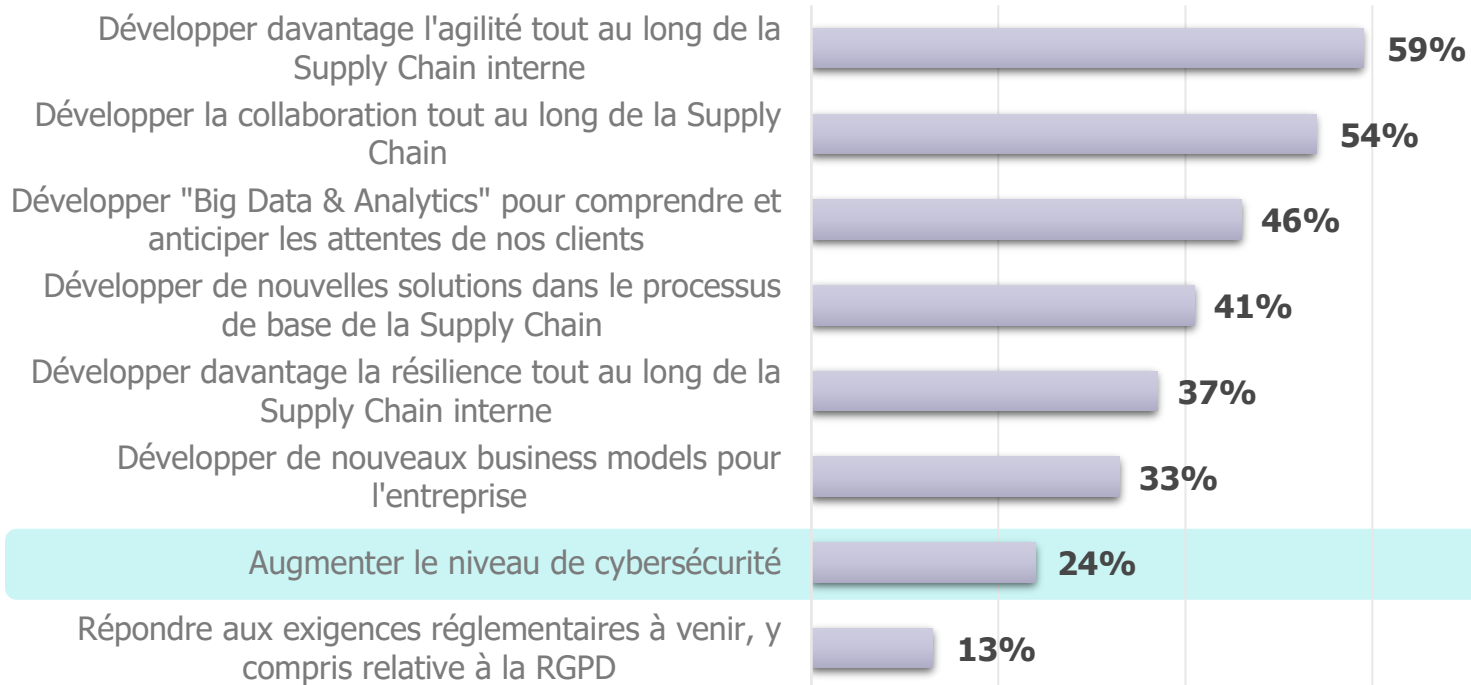


Des équipes Supply Chain à sensibiliser au risque cyber à la fois lors du choix de progiciels et des équipements métiers et à former aux bonnes pratiques d'utilisation des Systèmes d'Information.

Le fonctionnement de la Supply Chain est de plus en plus numérisé, tout problème de sécurité peut avoir des conséquences immédiates sur la Supply Chain. Il existe de moins en moins de modes dégradés possibles, ce sont alors les activités physiques qui sont contraintes d'être arrêtées.

# En dépit des risques liés à la vulnérabilité du Système d'Information, les enjeux de cybersécurité sont sous-estimés par les directions Supply Chain.

PRIORITÉ D'INVESTISSEMENT EN SUPPLY CHAIN PAR LES ENTREPRISES



En 2020, 24% des entreprises interrogées par France Supply Chain voient la cybersécurité comme un chantier prioritaire. Sur les 8 chantiers perçus comme prioritaires, la cybersécurité arrive en avant-dernière position.

Les entreprises priorisent d'abord la performance de la Supply Chain avec une recherche d'agilité et de collaboration de bout en bout (priorités 1 et 2).

Ensuite, elles priorisent l'utilisation de l'Intelligence Artificielle pour améliorer leur réponse aux demandes des clients en comprenant mieux voire en anticipant leurs attentes (priorité 3).



# Caractérisation de la menace cyber pour la Supply Chain

NOTICE TO ALL PERSONS  
RECEIVING THIS DRAWING:  
This drawing is only conditionally  
issued, and neither conveys nor  
conveys any right in, or license  
under any patent, copyright or other  
intellectual property rights in the  
drawing or any design or technical  
information shown therein. We  
have no right to reproduce this drawing  
in any form without our written  
consent. This is the property of  
Apple Computer, Inc. No right to  
copy or reuse this drawing, or any  
information hereon, without our  
written consent. This is the property of  
Apple Computer, Inc.



# Des attaques toujours plus nombreuses et opportunistes

“

En l'espace d'un an, on a une multiplication par 3 ou 4 à périmètre constant [du nombre de cyberattaques].  
Je ne vois pas de raisons pour que ça s'infléchisse à court terme.

”

Audition au Sénat le 4 novembre 2020



Guillaume Poupard  
Directeur général de l'ANSSI

“

75% des attaques sont opportunistes et sont liées à des méthodes de blocage avant demande de rançon.

”

Benchmark CERT Wavestone, Octobre 2021

Toutes les entreprises sont concernées : de la multinationale du CAC40 à l'ETI ou la startup !

# 3 motivations principales pour attaquer la Supply Chain

## GAINS FINANCIERS

- / RANÇONS
- / VOL DE DONNÉES PERSONNELLES ET FINANCIÈRES
- / VOL DE SECRETS INDUSTRIELS OU DONNÉES STRATÉGIQUES
- / TRANSACTIONS FRAUDULEUSES

## IDEOLOGIE

- / DÉNI DE SERVICE
- / MESSAGES IDÉOLOGIQUES
- / DIVULGATION D'INFORMATIONS
- / USURPATION D'IDENTITÉ

## DESTABILISATION

- / DESTRUCTION LOGIQUE ET/OU PHYSIQUE
- / VOL DE DONNÉES STRATÉGIQUES
- / DIVULGATION DE DONNÉES

Outre l'attaque directe, l'attaque par rebond fait figure de menace indirecte pour l'écosystème des sous-traitants et des fournisseurs connectés aux systèmes d'information des victimes.

Elle consiste à utiliser un ou plusieurs systèmes intermédiaires à leur insu pour atteindre leur cible : compromission de sites / logiciels de confiance, espionnage du réseau et contournement des mesures de sécurité.

# Une menace globale

IL EST DIFFICILE DE RETROUVER LES ATTAQUANTS, MAIS IL EXISTE UNE RÉCURRENCE DES PROFILS



## **MENACE INTERNE**

*Employés malveillants ou négligents*



## **HACKTIVISTES**

*Capables de lancer des attaques d'envergure aux quatre coins du globe*



## **GROUPES MAFIEUX**

*Capables d'attaques de grande envergure si le potentiel profit est conséquent*



## **ETATS (Renseignements)**

*Des attaques ciblées sur des acteurs spécifiques*



## **ETATS BELLIQUEUX**

*Destruction d'infrastructures essentielles pour déstabiliser un pays*



**Mais aussi...**

**CONCURRENTS**

**VENGEURS**

**TERRORISTES**

**AMATEURS**

# Les attaques Cybers font peser 3 types de risques sur la Supply Chain, en voici quelques exemples :

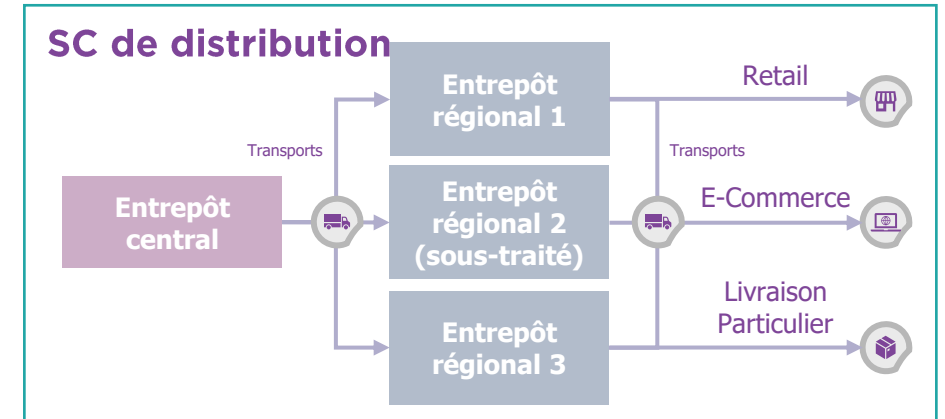
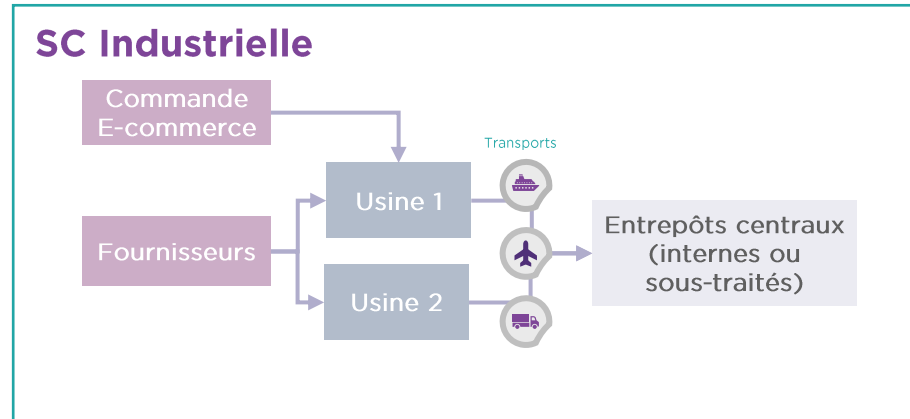
 <p><b>INACCESSIBILITÉ DES SYSTÈMES ET DES DONNÉES</b></p>	 <p><b>CORRUPTION DES DONNÉES OU DES PRODUITS</b></p>	 <p><b>VOL DES DONNÉES</b></p>
<p>L'ERP n'est plus accessible et <b>immobilise l'entreprise</b></p> <p>Un ransomware empêche le pilotage du Système d'Information industriel et <b>met les lignes de production à l'arrêt</b></p>	<p>Les données des prévisions sont fausses et <b>impactent les volumes de production</b></p> <p>De fausses commandes clients sont créées et <b>peuvent aboutir à du rebus sur une supply chain connectée</b></p>	<p>Des données sensibles sont volées par un concurrent à des fins <b>d'espionnage industriel</b></p> <p>Des <b>données clients</b> sont volées (informations personnelles, comptes, ...)</p>

Sur 40 sites industriels audités en 2021, **12% ont subi un arrêt de production suite à une attaque cyber\***

\* Source : Benchmark SI Industriel Wavestone, Avril 2021

# Illustration des risques cyber sur la Supply Chain

EXEMPLE DE RISQUES SUR LES 3 GRANDES PARTIES DE LA SUPPLY CHAIN - NON EXHAUSTIF



La **perte des outils** de planification entraîne un défaut de pilotage de la production et/ou de la livraison

L'**altération des données** entraîne la possibilité d'avoir des commandes / des productions différentes des quantités souhaitées

La **perte de confidentialité** sur les données de planification (volume, définition produit, lancement...) peut donner un avantage aux concurrents

Un **automate compromis** peut aboutir à un problème de sûreté (ex : un bras manipulant des palettes heurte un opérateur)

Un **pirate s'infiltrant dans le système de gestion** a la possibilité de créer de fausses commandes

La **compromission de systèmes** sur des sites « **Seveso** » peut entraîner un risque environnemental, de sûreté...

La perte des **outils de traçabilité** peut aboutir à un blocage du stock ou de la production pour des contraintes réglementaires

La **compromission d'un fournisseur** ou d'un **partenaire** peut également avoir un impact sur la gestion des stocks et des flux

La **perte du Système d'Information** entraîne l'arrêt des chaînes de production ou des entrepôts de plus en plus robotisés

La **corruption des données** de transport entraîne la perte des produits ou des écarts de stock entre deux entrepôts

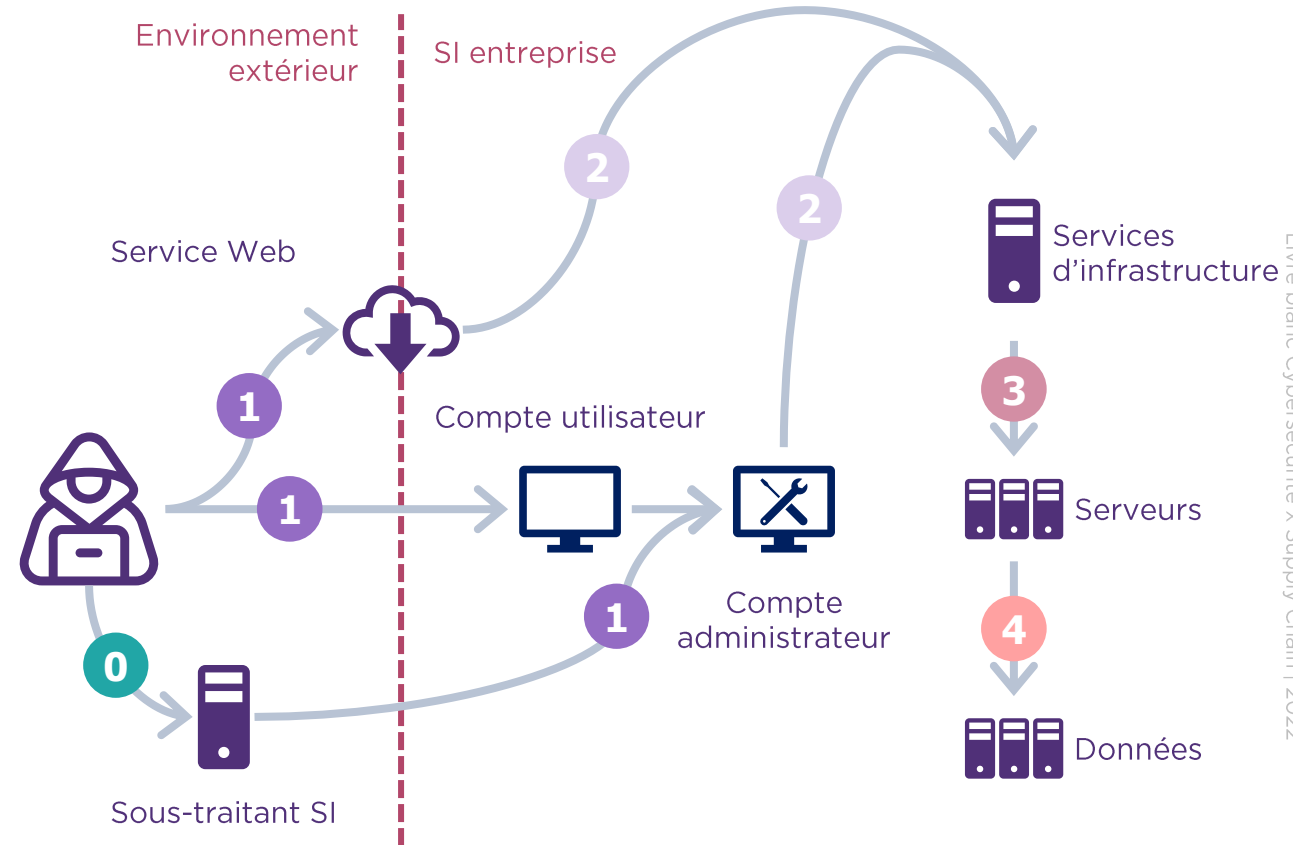
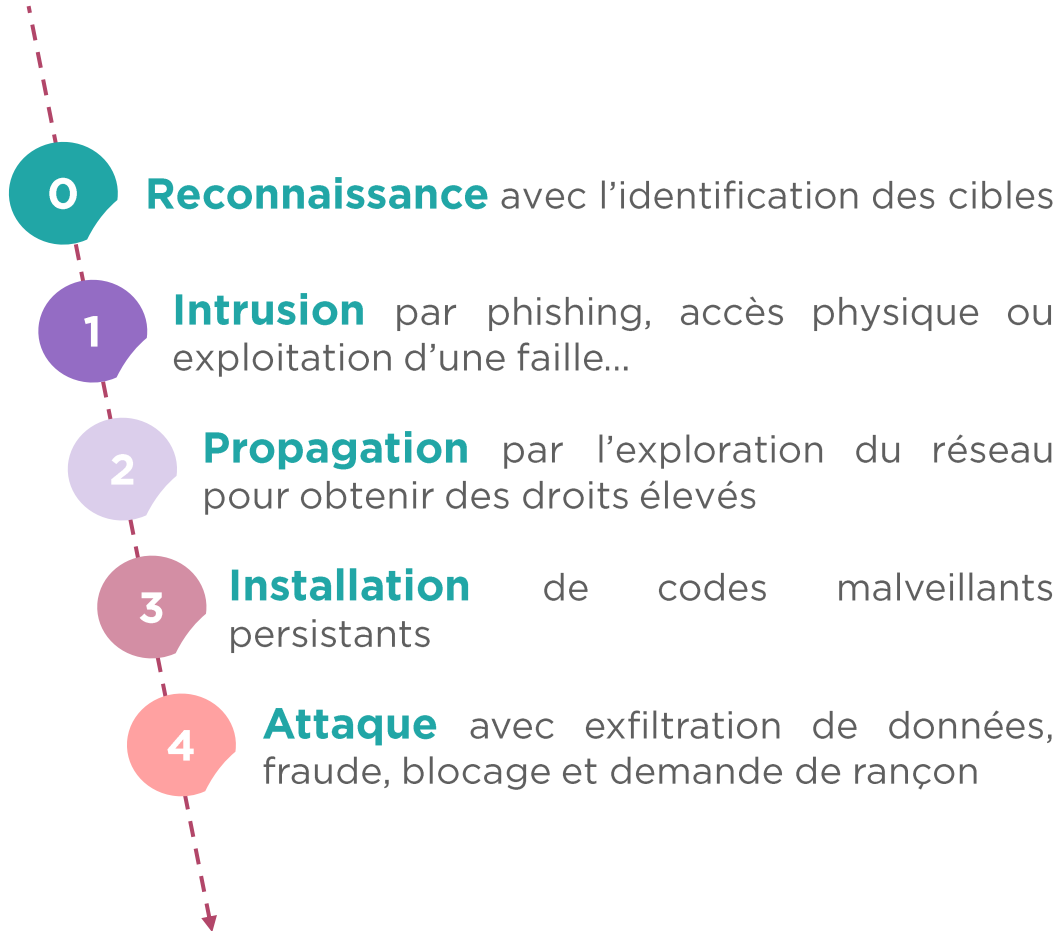
Un **pirate s'infiltrant dans le système de gestion** peut récupérer des données à caractère personnel

La **compromission du système de gestion de commande** peut aboutir à la création de fausses commandes et donc à la perte de marchandise

Le **perte de confidentialité** concernant le contenu et l'itinéraire des colis et des camions peut entraîner des problèmes de sûreté et de vol

# Les cyber-attaques suivent pratiquement toutes le même schéma...

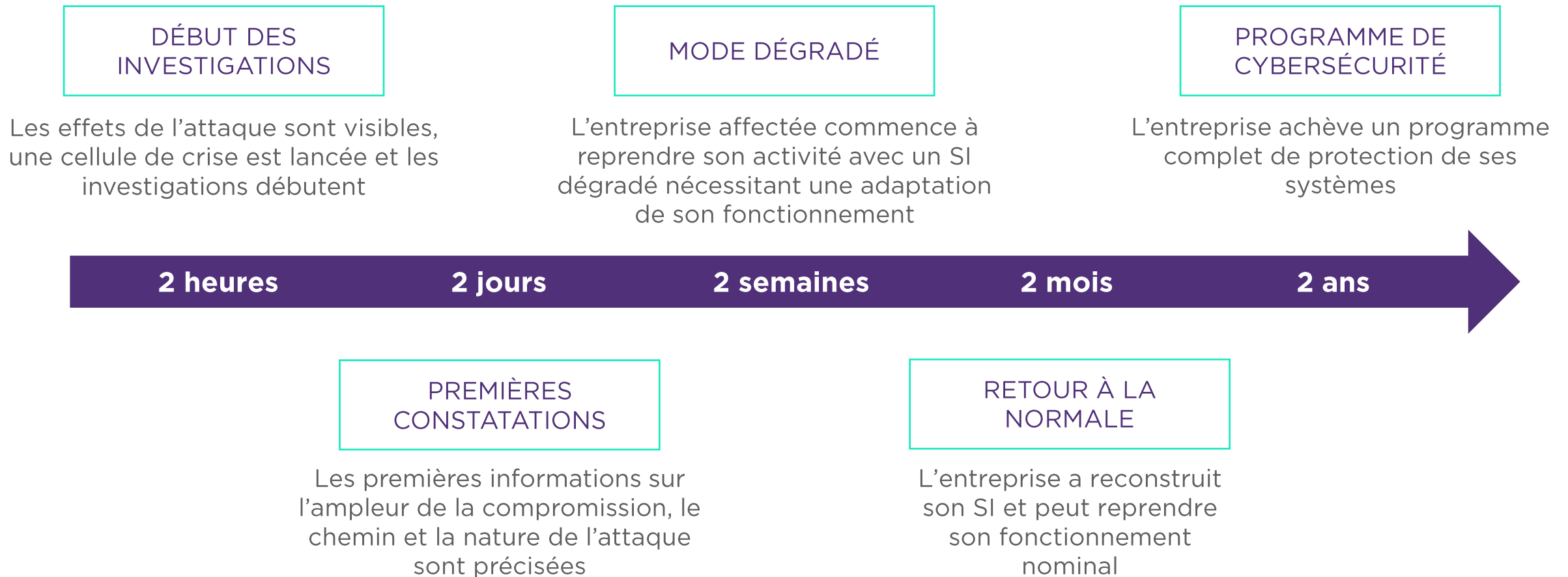
LES ATTAQUANTS VONT AVANCER PAR ÉTAPES POUR ATTEINDRE LEUR BUT



Il se passe en moyenne 52 jours\* entre l'intrusion et la détection de l'attaque.

# ... et ont des conséquences majeures perturbant durablement les opérations de votre Supply Chain

POUR ESTIMER LES DURÉES DES DIFFÉRENTES ÉTAPES D'UNE CRISE CYBER DE TYPE RANSOMWARE, LA RÈGLE DES CINQ '2' DONNE UN APERÇU DES ÉCHELLES DE TEMPS AFFECTANT LA DISPONIBILITÉ DES SYSTÈMES :



# 3 tendances qui vont perdurer en 2022...

## L'HYDRE DU RANSOMWARE

UN RANSOMWARE OU RANÇONGICIEL EST UN LOGICIEL MALVEILLANT CHIFFRANT LES DONNÉES DES VICTIMES. UNE RANÇON EST ALORS DEMANDÉE AUX CIBLES POUR RÉCUPÉRER LES DONNÉES RENDUES ILLISIBLES.

TYPES : RANSOMWARES NON-CIBLÉS VISANT DES PARTICULIERS OU ENTREPRISES; RANSOMWARES CIBLÉS CONTRE LES GRANDES ENTREPRISES, RANSOMWARES CIBLÉS AVEC FUITE DE DONNÉES.

L'entreprise américaine Colonial Pipeline a payé, en 2021, une rançon de \$4,4M à la suite d'une attaque par ransomware qui a paralysé 45% de l'approvisionnement en pétrole de la côte Est américaine

## L'ATTAQUE DES TIERS

DES ENTREPRISES ONT BESOIN DE FAIRE CONFIANCE ET DE DONNER À LEURS FOURNISSEURS, PRESTATAIRE ETC. UN ACCÈS PRIVILÉGIÉ À LEUR SI.

POSSIBILITÉ DE PIRATER UNE ENTREPRISE PAR PROPAGATION : SI DES PIRATES COMPROMETTENT UN FOURNISSEUR DE CONFIANCE, ILS PEUVENT ATTEINDRE LE SYSTÈME D'INFORMATION CIBLÉ EN UTILISANT LES PRIVILÈGES ACCORDÉS AU FOURNISSEUR POUR CONTOURNER LES MESURES DE SÉCURITÉ.

De multiples entreprises ont été attaquées via la compromission des éditeurs de logiciel SolarWinds en 2020 et Kaseya en 2021

## LES ATTAQUES CIBLÉES SUR LE CLOUD

DE PLUS EN PLUS DE SERVICES SONT BASÉS SUR UNE ARCHITECTURE CLOUD, CE QUI PEUT APPORTER DES FAILLES DE SÉCURITÉ

LE CLOUD DEVIENT DONC UN VECTEUR D'ATTAQUE RÉPANDU, ET CE À PARTIR DE DIFFÉRENTS MOYENS : TROUVER DES FAILLES DE CONFIGURATION, UTILISER L'INGÉNIEURIE SOCIALE, EXPLOITER LES MOTS DE PASSE TROP COURTS OU RÉUTILISÉS DANS LE CLOUD.

Une attaque sur les plateformes Cloud de la banque Capital One entre mars et juillet 2019 a abouti à la divulgation des données à caractère personnel de plus de 100 millions de personnes





# Rôle du responsable Supply Chain dans la mise en place de protections cyber

# En tant que responsable Supply Chain, comment se préparer ?

LA SUPPLY CHAIN DOIT ÊTRE INSCRITE DANS UNE DÉMARCHE CYCLIQUE DE REVUE DE LA CYBERSÉCURITÉ

## QUELQUES CHIFFRES :

- ✓ L'intégration de la sécurité dans les projets nécessite de 5 à 10% du budget total
- ✓ Le maintien en conditions de sécurité des systèmes requiert une augmentation du coût des opérations de 3 à 5%

## IDENTIFIER LA MENACE ET LES IMPACTS

- / Définir les catégories d'attaquants et leurs motivations
- / Évaluer les impacts d'une attaque cyber sur vos processus clés
- / Identifier les systèmes associés

## CONNAÎTRE LES ACTEURS

- / Formaliser les liens avec la DSI
- / Évaluer l'impact des partenaires, clients et fournisseurs
- / Auditer leur niveau de sécurité

## DÉTECTER ET RÉAGIR

- / Mettre en place les moyens de détection des incidents
- / Sensibiliser les équipes
- / Préparer la gestion de crise et vérifier la résilience des systèmes

## INTERAGIR AVEC LA DSI

- ✓ Faciliter l'intégration des mesures de sécurité
- ✓ Adapter les solutions (authentification, transfert de fichiers sécurisés, interfaces partenaires ...) aux besoins métier
- ✓ Intégrer la cybersécurité dès la conception

# Concrètement, quelles sont les actions à mener ?

CES ACTIONS VISENT À ASSURER UN NIVEAU DE SÉCURITÉ MINIMUM DE LA SUPPLY CHAIN, ELLES DOIVENT ÊTRE CONDUITES PAR LE RESPONSABLE SUPPLY CHAIN, CONJOINTEMENT AVEC LA DIRECTION DES SYSTÈMES D'INFORMATION

## CHECKLIST DES ACTIONS À MENER POUR IDENTIFIER ET RÉDUIRE LE RISQUE CYBER



### IDENTIFIER LA MENACE ET LES IMPACTS SUR LA SUPPLY CHAIN

- ❑ Définir les **risques** d'attaques cyber en fonction des **acteurs**, de leur **objectif** et des **moyens mis en œuvre**
- ❑ Evaluer les impacts qu'une attaque pourrait avoir sur la Supply Chain
- ❑ Identifier à partir d'une **cartographie des SI Supply Chain les vulnérabilités** présentes
- ❑ Définir un **plan d'action** pour **palier ces vulnérabilités** dans un **équilibre risques / coûts**



### CONNAÎTRE LES ACTEURS TIERS POUR MAÎTRISER LES RISQUES

- ❑ Réaliser l'**inventaire des tiers** (clients, prestataires, sous-traitants) afin d'identifier **le risque lié à leur compromission**
- ❑ Décrire à ces tiers les **attendus en termes de cybersécurité** pour permettre l'accès à votre SI
- ❑ Conduire des audits ciblés pour **évaluer la maturité des tiers** dont votre Supply Chain est **la plus dépendante**



### DÉTECTER ET RÉAGIR

- ❑ **Mettre en œuvre des systèmes de détection d'incidents 24h/24 et 7j/7** grâce à un Security Operation Center (SOC)
- ❑ Définir et adapter les processus de **gestion de crise** et de **cyber-résilience** sur chacun des sites
- ❑ **Garantir la continuité d'activité** via la mise en œuvre de processus **résilients** (sauvegarde, process papier, redondance)
- ❑ Entraîner les équipes en participant à des **exercices de crise** pour qu'elles **s'approprient ces processus**



- ❑ Identifier / nommer le **correspondant Cybersécurité** pour **la Supply Chain** pour **coordonner les actions** sur le périmètre



# Cyber x Supply Chain : retours terrain



# Client Story 1 : Leader de l'industrie cosmétique

## APPROCHE CYBERSÉCURITÉ EN 5 POINTS CLÉS

La Supply Chain cosmétique du Groupe est une **Supply Chain centralisée**, qui regroupe la **planification, l'industrie** (Production, Achats, Qualité, Développement produits, Maintenance) et la **logistique/distribution**.

Les **challenges actuels de la Supply Chain** sont :

- Gagner en agilité et en élasticité (répondre rapidement aux changements de la demande clients, anticiper et gérer d'éventuelles ruptures d'approvisionnement, ...),
- Optimiser les coûts,
- Contribuer à la politique RSE du Groupe,
- Répondre aux exigences réglementaires (packaging, transport, qualité, douane, ...),
- Accroître la digitalisation des process et les synergies inter marques.

Le Système d'information Supply Chain du Groupe est construit autour d'un **ERP** (Enterprise Resource Planning) en association avec des systèmes externes et intégrés tels que des **WMS** (Warehouse Management System) et **MES** (Manufacturing Execution System). Il existe également d'autres applications spécialisées permettant de compléter la couverture fonctionnelle des process de la Supply Chain.

**D'un point de vue Système d'Information, les défis à relever** sont d'adresser les challenges actuels de la Supply Chain et son évolution vers une industrie 4.0.

Le maintien en conditions opérationnelles et de sécurité des outils Supply Chain doit rester une ambition non négociable.

Dans ce cadre, pour la sécurisation de son système d'information **Supply Chain**, le Groupe a mis en place une **stratégie basée sur 5 piliers** :

### 1/ La cartographie des risques

Evaluer la maturité de la sécurité des SI des sites industriels au travers d'une grille de lecture standard et uniforme

### 2/ L'inventaire des assets

A l'aide de sondes, déterminer précisément les matériels, flux et interconnexions présents sur le SI

### 3/ L'architecture et le cadre technique cible

Elaborer une architecture et un cadre technique permettant de dégager le modèle idéal de sécurité du SI Industriel

### 4/ la remédiation

Mettre en place un plan d'action sur les process métier existants et dans le cadre des nouveaux projets

### 5/ la gouvernance

Formaliser une gouvernance pour les process IT/OT dans le cadre du Build et du Run en maintenant les règles de sécurité Architecture/Cadre technique dans le temps

“

Depuis plus de 15 ans maintenant, la cybersécurité a émergé vers une prise de conscience générale. Elle met en exergue l'impérieuse nécessité pour une entreprise de protéger ces systèmes vitaux. Notre système industriel est tout autant concerné, et probablement même davantage que nos autres environnements par les enjeux de la cybersécurité. Notre défi de demain est de continuer à accompagner nos métiers industriels dans leur transition numérique, tout en assurant une productivité efficace et garante d'une protection cyber.

Group Chief Information Security Officer

”

## ETAT DE LA CYBERSÉCURITÉ

### Maturité :

Le groupe a conscience de l'importance de la cybersécurité et des **risques associés pour sa Supply Chain**.

L'ambition donnée est que tous les projets industriels soient « Security by design »

### Interaction Equipes Informatique et Supply Chain :

La **sensibilisation** et la prévention des risques cyber sont effectuées auprès des métiers Supply Chain grâce à des cartographies des risques, des campagnes de faux phishing, des webinaires...

Une très forte interaction entre les équipes métier et informatique (incl. cybersécurité) est mise en place dès l'étape initiale des projets SI Supply Chain.

## 4 FACTEURS DE SUCCÈS POUR APPLIQUER LA CYBERSÉCURITÉ À LA SUPPLY CHAIN

- ✓ Connaître les **risques** et les **assets Supply Chain**
- ✓ **Sensibiliser la direction** aux impacts et obtenir du **sponsoring**
- ✓ **Créer une forte dynamique** entre les équipes industrielles et informatiques afin de réaliser une remédiation efficace
- ✓ Faire de la cybersécurité **un critère de valeur** des projets Supply Chain

# Client Story 2 : Acteur du retail alimentaire

## RETOUR SUR L'ÉTAT DE LA CYBERSÉCURITÉ ET DE SON IMPACT CHEZ UN GRAND ACTEUR DU RETAIL ALIMENTAIRE

Suite à un **incident cybersécurité** chez un grand acteur du Retail, des entrepôts ont perdu l'accès à leur données essentielles. Cela a abouti à un **delta d'une semaine dans l'inventaire** et à des **ruptures de stock** en magasins : **l'intégrité des données** est donc un **enjeu fort** pour la Supply Chain.

La Supply Chain du Groupe (composée de 14 entrepôts dont 4 sous-traités) a pour volonté de se **numériser** pour gagner en **agilité**. Cela passe par exemple par **l'augmentation de la performance** des accès SI aux entrepôts (diminuer les latences des outils SI pour être au plus proche de l'utilisateur,...), notamment par **l'utilisation du Cloud**, la mise en place de **18 firewalls** et l'introduction d'actions de **segmentation**.

Le Groupe cherche donc, dans cette démarche d'amélioration, à **optimiser son réseau informatique** et **ses performances** : réduire les flux d'information permet de **centraliser** tout en **réduisant la latence**, pour un réseau **plus réactif** et **mieux protégé**.

avec une offre de **sécurisation** plus **vaste** (les sociétés proposant des services de cybersécurité évoluent), cet acteur déploie **deux chantiers** pour sécuriser sa Supply Chain :

### 1/ Détection cyber dans un entrepôt

Suite au **manque de visibilité dans ses interactions** (interactions entre l'OT (Operational Technology), l'écosystème IT et les accès (IPsec,...)), le Groupe décide d'utiliser le **SOC** (Security Operation Center : équipe en charge de superviser le SI et de détecter toute action malveillante). Le but de cette action est de permettre au Groupe d'avoir une **meilleure visibilité** sur tout leur système informatique pour mettre en place une **supervision plus globale** dans des systèmes **très complexes**.

### 2/ Gestion du patch management

Le but de ce chantier est de mettre en place des actions pour **réduire la vulnérabilité** du système en **corrigeant ses défauts** (mise à jour, revue du code d'une application,...) : pour protéger son système le groupe cherche à **identifier ses points faibles** pour les corriger.

## ÉTAT DE LA CYBERSÉCURITÉ CHEZ CET ACTEUR

### Maturité :

Le niveau de maturité est encore aux prémices, cependant les risques sont maintenant plus **visibles** et **pris en compte** par la direction.

### Enjeux Cybersécurité

L'enjeu principal est de réussir à **embarquer les fournisseurs et les sous-traitants**, les principaux interlocuteurs du groupe ne sont pas habitués à parler sécurité et il n'y a **pas de contrainte réglementaire** qui les y obligent.

## 3 CLÉS DE RÉUSSITE POUR APPLIQUER LA CYBERSÉCURITÉ À LA SUPPLY CHAIN :

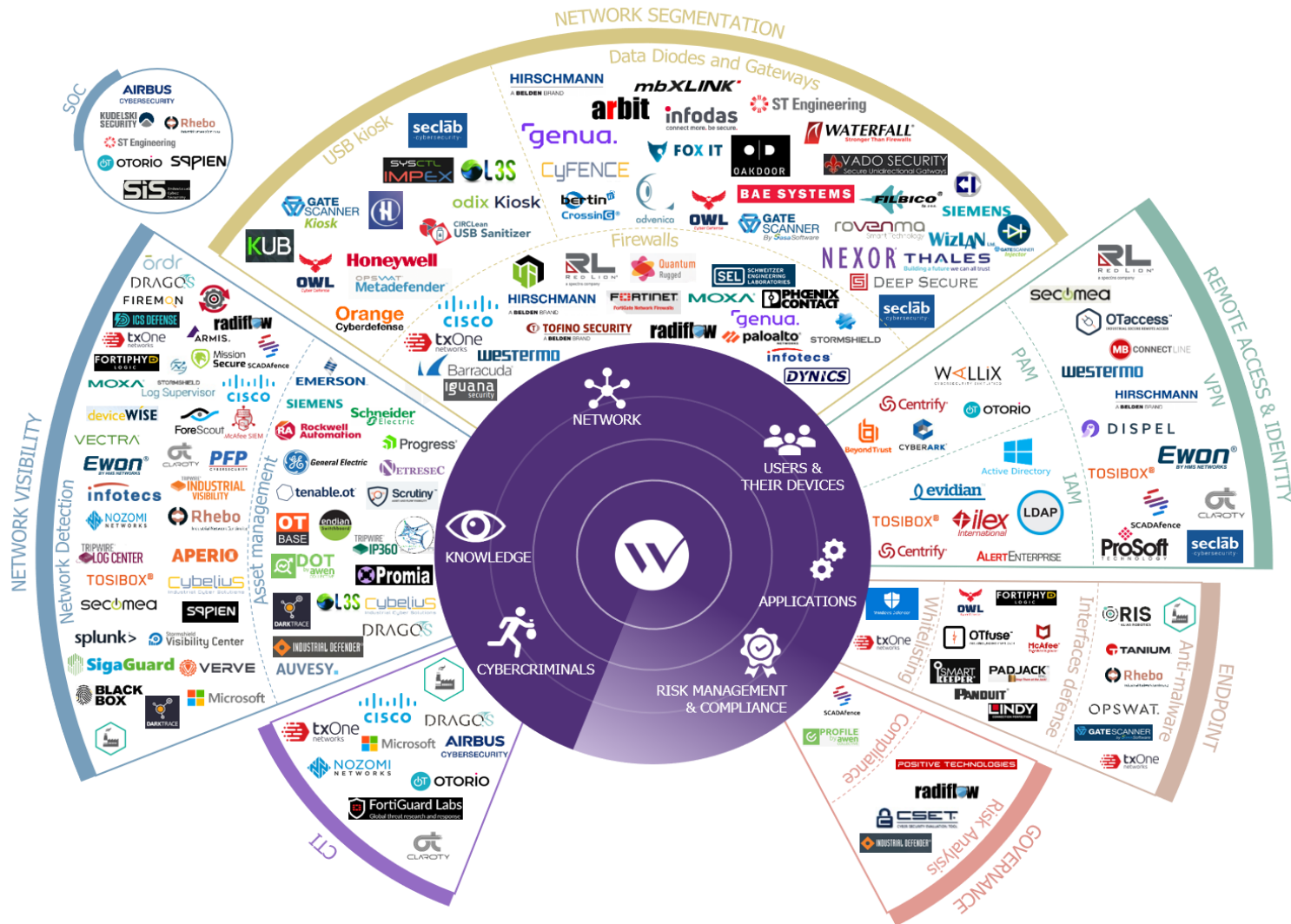
- ✓ Réussir à **collaborer** avec ses fournisseurs et faire comprendre le besoin de **produits sécurisés**
- ✓ Faire **prendre conscience** au collaborateur de **l'importance de la cybersécurité**
- ✓ Montrer que la cybersécurité apporte de la **valeur au métier**



# 05 Radar des solutions cyber

# Radar des solutions Cybersécurité pour les Systèmes d'Information Supply Chain

UNE MULTITUDE DE SOLUTIONS CYBERSÉCURITÉ À CHERCHER PARMİ CELLES EXISTANTES POUR SÉCURISER DES SI DE GESTION MAIS AUSSI DES SOLUTIONS PLUS SPÉCIFIQUES QUI S'APPLIQUENT AUX SI D'EXÉCUTION (USINE, ENTREPÔT, TRANSPORT...)



Le radar de la cybersécurité présente des produits de cybersécurité spécialisés dans les Systèmes d'Informations qui s'appliquent au monde de la Supply Chain.

Il existe de nombreuses solutions de cybersécurité, mais le plus important, au-delà de l'achat de solutions, est la mise en place d'une gouvernance et d'une gestion des risques efficace.



# Contributeurs



**MARC DAUGA**

Partner **Supply Chain**  
marc.dauga@wavestone.com



**GERÔME BILLOIS**

Partner - Expert **Cyber**  
gerome.billois@wavestone.com



**BENOIT BOUFFARD**

Manager - Expert **Cyber**  
benoit.bouffard@wavestone.com

Cette publication a été réalisée avec les contributions de France Supply Chain et de l'équipe Wavestone

Remerciements particuliers à tous les participants et contributeurs :

Camille Demarquilly (Michelin), Cyrille Faisant (Groupe Rocher), David Gallet (Schneider Electric), Karine Louarn (EOL), François Martin-Festa (Schneider Electric), Gino Meul (Groupe Avril), Eric Le Mignon (Les Mousquetaires), Tudor Mirica (Groupe Renault), Xavier Le Schaeve (Rémy Cointreau), Valérie Macrez (France Supply Chain), Steeve Michon (Wavestone), Marguerite Quichaud (Wavestone), Dimitri Vivier (Wavestone)

## Wavestone

---

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Wavestone rassemble plus de 3 000 collaborateurs dans 8 pays. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le premier cabinet de conseil indépendant en France. Wavestone est coté sur Euronext à Paris.

**WAVESTONE**

## France Supply Chain, by Aslog

---

Dans un monde de plus en plus complexe, faire de la Supply Chain un levier pour un monde plus durable est un enjeu essentiel pour toutes les entreprises. C'est pourquoi France Supply Chain apporte des solutions pertinentes à tous les acteurs de la Supply Chain, grâce à son réseau de 450 entreprises affiliées et une démarche reposant sur l'intelligence collective.

