Paris le 18 juin 2021

SAVVA Alexis
alexis.louis.savva@gmail.com
Master 2 Cybersécurité

Université de Paris

Etude de cas :
EBIOS RM

APSYS
AUGMENTED TRUST

Paris le 18 juin 2021

Table des matières

Paris le 18 juin 2021

Introduction

Cette analyse de risques est réalisée dans le cadre d'un projet de sécurisation d'un site de production industriel. La société ELECTRON conçoit et produit des composants électroniques et des capteurs destinés à équiper les éléments de sécurité de différentes marques automobiles, ainsi qu'au domaine du transport ferroviaire.

Elle a pour objet la sécurisation des activités tant en interne qu'en externe en utilisant Ebios RM.

Les mesures présentées dans ce rapport seront transmises à la direction de l'entreprise afin que les équipes techniques prennent connaissance des mesures de sécurité préconisées.

La principale activité de l'entreprise est de produire des composants électroniques et des capteurs destinés à équiper les éléments de sécurité de différentes marques automobiles, ainsi qu'au domaine du transport ferroviaire.

Pour cette analyse, nous procéderons donc avec une méthode en 5 étapes en suivant les grandes méthodes d'analyse de risques Ebios RM.

Le premier atelier vise à identifier l'objet de l'étude, les participants aux ateliers et le cadre temporel. Au cours de cet atelier, nous recensons les missions et les biens supports relatifs à l'objet étudié. Nous identifions les événements redoutés associés aux valeurs métier et évaluons la gravité de leurs impacts.

Dans le deuxième atelier, nous identifions et caractérisons les sources de risque (SR) et leurs objectifs de haut niveau, appelés objectifs visés (OV). Les couples SR/OV jugés les plus pertinents sont retenus au terme de cet atelier. Les résultats sont formalisés dans une cartographie des sources de risques.

Dans l'atelier 3, nous allons acquérir une vision claire de l'écosystème et établir une cartographie de menace numérique de celui-ci vis-à-vis de l'objet étudié. Ceci va nous permettre de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ils représentent les chemins d'attaque qu'une source de risques est susceptible d'emprunter pour atteindre son objectif. Ces scénarios se conçoivent à l'échelle de l'écosystème et des valeurs métier de l'objet étudié. Ils sont évalués en termes de gravité. À l'issue de cet atelier, nous pouvons déjà définir des mesures de sécurité sur l'écosystème.

Le but de l'atelier 4 est de construire des scénarios techniques reprenant les modes opératoires susceptibles d'être utilisés par les sources de risques pour réaliser les scénarios stratégiques. Cet atelier adopte une démarche similaire à celle de l'atelier précédent mais se concentre sur les biens supports critiques. Nous évaluons ensuite le niveau de vraisemblance des scénarios opérationnels obtenus.

Le dernier atelier consiste à réaliser une synthèse de l'ensemble des risques étudiés en vue de définir une stratégie de traitement du risque. Cette dernière est ensuite déclinée en mesures de

sécurité inscrites dans un plan d'amélioration continue. Lors de cet atelier, nous établissons la synthèse des risques résiduels et définissons le cadre de suivi des risques.

La phase dans laquelle nous sollicitons un représentant de l'entreprise ayant des activités sur les différents périmètres a été réalisée dans l'atelier 1 et 2 et nous remercions ce représentant de s'être rendu disponible et d'avoir répondu à nos questions.

Cette phase nous a permis de comprendre le fonctionnement métier et leurs besoins afin de cibler les critères de sécurité sur la base de la disponibilité, l'intégrité, la confidentialité et de la traçabilité.

Il s'agit d'une étape importante du processus métier.

Ce rapport a pour but de mesurer le niveau de sécurité à mettre en place, si cela le permet, afin d'avoir un niveau de sécurité suffisant et opérationnel. L'approche intègre la dimension métier de l'entreprise ainsi que les aspects humains, organisationnels et techniques. L'analyse porte sur les informations que nous détenons et celles fournies lors de l'échange avec le représentant de l'entreprise. Nous évaluons les mesures déjà mises en place sur les systèmes d'information.

Ebios RM repose sur 3 principes et objectifs:

- Proposer des outils adaptables et des référentiels normatifs en matière de sécurité numérique
- Evaluer les risques numériques et les mesures à mettre en œuvre pour les maîtriser
- Définir un niveau de sécurité à atteindre

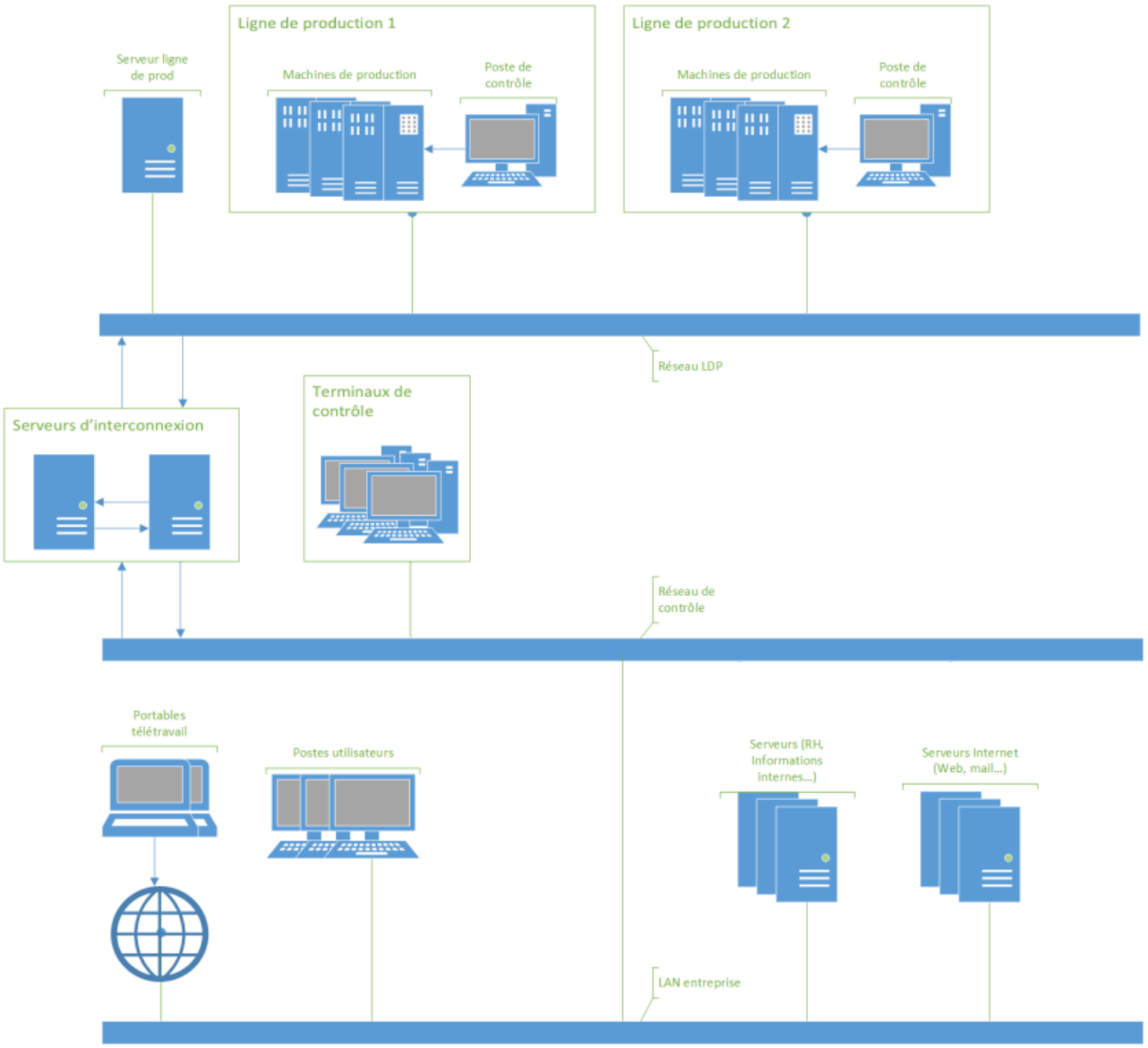
Notre cotation des impacts de la gravité et de vraisemblance est basée sur les grilles d'EBIOS RM que vous trouverez ci-dessous.

ÉCHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

ÉCHELLE	DESCRIPTION
V4 quasi certain	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée.
V3 Très vraisemblable	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée.
V2 Vraisemblable	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
V1 Peu vraisemblable	La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible.

Paris le 18 juin 2021

Architecture de la chaîne de production



Le réseau à étudier est constitué de 3 couches :

1. Le SI global de l'entreprise.
2. Une couche de contrôle, sur un site géographique distant (usines), qui a pour fonction principale la surveillance, et le pilotage de la ligne de production (on considérera qu'il existe une multitude de réseaux de contrôles similaires. (Un par ligne de production)
3. Une couche de production, c'est-à-dire la ligne de production elle-même. Chaque machine et outil sont accessibles au travers d'un poste de contrôle.

Paris le 18 juin 2021

Atelier 1

Le but de ce premier atelier est de définir le cadre de l'étude, son périmètre métier et technique, les événements redoutés associés et le socle de sécurité. Cet atelier est un prérequis à la réalisation d'une appréciation des risques.

Le cadre de l'étude

Pour initier l'atelier, commençons par cerner les objectifs ainsi que les biens essentiels de la société ELECTRON. Ensuite nous définirons les événements redoutés en fonction des biens essentiels. Enfin, nous classifierons ces menaces en fonction de leur criticité.

Objectifs : produire des composants électroniques

- Produire des composants de qualité
- Livrer dans les temps
- Produire dans les temps
- Innover pour maintenir l'avantage concurrentiel
- Traçabilité et contrôle

Acteurs

- MOA
- DSI
- Toute autre personne jugée essentielle ou ayant une valeur ajoutée dans le processus

Biens essentiels

- LDP (Ligne De Production)
- R&D
    - Innover (sécurité, coût, efficacité)
    - Tester
- SI
- Composants de base
- Savoir-faire
- La maîtrise d'œuvre
- Le composant final

Evènements redoutés

- Arrêt de la LDP
- Manque de composants de base
- Pénurie de composants
- Fuite de données (R&D et savoir-faire)
- Perte de données
- Altération de données
- Indisponibilité du SI
- Iso 9001 / 27000
- Indisponibilité d'usine par des événements climatique ou humain
- Pandémie mondiale
- Événement de sécurité sur le personnel
    - Cyber
    - Global

ÉCHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Arrêt de la LDP • <1 semaine • >1 semaine	 2 : Significatif 3 : Grave
Manque de composants de base • <1 semaine	 1 : mineur

• >1 semaine	3 : grave
Pénurie de composants (long terme)	3 : grave
Fuite de données • R&D • Savoir-faire	 3 : grave 2 à 3 : Significatif à grave
Perte de données	3 : Grave
Altération de données • R&D • Savoir-faire	 3 : grave 2 : significatif
Indisponibilité du SI • SI LDP • SI global • SI siège social	 2 : significatif 3 : grave 2 : significatif
Normatif (Iso 9001 / 27000…)	4 : critique
Pandémie mondiale	3 : grave
Indisponibilité d'usine par des événements climatique ou humain	2 : significatif
Événement de sécurité sur le personnel	3 : grave

Norme

Normes d'hygiène de base respectées :

- Sauvegardes hebdomadaires sur le même site que les serveurs
- Réplication des données et identités
- Un compte par utilisateur LDAP avec droits uniques
- Gestion des accès
- Sensibiliser les employés à la cybersécurité
- Sécuriser les postes de travail et la LDP
- Sécuriser le réseau
- Superviser, Auditer, Réagir
- Chiffrement
- Genis logiciel
- Segmentation du réseau
- Signature numérique
- Référentiel
- PRA et PCA

Paris le 18 juin 2021

Atelier 2

Le but de l'atelier 2 est d'identifier les sources de risque (SR) et leurs objectifs visés (OV), en lien avec le contexte particulier de l'étude. L'atelier vise à répondre à la question suivante : Qui ou quoi pourrait porter atteinte aux missions et valeurs métiers identifiées dans l'atelier 1, et dans quels buts ?

Sources de risque

- Concurrent
- Hacker
- Les hacktivistes ne sont pas vraiment une source de risque si les équipements créés par ELECTRON respectent l'environnement et les droits des hommes. Dans le sujet aucune information a été communiquée sur cela, nous partons du principe que les hacktivistes ne sont pas une source de risques.

Objectifs visés

- Prestige :
    - Hacker
        - Gagner du prestige au travers d'un hack difficile / remarqué
        - S'entraîner

- Arrêt de production :
    - Hacker
        - Ligne de production
            - Soutirer de l'argent à l'entreprise
            - Attaque cyber sur la LDP
            - Attaque sur les SI
            - Attaque au président
            - Attaque sur l'image de l'entreprise
        - R&D
            - Vol / Destruction des recherches et innovations
            - Altération des données
            - Interruption des phases de tests
    - Concurrent
        - Porter atteinte à l'entreprise dans le but de gagner un avantage concurrentiel
        - Attaquer l'image de la marque
        - Attaque cyber sur la LDP
            - Attaque cyber sur la LDP
            - Attaque sur les SI

- Absence de livraison de composants de base :
    - Concurrent
        - Provoqué par le concurrent (corruption du livreur)
        - Interrompre la LDP
- Vol d'information :
    - Hacker
        - Chantage
        - Injection de code malveillant
        - Extraction de données
    - Concurrent
        - Chantage
        - Salarié / prestataire corrompu ou malveillant
        - Injection de code malveillant
        - Extraction de données
        - Avantage concurrentiel
        - Perte de CA
- Altération des données
    - Hacker
        - Chiffrement des données
    - Concurrent
        - Injection de code malveillant
        - Atteinte à l'image de l'entreprise
        - Saboter les produits

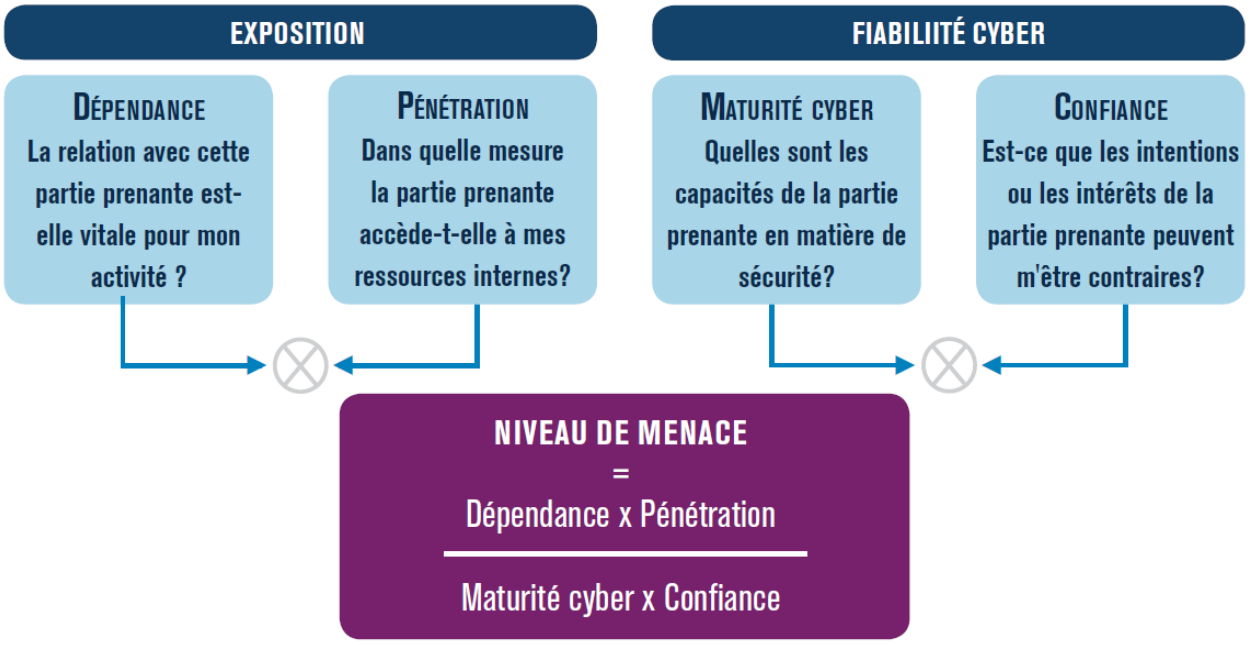
SR	OV	Motivation	Ressources	Activité	Pertinence
Hacker	Rançonnage	2	1	3	6 élevé
Hacker	Vol d'information	1	1	3	3 faible
Hacker	Prestige	1	1	2	2 faible
Concurrent	Arrêt de la production pour un avantage concurrentiel	2	3	2	12 Très élevé
Concurrent	Privation de composants de base	2	2	2	8 élevé
Concurrent	Vol d'information pour un avantage concurrentiel	3	3	3	27 Très élevé

Concurrent	Altération des données pour un avantage concurrentiel	1	3	1	3 faible

Atelier 3

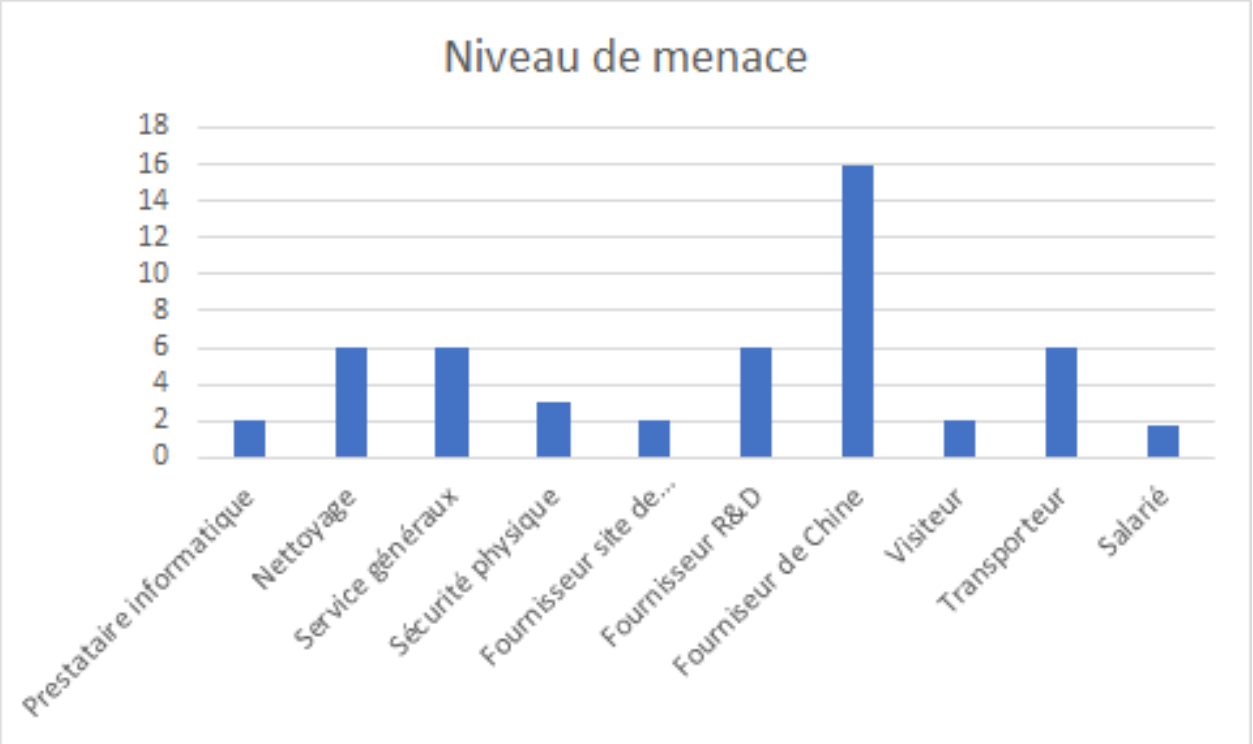
L'objectif de l'atelier 3 est de disposer d'une vision claire de l'écosystème, afin d'en identifier les parties prenantes les plus vulnérables. Il s'agit ensuite de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ces derniers sont autant de chemins d'attaques que pourraient emprunter une source de risque pour atteindre son objectif (i.e. un des couples SR/OV sélectionnés lors de l'atelier 2). L'atelier 3 est à aborder comme une étude préliminaire de risques. Il peut conduire à identifier les mesures de sécurité à appliquer vis-à-vis de l'écosystème. Les scénarios stratégiques retenus dans l'atelier 3 constituent la base des scénarios opérationnels de l'atelier 4.

Calcul du niveau de menace



	Dépendance	Pénétration	Maturité Cyber	Confiance	Indice
Prestataire informatique	3	4	3	2	2
Nettoyage	3	4	1	2	6
Services généraux	3	4	1	2	6

Sécurité physique	3	4	2	2	3
Fournisseur site de production	4	2	2	2	2
Fournisseur R&D	3	4	1	2	6
Fournisseur de Chine	4	4	1	1	16
Visiteur	1	2	1	1	2
Transporteur	3	2	1	1	6
Salarié	4	4	3	3	1.8



Cartographie de la menace

Retenus critiques :

- Nettoyage

- Service généraux
- Sécurité physique
- Fournisseur R&D
- Fournisseur de Chine
- Transporteur

- A surveiller (veille) :
  - Prestataire informatique
  - Fournisseur site de production
  - Visiteur

- Non retenus :
  - Salarié

Scénarios stratégiques

SR	OV	Chemin d'attaque	Gravité
Hacker	Rançonnage	• Attaque le SI de production • Attaque le SI de la R&D • Cibler les postes de travail des salariés • Par un prestataire informatique • Attaque la sous-traitance • Par des mails de phishing • Mauvaise configuration du VPN	4
Hacker	Vol d'information	• Cibler les postes de travail des employés • En attaquant le SI. • Attaque du SI de la R&D • Attaque d'un poste de travail d'un salarié en télétravail • Par un prestataire informatique • Faille dans le système • Faille humaine • Faille dans les composants venant de Chine • Code malveillant	4

		• Par des mails de phishing • Mauvaise configuration du VPN	
Hacker	Gagner de l'argent	• En infectant un poste dans un garage • En infectant un poste chez un revendeur • Par un prestataire informatique • Demande de rançon pour des informations confidentielles de l'entreprise	3
Hacker	Prestige	• Accès au site pour le défacer • Montrer ses compétences • Faille dans le système • Faille humaine	2
Concurrent	Arrêt de la production pour un avantage concurrentiel	• Attaque du SI • Attaque des fournisseurs • Attaque des transporteurs • Attaque la R&D • Par un prestataire informatique • Faille dans les composants venant de Chine • Interruption de la livraison de composants par le biais d'un livreur corrompu • Changement des composants volontaires des fournisseurs • Injection de code malveillant • Modifier les plans des composants lors de la R&D • Atteinte à l'image de l'entreprise	4
Concurrent	Privation de composants de base	• Soudoyer des transporteurs • Achats massifs des concurrents des composants • Concurrents qui achètent ou déposent un brevet sur des composants nécessaires afin d'avoir l'exclusivité • Créer une pénurie • Atteinte à l'image de l'entreprise afin que les fournisseurs ne vendent pas à l'entreprise	4
Concurrent	Vol d'information pour un avantage concurrentiel	• Attaque du SI • Attaque du SI de la R&D	3

		• En passant par un prestataire informatique • Soudoyer les prestataires et sous-traitants • Remplacement des composants avant d'être scellés • Vols des documents confidentiels et équipements par un visiteur ou une personne ayant accès à l'étage dans le bâtiment de R&D	
Concurrent	Altération des données pour un avantage concurrentiel	• Attaque du SI • Attaque du SI de la R&D • En passant par un prestataire informatique • Vols des documents confidentiels et équipements par un visiteur ou une personne ayant accès à l'étage dans le bâtiment de R&D • Modification des documents de R&D	3
Salarié corrompu ou malveillant	Vol d'information / Destruction de données Divulgation de données	• Copier des fichiers sensibles de l'entreprise sur une clé USB. • Imprimer des documents confidentiels. • Chiffrer les données de l'entreprise • Supprimer des fichiers auxquels il a accès. • Vente des documents aux concurrents • Infecter un poste dans un garage • Infecter un poste chez un revendeur	4

Mesures de sécurité

Partie prenante	Chemin d'attaque	Mesure de sécurité	Menace initiale	Menace résiduelle
Prestataire informatique	• Voler les informations auxquelles il a accès. • Peut injecter du code malveillant.	• Donner les accès sensibles par dérogations et les retirer une fois terminé.	2	1.33

	• Peut attaquer l'infrastructure comme les serveurs ou autre • Attaque de ransomware • Sabotage des équipements, salles de serveurs • Insertion de clefs USB • Détruire du matériel • Voler du matériel • Compromission du serveur centralisé VMWare • Microphone et caméras	• Cloisonnement du SI • Mettre en place un système de badge a plusieurs accès. • Traçabilité de leurs déplacements • Mise en place de serveurs de backup • Mise en place de PCA et PRA • Mise en place d'équipements de surveillance et de sécurité tels que des antivols et pièces avec badges • Secure by design • Vérification des solutions du prestataire • Station de désinfection des clefs USB • Traçabilité • Antivols Maturité cyber 3 -> 3 Confiance 2 -> 3		
Nettoyage	• Insertion d'un appareil malveillant sur un ordinateur. • Voler des documents qui traînent sur les bureaux ou dans les poubelles. • Couper le courant des salles des machines • Accéder à des documents confidentiels • Saboter les serveurs • Microphones et caméras	• Supprimer par défaut le droit de brancher des clés USB • Mettre en place des casiers sécurisés et des broyeurs de documents. • Traçabilité des personnes • Fermer les bureaux • Station de désinfection des clefs USB • Personne responsable du site présente lorsqu'une personne non habilité est présente dans les bureaux	6	2

		• Mise en place d'équipements de surveillance et de sécurité tels que des antivols et pièces avec accès • Protéger les ports • Traçabilité • Antivols Maturité cyber 1 -> 3 Confiance 2 -> 2		
Services généraux	• Créer des pannes volontaires • Voler des documents confidentiels • Insertion d'un appareil malveillant sur un ordinateur. • Couper le courant des salles des machines • Saboter les serveurs • Surchauffer des machines • Accéder à des documents confidentiels • Voler du matériel • Photo des équipements et des locaux • Microphone	• Mise en place de composants permettant d'éviter le vol. • Mise en place de service de secours • Présence d'un responsable sur le site • Protéger les ports • Mise en place de sécurité sur des équipements • Désactiver les prises non assignées • Sensibilisation du fournisseur au niveau cyber Maturité cyber 1 -> 2 Confiance 2 -> 2	6	3
Sécurité physique	• Peut attaquer l'infrastructure comme les serveurs ou autre • Insertion d'un appareil malveillant sur un ordinateur. • Voler des documents qui traînent sur les bureaux ou dans les poubelles. • Laissez passer des personnes non habilité comme les concurrents • Prise de photo d'équipements • Sabotage des équipements	• Supprimer par défaut le droit de brancher des clés USB • Mettre en place des casiers sécurisés et des broyeurs de documents. • Mettre en place un système de badges a plusieurs accès.	3	1.33

	• Insertion de clefs USB	• Un badge pour accéder au site et un autre pour l'infrastructure. • Station de désinfection des clefs USB • Mise en place de référentiel • Traçabilité • Antivols • Sensibilisation du fournisseur au niveau cyber Maturité cyber 2 -> 3 Confiance 2 -> 3		
Fournisseur site de production	• Peut immobiliser la production en ne donnant pas les composants critiques • Remplacer ou endommager les composants • Échanger les composants • Faire des photos des composant pour les concurrents	• S'assurer d'avoir plusieurs fournisseurs • S'assurer d'avoir les bons composants • Faire des testes sur les composants • Mise en place de procédure pour tester les composants avant envoi et après réception • Mise en place de référentiel • Traçabilité • Sensibilisation du fournisseur au niveau cyber Maturité cyber 2 -> 2 Confiance 2 -> 2	2	2
Fournisseur R&D	• Remplacer ou endommager les composants • Échanger les composants • Faire des photos des composants pour les concurrents • Modification des composants • Rupture des stocks	• S'assurer d'avoir plusieurs fournisseurs • S'assurer d'avoir les bons composants • Faire des tests sur les composants • Mise en place de procédure pour tester les composants avant envoi et après réception • Mise en place de caméras et agents de sécurité	6	1.5

		• Mise en place de référentiel • Stocks de côté des produits indispensables • Surveillance • Traçabilité • Sensibilisation du fournisseur au niveau cyber Maturité cyber 1 -> 2 Confiance 2 -> 2		
Fournisseur de Chine	• Modification des composants • Faille sur les composants • Matériaux de mauvaises qualités • Rupture des stocks	• Changer de fournisseur, choisir un fournisseur en Europe • Contrôle de qualité • Vérification des composants • Mise en place de référentiel • Stocks de côté des produits indispensables • Surveillance • Traçabilité • Sensibilisation du fournisseur au niveau cyber Maturité cyber 1 -> 2 Confiance 1 -> 1	16	8
Visiteur	• Insertion d'un appareil malveillant sur un ordinateur. • Voler des documents qui traînent sur les bureaux ou dans les poubelles. • Brancher des clés USB • Remplacer ou endommager les composants • Voler des composants • Prendre des photos des bureaux • Microphone	• Supprimer par défaut le droit de brancher des clés USB • Mettre en place des casiers de sécurité et des broyeurs de documents. • Un service de sécurité • Des badges permettant d'accéder aux équipements délivrés par le DSI • Surveillance • Traçabilité Maturité cyber 1 -> 2	2	0.5

		Confiance 1 -> 2		
Transporteur	• Peut voler des informations en livrant des composants • Échange de composants • Destruction de composants • Altération des composants • Livrer les mauvais composants intentionnellement • Endommager les composants	• Mettre en place un service qui s'occupe de la livraison pour éviter que les livreurs se baladent • Mise en place de référentiel • Sensibilisation du fournisseur au niveau cyber • Mise en place d'alternatives • Surveillance • Traçabilité • Antivols Maturité cyber 1 -> 1 Confiance 1 -> 2	6	3
Salarié	• Vol les informations auxquels il a accès • Injection de code malveillant • Suppression d'informations • Sabotage • Vol d'ordinateurs • Endommager les composants • Voler des composants • Prendre des photos des bureaux • Microphone	• Classifier des documents • Mettre en place un système de gestion des droits et des identités des accès. • Traçabilité des actions. • Sécuriser le matériel à l'aide de câble Kensington. • Surveillance • Traçabilité • Antivols • Sensibilisation du fournisseur au niveau cyber Maturité cyber 3 -> 3 Confiance 3 -> 3	1.8	1.8

Atelier 4

L'objectif de l'atelier 4 est de construire des scénarios opérationnels. Ils schématisent les modes opératoires que pourraient mettre en œuvre les sources de risques pour réaliser les scénarios stratégiques. Cet atelier adopte une démarche similaire à celle de l'atelier précédent mais se concentre sur les biens supports. Les scénarios opérationnels obtenus sont évalués en termes de vraisemblance.

ÉCHELLE	DESCRIPTION
V4 quasi certain	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée.
V3 Très vraisemblable	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée.
V2 Vraisemblable	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
V1 Peu vraisemblable	La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible.

Scénarios opérationnels

Chemin d'attaque	Vraisemblance
Un concurrent vole des informations en passant par un prestataire informatique	V4
Un concurrent vole des informations lors d'une attaque	V4

directe du SI du centre R&D	
Compromission d'un poste dans une usine par un hacker	V3
Compromission d'un poste chez sur le site de R&D	V4
Vol d'un poste de travail et rentre dans le réseau par le VPN car manque d'authentification	V3
Vol de document sur le site de R&D en demandant un badge à l'accueil	V4
Un prestataire informatique vole les informations auxquelles il a accès	V4
Un prestataire informatique injecte du code malveillant	V3
Un agent de nettoyage insert un appareil malveillant sur un ordinateur	V4
Un transporteur peut voler des informations en livrant des composants	V3
Un fournisseur immobilise la production en ne donnant pas les composants critiques	V3
Un fournisseur échange les composants	V3
Attaquer la sous-traitance et l'externalisation	V4
Un salarié vole des équipements	V4
Un membre du service de nettoyage vole ou dégrade du matériel	V3
Un employé vole des documents pour les revendre	V3
Le fournisseur chinois installe des failles de sécurité dans les équipements	V4
Un membre de la sécurité laisse entrer un concurrent sur le site de l'entreprise	V4
Un hacker vole des documents confidentiels	V4
Un hacker fait une attaque par rançonnage en compromettant le prestataire informatique, le fournisseur, le transporteur	V4

Un concurrent interrompt la production pour un avantage concurrentiel en compromettant une partie prenante de la production	V3
Un prestataire détruit des équipements	V4

Atelier 5

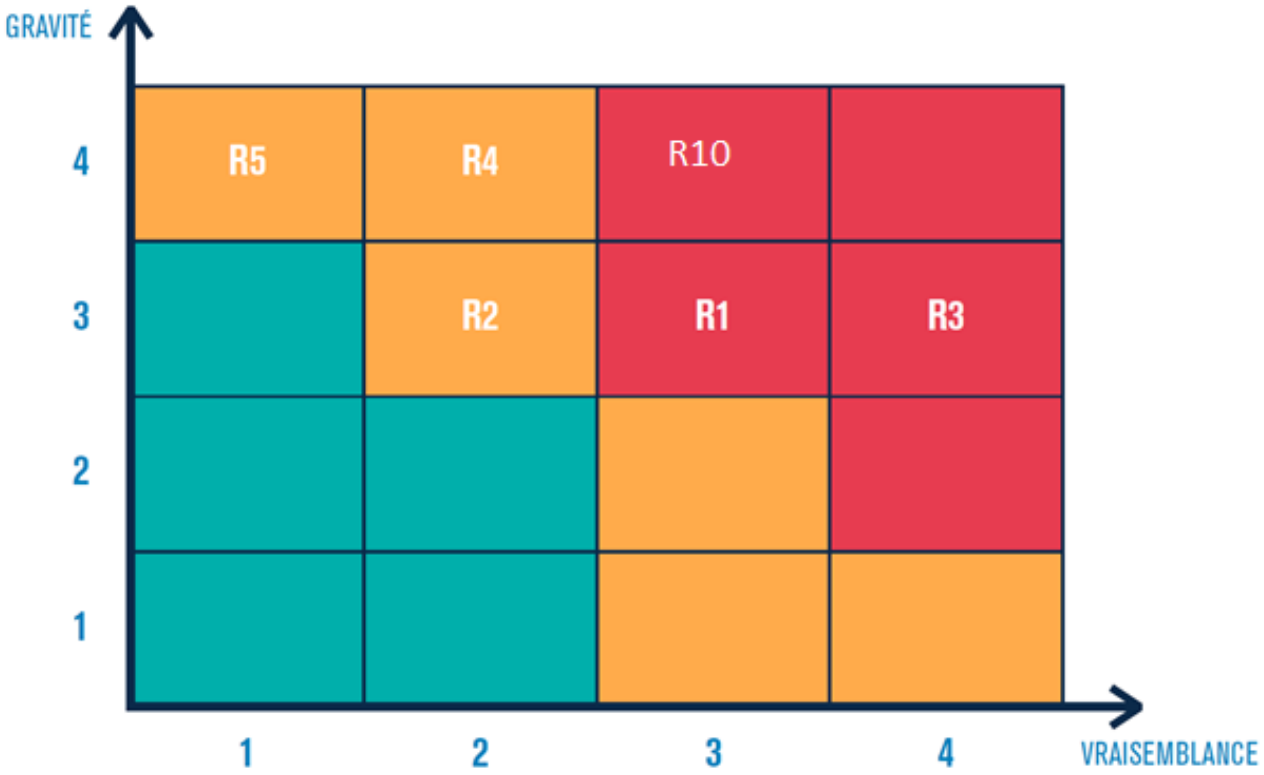
Le but de cet atelier est de réaliser une synthèse des scénarios de risque identifiés et de définir une stratégie de traitement du risque. Cette stratégie aboutit à la définition de mesures de sécurité, recensées dans un plan d'amélioration continue de la sécurité (PACS). Les risques résiduels sont ensuite identifiés ainsi que le cadre de suivi de ces risques.

Cartographie du risque

- Un concurrent vole des informations en passant par un prestataire informatique (R1)
- Un concurrent vole des informations lors d'une attaque directe du SI du centre R&D (R2)
- Compromission d'un poste dans une usine par un hacker (R3)
  Compromission d'un poste chez sur le site de R&D (R4)
- Vol d'un poste de travail et rentre dans le réseau par le VPN car manque d'authentification (R5)
- Vol de document sur le site de R&D en demandant un badge à l'accueil (R6)
- Un prestataire informatique vole les informations auxquelles il a accès (R7)
- Un prestataire informatique injecte du code malveillant (R8)
- Un agent de nettoyage insert un appareil malveillant sur un ordinateur (R9)
- Un transporteur peut voler des informations en livrant des composants (R10)
- Un fournisseur immobilise la production en ne donnant pas les composants critiques (R11)
- Un fournisseur échange les composants (R12)
- Attaquer la sous-traitance et l'externalisation (R13)
- Un salarié vole des équipements (R14)
- Un membre du service de nettoyage vole ou dégrade du matériel (R15)
- Un employé vole des documents pour les revendre (R16)
- Le fournisseur chinois installe des failles de sécurité dans les équipements (R17)
- Un membre de la sécurité laisse entrer un concurrent sur le site de l'entreprise (R18)
- Un hacker vole des documents confidentiels (R19)

- Un hacker fait une attaque par rançonnage en compromettant le prestataire informatique, le fournisseur, le transporteur (R20)
- Un concurrent interrompt la production pour un avantage concurrentiel en compromettant une partie prenante de la production (R21)
- Un prestataire détruit des équipements (R22)

Exemple de Risque sur la table de gravité et vraisemblance



Paris le 18 juin 2021

Traitement du risque

Mesure de sécurité	Scénario de risque	Responsabilité	Freins à la mise en oeuvre	Coût/complexité	Echéance	Statut
Contrôle d'intégrité des données entrantes du SI	R1,R3, R8, R9, R12, R15,R21 R22	DSI	Long à mettre en place	++	T+3 mois	En cours
Sensibilisation cyber des parties prenantes	R2, R3, R6, R8, R9, R11, R12, R13, R15,R20	RSSI/DSI	Veille constante		T+6 mois	En cours
Mise en place d'une charte d'hygiène	R2, R3, R6, R8, R9, R11, R12, R13, R15,R16	RSSI/DSI	Veille constante		T+3 mois	En cours
Mise en place d'une gestion des identités et des accès	R1, R2, R4, R5, R6, R7, R10, R11, R13, R14,R17	RSSI/DSI	Long et complexe et mettre en place	++	T+6 mois	En cours
Patch Management	R1, R2, R4, R5, R6, R7, R10, R11, R13, R14,R16, R19	RSSI/DSI	Veille constante	+	T+6 mois	En cours
Whitelist des médias amovibles	R2, R3, R4, R5, R6, R8, R9, R10, R11, R13,	DSI	Constante mise à jour de la whitelist		T+3 mois	En cours

	R14,R18, R21,R22					
Surveillance physique des locaux	R2, R3, R4, R5, R6, R8, R9, R10, R11, R13, R14,R16, R20,R21, R22	DSI/Responsable du site	Nécessite beaucoup de personnels	++	T+3 mois	Terminé
Protection physique des appareils sensibles	R11, R10,R17, R21,R22	DSI	Veille constante	++	T+12 mois	En cours
Traçabilité des produits transportés	R3,R9,R12,R15,R17,R19	DSI	Acceptation par les transporteurs	++	T+3 mois	En cours
Vérification physique des accès	R11,R16, R17,R8, R19,R20, R22	DSI	Veille constante	+	T+3 mois	En cours
Renforcement du plan de continuité d'activité	R3,R4,R5,R6,R7, R10,R12, R15,R18, R19,R20	RSSI/DSI	Veille constante	+	T+9 mois	En cours
Cloisonnement du SI R&D	R2,R3,R4,R5,R9, R12,R15, R16,R18, R19,R21	RSSI/DSI	Veille constante	++	T+9 mois	En cours
Accompagnement des visiteurs sur site	R1,R2,R3,R4,R6, R7R11,R14,R16,R18	DSI	Veille constante	+	T+3 mois	Terminé