Formation sur la méthode EBIOS Risk Manager

Module 1 : **Introduction à la méthode EBIOS Risk Manager**

Vidéo 1 : Présentation du Club EBIOS, de l'ANSSI, et des enjeux de la gestion des risques en cybersécurité

Bienvenue dans cette introduction à la formation sur la gestion des risques cyber avec la méthode EBIOS Risk Manager proposée par le Club EBIOS et l'ANSSI : l'Agence nationale de la sécurité des systèmes d'information.

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité dont l'objectif est de promouvoir l'échange d'idée et de bonnes pratiques.

L'ANSSI a développé la méthode EBIOS risk manager avec le support du **Club EBIOS** afin d'aider les organisations à anticiper et gérer les risques cyber de manière structurelle. La méthode **EBIOS risk manager** est une méthode d'analyse des risques qui permet de déterminer les mesures de sécurité adaptées au contexte et à la menace et de mettre en place un cadre de suivi et d'amélioration continue. Elle offre un cadre méthodologique pour identifier, analyser et traiter les risques cyber tout en permettant de prendre en compte les spécificités métiers de chaque organisation.

L'objectif : est de se concentrer sur les fondamentaux d'analyse de risques pour fournir une base solide qui facilitera ensuite l'apprentissage et l'application d'une méthode telle **EBIOS risk manager.**

Le paysage des menaces cyber évolue constamment, chaque année les Cyberattaques prolifèrent, touchant toutes les tailles d'organisation publique, collectivité ou établissement publique comme privées, en groupe le TI et PME.

Des rançongiciel paralysant les opérations, vol de données sensibles, les menaces sont variées et plus en plus sophistiquées.

Ces chiffres montrent que la cybersécurité n'est plus simplement une question technique mais un enjeu stratégique pour toutes les organisations et c'est pourquoi la décision de développement de cet accompagnement.

Ce MOOC vise à familiariser avec les principes de base d'une analyse de risques et à vous donner les outils nécessaires pour identifier, évaluer et gérer les risques cyber au sein de votre organisation. Elle ne se substitue pas à une formation sur la méthode **EBIOS risk manager,** elle se concentre sur les fondamentaux.

La gestion des risques cyber ne se limite pas seulement à éviter les attaques cyber, elle contribue aussi à assurer la continuité des activités (PCA), protéger les données sensibles et maintenir la confiance dans le système d'information concerné. En maîtrisant la gestion des risques, vous serez en mesure d'anticiper les risques et réagir rapidement en cas de cyber incident de développer une culture de la cybersécurité au sein de votre organisation, d'optimiser les investissements en cybersécurité en les priorisant sur les risques les plus critiques.

En suivant ce parcours, vous apprendrez donc à identifier les valeurs à protéger dans votre entreprise et évaluer les conséquences en cas d'attaque, définir les menaces qui pèsent sur vos systèmes, qualifier la dangerosité potentielle de votre écosystème, construire des scénarios de risques pertinents et réalistes, proposer des mesures adaptées pour réduire les conséquences des scénarios de risques.

Module 2 : Les fondamentaux de la cybersécurité

Vidéo 2 : les besoins de sécurité : Disponibilité, Intégrité et Confidentialité

Ces trois principes fondamentaux sont essentiels pour protéger les informations les plus critiques de l'organisation.

La Disponibilité garantie que les informations sont accessibles et utilisables lorsque cela est nécessaire. Ce principe est essentiel pour assurer la continuité des opérations d'une organisation. Par exemple, vos clients doivent pouvoir passer leurs commandes sur votre site où vous devez pouvoir accéder à vos outils RH pour poser vos congés. Si ça bloque, la disponibilité est rompue.

L'Intégrité garantie quant à elle, garantie que le système et information traitée ne soient modifiés que par une action volontaire et légitime. Si les données sont modifiées par erreurs ou intentionnellement comme un prix changé sans autorisation ou un solde congé réinitialisé alors l'intégrité est compromise.

La Confidentialité est le fait qu'une information ne puisse être accessible ou diffusée que seules les personnes autorisées. Par exemple, si les coordonnées clientes sont volées ou si des informations médicales sont exposées par erreurs, c'est une atteinte à la confidentialité.

Module 3 : Valeurs Métier

Vidéo 3 : Mise en situation avec le thème de la Boulangerie connectée

Pour mieux comprendre comment ces besoins fondamentaux **disponibilité, intégrité et confidentialité** s'appliquent dans la réalité, nous avons une proposition d'un exemple concret celui d'une boulangerie connectée qui sera le fil conducteur du MOOC.

Bienvenue dans le monde la baquette numérique, une boulangerie moderne qui a su évoluer en intégrant les nouvelles technologies pour offrir une expérience client innovante. Aujourd'hui, cette boulangerie utilise divers outils connectés :

1. **un site de commande en ligne** qui permet aux clients de choisir et réserver leurs produits ;
2. **des caisses automatiques en magasin** pour simplifier les paiements **;**
3. **une intelligence artificielle qui gère les stocks** pour éviter les ruptures de produits et un four électrique à commandes numériques.

Pour fonctionner, cette technologie dépend d'une infrastructure qui inclut des serveurs, des réseaux de communications internes et des logiciels spécifiques pour gérer les opérations quotidiennes. Grâce à ces innovations, la baquette numérique peut offrir un service rapide, personnalisé et gérer ces de manière efficace. Cependant, cette transformation expose la boulangerie à des risques que l'on retrouve dans l'actualité : les cyberattaques comme celles rapportées dans les médias peuvent des entreprises de toute taille y les commerces pour cette boulangerie. Par exemple des hackeurs ou des concurrents peuvent chercher à bloquer les systèmes pour réclamer une rançon, accéder aux informations sensibles des clients pour tout simplement perturber les activités.

Interview du responsable de la boulangerie sur les scénarios qui pourraient porter le plus de préjudices. Ces soucis peuvent causer pas mal de problèmes pour notre boulangerie. Si nos caisses tombent en panne, on ne peut plus encaisser les clients et ça nous fait perdre de l'argent tout de suite. Pareil pour notre site de commandes en ligne, s'il est piraté, les informations personnelles de nos clients pourraient en danger, ceux qui pourraient leur perdre confiance et même nous attirer des ennuis juridiques. Ça la réputation de notre boulangerie, nos fournisseurs comme ceux qui gèrent nos services en ligne, nos logiciels et ceux qui s'occupent de la maintenance jouent un rôle important dans la sécurité de tout le système. On doit compter sur eux pour éviter des problèmes ou des accès non autorisés ne perturbent notre activité.

Selon les médias, les scénarios d'attaques les plus fréquents inclus des emails frauduleux envoyés aux employés pour dérober des informations. Des virus introduits via des mis à jour non sécurisés ou encore des accès non autorisés par des tirs malveillants exploitant des vulnérabilités de sécurité.

Votre rôle, vous êtes chargés d'analyser les risques cyber auxquels la baquette numérique est exposée. Vous devrez identifier les menaces potentielles, évaluer leurs impacts sur les activités de la boulangerie et recommander des actions pour renforcer la sécurité des systèmes connectés. Votre analyse aidera la boulangerie à se protéger des analyses cyber et à garantir une expérience de qualité pour ces clients.

Vidéo 4 : Qu'est-ce qu'une Valeur Métier ?

Peut-être une activité indispensable produit, service ou d'une information qui doit être protégée, en d'autres termes ce sont des éléments vitaux de votre entreprise dans le cadre du périmètre de l'étude.

Imaginez-vous une entreprise avec laquelle chaque activité ou chaque information jouent un rôle dans l'accomplissement de sa mission, une valeur métier pourrait être un service client qui maintient la satisfaction des clients et la fidélisation. Elle pourrait aussi être la gestion de la production où l'efficacité et la qualité sont primordiales pour livrer les produits dans les délais.

Des exemples de Valeurs Métiers : activité de production, gestion du service client protefeuille

Comment identifier les valeurs métiers : Pour identifier les valeurs métiers, positionnez-vous dans l'objectif de réussite de votre mission. Posez-vous la question **quels sont les services, les informations, les activités qui sont vraiment critiques pour atteindre nos objectifs.** Ces valeurs métiers doivent être essentielles pour la direction des métiers et la maîtrise d'ouvrage.

Exemple concret de Valeurs Métiers : Prenons exemple d'un hôpital moderne, les valeurs métiers pourraient être inclure les services d'urgence qui est essentiel pour fournir des soins rapides et sauver des vies. Il pourrait également s'agir d'un processus de gestion de dossier de suivi médicaux crucial pour maintenir la confidentialité et l'accessibilité des informations des patients ou encore de l'approvisionnement en médicaments pour vital pour garantir que les traitements soient disponibles à tout moment.

Les Valeurs Métiers sont ce qui fait la richesse de votre entreprise, en les identifiant et en protégeant, vous contribuez directement à la pérennité et au succès de votre mission.

En définissant correctement les Valeurs Métiers, vous mettez en lumière ce qui est réellement important pour le succès de votre projet d'analyse de risques. C'est un exercice essentiel, car ces valeurs orientent les priorités de sécurisation et de gestion de risque. Les protéger, c'est assurer la pérennité et la performance de votre organisation.

Perspectives après avoir identifié les Valeurs Métiers : quelles sont les ressources concrètes sur lesquelles reposent ces valeurs ? Pour les répondre, il faudra s'intéresser aux biens supports. Ce sont les éléments techniques, organisationnels ou humains qui permet d'assurer le bon fonctionnement de votre activité au quotidien. Ce sont ces biens qu'il faut protéger, car ce sont eux qui portent les Valeurs Métiers dans la réalité.

Exercice 1 : Quelle est la meilleure définition d'une Valeur Métier ?

Une liste des équipements et logiciels nécessaires au fonctionnement de l'entreprise

Explication : une activité, un processus, une information ou un service critique qui contribue directement au succès et aux objectifs stratégiques.

Bonne réponse : Une activité, un processus, une information ou un service critique qui contribue directement au succès et aux objectifs stratégiques de l'entreprise

Explication : les Valeurs Métier représentent ce qui est vital pour atteindre les objectifs stratégiques d'une organisation. Elles incluent des activités comme la gestion des stocks, le service client ou la production.

Un ensemble de menaces potentielles identifiées pour une organisation donnée

Explication : les menaces potentielles ciblent les Valeurs Métier

Une mesure de sécurité mise en place pour protéger les systèmes de l'entreprise

Explication : une mesure de sécurité, comme un pare-feu ou l'authentification multi-facteurs, est un moyen permettant de protéger les Valeurs Métier, mais ce n'est pas une Valeur Métier en soi

Réponse : Une activité, un processus, une information ou un service critique qui contribue directement au succès et aux objectifs stratégiques de l'entreprise.

EXERCICE 2 : Identifier les Valeurs Métier de la boulangerie connectée

Parmi les propositions suivantes, cochez uniquement les Valeurs Métier. Plusieurs réponses possibles

Réponse : Gestion des stocks pour éviter les ruptures.

Explication : la gestion des stocks est au cœur des opérations d'une entreprise comme une boulangerie connectée. Une IA qui optimise les stocks garantit la disponibilité des produits, améliore l'efficacité, et évite les pertes financières dues à des ruptures.

Serveur de base de données hébergeant les informations des clients.

Explication : il s'agit d'une infrastructure technique qui soutient les Valeurs Métier, mais n'est pas une activité ou un service en soi.

Confidentialité des informations clients.

Explication : la confidentialité est un principe de sécurité appliqué aux données sensibles, mais ce n'est pas une activité centrale ou un service.

Caisses automatiques pour faciliter les paiements.

Explication : les caisses automatiques sont des outils qui soutiennent des Valeurs Métier comme le service client ou la gestion des ventes, mais elles ne sont pas une Valeur Métier en elles-mêmes.

Site web de commande en ligne pour les clients.

Explication : le site web est un outil facilitant des Valeurs Métier telles que le service client ou les ventes, mais il n'est pas une activité ou un service central.

Rançongiciel entraînant l'interruption des services.

Explication : il s'agit d'une menace ou d'un incident potentiel qui affecte une Valeur Métier, mais ce n'est pas une Valeur Métier.

Pare-feu pour protéger les connexions réseau.

Explication : le pare-feu est un équipement de protection technique, mais pas une activité critique ou un service.

Réponse : Service client pour gérer les commandes et réclamations.

Explication : le service client est un levier clé pour fidéliser les clients et maintenir une bonne réputation. Répondre efficacement aux commandes et aux réclamations est essentiel pour assurer la satisfaction client et, par conséquent, le succès commercial.

Administrateur des équipements numériques.

Explication : les fournisseurs jouent un rôle de soutien, mais ils ne représentent pas une activité stratégique de l'entreprise.

Accès non autorisé aux données sensibles par un pirate informatique.

Explication : cela représente une menace pour la sécurité des Valeurs Métier, mais ce n'est pas une activité ou un service.

Module 5 : événements rédoutés, impacts et gravité.

Vidéo 5 : Explication des Biens Support et leurs relations avec les Valeurs Métier

Comprendre les biens supports, c'est comprendre les fondations technologiques qui soutiennent les valeurs métiers, activités essentielles de votre organisation.

Les biens supports sont les composants matériels technologiques, infrastructures ou humains, personnes qui soutiennent directement les valeurs métiers de votre organisation.

Exemple : Dans une organisation, les biens supports peuvent être variés, par exemple :

1. les serveurs qui hébergent vos applications de gestion ;
2. les réseaux internes qui connectent les équipements et utilisateurs ;
3. les administrateurs qui supervisent l'informatique.

Pour identifier les biens supports, pensez à tous les éléments qui permettent à vos valeurs métiers de s'accomplir.

Quels sont les composants qui soutiennent les activités clés de votre organisation ?

Il s'agit de tout ce qui est en coulisse et rendent possible les opérations que vous souhaitez protéger.

Exemple d'un supermarché connecté : Les biens supports incluent les réseaux wifi internes qui connectent les caisses enregistreuses, les serveurs qui gèrent les stocks et les commandes,

les logiciels de gestion de paiement et de préparation de commandes. Sans ces biens supports, l'ensemble des services clients seraient impactés.

N'oubliez pas, les biens supports constituent les piliers technologiques et humains de votre entreprise. En les identifiant et en les protégeant, vous assurer la stabilité, la sécurité, la résilience de vos valeurs métiers.

EXERCICE 3 : Définir un Bien Support

Question : Quelle est la meilleure définition d'un Bien Support ?

Un ensemble de mesures de sécurité mises en place pour protéger les systèmes de l'entreprise.

Explication : les mesures de sécurité protègent les Biens Support et les Valeurs Métier, mais elles ne sont pas des Biens Support.

Réponse : Une infrastructure matérielle, logicielle ou humaine qui soutient directement les Valeurs Métier d'une organisation.

Explication : les Biens Support incluent les équipements, logiciels, et ressources humaines indispensables au fonctionnement des Valeurs Métier.

une menace pouvant affecter les activités critiques de l'entreprise.

Explication : Les menaces potentielles ciblent des Valeurs Métier.

une activité ou un service qui contribue directement au succès de l'entreprise.

Explication : Cela décrit une Valeur Métier, pas un Bien Support.

EXERCICE 4 : Identifier les Biens Support de la boulangerie connectée

<u>Question</u> : Parmi les propositions suivantes, cochez uniquement les Biens Support. Plusieurs réponses possibles.

Réponse : Serveur de base de données

Explication: le serveur est une infrastructure essentielle qui soutient les Valeurs Métier en hébergeant des données critiques nécessaires aux opérations.

Gestion des stocks via une IA pour éviter les ruptures

Explication: c'est une Valeur Métier. Il s'agit d'une activité centrale et stratégique, pas d'un support technique ou infrastructurel.

Réponse : Pare-feu pour protéger les connexions réseau

Explication: le pare-feu protège les systèmes et assure la continuité des Valeurs Métier en sécurisant les connexions réseau.

Confidentialité des informations clients

Explication: c'est un besoin de sécurité. Ce n'est pas un Bien Support mais un principe appliqué pour protéger les Valeurs Métier et Biens Support.

Réponse : Site web de commande en ligne pour les clients

Explication: le site web facilite le service client, une Valeur Métier essentielle. Il est donc un support technique indispensable.

Service client pour gérer les commandes et réclamations

Explication: c'est une Valeur Métier. Le service client est une activité clé et non une infrastructure ou un outil de soutien.

Réponse : Administrateur des équipements numériques

Explication: les fournisseurs assurent la disponibilité des outils nécessaires aux Valeurs Métier, comme les caisses automatiques ou les serveurs.

Réponse : Réseau interne permettant la connexion des équipements

Explication : le réseau est une infrastructure clé permettant aux Valeurs Métier, comme la gestion des stocks ou les paiements, de fonctionner correctement.

Accès non autorisé aux données sensibles par un pirate informatique

Explication : c'est un Événement Redouté (à voir dans le prochain module). Il s'agit d'une menace ou d'un incident potentiel, pas d'un Bien Support.

Réponse : Caisses automatiques pour faciliter les paiements

Explication : ces caisses soutiennent directement le service client, une Valeur Métier essentielle, en facilitant les paiements rapides et efficaces.

Vidéo 6 : Explication des événements redoutés et leur impact potentiel sur les Valeurs Métier

Dans cette partie, nous allons explorer un concept clé de la gestion des risques et des événements redoutés. Prédire et identifier les événements redoutés, c'est identifier les impacts potentiels qui peuvent affecter les valeurs métiers de votre organisation.

Les événements redoutés sont des incidents, des attaques qui s'ils se produisent, ont un impact négatif sur les valeurs métiers de votre organisation. Ils représentent ce que vous souhaiterez éviter à tout prix : les interruptions de service qui seraient une atteinte au besoin de disponibilité, des pertes de ou des modifications légitimes de données qui seraient une atteinte aux besoins d'intégrité ou encore une divulgation des informations sensibles qui seraient des atteintes aux besoins de confidentialité.

Exemple : Imaginer que plus aucun client ne puisse faire de commandes sur votre site, le service est à l'arrêt complet.

Résultat un manque de gagner d'1 million d'euros.

Là, on est clairement face à un problème de disponibilité.

Autre situation, les prix affichés sur votre site sont faux. C'est peut-être une erreur technique ou manipulation malveillante mais dans tous les cas, ça vous coûte très cher. 100 millions d'euro perdus en une journée, ici c'est l'intégrité des données qui est compromise.

Et enfin un cas classique mais très sensibles, le vol de données clients : les données carte bancaire par exemple comme d'autres données à caractères personnels. En plus du risque juridique avec la possible sanction de la part de la CNIL, cela peut nuire gravement la réputation de l'entreprise : là on touche à la confidentialité.

Chaque événement redouté a fait directement une ou plusieurs valeurs métiers que vous avez identifiées comme essentielles pour votre organisation.

Si votre entreprise repose sur un système de gestion de la commande en ligne (qui est une valeur métier), qui ne serait plus accessible, cela pourrait non seulement stopper vos ventes mais nuire à l'image de votre entreprise.

Identifier les événements redoutés vous permet de mettre en évidence les craintes métiers liés aux périmètres étudiés.

À partir de la liste des valeurs métiers essentiels que vous avez identifiées, réfléchissez maintenant aux événements qui pourraient impactés la **disponibilité, l'intégrité et la confidentialité** de ces valeurs métiers.

Posez-vous la question : quel est l'événement le plus grave qui pourrait arriver sur ces valeurs métiers ou qu'est-ce qui> m'empêche de dormir la nuit, qu'est-ce qui me fait faire des cauchemars ?

Exemple : Une entreprise qui gère une plateforme de vente en ligne. L'un des événements redoutés pourrait être : une perte de disponibilité du site marchant pendant plusieurs heures. L'impact qu'il y a est de nature financière mais aussi il y a des effets secondaires de natures réputationnelles engendrant une perte de confiance des clients et donc de sa part de marché.

Ces impacts montrent à quels points il est crucial d'identifier et de se préparer à ces événements.

Comme vous l'avez compris, les événements redoutés peuvent entrainer des impacts de différentes natures, qui peuvent compromettre les succès de votre mission.

Il est donc essentiel d'évaluer leur impact potentiel en s'appuyant sur une échelle de gravité mesurant les effets les plus critiques. Cette évaluation permet ensuite de déterminer la sévérité des risques associés. Autrement dit, si l'impact d'un événement redouté est sous-estimé ou négligé, les risques qui seront associés sur un papier auront une faible gravité et les potentielles mesures de traitement de ces risques seront dépriorisées ou tout simplement ignorées. Cette analyse doit être menée par des responsable métiers et des décideurs. Elle ne

nécessite aucune connaissance technique mais par contre une très bonne maîtrise des enjeux liés aux missions de la cible à étudier.

Nous avons vu comment ces événements qu'ils s'agissent d'une fuite de données, d'une indisponibilité ou d'une altération d'information peuvent avoir des conséquences directes sur les valeurs métiers comme la **confidentialité, la continuité de service ou la fiabilité des informations.**

Perspectives : prochaine vidéo sur la notion de gravité, quels critères à prendre en compte et comment hiérarchiser les risques en fonction de leur impact réel ?

Vidéo 7 : Estimer la gravité des événements redoutés : un des éléments clés de la gestion des risques

La gravité est l'évaluation de l'impact d'un événement redouté, la gravité traduit le niveau et l'intensité des effets d'un risque. Pour une analyse de risque, la gravité est déterminée par une échelle propre à chaque organisation. L'estimation de la gravité peut se faire sur une échelle allant de 1 à 4 :

1. Le niveau 1 n'affecte pas ou peu la valeur métier à protéger ;
2. Le niveau 2 n'aurait qu'un impact significatif ;
3. Le niveau 3 aurait un impact grave altérant les performances globales des activités du système d'information ;
4. Le niveau 4 serait à même de mettre en péril l'organisation ou des ressources humaines ;

Imaginer un service d'achat en ligne devient indisponible pendant plusieurs jours. En fonction des conséquences pour l'organisation, ces scénarios entraineraient donc une estimation de gravité de 4. En estimant la gravité des événements redoutés, vous serez en mesure de les prioriser et d'aboutir à une gestion des risques efficaces.

N'oubliez évidemment pas d'adapter cette estimation à la nature spécifique de vos valeurs métiers et aux exigences de votre organisation.

EXERCICE 5 : Identifier les événements redoutés - V2

Objectif : Évaluer la capacité des apprenants à distinguer les Événements Redoutés des autres éléments (Valeurs Métier, Biens Support, incidents mineurs, etc.).

L'accès aux données critiques de l'entreprise est bloqué à la suite d'une attaque par rançongiciel.

ER

Explication : cela impacte directement les Valeurs Métier (disponibilité des données) et représente un risque majeur.

Une panne temporaire du Wi-Fi dans un bureau qui n'impacte pas les activités principales.

NON ER

Explication : impact limité, n'affecte pas directement les Valeurs Métier. Le wi-fi est un Bien Support. Un ER aurait été formulé ainsi : « Il n'est pas possible de se connecter à Internet à partir d'un bureau »

Une fuite des données personnelles des clients après une cyberattaque.

ER

Explication : atteinte à la confidentialité des données personnelles, qui est une composante critique des Valeurs Métier.

La mise à jour planifiée d'un logiciel interne.

NON ER

Explication : ce n'est pas une menace ou un incident ; il s'agit d'une activité normale.

Une indisponibilité complète du site de commande en ligne pendant 48 heures.

ER

Explication : affecte directement la continuité des activités et la disponibilité des Valeurs Métier.

Le remplacement d'un employé technique dans l'équipe de support.

NON ER

Explication : bien que cela puisse avoir un impact organisationnel, ce n'est pas une menace ou un incident critique.

Un hacker accède illégalement à la base de données clients.

Explication : La source de risque est identifiée comme étant un hacker, or un événement redouté ne doit pas contenir de sources de risque. D'autre part, la conséquence de l'accès illégitime n'est pas identifiée dans la phrase.

NON ER

La perte d'une commande de faible valeur en raison d'une erreur humaine.

ER

Explication : impact négligeable, mais reste un événement redouté.

EXERCICE 6 : Identifier les impacts associés aux événements redoutés de la boulangerie connectée

Objectif : Classifier les impacts (juridique, financier, réputation, opérationnel) associés aux

Événements Redoutés d'une boulangerie connectée.

Instructions :

Pour chaque Événement Redouté ci-dessous, cochez les types d'impact associés parmi

les suivants :

- Juridique
- Financier
- Réputation
- Opérationnel

Certains Événements Redoutés peuvent avoir plusieurs impacts.

Scénarios de la boulangerie connectée :

Une cyberattaque expose les données personnelles des clients inscrits au programme de fidélité. (cocher 3 réponses)

Réponse : Juridique

Explication : une violation de données peut entraîner des sanctions juridiques (RGPD), des pertes financières (indemnisation, réparations), et nuire à la confiance des clients.

Réponse : Financier

Réponse : Réputation

Opérationnel

Une panne des caisses automatiques empêche les clients de régler leurs achats pendant une journée. (Cocher 3 réponses)

Juridique

Réponse : Financier

Explication : la panne entraîne des pertes de revenus (impossibilité d'encaisser), perturbe les opérations, et nuit à l'image de fiabilité auprès des clients.

Réponse : Réputation

Réponse : Opérationnel

Le site de commande en ligne est inaccessible pendant le week-end. (cocher 3 réponses)

Juridique

Réponse : Financier

Explication : l'indisponibilité réduit les ventes en ligne, complique la gestion interne, et affecte la satisfaction client.

Réponse : Réputation

Réponse : Opérationnel

Une corruption des recettes stockées dans le système du four numérique entraîne des erreurs dans les cuissons. (Cocher 2 réponses)

Juridique

Réponse : Financier

Explication : les erreurs dans les cuissons entraînent des pertes de produits et perturbent la production.

Réputation

Réponse : Opérationnel

Explication : les erreurs dans les cuissons entraînent des pertes de produits et perturbent la production.

Module 6 : Sources de Risques et Objectifs visés

Vidéo 8 : Comment identifier les Sources de Risque et les Objectifs visés ?

Deux éléments essentiels dans l'analyse de risque cyber, comprendre ces concepts vous permettra d'anticiper qui pourrait menacer votre organisation et pourquoi. Une source de risque est un des éléments déclencheur à l'origine des risques. Elle peut inclure des personnes, des groupes internes ou externes comme des hackeurs, des concurrents ou même une erreur humaine. Identifier ces sources vous aide à comprendre d'où peuvent venir les dangers. Dans le cas d'une attaque, les motivations de la source de risque sont appelées **objectifs visés.** Il s'agit de ce que cherche à obtenir les sources de risque en compromettant votre système. Cela peut inclure le vol des données, l'interruption de service, le sabotage ou encore l'extorsion financière. Par exemple, un hackeur, source de risque, peut cibler votre entreprise dans le but de voler des informations confidentielles, objectifs visés. Tandis qu'un concurrent malveillant pourrait chercher à perturber vos opérations pour gagner un avantage sur le marché. Chaque source de risque a une intension spécifique et c'est en comprenant ces intentions que vous pourrez anticiper les actions possibles.

Comment identifier les sources de risques et objectifs visés ?

Pour identifier les sources de risques, commencer par examiner les acteurs qui pourraient avoir un intérêt à compromettre vos valeurs métiers. Ensuite, analyser ce qu'il cherche à

atteindre : quelles sont leurs motivations, est-ce qu'elles peuvent causer des dommages financiers, accéder à des données sensibles ou déstabiliser votre organisation. Ces questions vous guideront vers une identification des sources de risques et les objectifs visés. Pour vous aider à déterminer les motivations et bénéfices éventuelles recherchées, les sources de risques peuvent être utiles pour reprendre les événements redoutés précédemment identifiés.

Exemple concret : Prenons l'exemple d'une entreprise technologie innovante, le couple sources de risque et objectifs visés pourrait être :

1. Des concurrents cherchant à voler des secrets industriels pour copier leurs produits ;
2. Des cybercriminels cherchant à dérober des données client dans le but de revendre dans un marché parallèle.

N.B. : Les sources de risques, les objectifs visés forment la base de toute menace.

Vous identifiez alors les sources de risques et objectifs de l'étude doivent faire face à l'éventualité d'une attaque conduite par ces sources de risques, objectifs visés.

EXERCICE 7 : Identifiez si chaque élément correspond à une Source de Risque et/ou à un Objectif Visé

Instructions :

Parmi les propositions suivantes, identifiez si chaque élément correspond à une Source de Risque et/ou à un Objectif Visé.

Un groupe de hackers tentant d'accéder aux données personnelles des clients.

Réponse : SR

Explication : une SR est une entité ou un acteur malveillant ayant une intention nuisible. Exploiter des données volées pour lancer une campagne de phishing.

OV

SR/OV

Voler des données clients pour lancer une campagne de phishing.

SR

Réponse : OV

Explication : un OV est l'objectif recherché par une SR, ici l'utilisation des données volées pour une attaque.

SR/OV

Un concurrent cherchant à espionner les projets de la boulangerie.

SR

OV

Réponse : SR/OV

Explication : une SR peut inclure une entité externe ayant un intérêt à nuire ou tirer profit d'une faiblesse.

Saboter les fours numériques pour ralentir la production.

SR

Réponse : OV

Explication : ralentir la production est un objectif visé par une SR.

SR/OV

Un employé mécontent et ayant des accès privilégiés aux données confidentielles souhaite les revendre sur Internet.

SR

OV

Réponse : SR/OV

Explication : un employé interne malveillant est une Source de Risque.

Perturber les commandes en ligne pour affecter les ventes.

SR

Réponse : OV

Explication : affecter les ventes est un objectif visé par une SR exploitant une opportunité.

SR/OV

EXERCICE 8 : Identifier les Objectifs Visés dans une boulangerie connectée

Instructions :

Identifier les Objectifs Visés dans une boulangerie connectée

Question : Parmi les propositions suivantes, cochez uniquement les Objectifs Visés.

Parmi les propositions suivantes, cochez uniquement les Objectifs Visés.

Réponse : Voler les recettes exclusives de la boulangerie pour les reproduire ailleurs.

Explication : un objectif typique d'une Source de Risque cherchant un avantage compétitif.

Réponse : Saboter le fonctionnement des fours numériques pour ralentir la production.

Explication : l’objectif ici est de perturber la production, ce qui impacte directement les opérations.

Revendre les données personnelles des clients à des tiers.

Explication : La revente des données personnelles est un objectif indirect. L'objectif visé devrait être l'exfiltration des données personnelles.

Permettre à un employé non autorisé d'accéder au système des commandes.

Explication : c’est une opportunité. Cela facilite l’atteinte d’un objectif, mais ce n’est pas un Objectif visé en soi.

Réponse : Réaliser des campagnes de phishing avec les informations clients volées.

Explication : les informations volées sont utilisées pour atteindre cet objectif malveillant.

Module 7 : Scénarios Stratégiques et Parties Prenantes

Vidéo 9 : Rôles des Parties Prenantes et des interactions dans les systèmes

Dans cette vidéo, il est question d’explorer le rôle des parties prenantes et comprendre comment leurs interactions peuvent influencer les systèmes des périmètres étudiés.

L’objet est d’identifier en quoi les parties prenantes représentent un vecteur d’attaque que les sources de risques peuvent utiliser pour atteindre leurs objectifs visés. L’ensemble des parties prenantes forment l’écosystème, c’est-à-dire **les personnes, groupes ou entités** et leurs systèmes qui sont en relation avec l’objet de l’étude. Les parties prenantes peuvent être internes comme **les employés tels les dirigeants, les équipes IT** ou externes comme **les clients, les fournisseurs, les prestataires, les partenaires ou même les régulateurs.** Chaque partie prenante peut avoir un rôle et des interactions spécifiques avec le système étudié. Elles peuvent prendre différentes formes : utilisation directe des logiciels internes, accès aux données, gestion de processus critiques ou collaboration via des plateformes partagées.

Dans une organisation, les parties prenantes peuvent être variées. Par exemple **les employés** qui utilisent le système peuvent être abusés pour produire une action illégitime ou l’organisation d’un fournisseur en charge de la maintenance peut être compromise et propagée à un rançongiciel sur le système objet de l’étude.

Exemple concret : Imaginons une entreprise de service financier, les parties prenantes inclues les clients qui utilisent les applications mobiles pour gérer leur compte, les employés qui traitent les transactions, les administrateurs et les partenaires technologiques qui fournissent des services d’infrastructures.

Chacune de ses parties prenantes est une surface d’exposition exploitable par des sources de risques. Ce qui constitue un danger pour le système à étudier.

Les parties prenantes et leur interaction avec l'objet de l'étude constitue un danger potentiel. Une interaction mal contrôlée ou une partie prenante non identifiée peut constituer un vecteur d'attaque et introduire un risque important comme les accès non autorisés et des fuites de données sensibles. En connaissant bien vos parties prenantes, vous pouvez mieux anticiper les risques et protéger vos systèmes. L'idée est d'évaluer le niveau de dangerosité des parties prenantes. Ce niveau traduit le degré de faiblesse de la partie prenante exploitable par une source de risque. Un scénario stratégique représente les différents chemins d'attaques possibles qu'une source de risque peut prendre vers une ou plusieurs valeurs métiers. Ces chemins sont directs : source de risque vers le système ou indirect en passant par les parties prenantes.

EXERCICE 9 : Définir une Partie Prenante

Quelle est la meilleure définition d'une Partie Prenante ?

Réponse : Un élément (personne, système d'information, organisation, ou source de risque) en interaction directe ou indirecte avec l'objet de l'étude.

Explication : les Parties Prenantes incluent toutes les entités ayant un intérêt ou une influence sur les activités, décisions ou résultats d'une organisation.

Une entité externe cherchant à nuire à l'entreprise.

Explication : la Partie prenante doit être vue comme un vecteur d'attaque mais pas comme une origine de l'attaque, qui est définie dans la méthode comme une Source de Risque.

Un ensemble de règles régissant les relations entre les employés d'une organisation.

Explication : cela décrit une politique interne, pas une Partie prenante.

Un outil technologique essentiel pour atteindre les objectifs d'une organisation.

Explication : cela correspond à un Bien Support, pas à une partie prenante.

EXERCICE 10 : Scénarios Stratégiques

Quels sont les Scénarios Stratégiques valides dans le cadre de la cybersécurité ? Cochez toutes les réponses valides.

Réponse : Un fournisseur de services d'infrastructure est compromis par des cybercriminels, menaçant la disponibilité des services financiers. Chemin d'Attaque : Indirect (via le fournisseur).

Explication : un fournisseur de services d'infrastructure (partie prenante) compromis par des cybercriminels (source de risque) menace la disponibilité des services financiers (valeur métier).

Réponse : Des employés sont dupés par des cybercriminels, compromettant l'intégrité des données sensibles. Chemin d'Attaque : Indirect (via les employés).

Explication : des employés trompés (partie prenante) par des hacktivistes mécontents (source de risque) compromettent l'intégrité des données sensibles (valeur métier).

Réponse : Un employé mécontent partage des informations sensibles avec des concurrents, menaçant la confidentialité des informations stratégiques. Chemin d'Attaque : Direct.

Explication : un employé mécontent (source de risque) partageant des informations sensibles (valeur métier) avec des concurrents menace la confidentialité des informations stratégiques (valeur métier).

Des employés utilisent des logiciels non autorisés, menaçant la conformité aux politiques internes. Chemin d'Attaque : Direct (via les employés).

Explication : l'utilisation de logiciels non autorisés est une menace, ce n'est pas un scénario stratégique typique. Il manque une valeur métier.

Réponse : Un collégien (source de risque) compromet le service WEB du collège pour modifier ses notes (valeur métier). Chemin d'Attaque : Direct.

Explication : le collégien (source de risque) attaque directement le système (valeur métier).

EXERCICE 11 : Identifier les Parties Prenantes dans une boulangerie connectée

Parmi les propositions suivantes, cochez uniquement les Parties Prenantes. Plusieurs réponses possibles.

Réponse : Les clients qui utilisent le site de commande en ligne de la boulangerie.

Explication : les clients sont des Parties Prenantes clés, car ils consomment les produits et influencent la satisfaction et les revenus.

Réponse : Les fournisseurs de farine et autres matières premières.

Explication : les fournisseurs sont des Parties Prenantes externes indispensables à la production.

Les hackers cherchant à accéder aux données clients.

Explication : c’est une Source de Risque. Ils ne participent pas aux objectifs de l’organisation.

Les concurrents cherchant à espionner les recettes exclusives.

Explication : c’est une Source de Risque. Ils agissent contre les intérêts de l’organisation.

Module 8 : Scénarios opérationnels et la vraisemblance

Vidéo 10 : Scénarios Opérationnels et leur influence sur la gestion des risques

L'objectif ici est d'imaginer des situations réalistes encrées dans votre contexte et en évaluer la vraisemblance. Cette étape permet de prioriser les risques de manière pertinente en tenant compte à la fois de leur gravité er de leur probabilité d'occurrence.

Qu'est-ce qu'un Scénario Opérationnel ?

C'est anticiper les actions malveillantes, les menaces potentielles et les vulnérabilités qui peuvent affecter votre système.

Les Scénarios Opérationnels représentent des différentes manières dont une attaque où un incident pourrait se dérouler en tenant compte des actions, des méthodes et des vecteurs utilisés par des attaquants. Ceci décrit l'enseignement des actions depuis l'intrusion initiale jusqu'à l'impact final sur les systèmes et les valeurs métiers de votre organisation.

Le Scénario décrit une action via une partie prenante ou bien directement chez l'organisation.

Exemple : Un concurrent vole des travaux de recherches en créant un canal de filtration de données portant sur directement sur les systèmes d'information de la RND par l'utilisation d'une attaque de harponnage qui a permis de déposer une porte dérobée sur le PC d'un chercheur non mis à jour. Les **Scénarios Opérationnels** sont essentiels, qu'ils permettent de modéliser les attaques possibles et de comprendre comment les menaces peuvent se concrétiser. En identifiant les Scénarios Opérationnels les plus probables, vous pouvez anticiper les points faibles de votre système et prioriser vos efforts de sécurisation.

Les Scénarios Opérationnels servent de guide pour mettre en place des mesures de protections spécifiques et adaptées. Nous pouvons estimer la faisabilité ou bien la probabilité qu'un risque se réalise selon l'échelle pour chaque **Scénario Opérationnel** étudié. L'estimation de la vraisemblance peut se faire sur une échelle de **1, 2, 3** ou **4**.

a. **1** signifie que l'événement est peu vraisemblable ;
b. **2** indique une relation de vraisemblance modérée ;
c. **3** correspond à la vraisemblance élevée ;
d. **4** désigne une vraisemblance très élevée.

Par exemple si un attaquant dispose de ressources suffisantes et que les vulnérabilités présentes sont bien connues, la vraisemblance d'exploitation de ce **Scénario Opérationnel** pourrait être soumise à **v3** ou **vraisemblance v4.**

L'estimation de la vraisemblance permet de déterminer le degré de faisabilité des **Scénarios Opérationnels** et de prioriser les actions de sécurité en conséquence.

N'oubliez pas la représentation des attaques sous forme de **Scénario Opérationnel** est utile pour comprendre les actions malveillantes qui pourraient être commises sur votre système. En les intégrant dans votre gestion des risques, vous pouvez élaborer des réponses efficaces pour protéger vos **Valeurs Métiers.**

EXERCICE 12 : Comprendre les Scénarios Opérationnels

Qu’est-ce qu’un Scénario Opérationnel ? Cochez la meilleure réponse.

Une description d’un événement futur sans lien avec les risques existants.

Explication : les Scénarios Opérationnels sont liés aux risques identifiés et non à des événements hypothétiques isolés.

Réponse : Une situation où une Source de Risque réalise une suite d’actions pour atteindre un Objectif Visé.

Explication : un Scénario Opérationnel relie une Source de Risque, une suite d’actions et un Objectif visé dans un scénario concret.

Une liste des équipements nécessaires à la gestion des risques dans une organisation.

Explication : cela correspond aux Biens Supports, pas aux Scénarios Opérationnels.

Une mesure technique mise en place pour empêcher une Source de Risque d’agir.

Explication : cela décrit une mesure de sécurité, pas un Scénario Opérationnel.

EXERCICE 13 : Évaluer la vraisemblance des Scénarios Opérationnels de la Boulangerie connectée

Un hacker accède au site de commande en ligne en exploitant une vulnérabilité logicielle pour voler des données clients.

Réponse : 1

Explication : Le site est exposé sur Internet. Il est vulnérable à la moindre faille technique présente sur le site. L’attaquant peut agir en toute impunité sans risquer d’être identifié.

2

3

4

Un concurrent sabote le tableau électrique de la boulangerie pour empêcher les fours numériques de fonctionner pendant 24 heures.

1

2

3

Réponse : 4

Explication : L’attaque est physique. Elle nécessitera un accès physique par l’attaquant, ce qui en général fait courir plus de risque à l’attaquant. Le scénario est donc moins probable.

Un concurrent accède physiquement au PC d'un employé pour extraire les processus de production et reproduire des produits similaires.

1

2

Réponse : 3

Explication : Les moyens que le concurrent devra employer sont importants, car il devra s'introduire dans le PC de l'employé, trouver les éléments qui ne sont pas forcément sur le PC.

4

Par vengeance, un employé désactive le système de commandes en ligne après s'être introduit dans l'interface administrateur.

1

Réponse : 2

Explication : Si les employés veulent se venger, ils pourraient commettre des actes bien plus graves. Désactiver le site, par exemple, laisserait des traces numériques qui les impliqueraient directement et les exposeraient à des poursuites judiciaires.

3

4

Module 9 : Évaluer les risques et les mesures

Vidéo 11 : Synthèse des risques (Etape cruciale de toute méthode d'analyse de risque).

Vue globale des risques pour faciliter la prise de décision.

La **synthèse des risques** permet d'agréger l'ensemble des scénarios et de présenter une vue globale des risques pour faciliter la prise de décision.

La **synthèse des risques** est une vue consolidée des scénarios étudiés dans les ateliers précédents. L'objectif est de pouvoir présenter de manière synthétique l'ensemble des risques et de faire ressortir les plus pratiques.

Comment calculer le niveau de risque ?

Le niveau de risque est déterminé par la combinaison de deux facteurs la gravité des impacts et la vraisemblance des **Scénarios Opérationnels** associés.

Exemple : Prenons l'exemple d'un scénario avec lequel une source de risque vise à perturber un service critique de votre organisation. La gravité des impacts est estimée à un **niveau 4** et la vraisemblance à un **niveau 3**. Par exemple la criticité d'un risque peut être classée en trois niveaux faibles**,** les risques peuvent être acceptés tels quels avec des mesures de base,

modérer des mesures de sécurité doivent être envisagées mais le risque peut être toléré, élevé, une intervention rapide et nécessaire pour atténuer le risque. Ce système de priorisation vous aide à allouer vos ressources de manière efficace en vous concentrant d'abord sur les risques les plus critiques. Cet arbitrage doit être pris en compte par la direction en fonction des objectifs stratégiques de votre organisation.

La **synthèse des risques** vous fournit une vue d'ensemble pour identifier, prioriser les risques et définir un plan d'action à d'autre. Comme nous allons voir dans la prochaine séquence, vous pourrez décider quelles mesures de réduction de risques doivent être mises en œuvre.

Vidéo 12 : Les mesures de sécurité

Comprendre les mesures, c'est de savoir comment protéger vos systèmes, vos données et vos **Valeurs Métiers** contre les menaces identifiées.

Qu'est-ce qu'une mesure de sécurité ?

Les mesures de sécurité sont des actions, des dispositifs ou des processus mis en place pour réduire les risques identifiés et protéger les **Valeurs Métiers** de votre organisation. Elles peuvent prévenir les risques, les détecter ou bien les corriger selon leur rôle dans la stratégie de défense.

L'objectif des mesures est de réduire les risques et de renforcer la résilience de vos systèmes.

Les **mesures** peuvent prendre diverses formes :

1. Un pare-feu **(firewall)** sert de barrière pour contrôler les entrées et les sorties du réseau et empêcher les intrusions ;
2. L'authentification multi facteurs ajoutent une couche de protection supplémentaire en vérifiant l'identité des utilisateurs avec plusieurs étapes, les sauvegardes régulières permettent rapidement de récupérer les données en cas de perte ou de corruption.

Les mesures jouent un rôle central dans la gestion des risques en offrant des protections adaptées aux risques identifiés. Elles contribuent à réduire les vulnérabilités, à rajouter les obstacles sur le chemin de l'attaquant et à détecter les incidents en temps réel ainsi qu'à anticiper les conséquences d'une attaque mieux réagir.

Exemple concret : Imaginons une entreprise utilisant un système de gestion en ligne pour ses opérations. Pour se protéger des attaques par forces brutes, elle imprimante l'authentification multi facteurs. Ce qui rend l'accès plus sécurisé même si un mot de passe est compromis. Cette authentification réduit efficacement le risque d'intrusion et protège l'accès au système d'information de l'organisation.

N.B. : Les mesures de sécurité sont la clé pour réduire les risques à un niveau acceptable. En choisissant et en implémentant des mesures adaptées, vous renforcez la sécurité de votre organisation et protéger vos **Valeurs Métiers.**

EXERCICE 14 : Associer les mesures aux risques

Risque : Un hacker accède au site pour voler les données client en exploitant une vulnérabilité logicielle du site.

Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

Attribuer les bons droits sur les ressources sensibles du système d'information

Cloisonner les services visibles depuis Internet du reste du système d'information

Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

Réponse : Définir une politique de mise à jour des composants du système d'information

Explication : la mise à jour des logiciels diminue le nombre de vulnérabilités

Définir et appliquer une politique de sauvegarde des composants critiques

Risque : Le concurrent sabote le tableau électrique.

Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

Attribuer les bons droits sur les ressources sensibles du système d'information

Cloisonner les services visibles depuis Internet du reste du système d'information

Réponse : Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

Explication : une gestion rigoureuse des accès physiques limite ou empêche la manipulation des équipements.

Définir une politique de mise à jour des composants du système d'information

Définir et appliquer une politique de sauvegarde des composants critiques

Risque : Un concurrent accède physiquement au PC du Boulanger pour voler les recettes.

Réponse : Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

Explication : sensibiliser le boulanger pour qu'il utilise un mot de passe suffisamment robuste pour ne pas être trop facilement compromis

Attribuer les bons droits sur les ressources sensibles du système d'information

Cloisonner les services visibles depuis Internet du reste du système d'information

Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

Définir une politique de mise à jour des composants du système d'information

Définir et appliquer une politique de sauvegarde des composants critiques

Risque : Un employé se venge en limitant le nombre de commandes.

Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

Réponse : Attribuer les bons droits sur les ressources sensibles du système d'information

Explication : les droits d'accès à la base des commandes doivent être limités

Cloisonner les services visibles depuis Internet du reste du système d'information

Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

Définir une politique de mise à jour des composants du système d'information

Définir et appliquer une politique de sauvegarde des composants critiques.

EXERCICE 15 : Définir une mesure de sécurité

Quelle est la meilleure définition d'une Mesure de Sécurité ?

Réponse : Une action ou une solution mise en place pour réduire, éliminer ou partager un risque.

Explication : une mesure de sécurité agit sur les risques identifiés pour en réduire la vraisemblance ou l'impact.

Un ensemble de règles définissant les objectifs stratégiques de l'organisation.

Explication : correspond à une politique ou une stratégie d'entreprise et non à une mesure de sécurité.

Un scénario où une Source de Risque exploite une opportunité pour atteindre un Objectif Visé.

Explication : décrit un Scénario Opérationnel et non une mesure de sécurité. Une entité externe cherchant à nuire à l'organisation.

Une entité externe cherchant à nuire à l'organisation.

Explication : correspond à une Source de Risque.

EXERCICE 16 : Identifier les mesures de sécurité pour une boulangerie connectée

Parmi les propositions suivantes, cochez uniquement les Mesures de Sécurité. Plusieurs réponses possibles.

Réponse : Configurer un pare-feu pour protéger le site de commande en ligne.

Explication : cette mesure réduit le risque d'intrusions malveillantes sur le site.

Réponse : Effectuer des sauvegardes régulières des recettes numériques.

Explication : une sauvegarde garantit la disponibilité des données critiques en cas de panne ou d'attaque.

Réponse : Former les employés à reconnaître les tentatives de phishing.

Explication : la sensibilisation réduit les risques liés aux erreurs humaines.

Voler les données clients d'une boulangerie concurrente.

Explication : c'est une action illégale ne réduisant pas un risque.

Réponse : Installer une solution anti-DDoS pour prévenir les attaques sur le site en ligne.

Explication : une solution anti-DDoS réduit l'impact des attaques sur la disponibilité du site.

Partager les recettes exclusives avec un concurrent pour négocier un partenariat.

Explication : c'est une action de stratégie commerciale qui ne réduit pas le risque.

Module 10 : Risques résiduels

Vidéo 13 : Évaluer les risques résiduels

Un risque résiduel est un scénario de risques qui persiste après la mise en ouvre des mesures de traitement. Il s'agit des risques qui ne peuvent être entièrement éliminés par l'application des mesures techniques, organisationnelles. Ils doivent être acceptés ou gérés de manière continue.

Exemple : Prenons l'exemple d'une organisation ayant renforcé la disponibilité d'un système critique par un système de secours sur le même site. Ces mesures réduisent le risque d'indisponibilité. Cependant dans le cadre d'un sinistre sur ce site, les deux systèmes seront indisponibles : ce qui constitue le risque résiduel.

Etapes pour évaluer les risques résiduels.

La question centrale est : la réduction des risques est-elle suffisante pour qu'ils soient acceptés ou des actions supplémentaires sont elles nécessaires et possibles. Dans certains cas bien qu'atténué, un risque peut subsister. Il est alors important de décider si ce risque peut être accepté en l'état et l'intégré dans une démarche de surveillance continue. Cette décision dépend des niveaux de tolérance aux risques de l'organisation. Le suivi du plan du traitement de risque doit être réalisé dans le temps. Sa mise à jour régulière participe aux processus d'amélioration continue du système, favorise l'élévation de maturité cyber de l'organisation et permet une gestion progressive des **risques résiduels.**

EXERCICE 17 : Définir un risque résiduel

Quelle est la meilleure définition d'un risque résiduel ?

Réponse : Un risque qui subsiste après traitement du risque.

Explication : scénario de risque subsistant après application de la stratégie de traitement du risque.

Un risque qui n'a pas été identifié lors de l'analyse initiale.

Explication : cela correspond à un risque non identifié ou latent, mais pas à un risque résiduel.

Une menace émergente qui n'a pas encore été évaluée.

Explication : une menace émergente peut accentuer le risque initial ou peut en générer un nouveau, mais elle ne constitue pas un risque résiduel sans une évaluation préalable.

Une faille technique ou organisationnelle exploitée par une Source de Risque.

Explication : cela décrit une opportunité de compromission ou une vulnérabilité, pas un risque résiduel.

EXERCICE 18 : Identifier les risques résiduels dans une boulangerie connectée

Parmi les propositions suivantes, cochez uniquement les Risques Résiduels. Plusieurs réponses possibles.

Une faille logicielle non corrigée dans le site de commande en ligne.

Explication : c'est une vulnérabilité existante. Tant que la faille n'est pas corrigée, ce n'est pas un risque résiduel mais un risque persistant.

Réponse : Des employés cliquent sur lien malveillant malgré une sensibilisation à la cybersécurité.

Explication : malgré la formation (mesure de sécurité), le facteur humain reste un risque résiduel difficile à éliminer totalement.

Réponse : Une attaque DDoS pouvant encore ralentir le site malgré la présence d'une solution anti-DDoS.

Explication : les solutions anti-DDoS réduisent l'impact mais ne l'éliminent pas totalement.

La perte des données clients en raison d'une absence de sauvegarde.

Explication : c'est un événement redouté non couvert. Il n'y a pas de mesure mise en place pour réduire ce risque.

Un concurrent utilisant les recettes exclusives divulguées par un ancien employé.

Explication : c'est une conséquence d'un scénario de risque insuffisamment géré. Ce n'est pas un risque résiduel si aucune mesure n'a été mise en place pour limiter cette fuite.

Un réseau interne vulnérable en raison de la désactivation accidentelle du pare-feu.

Explication : c'est une vulnérabilité non contrôlée. Il ne s'agit pas d'un risque résiduel car il résulte d'une absence de mesure.

Parfum de France :

Un laboratoire renomme international, situé à Grasse capitale mondiale du parfum. Cette entreprise, elle est l'artisanat traditionnel et la technologie moderne pour créer des parfums haute gamme destinés à des clients du monde entier. Le laboratoire repose sur plusieurs processus clés et infrastructure pour garantir la qualité et l'innovation de ses produits. Un

laboratoire de recherche et de développement ou des parfumeurs créent des fragrances exclusives, une ligne de production semi-automatisée utilisée pour fabriquer et conditionner les produits à grandes échelles, un site de commande en ligne permettant aux clients de commander des produits et de personnaliser certaines fragrances, un système de gestion numérique qui relie les stocks, les commandes en ligne et la production, un réseau informatique, internet sécurisé connectant les services industriels et les bureaux administratifs. Ce processus inclut **la création, la personnalisation des commandes clients** et **la production industrielle de parfum.**

L'infrastructure est composée de plusieurs réseaux tels que **le laboratoire, la ligne de production** et **le site de commande.**

La transformation numérique expose l'entreprise à divers risques des incidents récents mettent en lumière ces défis :

1. Une panne de réseau interne a interrompu la production pendant plusieurs heures retardant les expéditions ;
2. Une attaque de DDOS a bloqué le site de commande en ligne lors du lancement d'une nouvelle collection empêchant les clients d'accéder aux produits.
3. Une fuite d'information sensibles provoquée par un ancien employé a permis à un concurrent de copier des formules exclusives. Le responsable du laboratoire s'inquiète.

Mots du responsable : Ces problèmes ne sont pas seulement techniques, ils touchent directement nos opérations et notre réputation. Si les clients ne peuvent pas commander ou si nos produits sont copiés, cela pourrait avoir des conséquences graves sur notre marque. Nous devons aussi nous assurer que nos fournisseurs et partenaires respectent les normes de sécurité, car nous dépendront d'eux pour les matières premières et certains services critiques.

Ces incidents reflètent des situations fréquentes dans le secteur comme **les attaques ciblées** pour voler des données, **des perturbations des systèmes en ligne** ou **des sabotages de processus industriels.**