GUIDE MODERNCISO DES SERVICES MANAGÉS DE DÉTECTION ET DE RÉPONSES AUX MENACES (MDR)

KUDELSKI SECURITY

# Renforcer votre cyberrésilience

# Sommaire

# Résumé

**Si elles veulent être efficaces, les équipes de cybersécurité doivent d'abord devenir *efficientes*.**

Cela commence par une compréhension précise de leur mission et de leurs principaux objectifs. Une fois ceux-ci définis, l'efficience suivra. Le contexte des risques sera plus clair, ce qui permettra à votre équipe de sécurité de se concentrer sur les menaces les plus susceptibles de cibler votre entreprise. Votre équipe de réponse aux incidents pourra identifier ses priorités, et vous saurez dans quelles technologies vous devez investir.

Ce court guide pratique vous aidera à orienter votre réflexion. Il décrit les étapes à suivre pour définir vos priorités et accroître l'efficacité de votre programme.

# 1. Définir votre mission

**Prenez le temps de vous poser la question fondamentale suivante : quel est le principal but de votre équipe de sécurité à l'égard de l'entreprise ? Réfléchissez-y pour élaborer un énoncé de mission clair de votre programme de sécurité.**

Face aux innombrables tâches quotidiennes, projets annexes, missions ponctuelles et formalités administratives avec lesquels les groupes de sécurité doivent composer en permanence, il peut être difficile de déterminer la priorité n° 1.

Mais si vous ne le faites pas, votre équipe de sécurité risque d'être détournée de sa mission fondamentale.

La définition d'un énoncé de mission pour votre programme de cybersécurité aidera votre équipe à rester concentrée sur l'essentiel. En communiquant cet énoncé de mission aux différentes parties prenantes, vous leur permettrez de hiérarchiser correctement les objectifs de chacun et de se fixer des attentes appropriées. Enfin, la rédaction d'un énoncé de mission permettra de mieux protéger l'entreprise.

Comme tout énoncé de mission d'entreprise, votre énoncé de mission de cybersécurité doit refléter les objectifs de votre équipe. Que cherchez-vous à accomplir ?

Autrement dit : **quelle est votre raison d'être ?**

Un bon énoncé de mission doit développer les quatre points suivants :

01 La **principale fonction** de l'équipe de sécurité : qu'apportez-vous à l'entreprise dans son ensemble ? Indice : vous réduisez et gérez les risques tout en préservant les activités.

02 Vos **principaux clients** : pour qui votre équipe travaille-t-elle ?

03 Les **produits et services** qui génèrent la majeure partie des revenus de l'entreprise : que devez-vous protéger ?

04 Les **emplacements géographiques** où vous exercez vos activités : où allez-vous concentrer vos efforts ?

**Conseil : adaptez votre énoncé de mission à votre entreprise et au rôle de votre équipe de sécurité. Sinon, il risquerait de ne pas être pertinent. Il deviendra dès lors rapidement obsolète et finira par être ignoré.**

# 2. Aligner la mission sur les objectifs métier

**Assurez-vous que le programme et les priorités de votre équipe de sécurité sont alignés sur ceux de l'entreprise au sens large.**

Dans le pire des cas, votre entreprise n'a pas encore défini ni communiqué ses objectifs métier, ce qui signifie que chaque département finit par prendre une direction différente plutôt que d'adopter une approche cohérente et stratégique. La bonne nouvelle, c'est que vos questions peuvent aider la direction à mieux définir les objectifs de l'entreprise.

**Voici quelques questions qui peuvent favoriser l'identification des objectifs métier et l'alignement du programme de sécurité sur ceux-ci :**

| | |
|---|---|
| ✓ | Comment l'entreprise génère-t-elle des revenus ? |
| ✓ | Quelles sont les ressources physiques et numériques les plus précieuses de l'entreprise ? |
| ✓ | Quelles sont les principales cybermenaces qui ciblent l'entreprise ? |
| ✓ | Quelles sont les pratiques de l'entreprise qui peuvent la rendre vulnérable ? |
| ✓ | Quelle importance l'entreprise accorde-t-elle à la conformité ? |

**Réservez ces questions à l'équipe de sécurité :**

| | |
|---|---|
| ✓ | Comment pouvez-vous faire de la sécurité un catalyseur d'activités ? |
| ✓ | Quel type de culture essayez-vous d'instaurer au sein de votre équipe ? |
| ✓ | Qui sont les clients que vous essayez de protéger ? Quels types de ressources protégez-vous ? |
| ✓ | Quelles sont les limites et les capacités de votre programme de cybersécurité ? Comment se reflètent-elles dans les points forts et les faiblesses de votre équipe actuelle ? |

# 3. Traduire l'énoncé de mission en objectifs concrets

**Une fois que vous avez rédigé un énoncé de mission, vous êtes prêt à formuler des objectifs spécifiques qui vous permettront de concrétiser la mission de votre équipe de cybersécurité.**

Par exemple, si votre énoncé de mission est *« Protéger la société ABC en renforçant la sécurité de nos utilisateurs et de nos ressources critiques »*, vous pourriez définir les objectifs ci-dessous, en y joignant des deadlines et des chiffres spécifiques et mesurables afin de faciliter l'évaluation des progrès :

| | | | | |
|---|---|---|---|---|
| Adopter des normes de communication sécurisées qui protègent les intérêts des clients 01 | Élaborer et gérer un programme agile de réduction du risque 02 | Embaucher et/ou retenir des ressources de premier plan afin de se défendre contre les cybermenaces et de les neutraliser 03 | Identifier et neutraliser rapidement les menaces immédiates pour l'entreprise 04 | Innover afin de protéger et de renforcer le cœur de métier 05 |

**Conseil : quels que soient vos objectifs, ils doivent fournir une orientation claire à votre équipe de sécurité. Vous pouvez vous en servir comme d'une boussole pour vous guider lorsque des priorités concurrentes, des pressions externes ou les nouvelles tendances du marché menacent de vous faire dévier de la voie du succès.**

# 4. S'appuyer sur l'énoncé de mission pour hiérarchiser les menaces

**Vous devez vous appuyer sur votre énoncé de mission pour hiérarchiser les menaces sur lesquelles votre programme de sécurité doit se concentrer. Ce processus est complexe. Et si votre analyse était erronée et que vous passiez à côté d'informations essentielles ? Et si elle était incomplète ?**

Si la perfection n'existe pas en matière d'informations (ou de sécurité), de nombreux clients trouvent utile de commencer par poser les questions suivantes :

- **Quels incidents peuvent compromettre la capacité de l'entreprise à générer ou à percevoir des revenus ?**
- **Quels systèmes les cybercriminels sont-ils le plus susceptibles de cibler ? Sur quoi se concentreraient-ils ? Quelles étapes suivraient-ils ? Nous appelons ces étapes des « actions sur les objectifs ».**
- **Qu'est-ce qui permettrait à votre entreprise de poursuivre ses activités pendant un incident de sécurité majeur ?**
- **Quelles méthodologies les cybercriminels sont-ils le plus susceptibles d'employer au sein de votre environnement ?**
- **Sur quoi les équipes de réponse aux incidents doivent-elles se concentrer pour mieux identifier de telles activités ?**

Pour en savoir plus sur la lutte contre les menaces, lisez cet article sur le **blog ModernCISO**.

**Précision importante :**

Si bon nombre de responsables pensent disposer de fonctionnalités de détection des menaces supérieures à la moyenne, ils éprouvent pourtant des difficultés à déceler certaines menaces spécifiques :

| | | | | |
|---|---|---|---|---|
| 01 Piratage de la messagerie en entreprise | 02 Activités annonciatrices d'une attaque de ransomware (p. ex., reconnaissance ou déplacement latéral jusqu'aux outils de gestion informatique) | 03 Obtention d'un consentement illicite pour l'authentification | 04 Brute force ou collecte d'identifiants à partir d'endpoints compromis | 05 Utilisation d'identifiants compromis dans des services cloud |

Comment expliquer ces lacunes ? Elles découlent souvent d'une incompréhension des limites de l'environnement technologique, d'une incapacité à tirer parti ou à prendre conscience des pleines capacités des technologies, ou de l'absence de définition des menaces qui ciblent l'entreprise de manière à offrir une visibilité sur la sécurité et des exigences de détection claires.

**Dans une entreprise du classement Fortune 500 générant 10 milliards de dollars de chiffre d'affaires annuel et disposant d'un vaste environnement de sécurité, le responsable de la sécurité affirmait en toute confiance qu'il possédait d'excellentes fonctionnalités de détection. Pourtant, notre évaluation a révélé moins de 20 fonctionnalités de détection génériques offertes par leur plateforme SIEM, leur système de détection et d'intervention sur les endpoints (EDR) et d'autres outils. Dans la mesure où le programme n'avait pas identifié les menaces qui présentaient le plus grand risque pour l'entreprise, le responsable ignorait quelles fonctionnalités étaient les plus importantes et ne surveillait pas les menaces les plus dangereuses.**

Il n'est pas facile d'identifier les menaces les plus dangereuses qui pèsent sur l'entreprise. Cela requiert une compréhension approfondie de l'entreprise elle-même et du paysage des cybermenaces dans lequel elle évolue. Nous vous recommandons de dresser la liste des cinq principales menaces qui vous ciblent sur la base d'une modélisation détaillée propre à votre entreprise.

Nous classons les cybermenaces selon les motivations des cybercriminels. Chaque menace représente une occasion d'exécuter une campagne de cyberattaques contre une entreprise. **Pour en savoir plus sur notre approche, consultez la présentation de la solution MDR.**

## Principales cybermenaces pour les entreprises :

- Attaques cybercriminelles (ransomwares et extorsion)
- Perte et divulgation de données
- Compromission de la chaîne logistique
- Menaces internes
- Déni de service
- Risques tiers
- Manipulation de processus métier
- Piratage de ressources informatiques d'entreprise
- Cyberespionnage
- Non-respect des obligations réglementaires
- Intrusion dans le matériel ou ciblant un équipement de type Internet des objets (IoT)
- Mauvaise configuration ou erreur humaine
- Vol d'appareils physiques

- [x] **Menaces internes**
- [x] **Attaques cybercriminelles**
- [x] **Risques tiers**

Bien que la liste de chaque entreprise soit différente, certaines menaces sont omniprésentes dans le paysage actuel. Partez du principe qu'au moins deux des suivantes figureront sur votre liste : menaces internes, attaques cybercriminelles et risques tiers ou compromission de la chaîne logistique.

Une fois que vous avez dressé la liste des principales menaces qui ciblent votre entreprise, transmettez-la à vos équipes de réponse aux incidents et de surveillance.

**Conseil : prenez contact avec un fournisseur de services MDR pour obtenir de l'aide avec la modélisation des menaces. Il vous aidera à traduire les principales menaces qui ciblent votre entreprise en un ensemble complet de priorités en matière de visibilité sur la sécurité, de cyberrésilience et de détection. Il vous sera également utile pour comprendre le jargon et pallier l'absence de terminologie universelle pour les cybermenaces, les cybercriminels, les acteurs économiques, les risques métier, l'impact des incidents et les fonctionnalités. Pour découvrir ce que vous devez attendre d'un bon fournisseur de services MDR, consultez le Guide ModernCISO : S'assurer que votre partenaire MDR tient ses promesses.**

## Dans l'air du temps : le mécontentement des collaborateurs augmente le risque de menace interne

Les « utilisateurs internes » constituent une catégorie spécifique de cybercriminels, tandis que les menaces auxquelles font face les entreprises sont appelées « menaces internes ».

Le terme « utilisateur interne » peut désigner un collaborateur mécontent, un sous-traitant ou même un tiers de confiance.

Posez la question suivante : comment traduisez-vous les menaces internes en exigences concrètes pour une équipe de réponse aux incidents ?

Posez la question suivante : comment pouvez-vous associer avec précision vos fonctionnalités de détection existantes avec la capacité à identifier les comportements suspects ou inhabituels des utilisateurs ?

# 5. Traduire les menaces en actions concrètes afin d'atteindre les objectifs visés

**La dernière étape de ce processus consiste à traduire les cybermenaces qui ciblent l'entreprise en actions concrètes destinées à atteindre les objectifs visés. Heureusement pour les responsables de la sécurité, les cybercriminels affichant une motivation particulière suivent des étapes (relativement) prévisibles pour atteindre leurs objectifs.**

Ces « actions sur les objectifs » sont les tactiques, techniques et procédures sur lesquelles vous devez concentrer vos efforts de prévention et de détection des menaces.

Dressez la liste des « actions sur les objectifs » qu'un cybercriminel peut exécuter sur vos données et ressources critiques pour atteindre chacun des objectifs suivants :

**Profits financiers**

**Compromission de comptes**

**Perturbation des activités**

**Avantage concurrentiel dans votre secteur**

**Atteinte à votre réputation**

**Accès indirect à une cible**

**Collecte de renseignements**

Bien que ces étapes soient relativement prévisibles, elles peuvent toutefois être amenées à évoluer. Imaginez la scène suivante : nous sommes debout dans un champ avec la campagne qui s'étend devant nous. Je montre un point au loin et je vous dis d'y aller. Si aucune limite ne s'applique au chemin que vous pouvez prendre, vous pouvez faire simple ou exprimer toute votre créativité, tant que vous atteignez l'objectif.

C'est exactement ce que font les cybercriminels. Ils découvrent en permanence de nouveaux chemins qu'ils n'ont encore jamais empruntés. Cela signifie que les équipes de sécurité sont toujours un pas en arrière.

Conseil : **pour suivre l'évolution des tactiques, techniques et procédures des cybercriminels, il est indispensable de comprendre ce qu'ils essaient d'accomplir au sein de votre entreprise. Ceci étant fait, vous pouvez créer des contrôles et des fonctionnalités de détection pour réduire ces risques spécifiques.**

Prenons un exemple concret :

| Menace | Motivation | Actions sur les objectifs | Question(s) à se poser |
|---|---|---|---|
| Cybercriminel  | Profits financiers  | Une campagne de phishing entraîne le déploiement d'un ransomware sur 90 % de vos systèmes informatiques, ce qui met votre entreprise à l'arrêt. | **Quels contrôles seraient les plus efficaces dans ce scénario ?** |
| Cybercriminel  | Profits financiers  | Le cybercriminel collecte des mots de passe par le biais d'une attaque par brute force, puis s'en sert pour dérober des données de fichiers internes. La victime reçoit ensuite une demande de rançon. | **Pouvez-vous détecter les comportements suspects ou inhabituels des utilisateurs ? Des données peuvent-elles être exfiltrées par le biais d'un service cloud ?** |
| Cybercriminel  | Profits financiers  | Les cybercriminels utilisent des identifiants cloud qui ont été compromis ou divulgués pour déployer des mineurs de cryptomonnaie. Cela augmente vos demandes de ressources et les coûts associés à votre infrastructure cloud. | **Qu'est-ce qui aurait permis de limiter la capacité d'un cybercriminel à accéder à cet environnement ?** |

La rédaction d'un énoncé de mission, l'identification des principales cybermenaces qui ciblent votre entreprise et leur mise en correspondance avec les actions sur les objectifs doivent vous donner des informations plus détaillées sur le déroulement d'une attaque.

Naturellement, certains cybercriminels sont plus sophistiqués que d'autres. En outre, le paysage des menaces ne cesse d'évoluer. Il ne peut donc pas s'agir d'une préoccupation ou d'un processus ponctuel. Au gré de la croissance de votre entreprise, vous devrez réévaluer régulièrement votre stratégie de protection.

## Pour aller plus loin, prenez rendez-vous pour une consultation gratuite avec Kudelski Security.

Nous vous présenterons notre cadre propriétaire de scénarios d'utilisation, adapté à la matrice ATT&CK™ du MITRE, ainsi que les outils que nous avons développés pour vous aider à prioriser la visibilité sur la sécurité et la détection des menaces. Nous nous appuyons sur les scénarios d'utilisation de la détection de notre cadre pour **offrir une protection complète contre les menaces, adaptée à l'environnement de nos clients**. En tirant parti d'une cyberveille globale tout en tenant compte du paysage des menaces spécifiques de notre client, nous fournissons des services personnalisés et haut de gamme qui sont plus efficaces pour détecter et neutraliser les menaces.

Notre cadre de scénarios d'utilisation combine les éléments suivants :

- **Renseignements de cyberveille et informations métier**
- **Sources de données hiérarchisées**
- **Indicateurs de compromission**
- **Règles de corrélation**
- **Définitions des catégories et des niveaux de gravité**
- **Mesures de réponse personnalisées**
- **Mesures de remédiation pour les clients**
- **Une base dans la matrice MITRE ATT&CK™**

Notre équipe d'experts se fera un plaisir de vous aider à mieux comprendre les risques actuels et de vous accompagner dans votre migration vers un écosystème d'entreprise plus sécurisé.

# À propos des auteurs

## Francisco Donoso

**Vice-président de la stratégie globale de sécurité**

Francisco Donoso est Vice-président de la stratégie globale de sécurité chez Kudelski Security. Avant d'occuper ce poste, M. Donoso était l'architecte principal du Cyber Fusion Center et était à ce titre responsable de l'élaboration des offres mondiales de services de sécurité managés chez Kudelski Security.

M. Donoso est l'un des précurseurs des recherches sur les outils et fonctionnalités post-exploitation utilisés par l'Equation Group et révélés par The Shadow Brokers, et a présenté ces recherches lors d'événements tels que les conférences Derbycon, Thotcon, BlueHat de Microsoft et bien d'autres encore.

**Si vous vous trouvez sur le continent américain et que vous souhaitez discuter des services MDR avec Francisco Donoso, contactez-nous.**

## Olivier Spielmann

**Vice-président des services managés de détection et de neutralisation des menaces au niveau mondial**

Olivier Spielmann dirige la stratégie de réponse aux incidents et l'ensemble des équipes dédiées à travers le monde. Il a auparavant géré la stratégie et le projet MSS à l'échelle européenne pendant plus de huit ans, y compris les opérations du Cyber Fusion Center.

Fort de plus de 20 ans d'expérience dans le secteur de la cybersécurité, il a précédemment travaillé dans les domaines de la sécurité des entreprises de la sécurité de l'information et de la réponse aux incidents.

Depuis la Suisse, M. Spielmann met tout en oeuvre pour proposer des services managés de détection et de réponse aux menaces (MDR) alignés sur les besoins des clients, que l'entreprise soit une PME ou un leader mondial.

**Si vous vous trouvez en Europe et que vous souhaitez discuter des services MDR avec Olivier Spielmann, contactez-nous.**

Kudelski Security, une division du groupe Kudelski (SIX : KUD.S), est un éditeur indépendant de solutions de cybersécurité innovantes et personnalisées destinées aux entreprises et aux institutions du secteur public. Kudelski Security est implanté à Cheseaux-sur-Lausanne, en Suisse, ainsi qu'à Phoenix, aux États-Unis, et possède des bureaux dans de nombreux pays du monde.

info@kudelskisecurity.com
www.kudelskisecurity.com/fr/
www.modernCISO.com

### Nous contacter

Pour en savoir plus sur nos services MDR, téléchargez notre **brochure**.

### Exclusion de responsabilité

Ce document fournit des conseils sur les technologies et approches pertinentes qui permettent de résoudre un problème de sécurité spécifique rencontré par une entreprise. Dans la mesure où chaque environnement client et chaque besoin métier sont uniques, nous ne garantissons pas que ces recommandations sont appropriées dans tous les cas. Pour évaluer l'adéquation d'une stratégie ou tester l'impact d'un fournisseur spécifique, nous recommandons aux clients de contacter notre équipe avant-vente afin de procéder à une analyse plus approfondie.