Security Scorecard

GUIDE DE L'ACHETEUR

Supply Chain Detection and Response (SCDR)

Comment choisir la bonne solution pour opérationnaliser la cybersécurité de la chaîne d'approvisionnement

Sommaire

Résumé

Les risques liés à la chaîne d'approvisionnement ont gagné en complexité et en impact, mais la plupart des organisations peinent encore à opérationnaliser cet aspect de leurs programmes de sécurité. Il existe des lacunes fondamentales, telles qu'une visibilité insuffisante sur les fournisseurs, des plans de réponse aux incidents incomplets, ou encore un manque de compétences et de responsabilités pour résoudre les problèmes liés à la chaîne d'approvisionnement.

La détection et réponse aux risques de la chaîne d'approvisionnement (SCDR) est apparue comme une catégorie de solutions permettant d'opérationnaliser la cybersécurité des fournisseurs ou partenaires de votre organisation. C'est une technologie révolutionnaire qui permet aux équipes de gestion des risques liés aux tiers de se transformer en véritables intervenants face aux incidents dans la chaîne d'approvisionnement.

Une nouvelle catégorie de solutions de sécurité soulève naturellement un certain nombre de questions : Qu'est-ce que c'est ? Comment cela fonctionne-t-il ? Comment savoir si c'est nécessaire ? Ce guide vous aide à prendre une décision plus éclairée si vous envisagez de mettre en place une solution SCDR.

Qu'est-ce qu'une solution SCDR ?

Une solution de détection et réponse aux risques cyber de la chaîne d'approvisionnement (SCDR) améliore l'identification des problèmes critiques, la réactivité des fournisseurs et la rapidité de résolution des incidents. Les solutions SCDR offrent des renseignements sur les risques, des flux de travail pilotés par l'IA, ainsi que des capacités de collaboration pour améliorer la posture de sécurité de votre organisation et de vos fournisseurs.

Elles s'appuient sur des principes communs à d'autres approches de détection et réponse telles que XDR (Extended Detection and Response) et CDR (Cloud Detection and Response). Les principes partagés entre les solutions SCDR et les autres produits de détection et réponse sont les suivants :

Visibilité holistique :
La SCDR agrège des données sur les écosystèmes de fournisseurs, les surfaces d'attaque externes, ainsi que les contrôles de sécurité internes.

Corrélation des données et analyse contextuelle :
La SCDR priorise les fournisseurs selon leur niveau de risque et leur impact sur l'entreprise, tout en identifiant les actions de remédiation les plus efficaces.

Automation et orchestration :
La SCDR simplifie la détection et la réponse aux incidents grâce à l'intelligence artificielle et à des règles logiques prédéfinies.

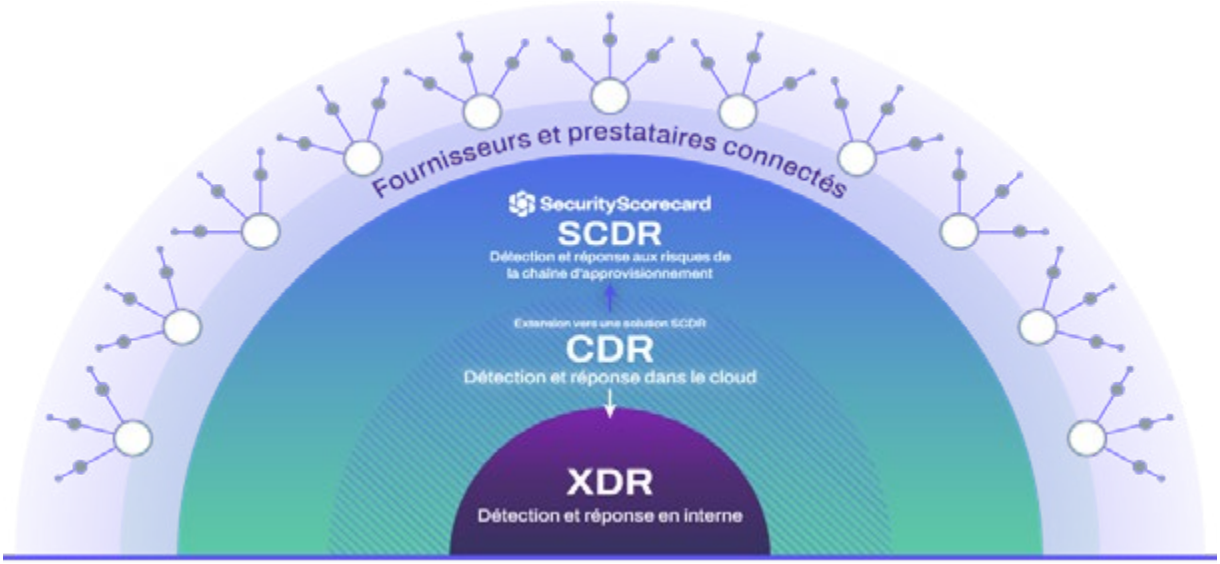
Centralisation des opérations de détection et de réponse :
La SCDR offre une vue unifiée des chaînes d'approvisionnement, des contacts chez les fournisseurs et des outils de remédiation.

La nécessité de faire appel à une solution SCDR découle de l'évolution de la surface d'attaque d'une organisation. À la base, la surface d'attaque de chaque organisation commence par ses propres terminaux, serveurs et réseaux. Comme de plus en plus d'organisations migrent leurs actifs dans le cloud, leur surface d'attaque s'étend à cet environnement. C'est pourquoi les solutions XDR et CDR sont devenues des éléments essentiels de l'arsenal technologique en matière de sécurité des organisations.

Aujourd'hui, la plupart des organisations dépendent des services d'autres entreprises ou autorisent leurs partenaires à accéder à leurs systèmes et données. Cette dynamique augmente la surface d'attaque de manière exponentielle. Par conséquent, les solutions SCDR ont un rôle tout aussi crucial à jouer dans la sécurité d'une organisation.

Raisons d'envisager l'acquisition d'une solution SCDR :

- Vous avez subi une violation coûteuse au sein de votre chaîne d'approvisionnement.
- Les régulateurs exigent des processus renforcés de gestion des risques.
- Un changement de stratégie commerciale accroît les dépendances externes.



Justification d'un investissement dans une solution SCDR

Bâtir un argumentaire solide pour investir dans de nouvelles solutions peut s'avérer difficile, surtout lorsque les budgets de sécurité stagnent ou diminuent. Justifier un investissement implique souvent d'exposer en détail votre situation actuelle, votre vision pour l'avenir et l'impact que ce changement aura sur l'organisation.

Mettre en évidence les défis organisationnels

Aujourd'hui, très peu d'organisations disposent d'une équipe d'intervention en cas d'incident au sein de la chaîne d'approvisionnement, car mettre en œuvre la cybersécurité dans ce domaine est un véritable défi.

Qui possède les compétences et le temps nécessaires pour répondre aux alertes liées aux plateformes tierces ? Quelles données sont partagées avec les fournisseurs, et quelle est leur importance pour l'entreprise ? Quel est le plan de réponse face aux différents types de violations impliquant des tiers ? Ces questions restent souvent sans réponse claire, ce qui accroît l'exposition aux risques liés à la chaîne d'approvisionnement.

Obstacles à l'opérationnalisation de la sécurité dans la chaîne d'approvisionnement :

1

Vision incomplète des risques liés à la chaîne d'approvisionnement

La prolifération et la spécialisation des outils logiciels, le marketing direct auprès des utilisateurs, ainsi que la recherche de technologies de pointe ont fait exploser le nombre de fournisseurs dont dépendent généralement les organisations. Il existe également une dépendance aux questionnaires, qui ne fournissent qu'une évaluation ponctuelle, sans saisir les nuances nécessaires ni assurer une visibilité continue sur les menaces actives et les vulnérabilités émergentes.

2

Absence de processus efficaces

La plupart des plans de réponse aux incidents ne prévoient pas de mesures concrètes à prendre lorsqu'un fournisseur présente un risque élevé ou a été victime d'une violation. Les gestionnaires des risques se retrouvent soit submergés par un excès de données, soit privés d'informations pertinentes. Les outils de surveillance externes génèrent quantité d'informations dénuées de contexte, provoquant une paralysie de l'analyse. Les questionnaires de sécurité ne sont que des auto-déclarations longues à analyser. Si un fournisseur n'a pas connaissance de problèmes susceptibles d'entraîner des incidents, ses réponses ne présentent guère d'intérêt.

3

Responsabilités floues en matière de réponse aux incidents

Les équipes de gestion des risques se concentrent sur l'établissement de contrôles préventifs contre les violations impliquant des tiers, tandis que les équipes chargées des opérations de sécurité ont pour mission de limiter les impacts après une violation. Il existe donc une faille dans la réponse quotidienne aux incidents de la chaîne d'approvisionnement susceptibles de provoquer une violation. Les gestionnaires des risques qui surveillent en continu les fournisseurs ne peuvent qu'informer leur SOC (Security Operations Center) des problèmes liés à la chaîne d'approvisionnement. Les SOC sont souvent submergés par les alertes internes et ne peuvent pas collaborer directement avec les fournisseurs pour résoudre les problèmes.

4

Processus de gestion des risques inefficaces

Beaucoup de programmes de gestion des risques se concentrent uniquement sur un nombre relativement restreint de fournisseurs critiques. Pourtant, les organisations comptent également une longue liste de fournisseurs qui offrent d'autres services, mais peuvent représenter des vecteurs d'attaque significatifs pour les cybercriminels. Cette liste secondaire est souvent négligée compte tenu du temps limité dont disposent les équipes pour effectuer des évaluations ou surveiller les fournisseurs. Ce problème est encore aggravé dans les organisations qui dépendent d'une gestion laborieuse via des feuilles de calcul et d'autres processus manuels d'évaluation des risques.

5

Manque d'expertise en cybersécurité

La gestion des risques est souvent assurée par des professionnels dont les compétences relèvent davantage des risques financiers, opérationnels, réglementaires, stratégiques et réputationnels. Ils font alors appel à des professionnels de l'informatique ou de la sécurité lorsque des évaluations approfondies ou l'exécution d'un plan de réponse aux incidents sont nécessaires. Compte tenu de la nature dynamique des risques cyber, le manque d'expertise en sécurité peut entraver la mitigation ou la réponse aux menaces actives ou aux nouvelles vulnérabilités.

Questions à se poser :

- Quel niveau de contrôle exercez-vous sur votre écosystème de fournisseurs ?
- Quels sont vos plans de réponse aux incidents liés à la chaîne d'approvisionnement ?
- Comment détectez-vous les incidents susceptibles de se transformer en violations au sein de votre chaîne d'approvisionnement ?

Identifier les bénéfices attendus

Une organisation ayant réussi à opérationnaliser la cybersécurité de sa chaîne d'approvisionnement peut mener à bien des activités qui ne sont pas à la portée d'une organisation moins avancée en la matière.

Identifier les fournisseurs non déclarés :

Utilisez les données transactionnelles ou les intégrations avec les systèmes internes pour vous assurer que toutes les dépendances de la chaîne d'approvisionnement sont bien prises en compte.

Évaluer la posture de sécurité d'un fournisseur :

Déterminez si un fournisseur est susceptible d'être à l'origine d'incidents grâce à des données sur sa surface d'attaque et à des preuves de mise en œuvre de mesures de sécurité.

Surveiller les risques liés à la chaîne d'approvisionnement :

Détectez les problèmes critiques, les vulnérabilités zero-day, ainsi que les indicateurs de compromission tels que les infections par des logiciels malveillants ou les fuites d'identifiants.

Prioriser les mesures de gestion des risques :

Classez les fournisseurs en fonction de leur impact commercial et de la probabilité d'un incident afin de cibler les actions d'engagement et de réponse.

Collaborer avec des fournisseurs à haut risque :

Alertez les fournisseurs sur leur exposition aux incidents de sécurité, recommandez-leur des actions de remédiation et demandez des preuves de résolution.

Valider la résolution des incidents :

Suivez l'avancement des actions de remédiation et vérifiez les preuves attestant que les plans de réponse aux incidents ont été exécutés.

Rendre compte régulièrement aux parties prenantes :

Communiquez le statut et les résultats du programme de réponse aux incidents de la chaîne d'approvisionnement aux parties prenantes du SOC ou de l'entreprise.

Questions à se poser :

- Quelle est votre vision de la cybersécurité dans la chaîne d'approvisionnement ?
- Quels sont les obstacles à la réalisation de cette vision ?
- Quelles tâches souhaitez-vous accomplir en matière de réponse aux incidents de la chaîne d'approvisionnement ?

Estimer le retour sur investissement

Opérationnaliser la cybersécurité de la chaîne d'approvisionnement grâce à une solution SCDR apportera une valeur commerciale intangible, ainsi que des résultats mesurables en termes de réduction des risques.

Le principal bénéfice tangible d'une solution SCDR est de réduire le nombre d'incidents liés à la chaîne d'approvisionnement et l'impact financier des violations ou des sanctions réglementaires. Il peut être difficile à mesurer, car l'objectif est justement d'éviter qu'un événement indésirable ne survienne. Si aucun incident ne se produit, est-ce effectivement grâce aux actions mises en place ? Malgré cette particularité, la performance d'un programme de cybersécurité de la chaîne d'approvisionnement peut être efficacement mesurée par des indicateurs qui renseignent sur la réduction des risques.

Taux de réponse des fournisseurs :

Pourcentage de fournisseurs qui acceptent l'invitation à rejoindre le programme de cybersécurité de la chaîne d'approvisionnement et s'engagent à respecter ses exigences.

Taux de diminution des fournisseurs à haut risque :

Pourcentage de fournisseurs passant d'un niveau de risque élevé à un niveau faible ou moyen.

Amélioration de la sécurité de la chaîne d'approvisionnement :

Pourcentage de réduction du nombre de problèmes au sein de l'ensemble de la chaîne d'approvisionnement.

Conformité des fournisseurs en matière de remédiation :

Pourcentage de fournisseurs qui résolvent les problèmes après notification.

Rapidité de remédiation des fournisseurs :

Durée écoulée entre la notification d'un problème au fournisseur et la constatation de sa résolution.

Les bénéfices immatériels pour l'entreprise sont également essentiels dans l'évaluation du retour sur investissement, car ils apportent une valeur significative, souvent à long terme, qui ne transparaît pas toujours immédiatement dans les indicateurs de performance ou financiers. Prendre en compte ces bénéfices offre une vision plus complète du véritable retour sur investissement.

1

Renforcer la confiance des clients

Des contrôles renforcés de la cybersécurité de la chaîne d'approvisionnement montrent à vos clients que vous agissez de manière proactive pour réduire les vulnérabilités liées aux fournisseurs, protégeant ainsi leurs données et leurs opérations. Cet engagement envers la sécurité suscite la confiance des clients dans la fiabilité de votre marque.

2

Renforcer les compétences et la capacité des équipes de sécurité et de gestion des risques

La mise en place de mécanismes d'efficience opérationnelle permet à vos équipes de gestion des risques et de sécurité d'automatiser les tâches répétitives, libérant ainsi du temps pour se consacrer à des activités plus complexes et formatrices. Ce changement accroît la capacité des équipes à gérer des projets stratégiques tout en renforçant leur expertise et leur adaptabilité.

3

Instaurer de meilleures relations avec les fournisseurs

Aider les fournisseurs à résoudre leurs problèmes de sécurité témoigne d'un engagement envers leur réussite et d'une approche proactive de la sécurité partagée, ce qui renforce la confiance et approfondit la collaboration. Vous montrez ainsi que vous accordez de la valeur à votre partenariat et que vous êtes prêt à investir dans leur résilience, forgeant ainsi une relation plus solide et coopérative.

Questions à se poser :

- Quels sont vos objectifs pour votre programme de cybersécurité de la chaîne d'approvisionnement ?
- Comment mesurez-vous la réussite ?

DÉTERMINATION DES CRITÈRES DE SCDR

Une fois que vous avez déterminé que la SCDR mérite d'être explorée, l'étape suivante consiste à définir précisément ce que vous attendez d'une solution de ce type. Posez-vous deux questions essentielles : Comment cette solution s'intégrerait-elle à mon organisation ? La solution dispose-t-elle des outils nécessaires pour atteindre les résultats souhaités ?

Adapter aux exigences organisationnelles

Toute organisation est amenée à engager un processus d'opérationnalisation de la cybersécurité de sa chaîne d'approvisionnement. Ce parcours peut être comparé à une courbe de maturité où l'efficacité et la valeur commerciale augmentent à chaque étape. Dans votre évaluation des solutions SCDR, il est utile de réfléchir à quelle étape vous vous trouvez sur cette courbe de maturité, aux objectifs que vous visez, et dans quels délais vous souhaitez les réaliser.

Étape 1 : Diligence raisonnable de base

C'est la phase la plus élémentaire du parcours de cybersécurité de la chaîne d'approvisionnement, où vous réalisez uniquement des évaluations ponctuelles de la sécurité à des moments clés du cycle de vie relationnel, tels que l'intégration des fournisseurs, ou avant les audits de conformité. Les évaluations de ce type génèrent rarement des informations exploitables, si bien qu'en réalité elles sont surtout réalisées à titre de formalité. Elles doivent néanmoins être effectuées pour repérer les signaux d'alerte en matière de sécurité, mais leur valeur en termes de réduction des risques reste limitée.

Étape 2 : Gestion ad hoc des risques liés aux tiers (TPRM)

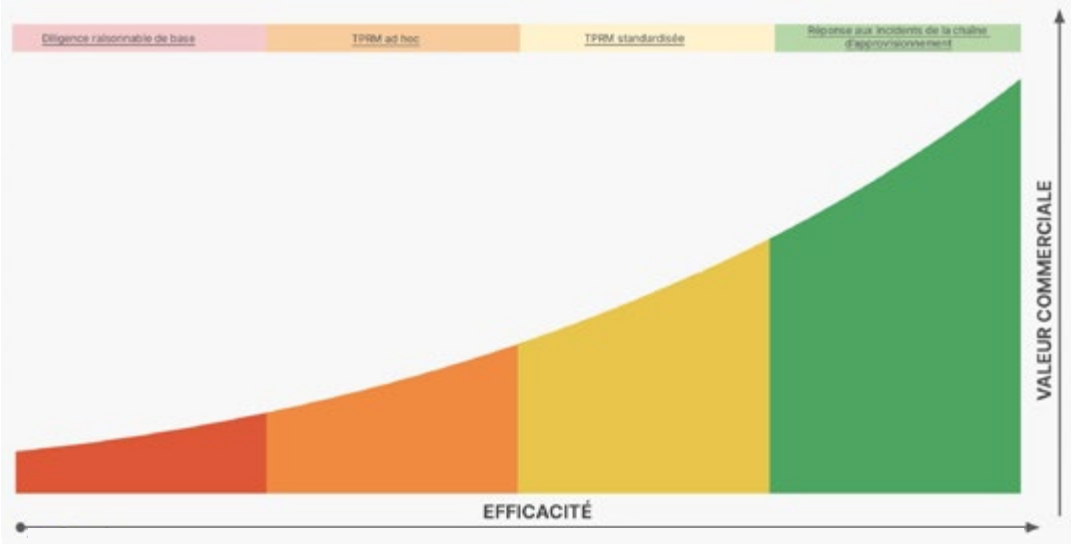
À ce stade, les organisations commencent à surveiller leurs fournisseurs de manière continue, mais leurs politiques et processus de gestion des risques restent relativement informels. Elles sont plus en mesure de détecter les risques, mais les résultats ne sont pas forcément meilleurs pour autant. L'approche est alors réactive, reposant sur des actions menées en urgence pour contenir les incidents au sein de la chaîne d'approvisionnement. Les processus manuels et l'incapacité à étendre la gestion des risques à l'ensemble des fournisseurs font que des incidents passent encore entre les mailles du filet et que seuls les plus graves sont traités, moyennant des coûts importants.

Étape 3 : Standardisation de la gestion des risques liés aux tiers (TPRM)

La mise en œuvre proactive et constante de contrôles préventifs contre les violations est la marque d'un programme standardisé de gestion des risques liés aux tiers (TPRM). Les questionnaires sont envoyés en temps voulu, les politiques sont appliquées à tous les fournisseurs intégrés, et les parties prenantes comprennent l'impact des risques liés à la chaîne d'approvisionnement. Cette étape présente des limites, car la TPRM ne porte que sur la mise en place de contrôles préventifs, et il reste difficile d'engager directement les fournisseurs pour corriger les problèmes avant qu'ils n'aboutissent à des violations.

Étape 4 : Réponse aux incidents de la chaîne d'approvisionnement

Il s'agit de la phase la plus performante en matière de cybersécurité de la chaîne d'approvisionnement, car votre organisation maîtrise la remédiation rapide des problèmes de sécurité dans ce domaine. Alors que les équipes TPRM ont tendance à déléguer la réponse aux incidents de la chaîne d'approvisionnement à un SOC débordé, une équipe dédiée assume la responsabilité du développement et de l'exécution des plans de réponse. Grâce à une intégration étroite avec le SOC, les équipes de réponse aux incidents de la chaîne d'approvisionnement communiquent leurs conclusions aux fournisseurs, expliquent les stratégies de remédiation, et collaborent avec le SOC pour contenir tout impact.



L'autre considération organisationnelle concerne votre stratégie de cybersécurité et la priorisation des risques liés à la chaîne d'approvisionnement. Ces risques peuvent être hiérarchisés en fonction de la nature de votre relation avec un fournisseur et de l'impact qu'une violation de leur côté pourrait avoir sur votre organisation. Une solution SCDR peut prendre en charge une priorisation hiérarchisée afin d'accorder l'attention et les ressources appropriées aux fournisseurs de tous les niveaux.

Niveau 1 : Fournisseurs critiques

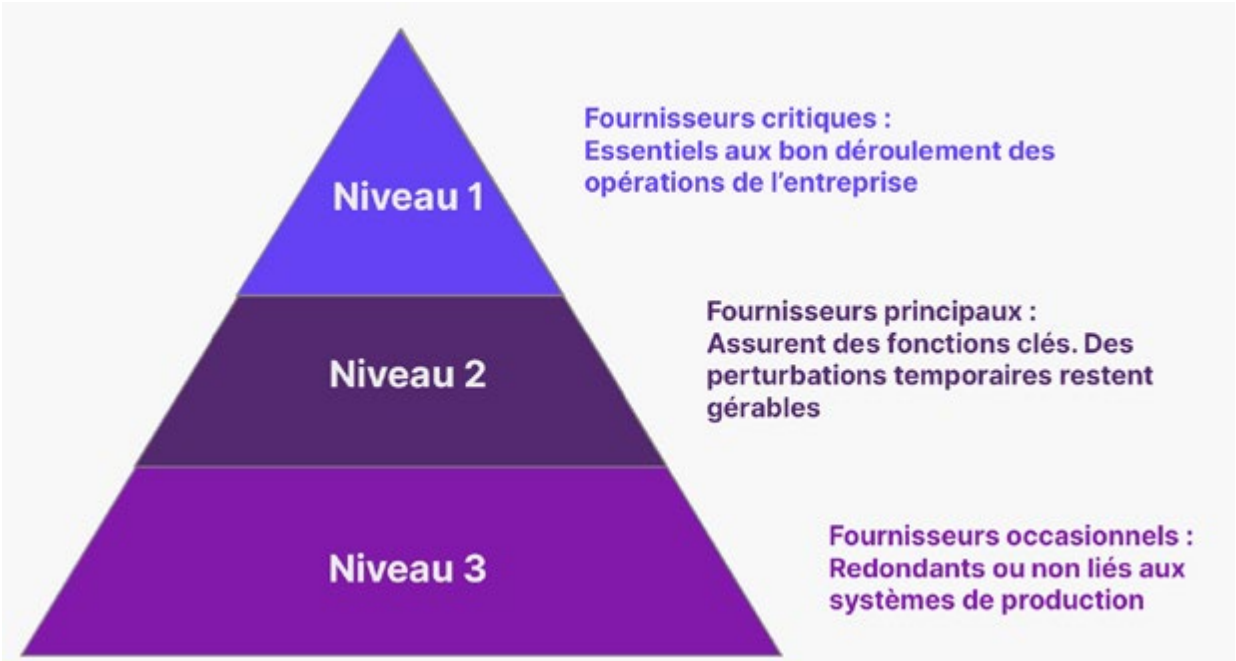
Tout fournisseur essentiel au bon déroulement des opérations de l'entreprise est qualifié de critique. Les fournisseurs critiques exigent des mesures de sécurité et de conformité très strictes, car ils sont susceptibles d'avoir accès à vos systèmes ou à vos données. Une diligence raisonnable approfondie et une surveillance continue sont nécessaires. Les relations avec ces fournisseurs doivent être actives afin de permettre une intervention immédiate pour piloter la remédiation en cas d'incident.

Niveau 2 : Fournisseurs principaux

Ce sont les fournisseurs assurant des fonctions clés, mais au niveau desquels des perturbations temporaires restent gérables en cas d'incident. Ils n'ont peut-être pas accès aux systèmes ou données critiques, mais les équipes métier comptent sur eux. En conséquence, les fournisseurs principaux doivent être informés des attentes en matière de sécurité que vous leur imposez, afin qu'en cas d'incident critique, ils sachent que vous assurerez un suivi pour vérifier que les remédiations ont été effectuées.

Niveau 3 : Fournisseurs occasionnels

Les fournisseurs redondants ou non liés aux systèmes de production sont classés comme occasionnels. L'impact organisationnel serait minime si l'un d'eux était victime d'une violation. Une diligence raisonnable lors de l'intégration ou chaque année est nécessaire pour repérer les signaux d'alerte. L'automatisation des activités de gestion des risques est idéale pour cette catégorie, avec une intervention humaine réservée aux scénarios imprévus.



Identifier les fonctionnalités requises

La sélection de critères permet souvent de définir une fonctionnalité nécessaire de la solution et sa capacité à aider les équipes à accomplir une tâche en cas d'incident dans la chaîne d'approvisionnement.

Une solution complète de détection et réponse dans la chaîne d'approvisionnement repose sur trois piliers essentiels.

Surveillance continue des risques :

Identification instantanée et continue des problèmes de sécurité, du comportement des acteurs malveillants et des incidents actifs impactant une organisation et ses fournisseurs.

Gestion du cycle de vie des fournisseurs :

Gestion des données des fournisseurs, suivi de leur engagement, et centralisation des preuves et documents qu'ils fournissent afin de faciliter la réduction des risques et le contrôle.

Collaboration et remédiation avec les fournisseurs :

Les informations sur les risques liés à la chaîne d'approvisionnement peuvent être transformées en actions concrètes grâce à des outils et flux de travail permettant aux fournisseurs de résoudre efficacement les problèmes identifiés et priorisés comme les plus critiques.

La sélection de critères permet souvent de définir une fonctionnalité nécessaire de la solution et sa capacité à aider les équipes à accomplir une tâche en cas d'incident dans la chaîne d'approvisionnement.

Éléments à rechercher	Raisons
Collecte non intrusive et automatisée de preuves auprès des fournisseurs	Le fournisseur peut ne pas être disponible ou disposé à remplir des questionnaires.
Utilisation d'un modèle de probabilité d'incident pour identifier les problèmes générateurs de risques	Un niveau de sécurité parfait étant impossible à garantir chez les fournisseurs, la remédiation doit privilégier les problèmes les plus impactants.
Capacité à surveiller simultanément l'ensemble de l'écosystème d'une organisation	Les problèmes de sécurité peuvent survenir à tout moment chez n'importe quel fournisseur.
Détection et alerte des incidents et des violations de la sécurité dans la chaîne d'approvisionnement	Satisfait aux exigences réglementaires ou internes en matière de réponse aux incidents.
Découverte proactive des fournisseurs inconnus au sein de la chaîne d'approvisionnement de l'organisation (Shadow IT)	Des fournisseurs peuvent être intégrés sans le consentement des équipes informatiques ou de sécurité, ce qui entraîne une visibilité insuffisante.
Alerte et détection précoce de l'exposition aux vulnérabilités zero-day	Les vulnérabilités de type zero-day peuvent être exploitées rapidement, nécessitant une intervention immédiate.
Visibilité du comportement des acteurs malveillants sur le deep web et le dark web	Évite les incidents en identifiant les fournisseurs qui sont activement ciblés.
Contextualisation des preuves par des références croisées aux normes du secteur ou à des règles de conformité	Offre une autre perspective de priorisation des problèmes sur la base de critères largement acceptés.
Analyse de l'impact financier des coûts directs suite à un incident ou à une violation dans la chaîne d'approvisionnement	Communique l'impact des risques liés à la chaîne d'approvisionnement ainsi que l'efficacité des investissements en matière de réponse aux incidents auprès des parties prenantes métier.

La collaboration et la remédiation avec les fournisseurs donnent tout son sens à la « réponse » dans un contexte SCDR.

Éléments à rechercher	Raisons
Invitation et intégration des fournisseurs	Les fournisseurs doivent comprendre les besoins de leur client en matière de sécurité, ainsi que les attentes du programme de cybersécurité de la chaîne d'approvisionnement.
Création, envoi et gestion des questionnaires	Certaines informations, impossibles à collecter de manière autonome, doivent néanmoins être obtenues rapidement et efficacement.
Alertes ciblées concernant des incidents cyber	Informe les équipes de réponse aux incidents de la chaîne d'approvisionnement et les fournisseurs des incidents que subit leur organisation.
Analyse automatisée de l'exposition aux incidents dans la chaîne d'approvisionnement et suivi des réponses	Accélère le suivi, la remédiation et le reporting sur l'impact commercial.
Intégration avec les systèmes de sécurité internes	Permet une maîtrise rapide des risques liés à la chaîne d'approvisionnement.
Gestion de la surface d'attaque des fournisseurs	Permet aux fournisseurs de remédier aux problèmes identifiés.
Priorisation des risques liés à la chaîne d'approvisionnement selon l'impact commercial et la probabilité d'un incident	Il n'existe pas de solution universelle pour gérer les risques liés à la chaîne d'approvisionnement, et l'affectation des ressources pour la réponse doit être efficace.
Tri et priorisation des communications avec les fournisseurs	Évite les sollicitations redondantes lorsque plusieurs organisations travaillent avec un même fournisseur.
Plateforme commune de gestion des risques entre les organisations et leurs fournisseurs	Simplifie le processus de consensus sur l'impact des risques de sécurité et des communications pour faciliter la résolution.

La gestion du cycle de vie des fournisseurs offre un contexte organisationnel sous-jacent qui combine des fonctionnalités de détection et de réponse.

Éléments à rechercher	Raisons
Système de collecte des caractéristiques de l'organisation d'un fournisseur	Permet la hiérarchisation selon l'impact commercial et l'exécution des plans de réponse aux incidents.
Gestion du backlog de réponse aux incidents de la chaîne d'approvisionnement	Aide les équipes à rester concentrées, organisées et coordonnées lors de la gestion de plusieurs incidents.
Mise en œuvre des politiques de cybersécurité de la chaîne d'approvisionnement	Déclenche des plans de réponse aux incidents automatisés et garantit une approche cohérente de la gestion des risques.
Rapports de gestion des risques cyber dans la chaîne d'approvisionnement	Surveille l'impact des stratégies de gestion des risques et rend compte des performances aux cadres de l'entreprise.

Évaluation des alternatives à une solution SCDR

Comme nous l'avons vu, les solutions SCDR offrent plusieurs propositions de valeur. Compte tenu du rythme de l'innovation et des investissements dans le secteur de la sécurité, d'autres solutions peuvent offrir des fonctionnalités présentant des similitudes. Il est important de rester attentif et d'évaluer si les alternatives sont adaptées.

Plateformes de notation cyber

Une plateforme de notation cyber est un outil ou un service qui évalue et attribue une note (scoring) à la posture de cybersécurité des organisations sur la base de divers facteurs externes. Ces plateformes collectent des données provenant de sources publiques et exclusives, les analysent, et génèrent des notations reflétant le niveau de risque de cybersécurité d'une organisation.

Les plateformes de notation disposent de solides capacités de détection, mais elles manquent des outils ou du contexte nécessaires pour répondre aux incidents ou gérer le cycle de vie des fournisseurs. Malgré leurs atouts en matière de détection, le mode de présentation des résultats peut s'avérer fastidieux.

Services de gestion de questionnaires

Des entreprises spécialisées peuvent gérer la création, la distribution, la collecte et l'analyse des questionnaires d'évaluation des risques envoyés aux fournisseurs. Cependant, ces services ne collectent des preuves qu'à travers des questionnaires, si bien que leurs fonctionnalités de détection dans la chaîne d'approvisionnement dépendent essentiellement de leur capacité à obtenir rapidement des réponses exhaustives.

Une solution SCDR va bien au-delà, car elle analyse des données relatives à la surface d'attaque qui sont impossibles à saisir via des questionnaires, tout en permettant une interaction directe avec les fournisseurs pour expliquer les conclusions et faciliter la remédiation.

Systèmes de gestion des risques liés aux tiers

Les systèmes TPRM offrent un cadre pour gérer et atténuer les divers risques associés aux fournisseurs, partenaires et prestataires externes. Ils couvrent généralement l'ensemble du cycle de vie des relations avec les tiers, de l'intégration au reporting, en passant par l'évaluation des risques, la surveillance continue et la remédiation.

Ces systèmes ne disposent pas de fonctionnalités de détection et leurs capacités de réponse sont limitées. Ils peuvent ingérer des données issues de plateformes de notation cyber ou de solutions SCDR pour les utiliser en entrée dans les flux de travail de gestion des relations.

Fonctionnalités SCDR	Notation cyber	Services de gestion de questionnaires	Systèmes TPRM	SCDR
Surveillance continue des risques	Forte	Faible	Faible	Forte
Gestion du cycle de vie des fournisseurs	Faible	Faible	Forte	Forte
Collaboration et remédiation avec les fournisseurs	Moyenne	Moyenne	Faible	Forte

Mise en œuvre de la SCDR

Le dernier facteur à prendre en compte lors de l'achat d'une solution SCDR concerne sa mise en œuvre, et plus précisément les moyens que votre équipe devra déployer en matière de gestion et d'administration. Il existe trois options de mise en œuvre des solutions SCDR.

Solution maison

Cette option est idéale pour les organisations souhaitant constituer une équipe interne de réponse aux incidents dans la chaîne d'approvisionnement, avec un accompagnement minimal et ponctuel de la part du fournisseur de la solution SCDR. Il faut pour cela une solution SCDR intuitive, des compétences pour analyser les conclusions et collaborer avec les fournisseurs afin de remédier aux problèmes, ainsi qu'une capacité à réaliser les tâches nécessaires pour l'ensemble des fournisseurs.

Sous-traitance

Cette option convient parfaitement aux organisations qui souhaitent tirer parti d'une équipe performante de réponse aux incidents dans la chaîne d'approvisionnement, sans pour autant déployer des ressources dédiées. Elle est généralement proposée sous forme de service géré par le fournisseur de la solution SCDR. Dans ce cadre, le fournisseur met à disposition sa propre équipe d'intervenants face aux incidents de la chaîne d'approvisionnement, qui agit au nom des clients pour gérer un programme de cybersécurité complet.

Cogestion

Il s'agit dans ce cas de combiner l'option « fait maison » et la sous-traitance. L'approche de déploiement type pour cette option implique que l'acheteur de la solution SCDR dispose d'une équipe responsable de l'engagement des fournisseurs à haut risque. Le fournisseur de la solution SCDR gère, quant à lui, la configuration et l'administration de la plateforme pour diriger les activités de réponse aux incidents dans la chaîne d'approvisionnement.

Considérations de mise en œuvre :

- La réponse aux incidents dans la chaîne d'approvisionnement est-elle une compétence essentielle que votre organisation doit maîtriser et développer elle-même ?
- Le domaine de la cybersécurité évolue très rapidement. Dans quelle mesure jugez-vous votre organisation capable de relever le défi ?
- La réponse aux incidents dans la chaîne d'approvisionnement exige des compétences mêlant cybersécurité, connaissance des menaces, TPRM et qualités relationnelles. Pouvez-vous constituer une équipe réunissant ces caractéristiques ?
- En général, les équipes les plus efficaces en matière de réponse aux incidents dans la chaîne d'approvisionnement sont capables d'examiner une alerte par fournisseur et par jour. Votre équipe a-t-elle la capacité de soutenir ce niveau d'activité ?

Êtes-vous prêts à MAXimiser la gestion des risques cyber dans votre chaîne d'approvisionnement ?

Pour en savoir plus, rendez-vous dès aujourd'hui sur securityscorecard.com/max

À PROPOS DE SECURITYSCORECARD

Financée par des investisseurs de premier rang tels qu'Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital et bien d'autres, SecurityScorecard est le leader mondial dans l'évaluation, la réponse et la résilience en matière de cybersécurité, avec plus de 12 millions d'entreprises évaluées en permanence.

Fondée en 2013 par Aleksandr Yampolskiy et Sam Kassoumeh, experts en sécurité et en gestion des risques, SecurityScorecard propose une technologie de notation brevetée qui est utilisée par plus de 25 000 organisations pour la gestion des risques d'entreprise, la gestion des risques liés aux tiers, le reporting destiné aux dirigeants, la diligence raisonnable, la souscription de cyber-assurances et la surveillance réglementaire.

SecurityScorecard contribue à rendre le monde plus sûr en transformant la manière dont les entreprises appréhendent les risques de cybersécurité, les traitent et communiquent à leur sujet auprès de leurs conseils d'administration, de leurs employés et de leurs fournisseurs. SecurityScorecard a obtenu la certification FedRAMP, programme fédéral américain de gestion des risques et des autorisations, ce qui témoigne des normes de sécurité robustes qu'elle déploie pour protéger les informations de ses clients. Par ailleurs, sa solution est répertoriée comme outil et service de cybersécurité gratuit par l'Agence de cybersécurité et de sécurité des infrastructures (CISA). Chaque entreprise dispose du droit universel à recevoir sa notation fiable et transparente SecurityScorecard. Pour plus d'informations, rendez-vous sur securityscorecard.com ou suivez-nous sur LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io