Checklist Préparation à la gestion de l’exposition

La gestion de l’exposition englobe des fonctionnalités qui sont très souvent déjà implémentées dans les organisations. Ainsi, sans nécessairement le savoir, vous avez peut-être déjà entamé une démarche pour gérer l’exposition.

La checklist présente les différents types de produits intervenant dans la gestion de l’exposition et leurs principales fonctionnalités. Organisée en quatre catégories — Visibilité, Priorisation, Validation et Remédiation — cette liste vous aidera à identifier les fonctionnalités déjà intégrées à votre pile technologique de cybersécurité et celles manquantes.

Parmi les types de produits mentionnés dans cette liste, certains relèvent de plusieurs catégories. Auquel cas, cela est spécifié.

Visibilité

Il suffit d'un seul angle mort pour qu'un cyberpirate puisse infiltrer votre environnement. Les technologies mentionnées dans cette section garantissent une bonne visibilité sur tous les cyberactifs, expositions et autres éléments qui constituent votre surface d'attaque. Cependant, vous n'avez pas besoin d'implémenter toutes les technologies mentionnées. Certaines ont des fonctionnalités qui se recoupent et d'autres ne sont peut-être pas pertinentes pour votre environnement. Vous devez plutôt trouver la combinaison qui vous permettra d'avoir une visibilité complète sur votre surface d'attaque.

Découverte des actifs IT

Visibilité	X
Priorisation	
Validation	
Remédiation	

Ces outils identifient et inventorient automatiquement les actifs matériels et logiciels de l'environnement IT d'une organisation. Cependant, ils peuvent échouer à découvrir certains types d'actifs et ne sont pas conçus pour découvrir les expositions. C'est pourquoi, d'autres outils sont nécessaires pour garantir une visibilité complète de la surface d'attaque.

Gestion unifiée des terminaux (UEM)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les outils UEM aident l'équipe IT à pleinement comprendre son environnement de postes client (ordinateurs de bureau, ordinateurs portables, périphériques mobiles et autres périphériques connectés à Internet). Ils servent aussi à gérer, configurer et sécuriser chaque poste client.

Gestion des périphériques mobiles (MDM)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les outils MDM (on entend ici gestion des périphériques mobiles) sont des outils UEM spécialisés dans la découverte et la gestion des périphériques mobiles, comme les smartphones et les tablettes.

Gestion moderne des périphériques (MDM)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Ce type d'outil MDM (ici, on parle de gestion moderne des périphériques) vous permet de surveiller, provisionner, doter de correctifs et sécuriser à distance une gamme de périphériques connectés au réseau plus large que celle gérée par les autres types d'outils MDM. Cela concerne notamment (mais pas seulement), les ordinateurs de bureau, les capteurs IoT, les dispositifs portatifs (comme les smartwatches), les dispositifs médicaux et les machines industrielles.

Découverte réseau

Visibilité	X
Priorisation	
Validation	
Remédiation	

Ces solutions logicielles détectent et cartographient automatiquement les actifs matériels, logiciels et virtuels d'un réseau. Elles créent ainsi une image complète de l'infrastructure réseau.

Scanners de vulnérabilités réseau

Visibilité	X
Priorisation	
Validation	
Remédiation	

En détectant et évaluant automatiquement les vulnérabilités de sécurité des périphériques et systèmes réseau, les scanners de vulnérabilités réseau aident les organisations à identifier les risques potentiels.

Outils de sécurité IoT (Internet des objets)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Même s'il n'existe aucune norme sectorielle sur le nom ou la définition des outils de découverte des actifs et expositions IoT, plusieurs outils de ce type sont disponibles sur le marché. Une simple recherche en ligne sur « outils de sécurité IoT » vous fournira une liste de solutions.

Plateformes de protection des systèmes cyberphysiques (CPS)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les plateformes de protection CPS sont conçues pour découvrir, catégoriser, cartographier et protéger les systèmes cyberphysiques. Cela inclut des ICS (Systèmes de contrôle industriel) et des solutions intelligentes de gestion des bâtiments, qui intègrent des composants physiques et des composants computationnels.

Gestion de la posture de sécurité Cloud (CSPM)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les organisations qui possèdent une infrastructure Cloud importante peuvent utiliser des outils CSPM pour gérer la visibilité de ces environnements. Ces outils identifient et cataloguent les actifs Cloud de l'organisation (qu'ils soient dans un Cloud privé, public, hybride ou dans un environnement multi-cloud). Ils les surveillent aussi en continu pour assurer leur conformité aux cadres de sécurité et de conformité, en vue d'identifier les vulnérabilités et les menaces.

Plateforme de protection des charges de traitement Cloud (CWPP)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les solutions CWPP détectent et traitent automatiquement les menaces, vulnérabilités et erreurs qui impactent les charges de traitement Cloud (applications et programmes qui s'exécutent dans le Cloud). Elles couvrent l'ensemble des machines virtuelles, des conteneurs et des fonctions sans serveur.

Plateforme de protection des applications natives Cloud (CNAPP)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les solutions CNAPP incluent les fonctions des outils CSPM et CWPP, en plus d'autres outils Cloud spécifiques, comme les outils de gestion des droits d'accès à l'infrastructure Cloud (CIEM). Il s'agit en fait d'un guichet unique pour la sécurité du Cloud.

Gestion de la surface d'attaque externe (EASM)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Contrairement aux pirates informatiques, les organisations négligent souvent de prendre en compte la « surface d'attaque externe », c'est-à-dire l'ensemble des actifs tournés vers Internet. Les outils EASM identifient tous les actifs pouvant être découverts sur Internet, notamment les domaines, les adresses IP et les ports ouverts, ainsi que les expositions associées. Les organisations connaissent ainsi l'angle de vue des pirates. Ces outils peuvent aussi servir à identifier de façon non invasive les actifs et expositions tournés vers Internet des tiers avec lesquels votre organisation interagit, comme les fournisseurs et les cibles d'acquisition.

Services de protection contre les risques numériques (DRPS)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

La technologie DRPS identifie les risques numériques associés aux actifs d'entreprise compromis qui ne sont pas considérés comme des actifs IT conventionnels. En effet, ils peuvent affecter la marque, la réputation ou la sécurité de l'organisation. Il s'agit notamment des domaines, des informations d'authentification, de la propriété intellectuelle et des informations de carte bancaire. Ces solutions offrent des fonctions de surveillance des expositions pour l'Open Web, le Deep Web, le Dark Web et les réseaux sociaux, ainsi que des fonctions de remédiation pour les corriger.

Gestion de la surface d'attaque des cyberactifs (CAASM)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Les outils CAASM consolident les données sur vos actifs et les données d'exposition collectées par les outils de gestion des actifs et de la sécurité via des intégrations API (les outils CAASM n'ont pas de fonctions natives d'analyse). Ces données sont mises en corrélation pour créer une image complète des actifs et des expositions de l'organisation.

Gestion de la posture de sécurité SaaS (SSPM)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les outils SSPM analysent et évaluent en continu les paramètres de sécurité et les configurations des applications SaaS (Logiciel comme service). Ils identifient ainsi les vulnérabilités et erreurs de configuration potentielles. Ils emploient aussi des fonctions automatisées de remédiation pour corriger les problèmes de sécurité et garantir l'application de bonnes pratiques.

Tests de sécurité des applications statiques (SAST)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Les outils SAST recherchent les vulnérabilités de sécurité dans le code sans avoir besoin d'exécuter celui-ci. Ils peuvent être utilisés dès le début du cycle de vie de développement du logiciel (SDLC), car ils ne nécessitent pas que l'application soit exécutable.

Tests dynamiques de sécurité des applications (DAST)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Les outils DAST analysent les applications exécutables pour identifier les vulnérabilités et faiblesses de sécurité. Les tests dynamiques de sécurité des applications se déroulent généralement lors de la phase de test du cycle SDLC ou même dans des environnements de production. Ils garantissent que les applications sont sûres dans les conditions d'exécution actuelles.

Tests de sécurité des applications mobiles (MAST)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Les outils MAST combinent analyse statique, analyse dynamique et tests d'intrusion en vue d'identifier les vulnérabilités des applis mobiles sur les plateformes comme Android et iOS.

Analyse de la composition des logiciels (SCA)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Les outils SCA identifient les composants Open Source dans une base de code, puis comparent ces composants aux bases de données des vulnérabilités connues afin de trouver les éventuels problèmes de sécurité ou exploitations connues.

Solutions de gestion des identités et des accès (IAM)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Les outils IAM servent principalement à gérer en toute sécurité les identités utilisateur, et à contrôler l'accès aux informations, applications et réseaux critiques de l'organisation. En matière de gestion de l'exposition, les outils IAM aident à brosser un tableau de la surface d'attaque liée aux identités. Ils conservent des données sur l'identité et les accès (profils utilisateur, informations d'authentification, rôles et permissions, par exemple). Certains de ces outils fournissent aussi des données sur les risques comme les tentatives de connexion, les schémas d'accès et les activités suspectes.

Fournisseur d'identités (IdP)

Visibilité	X
Priorisation	
Validation	
Remédiation	

L'IdP est un composant de l'IAM. Les solutions IdP se concentrent surtout sur la vérification de l'identité des utilisateurs et la fourniture de services d'authentification. Dans les situations où une offre IAM complète est impossible à obtenir ou indisponible, vous pouvez utiliser une solution IdP pour disposer d'une bonne visibilité sur la surface d'attaque liée aux identités.

Prévention des pertes de données (DLP)

Visibilité	X
Priorisation	
Validation	
Remédiation	

Les outils DLP identifient les données sensibles qui nécessitent une protection, comme les informations personnelles, les données financières ou la propriété intellectuelle. Ils surveillent la façon dont ces données sont utilisées et consultées, à la fois dans l'organisation et en dehors. Ils peuvent aussi générer des alertes et des rapports si une activité suspecte est détectée.

Gestion de la posture de sécurité des données (DSPM)

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Un produit DSPM identifie l'endroit où sont stockées vos données, qu'il s'agisse de bases de données, de services Cloud ou d'autres emplacements. Il évalue ensuite les risques associés à ces données, comme les vulnérabilités, les erreurs de configuration ou les contrôles d'accès trop laxistes. Ce type de produit fournit aussi des recommandations et des outils pour corriger les problèmes de sécurité et améliorer la sécurité globale des données.

Produits de protection des API

Visibilité	X
Priorisation	
Validation	
Remédiation	X*

Les produits de protection des API découvrent et inventorient les API (interfaces de programmation d'application) de l'organisation. Ils fournissent aussi les listes des remédiations recommandées pour les expositions des API.

*Les produits de protection des API offrent souvent des conseils de remédiation, mais aucune action concrète. À la place, ils vous recommandent des actions manuelles.

Outils de posture de sécurité des API

Visibilité	X
Priorisation	
Validation	
Remédiation	X*

Les outils de posture de sécurité des API identifient et cartographient automatiquement toutes les API d'un environnement, y compris les API non documentées ou fantômes. Ils utilisent aussi des analyses de vulnérabilités statiques et dynamiques pour détecter les vulnérabilités et autres problèmes de sécurité. Ils fournissent ensuite des recommandations de remédiation pour aider les organisations à corriger ces problèmes et à améliorer la sécurité globale des API.

*Les outils de posture de sécurité des API fournissent souvent des conseils de remédiation, sans toutefois proposer des actions de remédiation. À la place, ils vous recommandent des actions manuelles.

Priorisation

Les outils de priorisation récupèrent les données sur vos actifs et les données d'exposition collectées à partir des outils de visibilité, et les transforment en informations exploitables. Ils ne se contentent pas de vous montrer ce qui existe, mais vous aident à déterminer ce qu'il convient de faire face aux informations obtenues. Comme dit l'adage, vous ne pouvez pas protéger ce que vous ne voyez pas.

Notez que certains fournisseurs d'outils de visibilité affirment que leurs outils fournissent des fonctions de priorisation et c'est le cas, jusqu'à un certain point. De nombreux outils de visibilité peuvent aider à prioriser la remédiation des expositions dans leur domaine spécifique, mais cela n'est pas valable pour toutes les expositions de la surface d'attaque d'une organisation. Par exemple, les outils EASM priorisent uniquement les expositions associées aux actifs tournés vers l'extérieur.

Plateforme d'évaluation de l'exposition (EAP)

Visibilité	X
Priorisation	X
Validation	
Remédiation	X

Les plateformes EAP sont des produits émergents sur le marché de la gestion de l'exposition. Bien que la gestion de l'exposition combine des technologies préexistantes, les EAP ont été conçues spécialement pour intégrer des fonctions dédiées à la gestion de l'exposition. Ces plateformes offrent une visibilité sur les actifs et les expositions de toute la surface d'attaque, que ces données soient découvertes par des fonctions de scan natives ou importées d'outils tiers. En outre, elles priorisent des opérations de remédiation de l'exposition tenant compte de la criticité des actifs et du contexte de l'organisation. Enfin, elles sont capables d'orchestrer ou d'exécuter ces activités.

Gestion des vulnérabilités basée sur les risques (RBVM)

Visibilité	X
Priorisation	X
Validation	
Remédiation	

Comme leur nom l'indique, les outils RBVM priorisent les vulnérabilités pour effectuer une remédiation en fonction des risques. Ils récupèrent et consolident les résultats des scanners et autres outils de sécurité, puis les comparent à des points de données comme la threat intelligence et la criticité des actifs. Cela aide les organisations à établir un plan d'attaque en toute connaissance de cause. Certains offrent aussi des fonctions natives d'analyse de l'exposition.

Gestion de la posture de sécurité des applications (ASPM)

Visibilité	X
Priorisation	X
Validation	
Remédiation	

Les outils ASPM sont en fait des outils RBVM utilisés pour la sécurité des applications. Ils collectent les données sur les actifs et les données d'exposition à partir des scanners d'applications (ex. : SAST, DAST, SCA, conteneur). Ces données sont ensuite comparées à des points de données comme la threat intelligence et la criticité des actifs, afin de prioriser les opérations de remédiation de l'exposition. Certains fournisseurs combinent des fonctions RBVM et ASPM pour offrir à leurs clients une vue unifiée des cyber-risques sur toute leur surface d'attaque. Des fonctions natives d'analyse de l'exposition (SAST, notamment) peuvent aussi être intégrées dans les outils ASPM.

Threat intelligence (Intelligence des menaces)

Visibilité	
Priorisation	X
Validation	
Remédiation	

Les produits d'intelligence des menaces fournissent des informations sur le paysage des menaces dans son ensemble. Contrairement aux autres produits de priorisation cités dans ce document, ils ne traitent pas les données propres à l'environnement d'une organisation. Au lieu de cela, ils fournissent une vue d'ensemble qui permet aux équipes Sécurité de proactivement prioriser les menaces potentielles avant qu'elles ne soient identifiées dans l'environnement de l'organisation.

Validation

La validation sert à vérifier si les priorités sont bien définies. En vérifiant la façon dont des attaquants potentiels pourraient réellement exploiter une exposition identifiée, et la façon dont les systèmes de surveillance et de contrôle réagiraient, la validation aide l'organisation à déterminer les expositions qu'il faut vraiment corriger pour que son niveau de risque reste en accord avec son appétence au risque.

La validation peut être réalisée à l'aide de technologies AEV (Validation de l'exposition contradictoire) ou de processus manuels externalisés auprès d'un prestataire ou exécutés par des équipes internes. Pour des résultats optimaux, il convient de combiner différentes méthodes de validation.

Quelle que soit la méthode de validation choisie, il est recommandé de confier cette tâche à un intervenant distinct de celui en charge de la priorisation afin de garantir des résultats impartiaux. La validation, c'est comme obtenir un deuxième avis avant de subir une opération chirurgicale.

Analyse du trajet d'attaque (APA)

Visibilité	
Priorisation	
Validation	X
Remédiation	

Les outils d'analyse du trajet d'attaque (APA) cartographient visuellement les trajets que des pirates pourraient emprunter pour se déplacer dans l'environnement d'une organisation. Ils permettent aux équipes de sécurité d'identifier les « trajets » qu'un cyberattaquant pourrait exploiter pour mener une attaque. Ils mettent également en évidence les les expositions qui se terminent en impasses non exploitables.

Simulation de fuites de données et d'attaques (BAS)

Visibilité	
Priorisation	
Validation	X
Remédiation	

Les outils BAS vérifient en continu l'exposition d'une organisation en simulant toute une variété de cyberattaques. Contrairement aux opérations manuelles de Red Teaming et aux tests d'intrusion, les logiciels BAS offrent une approche entièrement automatisée de la validation.

Red teaming

Visibilité	
Priorisation	
Validation	X
Remédiation	

Le Red Teaming consiste à simuler des cyberattaques réalistes par un groupe de hackers éthiques, appelé « Red Team ». Leur mission est de mettre à l'épreuve les défenses d'une organisation afin d'identifier ses vulnérabilités et d'évaluer l'efficacité de ses mesures de sécurité.

Red Teaming automatisé en continu (CART)

Visibilité	
Priorisation	
Validation	X
Remédiation	

Alors qu'avec le Red Teaming, des hackers éthiques simulent manuellement des cyberattaques, les outils CART automatisent ces simulations. Ces tests fréquents réalisés en temps réel offrent une solution plus évolutive et économique. De plus, contrairement aux outils BAS qui vérifient si les contrôles de sécurité sont efficaces contre les méthodes d'attaque connues, les outils CART se concentrent sur la détection et l'exploitation sécurisée des vulnérabilités dans l'objectif d'évaluer si et comment un pirate pourrait contourner les défenses de l'organisation.

Tests d'intrusion

Visibilité	
Priorisation	
Validation	X
Remédiation	

Tout comme le Red Teaming, les tests d'intrusion impliquent des hackers éthiques qui simulent des attaques sur les systèmes de l'organisation. Cependant, la principale différence réside dans leur objectif : les tests d'intrusion se concentrent spécifiquement sur la détection et l'exploitation des vulnérabilités, tandis que le Red Teaming évalue la posture de sécurité globale de l'organisation. Par ailleurs, il est fortement recommandé de demander les résultats des tests d'intrusion de vos fournisseurs, partenaires et autres tiers, car leur surface d'attaque est une sous-partie de la vôtre.

Tests d'intrusion automatisés

Visibilité	
Priorisation	
Validation	X
Remédiation	

Comme son nom l'indique, un logiciel de tests d'intrusion automatisés exécute automatiquement ces tests pour les réaliser plus rapidement et plus régulièrement qu'avec une méthode manuelle.

Tests d'intrusion comme service (PTaaS)

Visibilité	
Priorisation	
Validation	X
Remédiation	

Le PTaaS est un modèle basé dans le Cloud, qui permet aux organisations d'accéder à des services de tests d'intrusion à la demande. Les offres PTaaS combinent des tests automatisés et manuels. Le processus de test étant géré par les fournisseurs PTaaS, les organisations peuvent régulièrement évaluer leur sécurité sans avoir besoin d'une équipe d'experts de sécurité en interne.

Bug Bounty (Prime aux bugs)

Visibilité	
Priorisation	
Validation	X
Remédiation	

Certaines organisations encouragent des hackers éthiques à trouver et à divulguer de façon responsable les vulnérabilités de leurs systèmes, logiciels ou sites Web. Elles offrent des récompenses ou des reconnaissances pour ces informations, ce qui en fait une vraie « chasse ou prime aux bugs ».

Cyber range

Visibilité	
Priorisation	
Validation	X
Remédiation	

Un cyber range est un environnement virtuel qui permet aux organisations de simuler des attaques réelles et de pratiquer leur réponse aux incidents de sécurité dans un espace sandbox contrôlé.

Remédiation

La remédiation constitue l'étape finale du processus de gestion de l'exposition. Une fois les expositions prioritaires identifiées en fonction de votre appétence au risque, les outils de remédiation vous aident à les corriger.

Gestion des correctifs

Visibilité	X
Priorisation	
Validation	
Remédiation	X

Les outils de gestion des correctifs appliquent des mises à jour ou des correctifs aux logiciels pour éliminer les vulnérabilités ou améliorer leur fonctionnement. Certains offrent aussi des fonctions de découverte, qui garantissent une bonne visibilité sur les systèmes d'exploitation et les applications tiers.

Gestion des configurations

Visibilité	
Priorisation	
Validation	
Remédiation	X

Les outils de gestion des configurations automatisent le processus de maintenance et d'application de configurations système cohérentes. Cette cohérence garantit que tous les périphériques et systèmes d'un environnement IT sont configurés et fonctionnent dans le respect des stratégies de sécurité définies et des meilleures pratiques.

À propos d’Ivanti

Ivanti élimine les barrières entre l’IT et la Sécurité pour favoriser l’essor de l’Everywhere Work. Ivanti a créé la première plateforme technologique spécialement conçue pour les DSI et les CISO (DSSI/RSSI). Elle offre aux équipes IT et Sécurité des solutions logicielles complètes et évolutives, adaptées aux besoins des entreprises, afin de faciliter, sécuriser et améliorer l’expérience collaborateur. La plateforme Ivanti repose sur Ivanti Neurons, couche intelligente d’hyperautomatisation à l’échelle du Cloud qui permet une réparation proactive, garantit une sécurité intuitive dans toute l’entreprise et fournit une expérience collaborateur qui ravit les utilisateurs. Plus de 40 000 clients, dont 85 des entreprises Fortune 100, font confiance à Ivanti pour relever leurs défis grâce à ses solutions de bout en bout. Chez Ivanti, nous nous efforçons de créer un environnement où tous les points de vue sont écoutés, respectés et valorisés. Nous nous engageons aussi pour un avenir plus durable pour nos clients, nos partenaires, nos collaborateurs et la planète. Pour en savoir plus, visitez le site www.ivanti.fr et suivez @GoIvanti.

ivanti

Pour en savoir plus ou pour contacter Ivanti, visitez le site www.ivanti.fr.