Checklist Surface d'attaque

Les surfaces d'attaque modernes sont chaque jour plus vastes et plus complexes. À chaque ajout d'un cyberactif à votre environnement, de nouveaux vecteurs d'attaque potentiels apparaissent.

Notre checklist vous aidera à déterminer les éléments de votre surface d'attaque qui sont bien pris en compte et ceux manquants de visibilité. Classifiez les éléments comme suit :

- Les connus connus : les cyberactifs identifiés comme faisant partie de votre surface d'attaque.
- Les inconnus connus : les cyberactifs identifiés comme appartenant à votre surface d'attaque, mais sur lesquels vous manquez de visibilité et/ou de contrôle.
- Les inconnus non connus : les cyberactifs dont vous ne savez pas s'ils font ou non partie de votre surface d'attaque.
- N/A : les cyberactifs pour lesquels vous êtes certain à 100 % qu'ils ne font pas partie de votre surface d'attaque.

Cette checklist vous permet de faire le suivi de vos réponses. Vous pourrez les reporter dans la dernière page de ce document (p. 11) pour avoir une vision globale de votre surface d'attaque.

Attention : certains types d'actifs peuvent entrer dans plusieurs catégories (ex. : un périphérique peut être à la fois un périphérique mobile et un périphérique de poste client). Ce n'est pas un problème. L'objectif est d'être aussi exhaustif que possible. Chaque angle mort éliminé réduit le risque qu'un pirate puisse s'infiltrer dans votre environnement.

Périphériques de poste client

Périphériques — fournis par l'entreprise ou appartenant au collaborateur (BYOD) — qui se connectent à un réseau. Il s'agit principalement de périphériques Android, ChromeOS, iOS, Linux, Mac et Windows.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Ordinateurs de bureau
- Ordinateurs portables

Outil(s) de gestion :

- Découverte des actifs IT
- Gestion moderne des périphériques (MDM)
- Gestion unifiée des terminaux (UEM)

Périphériques mobiles

Périphériques de poste client — fournis par l'entreprise ou appartenant au collaborateur (BYOD) — qui se connectent à un réseau généralement par Wi-Fi et sont conçus pour être faciles à transporter. Il s'agit principalement de périphériques Android et iOS.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Smartphones
- Smartwatches
- Tablettes

Outil(s) de gestion :

- Découverte des actifs IT
- Gestion des périphériques mobiles (MDM)
- Gestion moderne des périphériques (MDM)

Périphériques durcis

Périphériques équipés pour résister à des conditions qui endommageraient les périphériques mobiles standard. On les trouve par exemple sur les chantiers de construction, dans les usines et dans les entrepôts. Il s'agit principalement de périphériques Android, iOS et Windows.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Ordinateurs mobiles durcis
- Tablettes durcies
- Dispositifs portatifs durcis

Outil(s) de gestion :

- Découverte des actifs IT
- Gestion des périphériques mobiles (MDM)
- Gestion moderne des périphériques (MDM)

Périphériques IoT (Internet des objets)

Périphériques de poste client non standard, équipés de capteurs et de logiciels leur permettant d'échanger des données avec d'autres périphériques et systèmes sur un réseau ou sur l'Internet public. Selon le cas d'usage, on les appelle également eIoT (Internet des objets d'entreprise), XIoT (Internet étendu des objets), IIoT (Internet des objets industriels) ou IoMT (Internet des objets médicaux).

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Dispositifs de suivi des actifs (ex. : balises RFID)
- Capteurs industriels
- Appareils intelligents (ex. : grille-pains, frigos, ampoules)

Outil(s) de gestion :

- Découverte des actifs IT
- Gestion moderne des périphériques (MDM)
- Outils de sécurité IoT spécialement conçus (divers)
- Gestion unifiée des terminaux (UEM)

Systèmes cyberphysiques (CPS)

Systèmes qui relient des ressources computationnelles et physiques, qui se coordonnent étroitement pour accomplir leur travail.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Systèmes de gestion des bâtiments (BMS)
- Systèmes de contrôle industriel (ICS)
- Technologie opérationnelle (OT)
- Systèmes robotiques

Outil(s) de gestion :

- Découverte des actifs IT
- Plateformes de protection des systèmes cyberphysiques (CPS)
- Gestion moderne des périphériques (MDM)

Périphériques réseau

Périphériques qui permettent les communications et les interactions entre les autres périphériques d'un réseau. Ils constituent l'infrastructure réseau.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Routeurs
- Commutateurs
- Pare-feux
- Points d'accès

Outil(s) de gestion :

- Outils de découverte réseau

Serveurs/périphériques de centre de données

Périphériques qui assurent le traitement, le stockage et la diffusion des données. Ils constituent la colonne vertébrale de services comme les communications par e-mail et les sites Web.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Serveurs (ex. : serveurs d'e-mail, serveurs d'impression, serveurs Web)
- Systèmes de stockage

Outil(s) de gestion :

- Découverte des actifs IT
- Gestion moderne des périphériques (MDM)
- Gestion unifiée des terminaux (UEM)

Périphériques à fonction fixe

Périphériques conçus pour répondre à un cas d'usage spécifique. Souvent en contact avec le client.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Systèmes de point de vente (POS)
- Kiosques en libre-service

Outil(s) de gestion :

- Découverte des actifs IT
- Gestion moderne des périphériques (MDM)
- Gestion unifiée des terminaux (UEM)

Services Cloud

Le Cloud computing fournit un accès à la demande à des ressources informatiques sur Internet. Son orchestration passe par un Cloud privé (aussi appelé « Cloud interne » ou « Cloud d'entreprise »), un Cloud public, un Cloud hybride ou un environnement multi-cloud.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Conteneurs Cloud
- Solutions Cloud de stockage des données
- Cloud privé sous-jacent aux ressources informatiques (ex. : UC et stockage)
- Services de Cloud public (ex. : AWS, plateforme Google Cloud, service Cloud Microsoft Azure)

Outil(s) de gestion :

- Plateforme de protection des applications natives de Cloud (CNAPP)
- Gestion du niveau de sécurité Cloud (CSPM)
- Plateforme de protection des charges de traitement Cloud (CWPP)

Application SaaS (Logiciel comme service)

Applications sur demande, déployées via un modèle de services informatiques Cloud, où le fournisseur de services gère toute l'infrastructure sous-jacente.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Microsoft 365
- Salesforce
- Slack

Outil(s) de gestion :

- Gestion du niveau de sécurité SaaS (SSPM)

Code

Série d'instructions écrites dans un langage de programmation, qui indiquent à l'ordinateur ce qu'il doit faire. C'est le composant de base des logiciels.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Code de logiciels personnalisés développés pour un usage en interne ou par les clients
- Code de logiciels propriétaires développés pour la vente

Outil(s) de gestion :

- Scanners de conteneur
- Tests de sécurité des applications dynamiques (DAST)
- Tests de sécurité des applications mobiles (MAST)
- Scanners de logiciel Open Source (OSS)
- Analyse de la composition des logiciels (SCA)
- Tests de sécurité des applications statiques (SAST)

Logiciels et applications prêts à l'emploi (COTS)

Programmes informatiques achetés et utilisés par une organisation.
Ils peuvent être achetés chez un tiers ou être préinstallés sur un périphérique.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Systèmes d'exploitation (ex. : Windows, macOS, Linux)
- Suites de productivité (ex. : Microsoft Office)
- Applications tierces (ex. : Zoom)

Outil(s) de gestion :

- Découverte des actifs IT
- Gestion des correctifs

Actifs tournés vers Internet

Cyberactifs directement accessibles depuis l'Internet public. Ces actifs constituent ce que l'on appelle la « surface d'attaque externe ».

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Certificats/domaines
- Environnements Dev et QA (adresses IP)
- Sites Web (serveurs Web)

Outil(s) de gestion :

- Gestion de la surface d'attaque externe (EASM)

Actifs numériques

Regroupe différents actifs, comme les données du Dark Web et les réseaux sociaux, qui ne sont pas considérés comme des actifs IT conventionnels mais peuvent quand même affecter la marque, la réputation ou la sécurité de l'organisation.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Forums en ligne
- Comptes sur les réseaux sociaux

Outil(s) de gestion :

- Protection contre les risques numériques (DRP)

Identités et accès

Le terme « identité » désigne l'identité numérique d'une personne associée à une organisation : nom, intitulé de poste, responsable, subordonnés directs, numéro de téléphone et autres informations du même type. Le terme « accès » correspond aux ressources et données que cette personne est autorisée à voir et/ou modifier, en fonction de facteurs comme son intitulé de poste et ses droits de sécurité.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Identités utilisateur
- Niveaux d'accès

Outil(s) de gestion :

- Gestion des identités et des accès (IAM)
- Fournisseur d'identités (IdP)

Données

Données générées ou collectées par une organisation pour la planification, la prise de décision et les opérations quotidiennes.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Informations de carte bancaire des clients
- Propriété intellectuelle (IP)
- Dossier médical des patients
- Informations d'identification personnelle (PII) (ex. : coordonnées des clients)

Outil(s) de gestion :

- Prévention des pertes de données (DLP)
- Gestion du niveau de sécurité des données (DSPM)

API (Interfaces de programmation d'application)

Ensembles de règles et de protocoles qui permettent à différentes applications logicielles de communiquer entre elles.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- API HubSpot
- API Salesforce
- API Slack

Outil(s) de gestion :

- Produits de protection des API
- Outils de niveau de sécurité des API

Actifs tiers

Les organisations modernes interagissent souvent étroitement avec d'autres organisations, partageant des systèmes et des données. Lorsque deux parties sont aussi intimement liées, leurs surfaces d'attaque le sont également.

Connus connus	☐
Inconnus connus	☐
Inconnus non connus	☐
N/A	☐

Exemples :

- Site Web d'un partenaire revendeur
- Infrastructure Cloud d'une agence de marketing
- Environnement de développement d'un partenaire de la supply chain

Outil(s) de gestion :

- Gestion de la surface d'attaque externe (EASM)

	Visibilité			
Catégorie d'actifs	Connus connus	Inconnus connus	Inconnus non connus	N/A
Périphériques de poste client	☐	☐	☐	☐
Périphériques mobiles	☐	☐	☐	☐
Périphériques durcis	☐	☐	☐	☐
Périphériques IoT (Internet des objets)	☐	☐	☐	☐
Systèmes cyberphysiques (CPS)	☐	☐	☐	☐
Périphériques réseau	☐	☐	☐	☐
Serveurs/périphériques de centre de données	☐	☐	☐	☐
Périphériques à fonction fixe	☐	☐	☐	☐
Services Cloud	☐	☐	☐	☐
Application SaaS (Logiciel comme service)	☐	☐	☐	☐
Code	☐	☐	☐	☐
Logiciels et applications propriétaires (COTS)	☐	☐	☐	☐
Actifs tournés vers Internet	☐	☐	☐	☐
Actifs numériques	☐	☐	☐	☐
Identités et accès	☐	☐	☐	☐
Données	☐	☐	☐	☐
API (Interfaces de programmation d'application)	☐	☐	☐	☐
Relations avec les tiers	☐	☐	☐	☐

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 ivanti.fr et suivez @GoIvanti.

ivanti

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