Cet onglet présente une liste d
Chaque scénario est décrit à tr
- un intitulé (ex. Infection par u
- une description générique du
- les impacts potentiels,
- les actifs potentiellement con
- une indication précisant si le

Les scénarios identifiés comm
en sélectionnant les scénarios
environnement technique, leur

L'objectif n'est pas l'exhaustivi

Scénario
Infection par un malware avec propagation sur le réseau interne
Phishing exploitant l'ingénierie sociale pour compromettre les comptes agents
Agent interne provoquant la dégradation de ressources ou l'exfiltration de données

Exfiltration de données via un compte compromis ou un service exposé mal configuré
Attaque sur un fournisseur ou prestataire de services (chaîne d'approvisionnement)
Attaque sur un portail web public par déni de service (DDoS)
Indisponibilité d'un site ou d'une infrastructure physique vitale suite à un sinistre
Intrusion dans un système suite à l'exploitation d'une vulnérabilité technique
Infiltration sophistiquée et persistante visant à accéder à des informations sensibles

Perte, vol ou compromission d'un équipement mobile à usage professionnel

e scénarios de risques génériques illustrant les principaux risques de sécurité suscepti
avers :
n malware avec propagation sur le réseau interne, attaque sur un fournisseur ou presta
scénario,

ıcernés (systèmes, données, infrastructures, etc.),
scénario est recommandé ou optionnel dans le cadre de l'utilisation de cette liste.

e « optionnels » correspondent à des risques qui peuvent ne pas être pertinents pour to
les plus adaptés à leur contexte, en écartant certains scénarios optionnels ou en ajout
s missions ou leur exposition aux menaces.

té, mais la représentation réaliste des risques majeurs pour l'entité.

Description générique du scénario de risque
Introduction puis exécution d'un code malveillant (ransomware, trojan, worm, spyware, RAT, etc.) sur un poste, un serveur ou un environnement d'administration, permettant à un attaquant de compromettre un premier système puis de se propager latéralement au sein du réseau interne de l'administration. **Vecteurs d'attaque possibles :** pièces jointes/URL malveillantes,usage d'un compte compromis, exploitation de vulnérabilités, mise à jour logicielle compromise, supports amovibles, contournement de protections, etc.
Campagne visant à tromper des agents pour obtenir leurs identifiants, les inciter à exécuter du code ou à réaliser une action nuisible (paiement frauduleux, divulgation d'informations). **Vecteurs d'attaque possibles :** courriels ciblés, SMS, messages instantanés, faux portails d'authentification, usurpation d'identité (spear-phishing), appels téléphoniques frauduleux (vishing), scénarios d'urgence fictive, etc.
Risque lié à un collaborateur ou prestataire disposant d'accès légitimes qui, de manière intentionnelle ou accidentelle, exfiltre, altère ou détruit des ressources. **Vecteurs d'attaque possibles :** copie de données sur supports externes, abus de privilèges, divulgation volontaire, modifications non autorisées, mauvaise configuration, etc.

Accès frauduleux à un compte ou exploitation d'un service exposé insuffisamment sécurisé permettant l'extraction non autorisée d'informations (vol, copie, transfert illicite). **Vecteurs d'attaque possibles :** compromission de comptes, API mal sécurisée, serveur mal configuré, absence de contrôle d'accès, brute forcing, absence de supervision ou de journalisation suffisante, etc.
Compromission d'un service tiers, d'un prestataire, d'un logiciel ou d'un composant intégré dans l'environnement de l'entité, permettant l'introduction d'une menace dans le système d'information de l'entité. **Vecteurs d'attaque possibles :** mises à jour malveillantes, certificats compromis, dépendances tierces compromises, accès prestataires (VPN/SSO) exploités, etc.
Attaque visant à saturer ou à épuiser des ressources (bande passante, connexion, CPU, sessions applicatives) pour rendre indisponibles un ou plusieurs services accessibles en ligne (sites, portails, API, services cloud). **Vecteurs d'attaque possibles :** botnets, attaques par amplification (DNS/NTP/CLDAP), attaques applicatives (HTTP flood), exploitation de vulnérabilités pour provoquer des crashs de services web.
Sinistre impactant un datacenter, un bâtiment ou une salle technique, entraînant une indisponibilité ou une destruction d'équipements ou de locaux. **Causes et vecteurs possibles :** incendie, inondation, panne électrique prolongée, sabotage, défaillance de climatisation, accès physique non autorisé, événements climatiques majeurs.
Exploitation d'une vulnérabilité connue ou inédite sur un système, un serveur, une application ou un composant réseau permettant une intrusion non autorisée. **Vecteurs d'attaque possibles :** vulnérabilités non corrigées, mauvaise configuration, version obsolète, exposition involontaire de services sur internet, défauts de configuration de sécurité, exploitation d'une vulnérabilité de type 0-day.
Attaque ciblée et sophistiquée, souvent menée par un acteur étatique ou un groupe organisé, visant à établir une présence durable, discrète et persistante dans le système d'information pour exfiltrer des données stratégiques, espionner les activités ou préparer des actions de sabotage futur. **Vecteurs d'attaque possibles :** spear-phishing ciblé sur des profils à haute responsabilité, exploitation d'une vulnérabilité de type 0-day, compromission de matériel ou d'infrastructures réseau, utilisation d'infrastructures de rebond pour masquer l'origine de l'attaque.

Perte, vol ou compromission, d'un smartphone, d'une tablette ou d'un ordinateur portable appartenant à l'entité ou utilisé en mode BYOD/télétravail, contenant des données professionnelles ou des accès au SI.
Vecteurs d'attaque possibles : vol à l'arraché ou dans un véhicule, perte par négligence dans les transports ou lieux publics, vol ciblé lors de déplacements à l'étranger, absence de chiffrement des supports de stockage, absence de verrouillage de session.

bles d’affecter une entité publique.

taire de services, etc.),

utes les entités. Celles-ci peuvent donc adapter cette liste
ant des scénarios complémentaires selon leur

Impacts potentiels	Actifs potentiellement concernés
Chiffrement ou suppression de données, indisponibilité des applications métiers, coût de restauration et éventuelle rançon, perte ou corruption de sauvegardes non isolées, interruption des services métiers vitaux, impact réputationnel et juridique, etc.	Postes de travail, serveurs de fichiers, serveurs applicatifs, bases de données, systèmes de sauvegarde (s’ils sont accessibles), réseaux internes, environnements virtualisés, services cloud et conteneurs, etc.
Compromission de comptes d'agents, fraude administrative ou financière, installation de malware, accès non autorisé à des informations sensibles, utilisation du compte compromis pour mener d’autres attaques internes, perte de confiance des usagers et partenaires, perturbation de services métiers, etc.	Boîtes mail, comptes utilisateurs, systèmes d’authentification (LDAP/AD), portails métiers, données personnelles et documents administratifs, outils collaboratifs et plateformes cloud, etc.
Perte, destruction ou diffusion de données sensibles, atteintes à la continuité des services, coûts juridiques, perte de confiance interne et externe, impact réputationnel, etc.	Données sensibles, bases de données des usagers, serveurs de fichiers, environnements de production, comptes à privilèges, dispositifs de stockage externes, etc.

Divulgation de données sensibles, perte de confidentialité, risques juridiques, exploitation des données à des fins malveillantes, atteinte aux missions de l'administration, perte de confiance des citoyens, etc.	Bases de données, applications web, services cloud, API exposées, outils collaboratifs, comptes agents, archives numériques.
Indisponibilité de services critiques dépendants du prestataire, introduction de malware dans le SI (ex. via une mise à jour compromise), exfiltration de données via les accès du fournisseur, perte de confiance des partenaires et usagers, impact réputationnel et juridique.	Logiciels tiers, gestionnaires de paquets, environnements de déploiement, comptes et accès fournisseurs, intégrations SSO/OAuth, certificats et clés de signature.
Indisponibilité temporaire ou prolongée des services en ligne, blocage des communications externes, perte de confiance des usagers, dommages réputationnels, masquage d'une autre attaque (diversion), perturbation des partenaires, etc.	Équipements réseau (routeurs, pare-feu), serveurs web, applications en ligne, portails d'authentification, services cloud exposés, liaisons internet.
Indisponibilité totale ou partielle des services et applications métiers sur site, perte définitive de données (en cas de destruction des sauvegardes locales), coûts de reconstruction matérielle très élevés, etc.	Datacenters, équipements réseaux, systèmes d'alimentation (onduleurs, TGBT, groupes électrogènes), serveurs, postes de travail, archives physiques, infrastructures vitales.
Accès non autorisé à des données ou systèmes, installation de malware, mouvement latéral dans le SI, compromission durable, atteinte à l'intégrité ou à la continuité de service, etc.	Serveurs, bases de données, applications web, équipements réseau, services exposés, environnements virtualisés.
Espionnage étatique, exfiltration de données stratégiques ou de dossiers sensibles (état civil, données fiscales, secrets défense), altération discrète de bases de données, maintien d'un accès dormant pour une activation future, décrédibilisation des institutions, etc.	Postes de travail des décideurs et agents stratégiques, serveurs de fichiers, Active Directory, systèmes d'archivage numérique, bases de données, outils de communication chiffrés.

Accès non autorisé aux emails et documents internes, usurpation d'identité de l'agent, accès au réseau interne via les VPN enregistrés, fuite de données, coût de remplacement du matériel, etc.	Ordinateurs portables, smartphones et tablettes, clés USB et disques durs externes, certificats d'authentification (cartes LuxTrust d'un agent), accès VPN et sessions de messagerie.

Type de scénario
Recommandé
Recommandé
Recommandé

Recommandé
Recommandé
Optionnel
Optionnel
Optionnel
Optionnel

Optionnel