Risques pour les opérations mondiales de l'UNICEF

---

1. Inventaire des actifs avec quantités et emplacements spécifiques

1.1 Actifs matériels

- **Ordinateurs portables et de bureau**:
- **Série Dell Latitude (5000, 7000, 9000)** et **Série XPS**:
  - **Montant**: ~12 000 unités.
  - **Utilisation principale**: Personnel administratif, opérations de bureau, fonctions générales des employés.
  - **Répartition géographique**:
    - **Site**: **New York**, **Ginébre**, **Nairobi**, **Bangkok**, **Caire**
    - **Bureaux régionaux**: Dans des endroits clés comme **Mexique**, **Abuja (Nigéria)**, **Bangladesh**, **Zimbabwe**, et **Afrique du Sud**.
    - **Autres emplacements**: Bureaux nationaux en Asie, Europe et Amérique latine.
- **HP EliteBook** et **HP ProBook**:
  - **Montant**: ~10 000 unités.
  - **Utilisation principale**: Personnel de terrain, personnel opérationnel dans les zones à risque, agents de santé, d'éducation et d'intervention d'urgence.
  - **Répartition géographique**:
    - **Zones de conflit**: **Soudan du Sud**, **Syrie**, **Afghanistan**, **Yémen**, **Haïti**, **Colombie**.
    - **Régions en développement ** : **Bangladesh**, **Éthiopie**, **Nigeria**.
    - **Opérations sur le terrain**: Dans les zones volatiles ou isolées avec des besoins urgents d’exécution de programmes.
- **Apple MacBook Pro**:
  - **Montant**: ~3 000 unités.
  - **Utilisation principale**: Direction générale, développeurs informatiques, équipes spécialisées (recherche, analyse de santé, gestion de crise).
  - **Répartition géographique**: **New York**, **Ginébre**, **Singapour**, et **Siège social (bureaux régionaux)**.
- **Lenovo ThinkPad**:
  - **Montant**: ~2 000 unités.
  - **Utilisation principale**: Travail basé sur des projets dans des bureaux de terrain difficiles, en mettant l'accent sur les opérations à distance et temporaires.
  - **Répartition géographique**: Principalement en **Afrique**, **Asie**, et **L'Amérique latine**.

Total d'ordinateurs portables/de bureau: ~25 000 unités.

1.2 Appareils mobiles

- **Apple iPhone 12, 13, 14 Pro Max**:
- **Montant**: ~5 000 unités.
- **Utilisation principale**: Appareils mobiles essentiels pour le personnel de terrain dans les zones éloignées ou à haut risque nécessitant une communication sécurisée en temps réel.

- **Répartition géographique**: **Soudan du Sud**, **Syrie**, **Afghanistan**, **Colombie**, **Yémen**.
- **SamsungGalaxy S20/S21**:
- **Montant**: ~8 000 unités.
- **Utilisation principale**: Communication mobile pour les opérations dans les régions en développement et les environnements d'urgence.
- **Répartition géographique**: **Bangladesh**, **Afrique du Sud**, **Népal**, **Inde**, **Zambie**.
- **Apple iPad (modèles 10.2 et Pro)**:
- **Montant**: ~7 500 unités.
- **Utilisation principale**: Collecte de données et prestation de services en matière d'éducation, de santé et de protection de l'enfance.
- **Répartition géographique**: **Bangladesh**, **Ouganda**, **Haïti**, **Inde**, **Syrie**.

Total des appareils mobiles: ~20 500 unités.

1.3 Périphériques externes (clés USB, disques durs externes)

- **Clés USB (32 Go - 512 Go)** et **Disques durs externes (1 To - 5 To)**:
- **Montant**: ~20 000 unités.
- **Utilisation principale**: Stockage et transfert de données sensibles sur les opérations, la santé et les interventions d'urgence là où la connectivité Internet n'est pas fiable.
- **Répartition géographique**: Principalement utilisé dans **Soudan du Sud**, **Syrie**, **Yémen**, **RDC**, et **Haïti**.
- **Périphériques de stockage en réseau (NAS)**:
- **Montant**: ~500 To de stockage.
- **Utilisation principale**: Sauvegardes de données pour les opérations sur le terrain, sauvegarde des informations critiques lors de crises régionales.
- **Répartition géographique**: Principalement en **Nairobi**, **Bangkok**, **Ginébre**et d'autres bureaux régionaux.

Total des appareils externes: ~20 000 unités.

1.4 Centres de données et serveurs

- **Centres de données physiques**:
- **New York, États-Unis**:
  - **Serveurs**: 3 serveurs physiques, capacité totale de stockage **20 To**.
  - **Utilisation principale**: Stockage et hébergement de données opérationnelles pour les systèmes financiers, données opérationnelles régionales pour l'Amérique du Nord.
- **Genève, Suisse**:
  - **Serveurs**: 2 serveurs physiques, capacité totale de stockage **15 To**.
  - **Utilisation principale**: Stockage de données sanitaires et humanitaires, gestion de programmes Europe et Moyen-Orient.

- **Nairobi, Kenya**:
  - **Serveurs**: 2 serveurs physiques, capacité totale de stockage **10 To**.
  - **Utilisation principale**: Opérations en Afrique de l'Est, y compris des programmes de protection de l'enfance, de santé et d'éducation.
- **Bangkok, Thaïlande**:
  - **Serveurs**: 2 serveurs physiques, capacité totale de stockage **10 To**.
  - **Utilisation principale**: Programmes d'intervention d'urgence en Asie-Pacifique, opérations de secours et stockage de données pour les programmes régionaux.

Total des serveurs physiques: 9 serveurs avec **55 To** de données stockées.

1.5 Infrastructure basée sur le cloud

- **Amazon Web Services (AWS)**:
- **500 instances EC2**: Actif pour les besoins informatiques et informatiques des opérations mondiales.
- **250 To de stockage S3**: Pour stocker les données opérationnelles, les informations sur les donateurs, les données sur la santé des enfants et le matériel pédagogique.
- **75 bases de données RDS**: Utilisé à l'échelle mondiale pour gérer les systèmes opérationnels de l'UNICEF (systèmes financiers, programmatiques et de ressources humaines).
- **MicrosoftAzure**:
- **25 000 utilisateurs actifs**: Géré via Azure Active Directory, représentant le personnel de l'UNICEF dans le monde entier.
- **30 bases de données SQL**: Pour héberger les systèmes d’exploitation critiques, y compris les applications de ressources humaines, financières et programmatiques.
- **Stockage blob de 50 To**: Utilisé pour la reprise après sinistre et pour stocker les données sensibles du programme, y compris les dossiers d'intervention d'urgence et les données de protection de l'enfance.
- **Google Cloud**:
- **100 To de stockage cloud**: Pour la recherche et le stockage de données, en particulier pour les données sur la santé des enfants et l'éducation tout au long **Asie-Pacifique**.

---

2. Actifs logiciels

2.1 Applications développées par l'UNICEF

- **Signalez-nous**:
- **Utilisateurs actifs**: ~200 000 utilisateurs.
- **Utilisation principale**: Un outil pour impliquer les jeunes et collecter des données critiques en temps réel auprès d'un plus grand nombre **50 pays** en Afrique, en Asie et en Amérique latine.
- **Soins en communication**:
- **Utilisateurs actifs**: ~15 000 utilisateurs.

- **Utilisation principale**: Application mobile utilisée dans **30+ pays** pour la collecte de données dans les programmes de santé, d'éducation et de protection de l'enfance.
- **force de vente**:
- **Utilisateurs actifs**: ~2 500 utilisateurs.
- **Utilisation principale**: Pour les relations avec les donateurs, la collecte de fonds et la communication, notamment lors de grandes campagnes de collecte de fonds telles que **Je donne mardi**.
- **Sauge intacte**:
- **Utilisateurs actifs**: ~1 000 utilisateurs.
- **Utilisation principale**: Gestion financière et reporting pour suivre les dons, les subventions et les financements gouvernementaux.
- **Promis**:
- **Utilisateurs actifs**: ~500 utilisateurs.
- **Utilisation principale**: Système de logistique et de gestion des actifs, utilisé mondialement par le personnel de terrain pour gérer les approvisionnements.

---

3. Actifs de données

3.1 Données personnelles sensibles

- **Données sur les enfants**:
- **~10 millions d'enregistrements** de données sensibles sur les enfants, les familles et les communautés, couvrant les données sur la santé, l'éducation et l'aide d'urgence.
- **Emplacements de stockage principaux**: AWS, Azure et Google Cloud, avec une infrastructure distribuée dans des bureaux mondiaux.

3.2 Données de recherche

- **Données de recherche annuelles**:
- Recueilli de **5 millions d'enfants** chaque année dans des domaines tels que la santé, l'éducation, la pauvreté et le développement.
- Les données renseignent **Rapports sur la situation des enfants dans le monde**, annuel **évaluations pédagogiques**et d'autres enquêtes humanitaires mondiales.

3.3 Données financières

- **Dons annuels**:
- **~6 milliards de dollars** suivi à l'échelle mondiale en utilisant **force de vente** et **Sauge intacte**.
- **Utilisateurs financiers mondiaux**: ~1 000 utilisateurs financiers dans divers bureaux de pays de l'UNICEF.

---

4. Personnel et partenaires externes

4.1 Employés

- **Nombre total d'employés**: 15 000 collaborateurs répartis sur **190 bureaux de pays** monde.

- **Domaines de travail clés**: Opérations sur le terrain, logistique, santé, éducation, protection de l'enfance, réponse d'urgence et élaboration de politiques.
- **Risques de cybersécurité**: Salariés dans des régions éloignées ou à risque telles que **Soudan du Sud**, **Syrie**, et **Venezuela** Ils peuvent être plus vulnérables aux attaques de phishing ou d'ingénierie sociale.

4.2 Partenaires et fournisseurs tiers

- **Entrepreneurs externes**:
- Des milliers d'entrepreneurs travaillant dans des zones de conflit et d'après-crise, notamment **Soudan du Sud**, **Syrie**, **Afghanistan**, et **Yémen**.
- Les tâches comprennent la coordination des interventions d'urgence, le soutien logistique et les services informatiques.
- **Prestataires de services informatiques**:
- Services informatiques gérés fournis par **AWS**, **Microsoft**, **force de vente**, et **Google**.

---

5. Identification des menaces et analyse d'impact

5.1 Menaces externes

- **Menaces de cybersécurité**:
- **Vol d'identité**: Haut

probabilité de tentatives de phishing, ciblant en particulier le personnel ayant accès aux bases de données et aux systèmes d'exploitation des donateurs.

- **rançongiciel**: Risque accru d'attaques de chiffrement de données, notamment sur les données financières liées aux donateurs ou sur les données de terrain (santé, éducation).
- **Attaques DDoS**: Risque potentiel pour les plateformes de collecte de fonds en ligne pendant les périodes de pointe de dons, comme **Je donne mardi** ou des campagnes de Noël.
- **Violation de données**: Risque élevé dans les zones de conflit, où les infrastructures numériques peuvent être compromises.
- **Catastrophes naturelles**:
- **Inondations, tremblements de terre, ouragans** affectant les centres de données et les bureaux extérieurs, en particulier dans des domaines tels que **Asie du Sud**, **L'Amérique latine**, et **Caraïbes**.

5.2 Menaces internes

- **Menaces internes**: Risque que le personnel interne ou les sous-traitants utilisent potentiellement à mauvais escient ou divulguent des données sensibles, en particulier dans des environnements de crise ou de stress élevé.

- **Erreur humaine**: Perte ou suppression accidentelle de données, notamment en réponse à des urgences ou à des opérations de terrain où le traitement des données est manuel et urgent.

---

6. Évaluation des risques et priorisation

| **Risque** | **Probabilité** | **Impact** | **Évaluation du risque** | **Détails** | |---------- ---------- ---------- ---------- --- -| | **Attaques de phishing** | Élevé | Élevé | **Haut** | Les attaques de phishing sont l'une des menaces de cybersécurité les plus courantes auxquelles sont confrontées les organisations internationales telles que l'UNICEF. Ces attaques exploitent l'erreur humaine pour accéder à des informations sensibles via des e-mails trompeurs ou de faux sites Web. La structure décentralisée de l'UNICEF, avec un grand nombre de bureaux extérieurs dans les zones de conflit et les zones à haut risque, en fait une cible privilégiée pour les cybercriminels. Les campagnes de phishing sont devenues plus sophistiquées, utilisant des tactiques sur mesure, telles que le spear phishing et le BEC (Business Email Compromise), ciblant les cadres supérieurs, le personnel de terrain et les partenaires. Les conséquences peuvent inclure une perte financière, la divulgation de données sensibles (par exemple, informations sur les donateurs, plans d'intervention d'urgence) et une atteinte à la réputation de l'organisation. L'UNICEF doit continuellement mettre à jour ses systèmes de formation, de sensibilisation et de détection. | | **Ransomware/cyberattaques externes** | Moyen | Élevé | **Haut** | La dépendance croissante de l'UNICEF à l'égard des plateformes cloud (par exemple AWS, Azure) et des sous-traitants tiers augmente le risque d'attaques de ransomwares. Ces attaques peuvent paralyser les infrastructures critiques, compromettre les données sensibles et provoquer d'importantes perturbations opérationnelles. Les applications basées sur le cloud utilisées par l'UNICEF pour gérer de vastes ensembles de données (par exemple, données sur la protection de l'enfance, programmes éducatifs, bases de données sur les secours d'urgence) présentent un risque élevé, d'autant plus que les attaquants ciblent souvent les faiblesses des fournisseurs ou prestataires de services tiers. Ce risque est encore exacerbé par la menace d'attaques par déni de service distribué (DDoS), qui peuvent perturber les services en ligne et la disponibilité des données. Dans les zones de conflit, où l'infrastructure de données de l'UNICEF est moins résiliente, les cyberattaques pourraient retarder ou arrêter les opérations humanitaires, ce qui en ferait une priorité absolue en matière d'atténuation. | | **Violation de données** | Élevé | Très élevé | **Haut** | Les violations de données constituent une préoccupation majeure en raison de la nature sensible du travail de l'UNICEF. L'organisation collecte un large éventail d'informations sensibles, notamment des données de santé, des dossiers financiers et des données sur la protection de l'enfance, qui constituent une cible privilégiée pour les acteurs malveillants. Une violation pourrait entraîner la divulgation non autorisée d'informations personnelles identifiables (PII), mettant en danger les populations vulnérables et potentiellement en violation des réglementations en matière de confidentialité telles que le RGPD (Règlement général sur la protection des données). Le recours croissant à des sous-traitants externes, à des partenaires et à des bureaux sur le terrain augmente le nombre de points d'accès pour des violations potentielles, en particulier dans les zones où la cyberhygiène est mauvaise. En cas de non-respect, la confiance entre l'UNICEF, les donateurs et les bénéficiaires pourrait être sérieusement compromise, entraînant une atteinte à la réputation et une perte de financement. | | **Catastrophes naturelles (inondations, tremblements de terre)** | Moyen | Très élevé | **Haut** | Les catastrophes naturelles, telles que les inondations, les tremblements de terre et les ouragans, ont un impact considérable sur les opérations de l'UNICEF, en particulier dans les régions vulnérables et à faible résilience comme les Philippines, Haïti et certaines parties d'Afrique et d'Asie. Ces événements peuvent perturber les chaînes d'approvisionnement, détruire les infrastructures physiques (par exemple, bureaux, entrepôts) et déplacer des millions de personnes, créant ainsi une augmentation de la demande pour les services d'urgence de l'UNICEF. Les catastrophes naturelles présentent également des risques de perte de données ou d'indisponibilité du système si le matériel ou les serveurs critiques sont

endommagés. Le personnel de terrain travaillant dans des zones sujettes aux catastrophes est confronté à des problèmes de communication et de mobilité supplémentaires, ce qui complique encore davantage les efforts humanitaires. Malgré les stratégies de préparation aux catastrophes de l'organisation, l'imprévisibilité et l'ampleur de tels événements nécessitent un investissement continu dans des mesures d'atténuation pour garantir la continuité des activités pendant et après les catastrophes. | | **Vol/Perte d'appareils** | Moyen | Élevé | **Haut** | Avec plus de 10 000 employés répartis dans plus de 190 pays, le risque de vol ou de perte d'appareils (par exemple ordinateurs portables, téléphones portables, clés USB) constitue une menace constante. Cela est particulièrement problématique dans les régions où les taux de criminalité sont élevés ou lors du transport de personnel ou de matériel vers des zones de conflit et des contextes humanitaires. Un appareil perdu ou volé pourrait entraîner la divulgation de données hautement sensibles, notamment les dossiers des donneurs, les données de santé et les informations de sécurité. L'utilisation d'appareils non sécurisés ou l'incapacité à mettre en œuvre des mesures de sécurité appropriées (par exemple, protection par mot de passe, cryptage des appareils) augmente ce risque. Des exemples spécifiques d'incidents ont été signalés dans le passé, tels que le vol d'ordinateurs portables contenant des données sensibles dans les bureaux extérieurs ou la perte d'appareils en cas d'urgence. Par conséquent, des politiques strictes concernant la gestion des appareils, les protocoles de sécurité et les capacités d’effacement à distance sont nécessaires. | | **Menace interne** | Faible | Très élevé | **Moitié** | Les menaces internes, bien que moins courantes, comportent des risques importants en raison de la sensibilité des données traitées par les employés et sous-traitants de l'UNICEF. L’organisation dépend d’une main-d’œuvre nombreuse et diversifiée, y compris des employés travaillant dans des régions à haut risque. Les menaces internes peuvent inclure des actions malveillantes (par exemple, vol de données, sabotage) ou une mauvaise gestion par inadvertance d'informations sensibles (par exemple, non-respect des protocoles d'accès aux données). Bien que le risque soit relativement faible, les conséquences peuvent être dévastatrices, en particulier pour le personnel travaillant dans les zones de conflit et ayant accès à des données sensibles sur la protection de l’enfance et la santé. Les menaces internes peuvent également s’étendre aux sous-traitants, partenaires ou fournisseurs qui ont accès aux systèmes de données critiques. Une surveillance régulière, des contrôles d'accès stricts et des audits internes sont essentiels pour minimiser le risque de menaces internes. | | **Erreur humaine (perte de données)** | Élevé | Moyen | **Moitié** | L’erreur humaine est l’une des causes les plus courantes de perte ou d’exposition de données dans les organisations mondiales. Les opérations mondiales de l'UNICEF, combinées à la diversité des langues, des cultures et des niveaux de connaissances technologiques du personnel, augmentent la probabilité d'erreurs telles que la suppression accidentelle de données, le partage inapproprié de fichiers ou le non-respect des politiques de sécurité des données. Dans les bureaux de terrain, où le personnel est sous pression pour fournir des réponses rapides, l’erreur humaine peut entraîner une exposition accidentelle ou une perte d’informations critiques. L’utilisation de processus manuels ou de systèmes obsolètes dans certaines régions peut encore exacerber le risque d’erreurs. Une formation, des politiques claires de gestion des données et des systèmes de sauvegarde automatisés des données sont nécessaires pour minimiser les erreurs humaines. |

---

7. Stratégies d'atténuation

1. Campagne de sensibilisation au phishing

- **Action**:
- Mettre en place un système global **programme de sensibilisation au phishing** qui s’adapte aux contextes régionaux et aux menaces locales. Le programme comprendra **séances de formation**

interactives, **exercices de phishing simulés**, et **évaluations en cours** pour évaluer la préparation du personnel.
- Commettre **experts externes en cybersécurité** mener des simulations de phishing approfondies et fournir aux bureaux régionaux des directives spécifiques basées sur les types d'attaques les plus courants dans leur zone géographique.
- Sensibiliser le personnel à **drapeaux rouges** tels que les expéditeurs inconnus, les pièces jointes suspectes et les liens non sollicités dans les e-mails, avec une attention particulière à **hameçonnage** et **Fraude au PDG** qui ciblent souvent les hauts dirigeants.
- Collaborez avec les services mondiaux de filtrage des e-mails et assurez-vous **verrouillage automatique** d'e-mails liés au phishing et de pièces jointes malveillantes.
- **Chronologie**:
- Formation immédiate pour **régions à haut risque** (par exemple zones de conflit, marchés émergents) au sein **1 nous**.
- Achever la mise en œuvre du programme mondial au sein **3 mois**, régulièrement **cours de remise à niveau semestriels**.
- **Impact**:
- Réduction significative des incidents liés au phishing et personnel mieux informé, capable de reconnaître et de prévenir les tentatives de phishing. Amélioration de la résilience aux attaques d’ingénierie sociale.

2. Cryptage des données

- **Action**:
- Assurer **chiffrement de bout en bout** Il est appliqué sur les appareils mobiles, les ordinateurs portables et les services basés sur le cloud (par exemple AWS, Azure) pour protéger les données pendant la transmission et le stockage.
- Intégrez des solutions de chiffrement conformes à **RGPD** et d'autres lois régionales sur la protection des données, garantissant que toutes les données sensibles, y compris les dossiers médicaux et de protection de l'enfance, sont cryptées à la fois en transit et au repos.
- Mettre en œuvre **chiffrement matériel** solutions pour les appareils du personnel de terrain, avec cryptage automatique activé au démarrage.
- Mettez régulièrement à jour les normes de chiffrement et évaluez leur efficacité dans la lutte contre les menaces émergentes (par exemple, l'informatique quantique).
- **Chronologie**:
- **Mise en œuvre immédiate du chiffrement** pour les opérations sur le terrain à haut risque et les systèmes critiques (par exemple, données des donateurs, dossiers de protection de l’enfance).
- **Mise en œuvre complète** globalement à l'intérieur **6 mois**, avec journal **audits annuels**.
- **Impact**:
- Les données restent sécurisées même en cas de vol ou de violation de l'appareil, réduisant considérablement le risque d'accès non autorisé aux informations sensibles.

3. Authentification multifacteur (MFA)

- **Action**:
- Exigez l'authentification multifacteur pour tous les employés et sous-traitants accédant aux systèmes critiques (par exemple, services cloud, données financières, bases de données internes) afin d'empêcher tout accès non autorisé, même si les informations d'identification sont compromises.

- Apporter un soutien à **authentification biométrique** le **puces matérielles** pour les personnels de haut rang et ceux travaillant dans des régions sensibles ou sur des projets à risques.
- Intégrer MFA avec **VPN** et garantir un accès sécurisé aux systèmes distants pour le personnel de terrain.
- **Chronologie**:
- Implémenter l'AMF pour **systèmes critiques** dans **2 mois** (par exemple AWS, Salesforce et les plateformes de donateurs).
- Complet **MFA pour toute l'organisation** mise en œuvre sur tous les systèmes au sein **4 mois**.
- **Impact**:
- Réduit considérablement les risques d'accès non autorisé aux systèmes sensibles, notamment en cas de phishing ou de vol d'identifiants.

4. Plans de sauvegarde et de reprise après sinistre

- **Action**:
- Créer **centres régionaux de reprise après sinistre** pour garantir que les données peuvent être récupérées rapidement, même dans les régions sujettes aux catastrophes naturelles ou aux conflits. Les systèmes de sauvegarde doivent être diversifiés entre les emplacements physiques et cloud.
- Conduire **exercices semestriels de reprise après sinistre** pour tester la résilience du système et la préparation du personnel sur le terrain à récupérer les données à distance ou en personne.
- Améliorer **redondance des données**, garantissant que les données clés (telles que les dossiers des donateurs, les données de santé et les plans de projet) sont sauvegardées dans plusieurs zones géographiques, minimisant ainsi le risque de perte de données.
- **Chronologie**:
- **Révision d'un mois** des capacités actuelles de reprise après sinistre, suivies par **améliorations immédiates**.
- Complet **tests et mise en œuvre** de redondances de sauvegardes physiques et basées sur le cloud au sein **6 mois**.
- **Impact**:
- Réduit la perte de données en cas de catastrophe ou d'attaque de ransomware, garantissant ainsi la poursuite des opérations critiques de l'UNICEF même en cas de perturbations.

5. Contrôle d'accès aux données

- **Action**:
- Imposer **Contrôle d'accès basé sur les rôles (RBAC)** Tous les systèmes limitent l'accès aux données sensibles en fonction du rôle, des responsabilités et du besoin de savoir de l'individu.
- Mettre en œuvre **audits fréquents** des journaux d'accès pour détecter les tentatives non autorisées et les anomalies, et effectuer **revues trimestrielles** des droits d'accès des utilisateurs.
- Établir **accès au moindre privilège** protocoles et veiller à ce que les employés aient accès uniquement aux données nécessaires à l'exercice de leurs fonctions.
- Mettre en œuvre **examens d'accès automatisés** pour les sous-traitants et fournisseurs tiers ayant accès aux systèmes et données critiques.
- **Chronologie**:
- **Mise en œuvre en cours**, avec un premier examen dans **3 mois** pour garantir que le modèle RBAC fonctionne sur tous les principaux systèmes.
- **Impact**:

- Contrôle amélioré sur les données sensibles, avec réduction des risques de menaces internes ou d'exposition accidentelle des données grâce à des droits d'accès adaptés aux besoins du poste.