Politiques et procédures de sécurité de l'UNICEF

Table des matières

---

1. **Introduction au cadre de sécurité de l'UNICEF**

Le **Cadre de pratiques de sécurité de l'information de l'UNICEF** est conçu pour garantir que l'infrastructure numérique, les données sensibles et les ressources de l'UNICEF sont efficacement protégées contre les menaces et les risques, notamment les cyberattaques, les violations de données, les catastrophes naturelles et les erreurs humaines. Compte tenu de sa présence mondiale dans les domaines de la protection de l'enfance, de la santé, de l'éducation et des efforts humanitaires, l'UNICEF a besoin de mesures de sécurité robustes et complètes.

- **Vision** : Protéger les données sensibles de l'UNICEF, soutenir les opérations mondiales, assurer la sécurité des enfants dans le monde entier et maintenir la confiance des parties prenantes.
- **Éléments de base** :
  - **Confidentialité des données** : Conformité aux normes mondiales de confidentialité des données (RGPD, HIPAA, etc.).
  - **Réponse aux incidents** : établir des processus clairs et organisés pour détecter, gérer et atténuer les incidents.
  - **Continuité des activités** : Assurer une perturbation minimale des opérations critiques de l'UNICEF pendant une crise.
  - **Sensibilisation à la sécurité** : Formation continue pour réduire les erreurs humaines et maintenir une main-d'œuvre vigilante et bien informée.

---

2. **Gouvernance et conformité**

2.1 Réglementations clés et cadres de conformité

L'UNICEF opère dans diverses régions et juridictions, chacune avec ses propres lois sur la protection des données et réglementations en matière de cybersécurité. L'organisation aligne ses pratiques de sécurité sur les normes clés suivantes :

- **ISO/IEC 27001** : Cette norme décrit les meilleures pratiques pour un **Système de gestion de la sécurité de l'information (ISMS)**. L'UNICEF veille à ce que le cadre fournisse des contrôles de sécurité robustes, depuis l'identification des risques jusqu'à la mise en œuvre de mesures d'atténuation.
- **Règlement général sur la protection des données (RGPD)** : Le respect du RGPD est obligatoire pour le traitement des données personnelles des citoyens de l'UE. Les processus de l'UNICEF sont conçus pour faire respecter des droits tels que la minimisation des données, la transparence et la responsabilité.
    - Exemple : l'UNICEF fournit aux individus des formulaires de consentement clairs et des droits d'accès et de suppression de leurs données, conformément aux exigences du RGPD.
- **NIST SP 800-53** : norme fédérale américaine qui fournit un catalogue de contrôles de sécurité pour les systèmes d'information fédéraux, garantissant la conformité aux exigences de cybersécurité.
- **Contrôles de sécurité critiques CIS** : un ensemble de bonnes pratiques de cybersécurité prioritaires que l'UNICEF suit pour sécuriser ses systèmes contre les vulnérabilités et les menaces courantes.
- **Loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA)** : Applicable au traitement des données médicales par l'UNICEF dans des contextes humanitaires spécifiques (par exemple, la fourniture de services de santé aux enfants), nécessitant des protections strictes pour les informations de santé.

2.2 Structure de gouvernance de la sécurité

La **Structure de gouvernance de la sécurité** au sein de l'UNICEF est une approche multiforme et complète conçue pour garantir que la sécurité de l'information est intégrée à tous les niveaux de l'organisation. Cette structure assure le leadership, la supervision et la responsabilité des décisions en matière de sécurité, et garantit que les efforts de sécurité de l'UNICEF s'alignent sur ses objectifs organisationnels et les exigences réglementaires mondiales. Les composants suivants définissent ce cadre de gouvernance :

RSSI (Chief Information Security Officer)

Le **responsable principal de la sécurité de l'information (RSSI)** assume la responsabilité ultime de la stratégie globale de sécurité, de la direction et de l'exécution des initiatives de sécurité au sein de l'UNICEF. Le RSSI est chargé de garantir que tous les aspects de la sécurité de l'information, de la gestion des menaces à la conformité aux normes internationales, sont couverts et mis en œuvre efficacement.

Responsabilités clés :

- **Supervision stratégique** : Le RSSI s'assure que le programme de sécurité de l'information s'aligne sur la mission et les besoins opérationnels de l'UNICEF. Ils élaborent des stratégies de sécurité à long terme, garantissant que les ressources sont allouées efficacement et que les risques sont gérés de manière proactive.
- **Gestion des risques** : le RSSI évalue les risques et les vulnérabilités liés aux actifs numériques et physiques de l'UNICEF, y compris les données, les réseaux et la propriété intellectuelle. Ils créent et

mettent à jour des stratégies d'atténuation des risques et sont responsables de prendre des décisions sur les niveaux de risque acceptables.
- **Conformité et réglementations** : le RSSI garantit que l'UNICEF respecte les normes mondiales telles que **GDPR**, **ISO/IEC 27001**, **NIST SP 800-53** et **HIPAA** (le cas échéant), tout en garantissant le respect des lois sur la sécurité et la confidentialité des données des différents pays dans lesquels l'UNICEF opère.
- **Rapports à la direction générale** : le RSSI fournit régulièrement des rapports de sécurité à la direction exécutive et au conseil d'administration de l'UNICEF, y compris des mises à jour sur les risques de sécurité, les incidents et les initiatives stratégiques.

Intégration au comité de gestion des risques :

Le RSSI est un membre clé du **Comité de gestion des risques** de l'UNICEF. Ce comité est responsable des décisions stratégiques sur les risques organisationnels, la cybersécurité et la confidentialité des données, intégrant la sécurité dans le cadre global de gestion des risques de l'organisation. Le comité de gestion des risques se réunit régulièrement pour discuter des menaces émergentes, des changements réglementaires et de l'état de préparation de l'organisation à gérer les risques.

Centre d'opérations de sécurité (SOC)

Le **Centre d'opérations de sécurité (SOC)** est l'épine dorsale des opérations de sécurité de l'UNICEF, chargé de surveiller et de répondre aux incidents de sécurité en temps réel. L'équipe SOC fonctionne 24h/24 et 7j/7, utilisant des outils et des technologies de pointe pour surveiller tous les systèmes et infrastructures critiques.

Fonctions clés :

- **Détection des menaces en temps réel** : le SOC utilise des outils de sécurité avancés tels que **Splunk** pour l'agrégation et l'analyse des journaux, **CrowdStrike** pour la protection des points de terminaison et **AWS GuardDuty** pour les renseignements sur les menaces dans le cloud. . Ces outils surveillent en permanence les événements de sécurité, détectent les activités anormales et émettent des alertes pour une action immédiate.
    - **Splunk** : il facilite la **gestion des informations et des événements de sécurité (SIEM)**, en regroupant les données provenant de plusieurs sources (serveurs, points de terminaison, applications) pour identifier les incidents de sécurité potentiels tels que les violations de données et les attaques par déni de service. , ou des menaces internes.
    - **CrowdStrike Falcon** : un outil clé pour la sécurité des points finaux qui assure une surveillance en temps réel des appareils utilisés par le personnel, tels que les ordinateurs portables et les téléphones mobiles, pour détecter et atténuer les logiciels malveillants, les ransomwares et autres menaces liées aux points finaux.
- **Détection et réponse aux incidents** : le SOC détecte les activités suspectes, analyse les menaces potentielles et se coordonne avec l'équipe de réponse aux incidents (IRT) pour contenir, atténuer et résoudre les incidents rapidement.
    - Exemple : si le SOC détecte une tentative inhabituelle d'exfiltration de données grâce à la surveillance du réseau, l'équipe alerte instantanément l'IRT pour qu'il prenne des mesures, comme isoler le système concerné et bloquer tout transfert de données ultérieur.

- **Threat Intelligence** : le SOC intègre en permanence des flux de renseignements sur les menaces provenant de fournisseurs de sécurité mondiaux et de sources internes pour anticiper les menaces émergentes. Des outils tels que **FireEye** et **ThreatConnect** sont utilisés pour collecter et analyser des informations sur les nouvelles menaces ciblant des organisations comme l'UNICEF.
- **Surveillance et chasse proactives** : en plus de la surveillance réactive, le SOC recherche de manière proactive les vulnérabilités potentielles et les signes de compromission, en utilisant des techniques telles que les exercices de **Threat Hunting** et de **Red Teaming** pour tester et améliorer la sécurité. défenses.

Dotation en personnel du SOC :

Le SOC est composé d'**analystes de sécurité**, de **intervenants en cas d'incident**, de **spécialistes du renseignement sur les menaces** et de **experts en criminalistique** qui travaillent ensemble pour garantir la disponibilité, l'intégrité et la confidentialité des données et des données de l'UNICEF. systèmes.

Comité de sécurité informatique

Le **Comité de sécurité informatique** est un groupe interfonctionnel composé de professionnels chevronnés de l'informatique et de la sécurité au sein de l'UNICEF. La responsabilité principale du comité est de superviser la formulation, la mise en œuvre et l'examen de la stratégie, des politiques et des plans opérationnels de sécurité de l'organisation.

Responsabilités clés :

- **Planification stratégique** : Le comité de sécurité informatique travaille avec le RSSI pour définir et mettre à jour la stratégie de sécurité de l'organisation, en identifiant les domaines clés à améliorer et en assurant l'alignement avec les objectifs plus larges de l'organisation.
- **Élaboration de politiques de sécurité** : Le comité joue un rôle crucial dans la rédaction et la révision des politiques de sécurité, y compris la protection des données, les normes de cryptage, les contrôles d'accès des utilisateurs et les protocoles de gestion des incidents de sécurité.
- **Budget de sécurité et allocation des ressources** : Le comité décide des investissements liés à la sécurité, évaluant le financement des outils, de la formation et des opérations de sécurité nécessaires. Ils donnent la priorité à l'allocation budgétaire pour garantir que les ressources sont orientées vers des initiatives hautement prioritaires telles que la mise à niveau des infrastructures ou de nouveaux outils de sécurité.
- **Évaluation et atténuation des risques** : Le comité évalue l'efficacité des efforts de gestion des risques de l'organisation, en tenant compte de l'évolution du paysage des menaces de cybersécurité, des changements réglementaires et de l'exposition aux risques opérationnels de l'UNICEF.
- **Évaluation de la posture de sécurité** : Le comité de sécurité informatique travaille avec des auditeurs externes pour examiner la posture de sécurité actuelle de l'organisation, garantissant que les systèmes critiques sont protégés contre les vulnérabilités et les menaces potentielles.

Principales parties prenantes du comité de sécurité informatique :

- **CTO (Chief Technology Officer)** : Travaille en étroite collaboration avec le RSSI pour aligner l'infrastructure technique et les innovations avec les besoins de sécurité.

- **Responsables juridiques et conformité** : veillez à ce que les initiatives de sécurité soient conformes aux lois internationales et aux réglementations du secteur, telles que le RGPD et les normes ISO/IEC.
- **Équipe de gestion des risques** : Collabore avec le comité pour identifier et traiter les risques émergents pour les actifs informationnels de l'organisation.
- **Experts externes** : le comité consulte occasionnellement des experts externes tels que des **consultants en sécurité**, des **testeurs d'intrusion** ou des **auditeurs de conformité** pour évaluer et améliorer les pratiques de sécurité.

Auditeurs externes

Les auditeurs externes jouent un rôle essentiel pour garantir que les pratiques de sécurité de l'information de l'UNICEF restent efficaces et conformes aux normes les plus élevées. Ils apportent une perspective indépendante et impartiale à la gouvernance de la sécurité et jouent un rôle essentiel dans l'identification des lacunes et des vulnérabilités.

Rôles et responsabilités clés :

- **Audits de conformité** : l'UNICEF fait appel à des auditeurs tiers tels que **KPMG**, **PwC** et **Deloitte** pour mener des audits périodiques, évaluant la conformité de l'organisation aux principales réglementations et cadres de sécurité tels que comme **ISO 27001**, **SOC 2**, **GDPR** et **NIST SP 800-53**.
    - Exemple : Un **audit PwC** de la posture de sécurité du cloud de l'UNICEF évalue si les configurations cloud de l'organisation respectent les meilleures pratiques et les normes réglementaires en matière de protection des données.
- **Évaluations des vulnérabilités et tests d'intrusion** : les auditeurs externes sont souvent chargés de mener des évaluations de sécurité complètes, qui incluent des **tests d'intrusion**, une **analyse des vulnérabilités** et une **révision du code**. Ces évaluations aident l'UNICEF à identifier les faiblesses potentielles de son infrastructure numérique.
    - Exemple : un **test d'intrusion** pourrait révéler des failles de sécurité dans l'application mobile ou les portails Web de l'UNICEF, conduisant à des recommandations pour des mécanismes de cryptage et d'authentification plus robustes.
- **Analyse des écarts** : après avoir terminé leurs évaluations, les auditeurs externes réalisent des rapports d'analyse des écarts, mettant en évidence les domaines de vulnérabilité et conseillant sur les améliorations ou les actions correctives nécessaires.
    - Exemple : les auditeurs peuvent identifier que les mesures de protection des terminaux de l'UNICEF doivent être renforcées pour tenir compte de l'utilisation croissante des **appareils mobiles** pour les opérations à distance sur le terrain.
- **Rapports au Conseil** : Les auditeurs externes fournissent des rapports indépendants sur l'efficacité du programme de sécurité de l'information, proposant des recommandations pour une amélioration continue. Ces rapports sont souvent présentés directement à la haute direction et au conseil d'administration de l'UNICEF.

Avantages des audits externes :

- **Vérification indépendante** : les audits externes fournissent un examen neutre par un tiers des contrôles et pratiques de sécurité de l'UNICEF, ce qui permet de garantir que les systèmes de l'organisation sont sécurisés et conformes.

- **Assurance réglementaire** : un engagement régulier auprès des auditeurs aide l'UNICEF à prouver son engagement à respecter les lois internationales sur la protection des données et les normes de l'industrie.
- **Améliorations continues de la sécurité** : les résultats des audits externes alimentent directement le cycle d'amélioration continue de l'UNICEF, améliorant ainsi la posture de sécurité au fil du temps.

Intégration avec d'autres structures de gouvernance

En plus de ces rôles spécifiques, le cadre de gouvernance de la sécurité de l'UNICEF est intégré à des structures organisationnelles plus larges, garantissant que les considérations de cybersécurité sont intégrées dans tous les processus décisionnels. La structure de **Gouvernance des technologies de l'information (TI)** travaille en étroite collaboration avec les équipes de sécurité pour garantir que les nouvelles technologies et systèmes sont évalués pour les risques de sécurité avant d'être mis en œuvre.

---

3. Politique de sécurité des informations

3.1 Objectif et portée

La **Politique de sécurité de l'information** définit l'approche globale de l'UNICEF pour protéger ses actifs informatiques et technologiques. Cette politique garantit la confidentialité, l'intégrité et la disponibilité des informations et des systèmes de l'organisation, tout en respectant les réglementations mondiales en matière de conformité et de confidentialité. La politique s'applique à :

- **Employés** : Cela inclut tous les employés à temps plein, les sous-traitants, les travailleurs temporaires, les stagiaires et les prestataires de services tiers qui ont accès aux systèmes d'information de l'UNICEF. Tous les membres du personnel sont tenus de se familiariser avec la politique et de suivre les procédures de sécurité.
    - **Exemple** : Un entrepreneur travaillant sur un projet pour l'UNICEF doit adhérer aux mêmes protocoles de sécurité que le personnel à temps plein, y compris les mesures de contrôle d'accès et les exigences en matière de signalement des incidents.
- **Systèmes** : tous les systèmes exploités ou détenus par l'UNICEF, y compris :
    - **Infrastructure informatique** : serveurs internes, périphériques réseau, pare-feu et systèmes de stockage de données.
    - **Systèmes cloud** : tous les services hébergés sur des plates-formes cloud telles que **Amazon Web Services (AWS)**, **Microsoft Azure** et **Google Cloud Platform (GCP)**, où les applications et les données sont stockées.
    - **Points de terminaison** : tous les appareils tels que les ordinateurs portables, les ordinateurs de bureau, les tablettes, les smartphones et autres équipements connectés qui peuvent accéder aux réseaux et services internes de l'UNICEF.
    - **Réseaux** : Tous les réseaux de communication internes et externes, y compris les réseaux privés virtuels (VPN) utilisés par le personnel de l'UNICEF pour le travail à distance et l'accès sécurisé.
- **Données** : La politique couvre tous les types de données traitées par l'UNICEF, notamment :

- **Données personnelles** : données soumises aux réglementations en matière de confidentialité telles que le **Règlement général sur la protection des données (RGPD)**, qui couvre les données personnelles liées aux donateurs, aux employés et aux bénéficiaires de l'UNICEF.
- **Données opérationnelles** : comprend les données du projet, les communications internes et les informations de recherche.
- **Informations financières sensibles** : tous les dossiers financiers, budgets, données de paie et autres détails financiers sensibles.
- **Propriété intellectuelle** : documents, conceptions, logiciels et autres supports développés par l'UNICEF.

3.2 Objectifs de sécurité

La politique de sécurité de l'information est conçue pour atteindre les objectifs de sécurité suivants :

Confidentialité

La confidentialité garantit que les informations sensibles ne sont accessibles qu'aux personnes disposant d'un accès autorisé, réduisant ainsi le risque de divulgation non autorisée. L'UNICEF utilise une **approche de sécurité à plusieurs niveaux** pour garantir la confidentialité à tous les niveaux de son écosystème d'informations.

- **Cryptage des données** : toutes les données personnelles sensibles et informations opérationnelles sont cryptées au repos et en transit à l'aide de protocoles de cryptage puissants.
  - **Exemple** : Les données personnelles telles que les informations sur les donateurs et les dossiers des bénéficiaires sont cryptées au repos à l'aide de **AWS Key Management Service (KMS)** avec cryptage **AES-256**. Les données en transit sont chiffrées à l'aide de **Transport Layer Security (TLS)**.
- **Contrôle d'accès** : l'accès est accordé sur la base du **principe du moindre privilège**, garantissant que les employés n'ont accès qu'aux données nécessaires à leurs rôles spécifiques.
  - **Exemple** : les employés du service financier ne peuvent accéder qu'aux dossiers financiers, tandis que le personnel des ressources humaines peut accéder aux données des employés, mais pas aux données financières. Les droits d'accès sont gérés via **Okta** et sont révisés régulièrement.
- **Masquage et rédaction des données** : pour certaines opérations sensibles (par exemple, rapports publics, données partagées avec des partenaires), les champs sensibles sont masqués ou rédigés pour empêcher tout accès non autorisé.
  - **Exemple** : Les informations sur les donateurs dans les rapports partagés avec des partenaires externes sont masquées pour protéger l'identité personnelle.

Intégrité

L'intégrité garantit que les informations sont exactes, cohérentes et dignes de confiance tout au long de leur cycle de vie. Pour protéger l'intégrité des données, l'UNICEF utilise plusieurs mesures :

- **Validation des données et sommes de contrôle** : pour vérifier l'authenticité des données critiques, l'UNICEF utilise des hachages cryptographiques (par exemple, **SHA-256**) et des sommes de contrôle lors des transferts ou du traitement des données.

    - **Exemple** : lors du transfert de grands ensembles de données entre plates-formes ou lors de la sauvegarde de données, l'UNICEF génère des hachages cryptographiques pour vérifier que les données n'ont pas été falsifiées pendant la transmission.
- **Contrôle de version** : les modifications apportées aux documents, bases de code et données critiques sont suivies à l'aide de systèmes de contrôle de version tels que **GitHub** pour le code et **SharePoint** pour les documents.
    - **Exemple** : Une modification des prévisions financières internes de l'UNICEF est enregistrée et tout écart est signalé pour examen.

Disponibilité

La disponibilité garantit que les informations et les systèmes sont accessibles aux utilisateurs autorisés en cas de besoin, minimisant ainsi les temps d'arrêt et les interruptions de service.

- **Systèmes haute disponibilité** : l'UNICEF met en œuvre des configurations haute disponibilité pour les systèmes critiques, garantissant ainsi un temps d'arrêt minimal en cas de panne. Par exemple, **SAP** et **Salesforce** sont déployés sur l'infrastructure **AWS** à l'aide de déploiements de zones multi-disponibilité (AZ), garantissant des capacités de redondance et de basculement.
    - **Exemple** : en cas de panne d'un AWS AZ, le trafic est automatiquement redirigé vers une autre zone disponible dans la région, garantissant ainsi une disponibilité continue du service.
- **Reprise après sinistre** : un plan de reprise après sinistre robuste est en place, avec des sauvegardes fréquentes des données et des systèmes critiques pour garantir que les objectifs de récupération sont atteints dans des délais acceptables (objectifs de temps de récupération - RTO) et que la perte de données est minimisée (point de récupération). Objectifs - RPO).
    - **Exemple** : l'UNICEF effectue des sauvegardes quotidiennes des données et des systèmes à l'aide de **Veeam Backup** pour répliquer les données sur les compartiments **AWS S3** et **AWS Glacier** pour un stockage à long terme. Ces sauvegardes sont testées régulièrement pour l'intégrité et la restauration des données.

Non-répudiation

La non-répudiation garantit que les actions effectuées sur les systèmes et les données sont traçables, garantissant ainsi la responsabilité et empêchant les utilisateurs de nier leurs actions.

- **Pistes d'audit** : toutes les interactions des utilisateurs avec les systèmes et les données sensibles sont enregistrées. Les journaux sont regroupés et stockés en toute sécurité pour une analyse médico-légale si nécessaire. Des outils tels que **Splunk** sont utilisés pour surveiller et analyser les activités des utilisateurs, générant des alertes pour toute action anormale ou suspecte.
    - **Exemple** : Si un employé accède aux données financières d'un donateur, une entrée est créée dans le journal **Splunk**, capturant l'identité de l'utilisateur, l'heure et le type d'action entreprise (par exemple, lire, écrire, mettre à jour).
- **Signatures numériques** : les documents et transactions nécessitant des signatures sont signés numériquement pour garantir leur authenticité et éviter toute falsification. Cela comprend les accords, les contrats et les communications clés.
    - **Exemple** : L'UNICEF utilise **DocuSign** pour signer des documents officiels, garantissant que chaque document possède une signature numérique cryptée qui ne peut pas être modifiée.

3.3 Évaluation et gestion des risques

- **Évaluation continue des risques** : l'UNICEF effectue des évaluations continues des risques pour identifier les menaces potentielles à la sécurité de ses systèmes et de ses données. Ces évaluations sont conçues pour hiérarchiser les vulnérabilités en fonction de leur impact potentiel sur l'organisation et de la probabilité qu'elles se produisent.
    - **Exemple** : Chaque année, l'UNICEF effectue une **évaluation des risques** qui comprend des analyses de vulnérabilité à l'aide d'outils tels que **Qualys** et **Tenable.io**, suivies d'une **pénétration approfondie. tester** l'engagement avec une société de sécurité externe comme **KPMG**.
- **Audits de sécurité** : des audits de sécurité internes et externes périodiques sont effectués pour garantir la conformité aux normes de l'industrie et aux politiques organisationnelles.
    - **Exemple** : **PwC** effectue un audit de sécurité annuel de l'infrastructure informatique de l'UNICEF pour garantir la conformité aux normes **ISO 27001** et **SOC 2**.
- **Gestion des vulnérabilités** : les vulnérabilités identifiées lors d'analyses ou d'audits sont priorisées et corrigées en temps opportun. Les vulnérabilités critiques qui présentent un risque important pour les systèmes sont corrigées dans les **24 heures**.
    - **Exemple** : Si une vulnérabilité critique est identifiée dans **SAP** lors d'un audit, l'équipe de gestion des vulnérabilités s'efforce de la corriger dans le délai défini afin d'atténuer le risque potentiel.

3.4 Conformité des employés et des entrepreneurs

Tous les employés, sous-traitants et fournisseurs tiers de l'UNICEF sont tenus de se conformer à la **Politique de sécurité des informations**. Cela inclut le respect de :

- **Programmes de formation** : tous les employés suivent une formation annuelle de sensibilisation à la sécurité via des plateformes telles que **KnowBe4**, axée sur l'identification du phishing, la compréhension de la sécurité des mots de passe et le signalement des incidents de sécurité potentiels.
    - **Exemple** : Chaque nouvel employé doit suivre un cours d'intégration sur la sécurité au cours du premier mois d'emploi, qui comprend des modules sur les politiques d'utilisation acceptables, la protection des données et le contrôle d'accès au système.
- **Gestion tierce** : les sous-traitants et les fournisseurs tiers doivent signer des accords de confidentialité, se soumettre à des contrôles de sécurité et se conformer aux politiques de sécurité de l'UNICEF lorsqu'ils travaillent avec des données sensibles.
    - **Exemple** : Avant qu'un fournisseur tiers n'obtienne l'accès aux données de l'UNICEF, une **évaluation des risques par un tiers** est effectuée pour évaluer sa posture de sécurité et garantir qu'il respecte les normes de sécurité des informations de l'UNICEF.

3.5 Application des politiques et violations

- **Application** : Le **RSSI** et le **Comité de sécurité informatique** sont responsables de l'application de la politique de sécurité de l'information. Toute violation de la politique peut entraîner des mesures disciplinaires, notamment le licenciement, des poursuites judiciaires ou des sanctions financières.
    - **Exemple** : S'il s'avère qu'un employé a violé les contrôles d'accès aux données en partageant de manière inappropriée des données sensibles, il peut faire l'objet d'une enquête formelle et

d'un éventuel licenciement.

- **Surveillance et reporting** : l'UNICEF surveille en permanence la conformité de ses systèmes à la politique à l'aide d'outils automatisés tels que **Splunk** et d'audits manuels. Les employés sont encouragés à signaler toute activité ou violation suspecte via les canaux de signalement désignés.
    - **Exemple** : les employés peuvent signaler une tentative de phishing suspectée via l'e-mail de sécurité de l'entreprise ou un système de ticket interne, ce qui déclenchera une enquête.

3.6 Révision et mises à jour des politiques

- **Révision périodique** : la politique de sécurité des informations est révisée chaque année et mise à jour si nécessaire pour faire face aux menaces émergentes, aux nouvelles exigences de conformité et aux progrès technologiques.
    - **Exemple** : Après un événement mondial majeur de cybersécurité comme l'**attaque SolarWinds**, les politiques de sécurité de l'UNICEF sont revues et mises à jour pour garantir que l'organisation est protégée contre des types d'attaques similaires.
- **Mécanisme de rétroaction** : les employés, les sous-traitants et les auditeurs externes sont encouragés à fournir des commentaires sur la politique et à suggérer des améliorations, qui sont prises en compte lors de l'examen annuel.
    - **Exemple** : après une campagne d'attaque de phishing, le **RSSI** organise une session de feedback avec les employés clés pour discuter de ce qui n'a pas fonctionné et de la manière dont la politique peut être mise à jour pour améliorer la sensibilisation à la sécurité.

---

4. Contrôle d'accès et authentification des utilisateurs

4.1 Gestion des identités et des accès (IAM)

L'UNICEF adopte un cadre de **Gestion des identités et des accès (IAM)** robuste et centralisé pour gérer les identités des utilisateurs, l'authentification et les contrôles d'accès sur tous les systèmes et applications. Le système IAM garantit que seules les personnes autorisées ont accès aux informations et ressources sensibles, en fonction de leurs rôles et responsabilités au sein de l'organisation. Il permet d'atténuer le risque d'accès non autorisé, de violations de données et de menaces internes.

Okta - Plateforme IAM centralisée

L'UNICEF utilise **Okta** comme sa principale solution IAM, qui s'intègre à une variété de systèmes d'entreprise, garantissant une authentification transparente et sécurisée pour les utilisateurs sur toutes les plateformes et tous les services. Okta propose **Single Sign-On (SSO)** et **Multi-Factor Authentication (MFA)**, permettant aux utilisateurs d'accéder en toute sécurité à plusieurs systèmes sans avoir besoin de mots de passe distincts pour chacun.

- **Single Sign-On (SSO)** : la fonctionnalité SSO d'Okta permet aux utilisateurs de se connecter une seule fois et d'accéder à un large éventail d'applications, minimisant ainsi le besoin de mémoriser plusieurs noms d'utilisateur et mots de passe.
    - **Exemple** : un employé de l'UNICEF peut se connecter à Okta à l'aide de ses identifiants et accéder à une suite d'outils tels que **Workday** pour les tâches RH, **Salesforce** pour la gestion

des donateurs et **Slack** pour l'équipe. communication, sans qu'il soit nécessaire de saisir des informations d'identification distinctes pour chacun.
    - **Avantage** : cela améliore l'expérience utilisateur, réduit la fatigue de connexion et augmente la sécurité en minimisant les vulnérabilités liées aux mots de passe.

- **Authentification multifacteur (MFA)** : MFA est appliquée pour tous les utilisateurs accédant aux systèmes sensibles. MFA exige que les utilisateurs fournissent au moins deux facteurs de vérification, ajoutant ainsi une couche de sécurité supplémentaire. Cela peut inclure une combinaison de quelque chose que l'utilisateur connaît (mot de passe), quelque chose qu'il possède (appareil mobile ou jeton de sécurité) ou quelque chose qu'il possède (données biométriques comme les empreintes digitales ou la reconnaissance faciale).

    - **Exemple** : Lorsqu'un employé de l'UNICEF accède à son système de paie via **Workday**, il est invité à saisir son mot de passe, puis à s'authentifier via une méthode MFA, comme un code envoyé sur son téléphone par SMS ou une application. comme **Google Authenticator**.
    - **Avantage** : MFA réduit considérablement le risque d'accès non autorisé, même si un attaquant acquiert le mot de passe d'un utilisateur.

Contrôle d'accès basé sur les rôles (RBAC)

L'UNICEF utilise le **Contrôle d'accès basé sur les rôles (RBAC)** pour garantir que les utilisateurs ont accès uniquement aux ressources et aux données nécessaires à leurs fonctions spécifiques. RBAC minimise le risque de fuite de données ou d'accès non autorisé en limitant ce que les utilisateurs peuvent voir et faire en fonction de leur rôle au sein de l'organisation.

- **Définitions granulaires des rôles** : les rôles sont soigneusement définis dans le système IAM pour refléter diverses fonctions professionnelles, départements et exigences de sécurité. Les rôles sont mappés à des applications et autorisations spécifiques, garantissant que les utilisateurs ne peuvent accéder qu'aux données et fonctions pertinentes pour leur rôle.

    - **Exemple** : un **responsable RH** peut avoir accès aux dossiers des employés et aux données de paie, mais ne pourra pas consulter les rapports financiers, qui sont réservés à l'**équipe financière**.
    - **Exemple** : Un **administrateur informatique** dispose d'un large accès aux paramètres et configurations du système, mais n'aura pas accès aux systèmes RH ou de paie, qui ne font pas partie de ses responsabilités professionnelles.

- **Principe du moindre privilège** : les droits d'accès sont fournis sur la base du principe du **moindre privilège**, ce qui signifie que les utilisateurs ne bénéficient que du niveau d'accès minimal nécessaire pour qu'ils puissent exécuter leurs fonctions professionnelles. Les niveaux d'accès sont périodiquement revus et ajustés pour garantir qu'ils restent appropriés.

    - **Exemple** : un entrepreneur embauché pour un projet à court terme se verra accorder un accès limité aux fichiers du projet sur **SharePoint**, sans accès au réseau plus large de l'organisation ni aux systèmes financiers sensibles.

Gestion fédérée des identités

Outre Okta, l'UNICEF utilise également la **Federated Identity Management** pour un accès sécurisé aux services externes, permettant ainsi aux employés d'utiliser leurs identifiants d'entreprise pour accéder à des plateformes tierces sans créer de comptes séparés.

- **Exemple** : les employés de l'UNICEF peuvent accéder à des plateformes basées sur le cloud comme **AWS** ou **Google Cloud Platform (GCP)** à l'aide de leurs identifiants Okta, rationalisant ainsi l'accès tout en garantissant une gestion centralisée des autorisations.

4.2 Politiques de gestion des mots de passe

Une gestion efficace des mots de passe est essentielle pour protéger les comptes d'utilisateurs et les systèmes contre tout accès non autorisé. L'UNICEF applique des politiques de mots de passe strictes pour garantir que les mots de passe sont complexes et sécurisés tout en offrant un processus efficace permettant aux utilisateurs de gérer leurs informations d'identification.

Exigences relatives à la complexité du mot de passe

L'UNICEF exige que les mots de passe répondent à des exigences strictes en matière de complexité afin de garantir leur robustesse contre les attaques courantes par devinette de mot de passe (par exemple, les attaques par force brute et par dictionnaire).

- **Longueur du mot de passe et diversité des caractères** : tous les mots de passe doivent comporter au moins **12 caractères** et inclure une combinaison de :
    - Lettres majuscules et minuscules
    - Des chiffres (au moins un)
    - Caractères spéciaux (par exemple, @, #, $, %, &, etc.)
    - **Exemple** : Un mot de passe tel que "UNICEF$2024!Secure" répond à ces exigences, offrant un haut niveau de complexité pour résister aux attaques courantes.
- **Listes noires de mots de passe** : l'UNICEF utilise une liste noire de mots de passe pour empêcher les utilisateurs de sélectionner des mots de passe faibles ou couramment utilisés et faciles à deviner. Les mots de passe courants tels que « password123 » ou « qwerty » sont automatiquement signalés et rejetés par le système.
    - **Exemple** : Si un utilisateur tente de définir son mot de passe sur « 12345678 », le système l'en empêchera et l'invitera à sélectionner un mot de passe plus fort.

Expiration et rotation du mot de passe

Pour protéger davantage les comptes contre tout accès non autorisé dû au vol ou à la compromission de mots de passe, l'UNICEF impose l'expiration périodique des mots de passe.

- **Intervalle d'expiration des mots de passe** : tous les mots de passe des utilisateurs expirent tous les **90 jours** pour garantir que les anciens mots de passe ne restent pas vulnérables indéfiniment. Les utilisateurs sont informés 10 jours avant l'expiration de leur mot de passe et doivent mettre à jour leur mot de passe pendant cette période.

    - **Exemple** : **Okta** avertit un utilisateur par e-mail et par rappels dans l'application que son mot de passe expire dans 10 jours. Ils sont invités à choisir un nouveau mot de passe conforme aux exigences de complexité.

- **Historique des mots de passe** : il est interdit aux utilisateurs de réutiliser le même mot de passe après un certain nombre de modifications de mot de passe (par exemple, 5 mots de passe précédents) pour empêcher le recyclage de mots de passe non sécurisés.

    - **Exemple** : Une fois qu'un utilisateur a réinitialisé son mot de passe, il n'est pas autorisé à revenir à un mot de passe précédemment utilisé, favorisant ainsi la création de nouveaux mots de passe sécurisés.

Processus de récupération de mot de passe

Pour garantir que les utilisateurs peuvent récupérer en toute sécurité l'accès à leurs comptes sans compromettre la sécurité, l'UNICEF utilise un processus robuste de **récupération de mot de passe** qui intègre l'**authentification multifacteur (MFA)**.

- **Méthode de récupération** : si un utilisateur oublie son mot de passe, il peut utiliser le **portail libre-service Okta** pour lancer le processus de récupération du mot de passe. L'utilisateur doit s'authentifier à l'aide d'un deuxième facteur, tel qu'un code de vérification envoyé à son numéro de téléphone ou à son e-mail enregistré.

    - **Exemple** : Un utilisateur qui oublie son mot de passe est invité à saisir son adresse e-mail. Ils recevront un code d'authentification par **SMS** ou **email**, qu'ils devront saisir afin de réinitialiser leur mot de passe en toute sécurité.

- **Jetons de récupération basés sur le temps** : le processus de récupération utilise des **mots de passe à usage unique basés sur le temps (TOTP)**, garantissant que tous les jetons de récupération envoyés aux utilisateurs ne sont valides que pendant une courte fenêtre, renforçant ainsi la sécurité.

    - **Exemple** : Un utilisateur demandant une réinitialisation de mot de passe recevra un TOTP à 6 chiffres qui expire dans les 10 minutes, empêchant un attaquant d'intercepter et de réutiliser le code.

Outils de gestion des mots de passe

L'UNICEF encourage également l'utilisation de **Gestionnaires de mots de passe** permettant aux utilisateurs de stocker et de gérer en toute sécurité leurs mots de passe complexes. Des outils tels que **1Password** ou **LastPass** peuvent aider les utilisateurs à conserver des mots de passe forts et uniques pour chaque application sans risquer de les oublier.

- **Exemple** : un utilisateur accède à son compte **Salesforce** et utilise un gestionnaire de mots de passe pour générer un mot de passe unique, qui est stocké en toute sécurité et rempli automatiquement pour les connexions futures.

4.3 Audit et surveillance des accès

La surveillance et l'audit réguliers des activités d'accès des utilisateurs contribuent à garantir que les utilisateurs adhèrent aux politiques de sécurité et permettent de détecter des incidents de sécurité potentiels, tels qu'un accès non autorisé ou un comportement suspect.

- **Journaux d'audit** : Okta conserve des **journaux d'audit** détaillés pour toutes les activités d'authentification et d'accès des utilisateurs, qui sont stockés de manière centralisée et analysés pour déceler les anomalies. Ces journaux incluent des informations telles que les tentatives de connexion, les tentatives de connexion échouées, les adresses IP et les horodatages.
    - **Exemple** : si un utilisateur accède à un système sensible tel que **SAP**, le système enregistre chaque action entreprise par l'utilisateur. Si un nombre inhabituel de tentatives de connexion infructueuses est détecté, une **alerte de sécurité** est déclenchée pour examen.
- **Surveillance en temps réel** : l'intégration avec des outils tels que **Splunk** ou **CrowdStrike** permet une surveillance en temps réel de l'accès des utilisateurs sur tous les systèmes. Les alertes sont automatiquement déclenchées lorsque des modèles d'accès suspects (par exemple, plusieurs échecs de connexion, accès à partir d'adresses IP inhabituelles) sont détectés.
    - **Exemple** : si un employé se connecte à partir d'un emplacement ou d'un appareil inconnu, le système signale cette activité et demande une vérification supplémentaire via **Okta MFA** avant d'accorder l'accès.
- **Révisions d'accès périodiques** : des **révisions d'accès** régulières garantissent que les utilisateurs conservent les droits d'accès appropriés en fonction de leurs rôles et responsabilités actuels. L'accès aux systèmes et données critiques est périodiquement examiné par l'équipe de sécurité et les chefs de service.
    - **Exemple** : Chaque trimestre, le **service RH** examine les privilèges d'accès de tous les employés, garantissant que les utilisateurs qui ont changé de rôle ou quitté l'organisation voient leur accès rapidement révoqué.

#**5. Plan de réponse aux incidents (IRP)**

5.1 Cycle de vie de la gestion des incidents avec délais

| **Type d'incident** | **Outils de détection** | **Actes** | **Prochaines étapes** | **Planification pré-incident** | **Délai de réponse** | |-------- ----- |---------- ---------| ---------- ----------| | **Accès non autorisé** (Brute Force, Compromise) | - **Okta** : échec des tentatives de connexion.
- **CrowdStrike** : activité inhabituelle.
- **AWS GuardDuty** : détection d'anomalies. | - Verrouiller le compte concerné.
- Déclencher une **réinitialisation forcée du mot de passe**.
- Isoler les systèmes compromis. | - Analyse médico-légale des journaux pour identifier les mouvements latéraux.
- Avertir les utilisateurs concernés. | - Appliquer **MFA**.
- Implémenter la **détection de connexion avancée**. | **Immédiat (5 à 15 minutes)** pour la détection.
30 minutes pour le confinement.

1 à 2 heures pour l'éradication.
*4 à 12 heures * pour la récupération.| | **Infection par logiciel malveillant** (Ransomware, chevaux de Troie) |
- **CrowdStrike Falcon** : détection des points de terminaison.
- **Splunk** : trafic anormal.
- **AWS GuardDuty** : activité suspecte. | - Isolez l'appareil concerné.
- Exécutez une **analyse complète des logiciels malveillants**.
- Analysez les journaux système pour détecter le comportement des logiciels malveillants. | - **Reimage** des machines concernées.
- Informer les parties prenantes internes.
- Corriger la cause première. | - Déployer **ATP**.
- **Sauvegardes hors ligne** régulières.
- **Segmentation du réseau**. | **Immédiat (5 à 15 minutes)** pour la détection.
30 à 60 minutes pour le confinement.
1 à 4 heures pour l'éradication.
4 à 12 minutes heures pour la récupération. | | **Attaque de phishing** (récolte d'informations d'identification) |
- **Mimecast** : filtre de courrier électronique malveillant.
- **Splunk** : corrélation du trafic réseau anormal.
- **Proofpoint** : détection de phishing. | - Mettre en quarantaine les e-mails malveillants.
- Déclencher la réinitialisation du mot de passe pour les utilisateurs concernés.
- Examiner la source des e-mails et les journaux DNS. | - Exécutez une analyse de sécurité des appareils concernés.
- Avertissez les autres utilisateurs d'être prudents.
- Analysez et signalez les tentatives de phishing. | - Déployez des **solutions de filtrage des e-mails**.
- Organisez une **formation de sensibilisation au phishing**. | **Immédiat (5 à 15 minutes)** pour la détection.
30 à 60 minutes pour le confinement.
1 à 2 heures pour l'éradication.
2 à 4 minutes heures pour la récupération. | | **Attaque DDoS** (déni de service distribué) | - **AWS Shield**, **Cloudflare** : protection DDoS.
- **Splunk** : analyse du trafic.
- **Akamai** : surveillance du trafic. | - Activez la protection DDoS.
- Implémentez une **limitation de débit**.
- Appliquez un **géoblocage** si nécessaire. | - Redirigez le trafic vers d'autres régions.
- Surveillez les attaques en cours à l'aide de **CloudWatch**.
- Analyse médico-légale après incident. | - Configurez l'**équilibrage de charge**.
- Mettez en œuvre une **infrastructure évolutive** avec la protection **Cloudflare/AWS Shield**. | **Immédiat (5 à 15 minutes)** pour la détection.
30 à 60 minutes pour le confinement.
1 à 2 heures pour l'éradication.
4 à 12 minutes heures pour la récupération. |

5.2 Phases et calendrier de réponse aux incidents

| **Phase** | **Action** | **Laps de temps** | **Partie responsable** | |----------|---------- ----------|--------- ----------|---------- ----------| | **Détection** | Détection initiale grâce à des outils de surveillance et d’alerte. | **Immédiat (5-15 minutes)** | Analystes SOC | | **Triage** | Classification des incidents en fonction de leur gravité (Critique, Élevé, Moyen, Faible). | **15-30**

minutes | Responsable de la réponse aux incidents, analystes SOC | | **Endiguement** | Isolez les systèmes affectés pour limiter la propagation. | **30-60 minutes** | Ingénieurs informatiques, analystes SOC | | **Éradication** | Supprimez la cause première (par exemple, logiciel malveillant, accès non autorisé). | **1-4 heures** | Ingénieurs informatiques, analystes de sécurité | | **Récupération** | Restaurez les systèmes à partir de sauvegardes ou d'environnements alternatifs. | **4-12 heures** | Support informatique, continuité des activités | | **Examen post-incident**| Examinez l'incident pour améliorer les futurs processus de réponse. | **24 à 48 heures après la résolution**| Responsable de la réponse aux incidents, RSSI |

5.3 Scénarios d'incident détaillés avec échéanciers

1. Accès non autorisé (Brute Force / Credential Stuffing)

Détection:

- **Okta** détecte plusieurs tentatives de connexion infructueuses dans un court laps de temps.
- **CrowdStrike** identifie les modèles d'accès inhabituels (par exemple, connexion depuis un pays inconnu).

Actes:

- Verrouillez le compte concerné et effectuez une **réinitialisation du mot de passe**.
- Isoler les systèmes et restreindre l'accès aux ressources sensibles.
- Déclenchez **MFA** pour empêcher tout accès non autorisé.

Chronologie:

- **Détection** : **Immédiat (5 à 15 minutes)**
- **Confinement** : **30-60 min**
- **Éradication** : **1 à 2 heures** (analyse des causes profondes et mesures correctives)
- **Récupération** : **4 à 12 heures** (restauration et surveillance)

Planification pré-incident :

- Appliquez **MFA** pour tous les systèmes critiques.
- Implémentez des **politiques de verrouillage de compte** après plusieurs tentatives de connexion infructueuses.

---

2. Infection par logiciel malveillant (ransomware)

Détection:

- **CrowdStrike Falcon** détecte les signatures de logiciels malveillants ou les activités inhabituelles des fichiers.
- **Splunk** met en corrélation un trafic réseau anormal indiquant une violation de données.

Actes:

- Isolez immédiatement la machine infectée du réseau.

- Exécutez des **analyses antivirus** ou utilisez **CrowdStrike Falcon** pour la détection des logiciels malveillants.
- Bloquez toutes les communications sortantes pour empêcher toute exfiltration ultérieure de données.

Chronologie:

- **Détection** : **Immédiat (5 à 15 minutes)**
- **Confinement** : **30-60 min**
- **Éradication** : **1 à 4 heures** (suppression des logiciels malveillants et correction)
- **Récupération** : **4 à 12 heures** (réinstallation des systèmes et restauration des données)

Planification pré-incident :

- Déployez **ATP** sur tous les appareils.
- Maintenir des **sauvegardes hors ligne** pour les systèmes critiques.

---

3. Attaque de phishing

Détection:

- **Mimecast** signale les pièces jointes ou les liens malveillants.
- **Proofpoint** détecte les sites de phishing connus ou les comportements de courrier électronique inhabituels.

Actes:

- Mettez en quarantaine l'e-mail de phishing pour éviter qu'il ne se propage.
- Effectuez une **réinitialisation du mot de passe** pour tous les comptes concernés.
- Déclenchez un **balayage de sécurité** des appareils concernés.

Chronologie:

- **Détection** : **Immédiat (5 à 15 minutes)**
- **Confinement** : **30-60 min**
- **Éradication** : **1 à 2 heures** (suppression des liens ou fichiers malveillants)
- **Récupération** : **2 à 4 heures** (restauration des services de messagerie et révision des paramètres de sécurité)

Planification pré-incident :

- Déployez des **solutions de filtrage des e-mails** pour la détection du phishing.
- Organisez une **formation de sensibilisation au phishing** pour éviter les erreurs des utilisateurs.

---

4. Attaque DDoS

Détection:

- **AWS Shield** détecte les pics de trafic typiques d'une attaque DDoS.
- **Akamai** ou **Cloudflare** identifient les modèles de trafic anormaux ou les anomalies de requêtes HTTP.

Actes:

- Faites appel à des services d'atténuation DDoS tels que **AWS Shield** ou **Cloudflare** pour absorber le trafic.
- Implémentez une **limitation de débit** et un **blocage géographique** pour empêcher l'amplification des attaques.
- Redirigez le trafic vers les serveurs de sauvegarde ou utilisez l'**équilibrage de charge** pour atténuer la pression sur les systèmes principaux.

Chronologie:

- **Détection** : **Immédiat (5 à 15 minutes)**
- **Confinement** : **30 à 60 minutes** (Activer la protection DDoS, limitation du débit)
- **Éradication** : **1-2 heures** (gestion du trafic et filtrage)
- **Récupération** : **4 à 12 heures** (restauration de l'accès et service normal)

Planification pré-incident :

- Utilisez l'**équilibrage de charge** pour répartir le trafic réseau de manière uniforme.
- Mettez en œuvre une **infrastructure cloud évolutive** capable de gérer les pics de trafic.

5.4 Plan de communication avec échéanciers

| **Action** | **Description** | **Partie responsable** | **Chronologie** | |---------- --------- --|---------- ----------| | **Notification interne** | Informer la haute direction, le RSSI et les équipes de réponse aux incidents. | Responsable SOC, responsable de la réponse aux incidents | **Immédiat (0-15 minutes)** | | **Notification externe** | Informez les utilisateurs, les clients et les organismes de réglementation concernés si nécessaire (par exemple, notification de violation du RGPD). | Équipe de relations publiques, juridique, responsable de la réponse aux incidents | **Dès 1 heure après le confinement** | | **Divulgation publique** | Annoncez tout problème exposé au public (uniquement si nécessaire). | RSSI, équipe de relations publiques | **Post-résolution** | | **Mises à jour des parties prenantes** | Fournir des mises à jour régulières aux parties prenantes (y compris les utilisateurs concernés) jusqu'à la résolution. | Responsable de la réponse aux incidents, RSSI | **En continu (toutes les 1 à 2 heures)** | | **Rapport post-incident** | Documentez le calendrier complet et les mesures prises, y compris les éventuels échecs et améliorations. | Responsable de la réponse aux incidents, RSSI | **Dans les 24 à 48 heures** |

5.5 Examen post-incident

| **Action** | **Description** | **Partie responsable** | **Chronologie** | |---------- --------- --|--------- ----------| | **Rapport d'incident** | Créez un rapport d'incident détaillé décrivant ce qui s'est produit, comment il a été géré et son impact. | Responsable de la réponse aux incidents, RSSI | **Dans les 24 heures** | | **Séance sur les leçons apprises** | Organiser une réunion avec toutes les parties prenantes concernées pour examiner l'incident et en déduire des actions d'amélioration. | RSSI, responsable de la réponse aux incidents | **Dans les 48 heures** | | **Mettre à jour les procédures de réponse** | Réviser le plan de réponse aux incidents en fonction des leçons apprises. | Responsable de la réponse aux incidents | **Dans les 72 heures** | | **Formation de suivi** | Organiser des

formations de recyclage et des simulations pour les employés sur les protocoles de sécurité améliorés. | RH, équipe de sécurité | **En cours** |

#**6. Sauvegarde, récupération et continuité des activités des données**

Stratégie de sauvegarde 6.1 : la règle 3-2-1

Composants de sauvegarde :

Composant de sauvegarde	**Description**	**Outils/systèmes utilisés**	**Mise en œuvre dans le monde réel**	**Planification pré-incident**	**Délai de réponse**		---	---	---	---	---	---
3 copies de données	Conservez trois copies des données : la copie principale (en direct), une copie de sauvegarde stockée localement et une copie de sauvegarde hors site.	- **Données primaires** : systèmes actifs. - **Copie de sauvegarde 1** : sauvegarde sur site avec **Veeam Backup**. - **Copie de sauvegarde 2** : sauvegarde hors site avec ** AWS S3** ou **Azure Blob Storage**.	**Copie principale** : systèmes actifs, y compris les environnements de production tels que **SAP**, **Salesforce**, **Microsoft 365** et données opérationnelles critiques. **Copie de sauvegarde 1** : **Sauvegarde Veeam** sur site **NAS (NetApp)** situé dans le **Centre de données de l'UNICEF à Genève (Suisse)**. **Copie de sauvegarde 2** : stockage cloud dans **AWS S3** et **Azure Blob Storage** (Irlande pour l'Europe et Singapour pour l'Asie-Pacifique).	- Tâches de sauvegarde configurées à une fréquence **horaire** pour les systèmes critiques (par exemple, systèmes de paie, financiers et RH). - Configuration du **stockage cloud** pour inclure la **géoredondance**.	**Fréquence de sauvegarde** : **Horaire** pour tous les systèmes critiques. - **Vérifications de l'intégrité des sauvegardes** : **Hebdomadaire** pour les sauvegardes sur site (NAS) et **mensuellement** pour les sauvegardes dans le cloud (AWS S3, Azure Blob).	
2 médias différents	Utilisez deux types de supports différents pour garantir la redondance en cas de panne de l'un d'entre eux.	- **Sauvegarde sur site** : **NAS (Network Attached Storage)** pour le stockage local. - **Sauvegarde hors site** : stockage dans le cloud (par exemple, **AWS S3** ou **Azure Blob Storage **).	**Sauvegarde sur site** : appareil **NetApp NAS** d'une capacité de 10 To à **Genève (Suisse)**, connecté aux systèmes internes. **Sauvegarde hors site** : **AWS S3** en **UE-Irlande** et **Asie-Pacifique-Singapour**, avec des données de sauvegarde répliquées entre plusieurs régions pour la reprise après sinistre.	- Les appareils NAS sur site sont **mis en miroir** pour garantir la **redondance** au sein du centre de données de Genève. - La **réplication de sauvegarde dans le cloud** garantit que les données en **Irlande** et **Singapour** sont actives. -à jour avec la dernière sauvegarde horaire.	**Fréquence de sauvegarde** : mises à jour **horaires**. - **Vérification de sauvegarde dans le cloud** : tests de vérification mensuels à l'aide d'AWS et d'Azure pour garantir la disponibilité et l'intégrité des données.	
1 emplacement hors site	Stockez au moins une copie de sauvegarde hors site, de préférence dans des emplacements géographiquement distincts pour atténuer les catastrophes régionales.	- **Sauvegarde hors site** : stockage cloud sur **AWS S3** ou **Azure Blob Storage**.	**Sauvegarde hors site** : **AWS S3** en **Irlande (UE)** pour les opérations européennes, et dans la région **Singapour** pour l'Asie-Pacifique. Utilisez **la géoredondance d'AWS S3** pour répliquer les sauvegardes sur différentes zones et régions de

disponibilité pour plus de résilience. | - Assurez-vous que le **stockage cloud géo-redondant** est configuré pour garantir que les copies de sauvegarde sont géographiquement séparées.
- **Mécanismes de basculement automatique** en place pour restaurer les opérations à partir de l'emplacement secondaire. | **Fréquence de sauvegarde** : **Horaire**.
- **Simulation de reprise après sinistre** : simulation annuelle du processus de basculement dans le cloud pour la validation de la géoredondance. |

Mise en œuvre détaillée et réelle de la stratégie de sauvegarde :

- **Fréquence de sauvegarde** :
  Les systèmes critiques sont sauvegardés toutes les heures. Cela comprend :
  - **Systèmes financiers (SAP)**
  - **Systèmes RH (Workday, bases de données de paie)**
  - **Gestion de la relation client (Salesforce)**
  - **Données sur les infrastructures de base de l'UNICEF** Ces sauvegardes sont effectuées avec **Veeam Backup & Replication**, stockant les données sur **NetApp NAS** sur site et **AWS S3** hors site.
- **Tests de sauvegarde et intégrité** :
  Les sauvegardes sont vérifiées chaque semaine pour garantir la cohérence. Si des problèmes sont détectés, ils sont immédiatement résolus et la sauvegarde réussie la plus récente est restaurée pour garantir la disponibilité en cas de sinistre.

6.2 Objectif de point de récupération (RPO) et objectif de temps de récupération (RTO)

Objectif de point de récupération (RPO)

Le RPO définit le niveau de perte de données acceptable en cas d'incident, en précisant la fréquence à laquelle les sauvegardes doivent avoir lieu. Pour l'UNICEF, le **RPO est de 1 heure**, ce qui signifie que les sauvegardes de données doivent être effectuées au moins toutes les heures pour garantir que, dans le pire des cas, pas plus d'une heure de données ne soient perdues en cas de panne.

| **Métrique** | **Valeur** | **Description** | **Outils/systèmes utilisés** | **Mise en œuvre dans le monde réel** | **Délai de réponse** | |----------|----------|---------- ---------- -----|---------- ---------- ----|---------- ----------| | **RPO** | **1 heure** | Perte de données maximale autorisée lors d'un incident (la perte de données est limitée à une heure de données). | - **Veeam Backup** (sauvegardes horaires sur site).
- **AWS S3** (sauvegardes horaires hors site). | **Fréquence de sauvegarde** : les données sont sauvegardées toutes les **heures** pour les systèmes critiques à l'aide de **Veeam Backup** (sur site) et **AWS S3** (cloud). Toutes les sauvegardes sont validées et vérifiées pour leur intégrité afin de garantir une restauration précise. | **Fréquence de sauvegarde** : **Toutes les heures**.
Vérification des sauvegardes : Hebdomadaire pour les sauvegardes sur site et mensuellement pour les sauvegardes dans le cloud. |

Mise en œuvre RPO dans le monde réel :

- **Sauvegardes automatisées** :
  Les systèmes critiques tels que **SAP** et **Salesforce** sont automatiquement sauvegardés toutes les heures. Cela minimise le risque de perte de données, garantissant que la sauvegarde la plus récente contient des enregistrements à jour.

- **Stratégie de sauvegarde incrémentielle** :
  Pour améliorer l'efficacité, seules les modifications apportées aux données (sauvegardes incrémentielles) sont enregistrées après la sauvegarde complète initiale, réduisant ainsi le temps de sauvegarde et les besoins de stockage.

Objectif de temps de récupération (RTO)

Le RTO fait référence au temps maximum autorisé pour restaurer les systèmes et les données après une interruption. Le **RTO de l'UNICEF est de 4 heures**, ce qui signifie que l'organisation vise à restaurer les services et les données critiques dans les **4 heures** suivant une interruption.

| **Métrique** | **Valeur** | **Description** | **Outils/systèmes utilisés** | **Mise en œuvre dans le monde réel** | **Délai de réponse** | |----------|----------|---------- ---------- -----|---------- ---------- ---|---------- ----------| | **OTR** | **4 heures** | Temps d'arrêt maximum autorisé pour les systèmes critiques (les systèmes doivent être opérationnels dans les 4 heures). | - **Veeam Backup** : restauration de sauvegarde sur site.
- **AWS S3** : restauration basée sur le cloud. | **Restauration des systèmes critiques** : la restauration des systèmes essentiels (par exemple, **SAP**, **Salesforce**, **Workday**) doit être effectuée dans un délai de 4 heures. Les systèmes de sauvegarde sont restaurés à partir de **Veeam Backup** (sur site) ou **AWS S3** (cloud), selon les besoins. | **Délai de restauration** : dans les **4 heures** pour les systèmes principaux. |

Mise en œuvre RTO dans le monde réel :

- **Récupération prioritaire** :
  SAP (ERP), **Salesforce** (CRM) et **Workday** (HR) sont les principales priorités en matière de restauration. Ces systèmes sont essentiels aux opérations quotidiennes de l'UNICEF. Après un incident, ces systèmes doivent être restaurés en premier, dans les 4 heures suivant leur détection.

- **Redondance pour les systèmes critiques** :
  Des systèmes redondants sont en place pour garantir que ces applications sont disponibles dans la fenêtre de récupération. Par exemple, **SAP** est sauvegardé à la fois sur site et dans le cloud (via **AWS S3**), permettant une restauration flexible.

6.3 Planification de la continuité des activités (PCA)

Le BCP garantit que l'UNICEF peut poursuivre ses fonctions essentielles pendant et après un incident. Voici comment l'UNICEF a mis en œuvre son PCA :

| **Composant PCA** | **Description** | **Outils/systèmes utilisés** | **Mise en œuvre dans le monde réel** | **Planification pré-incident** | **Délai de réponse** | |----------|----------- ---------- ---------- ---------- -------|---------- ----------|---------- ---------- ----------|---------- ----------|---------- ----------|---------- ----------| |

Identification du système critique | Identifiez les systèmes critiques à prioriser lors de la récupération. | - **SAP**, **Salesforce**, **Veeam Backup**, **AWS S3** | **Systèmes critiques** : **Salesforce**, **SAP**, **Workday** sont répertoriés comme les plus critiques.
Ils sont restaurés en premier, suivis par les systèmes secondaires tels que les serveurs de messagerie et les outils de collaboration internes. | - Le **Plan de continuité des activités** donne la priorité aux **systèmes critiques**.
- Chaque application critique a un propriétaire de récupération désigné. | **Identification immédiate** : 0 à 15 minutes après la détection de l'incident. | | **Activation d'un site alternatif** | Établissez des environnements cloud alternatifs pour assurer la continuité en cas de panne. | - **AWS EC2**, **Microsoft Azure** | Le basculement s'effectue vers **AWS EC2** (Irlande) ou **Azure** (Singapour) pour les services critiques.
Si le centre de données de Genève devient indisponible, le basculement vers le cloud est automatiquement déclenché. | - Les paramètres de basculement vers le cloud et les **configurations de site alternatives** sont préétablis.
Les applications basées sur le cloud (par exemple, Salesforce) sont mises en miroir en permanence. | **Activation immédiate du basculement (dans un délai d'une heure)** si les systèmes principaux sont en panne. | | **Accès aux données et communication** | Assurez-vous que les employés peuvent accéder à distance et en toute sécurité aux données critiques et communiquer lors d'un incident. | - **Microsoft Teams**, **Slack**, **AWS WorkDocs** | **Microsoft Teams** et **Slack** servent d'outils de collaboration.
L'accès à distance est activé via **VPN** pour un accès sécurisé aux données. **AWS WorkDocs** est utilisé pour le partage de documents en cas de panne du système local. | - **VPN** préconfigurés pour le personnel distant. Les outils **Cloud Collaboration** tels que **Microsoft Teams** et **Slack** sont régulièrement testés. | **Accès immédiat aux communications** : dans les **30 minutes** suivant l'échec. |

6.4 Tests de continuité des activités et calendrier

| **Action** | **Description** | **Partie responsable** | **Chronologie** | |---------------------------|---------- -- ---------|-------------------------|--- ---| | **Vérification des sauvegardes** | Testez régulièrement les systèmes de sauvegarde pour vérifier l'intégrité des données et les processus de restauration. | Support informatique, responsable de la réponse aux incidents | **Hebdomadaire pour les sauvegardes sur site**.
Mensuel pour les sauvegardes dans le cloud | | **Exercices de reprise après sinistre** | Tests de récupération à grande échelle pour simuler différents scénarios de catastrophe et garantir que le RTO est respecté. | Support informatique, RSSI | **Trimestriel** | | **Test de continuité des activités** | Testez les protocoles de continuité d'activité pour les systèmes critiques, y compris le basculement des systèmes vers d'autres emplacements. | Responsable de la réponse aux incidents, RSSI | **Annuellement** | | **Examen post-incident et leçons apprises**| Après un incident, effectuez un examen pour identifier les domaines à améliorer et garantir une préparation continue. | Responsable de la réponse aux incidents, RSSI | **Dans les 48 heures suivant la résolution de l'incident** |

#**7. Sécurité des points de terminaison**

La stratégie de sécurité des terminaux de l'UNICEF est essentielle pour protéger tous les appareils utilisés par les employés, les sous-traitants et le personnel distant. Cela inclut les ordinateurs de bureau, les ordinateurs portables, les appareils mobiles et d'autres types de points de terminaison. Le but de cette politique est de garantir que tous les points finaux sont protégés contre les menaces de sécurité, les

vulnérabilités et les accès non autorisés, en minimisant le risque de violation de données et en garantissant le respect des exigences de sécurité organisationnelles et juridiques.

7.1 Outils pour la protection des points finaux

L'UNICEF déploie une suite complète d'outils pour la protection des terminaux, fournissant une stratégie de défense à plusieurs niveaux pour se protéger contre l'évolution des menaces de cybersécurité. Ces outils sont mis en œuvre à l'échelle mondiale dans tous les sites de l'UNICEF pour garantir le maintien de normes de sécurité uniformes.

| **Outil de sécurité** | **Description** | **Mise en œuvre** | **Lieux de déploiement** | |---|---|---|---| | **CrowdStrike Faucon** | Une plateforme avancée de protection des points de terminaison offrant une détection des menaces en temps réel, une réponse automatisée et une enquête sur les incidents. | Tous les appareils sont surveillés en permanence pour détecter les risques de sécurité potentiels tels que les logiciels malveillants, les ransomwares et les APT. | **Tous les bureaux et sites extérieurs de l'UNICEF dans le monde**, y compris **Genève**, **Bangkok**, **New York**, **Bangladesh** et **Soudan du Sud**. | | **Microsoft Defender pour point de terminaison** | Fournit une protection complète pour les points de terminaison **Windows** contre les logiciels malveillants, les ransomwares et les exploits. | Defender offre une protection en temps réel, une gestion des vulnérabilités et une correction automatisée pour tous les appareils Windows. | **Ordinateurs portables et de bureau Windows** dans tous les sites de l'UNICEF. | | **VMware AirWatch (MDM)** | Une solution de gestion des appareils mobiles qui gère et sécurise les appareils mobiles tels que les smartphones et les tablettes utilisés par les employés. | Applique des politiques de sécurité telles que le cryptage des appareils, la liste blanche des applications et l'effacement à distance en cas de vol ou de perte. | Déployé sur tous les appareils mobiles dans le monde, en particulier pour les agents de terrain dans des régions comme l'**Ouganda**, le **Mexique**, l'**Afghanistan** et la **Syrie**. | | **Sophos Antivirus** | Une solution offrant une protection avancée contre les logiciels malveillants, les ransomwares et autres activités malveillantes sur les appareils macOS. | Fournit une détection en temps réel des menaces sur les points de terminaison basés sur macOS. | Implémenté sur tous les **appareils macOS** utilisés par le personnel en **Europe**, **Asie** et **Amériques**. | | **BitLocker (Windows)** | Logiciel de cryptage complet du disque pour ordinateurs portables et de bureau **Windows** afin de protéger les données stockées sur l'appareil en cas de vol ou d'accès non autorisé. | Chiffre automatiquement tous les appareils pour garantir que les informations sensibles restent sécurisées. | Appliqué à tous les **ordinateurs portables et de bureau Windows** dans les **opérations mondiales**. | | **FileVault (macOS)** | Chiffrement complet du disque pour les appareils **macOS** garantissant que toutes les données sont chiffrées et protégées contre tout accès non autorisé. | Appliqué à tous les ordinateurs portables et tablettes **macOS** utilisés par le personnel et le personnel de terrain. | Appliqué à l'échelle mondiale, en particulier pour les opérations sur le terrain en **Syrie**, au **Liban** et au **Soudan du Sud**. | | **AppLocker (Windows)** | Outil de liste blanche d'applications qui contrôle quelles applications peuvent être exécutées sur les appareils **Windows**, minimisant ainsi le risque d'applications non approuvées ou de logiciels malveillants. | Configuré pour empêcher l'exécution d'applications non autorisées sur tous les appareils **Windows**. | Appliqué sur tous les **ordinateurs portables** et **ordinateurs de bureau** Windows en **Europe**, **Afrique** et **Amériques**. | | **Sauvegarde et réplication Veeam** | Solution de sauvegarde des données garantissant que toutes les données des points finaux sont sauvegardées régulièrement dans un emplacement sécurisé hors site, permettant une récupération rapide en cas de perte de données ou de panne de périphérique. | Sauvegardes régulières des données des points finaux pour garantir une récupération rapide en cas d'incident. | Déployé dans les **bureaux de l'UNICEF** et les **sites sur le terrain**, en

mettant l'accent sur l'**Afrique**, l'**Asie** et le **Moyen-Orient**. | | **Splunk Entreprise |** Gestion centralisée des journaux et plateforme SIEM (Security Information and Event Management) utilisée pour surveiller les activités des points finaux et identifier les menaces de sécurité potentielles. | Regroupe les journaux de sécurité des points finaux de tous les emplacements à des fins d'analyse des menaces, de détection des anomalies et d'audit. | Appliqué à l'échelle mondiale dans tous les **bureaux de l'UNICEF** et **opérations sur le terrain à distance**. |

7.2 Politique de protection des points de terminaison

L'UNICEF applique une **Politique de protection des points finaux** stricte qui garantit que tous les appareils respectent les normes de sécurité prédéfinies. Cette politique s'applique à tous les employés, sous-traitants et personnel distant utilisant n'importe quel point de terminaison pour accéder au réseau, aux données et aux systèmes de l'UNICEF.

| **Composant de stratégie** | **Détails de la politique** | **Mécanismes d'application** | **Lieux de mise en œuvre** | |---------------------------------|-------------- --- ---|--------- --- ---------|--- ---| | **Antivirus et anti-malware** | Tous les points de terminaison doivent disposer d'un logiciel antivirus et anti-malware installé, configuré et mis à jour régulièrement. | **Windows Defender** (pour **Windows**), **Sophos Antivirus** (pour **macOS**), **CrowdStrike Falcon** (pour tous les appareils). | Appliqué à l'échelle mondiale sur **Windows**, **macOS** et les appareils mobiles à **New York**, **Genève**, **Bangladesh**, **Syrie** et dans d'autres bureaux extérieurs. | | **Mises à jour automatiques** | Le logiciel antivirus doit être configuré pour se mettre à jour automatiquement afin de bénéficier d'une protection en temps réel contre les menaces nouvelles et émergentes. | Géré via des **systèmes de gestion centralisés** comme **Splunk** et **CrowdStrike**. Des mises à jour automatisées sont programmées quotidiennement. | Garanti dans tous les **bureaux de l'UNICEF** et **sites éloignés** en **Afrique**, **Asie** et **Amériques**. | | **Chiffrement complet du disque (FDE)** | Tous les appareils doivent utiliser le cryptage complet du disque pour garantir que les données sont protégées contre tout accès non autorisé en cas de perte ou de vol. | **BitLocker** (pour **Windows**) et **FileVault** (pour **macOS**) sont requis et appliqués sur tous les appareils. | Appliqué à tous les **ordinateurs portables Windows**, **ordinateurs portables macOS** et **appareils de terrain** dans le monde, en particulier pour le personnel en **Afrique** et au **Moyen-Orient**. | | **Politique de mot de passe** | Des politiques de mot de passe strictes sont appliquées sur tous les appareils pour empêcher tout accès non autorisé aux points finaux. Une complexité minimale et des changements périodiques sont requis. | **Okta** pour l'authentification centralisée et **Active Directory** pour renforcer la sécurité des mots de passe et modifier les politiques. | Appliqué à l'échelle mondiale pour tous les **employés de l'UNICEF** sur tous les sites. | | **Liste blanche des applications** | Seules les applications approuvées sont autorisées à s'exécuter sur les appareils afin de réduire le risque de logiciels malveillants ou d'exécution de logiciels non autorisés. | **AppLocker** pour **Windows** et **Gestion des applications mobiles** via **AirWatch**. | Appliqué à tous les **ordinateurs portables Windows** et **appareils mobiles** en **Europe**, **Moyen-Orient**, **Asie**, **Afrique** et **Amériques**. | | **Gestion des appareils mobiles (MDM) |** Tous les appareils mobiles utilisés pour accéder aux systèmes **UNICEF** doivent être gérés par un système MDM pour appliquer des politiques de sécurité telles que le cryptage, la liste blanche des applications et l'effacement à distance. | Géré via **VMware AirWatch**, qui applique les paramètres de sécurité pour les appareils mobiles. | Appliqué à l'échelle mondiale pour tous les appareils mobiles au **Soudan du Sud**, au **Liban**, au **Pakistan** et au **Mexique**. | | **Effacement à distance** | En cas de perte ou de vol, les appareils doivent être effacés à distance pour garantir que les données sensibles ne soient pas exposées. | Les stratégies d'effacement à distance** sont intégrées à **AirWatch**, **BitLocker** et **FileVault** pour les appareils mobiles et non mobiles. | Appliqué à l'échelle mondiale, en particulier dans les régions **à haut

risque comme la **Syrie**, le **Soudan du Sud**, l'**Ouganda** et le **Honduras**. | | **Rapport d'incident** | Toute activité suspecte ou incident de sécurité doit être immédiatement signalé au Security Operations Center (SOC) via la plateforme **ServiceNow**. | **SOC** répond aux incidents par une enquête et des mesures correctives immédiates, à l'aide d'outils tels que **Splunk** et **CrowdStrike**. | Appliqué dans **tous les bureaux** de **New York**, **Genève**, **Bangladesh**, **Soudan du Sud**, **Syrie**, **Mexique** et ** Liban**. |

7.3 Surveillance et réponse

L'UNICEF utilise une surveillance continue des points finaux, en utilisant des technologies de détection avancées et des systèmes centralisés de gestion des incidents pour garantir une réponse rapide aux incidents de sécurité potentiels. La surveillance et la réponse sont cruciales pour maintenir la sécurité des points finaux, en particulier pour détecter et atténuer toute menace susceptible de compromettre l'intégrité des données sensibles.

| **Outil de surveillance** | **Description** | **But** | **Mécanisme de réponse** | |---------------------------------|-- ---|--------- -- ---------|--- ---| | **Splunk** | Gestion centralisée des journaux et plateforme SIEM (Security Information and Event Management) pour la surveillance des points finaux en temps réel. | Fournit une vue globale de l'activité des points finaux, détectant les menaces et les comportements suspects sur tous les appareils. | Alertes immédiates en cas d'activité suspecte. Les équipes de sécurité sont prévenues et une enquête est ouverte. | | **CrowdStrike Faucon** | Outil de détection et de réponse des points finaux (EDR) pour la surveillance des menaces en temps réel et la réponse automatisée. | Surveille tous les points de terminaison pour détecter les menaces telles que les logiciels malveillants, les accès non autorisés et les vulnérabilités du système. | Quarantaine automatisée des appareils infectés. Les équipes de réponse aux incidents prennent des mesures en fonction de la gravité. | | **VMware AirWatch** | Outil de gestion des appareils mobiles qui assure une surveillance en temps réel des appareils mobiles et applique les politiques de sécurité. | Détecte et signale les incidents de sécurité impliquant les appareils mobiles. | Alertes automatisées déclenchées pour les appareils non conformes. L'effacement ou le verrouillage à distance est appliqué si nécessaire. | | **Microsoft Defender pour point de terminaison** | Fournit une gestion complète des menaces et des vulnérabilités pour les appareils Windows, y compris des capacités de détection et de correction. | Détecte et corrige les menaces sur les points de terminaison **Windows**. | Détection immédiate et isolation automatisée des points finaux compromis. Enquête de suivi et réparation. | | **Détection et réponse des points de terminaison (EDR)** | Ensemble d'outils intégré combinant **CrowdStrike**, **Microsoft Defender** et **Splunk** pour surveiller, détecter et répondre aux incidents de sécurité sur tous les points de terminaison. | Combine une surveillance en temps réel, une analyse des menaces et une réponse automatisée pour garantir la protection des points finaux. | Les appareils sont isolés, la source de la menace est identifiée et des actions correctives sont appliquées. |

En déployant ces outils et en appliquant les politiques décrites ci-dessus, l'UNICEF maintient un environnement sécurisé pour tous les points finaux et garantit que tous les employés, sous-traitants et personnel de terrain adhèrent aux normes de cybersécurité de l'organisation.

---

8. Sécurité du réseau et protection du cloud

Aperçu

La stratégie **Network Security & Cloud Protection** de l'UNICEF fait partie intégrante de la protection de son infrastructure numérique critique, garantissant que l'organisation peut gérer en toute sécurité les informations sensibles et opérer à l'échelle mondiale sans interruption. Avec la dépendance croissante aux services cloud et à un réseau décentralisé de personnel et de partenaires, la mise en œuvre d'outils avancés de sécurité réseau et cloud est cruciale. Ce qui suit décrit les mesures de sécurité du réseau et les outils de protection du cloud déployés dans l'infrastructure de l'UNICEF.

8.1 Outils de sécurité réseau

L'objectif principal de la sécurité du réseau est de garantir que le réseau interne et les actifs numériques de l'UNICEF sont protégés contre les accès non autorisés, les violations de données et les menaces persistantes avancées (APT). L'UNICEF utilise une approche à plusieurs niveaux pour la défense des réseaux qui intègre des technologies avancées telles que des pare-feu, des systèmes de détection d'intrusion, des solutions VPN et une analyse de réseau basée sur l'IA.

1. Palo Alto Networks NGFW (pare-feu de nouvelle génération)

Les NGFW **Palo Alto Networks** sont déployés sur tous les points du réseau périphérique des bureaux mondiaux et des centres de données de l'UNICEF, y compris le **siège**, les **bureaux régionaux** et les **environnements cloud**. Ces pare-feu protègent contre les menaces externes et internes, offrant une sécurité au niveau des applications et une intégration aux flux mondiaux de renseignements sur les menaces.

- **Principales fonctionnalités** :
    - **Deep Packet Inspection (DPI)** : analyse le trafic entrant et sortant au niveau de la couche application pour prévenir les attaques telles que l'**injection SQL**, le **cross-site scripting (XSS)** et d'autres attaques d'applications Web.
    - **Threat Intelligence** : intègre des flux de renseignements sur les menaces en temps réel pour bloquer l'accès aux adresses IP, domaines et URL malveillants associés à des menaces connues (par exemple, ransomware, phishing).
    - **Déchiffrement SSL** : garantit que le trafic chiffré (SSL/TLS) est inspecté à la recherche de menaces cachées, garantissant ainsi une sécurité de bout en bout.
- **Déploiement** :
    - **Couverture mondiale** : déployé dans les **centres de données de l'UNICEF** à **New York (Est des États-Unis)**, **Bruxelles (Europe)**, **Singapour (APAC)**, **Kenya. (Afrique)** et **Sydney (Australie)**.
    - **Environnements cloud** : intégré aux services cloud AWS et **Azure**, sécurisant les **VPC (Virtual Private Clouds)** et protégeant les applications internes déployées dans plusieurs régions.

2. Snort IDS/IPS (système de détection/prévention des intrusions)

Snort sert de principal système de détection et de prévention des intrusions (IDS/IPS) de l'UNICEF pour détecter et bloquer le trafic suspect sur la base de signatures prédéfinies. Il analyse le trafic réseau interne et externe, offrant une **surveillance en temps réel** et une détection des menaces.

- **Principales fonctionnalités** :

    - **Détection basée sur les signatures** : détecte les modèles d'attaque connus tels que les **débordements de tampon**, les **tentatives de connexion par force brute** et les **exploits Zero Day**.
    - **Analyse de protocole** : garantit que les protocoles tels que **HTTP**, **FTP**, **SMTP** et autres sont utilisés en toute sécurité et sans exploits.
    - **Alertes** : envoie des alertes en temps réel au **Centre d'opérations de sécurité (SOC)**, permettant une enquête et une réponse rapides.

- **Déploiement** :

    - Installé sur des segments de réseau internes critiques, notamment les postes de travail des employés, les serveurs de données et les environnements cloud, couvrant l'**Amérique du Nord**, l'**Europe** et l'**Afrique**.
    - Déployé dans **l'infrastructure sur site** et dans **l'infrastructure cloud** de l'UNICEF pour surveiller le trafic réseau interne dans **AWS** et **Microsoft Azure**.

3. VPN de Palo Alto Networks (GlobalProtect)

Palo Alto Networks GlobalProtect fournit un accès à distance sécurisé aux employés, sous-traitants et personnel de terrain de l'UNICEF opérant dans le monde entier. La solution VPN garantit que les données sensibles restent cryptées pendant leur transit et que les utilisateurs non autorisés ne peuvent pas accéder au réseau interne.

- **Principales fonctionnalités** :

    - **Cryptage SSL** : utilise le **cryptage SSL/TLS** pour sécuriser les échanges de données sur Internet et empêcher les interceptions non autorisées.
    - **Authentification multifacteur (MFA)** : garantit que seul le personnel autorisé peut accéder aux ressources internes en exigeant des facteurs d'authentification supplémentaires.
    - **Sécurité côté client** : les appareils doivent répondre à des critères de sécurité (par exemple, antivirus mis à jour, cryptage) avant d'accorder l'accès au réseau.

- **Déploiement** :

    - Les clients VPN sont déployés dans le monde entier, avec **priorité pour les bureaux distants** et les opérations sur le terrain dans des régions comme le **Soudan du Sud**, la **Syrie** et le **Brésil** où la sécurité Internet est cruciale.
    - Également utilisé par les employés de l'entreprise et les équipes administratives qui accèdent à distance aux applications et fichiers internes depuis des bureaux situés à **New York**, **Londres**, **Genève** et autres.

4. Darktrace AI pour l'analyse du trafic réseau

Darktrace est une solution basée sur l'IA déployée pour analyser et surveiller l'activité réseau à tous les niveaux de l'organisation. Il utilise l'**apprentissage automatique** pour s'adapter en permanence aux changements de comportement du réseau et identifier les menaces de sécurité potentielles qui pourraient autrement passer inaperçues par les méthodes traditionnelles.

- **Principales fonctionnalités** :

    - **Détection d'anomalies** : détecte les modèles d'activité inhabituels qui indiquent une violation potentielle, tels qu'un **mouvement latéral** au sein du réseau ou un accès inhabituel à des données sensibles.
    - **Capacité d'auto-apprentissage** : apprend et s'adapte en permanence au comportement normal du réseau, réduisant ainsi les faux positifs et permettant une détection plus précise des menaces.
    - **Réponse autonome** : peut entreprendre des actions automatisées, telles que la mise en quarantaine des appareils suspects ou le blocage du trafic associé à une activité malveillante.

- **Déploiement** :

    - Déployé à l'échelle mondiale, couvrant tous les bureaux de l'UNICEF, les environnements cloud et les réseaux de partenaires externes. Critique dans les régions à haut risque d'exposition aux cybermenaces, comme l'**Afrique de l'Est** et l'**Amérique du Sud**.

8.2 Sécurité du cloud

Compte tenu de l'utilisation par l'UNICEF de plates-formes cloud telles que **AWS**, **Microsoft Azure** et **Google Cloud**, la sécurisation de ces environnements est primordiale. Les outils et stratégies suivants garantissent la protection des données, la conformité et l'atténuation des menaces au sein des systèmes basés sur le cloud.

1. Prisma Cloud par Palo Alto Networks

Prisma Cloud offre une sécurité de bout en bout pour les charges de travail dans les environnements cloud de l'UNICEF, notamment **AWS**, **Azure** et **Google Cloud**. La plateforme garantit la conformité aux réglementations mondiales en matière de protection des données, telles que le **RGPD**, et analyse les environnements cloud à la recherche de vulnérabilités et de mauvaises configurations.

- **Principales fonctionnalités** :

    - **Cloud Security Posture Management (CSPM)** : surveille en permanence les environnements cloud pour détecter les erreurs de configuration, garantissant ainsi que les ressources sont configurées et conformes en toute sécurité.
    - **Analyse des vulnérabilités** : analyse les conteneurs, les machines virtuelles (VM) et d'autres ressources à la recherche de vulnérabilités connues.
    - **Surveillance de la conformité** : évalue les configurations cloud par rapport à des cadres tels que **ISO 27001**, **NIST** et **GDPR** pour garantir la conformité aux normes de sécurité.

- **Déploiement** :

    - Mis en œuvre sur les plateformes **AWS** de l'UNICEF (Irlande, Singapour, Est des États-Unis), **Microsoft Azure** (Europe, Amérique du Nord) et **Google Cloud** où résident les données critiques de l'organisation.
    - Surveille spécifiquement les **applications cloud natives**, les **fonctions sans serveur** et le **stockage de données** (par exemple, les **buckets S3**, **Azure Blob Storage**) pour détecter les accès ou les données non autorisés. fuite.

2. Netskope CASB (courtier de sécurité d'accès au cloud)

Netskope offre une visibilité et un contrôle sur les applications cloud, garantissant ainsi que les données stockées sur les plates-formes SaaS telles que **Google Workspace**, **Salesforce** et **Dropbox** sont accessibles en toute sécurité. Il permet d'éviter les **fuites de données** et d'appliquer les politiques de **prévention des pertes de données (DLP)**.

- **Principales fonctionnalités** :
    - **Contrôle d'accès aux données en temps réel** : surveille toutes les interactions de données avec les applications cloud pour garantir que les données sensibles ne sont pas exposées ou téléchargées par des utilisateurs non autorisés.
    - **Shadow IT Discovery** : identifie les applications cloud non autorisées (Shadow IT) utilisées par les employés et les partenaires pour stocker ou partager des informations sensibles.
    - **Protection contre les menaces** : détecte et prévient les tentatives de logiciels malveillants, de ransomware et de phishing dans les environnements cloud.
- **Déploiement** :
    - Déployé sur des applications **SaaS** utilisées par l'UNICEF dans le monde entier, telles que **Google Workspace** (Docs, Sheets), **Dropbox** et **Salesforce** pour le CRM et la gestion des donateurs.
    - Couvre la **présence mondiale** de l'organisation, y compris les zones à haut risque telles que l'**Europe de l'Est**, l'**Amérique latine** et l'**Asie du Sud-Est**.

3. AWS CloudTrail

AWS CloudTrail est utilisé pour enregistrer chaque appel d'API effectué au sein des services AWS, garantissant ainsi une visibilité sur toutes les interactions avec l'environnement cloud. CloudTrail fournit des enregistrements détaillés indiquant **qui a accédé à quelles ressources**, **quand** et **quelles actions ont été effectuées**.

- **Principales fonctionnalités** :
    - **Journalisation des activités API** : capture chaque action effectuée dans AWS, y compris la personne à l'origine de la demande, ce qui a été modifié et le résultat.
    - **Pistes d'audit** : aide les équipes médico-légales à enquêter sur les activités suspectes et fournit des preuves pour les audits de conformité.
    - **Support multi-région** : garantit que les journaux CloudTrail sont collectés et stockés dans plusieurs régions pour éviter la perte de données en cas de panne de service régional.
- **Déploiement** :
    - Actif dans toutes les régions **AWS** de l'UNICEF, y compris l'**Irlande**, **Singapour** et **USA Est**, où sont stockées des données sensibles telles que les informations sur les donateurs, les dossiers financiers et les données du programme.
    - Garantit que les journaux sont disponibles pour les audits de sécurité, aidant ainsi l'UNICEF à maintenir la conformité aux réglementations mondiales telles que **GDPR** et **FISMA**.

4. Centre de sécurité Azure

Azure Security Center offre un système de gestion de la sécurité de l'infrastructure unifié qui offre une protection contre les menaces dans Microsoft Azure. Il aide l'UNICEF à surveiller et à gérer les politiques de sécurité sur ses ressources Azure afin d'empêcher les accès non autorisés, les violations de données et les dérives de configuration.

- **Principales fonctionnalités** :
    - **Surveillance de la conformité réglementaire** : évalue en permanence les configurations de sécurité par rapport à des normes telles que **ISO 27001**, les directives **NIST** et **RGPD** pour garantir que les ressources restent conformes.
    - **Détection et atténuation des menaces** : s'intègre à d'autres services Azure comme **Azure Sentinel** pour détecter les vulnérabilités, les logiciels malveillants et les **menaces persistantes avancées (APT)**.
- **Déploiement** :
    - Mis en œuvre dans tous les services cloud **Azure** de l'UNICEF prenant en charge les opérations critiques, y compris les systèmes de gestion des données du personnel, les **applications SAP** et les plateformes de gestion financière hébergées en **Allemagne**, **Amérique du Nord**, et **Asie-Pacifique**.

Réponse aux incidents pour la sécurité du réseau et du cloud

Le plan de réponse aux incidents de l’UNICEF pour la sécurité des réseaux et du cloud est structuré pour identifier, contenir et atténuer rapidement les failles de sécurité potentielles. Le processus garantit que chaque incident est traité rapidement,

minimiser les dommages et garantir le respect des réglementations en matière de protection des données.

| **Phase** | **Action** | **Laps de temps** | **Partie responsable** | |----------------------|---------------------------- ----------|-------------- ----------------------|---------------------------- ------| | **Détection** | Les alertes de **Palo Alto NGFW**, **Snort** et **Prisma Cloud** signalent des failles de sécurité potentielles. | Immédiat (en quelques minutes) | Équipe SOC, analystes de sécurité | | **Triage** | Évaluer la portée et l'impact potentiel de l'incident, en hiérarchisant les efforts de réponse en fonction de la gravité. | 10-30 minutes | Responsable de la réponse aux incidents, équipe SOC| | **Endiguement** | Isoler les systèmes ou les ressources cloud compromis à l'aide de **pare-feu** et de **groupes de sécurité**. | 30 à 60 minutes | Opérations informatiques, analystes de sécurité | | **Éradication** | Identifier les processus malveillants ou les utilisateurs non autorisés et les supprimer de l'environnement. | 1-2 heures | Support informatique, analystes de sécurité | | **Récupération** | Restauration des services à partir de sauvegardes (par exemple, **AWS S3**, **Azure Recovery**) et vérification de la sécurité des systèmes. | 2-4 heures | Support informatique, équipes d'infrastructure cloud | | **Examen post-incident** | Analyse des causes profondes, évaluation de l’impact et enseignements tirés pour améliorer la réponse et la prévention futures. | 24 à 48 heures après résolution | RSSI, responsable de la réponse aux incidents |

---

9. Sensibilisation et formation des employés

9.1 Formation de sensibilisation à la sécurité

Les programmes de sensibilisation et de formation des employés de l'UNICEF sont conçus pour améliorer continuellement la culture de sécurité au sein de l'organisation. La formation se concentre sur des scénarios pratiques et des cybermenaces critiques, avec un fort accent sur les tests pratiques au moyen d'exercices simulés.

Plateformes et outils de formation

1. **KnowBe4** :
    - **Plateforme de simulation de formation et de phishing** : l'UNICEF utilise **KnowBe4** comme plate-forme principale pour diffuser du contenu de formation et réaliser des simulations de phishing. Cette plateforme propose des modules de formation interactifs sur un large éventail de sujets liés à la cybersécurité.
    - **Outil de simulation de phishing** : **KnowBe4** envoie des e-mails de phishing simulés aux employés pour évaluer leur capacité à reconnaître les e-mails malveillants. Ces e-mails sont adaptés pour refléter les vecteurs d'attaque du monde réel pertinents pour les opérations de l'UNICEF.
2. **Centre de sensibilisation à la cybersécurité** :
    - **Base de connaissances interne** : en plus de **KnowBe4**, l'UNICEF gère un hub interne pour les ressources de sécurité, qui comprend des guides, des FAQ et des didacticiels vidéo sur la gestion sécurisée des données, l'évitement de l'ingénierie sociale et l'utilisation d'outils internes (comme **Slack**, **Workday** et **Salesforce**) en toute sécurité.
    - **Formation de recyclage obligatoire sur la sécurité** : tous les trimestres, tous les employés doivent revoir les concepts de sécurité de base grâce à des cours de recyclage obligatoires, qui incluent l'examen des récents modèles d'attaques de phishing, des conseils de cybersécurité et des meilleures pratiques en matière de traitement des données.

Sujets de formation

1. **Phishing et ingénierie sociale** :
    - **Objectif** : doter les employés des compétences nécessaires pour reconnaître les tentatives de phishing courantes et les tactiques d'ingénierie sociale conçues pour voler des données sensibles.
    - **Durée de la formation** : 1h30 (initiale) / remise à niveau de 30 minutes (trimestrielle).
    - **Livraison** : cours interactif en ligne avec des simulations d'e-mails de phishing réels.
    - **Exemple** : les employés seront confrontés à un e-mail de phishing simulé prétendant provenir du service des ressources humaines de l'UNICEF leur demandant de cliquer sur un lien pour vérifier leurs coordonnées bancaires. La formation fournit des conseils pour identifier ces e-mails, y compris les liens suspects et les fautes d'orthographe.
2. **Protection des données et traitement sécurisé** :
    - **Objectif** : S'assurer que les employés comprennent l'importance de la protection des données, comment stocker et partager des informations sensibles en toute sécurité et comment se conformer aux réglementations telles que le RGPD et les politiques de confidentialité internes de l'UNICEF.

- **Durée de la formation** : 1 heure.
- **Fréquence** : Annuelle.
- **Exemple** : la formation comprend des directives sur l'utilisation de **Microsoft Teams** pour la messagerie sécurisée, le chiffrement des données sensibles à l'aide de **PGP** (Pretty Good Privacy) et sur l'utilisation de **SharePoint** et **. OneDrive** pour stocker des fichiers en toute sécurité.

3. **Gestion des mots de passe** :

   - **Objectif** : Encourager les employés à utiliser des mots de passe forts et une authentification multifacteur (MFA) pour protéger leurs comptes.
   - **Durée de la formation** : 45 minutes.
   - **Fréquence** : Annuelle.
   - **Exemple** : les employés apprennent comment utiliser **LastPass** pour générer et stocker des mots de passe complexes et comment configurer MFA pour des systèmes essentiels tels que **Workday** et **SAP**. La formation comprend également un segment sur les dangers de la réutilisation des mots de passe et des conseils sur la création de phrases secrètes.

4. **Sécurité des appareils mobiles** :

   - **Objectif** : Former les employés à la sécurisation des appareils mobiles, notamment les smartphones, les ordinateurs portables et les tablettes, en particulier pour ceux qui travaillent dans des environnements distants et sur le terrain.
   - **Durée de la formation** : 1 heure.
   - **Fréquence** : Annuelle (avec un rappel trimestriel en option).
   - **Exemple** : instructions sur l'utilisation de **VMware AirWatch** pour la gestion des appareils, l'application du chiffrement complet du disque, la configuration des VPN et la configuration de l'effacement à distance des appareils perdus ou volés.

5. **Rapport et réponse aux incidents** :

   - **Objectif** : Fournir aux employés une compréhension claire de la manière de signaler les incidents de sécurité et de leur rôle dans le plan plus large de réponse aux incidents de l'organisation.
   - **Durée de la formation** : 45 minutes.
   - **Fréquence** : Biannuelle.
   - **Exemple** : les employés sont formés pour reconnaître les incidents de sécurité potentiels tels que les violations de données, les e-mails de phishing et les tentatives d'accès non autorisés, et reçoivent des directives spécifiques sur le signalement des incidents via la plateforme **ServiceNow**.

9.2 Simulations et tests de phishing

L'UNICEF s'appuie sur **KnowBe4** pour effectuer des simulations de phishing mensuelles afin d'évaluer les capacités des employés à identifier les tentatives de phishing. Ces simulations sont spécialement conçues pour imiter les tactiques d'attaque du monde réel et tester l'état de préparation général des employés.

Processus de simulation de phishing

1. **Campagnes mensuelles** :

    - **Personnalisation** : chaque simulation de phishing est conçue sur mesure pour refléter les cybermenaces actuelles et les environnements spécifiques de l'UNICEF (par exemple, en se concentrant sur les e-mails prétendant provenir de donateurs ou de partenaires de l'UNICEF).
    - **Types d'attaques** :
    - **Spear Phishing** : e-mails personnalisés ciblant des personnes ou des services spécifiques, tels que les finances, avec des demandes de traitement de paiements urgents.
    - **Whaling** : attaques de phishing de haut niveau ciblant des cadres supérieurs, se faisant souvent passer pour d'autres cadres ou membres du personnel de direction.
    - **Credential Harvesting** : e-mails simulés demandant aux employés de cliquer sur un lien et de se connecter à une fausse page de connexion **Workday** ou **Salesforce** pour voler des informations d'identification.

2. **Surveillance et commentaires en temps réel** :

    - **Commentaires immédiats** : lorsqu'un employé clique sur un lien de phishing ou soumet des informations personnelles, il reçoit un retour immédiat de **KnowBe4**, qui comprend une brève session de formation pour l'informer sur la façon de détecter les attaques de phishing.
    - **Formation de suivi ciblée** : les employés qui tombent à plusieurs reprises dans le piège des simulations de phishing sont inscrits à des sessions de formation supplémentaires ciblées axées sur le phishing et l'ingénierie sociale.

3. **Rapports et suivi** :

    - **Rapports mensuels** : à la fin de chaque campagne de simulation, les résultats sont regroupés dans des rapports détaillés indiquant combien d'employés ont cliqué sur des liens malveillants, à quelle vitesse ils ont signalé la tentative de phishing et quels employés ont besoin d'une formation supplémentaire.
    - **Analyse des tendances** : les rapports permettent à l'équipe de sécurité de l'UNICEF d'identifier les tendances au fil du temps. Par exemple, si un service spécifique est systématiquement ciblé ou si un vecteur d’attaque particulier réussit, des sessions de formation supplémentaires seront programmées.

9.3 Formation basée sur les rôles et spécialisée

Certains rôles au sein de l'UNICEF, tels que le personnel informatique, les administrateurs système et la haute direction, nécessitent une formation spécialisée et approfondie en cybersécurité. Ces programmes de formation se concentrent sur les menaces avancées et les responsabilités en matière de sécurité opérationnelle.

Programmes de formation spécifiques au rôle

1. **Administrateurs informatiques et ingénieurs système** :

    - **Formation ciblée** : Techniques avancées de sécurité réseau, évaluations des vulnérabilités, gestion des correctifs, protocoles de réponse aux incidents et configuration sécurisée du système.

- **Outils couverts** : **Splunk**, **CrowdStrike**, **Palo Alto Networks** et **AWS CloudTrail**.
- **Fréquence** : Trimestriel.
- **Durée** : 3 heures par séance.

2. **Équipe de sécurité et personnel de réponse aux incidents** :

   - **Focus de formation** : Procédures de réponse aux incidents, criminalistique numérique, gestion d'une violation et coordination avec les forces de l'ordre si nécessaire.
   - **Fréquence** : simulations trimestrielles, telles que des exercices sur table et des exercices de réponse aux incidents dans le monde réel.
   - **Durée** : 4 à 5 heures par séance.

3. **Haute direction et dirigeants** :

   - **Objectif de formation** : Comprendre les risques de sécurité au niveau de l'entreprise, sécuriser les données critiques de l'entreprise et soutenir les stratégies de cybersécurité.
   - **Sujets** : Gestion de crise lors de violations de données, communication au niveau de la direction et gestion des cyber-risques.
   - **Fréquence** : Annuelle.
   - **Durée** : 2 heures par séance.

9.4 Calendrier et calendrier de la formation

Pour garantir que les employés reçoivent une formation régulière et pertinente en matière de cybersécurité, l'UNICEF respecte le **Calendrier de formation et de sensibilisation** suivant. Ce planning est intégré dans les plans de développement annuels des salariés, avec une participation obligatoire pour tout le personnel concerné.

| **Mois** | **Activité** | **Public cible** | **Durée** | **Fréquence** | |--------------|---------------------------------- ---------------------------|------------------------- ------------|------------------|------------------ ----| | **Janvier** | **Lancement de la sensibilisation à la sécurité du Nouvel An** | Tous les employés | 1 heure | Annuel | | **Février** | **Simulation d'hameçonnage** | Tous les employés | 15 minutes | Mensuel | | **Mars** | **Gestion des mots de passe et formation MFA** | Tous les employés | 1 heure | Annuel | | **Avril** | **Formation à la sécurité pour les informaticiens/administrateurs** | Personnel informatique, administrateurs système | 3 heures | Trimestriel | | **Peut** | **Sécurité des appareils mobiles** | Travailleurs à distance, personnel de terrain | 1 heure | Annuel | | **Juin** | **Protection des données et traitement des informations sensibles** | Tous les employés | 1,5 heures | Annuel | | **Juillet** | **Formation sur la réponse aux incidents** (Réponse aux incidents simulés) | Équipe de sécurité, intervenants en cas d'incident | 4 heures | Trimestriel | | **Août** | **Simulation d'hameçonnage** | Tous les employés | 15 minutes | Mensuel | | **septembre**| **Sécurité avancée pour les dirigeants** | Cadres, haute direction | 2 heures | Annuel | | **octobre** | **Essentiels de sécurité pour les travailleurs à distance** | Travailleurs à distance, personnel de terrain | 1 heure | Annuel | | **Novembre** | **Simulation d'hameçonnage** | Tous les employés | 15 minutes | Mensuel | | **Décembre** | **Examen de sécurité et sensibilisation de fin d'année** | Tous les employés | 1 heure | Annuel |

9.5 Mesurer l'efficacité de la formation

L'efficacité de la formation est évaluée à l'aide de plusieurs mesures pour garantir que le programme de sécurité évolue et atteint ses objectifs.

1

. **Taux de clics de phishing** : surveillez la fréquence à laquelle les employés cliquent sur les liens de phishing lors de simulations mensuelles. Au fil du temps, ces taux devraient diminuer, signe que la main-d'œuvre devient plus vigilante. 2. **Évaluation des connaissances** : Des quiz en fin de formation évaluent la compréhension des collaborateurs. Les employés dont le score est inférieur à un certain seuil sont signalés pour une formation de suivi. 3. **Mesures de réponse aux incidents** : évaluez dans quelle mesure les employés réagissent aux incidents de sécurité réels, notamment en termes de reporting en temps opportun, de respect des procédures et d'implication dans les efforts d'atténuation. 4. **Mesures de culture de sensibilisation à la sécurité** : les enquêtes et les commentaires des employés aident à évaluer l'efficacité des programmes de formation et à identifier les domaines qui nécessitent des améliorations.

9.6 Amélioration continue

Le programme de formation évolue constamment en fonction des commentaires, des tendances du secteur et des menaces émergentes.

- **Examen trimestriels** : réunions régulières avec l'équipe informatique, les ressources humaines et la sécurité pour examiner les derniers résultats de simulation de phishing, les rapports d'incidents et les retours de formation.
- **Menaces émergentes** : un nouveau contenu de formation est développé à mesure que de nouvelles menaces émergent, garantissant que les employés sont toujours équipés pour se défendre contre les dernières méthodes d'attaque.
- **Boucle de rétroaction continue** : les employés sont encouragés à fournir des commentaires sur l'expérience de formation et à suggérer des domaines à améliorer, garantissant ainsi que la formation reste pertinente, engageante et efficace.

Voici une présentation **détaillée, étendue** et **réaliste** des mesures de sécurité de l'UNICEF pour la **Sécurité physique**, la **Sécurité des fournisseurs et des tiers**, les **Audits et surveillance de sécurité**, et processus associés, complets avec des **échéanciers exploitables** et un formatage **clair et structuré**.

---

10. Sécurité physique

L'UNICEF utilise une stratégie globale de sécurité physique pour protéger ses données, son infrastructure et son personnel dans l'ensemble de ses opérations mondiales. L'approche comprend un contrôle d'accès avancé, une surveillance et une surveillance environnementale pour garantir que les installations critiques sont sécurisées contre les menaces internes et externes.

10.1 Sécurité du centre de données

Les centres de données de l'UNICEF sont des actifs essentiels qui hébergent des données et des systèmes sensibles essentiels aux opérations de l'organisation dans le monde entier. Il est primordial de protéger ces

actifs contre les menaces à la sécurité physique, telles que l'accès non autorisé, le vol, le vandalisme et les risques environnementaux (par exemple, incendies, inondations).

Mesures de sécurité :

- **Contrôle d'accès biométrique** :
    - **Objectif** : garantir que seul le personnel autorisé peut accéder aux zones de haute sécurité du centre de données, telles que les salles de serveurs, l'infrastructure réseau et d'autres emplacements sensibles.
    - **Processus** : l'UNICEF utilise des **contrôles d'accès biométriques** (par exemple, **scanners d'empreintes digitales**, **scanners de la rétine** et **reconnaissance faciale**) dans toutes les zones de haute sécurité de ses données. centres. Ces systèmes enregistrent chaque entrée et sortie, qui sont suivies et examinées régulièrement pour garantir que seules les personnes autorisées y ont accès.
    - **Chronologie** : Les systèmes d'accès biométriques font l'objet d'un **examen annuel** pour en vérifier l'efficacité et l'exactitude. De plus, les autorisations d'accès sont mises à jour **trimestriellement** pour refléter les changements dans les rôles et responsabilités du personnel. Par exemple, le personnel informatique peut disposer de privilèges d'accès plus étendus, qui sont mis à jour selon les besoins.
        - **Exemple** : Au **Geneva Data Center**, les systèmes biométriques garantissent que seul un groupe sélectionné d'employés informatiques a accès à l'infrastructure de base. Le personnel de sécurité effectue des examens mensuels des journaux pour identifier toute irrégularité ou tentative d'accès non autorisée, garantissant ainsi le respect des protocoles de sécurité internes.
- **Systèmes de surveillance** :
    - **Objectif** : Surveiller en permanence les locaux pour détecter tout accès physique non autorisé ou activité suspecte.
    - **Processus** : des caméras de vidéosurveillance haute définition sont installées dans tous les centres de données, avec des **capacités de vision diurne et nocturne infrarouge** pour une surveillance 24h/24 et 7j/7. Ces caméras sont intégrées à un **système de gestion de surveillance** avancé, qui fournit des **alertes en temps réel** pour toute activité inhabituelle. Les flux de surveillance sont surveillés en permanence par le **Global Security Operations Center (GSOC)**, qui est responsable de la coordination de la réponse aux incidents.
    - **Chronologie** : les caméras de vidéosurveillance sont **inspectées chaque semaine** pour garantir leur bon fonctionnement. Un **cycle de maintenance mensuel** est en place pour calibrer les caméras et vérifier tout dysfonctionnement du système. Le système stocke les images de surveillance pendant **30 jours**, après quoi elles sont archivées pour une conservation à long terme. Toute activité suspecte enregistrée est examinée par les agents de sécurité dans les **24 heures**.
        - **Exemple** : Le **centre de données de New York** est équipé de plus de **300 caméras haute définition**, avec des **capteurs de mouvement** capables de détecter les

mouvements en temps réel. En cas de mouvement suspect, le système déclenche une notification instantanée à l'**équipe de sécurité**, qui peut prendre des mesures immédiates. Les anomalies telles qu'une tentative de contournement des barrières de sécurité ou d'accès à des zones restreintes sont signalées et transmises pour une enquête plus approfondie.

- **Contrôles environnementaux** :
    - **Objectif** : Protéger l'infrastructure informatique critique des dommages causés par des risques environnementaux, tels que les incendies, les inondations et les fluctuations de température.
    - **Processus** : tous les centres de données sont équipés de **contrôles environnementaux** de pointe, y compris des **systèmes d'extinction d'incendie** (par exemple, **gaz halon**), **détection d'inondation. capteurs** et **contrôles de température et d'humidité** (systèmes CVC). Les systèmes d'extinction d'incendie sont conçus pour empêcher la propagation du feu sans endommager les équipements électroniques sensibles. Des **simulations de risques environnementaux** et des **exercices** réguliers sont effectués pour garantir que les systèmes fonctionnent comme prévu en cas d'urgence.
    - **Chronologie** : Les systèmes environnementaux sont soumis à des **vérifications de diagnostic mensuelles** par les équipes internes et les sous-traitants tiers. De plus, des **audits annuels de sécurité contre les incendies et les inondations** sont effectués pour garantir le respect des règles de sécurité et l'état de préparation opérationnelle.
        - **Exemple** : À **Singapour**, le centre de données dispose de **capteurs de détection d'inondation** qui alertent immédiatement les équipes de sécurité si le niveau d'eau dépasse un certain seuil. En cas d'incendie, le **Système de suppression des halons** est activé automatiquement. Un contrôle de diagnostic de routine est effectué par un sous-traitant externe tous les **premiers lundis du mois** pour garantir que l'ensemble de l'infrastructure est pleinement opérationnel.

10.2 Sécurité du bureau

Les bureaux de l’UNICEF constituent un autre aspect crucial de son infrastructure de sécurité physique. Ces bureaux abritent des employés, des sous-traitants et des visiteurs, et il est impératif de maintenir des protocoles de sécurité stricts pour protéger à la fois le personnel et les informations sensibles.

Mesures de sécurité :

- **Accès par carte à puce** :
    - **Objectif** : Réguler et contrôler l'accès aux zones sécurisées du bureau, en garantissant que seul le personnel autorisé puisse pénétrer dans les lieux sensibles tels que les salles de réunion, les laboratoires et les salles de serveurs.
    - **Processus** : l'UNICEF utilise la **technologie de carte à puce** pour le contrôle d'accès. Chaque employé, sous-traitant et visiteur reçoit une **carte à puce** qui donne accès à des zones spécifiques du bureau. Les cartes à puce sont intégrées avec **authentification par code PIN** et

chaque tentative d'accès est enregistrée. Ces journaux sont examinés régulièrement par l'équipe de sécurité pour garantir leur conformité.

- **Chronologie** : les journaux d'accès sont examinés **sur une base mensuelle** et toute anomalie est signalée à l'équipe de sécurité pour une enquête immédiate. De plus, des **mises à jour trimestrielles** sont effectuées sur le système de carte à puce pour garantir que les autorisations d'accès reflètent les rôles et les niveaux d'autorisation actuels des employés.
  - **Exemple** : Au **siège de l'UNICEF à New York**, le **bâtiment principal, les salles de serveurs et les laboratoires de recherche** sont tous sécurisés par un accès par carte à puce. Lorsque le rôle d'un employé change (par exemple, promotion, transfert), ses privilèges d'accès sont mis à jour dans les **24 heures** pour garantir que seul le personnel autorisé peut accéder aux zones sensibles.

- **Système de gestion des visiteurs** :
  - **Objectif** : Garantir que tous les visiteurs des bureaux de l'UNICEF sont correctement identifiés, suivis et escortés dans les zones sensibles.
  - **Processus** : Tous les visiteurs doivent **s'inscrire** à la réception à leur arrivée. Il leur est demandé de fournir une **pièce d'identité avec photo** valide et d'indiquer le but de leur visite. Les visiteurs reçoivent un **badge visiteur** valable pendant toute la durée de leur visite. Les visiteurs accédant aux zones sensibles se voient attribuer un accompagnateur salarié qui veille à ce qu'ils restent dans les zones autorisées.
  - **Chronologie** : les journaux des visiteurs sont examinés **trimestriellement** pour garantir le fonctionnement efficace du système. Toutes les tendances ou problèmes de sécurité (tels que les tentatives d'accès non autorisées ou les visites sans escorte) sont immédiatement traités et les protocoles de sécurité sont ajustés en conséquence.
    - **Exemple** : Au **Bureau de l'UNICEF à Genève**, les visiteurs des zones de haute sécurité comme les laboratoires de recherche et les centres de données doivent porter des **badges de visiteur suivis** et être accompagnés par un employé à tout moment. Le système enregistre également l'heure exacte d'entrée et de sortie, fournissant ainsi un historique détaillé de toutes les visites pour les audits de sécurité.

Résumé et amélioration continue

La stratégie de **sécurité physique** de l'UNICEF est conçue pour protéger ses données et infrastructures critiques contre les menaces internes et externes. Grâce à un contrôle d'accès, une surveillance et une surveillance environnementale rigoureux, l'organisation garantit que toutes ses installations sont sécurisées et conformes aux normes de sécurité mondiales. Des audits et des examens réguliers sont effectués pour améliorer continuellement les systèmes, et toutes les mesures de sécurité sont intégrées aux **Global Security Operations Centers (GSOC)** pour garantir une surveillance et une réponse aux incidents en temps réel.

** Calendrier de l'examen et des améliorations de la sécurité ** :

- **Mensuel** : Vérification des systèmes de surveillance, audits d'accès aux cartes à puce, examen du journal des visiteurs.
- **Testimaire** : mises à jour des autorisations d'accès, audit du système des visiteurs, ajustements du protocole de sécurité.
- **Annuellement** : examen complet des systèmes biométriques, des systèmes d'extinction d'incendie et des audits de sécurité environnementale fournis par les fournisseurs.

Voici une version étendue et plus détaillée de la section **Sécurité des fournisseurs et des tiers**, intégrant des processus opérationnels, des délais et des exemples concrets plus complets :

---

11. Sécurité des fournisseurs et des tiers

Compte tenu de la nature essentielle des services tiers pour soutenir les opérations de l'UNICEF, il est essentiel de garantir la sécurité et la conformité de ces partenaires externes. L'UNICEF adhère à des pratiques rigoureuses de gestion des risques liés aux fournisseurs et mène des évaluations de sécurité approfondies pour atténuer les risques associés aux fournisseurs tiers.

11.1 Gestion des risques liés aux fournisseurs

Avant l’intégration d’un fournisseur ou d’un service tiers, l’UNICEF s’assure que la posture de sécurité du fournisseur respecte ou dépasse les normes de l’industrie et est conforme aux réglementations en vigueur. Cela comprend un examen complet du traitement des données, des protocoles de sécurité et de la conformité légale du fournisseur.

Évaluation de la sécurité et intégration :

- **Évaluations de sécurité** :
    - **Objectif** : S'assurer que les fournisseurs s'alignent sur les politiques de protection des données de l'UNICEF, les mesures de sécurité des réseaux et les exigences réglementaires internationales.
    - **Processus** : tous les fournisseurs potentiels sont soumis à une **évaluation de sécurité** initiale avant d'être intégrés. Cette évaluation couvre une série de facteurs, notamment :
        - **Politiques de protection des données** : le fournisseur dispose-t-il de mesures appropriées pour le cryptage des données, le stockage sécurisé et la transmission sécurisée des informations sensibles ?
        - **Conformité aux normes réglementaires** : le fournisseur se conforme-t-il aux lois internationales telles que les normes **RGPD**, **HIPAA** et **ISO 27001** ?
        - **Protocoles de sécurité réseau** : le fournisseur met-il en œuvre des pare-feu, des systèmes de détection d'intrusion (IDS) et une protection des points de terminaison efficaces pour sécuriser ses systèmes ?
    - **Délai** : le processus d'évaluation de la sécurité est généralement terminé **dans les 30 jours** suivant le début d'une relation avec un fournisseur. Après l'intégration, l'UNICEF effectue des **examens semestriels** pour garantir le respect continu des protocoles de sécurité.

        - **Exemple** : lors de la sélection d'un **fournisseur de stockage cloud**, l'UNICEF demande au fournisseur de soumettre un rapport détaillé sur ses **normes de cryptage des données**, y compris son utilisation du **chiffrement de bout en bout*. * et authentification multifacteur pour accéder aux fichiers sensibles. Ce rapport est examiné par l'équipe de sécurité de l'UNICEF et des auditeurs externes, garantissant sa conformité avec la norme de conformité **ISO 27001**.

- **Protection des données et conformité** :

    - **Objectif** : S'assurer que tous les fournisseurs traitent les données personnelles et sensibles conformément aux lois mondiales sur la protection des données.

    - **Processus** : tous les fournisseurs sont tenus de signer un **Accord de traitement des données (DPA)** qui décrit les attentes en matière de traitement, de stockage et de protection des données, en particulier pour les **informations personnellement identifiables (PII)**. De plus, les fournisseurs doivent fournir des **évaluations annuelles de conformité** ou des rapports démontrant le respect des réglementations en matière de protection des données telles que le **RGPD**, **HIPAA** et **CCPA**.

    - **Calendrier** : le **DPA** est examiné et signé pendant la phase de négociation du contrat, avec des **révisions annuelles** prévues pour coïncider avec la période de renouvellement du contrat. Les fournisseurs sont tenus de soumettre des **rapports trimestriels de conformité en matière de sécurité**, garantissant ainsi leur conformité continue aux exigences réglementaires.

        - **Exemple** : le **fournisseur de services cloud tiers** de l'UNICEF doit se soumettre à un **audit trimestriel de protection des données**, axé sur le cryptage des données, les politiques de conservation des données et les contrôles d'accès des utilisateurs. Le fournisseur doit soumettre un rapport de conformité mis à jour chaque trimestre pour confirmer le respect du **RGPD** et des lois sur la protection des données. Le non-respect des exigences d’audit peut entraîner une révision ou une résiliation du contrat.

11.2 Audits de sécurité tiers

Des audits de sécurité annuels sont essentiels pour vérifier le respect par le fournisseur des politiques de sécurité strictes de l’UNICEF. Ces audits, menés par des organismes tiers indépendants, évaluent les contrôles internes des fournisseurs, les mesures de protection des données et la conformité aux normes de l’industrie.

Processus d'audit de sécurité :

- **Audits de sécurité annuels** :

    - **Objectif** : procéder à un examen complet de la posture de sécurité du fournisseur, en se concentrant sur des domaines tels que la gestion des risques, le cryptage des données, le contrôle d'accès, la réponse aux incidents et la gestion des vulnérabilités.

    - **Processus** : l'UNICEF emploie des auditeurs tiers réputés tels que **KPMG**, **PwC** et **Deloitte** pour effectuer des **audits de sécurité annuels**. Ces audits évaluent l’adhésion du fournisseur aux meilleures pratiques en matière de cybersécurité et de protection des données, notamment :

        - **Analyse des vulnérabilités** : identification des faiblesses potentielles de l'infrastructure réseau et des configurations système du fournisseur.
        - **Vérification de la conformité** : garantir que le fournisseur respecte les normes réglementaires mondiales (par exemple, **ISO 27001**, **GDPR**, **NIST**).
        - **Préparation à la réponse aux incidents** : évaluation de la capacité du fournisseur à détecter, répondre et récupérer des incidents de sécurité, tels que des violations de données ou des compromissions du système.

    - **Calendrier** : ces audits sont effectués **annuellement**, et les conclusions sont rapportées dans les **30 jours** suivant la fin de l'audit. Si une vulnérabilité importante ou un problème de non-conformité est identifié, des audits de suivi sont programmés plus tôt.

        - **Exemple** : Un **audit annuel** d'un **fournisseur de services informatiques gérés** peut découvrir plusieurs systèmes logiciels obsolètes présentant des vulnérabilités connues. L'équipe d'audit fournira un **plan d'actions correctives de 30 jours** au fournisseur afin de résoudre ces problèmes et de mettre à jour ses systèmes.

- **Suivi des conclusions de l'audit** :

    - **Objectif** : S'assurer que toutes les vulnérabilités ou défauts de conformité identifiés lors d'un audit sont traités rapidement par le fournisseur afin d'atténuer les risques de sécurité potentiels.

    - **Processus** : après chaque audit, l'UNICEF planifie une **réunion de suivi** avec le fournisseur pour discuter des résultats et convenir d'un **plan d'action corrective (CAP)**. Ce plan décrit les étapes de remédiation spécifiques, les délais d'exécution et les responsabilités assignées aux deux parties.

    - **Chronologie** : les actions correctives pour les **vulnérabilités critiques** (par exemple, failles de sécurité non corrigées ou accès non autorisé) doivent être mises en œuvre **dans un délai de 30 jours**. Pour les **constatations non critiques**, telles que des améliorations procédurales mineures, le fournisseur dispose de **90 jours** pour mettre en œuvre les modifications nécessaires. L'UNICEF suit les progrès de ces actions à travers des réunions et des mises à jour régulières.

        - **Exemple** : suite à un audit d'un **fournisseur de stockage cloud** externe, il a été découvert que ses contrôles d'accès à certains référentiels de données n'étaient pas suffisamment sécurisés. L'UNICEF a publié un **plan d'actions correctives de 30 jours**, exigeant que le fournisseur améliore son cryptage et mette en œuvre des mesures d'authentification des utilisateurs plus robustes. Le fournisseur a réussi à mettre à jour ses protocoles dans les délais impartis.

11.3 Exclusion de fournisseurs et élimination des données

Lorsqu'une relation avec un fournisseur prend fin, l'UNICEF veille à ce que tout accès au fournisseur soit révoqué et que les données sensibles soient restituées ou détruites en toute sécurité.

Mesures de sécurité :

- **Résiliation de l'accès** : à la fin du contrat du fournisseur, tous les identifiants d'accès et tous les comptes sont immédiatement désactivés, et tous les appareils ou systèmes fournis au fournisseur sont renvoyés ou effacés en toute sécurité.
- **Destruction des données** : toutes les données stockées par le fournisseur sont soit renvoyées à l'UNICEF, soit détruites en toute sécurité, conformément aux meilleures pratiques de l'industrie en matière de **désinfection des données**.
- **Délai** : la destruction des données a lieu dans les **30 jours** suivant la résiliation du contrat, avec un certificat signé du fournisseur confirmant l'achèvement du processus.
    - **Exemple** : Lorsque l'UNICEF met fin à un contrat avec un **fournisseur d'analyse de données**, le fournisseur est tenu de soumettre un **Certificat de destruction de données** dans un délai de **30 jours**, confirmant que toutes les données de l'UNICEF stockées dans leurs systèmes a été supprimé et effacé en toute sécurité de tous les appareils.

Résumé et surveillance continue

Les pratiques de **sécurité des fournisseurs et des tiers** de l'UNICEF garantissent que les fournisseurs respectent des normes rigoureuses en matière de protection des données, de conformité et de gestion des risques. En effectuant des **évaluations de sécurité**, des **audits** et une **surveillance continue**, l'UNICEF maintient une chaîne d'approvisionnement sécurisée et garantit que les données sensibles sont protégées à toutes les étapes de la relation avec le fournisseur.

Calendrier pour la gestion de la sécurité des fournisseurs :

- **Évaluation initiale** : effectuée dans les **30 jours** suivant l'engagement du fournisseur.
- **Revue semestrielle des fournisseurs** : effectuée tous les **6 mois**.
- **Audits de sécurité annuels** : effectués une fois par an, avec des actions de suivi réalisées dans un délai de **30 à 90 jours** selon la gravité des constatations.
- **Désengagement et élimination des données** : finalisé dans les **30 jours** suivant la résiliation du contrat.

---

12. Audits et surveillance de sécurité

12.1 Surveillance continue

La surveillance continue est un élément essentiel de la stratégie de cybersécurité de l’UNICEF. Cela implique le suivi en temps réel des systèmes, du trafic réseau et des points finaux pour détecter les menaces et répondre rapidement aux incidents de sécurité. Les outils de surveillance font partie intégrante de la garantie que les vulnérabilités ou attaques potentielles sont identifiées rapidement, permettant ainsi une atténuation rapide.

Outils de surveillance :

- **Splunk** :

    - **Objectif** : Splunk sert de plate-forme de **gestion centralisée des journaux** et d'**analyse en temps réel** pour surveiller tous les systèmes et réseaux critiques. L'outil regroupe des données provenant de plusieurs sources, notamment des serveurs, des périphériques réseau, des plates-formes cloud, des pare-feu et des points de terminaison, pour fournir des informations détaillées sur l'état de sécurité global.

    - **Processus** : les données sont collectées, normalisées et analysées pour générer des **alertes en temps réel** pour les anomalies qui pourraient signifier des menaces potentielles, telles que des tentatives d'accès non autorisées, une activité utilisateur suspecte ou des erreurs de configuration. Cela permet au **Security Operations Center (SOC)** d'identifier et de répondre rapidement aux incidents de sécurité.

    - **Chronologie** : une surveillance continue est active **24h/24 et 7j/7**, avec des évaluations mensuelles des processus d'agrégation et d'alerte pour garantir l'absence de lacunes dans la collecte de données. L'équipe SOC examine les journaux de sécurité en temps réel, avec des **audits mensuels** effectués pour garantir l'exactitude et l'exhaustivité des données. Des mises à jour régulières des règles de surveillance et des flux de renseignements sur les menaces sont effectuées **trimestriellement** pour s'adapter aux menaces émergentes.

        - **Actions clés** :
        - **Génération d'alertes en temps réel** lorsqu'une activité réseau inhabituelle ou des connexions non autorisées sont détectées.
        - **Analyse détaillée** et enquête sur tous les incidents signalés par Splunk, permettant une identification rapide des violations potentielles.

- **CrowdStrike Faucon** :

    - **Objectif** : CrowdStrike fournit une **protection des points finaux** grâce à la surveillance en temps réel de tous les appareils, en détectant les logiciels malveillants, les ransomwares et les comportements anormaux indiquant une cyberattaque.

    - **Processus** : l'outil surveille en permanence les points finaux (serveurs, ordinateurs portables, appareils mobiles, etc.) pour détecter des activités inhabituelles telles que des modifications de fichiers, un accès non autorisé à des données sensibles ou l'exécution de logiciels malveillants connus. Dès la détection d'une menace, CrowdStrike isole le point de terminaison concerné, empêchant ainsi la propagation de la menace et envoyant une alerte à l'équipe SOC.

    - **Chronologie** : la surveillance s'exécute **24h/24 et 7j/7**, avec des **mises à jour hebdomadaires** et des correctifs pour garantir que les points de terminaison sont protégés contre les dernières menaces. L'équipe SOC reçoit des alertes en temps réel, avec des examens quotidiens de l'état des points finaux dans toute l'organisation.

        - **Actions clés** :
        - **Isolement des logiciels malveillants ou des ransomwares** : lorsqu'une activité malveillante est détectée, CrowdStrike isole le point de terminaison pour empêcher toute propagation ultérieure.
        - **Alertes d'incident en temps réel** envoyées au SOC, permettant une réponse immédiate pour éviter les dommages.

- **Outils d'analyse du trafic réseau (par exemple, Darktrace)** :

- **Objectif** : Darktrace utilise l'**intelligence artificielle (IA)** et l'apprentissage automatique pour détecter les **comportements réseau anormaux** qui peuvent indiquer une menace de cybersécurité, notamment l'exfiltration de données, les mouvements latéraux non autorisés ou les modèles d'accès anormaux.

- **Processus** : Darktrace utilise l'IA pour établir une base de référence du comportement normal du trafic réseau. Une fois les modèles de base établis, il détecte automatiquement les écarts pouvant suggérer une attaque en cours. Le système envoie des alertes au SOC lorsque des modèles suspects sont identifiés, tels qu'un accès non autorisé à des données sensibles, un trafic sortant inhabituel ou des tentatives de contournement des contrôles de sécurité du réseau.

- **Chronologie** : une surveillance continue et en temps réel est effectuée, avec des **évaluations trimestrielles** des capacités de détection des menaces et des politiques d'analyse du trafic réseau. Des mises à jour régulières des modèles d'IA sont effectuées pour suivre les techniques d'attaque émergentes.

    - **Actions clés** :
    - **Détection d'anomalies basée sur l'IA** pour identifier les menaces internes potentielles ou les comptes compromis.
    - **Alertes en temps réel** et notifications lorsqu'un trafic anormal ou des activités suspectes sont détectés.

12.2 Audits externes

Les audits externes jouent un rôle essentiel pour garantir que l'infrastructure de sécurité de l'UNICEF est conforme aux réglementations en vigueur et aux normes mondiales. Ces audits permettent de garantir que l'organisation maintient des normes de sécurité élevées et s'aligne sur les meilleures pratiques en matière de gestion des risques, de protection des données et de contrôles du système.

Processus d'audit :

- **Audits de conformité ISO 27001 et RGPD** :

    - **Objectif** : Évaluer l'efficacité du système de gestion de la sécurité de l'information (ISMS) de l'UNICEF conformément à la norme **ISO 27001** et vérifier le respect des lois mondiales sur la protection des données, telles que le **Règlement général sur la protection des données (RGPD) **.

    - **Processus** : l'UNICEF engage des auditeurs tiers indépendants pour mener des examens complets de son cadre de sécurité et de ses pratiques de protection des données. Les auditeurs évaluent différents aspects, notamment :

        - **Processus de gestion des risques** : évaluer la manière dont les risques sont identifiés, évalués et atténués dans l'ensemble de l'organisation.
        - **Mesures de protection des données** : examen du cryptage des données, des contrôles d'accès et des mécanismes de conformité au RGPD.
        - **Procédures de réponse aux incidents** : tester l'état de préparation et l'efficacité de la réponse aux violations de données ou aux incidents de sécurité.

        - **Contrôles d'accès** : garantir que seules les personnes autorisées peuvent accéder aux données et aux systèmes sensibles.

    - **Calendrier** : des **audits annuels** sont effectués, généralement à partir du **1er trimestre**, avec des rapports livrés dans les **30 à 45 jours** suivant la fin de l'audit. Les résultats sont utilisés pour éclairer les actions correctives et les améliorations des processus. Tous les problèmes immédiats sont traités et résolus dans un délai de **30 jours**.

        - **Actions clés** :
        - **Audit ISO 27001** : Évaluation des politiques et contrôles globaux du SMSI pour garantir qu'ils répondent aux normes internationales.
        - **Contrôle de conformité RGPD** : Examiner les pratiques pour garantir que les données personnelles sont traitées et protégées conformément à la réglementation.
        - **Actions correctives de suivi** : mise en œuvre rapide de toute action corrective identifiée lors de l'audit.

- **Suivi des conclusions de l'audit** :

    - **Objectif** : Garantir que les vulnérabilités identifiées ou les problèmes de conformité sont résolus rapidement et efficacement.

    - **Processus** : Après chaque audit, une réunion de suivi est organisée entre l'équipe de sécurité de l'UNICEF, les auditeurs externes et les parties prenantes concernées. Un plan d'actions correctives (CAP) est créé pour répondre aux constatations. L'UNICEF travaille en étroite collaboration avec des auditeurs externes et des équipes internes pour résoudre les problèmes rapidement et efficacement.

    - **Délai** : les actions correctives sont généralement effectuées dans un délai de **30 jours** pour les problèmes hautement prioritaires (par exemple, vulnérabilités de sécurité ou non-conformité aux réglementations critiques). Les problèmes moins critiques sont résolus dans un délai de **60 à 90 jours**.

        - **Actions clés** :
        - **Correction immédiate** des vulnérabilités hautement prioritaires.
        - **Documentation des actions correctives** prises et vérification que les problèmes ont été résolus.
        - **Suivi des progrès** à travers des réunions de suivi et des audits internes.

- **Audits de surveillance ISO 27001** :

    - **Objectif** : Garantir que le SMSI de l'UNICEF reste conforme aux normes ISO 27001 et que les mesures de sécurité sont continuellement améliorées.
    - **Processus** : des audits de surveillance ISO 27001 ont lieu chaque année et évaluent la capacité de l'organisation à maintenir et à améliorer son SMSI. L'audit comprend un examen de l'efficacité des stratégies de gestion des risques, des pratiques de traitement de l'information, des procédures de réponse aux incidents et de la sensibilisation des employés aux protocoles de sécurité.
    - **Calendrier** : ces audits sont effectués **annuellement** et l'organisation est tenue d'apporter des améliorations en fonction des conclusions de l'audit. Le processus commence généralement au

T2 avec un audit de suivi réalisé à la fin de l'année pour vérifier la mise en œuvre des actions correctives.

12.3 Réponse aux incidents et intégration des audits

L'intégration des audits de sécurité aux protocoles de réponse aux incidents est cruciale pour garantir que les problèmes de sécurité sont résolus efficacement et que l'organisation tire les leçons des incidents passés pour améliorer ses défenses.

Intégration de la gestion des incidents :

- **Objectif** : Garantir que les résultats des audits et les outils de surveillance continue soutiennent des actions de réponse aux incidents rapides et efficaces.
- **Processus** : lorsqu'un incident de sécurité est détecté, l'équipe SOC collabore avec les équipes informatiques, juridiques et de conformité pour évaluer la portée de l'incident. Les résultats d'audit et les données des outils de surveillance tels que Splunk, CrowdStrike et Darktrace sont examinés pour comprendre comment la violation s'est produite, quels systèmes ont été affectés et comment la réponse pourrait être améliorée à l'avenir.
- **Chronologie** : la réponse aux incidents commence immédiatement après la détection d'une menace, avec un confinement et une analyse initiaux effectués dans un délai de **minutes à heures** selon la gravité de l'incident. Des examens post-incident ont lieu **dans les 7 jours** pour évaluer l'efficacité de la réponse et intégrer les enseignements tirés dans les futures stratégies de sécurité.
    - **Actions clés** :
    - **Examen post-incident** pour identifier les lacunes dans les contrôles de sécurité.
    - **Collaboration avec des auditeurs externes** pour évaluer l'impact de l'incident et garantir que toutes les conclusions de l'audit sont intégrées dans le plan de réponse.
    - **Amélioration des plans de réponse aux incidents** sur la base des retours d'audit.

Résumé et calendrier des audits et de la surveillance de sécurité :

- La **surveillance continue** avec des outils tels que Splunk, CrowdStrike et Darktrace est opérationnelle **24h/24 et 7j/7** avec des alertes en temps réel et des mises à jour hebdomadaires pour maintenir une protection optimale du système.
- Les **audits annuels** (ISO 27001, RGPD, etc.) sont réalisés par des auditeurs tiers, généralement réalisés dans les **30 à 45 jours** suivant la fin de l'audit, suivis de mesures correctives immédiates si nécessaire.
- Les **examens post-incident** sont intégrés aux outils de surveillance et aux commentaires d'audit, et des actions correctives sont lancées **dans les 30 jours** pour les problèmes critiques et dans les **90 jours** pour les constatations moins graves.

---

13. Cycle de contrôle et d’examen des documents

Pour garantir l'efficacité et la pertinence continues des politiques, procédures et contrôles de sécurité, l'UNICEF utilise un **cycle formel de contrôle et d'examen des documents**. Ce cycle garantit que toute la

documentation relative à la sécurité est continuellement évaluée, mise à jour et maintenue en conformité avec l'évolution des menaces, des exigences réglementaires et des changements organisationnels.

13.1 Révision de la politique

Le processus d'examen des politiques est essentiel pour garantir que les politiques de sécurité de l'UNICEF restent à jour avec les risques actuels, les normes juridiques et les meilleures pratiques.

- **Objectif** : évaluer et mettre à jour régulièrement les politiques et pratiques de sécurité en réponse à l'évolution des menaces de sécurité, des progrès technologiques et des exigences réglementaires.
- **Chronologie** : les politiques de sécurité sont révisées **annuellement** pour garantir qu'elles restent efficaces et pertinentes. En cas de faille de sécurité ou de changement réglementaire important, une révision de la politique est immédiatement déclenchée, avec des mises à jour effectuées dans un délai de **30 jours**.

Processus de révision :

1. **Révision annuelle** :
    - Chaque année, toutes les politiques et directives de sécurité sont révisées de manière approfondie. Cela garantit que toutes les procédures reflètent les dernières meilleures pratiques et sont conformes aux normes de l'industrie et aux exigences légales.
    - Tous les changements internes, tels que les mises à niveau du système, les modifications de politique ou les changements opérationnels, sont pris en compte lors de l'examen.
2. **Examen post-incident** :
    - Si un incident de sécurité se produit, un examen immédiat des politiques pertinentes est effectué pour déterminer leur efficacité à atténuer la menace. Suite à l'examen, les mises à jour nécessaires sont effectuées pour éviter de futurs événements. Ces mises à jour doivent être mises en œuvre dans un délai de **30 jours**.
3. **Avis ponctuels** :
    - En réponse à de nouveaux risques émergents, à des changements réglementaires ou à des avancées technologiques, les politiques peuvent être revues en dehors du cycle de révision prévu. Ces examens sont lancés rapidement et les mises à jour sont effectuées dans les **30 jours** suivant l'identification.

13.2 Contrôle des documents

Le contrôle des documents garantit que les politiques de sécurité, les procédures et les documents associés sont correctement conservés, mis à jour et stockés de manière sécurisée et accessible.

- **Objectif** : Garantir que toute la documentation de sécurité est contrôlée par version, stockée en toute sécurité et accessible uniquement au personnel autorisé.
- **Processus**:
    1. **Dépôt centralisé** : tous les documents liés à la sécurité sont stockés dans un référentiel centralisé et sécurisé. L'accès à ce référentiel est strictement contrôlé et seul le personnel

autorisé peut modifier ou approuver les documents.
2. **Contrôle de version** : un mécanisme de contrôle de version strict est utilisé pour garantir que les versions historiques des documents sont préservées tandis que seule la dernière version est activement utilisée. Toute modification apportée aux documents est suivie avec un historique détaillé des versions, y compris les dates de modification et les raisons des modifications.
3. **Processus d'approbation** : Avant qu'un document ne soit finalisé ou mis à jour, il doit passer par un processus d'approbation formel. Ce processus garantit que les parties prenantes concernées, y compris les équipes de sécurité, juridiques et de conformité, examinent et approuvent les modifications avant leur adoption.

- **Chronologie**:
  - **Audits mensuels de documents** : tous les documents de sécurité sont audités sur une base mensuelle pour garantir qu'ils sont à jour, pertinents et alignés sur les dernières réglementations.
  - **Cycle d'examen trimestriel** : en plus des audits mensuels, un examen plus complet de tous les documents de sécurité a lieu chaque trimestre. Ce processus garantit que la documentation est complète et conforme à la stratégie de sécurité actuelle.

13.3 Communication documentaire et formation

Une communication et une formation efficaces garantissent que tous les employés et parties prenantes concernées comprennent et respectent les politiques de sécurité mises à jour.

- **Objectif** : Garantir que les mises à jour des politiques de sécurité sont efficacement communiquées à toutes les parties concernées et que les membres du personnel sont formés pour mettre en œuvre des mesures de sécurité nouvelles ou révisées.

- **Processus**:
  1. **Communication des changements de politique** : tous les changements de politique sont communiqués aux employés et aux parties prenantes via des canaux de communication internes, tels que le courrier électronique, les publications intranet ou les bulletins de sécurité. Cela garantit que chacun est informé des mises à jour et comprend ses responsabilités.
  2. **Formation sur les politiques mises à jour** : Les employés doivent suivre des sessions de formation sur toute politique nouvelle ou mise à jour. Cela garantit que tous les membres du personnel disposent des connaissances et des compétences nécessaires pour adhérer aux mesures de sécurité mises à jour.
  3. **Suivi de la conformité** : La conformité aux exigences de formation est suivie via un système de certification. Les enregistrements de formation terminée sont stockés et examinés lors des audits pour garantir que tout le personnel concerné est à jour sur les protocoles de sécurité.

- **Chronologie**:
  - **Formation semestrielle** : Une formation sur les politiques de sécurité est dispensée au moins deux fois par an. Des sessions de formation supplémentaires sont programmées si nécessaire suite à des changements de politique importants ou à des incidents de sécurité.

13.4 Audit et examen de la conformité

Pour garantir que le processus de contrôle des documents est correctement suivi, des audits et des examens de conformité réguliers sont effectués.

- **Objectif** : Vérifier que toutes les politiques et documents de sécurité sont examinés, mis à jour et suivis conformément aux procédures internes et aux exigences réglementaires externes.
- **Processus**:
    1. **Audits internes** : Des audits internes sont menés régulièrement pour évaluer le respect des procédures de contrôle des documents. Ces audits évaluent si les politiques sont examinées et mises à jour conformément aux délais établis et si tous les changements nécessaires sont mis en œuvre.
    2. **Audits de conformité** : des audits de conformité annuels sont effectués pour vérifier que le processus de contrôle des documents est conforme aux exigences réglementaires telles que **ISO 27001**, **RGPD** et d'autres normes pertinentes. Ces audits évaluent également l'efficacité de la documentation de sécurité par rapport aux objectifs de sécurité globaux de l'organisation.
- **Chronologie**:
    - **Audits internes** : menés trimestriellement pour garantir l'efficacité du cycle de contrôle et d'examen des documents.
    - **Audits de conformité** : menés chaque année pour évaluer la conformité aux normes de l'industrie et aux exigences réglementaires.

13.5 Éléments clés du cycle de contrôle et d'examen des documents

- **Révisions régulières** : les politiques de sécurité sont révisées chaque année et mises à jour si nécessaire. Des examens immédiats ont lieu suite à des incidents ou à des changements réglementaires majeurs.
- **Contrôle de version** : les documents sont maintenus avec un contrôle de version strict pour garantir la traçabilité des modifications.
- **Approbation et formation** : les politiques de sécurité sont soumises à un processus d'approbation formel et sont suivies d'une formation pour toutes les parties prenantes concernées.
- **Audits de conformité** : les audits internes et externes garantissent le respect du processus de contrôle des documents et la conformité globale aux normes de sécurité.

---

14. Amélioration continue

L’amélioration continue est un élément essentiel de la stratégie de cybersécurité de l’UNICEF. Ce processus garantit que les mesures de sécurité évoluent constamment en réponse aux menaces émergentes, aux nouveaux développements technologiques et aux leçons tirées des incidents de sécurité précédents. L'UNICEF vise à maintenir une posture de sécurité proactive et adaptative pour protéger son infrastructure, ses données et ses opérations.

14.1 Cadre d'amélioration continue

Le cadre d'amélioration continue suit une approche structurée en plusieurs étapes pour améliorer les pratiques de sécurité au fil du temps. Ce processus est conçu pour combler les failles de sécurité actuelles, intégrer les nouvelles technologies et garantir la conformité aux dernières normes et réglementations.

Composants clés :

- **Adaptation** : réponse aux nouveaux risques de sécurité, aux tactiques des acteurs menaçants et aux changements réglementaires.
- **Efficacité** : rationaliser les processus et éliminer les inefficacités dans la détection, la prévention et la réponse aux menaces.
- **Innovation** : adopter des technologies et des méthodologies avancées pour garder une longueur d'avance sur l'évolution des cybermenaces.
- **Résilience** : Renforcement de la capacité de l'organisation à prévenir, détecter et récupérer des incidents de sécurité.

14.2 Boucles de rétroaction de sécurité

Les boucles de rétroaction sur la sécurité sont essentielles au processus d'amélioration continue. Ces boucles capturent des informations provenant de diverses sources, telles que les évaluations internes, les examens des incidents, les commentaires des employés et les informations sur les menaces du secteur. Ils font partie intégrante du perfectionnement des politiques, procédures et outils de sécurité.

Sources de commentaires :

- **Examen des incidents** : suite à tout incident de sécurité important, une analyse post-mortem est effectuée pour identifier les causes profondes et les domaines à améliorer dans les pratiques de sécurité. Ces résultats éclairent directement les révisions des politiques de sécurité.
    - **Chronologie** : les examens post-incident ont lieu dans les **48 heures** suivant un événement et des plans d'action d'amélioration sont créés dans les **30 jours**.
- **Commentaires des employés** : des enquêtes régulières et des discussions internes sont utilisées pour recueillir les commentaires du personnel sur l'efficacité des programmes de formation à la sécurité, des outils et de la sensibilisation globale à la sécurité.
    - **Chronologie** : les commentaires sont collectés deux fois par an, avec des mesures immédiates prises pour les problèmes urgents identifiés dans les enquêtes.
- **Informations sur les menaces** : l'UNICEF exploite les informations sur les menaces partagées par des partenaires externes, des organismes gouvernementaux et des groupes industriels pour obtenir des informations sur les menaces émergentes et les tactiques utilisées par les cybercriminels. Ces informations sont utilisées pour ajuster les mesures de sécurité internes en conséquence.
    - **Chronologie** : les renseignements sur les menaces sont surveillés en permanence et intégrés dans le cadre de sécurité de l'organisation.

14.3 Évaluations et audits de sécurité

Des évaluations et des audits de sécurité réguliers sont essentiels pour identifier les vulnérabilités, mesurer l'efficacité des mesures de sécurité actuelles et garantir la conformité aux réglementations du secteur. Ces évaluations aident à identifier les lacunes dans les contrôles de sécurité et fournissent une base pour prioriser les améliorations.

Types d'évaluations de sécurité :

- **Analyse des vulnérabilités et tests de pénétration** : des analyses de vulnérabilité et des tests de pénétration réguliers sont effectués pour simuler des attaques et identifier les faiblesses du système.
    - **Chronologie** : des évaluations de vulnérabilité sont effectuées **trimestriellement**, avec une résolution immédiate des problèmes critiques identifiés. Les tests d'intrusion sont effectués **annuellement** ou après des changements importants dans le système.
- **Audits de conformité** : Pour garantir la conformité aux normes réglementaires telles que le RGPD, la norme ISO 27001 et d'autres cadres pertinents, l'UNICEF se soumet régulièrement à des audits internes et externes.
    - **Calendrier** : des audits de conformité sont effectués **chaque année**, avec une surveillance continue pour une conformité continue tout au long de l'année.
- **Audits tiers** : des sociétés de sécurité externes sont embauchées pour auditer les pratiques de sécurité des fournisseurs et sous-traitants tiers, garantissant ainsi qu'elles respectent les normes de sécurité et de confidentialité de l'UNICEF.
    - **Calendrier** : des audits tiers sont effectués chaque année, avec des évaluations de suivi requises si des failles de sécurité sont identifiées.

14.4 Adoption et intégration de la technologie

L’adoption de nouvelles technologies est une stratégie clé pour améliorer la posture de sécurité de l’UNICEF. L'évaluation continue des outils et techniques émergents garantit que l'organisation garde une longueur d'avance sur les nouvelles menaces et reste conforme aux réglementations en évolution.

Domaines d'intervention clés :

- **Automation et orchestration** : l'automatisation des workflows de détection des menaces, de réponse aux incidents et de sécurité permet de réduire les erreurs humaines, d'augmenter l'efficacité opérationnelle et d'accélérer les temps de réponse.
    - **Chronologie** : les technologies d'automatisation sont évaluées pour leur intégration **tous les six mois**. De nouveaux outils d'automatisation sont mis en œuvre en fonction de l'efficacité et des besoins organisationnels.
- **Intelligence artificielle (IA) et apprentissage automatique (ML)** : l'IA et le ML sont intégrés dans les systèmes de détection des menaces pour améliorer la précision et la rapidité d'identification des menaces potentielles. Ces technologies aident à identifier des modèles qui seraient difficiles à repérer pour les analystes humains.
    - **Chronologie** : les outils d'IA et de ML sont examinés pour l'intégration **trimestriellement**, avec une formation continue de ces systèmes pour améliorer les capacités de détection.
- **Outils de sécurité de nouvelle génération** : l'UNICEF examine régulièrement son utilisation des pare-feu de nouvelle génération, de la protection des points finaux et des outils de surveillance du réseau. L’objectif est de garantir que les outils les plus récents, intégrant des informations avancées sur les menaces et des analyses comportementales, sont utilisés pour sécuriser l’organisation.

    - **Chronologie** : un examen des outils et systèmes de sécurité a lieu **semestriellement**, et des mises à jour sont programmées en fonction de l'évolution du paysage des menaces et des avancées technologiques.

14.5 Formation et sensibilisation des employés

La sensibilisation des employés est un élément essentiel de la stratégie d'amélioration continue de l'UNICEF. L'élément humain étant souvent le maillon le plus faible de la cybersécurité, des programmes de formation continue et de sensibilisation sont conçus pour garantir que les employés sont prêts à reconnaître les menaces potentielles et à y répondre.

Programmes de formation :

- **Formation continue sur la sécurité** : Tous les employés suivent une formation de sensibilisation à la sécurité qui est régulièrement mise à jour pour refléter les dernières menaces et les meilleures pratiques. Cela comprend une formation sur le phishing, la gestion des mots de passe, la gestion sécurisée des données et le reporting des incidents.
    - **Chronologie** : La formation à la sécurité est dispensée **trimestriellement**, avec des cours de remise à niveau obligatoires pour les employés n'ayant pas suivi la formation au cours des six derniers mois.
- **Simulations de phishing** : des attaques de phishing simulées sont menées régulièrement pour tester la sensibilisation et la préparation des employés à l'identification des tentatives de phishing. Les résultats de ces simulations guident d'autres améliorations de la formation.
    - **Chronologie** : des simulations de phishing sont effectuées **semestriellement**, avec une formation de suivi ciblée dispensée aux employés qui échouent aux tests.
- **Programme des champions de la sécurité** : Certains employés sont désignés comme champions de la sécurité au sein de leurs équipes. Ces champions promeuvent les meilleures pratiques de sécurité, encouragent la sensibilisation et agissent comme agent de liaison entre leurs équipes et le service de sécurité.
    - **Chronologie** : les champions de la sécurité sont sélectionnés **chaque année**, avec des contrôles et des évaluations périodiques sur leur efficacité à promouvoir la sécurité au sein de leurs équipes.

14.6 Indicateurs clés de performance (KPI)

Pour mesurer l'efficacité des efforts d'amélioration continue, l'UNICEF utilise des indicateurs clés de performance (KPI). Ces KPI permettent de suivre les progrès, d'identifier les domaines à améliorer et d'évaluer l'impact des modifications apportées aux protocoles et outils de sécurité.

Les KPI clés incluent :

- **Délai de détection d'incident** : temps moyen nécessaire pour détecter un incident de sécurité à partir du point d'occurrence.
- **Temps de réponse** : temps nécessaire pour contenir et résoudre un incident de sécurité une fois détecté.

- **Taux de correction des vulnérabilités** : pourcentage de vulnérabilités identifiées qui sont corrigées dans les délais spécifiés.
- **Efficacité de la formation** : Mesurée par le taux d'achèvement des sessions de formation et le taux de réussite des simulations de phishing.
- **Statut de conformité** : le niveau de conformité aux politiques de sécurité internes, ainsi qu'aux réglementations externes (par exemple, RGPD, ISO 27001).

14.7 Rapports et documentation

Tous les efforts d'amélioration continue sont documentés pour maintenir la responsabilité et assurer la transparence envers les parties prenantes internes et externes. Des rapports réguliers sur l'avancement des initiatives d'amélioration, les conclusions des audits, les activités de formation et la gestion des vulnérabilités sont partagés avec la haute direction et, si nécessaire, avec les auditeurs externes.

Documentation :

- **Rapports trimestriels** : rapports détaillés sur l'état des initiatives d'amélioration de la sécurité en cours, y compris les évaluations, les audits et les mesures de réponse aux incidents.
    - **Chronologie** : Les rapports sont soumis **trimestriellement**, avec un examen annuel complet résumant les activités, les améliorations et les résultats de l'année.
- **Examen annuel de sécurité** : un examen complet de la posture de sécurité de l'organisation, y compris l'efficacité des politiques, des technologies et des programmes de formation, ainsi que la réponse de l'organisation aux nouvelles menaces et aux changements réglementaires.
    - **Calendrier** : L'examen annuel de la sécurité est terminé **à la fin de chaque exercice**, en mettant l'accent sur la définition des objectifs pour l'année suivante.

14.8 Gouvernance et surveillance

Le processus d'amélioration continue est supervisé par la haute direction de l'UNICEF, avec des mises à jour régulières fournies au conseil d'administration et aux parties prenantes concernées. Cela garantit que la sécurité reste une priorité à tous les niveaux de l'organisation et que des ressources sont allouées pour améliorer les contrôles de sécurité.

Gouvernance :

- **Comité directeur de la sécurité** : un comité interfonctionnel composé de la haute direction, de la sécurité informatique, des services juridiques, de la conformité et d'autres départements concernés se réunit régulièrement pour examiner les performances de sécurité et guider les efforts d'amélioration.
    - **Chronologie** : Le comité directeur de la sécurité se réunit **trimestriellement** pour examiner les progrès et ajuster la stratégie de sécurité de l'organisation si nécessaire.

---

15. Menaces émergentes et tendances futures en matière de sécurité

L'UNICEF s'engage à garder une longueur d'avance sur l'évolution des défis de sécurité pour protéger ses données, infrastructures et opérations sensibles. Cette approche prospective implique de se préparer aux

menaces émergentes et d'adopter des technologies de pointe qui peuvent contribuer à atténuer les risques et à améliorer la résilience globale de la cybersécurité.

15.1 Ransomware et protection des données

Les ransomwares restent l'une des cybermenaces les plus importantes pour les organisations du monde entier, y compris celles des secteurs humanitaires et de développement international comme l'UNICEF. À mesure que les cybercriminels développent des souches de ransomwares plus sophistiquées, il est essentiel de renforcer les défenses et les capacités de réponse.

Stratégies d'atténuation des ransomwares :

- **Stratégies de sauvegarde** : l'UNICEF améliore continuellement ses stratégies de sauvegarde pour garantir que les données critiques sont stockées en toute sécurité et peuvent être rapidement restaurées en cas d'attaque de ransomware. Des **tests de sauvegarde** réguliers sont effectués pour vérifier les procédures de récupération et garantir l'intégrité des données.
    - **Chronologie** : les systèmes de sauvegarde sont testés tous les trimestres et des exercices de restauration complets sont effectués **chaque année** pour valider les processus de récupération des données.
- **Protection des points finaux** : à l'aide d'**outils avancés de protection des points finaux**, tels que **CrowdStrike Falcon**, l'UNICEF s'efforce d'empêcher les ransomwares d'atteindre les points finaux grâce à l'analyse du comportement, à la détection des anomalies et à une réponse en temps réel.
    - **Chronologie** : les outils de protection des points finaux sont continuellement mis à jour avec les dernières informations sur les menaces pour garder une longueur d'avance sur l'évolution des tactiques de ransomware. Des mises à jour mensuelles sont effectuées pour les bases de signatures et les règles de détection.
- **Plans de réponse aux incidents** : pour minimiser l'impact des attaques de ransomwares, le **plan de réponse aux incidents (IR)** de l'UNICEF intègre des procédures détaillées pour le confinement, la communication et la récupération. Le plan est testé et mis à jour régulièrement.
    - **Chronologie** : Le plan IR est révisé et mis à jour **annuellement**. Des simulations de réponse spécifiques aux ransomwares et des exercices sur table sont effectués deux fois par an.
- **Formation des employés** : le phishing reste l'un des principaux vecteurs d'infection par ransomware. C'est pourquoi une sensibilisation continue à la sécurité et des simulations de phishing sont menées pour garantir que les employés sont prêts à identifier les e-mails suspects.
    - **Chronologie** : une formation de sensibilisation au phishing est dispensée tous les trimestres et des attaques de phishing simulées sont exécutées **semestriellement** pour évaluer l'état de préparation des employés.

15.2 Intelligence artificielle et apprentissage automatique en sécurité

L'intelligence artificielle (IA) et l'apprentissage automatique (ML) jouent un rôle de plus en plus important dans la cybersécurité en améliorant la détection et la réponse aux menaces de sécurité. Ces technologies peuvent

aider l'UNICEF à identifier les menaces émergentes, à prédire les vulnérabilités potentielles et à automatiser les réponses aux incidents.

Intégration IA et ML :

- **Détection et analyse des menaces** : l'UNICEF investit dans les technologies d'IA/ML pour améliorer la détection des menaces persistantes avancées (APT), des menaces internes et des vulnérabilités Zero Day. En analysant de grands volumes de données, les systèmes d'IA peuvent identifier des modèles et des anomalies qui pourraient passer inaperçus par les systèmes traditionnels.
    - **Chronologie** : les outils d'IA/ML sont continuellement évalués et affinés pour s'adapter aux nouvelles menaces. Une évaluation complète des outils de détection des menaces basés sur l'IA est menée **chaque année**.
- **Analyse comportementale** : des algorithmes d'apprentissage automatique sont utilisés pour surveiller le comportement des utilisateurs et des appareils sur le réseau, créant ainsi des profils de base. Tout écart par rapport à la ligne de base peut déclencher des alertes, permettant une identification plus rapide des menaces potentielles.
    - **Chronologie** : les outils d'analyse comportementale sont mis à jour et calibrés **trimestriellement** pour améliorer la précision de la détection et minimiser les faux positifs.
- **Réponse automatisée aux incidents** : l'IA/ML est également utilisée pour automatiser certains aspects du processus de réponse aux incidents, tels que le blocage du trafic malveillant, l'isolation des systèmes compromis et l'application de correctifs de sécurité. Cela réduit le temps de réponse et permet de contenir les menaces plus efficacement.
    - **Chronologie** : les processus de réponse automatisés sont évalués tous les six mois, avec des mises à jour mises en œuvre si nécessaire en fonction des nouvelles informations sur les menaces.

15.3 Architecture Zero Trust (ZTA)

Alors que les organisations continuent de faire face à des risques de sécurité en constante évolution, le modèle de sécurité traditionnel basé sur le périmètre devient de plus en plus inefficace. L'UNICEF passe à une **Architecture Zero Trust (ZTA)**, qui suppose qu'aucun utilisateur ou appareil, qu'il soit à l'intérieur ou à l'extérieur du réseau, ne peut faire confiance par défaut.

Mise en œuvre Zero Trust :

- **Gestion des identités et des accès (IAM)** : le fondement de ZTA est le principe du moindre privilège, ce qui signifie que les utilisateurs n'ont accès qu'aux ressources spécifiques dont ils ont besoin pour effectuer leurs tâches. L'**authentification multifacteur (MFA)** et des **contrôles d'accès** stricts sont appliqués à tous les utilisateurs, appareils et applications.
    - **Chronologie** : la mise en œuvre de ZTA est en cours. La MFA est requise pour tous les systèmes critiques, avec des audits périodiques des contrôles d'accès effectués tous les 6 mois pour garantir la conformité au modèle Zero Trust.

- **Micro-segmentation** : Pour éviter les mouvements latéraux en cas de violation, l'UNICEF met en œuvre la **micro-segmentation** sur l'ensemble de son réseau. Cela implique de segmenter le réseau en parties plus petites et isolées, de sorte que même si un segment est compromis, l'attaquant ne peut pas se déplacer librement sur l'ensemble du réseau.
    - **Chronologie** : la segmentation du réseau et le déploiement de ZTA sont progressifs, avec des progrès significatifs attendus d'ici la fin de **2025**. Les étapes clés incluent l'achèvement de la mise en œuvre de la micro-segmentation dans les zones critiques du réseau dans un délai de **12 mois**.
- **Authentification et surveillance continues** : dans un environnement Zero Trust, l'authentification est continue et tout le trafic est surveillé pour détecter tout comportement inhabituel. Cela inclut l'évaluation de la fiabilité des appareils et des utilisateurs à chaque étape de l'interaction, quel que soit leur emplacement.
    - **Chronologie** : les mécanismes d'authentification continue sont déployés progressivement, avec un déploiement initial prévu au **T2 2025**. Une surveillance continue et des ajustements sont effectués à mesure que le système évolue.

15.4 Sécurité du cloud et transition vers le cloud d'abord

À mesure que de plus en plus de services et d'applications migrent vers le cloud, la sécurisation des environnements cloud devient une priorité croissante. La stratégie de l'UNICEF comprend l'adoption d'une **approche cloud first**, tout en garantissant que les services cloud répondent à des normes de sécurité rigoureuses et aux réglementations pertinentes en matière de protection des données.

Mesures de sécurité du cloud :

- **Cloud Access Security Brokers (CASB)** : l'UNICEF utilise des **CASB** pour surveiller et contrôler les mouvements de données sur diverses plates-formes cloud, garantissant ainsi que l'accès aux données est correctement régi et que les politiques de sécurité sont appliquées de manière cohérente.
    - **Chronologie** : les solutions CASB sont déployées sur toutes les principales plates-formes cloud d'ici **mi-2025**, avec une surveillance et un ajustement continus en fonction de l'évolution des besoins de sécurité.
- **Cryptage dans le cloud** : toutes les données sensibles stockées dans le cloud sont cryptées à la fois en transit et au repos. Les clés de cryptage sont gérées via un système sécurisé pour empêcher tout accès non autorisé.
    - **Chronologie** : les stratégies de chiffrement dans le cloud sont révisées **chaque année** pour garantir qu'elles s'alignent sur l'évolution des normes de chiffrement et des exigences de conformité.
- **Gestion des risques liés aux fournisseurs** : alors que l'UNICEF continue de collaborer avec des fournisseurs de services cloud tiers, les pratiques de gestion des risques liés aux fournisseurs garantissent que ces fournisseurs respectent les normes de sécurité, les réglementations sur la protection des données et les politiques internes.

- **Chronologie** : des audits de sécurité des fournisseurs sont effectués **chaque année**, avec des évaluations supplémentaires déclenchées après toute mise à jour majeure du contrat ou modification du service cloud.

15.5 Partage et collaboration de renseignements sur les menaces

Face à des menaces en évolution rapide, la cybersécurité devient de plus en plus collaborative. L'UNICEF participe activement aux initiatives de partage d'informations et collabore avec d'autres organisations, leaders de l'industrie et entités gouvernementales pour échanger des renseignements sur les menaces.

Efforts de collaboration :

- **Partenariats public-privé** : l'UNICEF collabore avec des agences gouvernementales, des organisations non gouvernementales (ONG) et des entreprises de cybersécurité du secteur privé pour rester informé des nouvelles menaces et partager les meilleures pratiques.
  - **Chronologie** : les partenariats sont examinés et actualisés **chaque année**, avec des échanges réguliers de renseignements sur les menaces au fur et à mesure que de nouvelles informations deviennent disponibles.
- **Groupes et forums industriels** : l'UNICEF est un membre actif de divers forums et groupes industriels sur la cybersécurité, où des renseignements sur les menaces sont partagés et où des mesures de défense communes sont discutées.
  - **Chronologie** : La participation aux groupes industriels se fait de manière continue, avec des mises à jour trimestrielles sur les renseignements sur les menaces et les nouvelles techniques de cyberdéfense.

15.6 Intelligence artificielle et systèmes de sécurité autonomes

Dans le cadre de sa stratégie prospective, l'UNICEF étudie l'utilisation de **systèmes de sécurité autonomes** alimentés par l'IA pour surveiller, détecter et répondre de manière proactive aux cybermenaces sans intervention humaine directe. Ces systèmes utiliseront des algorithmes d'apprentissage automatique pour analyser de grandes quantités de données réseau et prendre des décisions de sécurité en temps réel.

Plans de mise en œuvre :

- **Détection des menaces basée sur l'IA** : des modèles avancés d'apprentissage automatique seront développés pour détecter de nouveaux types inconnus de cybermenaces en analysant les modèles de trafic réseau, les comportements des utilisateurs et les anomalies du système.
  - **Chronologie** : la phase pilote de détection des menaces basée sur l'IA devrait commencer en **fin 2025**, avec un déploiement complet prévu pour **2027**.
- **Systèmes de réponse autonomes** : à mesure que les technologies d'IA évoluent, l'UNICEF prévoit d'intégrer des capacités de réponse de sécurité autonomes, où le système peut prendre des mesures (par exemple, bloquer le trafic malveillant, isoler les points finaux infectés) sans nécessiter d'intervention manuelle.

    - **Calendrier** : le déploiement complet des systèmes de réponse autonomes est prévu pour **2027**, avec une mise en œuvre progressive à partir de **2026**.

15.7 Informatique quantique et cryptographie post-quantique

L’informatique quantique devrait révolutionner le domaine de la cybersécurité, avec à la fois le potentiel de briser les schémas de chiffrement actuels et la capacité de proposer des modèles de chiffrement plus puissants. L'UNICEF surveille activement les développements dans le domaine de la **cryptographie post-quantique (PQC)**, s'assurant qu'elle est prête à passer à des méthodes cryptographiques résistantes aux quantiques.

Stratégie PQC :

- **Surveillance des progrès quantiques** : l'UNICEF suit les développements dans le domaine de l'informatique quantique et de la cryptographie post-quantique pour anticiper la nécessité de passer à des protocoles de cryptage quantiques sécurisés.
    - **Chronologie** : Une stratégie formelle pour la transition vers la cryptographie post-quantique est en cours d'élaboration, avec des recherches et des préparatifs initiaux prévus pour **2026**.