



Politique de sécurité des opérations

Responsable de la politique : CEO

Date d'entrée en vigueur : 22 Février 2024

Visée

Assurer le fonctionnement correct et sécurisé des systèmes et installations de traitement de l'information.

Champ d'application

Tous les systèmes d'information de Evalandgo Software qui sont essentiels à ses activités et/ou qui utilisent, stockent ou transmettent des données d'entreprise. La présente politique s'applique à tous les employés de Evalandgo Software ainsi qu'aux autres entités tierces ayant accès aux réseaux et ressources système de Evalandgo Software.

Sécurité des opérations

Documentation des procédures opérationnelles

Les procédures opérationnelles techniques et administratives doivent être documentées le cas échéant et mises à la disposition de tous les utilisateurs qui en ont besoin.

Gestion des modifications

Avant le déploiement en production, il est nécessaire de tester, d'évaluer et d'approuver les modifications apportées à l'organisation, aux processus d'exploitation, aux installations de traitement de l'information, aux logiciels et infrastructures de production ainsi qu'aux systèmes qui ont une incidence sur la sécurité de l'information dans l'environnement de production et les systèmes financiers. Toute modification importante apportée aux systèmes et réseaux visés doit être documentée.

1. Documentation et examen des modifications :

- Toutes les modifications importantes apportées aux systèmes, aux réseaux et aux installations de traitement doivent être documentées.
- La documentation doit inclure l'objectif, les spécifications, l'impact potentiel du changement en tenant compte des dépendances, et le plan de déploiement.
- Les modifications doivent être testées et examinées dans des environnements distincts de la production et du développement (par exemple, des environnements de pré-production).

2. Approbation et autorisation :

- Les modifications ayant un impact substantiel sur la sécurité de l'information et les fonctionnalités opérationnelles, doivent obtenir une autorisation formelle avant le déploiement.
- Les modifications urgentes peuvent être accélérées mais doivent faire l'objet d'une autorisation et d'une vérification a posteriori.

3. Procédures de gestion des modifications :

- Planification et évaluation de l'impact : évaluez les impacts potentiels des modifications en tenant compte des dépendances du système.
- Autorisation : obtenez les approbations nécessaires avant d'initier les modifications. Informez à l'avance les parties prenantes internes et externes concernées des modifications prévues, des plannings et de l'impact attendu.
- Tests et contrôle qualité : Assurez-vous que les modifications sont testées de manière approfondie (reportez-vous à la section 8.29 concernant les détails relatifs aux tests et à la validation) et qu'elles répondent aux normes de qualité avant leur mise en œuvre.
- Mise en œuvre et déploiement : effectuez les modifications conformément au calendrier de déploiement prévu
- Gestion des urgences : Remédiation : si les modifications échouent ou génèrent des problèmes inattendus, elles doivent être annulées
- Tenue à jour de la documentation : Assurez-vous que les systèmes de tickets ou la plateforme de dépôt de codes enregistrent les modifications, les validations et les déploiements.

4. Continuité et cohérence :

- Veillez à ce que les plans de continuité des technologies informatiques et de communication (ICT), les procédures de réponse et de reprise soient mis à jour pour rester valides et cohérents en dépit des modifications.
- Veiller à ce que la documentation et les procédures en cours d'utilisation soient modifiées et conformes.

5. Sécurité et intégrité :

- Assurez-vous que les modifications préservent et ne compromettent pas la confidentialité, l'intégrité et la disponibilité des informations au niveau des installations et des systèmes de traitement.

Gestion des capacités

L'utilisation des ressources de traitement et de stockage du système doit être surveillée et ajustée pour garantir que la disponibilité et les performances du système répondent aux exigences de Evalandgo Software.

Les compétences, la disponibilité et les capacités des ressources humaines doivent être examinées et prises en compte dans le cadre de la planification des capacités et du processus annuel d'évaluation des risques.

L'ajustement des ressources en vue d'obtenir des capacités de traitement ou de stockage supplémentaires, sans apporter de modifications au système, peut être effectué en dehors du processus standard de gestion des modifications et de déploiement de code.

Prévention des fuites de données

Conformément à la présente politique de prévention des fuites de données, et afin de minimiser le risque de fuite d'informations sensibles, l'entreprise doit :

- Identifier et classer les informations conformément à la politique de gestion des données
- Proposer des formations de sensibilisation aux utilisateurs, notamment sur l'utilisation et le traitement appropriés des informations sensibles

Envisager l'utilisation d'outils de surveillance technique et de prévention des pertes de données (DLP) conformément aux risques pour l'entreprise et les personnes concernées.

Filtrage Web

L'organisation doit garantir une utilisation Internet sûre, sécurisée et appropriée par le personnel de l'organisation.

Accès et blocage du site Web :

- Mettre en œuvre des mécanismes, tels qu'un DNS sécurisé et le blocage d'adresses IP ou de domaines, afin de restreindre l'accès aux sites Web qui présentent un risque important en raison de leur contenu ou de la distribution connue de logiciels malveillants, de virus ou de matériel d'hameçonnage.
- Utiliser des navigateurs et des technologies anti-malware capables de bloquer automatiquement les sites Web ou de les configurer de la même manière.
- À l'exception des motifs commerciaux légitimes, envisagez de bloquer l'accès aux sites Web contenant :
 1. Des outils de téléchargement d'informations.
 2. Des contenus malveillants connus ou suspectés.
 3. Des serveurs de commande et de contrôle.
 4. Des contenus identifiés comme malveillants grâce aux renseignements sur les menaces.
 5. Un partage de contenu illégal.

Règles et directives d'utilisation :

- L'utilisateur doit se conformer à toutes les règles de l'entreprise conformément au Code de conduite et à la Politique d'utilisation acceptable figurant dans la Politique de sécurité de l'information.

Séparation des environnements de développement, de test et de production

Les environnements de développement et de test doivent être strictement séparés des environnements de production SaaS afin de réduire les risques d'accès non autorisé ou d'apport de modifications à l'environnement opérationnel. Les données de production confidentielles des clients ne doivent pas être utilisées dans des environnements de développement ou de test sans l'approbation expresse du VP Support client.

La politique de gestion des données contient une description des données confidentielles. Si l'utilisation de données de production des clients est approuvée au cours de la phase de développement ou de test, toute information sensible doit, si possible, être retirée.

Configuration, renforcement et révision des systèmes et des réseaux

Les systèmes et réseaux doivent être provisionnés et maintenus conformément aux normes de configuration et de renforcement décrites dans l'annexe A de la présente politique.

Des pare-feu et/ou des contrôles et configurations d'accès au réseau appropriés doivent être utilisés pour contrôler le trafic réseau vers et depuis l'environnement de production, conformément à la présente politique.

Les règles de configuration des accès au réseau en production doivent être passées en revue au moins une fois par an. Des tickets doivent être créés pour obtenir des approbations pour toute modification nécessaire.

Protection contre les logiciels malveillants

Afin de protéger l'infrastructure de l'entreprise contre l'introduction de logiciels malveillants, des dispositifs de contrôle de détection, de prévention et de restauration pour la protection contre les logiciels malveillants doivent être mis en œuvre, ainsi qu'une sensibilisation appropriée des utilisateurs.

Des protections anti-malware doivent être utilisées sur tous les terminaux fournis par l'entreprise, à l'exception de ceux opérant sur des systèmes d'exploitation qui ne sont normalement pas sujets à des attaques de logiciels malveillants. En outre, des logiciels de détection et de réponse aux menaces doivent être utilisés pour la messagerie électronique professionnelle. Les protections anti-malware utilisées doivent être capables de détecter toutes les formes courantes de menaces malveillantes et d'exécuter les activités d'atténuation appropriées (telles que la suppression, le blocage ou la mise en quarantaine).

Evalandgo Software doit analyser tous les fichiers lors de l'introduction de ceux-ci dans ses systèmes et analyser en permanence les fichiers lors des accès, modifications ou téléchargements. Les mises à jour de listes et de moteur anti-malware doivent être configurées pour être téléchargées et installées automatiquement chaque fois que de nouvelles mises à jour sont disponibles. Les incidents connus ou présumés en lien avec des logiciels malveillants doivent être signalés comme des incidents de sécurité.

Désactiver ou modifier la configuration des protections anti-malware sans autorisation constitue une violation de la politique de l'entreprise.

Sauvegarde des informations

Le besoin de sauvegarder les systèmes, bases de données, informations et données doit être étudié et les processus de sauvegarde appropriés doivent être conçus, planifiés et mis en œuvre. Les procédures de sauvegarde doivent inclure des procédures de maintien et de récupération des données clients, conformément aux accords de niveau de service documentés. Des mesures de sécurité visant à protéger les sauvegardes doivent être conçues et appliquées selon la confidentialité ou le degré de sensibilité des données. Des copies de sauvegarde des informations, des logiciels et des images système doivent être prises régulièrement dans un but de protection contre la perte de données. Les capacités de sauvegarde et de restauration doivent être testées régulièrement, au moins une fois par an.

Les sauvegardes doivent être stockées séparément dans une région différente de l'emplacement des données en production.

Evalandgo Software ne sauvegarde pas régulièrement les appareils des utilisateurs tels que les ordinateurs portables. Les utilisateurs doivent conserver leurs fichiers et informations essentiels dans des référentiels de stockage de fichiers autorisés par l'entreprise.

Les sauvegardes sont configurées pour être exécutées chaque jour sur les systèmes concernés. Les calendriers de sauvegarde sont conservés dans le logiciel de l'application de sauvegarde.

Un test de restauration de sauvegarde doit être effectué au moins une fois par an pour valider les données de sauvegarde et le processus de sauvegarde.

Journalisation et surveillance

L'infrastructure de production doit être configurée de manière à pouvoir produire des journaux détaillés appropriés à la fonction assurée par le système ou l'appareil concerné. Les journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être produits, conservés et examinés au moyen de processus manuels ou automatisés selon les besoins. Des alertes appropriées doivent être configurées pour les événements représentant une menace significative pour la confidentialité, la disponibilité ou l'intégrité des systèmes de production ou des données confidentielles.

La journalisation doit répondre aux critères suivants pour les applications en production et l'infrastructure de prise en charge :

- Enregistrer les connexions et déconnexions des utilisateurs
- Enregistrer les opérations CRUD (création, lecture, mise à jour et suppression) sur les utilisateurs et les objets de l'application et du système
- Enregistrer les modifications des paramètres de sécurité (y compris la désactivation ou la modification de la journalisation)
- Enregistrer les accès du propriétaire ou de l'administrateur de l'application aux données clients (p. ex. Access Transparency)
- Les journaux doivent inclure l'identifiant utilisateur, l'adresse IP, l'horodatage valide, le type d'action effectuée et l'objet de cette action.
- Les journaux doivent être stockés pendant au moins 30 jours et ne doivent pas contenir de données sensibles ou utiles

Protection des informations de journal

Les installations de journalisation et les informations de journal doivent être protégées contre les altérations et les accès non autorisés.

Journaux des administrateurs et des opérateurs

Les activités des administrateurs ou des opérateurs réseau doivent être enregistrées et examinées et/ou faire l'objet d'une alerte selon la classification et le caractère critique du système.

Journaux de restauration des données

Si l'entreprise doit restaurer les données en production contenant des données à caractère personnel issues de sauvegardes, soit à des fins de prestation de services, soit à des fins de test, l'opération doit être enregistrée ou suivie à l'aide de tickets vérifiables.

Synchronisation des horloges

Les horloges de tous les systèmes de traitement de l'information pertinents au sein d'une entreprise ou d'un domaine de sécurité doivent être synchronisées avec les serveurs de synchronisation réseau à l'aide de sources temporelles fiables.

Surveillance de l'intégrité des fichiers et détection des intrusions

Lorsque cela est possible, les systèmes de production de Evalandgo Software doivent être configurés pour surveiller, enregistrer et se réparer eux-mêmes et/ou alerter en cas de modifications

suspectes apportées à des fichiers système critiques.

Des alertes doivent être configurées pour détecter les situations suspectes et les ingénieurs doivent régulièrement examiner les journaux.

Les intrusions non autorisées et les tentatives d'accès ou les modifications apportées aux systèmes de Evalandgo Software doivent être étudiées et corrigées conformément au plan de réponse aux incidents.

Contrôle des logiciels opérationnels

L'installation de logiciels sur les systèmes de production doit respecter les exigences de gestion des modifications définies dans la présente politique.

Informations sur les menaces

Les informations relatives aux menaces à la sécurité de l'information doivent être collectées et analysées pour alimenter les renseignements sur les menaces.

Collecte : tirez parti de diverses sources, telles que des blogs, des articles de presse, des mises à jour de fournisseurs, des bases de données publiques et des communautés sectorielles.

Analyse : examinez les données pour obtenir des informations exploitables et favoriser des initiatives de réponse proactives. Signalez toute information exploitable ou toute menace spécifique à l'équipe de sécurité.

Diffusion : assurez une communication efficace des renseignements sur les menaces aux équipes concernées pour plus d'efficacité. L'équipe de sécurité diffusera des informations exploitables via des canaux de communication tels que Slack, les e-mails et les alertes d'urgence.

Commentaires : cultivez l'amélioration continue en tirant parti des commentaires pour améliorer les politiques. Intégrez les commentaires dans les modifications des politiques et effectuez des examens réguliers des politiques.

Gestion des vulnérabilités techniques

Les informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues en temps voulu, l'exposition de l'entreprise à ces vulnérabilités doit être évaluée et des mesures appropriées doivent être prises pour répondre aux risques associés. Différentes méthodes doivent être utilisées pour obtenir des informations sur les vulnérabilités techniques, notamment les analyses de vulnérabilité, les tests d'intrusion, l'étude des alertes de fournisseurs externes.

Des analyses de vulnérabilité doivent être effectuées sur des systèmes destinés au public dans l'environnement de production au moins une fois par trimestre.

Des tests d'intrusion doivent être effectués au moins une fois par an sur les applications et le réseau en production. Des analyses et tests supplémentaires doivent être conduits à la suite de modifications majeures apportées aux systèmes et logiciels en production.

Les services informatiques et d'ingénierie doivent évaluer la gravité des vulnérabilités identifiées à partir de toute source, et s'il est déterminé qu'il s'agit d'une vulnérabilité critique ou à haut risque, un ticket d'assistance sera créé. Le niveau de gravité évalué par Evalandgo Software peut différer du niveau généré automatiquement par le logiciel d'analyse ou déterminé par des chercheurs externes, en raison des connaissances internes de Evalandgo Software et de sa compréhension de l'architecture technique ainsi que de l'impact et l'exploitabilité réels. Les tickets sont affectés aux propriétaires du système, de l'application ou de la plateforme concernée pour un examen et/ou une correction plus approfondis.

Les vulnérabilités identifiées par Evalandgo Software doivent être corrigées ou résolues dans les délais suivants :

Gravité déterminée	Durée de correction
Critique	30 jours
Élevée	30 jours
Moyenne	60 jours
Faible	90 jours
Pour information	Selon les besoins

Pour toute vulnérabilité qui ne peut pas être corrigée dans le délai standard, les tickets d'assistance doivent inclure un plan de traitement des risques et un calendrier de remédiation planifiée.

Restrictions à l'installation de logiciels

Les règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre, conformément à la politique de sécurité de l'information de Evalandgo Software.

Considérations relatives à l'audit des systèmes d'information

Les exigences et les activités d'audit comprenant la vérification des systèmes opérationnels doivent être soigneusement planifiées et convenues afin de limiter les perturbations des processus opérationnels.

Évaluation et exigences en matière de sécurité des systèmes

Les risques doivent être pris en compte avant l'acquisition ou toute modification importante de systèmes, de technologies ou d'installations. Lorsque les exigences sont formellement identifiées, toutes les exigences de sécurité pertinentes doivent être satisfaites. L'acquisition de nouveaux fournisseurs et services doit se faire conformément à la politique de gestion des tiers.

L'entreprise doit effectuer une évaluation annuelle de la sécurité du réseau comprenant une évaluation des modifications importantes apportées à l'environnement, telles que les nouveautés relatives aux composants système et à la topologie du réseau.

Masquage des données

Directives techniques :

- Adopter des techniques appropriées telles que le masquage des données, la pseudonymisation ou l'anonymisation afin de protéger efficacement les informations personnelles et autres données sensibles.
- Garantir que les méthodes de pseudonymisation et d'anonymisation rompent efficacement le lien entre les données personnelles et les individus ou les éléments de données sensibles.
- Confirmer que tous les éléments d'information sont pris en compte pour une anonymisation adéquate des données.
- Utiliser des méthodes supplémentaires de masquage des données, telles que le chiffrement, l'annulation/la suppression de caractères, la modification des nombres et des dates, la substitution et le remplacement des valeurs par leur hachage.

Considérations relatives au masquage des données :

- Concevoir des requêtes et des masques de données pour ne divulguer que les données minimales requises aux utilisateurs, garantissant ainsi la confidentialité et la sécurité.

- Développer des mécanismes de dissimulation des données, en tenant compte des circonstances spécifiques dans lesquelles certaines données doivent être cachées aux utilisateurs.
- Fournir des options pour les principes relatifs aux informations personnelles afin de contrôler la visibilité de leurs données masquées et de respecter toutes les exigences juridiques ou réglementaires applicables en matière de masquage des données.

Utilisation du masquage des données, de la pseudonymisation ou de l'anonymisation :

- Déterminer le niveau de force, les contrôles d'accès, les contrats d'utilisation et les restrictions d'utilisation appropriés pour les données traitées.
- Empêcher le croisement de données traitées avec d'autres informations afin d'identifier les principales informations personnelles et de garantir la traçabilité des données traitées fournies et reçues.

Exceptions

Les demandes d'exception à cette politique doivent être soumises à l'approbation du responsable informatique et sécurité.

Violations et application

Toute violation connue de la présente politique doit être signalée au responsable informatique et sécurité. Toute violation de la présente politique peut entraîner le retrait ou la suspension immédiats des privilèges système et réseau, et/ou une sanction disciplinaire conformément aux procédures de l'entreprise, pouvant aller jusqu'au licenciement.

Version	Date	Description	Auteur	Approuvé par
1.0	22-Fev-2024	Première version	Hugo Bachelet	Valentin Boschattel

ANNEXE A - Normes de configuration et de renforcement

Veillez à inclure des liens vers des sources externes ou des échantillons créés en interne :

<https://aws.amazon.com/compliance/resources/>

Abordez la gestion et le déploiement de la configuration des lignes de base par contrôle 3.4, 7.1.

Serveurs et machines virtuelles

Il s'agit de la norme concernant le renforcement de la configuration des serveurs système et des serveurs virtuels (MV). Une certaine personnalisation de ces paramètres peut être nécessaire pour configurer le système en fonction de son environnement cible spécifique, comme la définition des noms propres, des groupes, des paramètres d'authentification et d'autres options de personnalisation.

Outre les exigences en matière de sécurisation des systèmes par rapport à la ligne de base présentée ci-dessus, tous les systèmes physiques et virtuels doivent respecter les exigences techniques suivantes :

- Tous les mots de passe par défaut des fournisseurs (y compris les mots de passe par défaut sur les systèmes d'exploitation, les logiciels fournissant des services de sécurité, les comptes d'applications et de systèmes, les chaînes de communauté SNMP, etc.) doivent être modifiées avant l'installation du système sur le réseau.
- Les comptes par défaut non nécessaires (y compris les comptes utilisés par les systèmes d'exploitation, les logiciels de sécurité, les applications, les systèmes, les SNMP, etc.) doivent être supprimés ou désactivés avant l'installation du système sur le réseau.
- Une seule fonction principale peut être mise en œuvre par serveur ou machine virtuelle pour empêcher les fonctions exigeant différents niveaux de sécurité de coexister sur le même système.
- Seuls les services, protocoles, démons, etc. nécessaires peuvent être activés, et uniquement dans la mesure où cela est nécessaire au fonctionnement du système. Toutes les fonctionnalités non nécessaires (comme les scripts, les pilotes, les fonctionnalités, les sous-systèmes, les systèmes de fichiers et les serveurs Web inutiles) doivent être désactivées.
- Tous les correctifs de sécurité identifiés comme critiques, élevés ou moyens doivent être appliqués aux systèmes dans le cadre des accords de niveau de service établis dans la présente politique.

Normes de réseau

- La gestion des règles et paramètres du réseau ne peut être effectuée que par des membres autorisés de l'équipe d'ingénierie ou par le prestataire externe dûment contracté pour la gestion de l'infrastructure Internet. Toute modification doit respecter les procédures de gestion des modifications définies dans la politique de sécurité des opérations.
- Les contrôles réseau pris en charge pour les réseaux en production sont les listes de contrôle d'accès réseau AWS (NACL), les groupes de sécurité, ainsi que les configurations réseau mises en place par le prestataire.
- Dans l'environnement de production, les règles et configurations définies doivent être appliquées pour contrôler le trafic provenant de réseaux non fiables (ex. services accessibles au public) vers les systèmes internes, en appliquant notamment des politiques de "moindre privilège" et de filtrage par ports/protocoles.
- Les systèmes de contrôle réseau doivent utiliser la traduction d'adresse réseau (NAT) afin d'éviter toute divulgation d'adresses internes sur Internet.
- Les appareils mobiles connectés aux réseaux de production doivent être en conformité avec les exigences de la Politique relative aux appareils mobiles incluse dans la Politique de sécurité de l'information.
- Tous les systèmes de contrôle réseau doivent être configurés avec des règles d'anti-spoofing par défaut pour bloquer ou refuser les adresses internes entrantes provenant d'Internet.
- Les configurations externes doivent limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles au public et autorisés.
- L'utilisation de services et protocoles non sécurisés sans justification ni documentation des fonctionnalités de sécurité supplémentaires mises en œuvre pour atténuer les risques est interdite.
- Les sessions d'accès à distance doivent être configurées pour appliquer un délai d'inactivité de **1 heure** (modifiable selon les besoins métiers).
- Les technologies d'accès à distance destinées aux fournisseurs et aux partenaires commerciaux pour accéder aux systèmes en production doivent être activées uniquement lorsque cela est nécessaire à des fins commerciales et désactivées immédiatement après utilisation.
- Tout réseau hybride disposant à la fois d'un accès cloud et sur site doit être analysé et testé au moins une fois par an afin de garantir le respect des exigences en matière de sécurité.

I. Renforcement du cloud

1. Gestion des identités et des accès (IAM)

- Principe du moindre privilège : assurez-vous que chaque entité (utilisateur, service, système) possède le minimum d'accès nécessaire.
- Application de l'authentification multifactorielle (MFA) pour l'accès à la production

2. Stockage et gestion des données

- Chiffrement des données : assurez le chiffrement des données au repos et en transit conformément à la *Politique de chiffrement*.
- Terminaux privés : activez les terminaux privés et les VPN pour vous protéger contre l'interception des données.
- Gestion du cycle de vie des données : configurez des sauvegardes pour les référentiels de données client.

3. Sécurité du réseau

- Isolation : utilisez les VPC et les sous-réseaux pour isoler les environnements et segmenter les réseaux.
- Pare-feu : mettez en œuvre des solutions de pare-feu cloud-natifs ou tiers, ainsi que des services de protection contre les attaques DDoS.

4. Surveillance et journalisation

- Journalisation : configurez la journalisation en mettant l'accent sur le stockage de type « write-once-read-many » afin d'éviter les altérations.
- Attention : mettez en œuvre un système d'alerte basé sur le cloud (Amazon CloudWatch, Azure Alerts) pour une réponse en temps réel aux incidents.

II. Renforcement des conteneurs

1. Sécurité des images

- Image source sécurisée : créez des images uniquement à partir d'images ou référentiels de base autorisés par Evalandgo Software
- Conception minimaliste : utilisez des images basiques pour réduire les vecteurs d'attaque.

2. Sécurité de l'exécution

Analyse d'exécution : mettez en œuvre des outils de sécurité d'exécution pour la détection des vulnérabilités et des menaces en direct.

3. Sécurité du réseau

Contrôles basés sur des politiques : mettez en œuvre des politiques réseau à l'aide d'outils tiers ou cloud-natifs.

4. Sécurité de l'orchestration

- Serveur d'API : protégez le serveur d'API avec des pare-feu, des contrôles IAM et des canaux de communication sécurisés appropriés.
- RBAC : établissez et examinez régulièrement les privilèges d'accès à l'orchestration, en garantissant la conformité au principe du moindre privilège.

5. Sécurité CI/CD

Accès aux pipelines : minimisez l'accès aux pipelines CI/CD en utilisant des contrôles d'accès basés sur les rôles et des pistes d'audit.

- Analyse des dépendances : recherchez des dépendances vulnérables lors des processus d'élaboration

III. Serveurs et machines virtuelles

Configuration de base

- Assurez-vous que les systèmes sont alignés sur les normes de référence de l'industrie (CIS Benchmarks, NIST Guidelines).

Conformité technique

- Valeurs par défaut du fournisseur : toutes les configurations par défaut, en particulier les mots de passe, doivent être modifiées avant l'intégration au réseau.
- Spécialisation des rôles : conservez une fonction principale unique par machine virtuelle afin de garantir la séparation des tâches et réduire les possibilités de mouvements latéraux.
- Gestion des correctifs : établissez une stratégie de gestion des correctifs pour respecter les accords de niveau de service (SLA) définis.

IV. Normes réseau

Gestion et documentation du réseau

- Gestion des modifications : toute modification des paramètres réseau doit respecter les processus de gestion des modifications.

Gestion du trafic dans les environnements de production

- Application des règles : appliquez strictement les règles prédéfinies. Celles-ci doivent être révisées et validées au moins une fois par an.
- Contrôle d'accès à distance : assurez un contrôle et un audit stricts de l'accès à distance, en limitant et en enregistrant toutes les connexions.

Listes de contrôle d'accès réseau (NACL) et contrôle du trafic

- Établissez des règles strictes régissant le trafic conformément à une justification commerciale définie