PRIVAL

Sécuriser la maintenance OT à distance pour les tiers :

Un Guide des Meilleures Pratiques

Table Des Matières

Introduction:

La convergence des systèmes de technologies de l'information (IT) et de technologies opérationnelles (OT) a apporté de nombreux avantages, mais elle a également amplifié les risques en matière de cybersécurité.

Les systèmes OT, qui contrôlent les infrastructures critiques et les processus industriels, dépendent de plus en plus des opérations de maintenance effectuées à distance, par des équipes internes et des prestataires tiers opérant sous accords de niveau de service (SLA).

Si l'accès à distance améliore l'efficacité et permet un support rapide, il introduit également des vulnérabilités significatives qui doivent être maîtrisées avec soin.

Cet article présente les meilleures pratiques pour sécuriser ces opérations, en s'appuyant sur des recherches récentes et des discussions au sein de l'industrie.

Comprendre
les risques

Les organisations qui dépendent des systèmes OT peuvent subir des conséquences dévastatrices en cas de cyberattaques, notamment des arrêts de production, des dommages aux équipements et des menaces pour la sécurité des personnes.

L'interconnexion des systèmes IT et OT augmente la surface d'attaque, et la montée du travail à distance a encore renforcé la nécessité de protocoles sécurisés pour l'accès à distance.

Les prestataires tiers sur les systèmes OT posent des risques uniques en raison de pratiques de sécurité incohérentes, d'outils IT inadaptés aux environnements OT et d'un manque de visibilité sur leurs activités.

Exemples concrets de ces risques :

- L'attaque sur le réseau électrique ukrainien en 2015, réalisée via un accès à distance compromis utilisé par les opérateurs.
- L'attaque par le ransomware NotPetya en 2017, exploitant des vulnérabilités dans les outils d'accès à distance d'une entreprise pour se propager rapidement.
- Une attaque par ransomware contre une grande entreprise de pipeline aux États-Unis en 2021, attribuée à une vulnérabilité dans son système d'accès à distance, soulignant l'importance de mesures de sécurité robustes.

Ces incidents démontrent que l'absence de contrôles de sécurité adéquats dans les accès à distance peut entraîner des conséquences sévères, soulignant l'importance de mettre en œuvre des mesures de sécurisation rigoureuses.

Sécuriser la maintenance OT à distance pour les tiers :

Pour atténuer les risques liés à la maintenance OT à distance par des tiers, les organisations devraient adopter une approche de sécurité multi-niveaux englobant des politiques, des technologies et une surveillance continue.

1. Mettre en œuvre un cadre Zero Trust

L'approche Zero Trust, basée sur le principe « ne jamais faire confiance, toujours vérifier », est idéale pour sécuriserl'accès OT à distance. Ce modèle considère chaque utilisateur et appareil comme une menace potentielle, nécessitant une authentification, autorisation et validation continues avant l'accès. Les éléments clés d'une architecture Zero Trust pour les systèmes OT incluent :

- Gestion des identités et des accès : Mise en place de mécanismes d'authentification forte comme l'authentification multi-facteurs (AMF) et vérification de l'identité de tous les utilisateurs, y compris les prestataires tiers. Les mécanismes de contrôle d'accès doivent appliquer le principe des moindres privilèges, en n'accordant aux prestataires que les permissions minimales nécessaires à leurs tâches spécifiques.
- Segmentation réseau : Division du réseau OT en segments plus petits et isolés pour limiter l'impact d'une éventuelle violation. Cela peut être réalisé à l'aide de VLAN, pare-feu et VPN. Les organisations doivent s'assurer que le réseau du prestataire est suffisamment segmenté par rapport à ceux d'autres clients.
- Surveillance continue et renseignement sur les menaces : Utilisation d'outils qui surveillent en temps réel les utilisateurs et appareils pour détecter anomalies et menaces. Le renseignement sur les menaces permet d'identifier les activités suspectes et de réagir rapidement.
- Technologies d'accès à distance sécurisées : Utilisation de protocoles sécurisés comme Virtual Desktop Infrastructure (VDI) ou des sessions restreintes via Remote Desktop Protocol (RDP) au lieu d'un accès direct au réseau. VDI permet aux prestataires d'utiliser leur propre matériel tout en maintenant le contrôle sur l'environnement d'accès et en empêchant l'accès direct de leurs appareils aux systèmes OT.

2. Établir des politiques de sécurité claires pour les prestataires tiers

Les organisations doivent définir des attentes et des exigences explicites concernant la sécurité de l'accès et de la maintenance à distance pour les prestataires tiers sous SLA. Cela inclut :

- Surveillance et audit des activités : Spécifier que les activités des prestataires seront surveillées et enregistrées. Les logiciels d'enregistrement de session sur les serveurs intermédiaires (jump boxes) sont particulièrement utiles.
- Plans de Réponse aux Incidents: S'assurer que les prestataires disposent de capacités robustes de réponse aux incidents conformes ou supérieures aux attentes de l'organisation.
- Mises à Jour de Sécurité et Gestion des Patches : Vérifier que les fournisseurs appliquent régulièrement des mises à jour de sécurité et des correctifs à leur infrastructure.
- Conformité et audits: Effectuer des audits réguliers pour assurer la conformité des fournisseurs aux normes et bonnes pratiques. Exiger une attestation de leur respect des contrôles de sécurité.
- Accords contractuels : Inclure des clauses strictes telles que des accords de confidentialité (NDA) qui précisent les responsabilités, exigences, périmètres et responsabilités des prestataires.
- Politiques de contrôle d'accès : Définir qui peut accéder à quels actifs et avec quels privilèges nécessaires. Les politiques doivent respecter le principe des moindres privilèges.
- Procédures d'authentification et d'autorisation : Utiliser des méthodes fortes telles que l'AMF, vérifier l'application du principe du moindre privilège par les prestataires, et envisager des comptes temporaires « just-in-time » automatisés.
- Canaux de communication sécurisés : Exiger des prestataires l'utilisation de canaux sécurisés comme les VPN, avec des règles de pare-feu strictes limitant l'accès à certains serveurs selon les groupes d'utilisateurs.

3. Mettre en place des contrôles d'accès robustes

L'application de contrôles d'accès stricts est essentielle pour limiter l'impact potentiel d'un compte tiers compromis.

Cela inclut :

- Principe du moindre privilège (PoLP) : Les organisations doivent appliquer le principe du moindre privilège, en veillant à ce que les fournisseurs tiers ne disposent que de l'accès minimum nécessaire pour accomplir leurs tâches assignées, et rien de plus.
- Contrôle d'accès basé sur les rôles (RBAC) : La mise en œuvre d'un contrôle d'accès basé sur les rôles permet de raffiner davantage les accès en attribuant des permissions en fonction des rôles et responsabilités spécifiques du personnel tiers.
- Contrôles d'accès basés sur le temps : Utilisez des contrôles d'accès basés sur le temps pour limiter les connexions uniquement lorsque cela est nécessaire et les révoquer automatiquement après une période prédéfinie.
- Accès réseau Zero Trust (ZTNA) : Dirigez les utilisateurs directement vers les applications spécifiques dont ils ont besoin, rendant le reste du réseau invisible et empêchant les mouvements latéraux.
- Authentification multi-facteurs (MFA) : Exigez plusieurs formes de vérification (par exemple, mot de passe, jeton de sécurité, biométrie) pour valider l'identité des utilisateurs.

C'EST QUOI LE ZTNA ?

Gartner définit le Zero-Trust Network Access (ZTNA) comme un accès adaptatif, basé sur les permissions minimales nécessaires, aux ressources d'une organisation.

Cet accès repose sur des politiques basées sur l'identité et le contexte pour les appareils utilisés par les employés et les tiers.

Le ZTNA réduit la surface d'attaque en dissimulant les infrastructures et les ressources, tout en utilisant des contrôles d'accès adaptatifs continus via un courtier de confiance pour accorder l'accès à une collection d'entités spécifiques, limitant ainsi les mouvements latéraux au sein du réseau.

3. Mettre en place des contrôles d'accès robustes (Suite)

- Gestion des accès privilégiés (PAM) et gestion des accès privilégiés des fournisseurs (VPAM) : Utilisez des solutions PAM ou VPAM pour appliquer un contrôle strict sur les comptes privilégiés utilisés par les tiers. Ces systèmes permettent l'isolation des sessions, la surveillance, l'enregistrement et la rotation automatisée des identifiants. Réduisez davantage les risques en travaillant vers des privilèges permanents nuls (ZSP) grâce à l'accès juste-à-temps (JIT) via des solutions PAM.

- Méthodes d'accès à distance sécurisées : Exigez l'utilisation de dispositifs approuvés par l'organisation ou d'une infrastructure de bureau virtuel (VDI) pour les sessions à distance. Mettez en place des serveurs intermédiaires (jump servers) avec des capacités de journalisation et de surveillance entre les tiers et les systèmes internes. Assurez-vous que toutes les solutions d'accès à distance respectent des normes de chiffrement robustes telles que TLS 1.2+ ou IPsec.

- Gestion des identifiants : Utilisez des systèmes de coffre-fort pour stocker les identifiants privilégiés dans un coffre-fort chiffré, empêchant les fournisseurs de voir les informations de connexion réelles.

- Contrôles d'accès granulaires : Mettez en œuvre des restrictions supplémentaires sur la manière dont les fournisseurs peuvent utiliser leurs droits d'accès, telles que des horaires d'accès (accès basé sur le temps), des notifications d'accès et des approbations d'accès.

C'EST QUOI UN PAM ?

Gartner définit la gestion des accès privilégiés (PAM) comme des outils offrant un niveau élevé d'accès technique grâce à la gestion et à la protection des comptes, des identifiants et des commandes, utilisés pour administrer ou configurer des systèmes et des applications.

Les outils PAM – disponibles sous forme de logiciels, SaaS ou appareils matériels – gèrent l'accès privilégié pour les personnes (administrateurs système et autres) ainsi que pour les machines (systèmes ou applications).

4. Assurer une surveillance et une visibilité continues

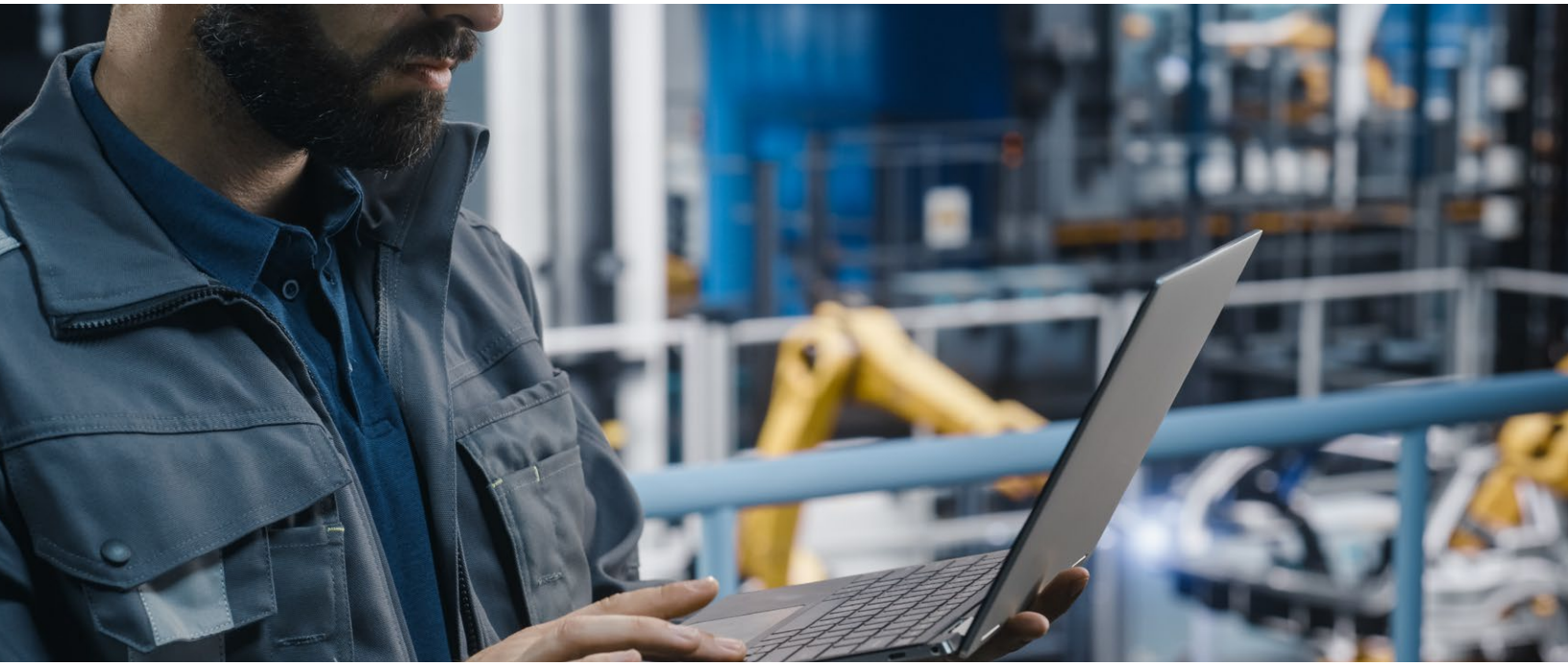
Une surveillance proactive des activités des prestataires est essentielle pour détecter et répondre aux comportements suspects.

Les organisations devraient :

- Journalisation et surveillance complètes : Enregistrez toutes les sessions d'accès à distance, y compris les détails des utilisateurs, les systèmes accédés, les commandes exécutées et la durée des sessions. Implémentez une surveillance en temps réel et des alertes pour toute activité suspecte.
- Enregistrer les sessions à distance lorsque possible pour l'audit et l'analyse. Examiner régulièrement les journaux pour détecter les anomalies et assurer la conformité.
- Passez régulièrement en revue les journaux pour détecter des anomalies et garantir la conformité.
- Corrélez les journaux et les alertes générées par divers outils de réseau et de sécurité pour obtenir une vue holistique des menaces potentielles

Audits et révisions régulières : Effectuez des évaluations de sécurité périodiques et des audits des politiques et pratiques d'accès des prestataires. Mettez régulièrement à jour les politiques d'accès des prestataires pour les adapter aux nouvelles menaces.

- Exploitez l'apprentissage automatique (Machine Learning) pour observer le comportement des utilisateurs et générer des alertes en cas d'activité anormale.



5. Sensibilisation et formation des utilisateurs

Éduquer les employés et les prestataires tiers sur les cybermenaces spécifiques aux systèmes OT et les meilleures pratiques en matière d'accès à distance sécurisé est crucial.

Les programmes de formation devraient inclure :

- Les principes de base de la cybersécurité.
- Les menaces spécifiques aux systèmes OT.
- Les bonnes pratiques pour un accès à distance sécurisé, notamment en ce qui concerne l'hygiène des mots de passe et la reconnaissance des tentatives de phishing.
- Les politiques d'utilisation acceptables, décrivant les activités permises et interdites.
- Les procédures de signalement des incidents.

6. Envisager des solutions dédiées pour l'accès à distance des tiers

Plusieurs solutions spécialisées sont conçues pour fournir un accès à distance sécurisé aux prestataires tiers.

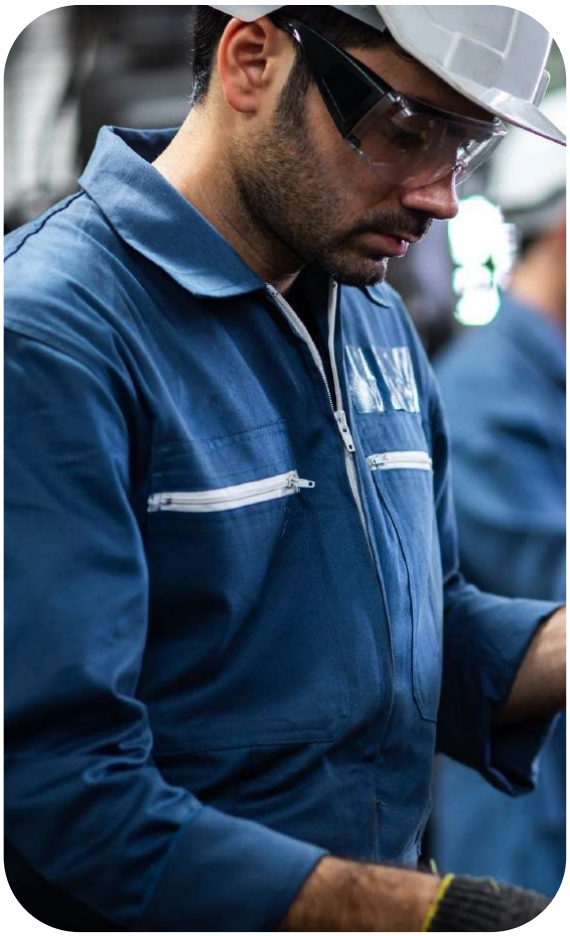
Ces plateformes offrent souvent des fonctionnalités telles que :

- Gestion de l'identité des prestataires.
- ZTNA et outils d'authentification robuste.
- Contrôles d'accès granulaires.
- Surveillance et enregistrement des sessions.
- Gestion et audit centralisés.

Des exemples de telles solutions incluent SecureLink, Bomgar, Osirium et des solutions VDI cloud comme Azure WVD. Certaines organisations exploitent également des plateformes RMM existantes avec des accès restreints et une authentification multi-facteurs (AMF).

7. Distinguer les Exigences de Sécurité Internes et Externes

Bien que les principes fondamentaux de la sécurité s'appliquent à la fois aux accès internes et externes, certains aspects nécessitent une attention particulière pour les prestataires externes :



- Contrôle : Les organisations ont plus de contrôle direct sur les processus internes en termes de contrôle d'accès, d'authentification, de segmentation du réseau, de surveillance et de gestion des correctifs. Pour les prestataires externes, elles doivent s'appuyer sur des accords contractuels et des audits pour garantir la conformité.
- Complexité : Les cadres d'accès pour les prestataires tiers peuvent être plus complexes en raison de la nécessité d'intégrer des identités externes et de gérer différents niveaux de sécurité.
- Vérification : Les organisations doivent activement vérifier que les prestataires appliquent une authentification forte, l'accès au moindre privilège, une segmentation réseau adéquate et qu'ils disposent de capacités robustes de surveillance de la sécurité et de réponse aux incidents.

8. Maintenir une posture de sécurité proactive

ÉLa sécurité ne se limite pas uniquement au contrôle d'accès et à la surveillance

- Gestion des correctifs et mises à jour de sécurité : Assurez-vous que les prestataires suivent des pratiques sécurisées de développement logiciel et de gestion des correctifs. Exigez des solutions antivirus et de protection des points finaux à jour sur les appareils des prestataires. Renforcez la nécessité d'évaluations périodiques des systèmes des prestataires qui accèdent à votre réseau.

- Réponse aux incidents et résiliation de l'accès : Définissez des procédures claires de réponse aux incidents pour les violations de sécurité impliquant les accès tiers. Mettez en œuvre des mécanismes automatisés pour révoquer l'accès des prestataires en cas d'anomalies détectées ou de résiliation de contrat. Exigez que les prestataires signalent tout incident de sécurité affectant leurs systèmes pouvant avoir un impact sur votre organisation. Exploitez PAM/VPAM pour révoquer rapidement l'accès aux comptes privilégiés pendant un incident. Assurez-vous que des procédures de départ définies sont en place pour mettre fin à l'accès lorsqu'il n'est plus nécessaire.

- Conformité et évaluation continue : Alignez les opérations de maintenance à distance sur les normes de l'industrie telles que NIST, ISO 27001 et les CIS Controls. Effectuez régulièrement des formations de sensibilisation à la sécurité pour les équipes internes qui gèrent les relations avec les prestataires tiers. Utilisez les fonctionnalités de conformité de PAM/VPAM pour appliquer les exigences réglementaires.

9. Exploiter l'automatisation

L'automatisation du provisionnement et du retrait des prestataires peut alléger le fardeau administratif et réduire le risque de comptes orphelins.

L'utilisation d'outils automatisés pour rationaliser les processus d'évaluation desprestataires et la surveillance continue peut également améliorer l'efficacité et la sécurité.

Envisagez de mettre en œuvre des solutions sans agent, sans VPN, et sans mot de passe pour réduire la charge administrative et les failles de sécurité associées aux méthodes traditionnelles de gestion des identités.

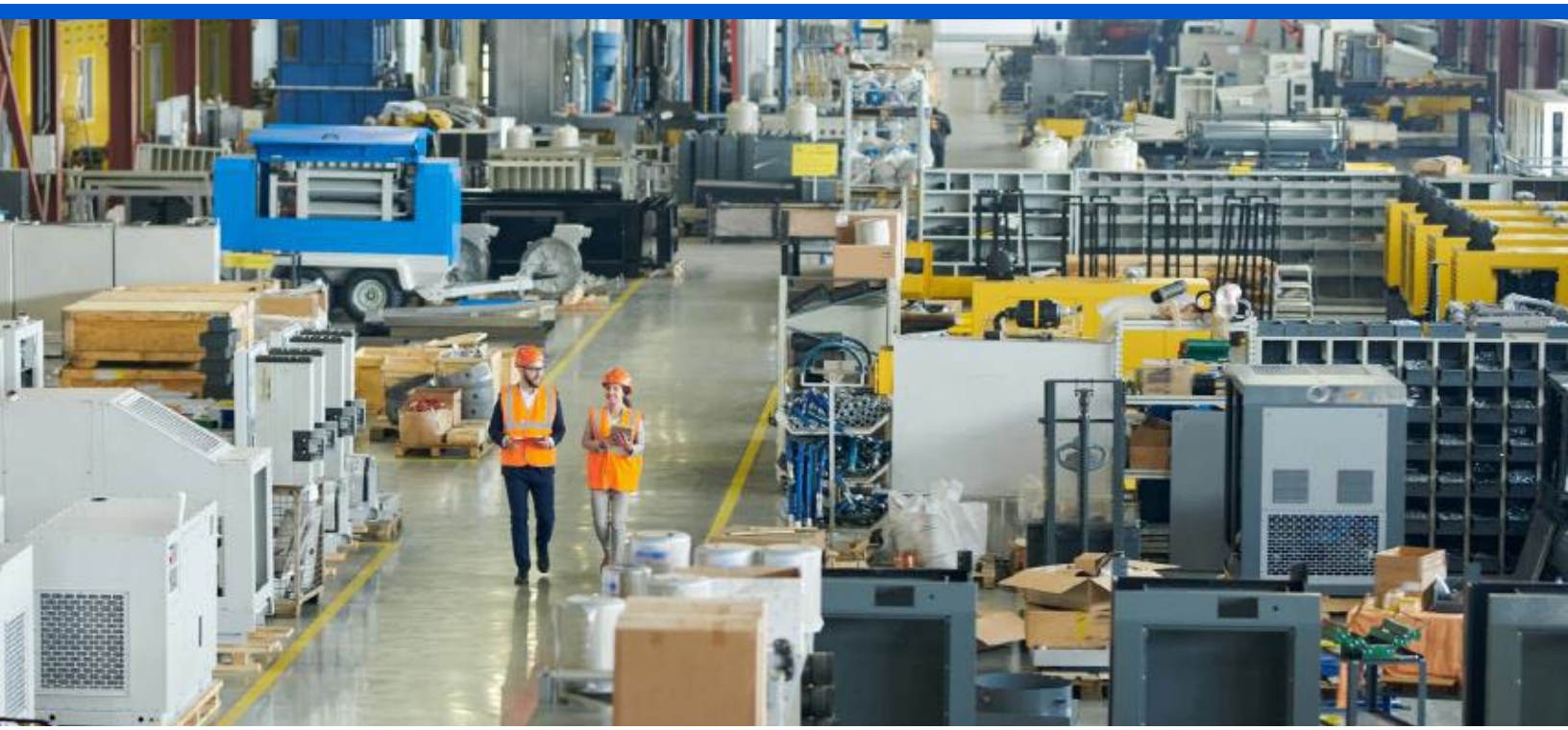
Conclusion

Sécuriser l'accès à distance des prestataires tiers pour la maintenance OT est essentiel pour protéger les infrastructures critiques et les opérations industrielles.

En mettant en œuvre ces meilleures pratiques de manière exhaustive et cohérente, les organisations peuvent considérablement minimiser les risques liés à l'accès non autorisé, aux violations de données et aux violations de conformité.

Une approche proactive et multi-facette est cruciale pour maintenir la sécurité et la résilience des environnements OT dans un monde de plus en plus interconnecté.

Les organisations devraient régulièrement évaluer leurs pratiques d'accès à distance et adapter leurs mesures de sécurité à l'évolution des menaces et aux besoins spécifiques de leurs systèmes OT.



Sources

Dans cette section, vous trouverez les sources qui ont servi de base à l'élaboration de ce rapport. Chez Prival, nous accordons une importance primordiale à fonder nos recommandations sur notre propre expérience ainsi que sur des sources fiables et crédibles.

Cette approche garantit que nos propositions sont pertinentes, solides et adaptées à votre réalité.

- Third-Party risk management Best Practices for 2024. (n.d.). https://www.venminder.com/blog/third-party-risk-management-best-practices-2024
- Zhurer, Y. (2024, November 29). 10 Data Security Best Practices for Enterprise Protection | SYTECA. Syteca. https://www.syteca.com/en/blog/data-security-best-practices
- Securing Remote Access: Best Practices for Third-Party Risk Management. (n.d.). Securing Remote Access: Best Practices for Third-Party Risk Management. https://www.cyberark.com/resources/blog/securing-remote-access-best-practices-for-third-party-risk-management
- Certa. (2024, July 22). 7 tips for managing third party Vendors. Certa. https://www.certa.ai/resources/7-tips-for-managing-third-party-vendors
- Ltd, N. (2024, October 17). Third-Party Risk Management - TPRM Framework & Risk Assessment. Neotas - Due Diligence and Employment Screening. https://www.neotas.com/third-party-risk-management-tprm/
- 11 Third-Party risk management Best Practices in 2025 | UpGuard. (n.d.). https://www.upguard.com/blog/11-tprm-best-practices-2024
- Third party access: considerations and security risks. (2024, September 25). Perception Point. https://perception-point.io/guides/endpoint-security/third-party-access-considerations-and-security-risks
- What is access Management? Risks, technology & best practices. (2025, March 7). Frontegg. https://frontegg.com/guides/access-management
- 9 TPRM Best Practices to Jumpstart your Third-Party Risk Management Program. (n.d.). Metricstream. https://www.metricstream.com/insights/best-practices-third-party-mgmt-program.
- Third-party vendor remote access best practices. (2024, May 14). Imprivata. https://www.imprivata.com/blog/best-practices-third-party-vendor-access
- Stechynskyi, I. (2024, October 28). Practical Guide to Third-Party Security Risk Management | SYTecA. Syteca. https://www.syteca.com/en/blog/third-party-providers
- What is access Management? Risks, technology & best practices. (2025b, March 7). Frontegg. https://frontegg.com/guides/access-management

Pour en apprendre plus sur nous : www.prival.ca

À Jour Avec Vos TI

PRIVAL