PcVue LET'S ENGINEER

Guide des bonnes pratiques PcVue pour sécuriser efficacement votre système

2024

LIVRE BLANC

SÉCURISER LA SUPERVISION DES SYSTÈMES INDUSTRIELS ET AUTOMATISÉS

A QUI S'ADRESSE CE DOCUMENT ?

Ce document présente les questions qu'il convient de se poser pour sécuriser la supervision d'une installation industrielle et automatisée, et décrit les bonnes pratiques à appliquer avec PcVue.

GLOSSAIRE

OT	Operation Technology
IT	Information Technology
ICS	Industrial Control System
SSI	Sécurité des Systèmes d'Information
SIIV	Systèmes d'Information d'Importance Vitale
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
LPM	Loi de Programmation Militaire
OIV	Organisme d'Importance Vital
SIV	Système d'Importance Vital
OSE	Opérateur de Services Essentiels
SAIV	Secteur d'Activité d'Importance Vitale
POC	Proof of Concept
SOC	Security Operation Center
SIEM	Security Information and Event Management
DSI	Directeur Système d'Information
RSSI	Responsable Sécurité des Systèmes d'Information
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information
CESTI	Centre d'Évaluation de la Sécurité des Technologies de l'Information
PSSI	Politique de Sécurité des Systèmes d'Information
RDS	Remote Desktop Services

LES BONNES QUESTIONS À SE POSER POUR ABORDER UNE DÉMARCHE DE SÉCURITÉ 4

POURQUOI MON SYSTÈME DOIT-IL ÊTRE SÉCURISÉ ? 6

QUELLES SONT LES OBLIGATIONS LÉGALES ? 12

LES BONNES PRATIQUES POUR SÉCURISÉ SIMPLEMENT ET EFFICACEMENT SON SYSTÈME 14

LES ENGAGEMENTS D'ARC INFORMATIQUE EN MATIÈRE DE CYBERSÉCURITÉ 42

1. LES BONNES QUESTIONS À SE POSER POUR ABORDER UNE DÉMARCHE DE SÉCURITÉ

1. LES BONNES QUESTIONS À SE POSER POUR ABORDER UNE DÉMARCHE DE SÉCURITÉ

POURQUOI MON SYSTÈME DOIT ÊTRE SÉCURISÉ ? EST-CE-QUE CELA EST OBLIGATOIRE ?

- Quels sont les risques inhérents au système ?
- Quelles sont les obligations légales ?

QUELS ÉLÉMENTS DE MON SYSTÈME DOIVENT ÊTRE SÉCURISÉS ?

- Quel est le périmètre fonctionnel et technique attendu ?
- Quelles exigences s'appliquent ?

J'AI BESOIN D'EXPERTISE

- Quelles offres d'accompagnement existent ?
- Par des prestataires d'audit qualifiés
- Par l'éditeur

QUELLES SONT LES FONCTIONS INDISPENSABLES ?

- Quelles sont les possibilités offertes par les logiciels déjà en place ?
- Dans le cas d'un projet existant ?

COMMENT GARANTIR QUE MON SYSTÈME EST SÉCURISÉ ?

- Les éléments du système sont-ils sécurisés ?
- Permettront-ils une homologation si nécessaire ?

2. POURQUOI MON SYSTÈME DOIT-IL ÊTRE SÉCURISÉ ?

2. POURQUOI MON SYSTÈME DOIT-IL ÊTRE SÉCURISÉ ?

- DES SYSTÈMES SENSIBLES, DES RISQUES RÉELS
- SPÉCIFICITÉ DES SYSTÈMES D'INFORMATION INDUSTRIELS
- MYTHES ET RÉALITÉS

Les solutions de supervision sont mises en œuvre dans des contextes de projets et d'exploitation sensible, que ce soit pour la conduite de procédés automatisés ou les systèmes mettant en jeu la sécurité des biens et des personnes.

La convergence IP facilite l'intégration d'équipements hétérogènes, l'interopérabilité et le déploiement de systèmes de supervision, mais apporte en contrepartie des risques en matière de sécurité si la méthodologie projet et les produits utilisés n'intègrent pas la composante "sécurité". En outre, l'évolution des architectures intégrant des objets connectés, la mobilité et globalement des systèmes de plus en plus ouverts et interconnectés induisent de nouvelles menaces qui rendent la cybersécurité indispensable.

Dans le guide sur la sécurité industrielle, l'ANSSI décrit en détail le contexte et les enjeux de la cybersécurité des systèmes industriels. Nous en reprenons dans cette partie, certains éléments essentiels pour bien comprendre la nécessité de protéger son système.

Guide_securite_industrielle_Version_finale.pdf

DES SYSTÈMES SENSIBLES, DES RISQUES RÉELS

Toutes les installations industrielles et automatisées ont des contraintes de qualité de service et de productivité qui les rend sensibles à toutes perturbations (attaque extérieure, négligence involontaire ou tout simplement une vulnérabilité du système) qui peuvent avoir des conséquences réelles.

12 SECTEURS D'ACTIVITÉS D'IMPORTANCE VITALE RÉPARTIS EN 4 DOMINANTES

DES INSTALLATIONS HÉTÉROGÈNES

Alimentation Gestion de l'eau Santé	Activités civiles de l'Etat Activités judiciaires Activités militaires de l'Etat	Energie Finances Transports	Communications électroniques, Audiovisuel, Information Industrie Espace et recherche

DES RISQUES IMPORTANTS

- Variété des attaques
- Négligence humaine
- Vulnérabilités des systèmes

DES IMPACTS RÉELS

- Sécurité des personnes et des biens
- Risque de santé publique
- Risque environnemental
- Accidents, intrusions
- Actions néfastes
- Obérer la capacité d'action de l'Etat
- Déni de service
- Risque économique
- Propriété intellectuelle
- Fuite de données

SPÉCIFICITÉ DES SYSTÈMES D'INFORMATION INDUSTRIELS

Les systèmes d'information des systèmes industriels se distinguent des systèmes d'information de gestion de part un certain nombre de spécificités qu'il convient de connaitre pour comprendre l'importance de les sécuriser.

Objectifs des systèmes

Piloter des installations
(physique, concret)
Réguler des procédés
Acquérir et traiter des données

Aspects fonctionnels

Contraintes métier
Contraintes « temps réel »,
Contraintes de sûreté de fonctionnement (SdF)
Haute disponibilité

Culture des intervenants

Automaticiens,
Instrumentistes électrotechniciens
Spécialistes en génie du procédé

Hétérogénéité des composants

La grande durée de vie des installations conduit à une « superposition » des vagues technologiques successives sur un même site entraînant un phénomène d'obsolescence des matériels

Environnement physique

Ateliers de production :
poussière, température, vibrations, électromagnétisme, produits nocifs à proximité, environnement extérieur, etc.

Localisation géographique

Dans des entrepôts, des usines, sur la voie publique, dans la campagne (stations de pompage, sous-stations électriques).

Gestion des incidents

La multitude de paramètres et la complexité de l'environnement limite la reproductibilité de l'incident

Durée de vie

Plus de 10 ans
(parfois 30 ou 40 ans)

MYTHES ET RÉALITÉS

«Mes réseaux industriels sont isolés, je suis protégé.»

Les systèmes d'information industriels sont souvent connectés aux réseaux de gestion et parfois directement à Internet. Les clés USB et les consoles de maintenance sont par ailleurs des vecteurs majeurs de propagation de virus y compris sur des systèmes isolés. Si l'isolation des réseaux industriels est impérative, elle n'est pas suffisante et devra être complétée par d'autres moyens.

«J'utilise des protocoles et bases de données propriétaires, je suis protégé.»

Même les solutions propriétaires comportent des composants standards, pour des raisons d'interopérabilité (avec le système d'exploitation par exemple) et de moindre coût. Les solutions propriétaires sont susceptibles d'être vulnérables car elles peuvent n'avoir fait l'objet d'aucune analyse de sécurité.

«L'intégration des mécanismes de sécurité (chiffrement, filtrage, authentification) est incompatible avec les contraintes de temps de réponse exigées et la continuité de service des installations industrielles.»

Les performances des composants et matériels utilisés ne sont plus un frein au déploiement de fonctions de sécurité. De plus la mise en place de moyens de cybersécurité s'inscrit dans une démarche anticipée et planifiée qui permet de prévoir des arrêts sans incidence sur la productivité ou l'efficacité des procédés.

«Une cyberattaque aura toujours moins d'impact qu'un incident physique comme un vol ou un incendie.»

Une attaque peut créer un dysfonctionnement global des installations plus difficiles à identifier et plus pernicieux (sabotage industriel, ralentissement de la production) qu'une attaque physique pouvant entrainer un temps de rétablissement très long (plusieurs semaines).

3. QUELLES SONT LES OBLIGATIONS LÉGALES ?

3. QUELLES SONT LES OBLIGATIONS LÉGALES ?

Si la cybersécurité est primordiale pour assurer la continuité des installations industrielles, elle est également encadrée par un certain nombre d'outils législatifs qu'il est important de connaitre et de distinguer. L'ANSSI définit ainsi les éléments suivants :

HOMOLOGATION - SYSTÈMES

Permet d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré. Délivrée par une autorité d'homologation pour un système d'information avant sa mise en service opérationnelle.

QUALIFICATION - PRESTATAIRES

Recommandation par l'État français de produits ou services de cybersécurité éprouvés et approuvés par l'ANSSI.

CERTIFICATION - PRODUITS

Atteste de la conformité de fonctions de sécurité du produit implémentées, décrites dans la cible de sécurité. Basée sur une analyse de conformité et des tests de pénétration réalisés par un évaluateur tiers sous l'autorité de l'ANSSI.

LABELLISATION - FORMATION

Ce terme est utilisé pour les programmes de soutien à la formation des métiers de la sécurité du numérique.

A RETENIR

- L'homologation est obligatoire pour un SIV
- La mise en œuvre de produits certifiés n'est pas une obligation pour l'homologation
- Les certifications sont valables pour des fonctions particulières et pour une durée limitée

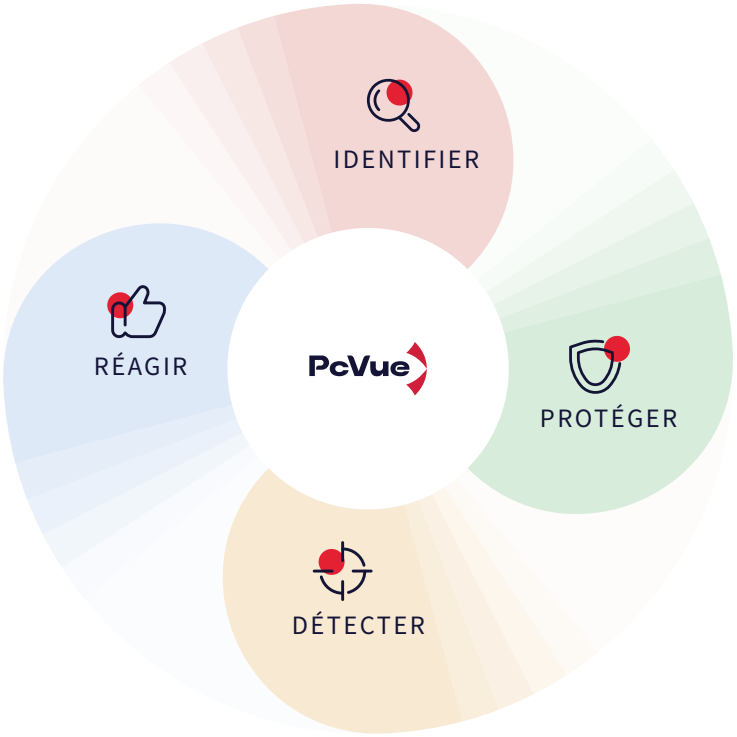
4. LES BONNES PRATIQUES POUR SÉCURISER SIMPLEMENT ET EFFICACEMENT SON SYSTÈME

4. LES BONNES PRATIQUES POUR SÉCURISER SIMPLEMENT ET EFFICACEMENT SON SYSTÈME

- ANALYSER LE SYSTÈME - identifier les vulnérabilités
- PROTÉGER LE SYSTÈME CONTRE LES INTRUSIONS
- DÉTECTER LES DYSFONCTIONNEMENTS
- ASSURER LE MAINTIEN EN CONDITIONS OPÉRATIONNELLES - Permettre la reprise d'activité

La plateforme de supervision PcVue s'appuie sur des dispositifs et emploie des technologies qui permettent de renforcer la sécurité d'un système de supervision autour des 4 piliers de la cybersécurité :

- Analyse du système et identification des vulnérabilités
- Protection du système pour limiter les intrusions
- Surveillance et détection des anomalies
- Maintien en conditions opérationnelles - Reprise d'activité



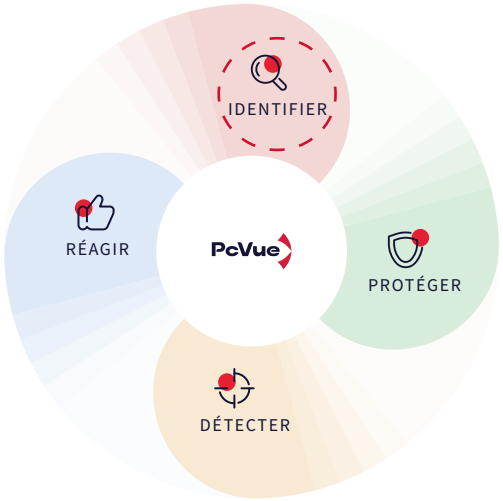
Décrits dans le document
Managing_Cybe_for_ICS_EN.pdf

ANALYSER LE SYSTÈME - IDENTIFIER LES VULNÉRABILITÉS

L'analyse du système et l'identification de ses vulnérabilités sont des étapes préalables indispensables dans la sécurisation de celui-ci.

Elle consiste à :

- Etablir le périmètre de sécurité du système d'automatisme et de supervision
- Définir les moyens nécessaires à mettre en œuvre en matière de sécurité



Systèmes neufs

Cette étude est menée en amont lors des phases de conception du système.

Systèmes existants

Un état des lieux de l'infrastructure réseau devra être fait. Pour cela une cartographie physique du réseau et logique des flux devra être établie.

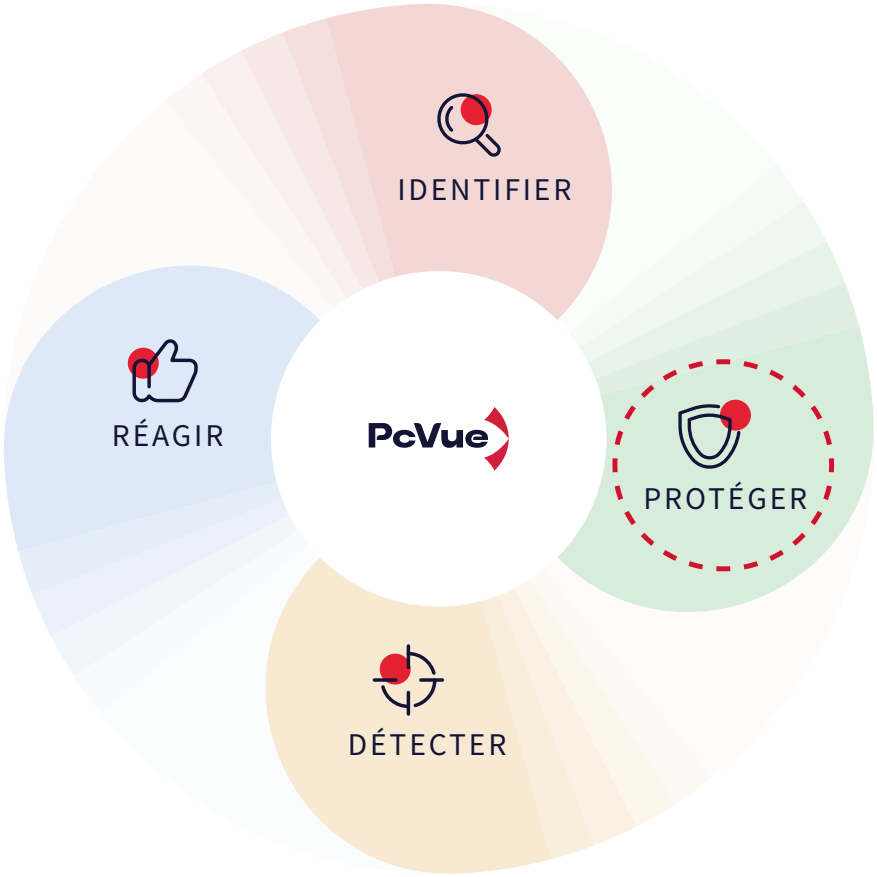
Dans ce contexte, les concepteurs doivent pouvoir s'appuyer sur les différents fournisseurs des composants du système tel que les outils de supervision. Dans ce cadre, les prestations de conseils de notre offre « Services » vous permettront d'être accompagnés dans ces démarches.

A RETENIR

- Une offre de service adaptée vous accompagnera dans cette démarche

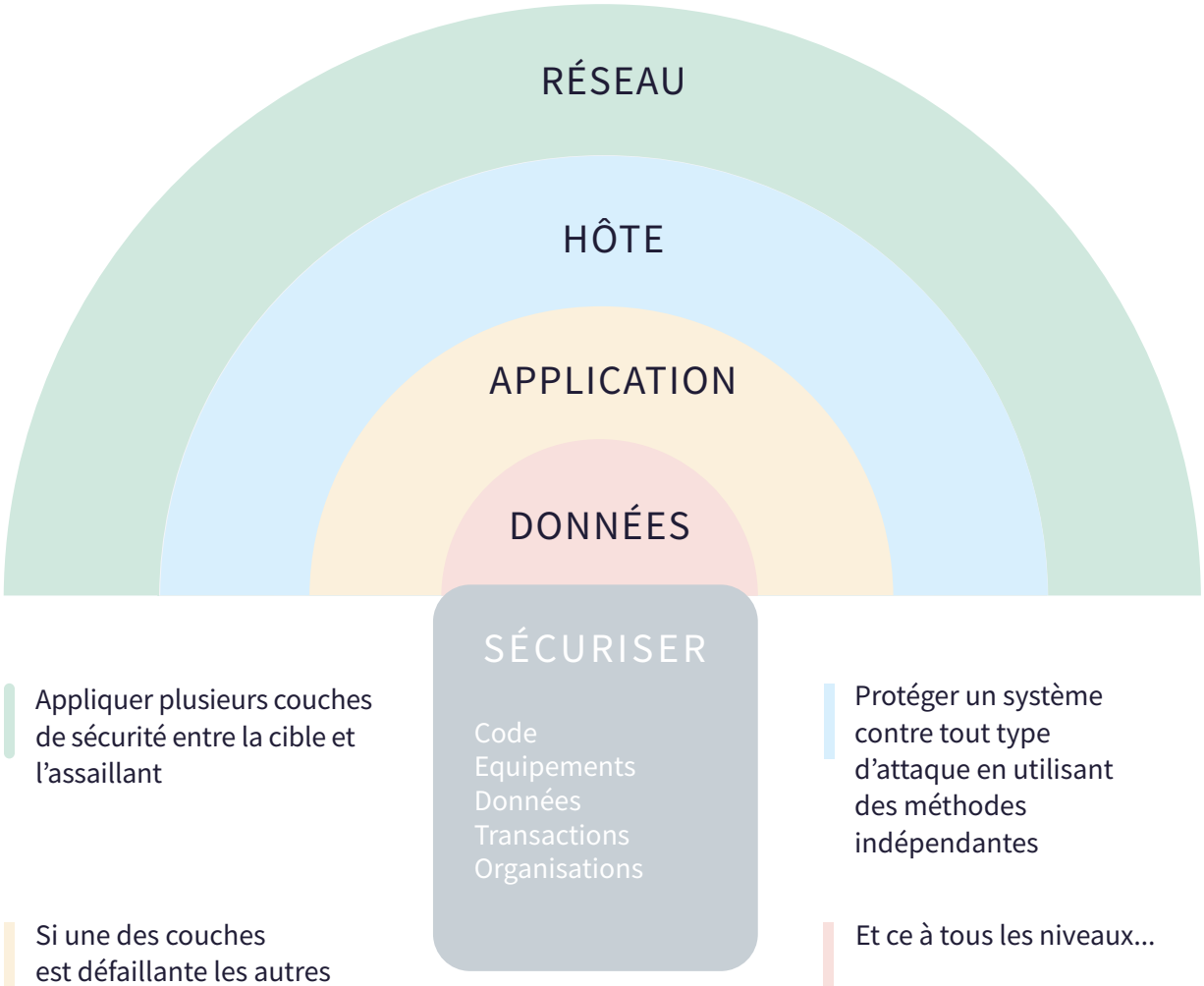
PROTÉGER LE SYSTÈME CONTRE LES INTRUSIONS

La connaissance approfondie du système et les risques associés permettent à l'administrateur de savoir ce qu'il convient de mettre en place pour la protection de celui-ci, pilier majeur dans la sécurité informatique. Les solutions que nous proposons apportent une multitude de moyens de protection du système de supervision.



PRINCIPE FONDAMENTAL : LA DÉFENSE EN PROFONDEUR PAR COUCHE DE SÉCURISATION

La protection du système se base sur le principe fondamental de la défense en profondeur qui consiste à appliquer des couches de sécurité successives au sein du système.



Appliquer plusieurs couches de sécurité entre la cible et l'assaillant

Si une des couches est défaillante les autres continuent de fonctionner et protègent les données

Protéger un système contre tout type d'attaque en utilisant des méthodes indépendantes

Et ce à tous les niveaux...

PEUT-ON FAIRE CONFIANCE AU LOGICIEL QUE L'ON INSTALLE ?

Avant même d'utiliser le logiciel il convient d'être sûr qu'il a bien été créé par l'éditeur, on parle d'authenticité, et qu'il est conforme à l'origine, que ses composants n'ont pas été altérés, on parle d'intégrité. Cela constitue la première couche de sécurisation.

Depuis la version 11.2, les packages d'installation et les fichiers binaires de PcVue sont signés numériquement, ce qui vous garantit à la fois l'intégrité et l'authenticité des fichiers, tant à l'installation, que plus tard à l'exécution.

Pour faciliter la diffusion de nos logiciels, ils sont disponibles dans leur ensemble en téléchargement via un serveur FTP.
Nous avons conscience que ce service très pratique nécessite toutefois de prendre quelques précautions de sécurité, comme l'utilisation d'un serveur FTP n'acceptant que les connexions sécurisées.

En outre, afin de vous permettre de vérifier l'intégrité des fournitures téléchargées depuis notre serveur, nous vous transmettons la signature unique appelée « hash » de tous les composants logiciels téléchargeables.
Nous utilisons cette méthode pour que vous puissiez vous assurer que le ou les fichiers téléchargés sont exactement tels que nous les avons produits, qu'ils n'ont pas été modifiés par un tiers illégitime ou endommagés. Depuis PcVue 11.2, nous utilisons l'algorithme SHA-256 qui est l'un des plus utilisés pour ce type de vérification.

A RETENIR

PcVue garantit l'authenticité et l'intégrité des fournitures d'installation

Téléchargements sécurisés
- Accès au serveur par connexions sécurisées

Authentification et intégrité
- Les fournitures que vous installez ont été créées par l'éditeur et sont signées numériquement
- Vérification de l'intégrité des téléchargements par algorithme SHA-256

Installation sécurisée
- Signature des composants d'installations
- Fichiers binaires signés

QUELLES PRÉCAUTIONS FAUT-IL PRENDRE POUR SÉCURISER MON PROJET DÈS L'INSTALLATION ?

Au moment d'installer le logiciel la question des fonctions qui seront utilisées en exploitation doit se poser. En effet, l'installation de certains composants peut exposer le logiciel à des attaques. Il convient donc de réduire la surface d'exposition en installant uniquement les composants nécessaires.

PcVue permet lors de son installation de choisir les composants à installer tels que :

- Composant d'acquisition de données
- Fichiers de configuration
- Composants web
- SDK et API
- …

Les projets applicatifs et les bibliothèques d'objets devront être déployés par media sécurisé (station blanche) externe au réseau d'exploitation. Une fonction de gestion de version intégrée disponible dans PcVue permettra de s'assurer du déploiement d'une version de projet et de bibliothèques de référence unique, sur l'ensemble des postes de l'architecture. PcVue vérifie en permanence la version utilisée sur chaque poste et alerte l'opérateur en cas de discordance.

A RETENIR

Lors de l'installation :

- N'installez que les composants nécessaires au projet
- Déployez les projets et bibliothèques par média sécurisé (station blanche) externe au réseau d'exploitation
- Utilisez la version de référence sur tous les postes

JE DOIS M'ASSURER QUE LE SYSTÈME RÉPOND AUX EXIGENCES IT

Les logiciels de supervision comme PcVue sont utilisés dans des infrastructures IT qui nécessitent le respect d'un certain nombre d'exigences, pour la sécurité du système. Un déploiement et des outils adaptés sont des éléments essentiels à prendre en compte.

ADAPTER LE DÉPLOIEMENT EN FONCTION DU BESOIN

Les solutions PcVue offrent diverses possibilités de déploiement pour répondre aux contraintes actuelles, tout en maintenant un niveau de sécurité important.

CHOISIR LE MODE D'EXÉCUTION APPROPRIÉ

Windows permet l'exécution des logiciels en tant que service ou en tant qu'application. Le mode d'exécution en tant que service est approprié pour des logiciels qui doivent s'exécuter en continu sur de longues périodes sans besoin d'interface utilisateur et ne nécessitant pas d'intervention. Concernant les logiciels de supervision comme PcVue cela correspond au fonctionnement des postes serveurs d'acquisition ou d'historique.

Le mode d'exécution en tant qu'application est lui adapté à un usage d'exploitation par un utilisateur au travers une interface graphique. Cela correspond aux postes clients PcVue. L'avantage d'utiliser l'un ou l'autre de ces modes est de pouvoir isoler les fonctions serveur spécifiques sans interface utilisateur des fonctions clientes avec un niveau de sécurité approprié.

A RETENIR

- Déployez les postes serveurs en tant que service, les postes clients en tant qu'application.

DÉPLOIEMENT WEB & MOBILE

Les solutions permettant de déployer différents types de clients légers tels que des clients web ou des applications mobiles doivent intégrer toutes les fonctionnalités de sécurité nécessaires (https, Oauth, certificats, HTML5) ainsi que des outils de maintenance. Le déploiement de ces solutions nécessite également une architecture réseau sécurisée décrite par ailleurs dans ce document.

Les solutions web et mobiles PcVue fonctionnent en mode client /serveurs, et s'appuient sur le composant IIS de Windows, tirant parti des protections associées.

PcVue intègre nativement une console de déploiement web permettant de définir, déployer et gérer une architecture web ou mobile.

Elle supporte les fonctionnalités suivantes :

- Déploiement de services Web et d'applications web sur IIS
- Gestion de la protection des données
- Gestion des certificats
- Enregistrement des accès utilisateur et gestion du serveur OAuth
- Audit / diagnostic IIS

La console de déploiement web s'exécute sur un serveur hébergeant un serveur Web IIS.

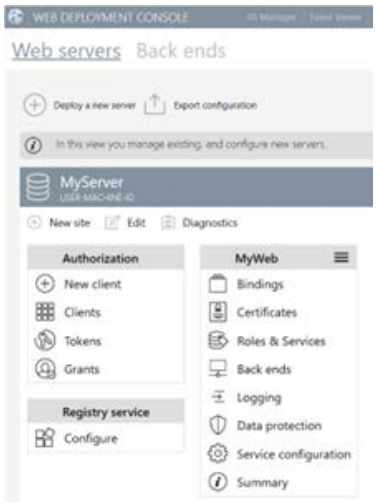


FIGURE 1 - DEPLOIEMENT CONSOLE WEB

Le déploiement web et mobile nécessite les éléments suivants :

- L'implémentation du protocole d'échange sécurisé HTTPS
- L'utilisation et la gestion de certificats de sécurité
- La compatibilité avec OAuth
- Une console permettant la configuration, la maintenance et le diagnostic.

ENVIRONNEMENTS VIRTUELS

En complément des architectures standards clients / serveurs de PcVue, nos produits sont utilisés sous des environnements de virtualisation comme VMware® et Hyper-V™.

FIGURE 2 - ENVIRONNEMENT VIRTUEL

Ces environnements permettent de faire fonctionner plusieurs serveurs d'applications PcVue avec différents systèmes d'exploitation sur une machine physique unique.

Cette machine pourra ainsi être hébergée dans une salle informatique sécurisée et secourue électriquement, ce qui évitera la prolifération géographique au sein de l'infrastructure clients de PC et limitera ainsi les failles pour l'accès physique aux ressources matérielles, tout en garantissant la continuité du même niveau de services et de disponibilité de l'application PcVue.

A RETENIR

Déployer un environnement virtuel pour :

- Centraliser la gestion des serveurs dans un endroit unique et sécurisé
- Limiter les failles de sécurité liées à l'accès physique aux ressources machines.

BUREAU D'ACCÈS À DISTANCE WINDOWS

Le Bureau d'accès à distance (aussi appelé RDS) est une fonctionnalité Windows qui permet d'héberger une application sur un serveur et de l'exécuter à distance sur un smartphone, une tablette ou un PC sur lesquels elle n'est pas installée.

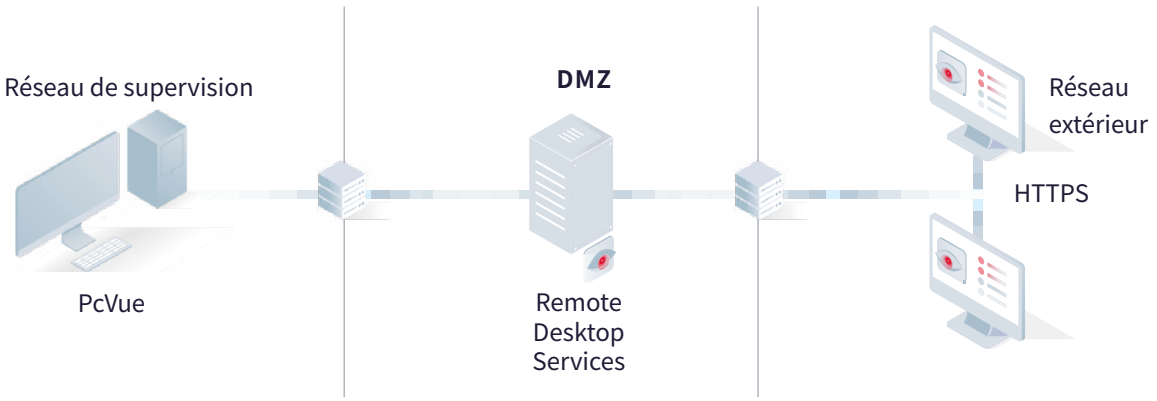


FIGURE 3 - ARCHITECTURE REMOTE DESKTOP

Concrètement cela revient à installer PcVue sur un poste serveur et à configurer la fonctionnalité RDS. PcVue n'est pas installé sur les terminaux, dits « banalisés ».
Un tel déploiement offre l'avantage de centraliser la gestion sur un poste serveur centralisé dont l'accès et la maintenance seront limités, réduisant les failles de sécurité. Les échanges de données se limitent aux actions claviers/souris et utilisent le protocole HTTPS, ce qui réduit les risques de corruption de données. Enfin la fonctionnalité RDS bénéficie des sécurités Windows.

A RETENIR

Déployer un environnement RDS pour :

- Centraliser la gestion des serveurs dans un endroit unique et sécurisé
- Sécuriser les échanges à distance avec HTTPS
- Limiter les failles de sécurité liées à l'installation de postes clients
- Bénéficier des fonctionnalités de sécurité Windows
- Limiter les risques de corruption des données échangées : seules les actions claviers/souris transitent sur le réseau.

Pour plus de détails sur la mise en œuvre sécurisée de RDS,
veuillez consulter les recommandations de l'ANSSI dans l'article suivant :
https://www.ssi.gouv.fr/uploads/IMG/pdf/Securite_de_RDP_article.pdf

INFRASTRUCTURE À CLÉS PUBLIQUES

Pour assurer la sécurité des données, une infrastructure à clé publique (PKI) doit être utilisée pour gérer des certificats numériques de sécurité qui permettront :

- la gestion de l'accès aux données (l'authentification)
- la vérification de l'intégrité des données
- la confidentialité des données

Ces certificats sont notamment utiles pour certains protocoles de communication sécurisés comme OPC UA, ou IEC 62351 pour ICCP. En général les utilisateurs de la supervision sont tributaires des services informatiques pour l'administration des PKI. Afin de permettre aux utilisateurs d'être autonomes PcVue fournit une PKI intégrée pour créer et déployer des certificats.

A RETENIR

- La sécurisation des données nécessite une infrastructure à clé publique (PKI)
- PcVue fournit une PKI intégrée pour gérer de manière autonome les certificats de sécurité nécessaires

L'ARCHITECTURE PERMET-ELLE LA SÉCURISATION DES DONNÉES ÉCHANGÉES ?

L'architecture réseau doit être conçue pour sécuriser l'échange des données c'est-à-dire de faire en sorte que les accès soient strictement définis et les flux de données contrôlés en fonction de la nature des réseaux.

Ainsi des postes extérieurs (réseaux administratifs, internet) ne doivent pas pouvoir accéder directement aux réseaux industriels sur lesquels se trouvent des équipements.
Classiquement un poste serveur d'acquisition devra être isolé des autres réseaux car il est en lien direct avec les équipements et représente un point de vulnérabilité.

Pour cela il conviendra de suivre les recommandations suivantes :

SEGMENTER LES RÉSEAUX PAR LA MISE EN PLACE DE ROUTEURS
- Réseaux physiques séparés, zone de logiques séparées (VLAN)
- Utilisation de DMZ pour isoler les réseaux et éviter les intrusions indésirables
- Utilisation de solutions de tunneling pour protéger le trafic entre 2 zones

FILTRER LES DONNÉES EN INSTALLANT DES PARE-FEUX POUR CONTRÔLER LES FLUX DE DONNÉES, NOTAMMENT DEPUIS L'EXTÉRIEUR VERS L'INTÉRIEUR DES RÉSEAUX
- Filtrage du trafic entrant/sortant par adresse source : destination, protocole, port

SÉCURISER LES DONNÉES ÉCHANGÉES
- Échanges HTTPS
- Utilisation de protocoles ouverts intégrant des fonctions de sécurité
(OPC UA, SNMP v3, IEC…)

PcVue offre la possibilité de concevoir des architectures multi postes clients/serveurs sur un réseau Ethernet en utilisant une messagerie inter-poste s'appuyant sur les couches TCP/IP standards.

D'autre part, sur une architecture client – serveur existante, l'adjonction d'un poste PcVue, à version identique et disposant du jeu d'application projet, sera impossible et le poste ne pourra pas se connecter aux postes existants tant que l'administrateur du projet n'aura pas déclaré explicitement ce nouveau poste et les relations qu'il doit entretenir au sein de l'application.

PcVue est une plateforme très flexible et évolutive permettant une multitude d'architectures. Le schéma ci-dessous montre un exemple d'architecture possible.

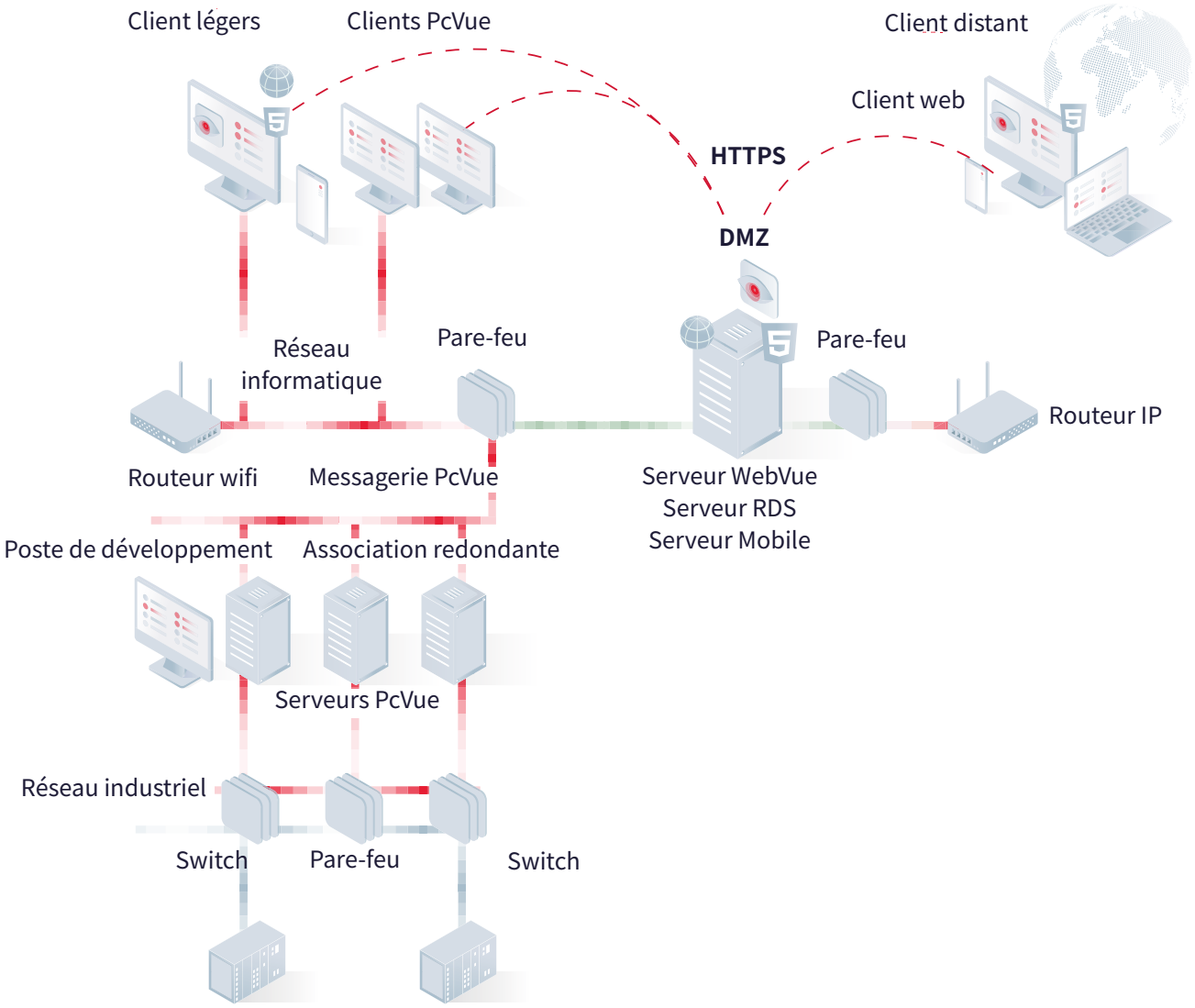


FIGURE 4 - EXEMPLE D'ARCHITECTURE

Cet exemple d'architecture s'articule autour des éléments suivants :

- L'acquisition des données est réalisée par des serveurs d'acquisition redondants sur le réseau industriel.
- Un poste de développement est utilisé pour la gestion centralisée du projet.
- Dans une architecture devant être homologuée, il est demandé d'isoler ce poste et d'utiliser un média spécifique sécurisé certifié non corrompu pour déployer une version de référence du projet.
- L'exploitation est réalisée par des postes clients sur le réseau informatique isolé par un pare-feu.
- Un poste installé sur un serveur Windows situé dans une zone démilitarisée (DMZ[1]) isolée par des pare-feux, héberge un serveur web, un serveur mobile et un serveur d'accès distant Windows (RDS[2]).

[1] Demilitarized Zone
[2] Remote Desktop Services

• Les clients peuvent être exécutés à distance au travers d'instances RDS en utilisant le bureau d'accès distant de Windows.
• Une interface installée sur le serveur permet l'affichage des instances clientes sur tous les terminaux supportant HTML5.
• Des clients web permettent l'exploitation depuis un navigateur web standard.
• Une application mobile connectée au serveur mobile est utilisée pour la notification et l'acquittement d'alarmes et le contrôle depuis un smartphone ou une tablette.
• Les échanges entre le serveur web et les terminaux utilisent des sockets sécurisés sous HTTPS[3].
• Les accès utilisateurs de l'ensemble du système sont gérés par Windows
• Active Directory permettant l'authentification unique (SSO[4]).

PcVue en partenariat avec ALLIED Telesis, offre une solution complète de protection matérielle pour répondre aux problématiques mentionnées ci-dessus :

• Gamme complète de Firewall/VPN industriels sécurisés
• Limitation et contrôle du trafic entre différentes zones du réseau
• Création de restrictions de trafic

A RETENIR

- Segmenter les réseaux avec des routeurs
- Filtrer les données
- Utiliser des solutions de « tunneling » : Chiffrement et authentification
- Sécuriser les échanges de données avec des pare-feux
- Isoler les serveurs dans une zone démilitarisée (DMZ).

[3] HTTPS : HyperText Transfer Protocol Secure
[4] Single Sign-On

QUELLES RECOMMANDATIONS POUR SÉCURISER L'ACQUISITION DES DONNÉES?

L'échange de données entre les équipements de terrain et les serveurs d'acquisition présente des risques particuliers qui doivent être pris en compte dans un système de supervision.

La variété des protocoles utilisés, leurs différents modes de fonctionnement, et leur nature (propriétaires, ou standards) ne les rendent pas égaux face aux menaces actuelles. Les protocoles les plus anciens sont bien souvent inadaptés aux contraintes de sécurité. A contrario, les protocoles récents souvent issus de standards internationaux disposent de fonctions de sécurité.

Lorsque cela est possible en matière d'interopérabilité, PcVue intègre les fonctions de sécurité des protocoles de communication industrielles :

- OPC UA (support d'OPC-Security pour l'authentification et les autorisations) et le déploiement des certificats avec la PKI intégrée
- SNMP - L'implémentation SNMP Manager de PcVue supporte SNMP v3 qui permet l'authentification, la garantie d'intégrité et le chiffrement des échanges.
- Les protocoles IEC
- MQTT (Via TLS)

Les mêmes recommandations sur la sécurisation des réseaux s'appliquent pour les réseaux terrains (segmentation, filtrage).

A RETENIR

- Privilégier l'usage de protocoles intégrant des mécanismes de sécurité
- Appliquer une segmentation et un filtrage entre les réseaux automates
- Utiliser des routeurs et tunnels VPN pour les flux d'acquisition

LA SÉCURITÉ ET COMMENT ASSURER L'INTÉGRITÉ DES DONNÉES ARCHIVÉES ?

Les données historiques produites par la supervision deviennent de plus en plus critiques et stratégiques au sein de l'organisation d'une entreprise et ce pour :

- des raisons de traçabilité
- une bonne compréhension du procédé et de son analyse
- l'optimisation de l'exploitation ou de l'infrastructure
- l'analyse après incidents et ce vis-à-vis éventuellement de tiers

D'autre part les données produites et historisées peuvent révéler les caractéristiques de fabrication, cœur de métier de l'entreprise, ou des informations confidentielles.
Face à la menace cybercriminelle les principes de production et d'accès aux données historiques reposent sur des sécurités actives au sein de notre produit :

- Accès aux données filtré et restreint selon les droits utilisateurs
- Production des données selon différents formats (propriétaires et non accessibles par des tiers, base de données SQL Server, …)

La sécurité et l'intégrité des données peuvent être renforcées par les dispositifs standards proposés par Windows Server et SQL Server en vigueur au sein de l'organisation.

Par exemple :

- L'authentification de l'utilisateur, que SQL Server gère sous la forme d'un objet "connexion". Ainsi, seules les applications utilisant ces connexions auront le droit d'exploiter l'instance. Dans le cas contraire, l'application se voit rejetée du système.
- Lorsque la connexion est créée, l'administrateur peut lui attribuer des droits sur l'administration du moteur de base de données. Pour ce faire, SQL Server propose une palette de scénarios dénommés "Rôles du serveur".
- Lorsqu'une connexion est créée, elle ne peut à elle seule accéder aux ressources du moteur de base de données (bases, tables, fonctionnalités,...), il est nécessaire de l'associer à un utilisateur de la/des bases de données concernées par la connexion. Une fois l'utilisateur créé, il est indispensable de lui attribuer des rôles qui permettront de définir les champs d'action autorisés (gestion des connexions, sauvegarde, accès en lecture – suppression – modification, etc …)

A RETENIR

- Accès aux données filtré et restreint selon les droits utilisateurs
- Production des données selon différents formats (propriétaires et non accessibles par des tiers, base de données type SQL Server, …)
- Sécurité et intégrité des données renforcées par les dispositifs standards proposés par Windows Server et SQL Server

QUELS SONT LES PRÉREQUIS CONCERNANT LES UTILISATEURS DU SYSTÈME ?

La gestion des droits utilisateurs est primordiale dans la protection du système de supervision car elle permet de contrôler le périmètre d'actions des utilisateurs.

Les caractéristiques d'une application PcVue par exemple dépendent des droits utilisateurs de l'opérateur qui est connecté.

Avant d'utiliser PcVue, un utilisateur doit se connecter en s'identifiant avec un nom et un mot de passe correspondant à un compte. La configuration de ce compte utilisateur détermine les caractéristiques du projet disponible en exploitation (par exemple les fenêtres que l'utilisateur peut ouvrir) ainsi que l'accès aux outils de configuration et au système d'exploitation.

Le compte utilisateur peut également être utilisé pour fournir une sélection de fenêtres associées à l'utilisateur et sélectionner un programme qui s'exécute lorsque l'utilisateur se connecte.

DÉFINISSEZ DES RÔLES

La première étape est de définir des rôles pour chaque utilisateur en fonction de son périmètre d'action dans la supervision (administrateur, développeur, opérateurs,…)

Pour PcVue, chaque compte utilisateur est associé à un nom et un mot de passe utilisés pour la connexion et d'un profil qui définit les droits.
Il n'y a pas de limitation du nombre d'utilisateurs configurés mais un seul utilisateur peut être connecté à la fois sur un même poste. Selon le poste à partir duquel l'utilisateur est connecté ses droits peuvent être différents. Des zones peuvent également être configurées. La configuration du profil fournit les droits d'accès à l'utilisateur. Le même profil peut être associé à plusieurs utilisateurs. Il n'y a pas de limitation du nombre de profils configurés.
Lorsqu'un nouvel utilisateur est créé, un profil lui est associé. Selon le poste sur lequel l'utilisateur est connecté, ses droits peuvent être différents et la création de différentes zones peut être configurée.

OPTIMISEZ LA GESTION DES DROITS

Il convient ensuite d'optimiser la gestion des droits en sélectionnant les options disponibles :

- Auto-déconnexions de l'utilisateur connecté après un temps d'inactivité configurable
- Configuration d'une période de validité pour les mots de passe
- Contrôle de la robustesse du mot de passe
- Niveaux de profils hiérarchiques

- Verrouillage de l'accès à des synoptiques particuliers, à des variables de commande, ou archivées, aux acquittements et masquage d'alarmes, etc…
- Configuration des profils différents pour un utilisateur selon le poste sur lequel il est connecté, dans une architecture multipostes
- Changement de mot de passe à la première connexion
- Gestion de la « mise en quarantaine » d'un utilisateur après trois tentatives de connexions infructueuses
- Chiffrement des informations des comptes utilisateurs

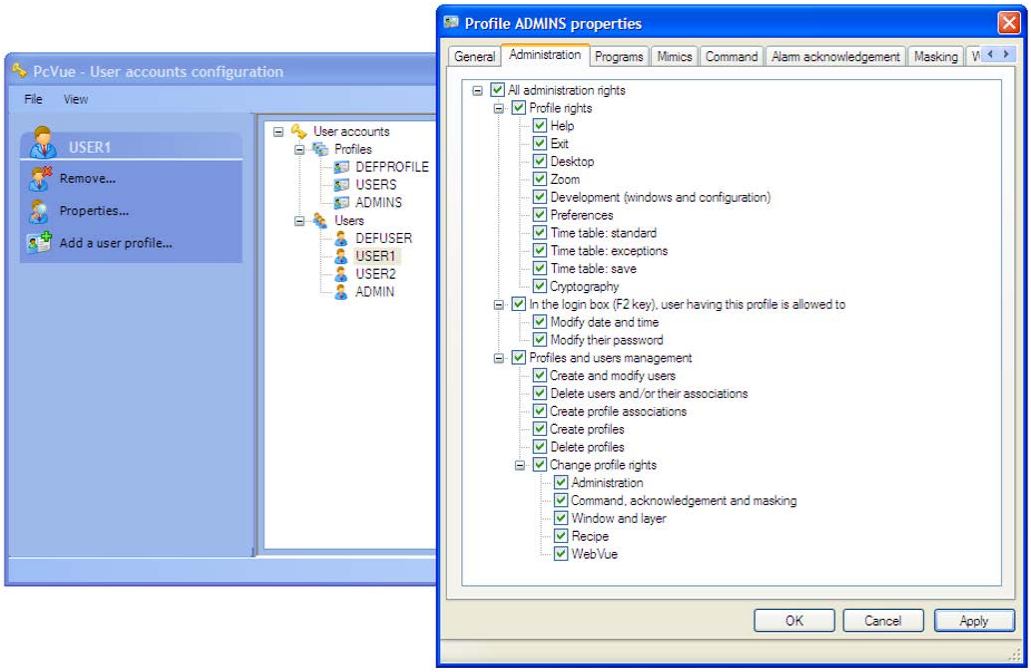


FIGURE 5 - CONFIGURATION DES PROFILS UTILISATEURS
UTILISEZ LA GESTION DES DROITS ET ANNUAIRE D'ENTREPRISE

Certaines entreprises imposent au sein de leur architecture I.T. de ne disposer que d'un annuaire central référençant l'ensemble des utilisateurs potentiels de leurs ressources informatiques. PcVue permet de s'appuyer sur l'annuaire Windows Active Directory afin d'assurer l'identification et l'authentification des utilisateurs.

Dans ce cas, les utilisateurs ne sont pas déclarés directement au sein du Superviseur, mais l'association "Profils PcVue" et "Groupes Active Directory" permet à PcVue de déterminer les autorisations et les privilèges des utilisateurs au sein de l'application de supervision, comme par exemple les droits de conduite (commande, consigne), ou bien encore les droits d'acquittement d'alarmes (par niveau, priorité, etc…).
Ces principes d'échange sont complètement automatisés et transparents au niveau de l'exploitation.

Il conviendra également de vérifier le chiffrement de l'annuaire.

CHOISISSEZ LE BON MODE DE LICENCE

Indépendamment des droits utilisateurs, les modifications ne peuvent être apportées au niveau de la configuration d'un projet que si les licences PcVue intègrent le mode « développement ».
En toute logique les licences dites « runtime » ne permettent en aucun cas d'accéder aux menus de configuration du produit, ce principe renforce les capacités de modification de l'application en ne déployant que des licences de ce type.

Ces principes sont renforcés par la gestion des droits utilisateurs puisque même si une personne accède au poste disposant d'une clé de protection permettant les développements, si ce dernier ne dispose pas du profil et mot de passe nécessaires, il ne pourra pas accéder aux phases de développement du projet.

Cartographiez et suivez les comptes utilisateurs

Il est impératif d'avoir une vision des utilisateurs du système et notamment des utilisateurs actifs. Les comptes ou profils inutiles devront être supprimés. Les comptes génériques (un compte pour une équipe par exemple) devront être proscrits. Les activités des utilisateurs pourront être consignées pour pouvoir comprendre le déroulement d'événements en cas d'incident ou d'attaque.

A RETENIR

- Définissez des rôles
- Cartographiez et suivez les comptes utilisateurs
- Optimisez la gestion des droits
- Utilisez les droits de l'annuaire d'entreprise si possible
- Vérifiez le chiffrement de l'annuaire

TABLE DES FONCTIONS DE SÉCURITÉ DISPONIBLES DANS PCVUE

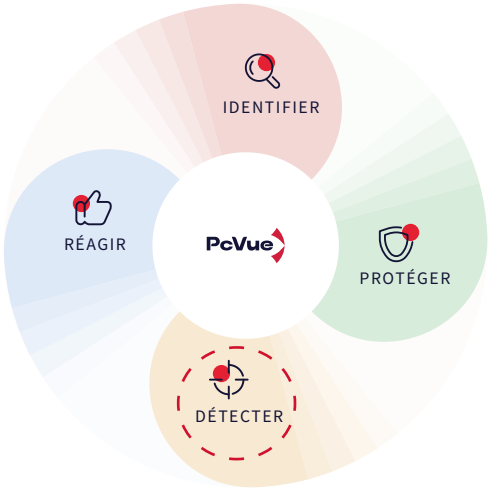
FONCTIONNALITÉ/TECHNOLOGIE SUPPORTÉE	COMMENTAIRES
Secure HTTP (HTTPS)	WebVue et WebServices sont des interfaces compatibles avec un proxy
Proxy	Il est possible d'utiliser les mécanismes d'authentification de PcVue ou de déléguer l'authentification à LDAP en utilisant Active Directory seulement.
Capacité de désactiver ou de désinstaller des fonctionnalités ou interfaces non utilisées. Par exemple : Accès Telnet, FTP, Interface WEB, Protocoles de contrôle commande, Interface série, Port USB ...	La plupart des fonctionnalités optionnelles peuvent déjà être désactivées ou bloquées. La configuration par défaut des nouvelles versions est plus restrictive afin d'améliorer la sécurité.
Infrastructure à clé publique (PKI)	Prise en charge d'une PKI intégrée

FIGURE 6 - TABLE DES FONCTIONS DE SÉCURITÉ DISPONIBLES

DÉTECTER LES DYSFONCTIONNEMENTS

Lorsque les étapes d'identification et de protection ont été réalisées, il est nécessaire de contrôler que le système fonctionne comme il devrait et de détecter un comportement anormal par rapport à un état de référence.

PcVue propose divers moyens de surveiller l'état de santé d'une installation, tant au niveau des applications que des réseaux et s'appuie sur de nombreux outils pour assurer la surveillance et le diagnostic d'un système de supervision.



COMMENT DIAGNOSTIQUER LE FONCTIONNEMENT DU SYSTÈME?

AUDIT DIAGNOSTIC

L'« audit diagnostic » est un composant PcVue qui permet de visualiser des informations relatives au fonctionnement interne du superviseur. Son utilisation principale est une aide au diagnostic mais il peut également être utilisé pour vérifier le bon fonctionnement général d'un système. Deux pages de suivi sont proposées : Compteurs et Surveillance.

COMPTEURS

Cette vue fournit une liste détaillée des compteurs internes au superviseur.

Objet - Compteurs des ressources système et des objets de l'application.
Instance - Compteurs de messages entre les gestionnaires de PcVue et la mémoire qui leur est allouée.
Temps - Temps passé à traiter les messages au niveau de chaque gestionnaire.

Flux - Flux de données associé aux transitions de valeur temps réel des variables dans l'arbre des variables.

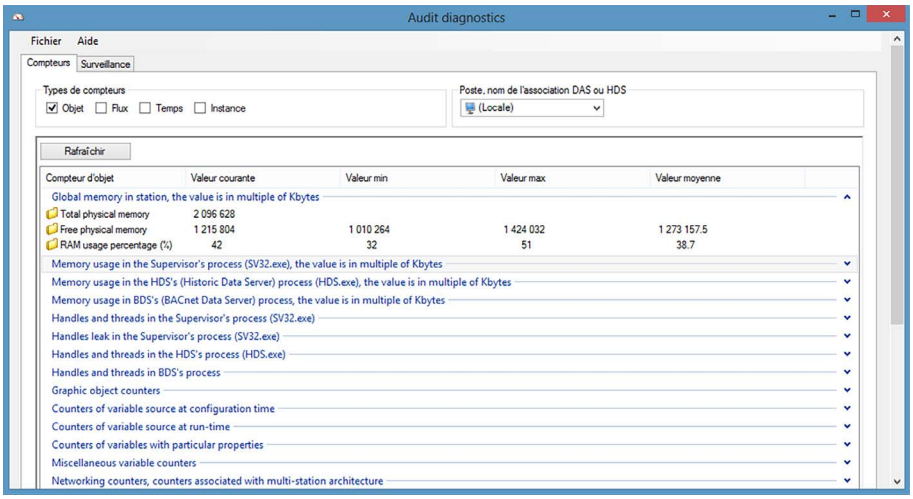


FIGURE 7 - OUTILS DE DIAGNOSTICS

Surveillance

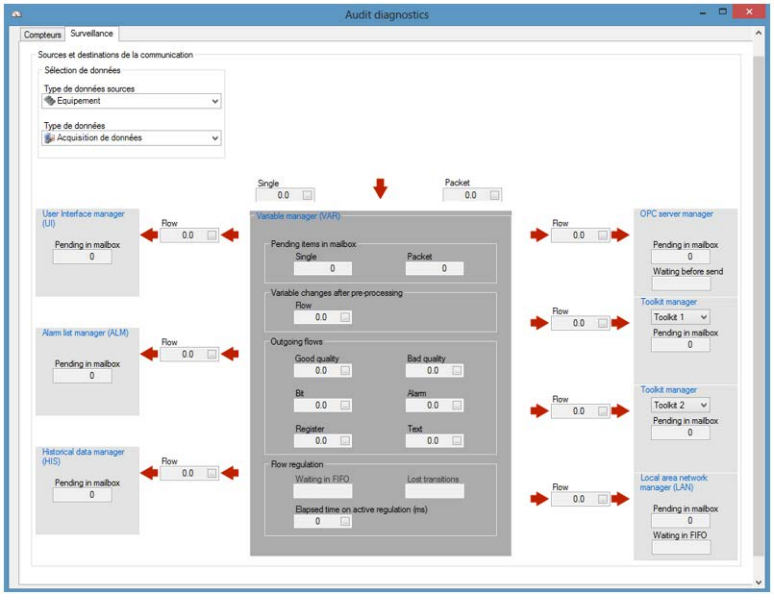


FIGURE 8 - VISUALISATION DES FLUX

Cette vue permet à l'utilisateur d'avoir une vision instantanée précise des échanges entre les différents modules internes de PcVue et d'avoir des informations détaillées sur les flux de données correspondant aux transitions de valeur temps réel des variables.

Ainsi l'utilisateur est en mesure d'analyser l'état de santé du système. Deux vues sont disponibles : une affichant les flux d'acquisition de données (données entrantes dans PcVue) et l'autre affichant les flux d'écriture (données envoyées depuis PcVue).

LA TRAÇABILITÉ EST-ELLE ASSURÉE?

CONSIGNATION D'EVÉNEMENTS

PcVue dispose d'un module d'enregistrement de données concernant les événements tels que les alarmes, les actions opérateurs, ou les changements de valeurs. Ces évènements archivés peuvent être affichés aux exploitants en utilisant une fenêtre de consignation.

VARIABLES SYSTÈMES

PcVue propose un grand nombre de variables systèmes indiquant l'état de fonctionnement du superviseur (nombre de requêtes en cours, en attente, flux archivé, …). Ces données peuvent être visualisées sous de multiples formes (valeurs instantanées, vue mètre, courbes, …) dans des synoptiques de la supervision et archivées si besoin. De plus, elles peuvent être transmises à un système de supervision tiers, grâce au protocole SNMP Agent de PcVue.

JOURNAUX D'EVÈNEMENTS

Tous les modules de PcVue génèrent des traces collectées dans des journaux d'événements. Ces journaux, stockés sous forme de fichiers de traces locaux, peuvent également être centralisés au sein d'un SIEM. Cette journalisation est utile dans tous les cas où des analyses post mortem doivent être menées : dysfonctionnement du système, soupçon d'intrusion…

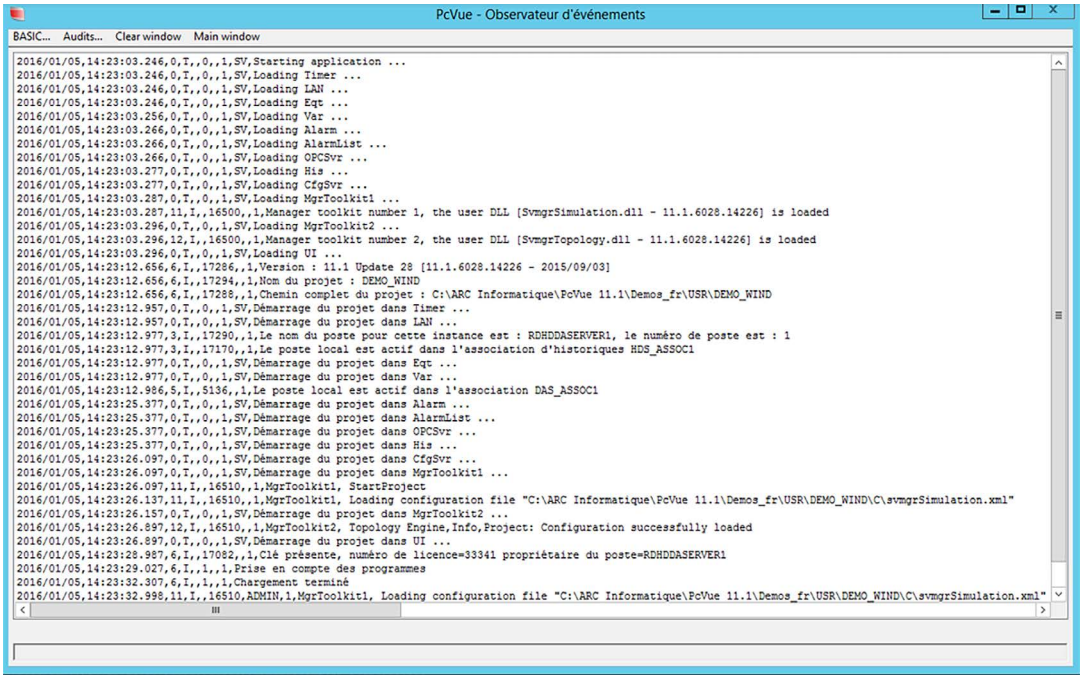


FIGURE 9 - OBSERVATEUR D'ÉVÈNEMENTS

JE DOIS METTRE À DISPOSITION L'ANALYSE LE REPORT D'INCIDENTS VERS LES OUTILS DE SUPERVISION IT

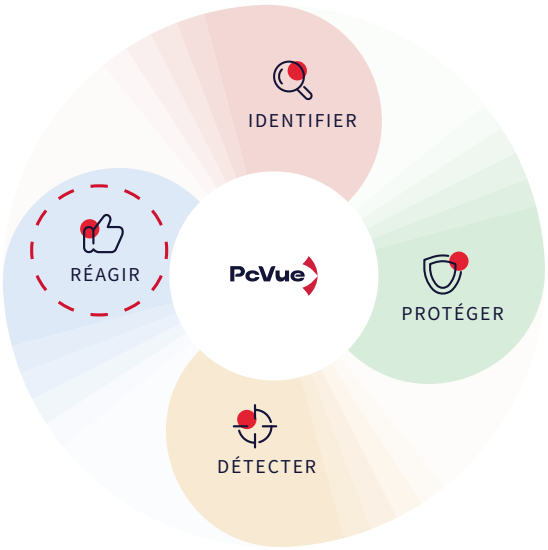
SYSLOG et journaux d'événements Windows

PcVue permet d'agréger les journaux d'événements par des outils de surveillance de systèmes informatiques tiers pour la corrélation et l'analyse des événements : PcVue prend en charge l'observateur d'événements Windows et SYSLOG sur UDP, TCP et TLS - RFC 3164 et 5424 et est conforme aux exigences ANSSI et CEI 62443 pour journalisation et traçage.

A RETENIR

- Vérifiez le fonctionnement du système avec les fonctions d'audit et de diagnostic intégrés
- Consultez les outils de traçabilité
- Partagez les données système aux outils de supervision IT

ASSURER LE MAINTIEN EN CONDITIONS OPÉRATIONNELLES - PERMETTRE LA REPRISE D'ACTIVITÉ



PcVue intègre nativement une gestion de version de projet avancée permettant de rétablir le comportement approprié de l'application après un incident.

La "gestion de versions de projet" s'appuie sur un référentiel de configuration.
Il permet de gérer un point d'accès où sera localisé l'ensemble du jeu de données "application" (bibliothèque d'objet, configuration de la base de données, droits utilisateurs, …). Renforcé par les dispositifs de sécurité des fonctions Serveur de Microsoft Windows, cela limitera l'accès à ces informations aux seules personnes habilitées à pouvoir modifier les caractéristiques de l'application.

Habituellement un poste dédié au développement de l'application de Supervision PcVue est utilisé pour héberger le répertoire central des versions de projet et faire les modifications sur ce projet. Dans une architecture devant être homologuée il est demandé d'isoler ce poste et d'utiliser un média spécifique sécurisé certifié non corrompu pour déployer une version de référence du projet.

En outre, pour garantir l'intégrité des données et la fiabilité de fonctionnement du procédé, nous avons complété les principes de gestion des applications par des dispositifs de traçabilité reposant sur la gestion des indices de version.

Ainsi le client peut préserver l'ensemble du jeu de données de son application comme par exemple :

- La version N-1, afin de pouvoir en cas de problème très rapidement revenir sur la version précédente
- La version N en cours d'exploitation, ayant fait l'objet précédemment de toutes les phases de qualification et vérification
- La ou les version(s) N+1 en cours de développement ayant fait l'objet ou non des phases de qualification et vérification

Une zone de commentaires permet de préciser le statut ou les informations nécessaires à la situation de la version et permet la traçabilité des modifications.

La gestion de version permettra pour les aspects de déploiement :

- De diffuser automatiquement à l'ensemble des postes de l'architecture le nouveau jeu de données afin de garantir une intégrité et cohérence des données exploitées
- A tout nouveau poste déclaré dans l'architecture de télécharger la version de référence, sans crainte d'exploiter un jeu de données non validé ou ancien
- A tout poste temporairement arrêté, dès sa phase de démarrage de vérifier si la version projet dont il dispose est bien la version en cours, ce en quoi il procédera au téléchargement automatique de la version de référence.

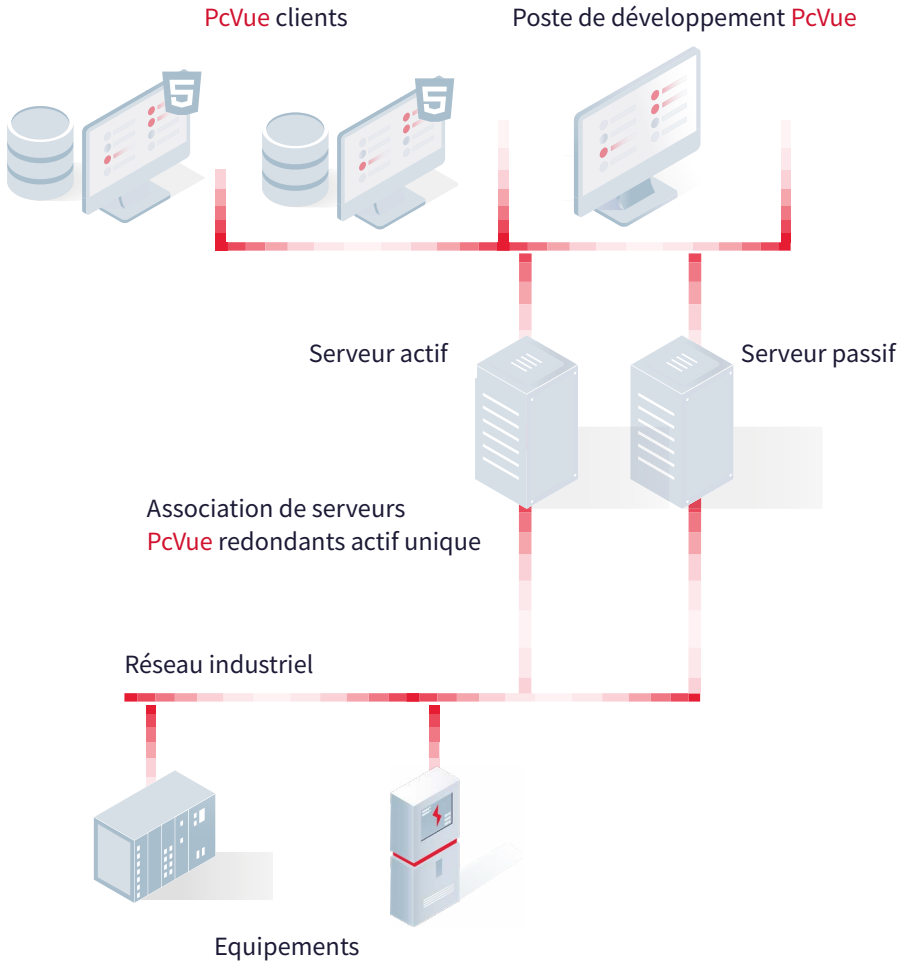


FIGURE 10 - ARCHITECTURE AVEC GESTION CENTRALISÉE DE VERSION

5. LES ENGAGEMENTS D'ARC INFORMATIQUE EN MATIÈRE DE CYBERSÉCURITÉ INFORMATIQUE

LES ENGAGEMENTS D'ARC INFORMATIQUE EN MATIÈRE DE CYBERSÉCURITÉ INFORMATIQUE

CONCEPTION PRODUITS

La dimension sécurité dépend largement des conditions dans lesquelles nos produits sont conçus et développés.

Ceci repose sur certains principes :

Processus de conception, développement, qualification et production issus de notre système de management par la Qualité ISO 9001 incluant :

- Méthodologie de spécifications, conception et développement
- Plan de vérification
- Plan de qualification
- Utilisation de robots logiciels pour tests unitaires
- Validation en grandeur nature sur beta sites
- Qualification interne en plateforme sur des projets en grandeur nature (mesures de charge et de performance)
- Tests de non-régression
- Système qualité de traçage d'anomalies

- L'entreprise ne sous-traite pas d'études, ni de développement, ni de qualification de ces produits. Aucune activité offshore
- Nos produits disposent de mécanismes de surveillance et de journalisation, permettant de détecter toute anomalie et ainsi faciliter les phases de diagnostic client
- Statuts de fonctionnement des différents composants d'une architecture permettant au client de connaitre et maitriser le comportement de son système

SÉCURITÉ ET CONDUITE DE PROJETS

Comme évoqué en introduction, l'approche sécurité d'un projet de supervision ne peut reposer que sur les seuls précautions et dispositifs introduits au sein des produits ou technologies (superviseur, architecture réseau Vlan, accès web, etc …).

Il faut pour cela que la méthodologie projet incluant les phases d'études, de spécifications, de tests et de mise en service intègre cette dimension. Il en est de même pour les phases d'exploitation et de maintenance.

Pour cela notre offre "Services" incluant des prestations de formation, assistance, conseils aussi bien en avant-projet qu'en phase de réalisation ou de maintenance, permet d'accompagner nos clients et leur faire bénéficier de notre expérience sur ce sujet dans le périmètre de notre champ d'action.

Nous avons ainsi accompagné nos clients dans des contextes projets comme :

- La conduite d'installations de production d'énergie en environnement nucléaire
- La sécurité et la conduite d'expérimentation en environnement nucléaire (Projets classés SIL II)
- La supervision d'infrastructures de transport ou ouvertes au public pour la sécurité des biens et personnes
- Les réseaux de transport d'énergie
- Des sites classés OIV
- Etc …

POLITIQUE DE SÉCURITÉ

Malgré tous les efforts mis en œuvre, nos produits peuvent être l'objet de vulnérabilités susceptibles de mettre en danger les systèmes dans lesquels ils sont intégrés. Dans le but de minimiser l'impact de ces vulnérabilités, ARC Informatique met en œuvre des pratiques transparentes vis-à-vis de ses clients, des autorités et du grand public.

En pratique, et au-delà des phases de conception de nos produits, nous nous engageons à :

1. Mettre notre savoir-faire à disposition de nos clients et de nos partenaires pour les aider à mettre en œuvre des solutions sécurisées,

2. Assurer une veille active et le suivi des alertes concernant nos produits,

3. Coordonner nos actions avec le réseau des CERT – Computer Emergency Response Teams – ainsi que les acteurs de la sécurité informatique qui adhèrent à ces engagements et aux recommandations des CERT,

4. Communiquer en toute transparence sur les vulnérabilités connues de nos produits avec des alertes de sécurité – Qu'il s'agisse de problèmes découverts en interne ou par des tiers.

5. En cas d'alerte, fournir des bulletins de sécurité afin d'apporter aussi vite que possible à nos clients des informations permettant de réduire les risques immédiats :
https://www.pcvue.com/security/
6. Tirer parti du retour d'expérience pour concevoir des produits plus sûrs.

SOURCES

PcVue - Les bonnes pratiques du déploiement web & mobile en supervision

PcVue - Architectures et déploiement

Cybersécurité des systèmes industriels (DI-Cyber) | ANSSI

ANSSI – Guide de l'homologation en 9 étapes

Table des illustrations

FIGURE 1 - DEPLOIEMENT CONSOLE WEB 23

FIGURE 2 - ENVIRONNEMENT VIRTUEL 24

FIGURE 3 - ARCHITECTURE REMOTE DESKTOP 25

FIGURE 4 - EXEMPLE D'ARCHITECTURE 28

FIGURE 5 - CONFIGURATION DES PROFILS UTILISATEURS UTILISEZ LA GESTION DES DROITS ET ANNUAIRE D'ENTREPRISE 33

FIGURE 6 - TABLE DES FONCTIONS DE SÉCURITÉ DISPONIBLES 35

FIGURE 7 - OUTILS DE DIAGNOSTICS 37

FIGURE 8 - VISUALISATION DES FLUX 37

FIGURE 9 - OBSERVATEUR D'ÉVÈNEMENT 39

FIGURE 10 - ARCHITECTURE AVEC GESTION CENTRALISÉE DE VERSION 41

ARC Informatique

Siège social
40 Av. Pierre Lefaucheux
92100 BOULOGNE-BILLIANCOURT

arcnews@arcinfo.com
www.pcvue.com

ARC Informatique is ISO 9001,
ISO 14001 and 27001 certified