

Supervision : détecter la panne avant qu'elle ne vous arrête

Disque plein, certificat expiré, sauvegarde en échec, site down : tout cela prévient — encore faut-il écouter. Le monitoring pour PME.

8 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/supervision-informatique

La plupart des pannes informatiques ne tombent pas du ciel : le disque était plein à 95 % depuis des semaines, la sauvegarde échouait depuis un mois, le certificat expirait à date connue. La supervision (monitoring) consiste à surveiller ces signaux en continu et à alerter la bonne personne AVANT l'arrêt. C'est la différence entre « on a changé le disque mardi soir » et « on a perdu deux jours et des données ».

1. Ce qu'une PME doit surveiller

- Les sauvegardes : succès/échec de chaque exécution — l'alerte la plus critique de toutes (voir notre guide)
- Les serveurs et le NAS : espace disque, état des disques (SMART, RAID dégradé), charge anormale, redémarrages
- Le site web et les services en ligne : disponibilité, temps de réponse, expiration du certificat HTTPS ET du nom de domaine
- Le réseau : connexion Internet, équipements clés (pare-feu, switches), VPN
- La sécurité : alertes de l'EDR, connexions suspectes, comptes verrouillés en série (voir notre guide EDR)
- Les onduleurs et la salle technique : batterie, température — la clim en panne un week-end d'été tue des serveurs

2. Les outils, du gratuit au supervisé

- La surveillance de site web : des services simples (dont de très bons gratuits) testent votre site chaque minute et alertent par email/SMS — dix minutes à mettre en place, faites-le aujourd'hui
- Les alertes natives : NAS, onduleurs, solutions de sauvegarde et suites cloud savent tous envoyer des alertes email — la moitié du monitoring consiste à ACTIVER et ROUTER ces alertes existantes
- Les plateformes de supervision (RMM) : agents sur postes et serveurs, tableau de bord central, alertes fines — l'outil standard des prestataires d'infogérance
- La supervision par le prestataire : dans un contrat d'infogérance sérieux, c'est lui qui reçoit et traite les alertes, avec des engagements de réaction — la formule adaptée à la PME sans équipe technique

ATTENTION

Le piège mortel du monitoring : les alertes qui partent vers une boîte que personne ne lit — l'adresse de l'ancien informaticien, un dossier spam, une boîte « alertes@ » jamais ouverte. Une alerte sans humain désigné pour la traiter n'existe pas. Chaque alerte doit avoir un destinataire vivant, et les alertes critiques un second canal (SMS, notification).

3. Régler pour être écouté

- Hiérarchiser : critique (réveille quelqu'un — sauvegarde en échec, site down, RAID dégradé), important (traité dans la journée), informatif (revue hebdomadaire)
- Lutter contre la fatigue d'alerte : une alerte qui crie pour rien chaque jour finit ignorée — et masque la vraie ; on affine les seuils, on supprime le bruit
- Tester les alertes : provoquer volontairement un déclenchement (débrancher, remplir un disque de test) vérifie toute la chaîne jusqu'au téléphone du destinataire
- Consigner : chaque alerte critique traitée laisse une trace — quoi, quand, action — qui nourrit la prévention

4. De la détection à la prévention

La supervision mûre ne se contente pas d'alerter : elle donne les tendances. L'espace disque qui se remplit de 2 % par semaine annonce l'échéance à trois mois — le remplacement se planifie en maintenance, pas en urgence. Le temps de réponse du site qui se dégrade lentement signale le problème avant les plaintes clients. Ces courbes transforment l'informatique subie en informatique pilotée — et alimentent directement le plan de renouvellement du matériel et le PRA.

L'essentiel à retenir

- 01 Mettre une surveillance sur le site web et le certificat (dix minutes)
- 02 Activer et router les alertes natives (NAS, sauvegardes, onduleur, cloud)
- 03 Désigner un destinataire vivant pour chaque alerte, avec canal de secours
- 04 Hiérarchiser critique / important / informatif et chasser le bruit
- 05 Tester la chaîne d'alerte en conditions réelles
- 06 Exiger du prestataire d'infogérance la supervision avec engagements

Questions fréquentes

Est-ce utile si nous n'avons ni serveur ni informaticien ?

Oui, en version légère : surveillance du site web et du certificat (gratuit), alertes de la suite cloud et de la sauvegarde routées vers une personne désignée, alerte d'expiration du domaine. Une heure de mise en place, et les pannes les plus bêtes — celles qui durent parce que personne ne savait — disparaissent.

Qui doit recevoir les alertes dans une petite structure ?

Le principe : une personne principale + une suppléante, et le prestataire pour ce qu'il couvre au contrat. Évitez l'alerte envoyée « à tout le monde » (donc à personne) comme l'alerte envoyée au seul dirigeant déjà débordé. Et mettez les canaux dans la fiche réflexe incident : en crise, savoir où regarder les alertes fait gagner du temps.

La supervision peut-elle détecter une cyberattaque ?

Elle y contribue : connexions à heures anormales, charge inexpliquée, sauvegardes qui échouent soudainement, comptes verrouillés en série sont des signaux typiques de compromission en cours. La détection sécurité proprement dite est le rôle de l'EDR — mais c'est bien la combinaison des deux, avec des humains qui lisent, qui attrape les attaques dans leur fenêtre silencieuse.

Pour aller plus loin

ANSSI — Guide d'hygiène informatique (supervision) — cyber.gouv.fr/publications/guide-dhygiene-informatique

Cyberionis — notre service maintenance & support — cyberionis.fr/#support

Vos sauvegardes tiendraient-elles le choc ?

Mise en place, tests de restauration, plan de reprise : nous rendons votre activité résiliente, à votre échelle.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr