LOUIS70 CONSEIL | CYBERSÉCURITÉ & CONSEIL STRATÉGIQUE

# Rapport d'audit
# *Infrastructure réseau*

PÉRIMÈTRE LAN / WAN / DMZ -- ANALYSE DE LA POSTURE DE SÉCURITÉ

RÉSEAU

RÉFÉRENCE
L70C-AR-2026-03

DATE
Avril 2026

VERSION
1.0 -- Finale

CLASSIFICATION
Restreinte

DESTINATAIRE
DSI / DG


RÉSUMÉ EXÉCUTIF

L'audit conduit en mars 2026 sur l'infrastructure réseau d'une ETI du secteur industriel (périmètre : siège social, deux sites de production, accès distants) révèle une posture de sécurité globalement insuffisante au regard des exigences NIS2 et des menaces actives documentées sur ce segment sectoriel. Trois constats sont classés critiques, dont deux requièrent une action corrective immédiate sans attendre la mise en oeuvre du plan de remédiation complet. Cinq constats majeurs et trois mineurs complètent le tableau. Une feuille de route à 90 jours est proposée en section 4.


## 01 Synthèse des risques identifiés

**3** CRITIQUE
Action immédiate requise. Exposition directe à une compromission.

**5** MAJEUR
Remédiation dans les 30 jours. Risque élevé en cas d'exploitation combinée.

**3** MINEUR
Traitement dans les 90 jours. Impact limité mais durcissement nécessaire.

## 02 Constats détaillés

C-01 CRITIQUE Absence de segmentation réseau entre OT et IT

OBSERVATION

Les équipements de supervision industrielle (SCADA, automates, IHM) partagent le même segment réseau que les postes bureautiques et les serveurs de messagerie. Aucune barrière de filtrage n'est positionnée entre l'environnement opérationnel (OT) et le réseau d'entreprise (IT). Un équipement bureautique compromis dispose d'un accès direct et non contrôlé aux automates de production.

```
Éléments techniques :
VLAN unique constaté sur les switches de distribution (172.16.0.0/16 non segmenté)
Ping ICMP depuis un poste bureau vers 3 IHM de production : réponse positive
Accès Modbus TCP ouvert (port 502) depuis le LAN bureautique
Absence de firewall inter-zones documentée
```

RECOMMANDATION

Mise en place urgente d'une architecture de zones distinctes (IT / DMZ industrielle / OT strict) avec firewall de niveau 3/4 en coupure. Désactivation immédiate des accès directs IT vers OT dans l'attente du redécoupage VLAN. Délai cible : 72 heures pour l'isolation d'urgence, 21 jours pour la segmentation pérenne.

C-02 CRITIQUE Comptes d'administration locaux non gérés, mots de passe partagés

OBSERVATION

L'ensemble des serveurs Windows du périmètre audité utilisent un compte administrateur local commun avec un mot de passe identique, non renouvelé depuis 2022. Aucune solution de gestion des comptes à privilèges (PAM) n'est déployée. La compromission d'un seul équipement permet une latéralisation immédiate sur l'intégralité du parc serveur.

```
Éléments techniques :
27 serveurs Windows Server (2016-2022) avec compte local "Administrateur" actif
Hash NTLM identique constaté sur 100% des machines testées (pass-the-hash trivial)
Absence de LAPS ou équivalent
Journaux d'accès administrateurs non centralisés
```

RECOMMANDATION

Déploiement immédiat de Microsoft LAPS (ou équivalent open source) pour la gestion des mots de passe locaux. Rotation forcée des mots de passe sur l'ensemble du parc. Mise en place d'une solution PAM (CyberArk, Wallix Bastion ou équivalent) dans les 30 jours. Activation de la journalisation centralisée des accès privilégiés.

C-03 CRITIQUE Accès VPN sans MFA, certificats expirés

OBSERVATION

L'accès VPN distant (utilisé par 47 collaborateurs et 6 prestataires externes) repose uniquement sur une authentification par identifiant et mot de passe. Aucun second facteur n'est requis. Par ailleurs, le certificat SSL de la passerelle VPN est expiré depuis 114 jours, désactivant de facto les avertissements de sécurité sur les clients configurés en mode permissif.

```
Éléments techniques :
Gateway VPN : Fortinet FortiGate 100F, firmware 7.0.9 (non à jour)
Certificat expiré le 23 décembre 2025 (non renouvelé)
6 comptes prestataires actifs sans date d'expiration ni traçabilité d'usage
Authentification : login/password uniquement, pas de TOTP ni de certificat client
```

RECOMMANDATION

Renouvellement immédiat du certificat SSL (délai maximal : 48 heures). Activation du MFA sur l'ensemble des comptes VPN avant toute reconnexion prestataire. Audit et désactivation des comptes prestataires inactifs. Mise à jour firmware FortiGate. Mise en place d'une politique d'expiration automatique des comptes à accès temporaire.

M-01 MAJEUR Absence de supervision et de détection d'incidents (SIEM)

OBSERVATION

Aucun outil de centralisation et de corrélation des journaux n'est déployé. Les logs des équipements actifs (firewalls, AD, serveurs) ne sont pas collectés de façon centralisée. En cas d'incident, la capacité de reconstruction de la chronologie des événements est nulle au-delà de 7 jours (rotation locale des logs). La détection d'une compromission silencieuse est impossible dans l'état actuel.

RECOMMANDATION

Déploiement d'un SIEM léger (Wazuh, Elastic SIEM ou équivalent) avec collecte prioritaire sur AD, firewalls et accès VPN. Définition d'une politique de rétention minimale à 90 jours. Mise en place d'alertes sur les événements critiques (connexions en dehors des horaires, échecs d'authentification multiples, accès comptes privilégiés).

M-02 MAJEUR Plan de sauvegarde sans test de restauration depuis 18 mois

OBSERVATION

Les sauvegardes sont réalisées quotidiennement (Veeam Backup) mais aucun exercice de restauration complète n'a été conduit depuis octobre 2024. Les sauvegardes hors site reposent sur un prestataire tiers dont le contrat de niveau de service n'a pas été vérifié. En cas d'incident ransomware, la capacité réelle de reprise est inconnue.

RECOMMANDATION

Conduire un exercice de restauration complète d'un serveur de référence dans les 30 jours. Vérifier contractuellement le RTO/RPO avec le prestataire hors site. Mettre en place un calendrier de tests semestriels documentés. Vérifier l'isolation des sauvegardes du réseau de production (protection anti-ransomware).

M-03 MAJEUR Politique de mises à jour non appliquée, correctifs critiques en retard

OBSERVATION

L'inventaire des correctifs appliqués révèle 14 vulnérabilités CVSS supérieur ou égal à 9.0 non corrigées sur des systèmes exposés, dont deux faisant l'objet d'exploits publics actifs (CVE documentées en 2025). La politique de patch management existe documentairement mais n'est pas appliquée faute de ressources dédiées.

RECOMMANDATION

Application prioritaire des correctifs pour les 14 vulnérabilités CVSS ≥9.0 dans un délai de 15 jours. Déploiement d'un outil de gestion centralisée des mises à jour (WSUS renforcé, ou solution tierce). Définition d'un SLA interne : correctifs critiques sous 72h, majeurs sous 14 jours.

M-04 MAJEUR Exposition de services internes sur Internet sans inventaire formalisé

OBSERVATION

Un scan de la surface d'exposition externe révèle 9 services actifs sur des ports non standard, dont 3 non répertoriés dans la documentation réseau fournie. Parmi eux : un accès RDP direct (port 3389) vers un serveur de fichiers et une interface de gestion de switch non protégée par authentification renforcée.

RECOMMANDATION

Fermeture immédiate du RDP direct exposé sur Internet (basculement vers accès VPN uniquement). Inventaire exhaustif des services exposés. Protection de l'interface de gestion switch par authentification et restriction d'IP sources. Réalisation trimestrielle d'un scan de surface externe.

M-05 MAJEUR Absence de politique de gestion des équipements personnels (BYOD)

OBSERVATION

Des équipements personnels (smartphones, tablettes, postes non managés) accèdent au réseau Wi-Fi d'entreprise et potentiellement aux ressources internes via des partages non contrôlés. Aucune politique BYOD n'est définie ni communiquée. Le réseau Wi-Fi invité n'est pas isolé du réseau de production.

RECOMMANDATION

Séparation immédiate du SSID invité du réseau de production. Rédaction et diffusion d'une charte BYOD. Déploiement d'une solution NAC (Network Access Control) pour conditionner l'accès réseau à la conformité du poste. Mise en place d'un portail captif sur le Wi-Fi invité.

N-01 MINEUR Documentation réseau incomplète et non maintenue à jour

OBSERVATION

Les schémas réseau fournis datent de 2023 et ne reflètent pas les évolutions récentes (ajout d'un site de production, déploiement d'une baie de stockage NAS). L'absence de documentation à jour complique l'analyse d'impact en cas d'incident et allonge les délais d'intervention.

RECOMMANDATION

Mise à jour de la cartographie réseau dans les 90 jours. Adoption d'un outil de documentation vivante (NetBox ou équivalent). Processus formalisé de mise à jour lors de chaque changement d'infrastructure.

N-02 MINEUR Bannières d'identification sur les équipements actifs exposant la version firmware

OBSERVATION

Les interfaces d'administration des switchs core et du pare-feu affichent par défaut la version exacte du firmware dans la bannière de connexion. Cette information facilite le ciblage par un attaquant ayant accès aux interfaces, en lui permettant d'identifier directement les vulnérabilités applicables.

RECOMMANDATION

Suppression ou remplacement des bannières par défaut sur l'ensemble des équipements actifs. Configuration d'une bannière légale standard (mention d'accès restreint). Vérification que les pages de login web n'exposent pas d'informations de version.

N-03 MINEUR Protocoles obsolètes actifs (Telnet, SNMPv1) sur équipements périphériques

OBSERVATION

Telnet (port 23) et SNMPv1 sont actifs sur plusieurs équipements d'accès périphériques (switches d'étage, imprimantes réseau). Ces protocoles transmettent les identifiants en clair et permettent une interception triviale sur un réseau local compromis.

RECOMMANDATION

Désactivation de Telnet et remplacement par SSH sur tous les équipements compatibles. Migration de SNMPv1/v2 vers SNMPv3 avec authentification et chiffrement. Inventaire des équipements ne supportant pas SSH (remplacement planifié).

## 03 Feuille de route à 90 jours

J+0 -- J+15

### Actions immédiates

- Isolation d'urgence OT/IT (ACL temporaires)
- Renouvellement certificat SSL VPN
- Activation MFA sur tous les comptes VPN
- Rotation mots de passe administrateurs locaux + déploiement LAPS
- Fermeture exposition RDP Internet
- Correctifs CVSS ≥9.0 sur systèmes exposés

J+15 -- J+45

### Remédiation majeure

- Architecture segmentation OT/IT pérenne (VLAN + firewall inter-zones)
- Déploiement SIEM (collecte AD, firewall, VPN)
- Test de restauration sauvegarde complet
- Isolation SSID Wi-Fi invité
- Inventaire et fermeture services exposés non documentés
- Déploiement PAM (comptes à privilèges)

J+45 -- J+90

### Durcissement et gouvernance

- Mise à jour documentation réseau (NetBox)
- Suppression bannières firmware équipements
- Migration SNMPv3, désactivation Telnet
- Rédaction et diffusion charte BYOD
- SLA patch management formalisé et outillé

- Scan de surface externe trimestriel -- premier cycle

*Ce rapport constitue un livrable de démonstration anonymisé, produit à des fins de présentation commerciale de Louis70 Conseil SAS. La démarche, les constats et les recommandations reflètent le niveau d'analyse et le format delivrable appliqués dans le cadre de missions réelles. Les données techniques citées sont fictives ou représentatives d'un environnement générique. Toute mission fait l'objet d'un contrat de prestation avec clause de confidentialité renforcée et engagement de non-divulgation.*

**L. Bonjean**

CAPITAINE DE FRÉGATE (H) -- GÉRANT LOUIS70 CONSEIL SAS -- SIREN 989 600 481