Rapport GRC – Global Solutions (Cas Fictif)

1. Analyse des Risques et Vulnérabilités

Risques identifiés :

Menace	Vulnérabilité	actifs concernés	Impact (CID)	Score	Probabilité	Score Critique
Phishing ciblé	Absence de formation sur le sujet.	Employés, boite mail professionnelle	C,I	4	3	12
Ransomware	Absence d'équipement de protection.	Poste de travail, Serveur, base de données	C,I,D	4	4	16
Infostealer	Politique de sécurité laxiste concernant l'installation de plugins ou extensions non vérifiés.	Données sensibles, poste avec des informations importantes.	C,I,D	4	3	12
Faible segmentation VLAN	Réseau sans séparation entre environnements sensibles et utilisateurs standards.	Serveurs, réseau interne.	I,D	2	3	6
Absence de MFA	Accès aux services critiques uniquement protégés par mot de passe.	Comptes de personnes à hautes responsabilités.	C,I,D	2	4	8
Pas de supervision centralisée	Aucun SIEM ou solution de log centralisée pour détecter et analyser les incidents.	Gestion des postes. Gestion du réseau.	D,I	3	3	9

2. Recommandations Techniques

a) Infrastructure & Réseau

1. **Pare-feu nouvelle génération (NGFW) avec Inspection approfondie des paquets (DPI)**
    - Déployer un NGFW en front end pour filtrer le trafic entrant et sortant, détecter les attaques applicatives (Web App Firewall) et bloquer les menaces en temps réel.

2. **Séparation stricte (cloisonnement) entre VLANs via des ACL (Access Control Lists)**
    - Segmenter le réseau en plusieurs zones logiques :
        - VLAN Production (serveurs métiers, bases de données internes)
        - VLAN Infra (serveurs d'infrastructure : AD, DNS, DHCP, stockage, backups)
        - VLAN Bureautique (Direction, Utilisateurs)
        - VLAN Développement (postes développeurs, environnements de test)
        - VLAN WEB (serveurs web publics, bases de données web)
        - VLAN Serveur DSI (SIEM, EDR, serveurs d'authentification Radius/LDAP)
        - DMZ (Proxy Web, serveurs applicatifs publics, database web)
    - Appliquer des règles ACL sur les routeurs et commutateurs pour n'autoriser que le minimum nécessaire :
        - Interdiction du trafic direct "Bureautique → Production"
        - Blocage des flux non justifiés entre VLAN Développement et VLAN Production

3. **Proxy Web et filtrage des connexions sortantes dans une DMZ**
    - Installer un proxy web dédié dans la DMZ pour filtrer les accès Internet :
        - Liste noire/jaune des sites malveillants
        - Inspection des certificats HTTPS
        - Blocage des téléchargements d'exécutables non approuvés
4. **Pare-feu interne entre VLANs Employés et VLANs sensibles**
    - Déployer un pare-feu interne (voire une UTM virtuelle) permettant d'isoler les machines bureautiques (postes utilisateurs) des ressources serveurs.
5. **Création d'un VLAN distinct pour les bases de données (BDD) web et internes**
    - Les bases de données destinées au site web public (VLAN WEB) doivent être dans un sous-VLAN BDD dédié.
    - Les BDD internes (comptabilité, RH) sont segmentées dans le VLAN Serveur DSI.
6. **Création d'un VLAN dédié DSI avec SIEM et EDR pour la supervision**
    - Le VLAN DSI regroupe les serveurs de sécurité :
        - SIEM (collecte et corrélation des logs)
        - EDR (détection des anomalies sur les endpoints)
        - Serveur Radius/LDAP pour l'authentification centralisée.
7. **Ajout d'un système d'authentification type RADIUS / LDAP pour contrôler l'accès au réseau**
    - Registration des postes (802.1X) et authentification par RADIUS pour tout nouvel équipement se connectant au LAN filaire ou Wi-Fi.

b) Postes & Environnements Développeurs

1. **Blocage de l'installation de plugins non vérifiés (via GPO)**
    - Mettre en place une GPO (Active Directory) restreignant l'installation de modules/plugins uniquement depuis une liste approuvée (whitelist).
    - Interdire les droits d'installation "software" aux utilisateurs non-administrateurs.
2. **Déploiement d'un EDR (Endpoint Detection & Response)**
    - Installer un agent EDR sur tous les endpoints (postes bureautiques, postes développeurs, serveurs) pour :
        - Détecter les comportements suspects (mouvements latéraux, exfiltration, rançonnage)
        - Effectuer des quarantaines automatiques et fournir des rapports de forensic.
3. **Application automatique des mises à jour via un serveur WSUS (Windows Server Update Services)**
    - Chaque poste Windows doit remonter au WSUS interne.
    - Configurer un planning de redémarrage minimal pour ne pas perturber la production.

c) Contrôle des accès

1. **Mise en place du MFA (Multi-Factor Authentication) pour tout accès distant et ressources critiques**
    - Exiger un deuxième facteur (OTP, push, token matériel) pour :
        - VPN IPsec/SSL des administrateurs et cadres
        - Accès aux consoles de management (firewall, SIEM, serveurs DSI)

        - Connexions RDP/SSH vers la production

2. **Application du principe du moindre privilège**
    - Créer des comptes locaux “standard” pour le travail quotidien.
    - Attribuer les droits d'administrateur (local ou domain) uniquement si strictement nécessaire pendant la durée d’une tâche.
    - Séparer les comptes “usage” et “administration” sur les postes Windows/Linux.
3. **Revue mensuelle des droits utilisateurs et comptes inactifs**
    - Procéder à une revue des permissions AD, des groupes “Admin” et “VPN-Users” mensuellement.
    - Désactiver ou archiver tout compte n’ayant pas été utilisé depuis plus de 90 jours.

d) Supervision & Journalisation

1. **Mise en place d’un SIEM (Security Information and Event Management)**
    - Collecte centralisée des logs syslog/Windows Event, alertes IPS/IDS, agent EDR, journaux de firewall.
    - Corrélation des événements pour détecter :
        - Brute force authentification (SSH, RDP, VPN)
        - Exfiltration de données (logs proxy)
        - Comportement anormal (scanning interne, exécutions de code suspect)

2. **Centralisation des logs système, applicatifs, sécurité**
    - Configurer chaque serveur/pare-feu/application pour envoyer ses logs au SIEM.
    - Mettre en place des rétentions minimales (au moins 6 mois de stockage, 1 an d'indexation).
3. **Détection des comportements anormaux / exfiltration**
    - Définir des use cases de détection :
        - Volume inhabituel de données sortantes vers un même domaine
        - Tentatives d'accès à des ressources sensibles en dehors des plages horaires usuelles
        - Création ou modification massive de comptes
    - Mettre en place des playbooks d'alerte et d'escalade.

3. Sensibilisation des Employés

Objectif	Action proposée
Détection de phishing	- Simulations mensuelles de campagnes de phishing (phish-test) - Tableaux de score par service et retours pédagogiques personnalisés
Sécurité des mots de passe	- Mise à disposition d'un gestionnaire de mots de passe (ex. Bitwarden, KeepassXC) - Formation à la création de mots de passe robustes (longueur, complexité)
Réponse aux incidents	- Formation courte sur le plan de réponse aux incidents (flux d'escalade, contacts DSI) - Exercice de crise (tabletop) semestriel
Conformité & charte informatique	- Signature obligatoire de la charte informatique à l'embauche et rappel annuel - Quiz de compréhension de la charte tous les ans
Risques de la supply chain logicielle	- Session dédiée aux équipes de développement : • Gouvernance des dépendances (npm, pip, etc.) ; • Vérification de la provenance des plugins et librairies tierces.

4. Résumé de l’Architecture Sécurisée Proposée

1. **Pare-feu nouvelle génération (NGFW) avec DPI en périmètre réseau :**
    - Inspection complète du trafic, filtrage applicatif et anti-malware intégré.
2. **VPN IPsec/SSL avec authentification MFA**
    - Accès distant chiffré, MFA obligatoire (OTP ou token physique) pour tous les profils administratifs et cadres.
3. **VLANs correctement isolés :**
    - VLAN Production (serveurs métiers)
    - VLAN Infra (Domain Controllers, DNS, DHCP, sauvegardes)
    - VLAN Bureautique (postes utilisateurs / Direction)
    - VLAN Développement (environnements de dev et test)
    - VLAN WEB (serveurs web, BDD Web)
    - VLAN Serveur DSI (SIEM, EDR, Radius, Auth)
4. **DMZ dédiée :**
    - Serveurs applicatifs publics (web/app) isolés du réseau interne par un segment DMZ.
    - Proxy Web placé en DMZ pour filtrage des connexions sortantes des utilisateurs.
5. **SIEM, EDR et RADIUS en place pour une supervision continue :**
    - Agents EDR sur tous les endpoints
    - Collecte centralisée dans le SIEM de toutes les sources de logs
    - Serveur RADIUS/LDAP pour l’authentification 802.1X du parc réseau.

6. **Politique d’accès “Zero Trust” pour tout composant critique :**

    - Vérification systématique de l’identité, segmentation stricte, principe du moindre privilège et authentification multi-facteur partout où nécessaire.

5. Feuille de Route (Roadmap)

Action	Responsable	Échéance	Statut
Déploiement MFA (sur VPN & consoles sensibles)	Équipe IT	2 mois	À faire
Installation de l’EDR sur tous les endpoints	Équipe IT	2 mois	À faire
Segmentation VLAN renforcée et ACL strictes	Équipe Réseau	1 mois	Planifié
Déploiement SIEM (collecte & corrélation des logs)	Consultant externe / DSI	3 mois	À faire
Lancement de la campagne de phishing simulée	RH + RSSI	1 mois	Planifié
Blocage des plugins tiers non vérifiés (GPO)	Équipe Développement	En cours	Partiel

Notes supplémentaires :

- La mise en place de l’EDR inclut la formation de l’équipe IT à l’utilisation de la console de détection et de réponse.
- La segmentation VLAN devra impérativement s’accompagner de la mise en place d’ACL sur chaque commutateur et routeur, ainsi que d’une revue de la politique de pare-feu interne.

- Le déploiement du SIEM s’appuiera sur une solution “clé en main” (on-premise ou cloud selon budget), en commençant par les logs critiques (firewall, proxy, AD).

6. Mapping aux Standards (NIST CSF / CIS Controls)

Mesure	NIST CSF Référence	CIS Control
MFA (multi-factor authentication)	PR.AC-1	6
EDR (Endpoint Detection & Response)	DE.CM-7	8
SIEM (Security Information & Event Management)	DE.CM-1	6
Formation / Sensibilisation	PR.AT-1	14
Segmentation VLAN / Cloisonnement	PR.IP-1	3

Explications :

- PR.AC-1 (NIST) : Contrôle des accès basés sur l’identification (MFA)
- DE.CM-7 (NIST) : Surveillance continue des comportements (EDR)
- DE.CM-1 (NIST) : Collecte continue des journaux (SIEM)
- PR.AT-1 (NIST) : Formation et sensibilisation aux risques cyber
- PR.IP-1 (NIST) : Définition et mise à jour des politiques de protection des données (segmentation réseau)

7. Conclusion

L’analyse conduite sur l’infrastructure de Global Solutions révèle plusieurs vulnérabilités critiques liées à la segmentation réseau, à l’absence de MFA, au manque de supervision centralisée ainsi qu’à la faible sensibilisation des utilisateurs. Les recommandations proposées (pare-feu NGFW, segmentation VLAN stricte, solution EDR, SIEM, MFA généralisé, politique de blocage des plugins non vérifiés, etc.) visent à réduire significativement la surface d’attaque, à détecter plus rapidement tout incident et à améliorer la réactivité de la DSI face aux menaces.

La feuille de route détaillée permettra de prioriser les actions en fonction du niveau de risque et de la criticité des actifs :

- Court terme (1–2 mois) : Séparation VLAN, déploiement EDR, MFA
- Moyen terme (2–3 mois) : Mise en place du SIEM, renforcement des politiques de contrôle d’accès
- Long terme (3–6 mois) : Compléter les processus de gestion de la vulnérabilité, formaliser le plan de réponse aux incidents et poursuivre la formation périodique des équipes.

En suivant ce plan d’action, Global Solutions pourra atteindre un niveau de sécurité “enterprise-grade” aligné sur les bonnes pratiques du NIST CSF et des CIS Controls, réduire les risques de compromission et assurer une meilleure résilience face aux menaces actuelles et futures.