



PCI DSS et GFI LANguard N.S.S. 8

Conditions PCI DSS	Vérification	Surveillance & Rapports	Alertes	Exécution	Remarques
Condition 1: Installer et maintenir une configuration de pare-feu pour protéger les données de propriétaires de carte					
1.3 Etablir une configuration de pare-feu pour limiter l'accès aux données de propriétaires de cartes					
1.3.9 Installer un logiciel pare-feu personnel sur les ordinateurs portables ou appartenant aux employés ayant une connectivité directe à Internet, qui sont utilisés pour accéder au réseau d'une organisation	✓	✓	●	✓	Profils et rapports de balayage de défaut
Condition 2: Ne pas utiliser de mots de passe créés par les distributeurs					
2.1 Modifier toujours les paramètres par défaut créés par les distributeurs avant d'installer un système	●	✓	●		Profils et rapports de balayage de défaut
2.2 Etablir des normes de configuration du système basées sur toutes les vulnérabilités de sécurité connues					
2.2.2 Désactiver tous les services et protocoles inutiles et non sécurisés (services et protocoles qui, dans l'immédiat, ne sont pas nécessaires pour effectuer une fonction spécifique d'un dispositif)	✓	✓	●		Profils et rapports de balayage de défaut
2.2.3 Configurer les paramètres de sécurité de système pour empêcher l'abus	✓	✓	●		Profils et rapports de balayage de défaut
2.2.4 Supprimer toute fonctionnalité inutile tels que les scripts, les pilotes, les serveurs web	✓	✓	●		Profils et rapports de balayage de défaut
Condition 5: Utiliser et régulièrement mettre à niveau les programmes et les logiciels anti-virus					
5.1 Déployer des logiciels anti-virus sur tous les systèmes communément affectés par les virus	✓	✓	●	✓	Profils et rapports de balayage de défaut
5.2 Assurer que tous les mécanismes anti-virus sont activés et fonctionnent correctement	✓	✓	●	✓	Profils et rapports de balayage de défaut
Condition 6: Etablir et maintenir des systèmes et des applications sécurisés					
6.1 Assurer que les plus récentes patches de sécurité sont installées pour tous les composants des systèmes et les logiciels	✓	✓	●	✓	Profils et rapports de balayage de défaut
6.2 Etablir un processus d'identification des vulnérabilités de sécurité récemment découvertes	✓	✓	●	✓	Programmer les audits de réseau
6.4 Suivre des procédures de contrôle de toute modification de configuration des systèmes et des logiciels					
6.4.3 Tester que les fonctionnalités sont opérationnelles	✓	✓	●	✓	Roulement en arrière pour les patches
6.5 Développer toutes les applications web selon des critères de programmation privilégiant la sécurité	✓	✓	●		Vérification de vulnérabilité sous OVAL
6.6 Assurer que les applications d'interface avec le web sont protégées contre les attaques connues en installant une application de pare-feu	✓	✓	●	✓	Profils et rapports de balayage de défaut
Condition 8: Assigner une identification unique à chaque personne ayant l'accès par ordinateur					
8.2 Assigner des identifications et des mots de passe uniques	✓	✓	●		Profils et rapports de balayage de défaut
8.5 Assurer l'authentification et la gestion appropriées d'utilisateur et de mots de passe					
8.5.3 Assigner aux utilisateurs un mot de passe unique d'accès qui est modifié après le premier usage	●	●	●		Profils et rapports de balayage de défaut
8.5.5 Supprimer les comptes d'utilisateur inactifs, au moins tous les 90 jours	●	●	●		Profils et rapports de balayage de défaut
8.5.6 Activer seulement au besoin, les comptes utilisés par les distributeurs pour l'entretien à distance	●	●	●		Profils et rapports de balayage de défaut

Conditions PCI DSS	Vérification	Surveillance & Rapports	Alertes	Exécution	Remarques
8.5.9 Changer les mots de passe d'utilisateur au moins tous les 90 jours	✓	✓	●		Profils et rapports de balayage de défaut
8.5.10 Exiger une longueur minimum de mot de passe d'au moins sept caractères	✓	✓	●		Profils et rapports de balayage de défaut
Condition 10: Traquer et surveiller tous les accès aux ressources de réseau et aux données de propriétaires de carte					
10.4 Synchroniser toutes les principales horloges et l'heure du système	✓	✓	●		Profils et rapports de balayage de défaut
Condition 11: Tester régulièrement la sécurité des systèmes et les processus					
11.1 Tester chaque année les fonctions de sécurité, les restrictions, les connexions au réseau pour assurer la capacité d'identifier adéquatement et d'arrêter toutes tentatives d'accès non autorisé	✓	✓	●	✓	Programmer les audits de réseau
11.2 Effectuer des balayages internes de vulnérabilités de réseau au moins une fois par trimestre	✓	✓	●	✓	Programmer les audits de réseau
11.4 Utiliser des systèmes de détection et de prévention d'intrusion au sein de tout le réseau et sur les machines hôtes pour surveiller le trafic et alerter les responsables en cas de menaces	✓	✓	●		Profils et rapports de balayage de défaut
11.5 Déployer un logiciel de contrôle de l'intégrité des fichiers pour envoyer des alertes en cas de modifications non autorisées du système central ou du contenu des fichiers	✓	✓	●	✓	Profils et rapports de balayage de défaut

Légende

- ✓ Conditions entièrement supportées
- Condition supportée partiellement grâce aux rapports ou à une adaptation du produit. Certaines conditions pourraient s'appliquer.

REMARQUE: Les conditions applicables incluent mais ne sont pas limitées à :

- Windows Security Settings, tels que 'Password Policy' et 'Audit Policy'
- Paramétrages de compte utilisateur
- Installation et configuration appropriée d'autres logiciels et dispositifs, tels que des pare-feu

