Comment Rapid7 répond aux

40 règles d'hygiène informatique de l'ANSSI

Selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI), de nombreuses attaques informatiques auraient pu être évitées si des mesures de base avaient été appliquées. Le guide des 40 règles d'hygiène a été développé pour aider les organisations à mettre en œuvre les règles de sécurité essentielles, afin de protéger leurs systèmes d'information. Les solutions de cybersécurité de Rapid7 peuvent vous aider à appliquer et surveiller la bonne exécution de ces règles et ainsi diminuer le risque d'attaque.

I – CONNAÎTRE LE SYSTÈME D'INFORMATION ET SES UTILISATEURS

	Mesure essentielle	Comment Rapid7 y répond
Règle 1	Disposer d'une cartographie précise du système d'information et la maintenir à jour.	• Nexpose scrute le réseau pour identifier tous les équipements et leurs adresses IP, et effectue un inventaire du système d'information, et des logiciels installés sur chaque équipement.
Règle 2	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour.	• UserInsight permet de voir tous les comptes administrateur et autres comptes à privilèges sur le réseau, sur les équipements en local et dans les applications Cloud de l'entreprise.
Règle 3	Rédiger et appliquer des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaires, etc.).	• UserInsight fournit de la visibilité sur tous les comptes utilisateur actifs, et alerte lorsque les utilisateurs tentent d'accéder aux applications Cloud de l'entreprise.

II – MAÎTRISER LE RÉSEAU

	Mesure essentielle	Comment Rapid7 y répond
Règle 4	Limiter le nombre d'accès à Internet de l'entreprise au strict nécessaire.	• Nexpose scanne le réseau pour recenser tous les équipements et leurs adresses IP, y compris les points d'accès à Internet.
Règle 5	Interdire la connexion d'équipements personnels au système d'information de l'organisation.	• Nexpose détecte automatiquement les périphériques mobiles connectés au serveur Exchange ActiveSync de l'entreprise. • UserInsight identifie tous les périphériques mobiles qui accèdent au réseau, y compris le lieu et l'heure du dernier accès.

III – METTRE À NIVEAU LES LOGICIELS

	Mesure essentielle	Comment Rapid7 y répond
Règle 6	Connaître les modalités de mise à jour de l'ensemble des composants logiciels utilisés et se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.	• Nexpose scrute automatiquement tous les équipements du réseau pour identifier les vulnérabilités logicielles en les priorisant selon le niveau de risque.
Règle 7	Définir une politique de mise à jour et l'appliquer.	• Nexpose génère et édite automatiquement des reporting avec des instructions précises pour remédier aux vulnérabilités identifiées.

IV – AUTHENTIFIER L'UTILISATEUR

	Mesure essentielle	Comment Rapid7 y répond
Règle 8	Identifier nommément chaque individu ayant accès au système d'information.	• UserInsight offre une visibilité sur tous les comptes de l'entreprise, y compris ceux attachés au nom de domaine, en local et aux applications Cloud.
Règle 9	Définir des règles de choix et de dimensionnement des mots de passe.	• Nexpose offre la possibilité de complexifier les mots de passe du système si ceux-ci se révèlent faibles, avec une longueur et un type de caractères requis.
Règle 10	Mettre en place des moyens techniques permettant de faire respecter les règles relatives à l'authentification.	• Metasploit teste la force du mot de passe grâce à des attaques en ligne par force-brute, des techniques de hacking hors connexion et des contrôles de la qualité des mots de passe requise.
Règle 12	Renouveler systématiquement les éléments d'authentification par défaut (mots de passe, certificats) sur les équipements (commutateurs réseau, routeurs, serveurs, imprimantes).	• Nexpose scanne le réseau pour détecter les équipements qui ne respectent pas le niveau de sécurité requis.

V – SÉCURISER LES POSTES DE TRAVAIL

	Mesure essentielle	Comment Rapid7 y répond
Règle 14	Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique.	• Nexpose scrute automatiquement tous les équipements sur le réseau pour vérifier la conformité avec les règles de sécurité définies.
Règle 15	Interdire techniquement la connexion des supports amovibles, sauf si cela est indispensable ; désactiver l'exécution des fichiers de démarrage automatique depuis de tels supports.	• Nexpose permet de savoir si l'exécution automatique est activée sur les systèmes.
Règle 17	Gérer les terminaux nomades selon une politique de sécurité au moins aussi stricte que celle des postes fixes.	• Nexpose scanne automatiquement tous les équipements sur le réseau pour vérifier la conformité avec les règles de sécurité définies.

VI – SÉCURISER L'INTÉRIEUR DU RÉSEAU

	Mesure essentielle	Comment Rapid7 y répond
Règle 21	Mettre en place des réseaux cloisonnés. Pour les postes ou les serveurs contenant des informations importantes pour l'entreprise, créer un sous-réseau protégé par une passerelle d'interconnexion spécifique.	• Metasploit rend les tâches de tests de segmentation du réseau opérationnelles et efficaces. • UserInsight permet de configurer des zones et des politiques d'accès utilisateur, et d'alerter en cas de non respect des règles.
Règle 22	Éviter l'usage d'infrastructures sans fil (Wifi). Si l'usage de ces technologies ne peut être évité, cloisonner le réseau d'accès Wifi du reste du système d'information.	• Metasploit rend les tâches de tests de segmentation du réseau opérationnelles et efficaces. • UserInsight permet de configurer des zones et des politiques d'accès utilisateur, et d'alerter en cas de non respect des règles.
Règle 23	Utiliser systématiquement des applications et des protocoles sécurisés.	• AppSpider scanne et teste les applications web en temps réel pour identifier les vulnérabilités et les risques.

VIII – SURVEILLER LES SYSTÈMES

	Mesure essentielle	Comment Rapid7 y répond
Règle 26	Définir concrètement les objectifs de la supervision des systèmes et des réseaux.	• UserInsight surveille l'activité du réseau et alerte sur les incidents tels que les accès utilisateur inhabituels, les tentatives d'authentification par force-brute, et les tentatives de connexion à partir d'un compte désactivé.
Règle 27	Définir les modalités d'analyse des événements journalisés.	• UserInsight collecte les logs, corrèle les événements par utilisateur, machine et adresse IP et tire parti de l'analyse de sécurité en se basant sur l'apprentissage automatique (machine learning) pour détecter les comportements de hacker.

XI – ORGANISER LA RÉACTION EN CAS D'INCIDENT

	Mesure essentielle	Comment Rapid7 y répond
Règle 36	Disposer d'un plan de reprise et de continuité d'activité informatique, même sommaire, en décrivant comment sauvegarder les données essentielles de l'entreprise et le tenir régulièrement à jour.	• Rapid7 peut fournir la situation à l'instant T de l'entreprise face à la menace et accompagne les entreprises dans leur plan de réponse aux incidents, et leur plan de reprise et de continuité d'activité (PRA/PCA).
Règle 37	Mettre en place des procédés et prévenir tous les interlocuteurs concernés en cas d'attaque.	• Rapid7 peut fournir la situation à l'instant T de l'entreprise face à la menace et accompagne les entreprises dans leur plan de réponse aux incidents.
Règle 38	Ne jamais se contenter de traiter l'infection d'une machine sans tenter de savoir comment le code malveillant a pu pénétrer, s'il a pu se propager ailleurs dans le réseau et quelles données ont été touchées.	• UserInsight simplifie la recherche d'incidents grâce à une interface de recherche visuelle pour rapidement déterminer quelle(s) machine(s) ou quel(s) utilisateur(s) a/ont été compromis. • Rapid7 accompagne les entreprises dans toutes les étapes de la réponse aux incidents, de l'analyse à la remédiation et passant par la détection.

XII – SENSIBILISER

	Mesure essentielle	Comment Rapid7 y répond
Règle 39	Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires.	• Rapid7 offre des modules de formation aux principes de sécurité personnalisables et en ligne.

XIII – FAIRE AUDITER LA SÉCURITÉ DU SYSTEME D'INFORMATION

	Mesure essentielle	Comment Rapid7 y répond
Règle 40	Faire réaliser des audits de sécurité périodiques (au minimum tous les ans). Chaque audit doit être associé à un plan d'action dont la mise en œuvre est suivie au plus haut niveau.	• Rapid7 peut fournir la situation à l'instant T de l'entreprise face à la menace et accompagne les entreprises dans leur plan de réponse aux incidents, et leur plan de reprise et de continuité d'activité (PRA/PCA).

A propos de Rapid7

Rapid7 est un éditeur majeur de solutions de sécurité analytique des données qui permettent aux entreprises de mettre en œuvre une approche active de la cyber sécurité. Les solutions de Rapid7 permettent aux entreprises de prévenir les attaques en fournissant une visibilité sur les vulnérabilités et de détecter rapidement les compromissions de sécurité, d'évaluer les violations et de corriger les causes sous-jacentes des attaques. Rapid7 a gagné la confiance de plus de 4150 entreprises dans 90 pays, dont 34% du Fortune 1000. Pour en savoir plus: www.rapid7.com.