



Principe

Vous souhaitez :

- ... avoir la meilleure garantie que le système d'information de votre entreprise est sécurisé.
- ... être informé en permanence et dans les meilleurs délais sur les risques de sécurité **concernant votre environnement**.
- ... avoir l'assurance de n'avoir omis aucune faille critique dans votre système d'information.

Le moteur de veille sécuritaire Ariane® analyse 24/24h et 7/7j les nouvelles failles publiées sur différentes sources Internet (mailing lists, forums, sites web...). Dès qu'une faille est publiée et qu'elle concerne **votre système d'information** (serveurs, routeurs, firewalls, équipements réseau...) : une alerte est émise, validée par un expert sécurité, enrichie de **commentaires propres à votre configuration, hiérarchisée en niveaux de dangerosité**, et enfin transmise par le média de votre choix (mail, sms, fax...) aux personnes responsables des machines ou applications concernées.

Vous êtes ainsi prévenus dans les meilleurs délais et pouvez donc sécuriser votre système d'information avant que les hackers ne s'introduisent dans votre réseau.

Enjeux

Un audit de sécurité reflète la sécurité d'un système d'information à un instant T. Si, par exemple, le jour de l'audit aucune faille n'est référencée sur votre serveur mail, votre système peut être considéré comme sûr; Mais si une faille est publiée le lendemain sur ce même serveur mail ?

Toutes les entreprises sont concernées par les risques liés à la sécurité informatique, mais les responsables sécurité n'ont pas forcément le temps de surveiller les mailing lists et les sites dédiés à la sécurité 24/24h.

La sécurité d'un système repose sur la solidité de son maillon le plus faible. Comment être sûr de ne pas avoir oublié de prendre en compte ce dernier ?

Name	Description	Application	Date	Change
MS06-022 - Microsoft Windows TCP/IP Remote Command Execution Vulnerability (917953)	- Microsoft Windows 2000 Professional Standard - Microsoft Windows 2000 Professional Server Standard - Microsoft Windows XP Professional Standard - Microsoft Windows XP Home Edition Standard - Microsoft Windows 2003 Standard		2006-06-13 22:26:44	
MS06-030 - Microsoft Windows SMB Protocol Execution and Denial of Service Vulnerability (914388)	- Microsoft Windows 2000 Professional Standard - Microsoft Windows 2000 Advanced Server Standard - Microsoft Windows XP Professional Standard - Microsoft Windows XP Home Edition Standard - Microsoft Windows 2003 Standard		2006-06-13 22:23:24	
MS06-023 - Microsoft Windows Remote Command Execution Vulnerability (917346)	- Microsoft Windows 2000 Professional Standard - Microsoft Windows 2000 Advanced Server Standard - Microsoft Windows XP Professional Standard - Microsoft Windows XP Home Edition Standard - Microsoft Windows 2003 Standard		2006-06-13 22:18:44	
MS06-022 - Microsoft Windows ART	- Microsoft Windows XP Professional Standard - Microsoft Windows XP Home Edition Standard		2006-06-13	

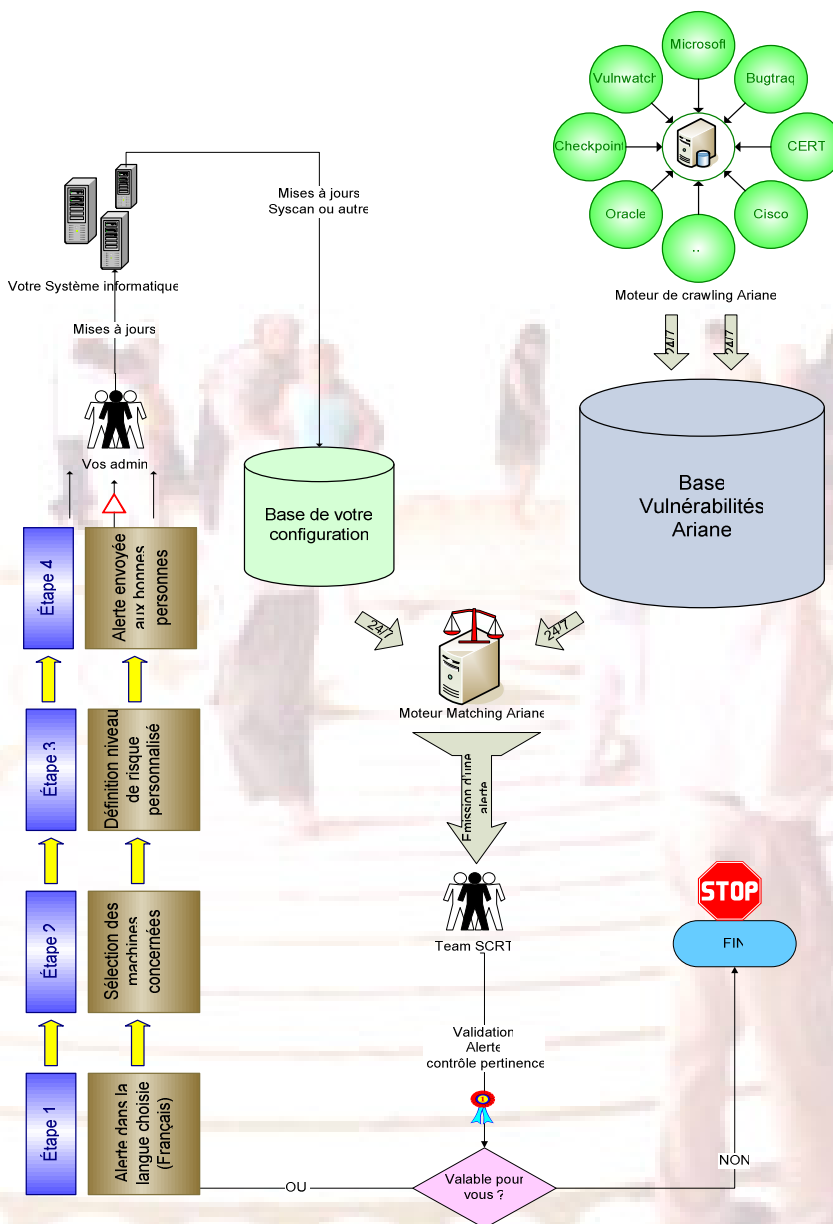
Méthodologie

La mise en place du système de veille sécuritaire Ariane s'articule autour des étapes suivantes :

1. **Définition** avec nos spécialistes sécurité des **points critiques de votre système d'information** afin de bien cerner le périmètre d'action de notre moteur.
2. Nos spécialistes audient la configuration et les paramètres des équipements concernés
3. Votre configuration est **analysée, modélisée** et entrée dans le moteur de matching. Chaque machine ou groupe de machines est affecté à une personne (ou groupe de personnes) de votre entreprise (interlocuteurs responsables en cas d'alerte).
4. Emission d'un **premier rapport visant à corriger les failles déjà existantes** afin de démarrer sur des bases saines
5. Démarrage de la surveillance : le moteur Ariane **analyse 24/24h et 7 jours sur 7** les nouvelles vulnérabilités publiées.
6. **Chaque fois** qu'une nouvelle faille est publiée, le moteur Ariane analyse cette vulnérabilité.
7. Si cette nouvelle faille **vous concerne**: une alerte est immédiatement gérée, vérifiée et complétée de conseils par nos spécialistes sécurité. Dans un délai contractuel et garanti, cette alerte est ensuite communiquée aux personnes concernées dans votre entreprise.
8. Mise en application de la solution préconisée: par vos équipes dédiées ou par l'intervention de l'un de nos spécialistes. Les données surveillées par le moteur Ariane sont ensuite mises à jour (syscan, ou autre solution d'inventaire).
9. Bilan et rapport trimestriel présentant : les failles publiées, les machines concernées, les failles corrigées, les failles en attente d'être corrigées, les statistiques...



LE PROCESSUS DE VEILLE SECURITAIRE ARIANE



Contact :

SCRT

Votre revendeur Ariane :

Le tres 6
1028 Préverenges
SUISSE
Tel : +41 21 802 64 01
Fax : +41 21 802 64 02
Mail : info@scrt.ch