

ITrust Security Metrics : le label sécurité

ITrust
IT Security Services

26 Septembre 2011

Label sécurité ITrust : *ITrust Security Metrics*

ITrust
Security Metrics
Level 2+ compliant

Objet : Ce document présente le label de sécurité ITrust et formalise les conditions générales d'utilisation et de vente du label.

En 2011, le piratage informatique est devenu une actualité brulante, révélée au grand jour avec les piratages successifs de grandes entreprises et d'institutions gouvernementales dans le monde entier. Les entreprises prennent désormais conscience que la sécurité de leur système informatique est une réalité à prendre en compte...

Parallèlement à ce constat, les experts en sécurité dressent un autre bilan : une grande partie des attaques informatiques pourraient être évitées si les bonnes pratiques dites de "bon sens" étaient systématiquement mises en place.

Dans ce contexte, ITrust a décidé de réagir en créant le label sécurité ***ITrust Security Metrics****.*

1. Sécurisez vos Sites Web et Réseaux, Rassurez vos clients

La délégation des moyens informatiques à un tiers (par exemple : la migration vers le Cloud), entraine une perte de contrôle du système d'information et une augmentation des risques liés à la centralisation des données.

L'enjeu dans le cloud et l'informatique étendue et distribuée pour le client est de pouvoir maitriser ses données externalisées par le contrôle des SLA et qualité de service, de la confidentialité et l'intégrité de ses données.

Le tout dans un contexte de conformité réglementaire important : CNIL, E-Privacy, DMP, HDS, SoX, Bale III, PCI, ISO 2700X/27001, HIPAA, SAS70.

ITrust Security Metrics est un service proposé par ITrust pour établir de manière indépendante le niveau de sécurité d'une architecture suivant des critères et objectifs basés sur des normes internationales.

Le principe est de scanner, grâce à IKare, les sites Web et/ou réseaux de l'entreprise, afin de détecter failles et vulnérabilités et de mener conjointement une politique sécurité, grâce l'accompagnement des Ingénieurs sécurité ITrust.

Un label est alors généré et affiché sur le site web de l'entreprise afin de prouver à ses clients les efforts rigoureux qu'elle entreprend pour maintenir un niveau de sécurité maximal.

2. Les Avantages

- Identification des vulnérabilités
- Supervision de l'application des mises à jour systèmes

- Vérification des contrôles de sécurité et d'intégrité
- Reporting détaillé avec la solution IKare
- Réalisation de scans « à la demande » pour s'assurer de la correction
- Traçabilité des corrections effectuées
- Accompagnement organisationnel par des Ingénieurs spécialisés en Sécurité
- Rassurement de vos clients sur vos efforts pour maintenir un niveau de sécurité maximal.

3. Description du label

S'appuyant d'une part sur la solution logicielle SaaS, IKare (Monitoring de sécurité développé par ITrust, labellisé par Oséo), pour les scans de vulnérabilités et les contrôles de sécurité et d'autre part sur les normes ISO 27001 et 27002 pour les bonnes pratiques en termes de gestion.

Le label *ITrust Security Metrics* garantit que le système d'information est configuré et exploité selon les meilleures pratiques de sécurité et conforme aux réglementations et l'état de l'art.

ITrust Security Metrics est décliné en quatre niveaux de certification :

Critères / Exigences	Niveau 1	Niveau 2	Niveau 2+	Niveau 3	Niveau 4
Scan de Vulnérabilités via IKare	1/semaine	2/semaine	2/semaine	1/jour	1/jour
Contrôle de sécurité via IKare	2/semaine	1/jour	1/jour	2/jour	2/jour
Délais de correction des vulnérabilités	1 semaine	3 jours	3 jours	48H	24H
Sécurité physique			√	√	√
Gestion des actifs			√	√	√
Gestion des communications et des opérations			√	√	√
Contrôle d'accès				√	√
Gestion des incidents				√	√
Politique de sécurité				√	√
Organisation de la fonction sécurité				√	√
Ressources humaines				√	√
Reprise et continuité d'activité				√	√
Conformité				√	√
Accréditation client ISO 27001					√
	En savoir plus	En savoir plus	En savoir plus	En savoir plus	En savoir plus

IKare

Technique

Organisationnel

4. A qui est destiné le label ITrust Security Metrics

Le label *ITrust Security Metrics* est proposé aux Editeurs, aux Hébergeurs de données et d'applications, aux Cloud Providers afin de valoriser leurs processus et la qualité de leurs prestations.

5. Description de chaque niveau

S'appuyant d'un coté sur la solution IKare pour les scans de vulnérabilités et les contrôles de sécurité et de l'autre sur la norme iso 27001/2 pour les bonnes pratiques en terme de gestion, le label ITrust Security Metrics offre une vision globale de la sécurité…

ITrust Security Metrics propose quatre niveaux de certification :

Niveau 1 :

Un scan de vulnérabilité est effectué au moins une fois par semaine

Un contrôle de sécurité est effectué au moins deux fois par semaine.

Engagement :

- L'utilisateur s'engage à corriger les vulnérabilités critiques et hautes dans la semaine qui suit la découverte.
- En cas de non respect de cet engagement, un label vide est affiché en lieu et place du label niveau 1 sur le site tant que la correction n'a pas été apportée.

Niveau 2 :

Un scan de vulnérabilité est effectué au moins deux fois par semaine

Un contrôle de sécurité est effectué au moins une fois par jour.

Engagement :

- L'utilisateur s'engage à corriger les vulnérabilités critiques et hautes dans les 3 jours qui suivent la découverte.
- En cas de non respect de cet engagement, le label est « rétrogradé » vers le niveau 1 puis le label « vide » si rien n'est fait dans les délais impartis.

Niveau 2+ :

Ce niveau répond aux mêmes exigences que celles du niveau 2 avec en plus les exigences issues des bonnes pratiques iso 27002 sur les thèmes de :

- La sécurité physique
- La gestion des actifs
- La gestion des communications et des opérations.

Niveau 3 :

Un scan de vulnérabilité est effectué au moins une fois par jour

Un contrôle de sécurité est effectué au moins deux fois par jour.

Ce niveau reprend les exigences organisationnelles du niveau 2+ en y ajoutant les thèmes suivants :

- contrôle d'accès
- gestion des incidents
- politique de sécurité
- organisation de la fonction sécurité
- conformité.

Engagement :

- L'utilisateur s'engage à corriger les vulnérabilités critiques et hautes dans les 48H qui suivent la découverte.
- En cas de non respect de cet engagement, le label est « rétrogradé » vers le niveau 2.

Niveau 4 :

Un scan de vulnérabilité est effectué au moins une fois par jour

Un contrôle de sécurité est effectué au moins deux fois par jour.

Le périmètre supervisé par le label est conforme à la norme iso 27001.

Engagement :

- L'utilisateur s'engage à corriger les vulnérabilités critiques et hautes dans les 24H qui suivent la découverte.
- En cas de non respect de cet engagement, le label est « rétrogradé » vers le niveau 3.

6. Fonctionnement

L'installation nécessite l'ajout d'un lien HTML sur le site institutionnel du client. Celui ci affiche le niveau du label de la cible et redirige sur une page spécifique à la cible sur le site ITrust qui liste les éléments de sécurité implémentés.

Le label nécessite l'installation du service IKare au sein de la cible pour effectuer les scans de vulnérabilités et les contrôles de sécurité. ITrust devra pouvoir accéder au service IKare afin d'examiner les rapports et obtenir les dernières dates de scans (affichées sur la page spécifique du label)

A partir du niveau 2+, ITrust accompagne le client à raison d'un jour par mois pour valider et améliorer les exigences organisationnelles.

7. Liste des critères

Critères / Exigences	Moyens
Sécurité physique	
Restriction de l'accès physique	• Salle dédiée avec contrôle d'accès • Armoire verrouillée
Protection contre les risques environnementaux	• Alarmes • Site distant de secours • Protection incendie • Climatisation
Protection contre les problèmes électriques	• Alimentation redondée • Onduleur
Gestion des actifs	
Inventaire matériel et logiciel	
Identification des propriétaires des ressources	
Classification des ressources en fonction du besoin de sécurité	
Gestion des communications et des opérations	
Sauvegarde / restauration	
Gestion des journaux	
Gestion des mises à jour	
Supervision de sécurité (assuré par les exigences de niveau 2)	
Ségrégation réseau	
Protection des communications externes	• Authentification forte • VPN
Traçabilité	• Correction et changement • Responsabilités
Contrôle d'intégrité	
Gestion des prestations de service tierces	
Contrôle d'accès	
Politique de contrôle d'accès	
Cycle de vie des accès	• Enregistrement initial • Politique de mots de passes • Audit des droits d'accès • Suppression des droits
Accès réseau	• Ségrégation réseau utilisateur / système • Authentification utilisateur externe • Journalisation firewall

Accès système	• Identifiant unique / utilisateur • Journalisation des accès
Gestion des incidents	
Reporting	• Procédure d'alarme et réaction (escalade) • Point de contact unique
Gestion des journaux	• Audit • Collecte (forensique)
Politique de sécurité	
Politique de sécurité de l'information	
Guidelines	
Procédures	
Organisation de la fonction sécurité	
RSSI	
Sécurité contractuelle avec les tiers accédant au système	
Ressources humaines	
Prise en compte du besoin de sécurité	
Procédures de sensibilisation et formation	
Procédure de départ	
Reprise et continuité d'activité	
Procédure de PCA/PRA	
Test et validation	
Conformité	
Respect des règlementations et lois	• CNIL • PCI DSS • Package Telecom…
Respect des procédures de la politique	
Efficacité des dispositifs : Pentest, audit de configuration…	
Accréditation ISO 27001	

8. Conditions générales de vente et d'utilisation

Les conditions de vente seront où ont été transmises dans une proposition Technique et Financière.

Le client reconnait avoir pris connaissance des conditions ci-dessus explicitées.

Il s'engage à respecter les délais de correction des failles de sécurité.

Toute condition non respectée fera l'objet d'une rétrogradation du niveau à un niveau inférieur.

Le client et ITrust ont le droit de communiquer sur le label.

Le client se doit de conserver le logo du label sur son site et ses produits.

ITrust s'autorise à communiquer sur les clients qui utilisent son label.

BON POUR ACCORD

J'accepte et comprends le principe et les conditions du label *ITrust Security Metrics* explicités ci-dessus.

Signature et date du Client et Bon pour accord pour mise en place du label

ITrust IT Security Services

Immeuble Actys 1
55 Avenue l'Occitane BP 67303
31673 Labège Cedex
Tél. : 05.67.34.67.80

contact@itrust.fr
www.itrust.fr
www.ikare-monitoring.com

Rejoignez-nous sur nos pages et groupes officiels.