protiviti®
Global Business Consulting

Urbanisation des activités du RSSI

Travail à distance, cyber attaque, guerre asymétrique, fuite de données : les enjeux de la cyber sécurité sont de plus en plus importants. Certes, les investissements au sein des entreprises sont réels mais les attentes du management et des parties prenantes internes et externes sont de plus en plus présentes et les réponses attendues pour les actifs clé se doivent d'être relativement binaires, c'est-à-dire sous contrôle ou non.

Pour répondre à ces enjeux, le responsable de la Sécurité des Systèmes d'Information (RSSI) se doit de mettre en place des organisations, des processus et des outils de plus en plus sophistiqués et donc plus complexes à mettre en cohérence.

En outre, les réglementations, comme la RGPD, demandent aussi une réactivité accrue de l'entreprise dans sa déclaration des incidents et sa capacité plus générale à « rendre compte". Dans certains cas, cela demande des dispositifs dédiés et une grande coordination en interne entre différents départements de l'entreprise (CDO, DPO, CRO, CAO, CCO, …[1]). Aussi, il est nécessaire de penser et d'appréhender les processus de bout en bout pour leur meilleure intégration.

La rationalisation et l'automatisation des différents dispositifs de gestion de la sécurité et des risques IT devient une obligation quasi incontournable. Il est très difficile d'avoir une vue d'ensemble tant les équipes ont souvent tendance à adresser les sujets en silo avec des outillages spécialisés et/ou « bureautique », souvent au motif d'une plus grande efficacité à court terme.

Pour adresser ces enjeux, il est primordial d'avoir des référentiels partagés (organisation, CMDB, référentiels projet, référentiels des fournisseurs, …). Il faut aussi définir des taxonomies et des méthodologies communes (univers des risques, matrice de risque, …). Le RSSI doit avoir une vision à long terme de sorte à donner de la cohérence au niveau de l'organisation cible, des processus et des technologies à mettre en œuvre.

[1] Chief Data Officer, Data Protection Officer, Chef Risk Officer, Chief Audit Officer, Chief Compliance Officer, ...

Thèmes clés adressés par le RSSI

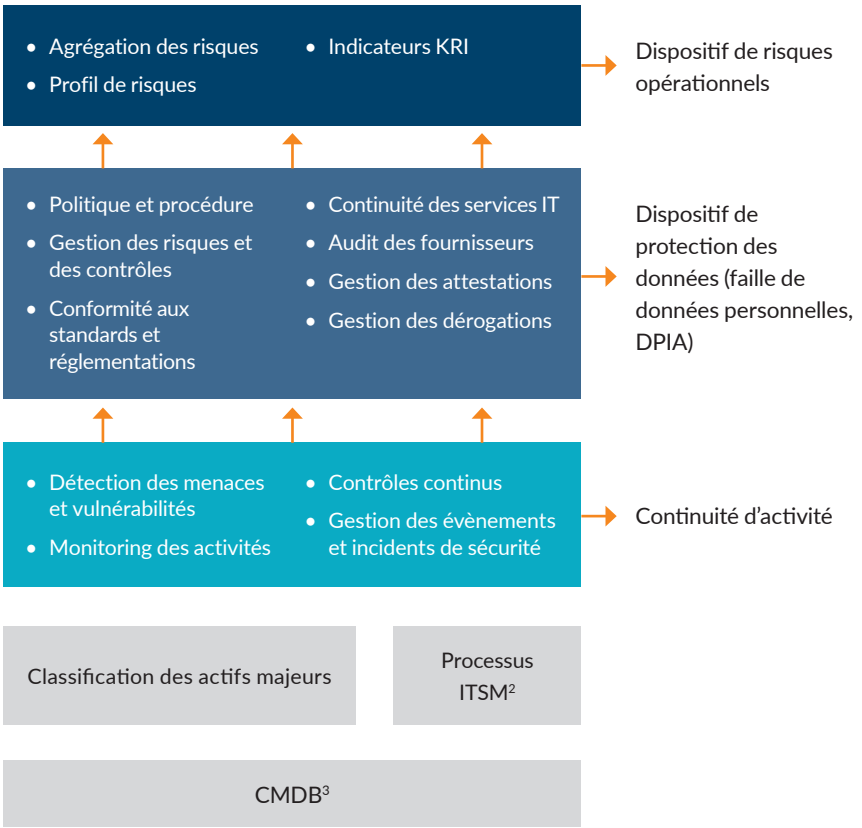
- Gestion des politiques et des procédures, définissant les pratiques de cyber sécurité à respecter ; lien entre ces politiques et les standards & réglementations
- Gestion des risques et des contrôles dans les patrimoines et les projets
- Gestion des recommandations de l'audit interne ou des régulateurs
- Gestion des indicateurs de sécurité avec seuils d'alerte
- Gestions de référentiels et des réglementations, tels que NIST, PCI-DSS, gestion des certifications
- Gestion des dérogations
- Classification des systèmes et des données
- Sécurité opérationnelle, comme
  - La détection et le traitement des vulnérabilités
  - La qualification et le traitement des évènements et incidents de sécurité
  - Anonymisation/encryptage des données en dynamique

Ces éléments pourraient s'articuler selon l'architecture suivante :

Référentiels d'entreprise (organisation, application, projet, fournisseurs, contrats, CMDB, ...)

Source de données (réglementations, bibliothèque des risques, processus, situations shadow & light IT, usages cloud..)

Catalogue de données



[2] IT Service Management

[3] Configuration management database

L'enjeu est d'éviter les silos entre les différents experts de sécurité (CSIRT, Sécurité applicative, Pentesters, auditeurs, …) et d'impliquer les métiers via notamment les responsables d'application.

Une vision consolidée au niveau de l'actif (l'application, le contrat, l'entité, le projet, la data …) permet aux intervenants concernés de consulter les informations et d'être acteur à son niveau.

Pour cela, il est crucial de :

- Comprendre l'ensemble des usages
- Construire et unifier un modèle de données permettant de structurer et consolider l'information au sein de l'entreprise.
- Via les outils de reporting, être capable d'adresser les besoins de décision à chaque niveau de l'organisation
- Impliquer les opérationnels via une intégration avec des outils collaboratifs existants dans l'entreprise pour que l'impact du changement soit minimal

Protiviti peut vous aider sur les différentes composantes de la démarche :

- Définition de Business case permettant de valider un investissement (Quels cas d'usage pour quels périmètres ? Quelle Gouvernance ? Quels gains, quel ROI ?)
- Définition de la roadmap à moyen terme (1–2 ans). Définition de la vision produit, séquencement de la mise en œuvre dans le temps en préservant un data model cohérent
- Standardisation/homogénéisation des processus, des méthodologies et des procédures pour intégrer la mise en place des technologies dans les pratiques opérationnelles
- Appui sur la sélection d'outils et/ou des intégrateurs
- Gestion de projet
- Accompagnement au changement. Intégration des nouvelles technologies dans les pratiques opérationnelles.

Nos atouts :

Expérience dans la réalisation de projets de transformation

Indépendance vis-à-vis des éditeurs

Expertise sur la maitrise d'ouvrage

Contact

Bernard Drui
Country Market Leader
+33.1.42.96.41.11
bernard.drui@protiviti.fr

Alexandre Roset
Associate Director
+33.6.77.77.97.52
alexandre.roset@protiviti.fr