Utilisation du SOC REVEELIUM
dans le cadre de la
Réglementation Générale
sur la Protection des Données

Introduction :

Le règlement européen 2016/679 du 27 avril 2016 (dit « règlement général sur la protection des données » ou RGPD) précise que la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (article 32).
La CNIL reste en charge du contrôle de la bonne mise en application de la réglementation par les entreprises qui encourent, à défaut de conformité, des amendes pécunières lourdes.

Ainsi la liste des dispositions à prendre, tant techniques qu'organisationnelles, peut être mise en œuvre, contrôlée et justifiée dans le cadre de la mise en place du SOC REVEELIUM d'ITRUST.

Le SOC REVEELIUM inclut des outils et des technologies informatiques qui permettent de collecter tous types de journaux informatisés, de centraliser les alertes de sécurité dans un SIEM (Security Information Event Management) , de détecter les vulnérabilités de sécurité et de détecter les attaques avancées ou les comportements anormaux dans le système d'information.

Les guides de procédures d'utilisation, de supervision, de contrôle et d'intervention mis en œuvre avec le SOC, viennent compléter la dimension technique pour offrir une couverture essentielle des obligations légales liées à la RGPD.

Rappel des grandes lignes reliant la RGPD et le SOC Itrust :

Pour mémoire, la CNIL recense 17 points différents exposés sous forme de fiches CNIL reliant la RGPD et la sécurité informatique.

Parmi ces sujets nous retrouverons notamment des dispositions obligatoires qui sont couvertes par l'utilisation du SOC d'Itrust :

- **Authentifier les utilisateurs (Réf. CNIL RGPD fiches 2 et 3)**

Pour assurer qu'un utilisateur accède uniquement aux données dont il a besoin, il doit être doté d'un identifiant qui lui est propre et doit s'authentifier avant toute utilisation des moyens

informatiques. Les mécanismes permettant de réaliser l'authentification des personnes sont catégorisés selon l'accès aux différents moyens informatiques de l'entreprise qui doit contrôler les accès et assurer la traçabilité des tentatives d'accès, que celles-ci soient réussis ou en échec.

Le SOC permet par exemple de suivre les activités d'accès aux ressources du système d'information, tant au travers des Active-Directory que des alertes d'échecs de connections suspectes.
Le SOC suit les recommandations de base de la CNIL dans le suivi des authentifications fortes, des limites de nombre de tentatives d'accès, du suivi de la politique de changement de mot de passe, changement de privilèges d'un utilisateur, règles d'authentification, vérification des bonnes règles de cryptage, remontée d'alerte en cas de violation des règles définies.

- **Tracer les accès et Gérer les incidents de sécurité (Réf. CNIL RGPD fiche 4)**

Le Soc répond directement à la recommandation légale qui précise l'obligation de :

« Journaliser les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité). »

Le SOC d'Itrust permet d'identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques dans un soucis de traçabilité. Pour ce faire, un dispositif de gestion des traces et des incidents est mis en place permettant d'assurer la supervision des alertes de sécurité dites classiques ainsi que la gestion alertes de sécurité dites 'originales' grâce à Reveelium qui permettra de détecter les possibles attaques informatiques non encore répertoriées.

Suivant directement les recommandations de la CNIL sur l'application de la RGPD, le SOC d'Itrust permettra notamment :

De disposer d'un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité :
Ces journaux doivent conserver les évènements de sécurité sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important) ;

La journalisation doit concerner, au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ; dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné. Toutes les alertes de sécurité doivent être journalisées ce qui implique qu'il faudra idéalement journaliser tous les équipements du réseau informatique.

La protection des équipements de journalisation et des informations journalisées contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée fait également partie du SOC Itrust qui possède son propre système de cyber sécurité avec un chiffrement des données collectées, transmises, analysées et archivées.

Le SOC permet de notifier dans les plus brefs délais toute anomalie ou tout incident de sécurité au responsable de traitement, ceci conformément à la réglementation.

- **Sécuriser les postes de travail et l'informatique mobile (Réf. CNIL- RGPD fiche 5)**

Au-delà de l'utilisation recommandée des antivirus régulièrement mis à jour et de la prévision d'une politique de mise à jour régulière des logiciels, le scanner de vulnérabilité Ikare qui fait partie intégrante du SOC Itrust permet d'identifier les failles critiques pour leur apporter un correctif dans les meilleurs délais. L'installation des mises à jour critiques des systèmes d'exploitation sans délai, tel qu'imposée par la réglementation, est également suivie et un mécanisme de reporting automatique permet de suivre l'évolution en continue du niveau de sécurité des infrastructures supervisées.
Pour les postes mobiles le SOC permet notamment de s'assurer que les clés de chiffrement sont conformes aux dernières recommandations de sécurité.

- **Sécuriser les Serveurs et l'Informatique Interne (Réf. CNIL - RGPD fiches 7 et 8)**

Comme pour les postes de travail, il est recommandé d'avoir une politique restrictive d'accès aux serveurs tout en assurant la traçabilité des accès, la correction des failles de sécurités, l'archivage et l'analyse des tentatives d'intrusion, les tentatives de vol de données, les infiltrations de logiciels malveillants ou tout autre élément qui permettrait de rompre la sécurité des données.
Le SOC Itrust permet d'assurer la supervision de l'ensemble de ces éléments au travers de la collecte et de l'analyse immédiate des journaux avec son SIEM, du suivi en continue des vulnérabilités du système informatique avec Ikare et de la détection des cyber-attaques avancées avec Reveelium qui est la technologie d'intelligence artificielle venant compléter les outils traditionnels tels que les anti-les firewall ou les sandbox qui ne sont plus assez efficaces.

- **Sécuriser les Sites Web (Réf. CNIL - RGPD fiche 9)**

Il est demandé de s'assurer du suivi des bonnes pratiques minimales de sécurité et plus particulièrement, de contrôler que ce sont bien les versions les plus récentes des protocoles TLS qui sont mis en œuvre, de vérifier les ports utilisés pour les flux IP, de contrôler et de tracer les accès aux outils d'administration. La CNIL recommande l'usage régulier d'un scanner de vulnérabilités et d'un système de détection et de prévention des attaques couplés à un système d'alerte. Le SOC D'Itrust répond entièrement à ces recommandations avec l'ensemble de ses outils qui sont packagés (Journalisation, Siem, Ikare, Reveelium).

- **Sauvegarder et archiver de manière sécurisée, encadrer la destruction des données (Réf. CNIL - RGPD fiches 10, 11, 12,13)**

Le SOC permet de s'assurer de la bonne exécution des sauvegardes et permet d'historiser à la fois les accès aux sauvegardes mais aussi la fréquence des archivages comme la sécurité du canal de transmission des données. Sur la partie Infrastructure il permet de vérifier la sécurité des équipements informatiques de redondance de manière à garantir leurs caractéristiques opérationnelles en cas de besoin. Dans le cadre d'exigences de haute disponibilité des systèmes, la supervision de la sécurité permanente permet d'assurer la continuité d'exploitation dans des conditions optimales.
L'accès des prestataires et sous-traitants aux opérations de maintenance est également suivi et il est possible de journaliser et d'alerter sur les accès des applications de maintenance à distance.

- **Encadrer les développements informatiques et assurer l'intégrité des informations (Réf. CNIL - RGPD fiches 16,17)**

Dans le cadre du développement applicatif, et au-delà de l'intégration des règles de sécurité au sein même du code des applications, il est indispensable de superviser la sécurité des environnements de

développement de la même manière que les systèmes d'information de l'entreprise. Une attention particulière pourra être apporter à la supervision des accès habilités aux codes sources. Les méthodes de garantie d'intégrité de la donnée devront inclure des fonctions de hachage et l'utilisation d'une méthode de chiffrement des données permettra de garantir la protection et la confidentialité.

- **Sécurité interne et conformité du SOC Reveelium**

Comme exposé précédemment, La Réglementation Générale pour la Protection des Données personnelles a pour vocation de :

- ✔ **Renforcer les droits des personnes**, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
- ✔ **Responsabiliser les acteurs traitant des données** (responsables de traitement et sous-traitants) ;
- ✔ **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

Dans le cadre du SOC, ce sont notamment les points 1 et 2 qui sont concernés, à l'exception de SOC transnationaux dont les données pourraient être disséminées dans des serveurs présents dans plusieurs pays pour le point 3.

Pour les points 1 et 2 de l'objet réglementaire, il faut prendre en compte plusieurs facteurs juridiques concomitants dont les contours législatifs restent très clairs. Ainsi, l'obligation de traçabilité pour les besoins d'investigations prime dans les systèmes de surveillance en temps réel dont font partie les SOC.

La réglementation impose une protection de la donnée en anonymisant par exemple les données à caractère personnel pour protéger les personnes en cas de vol ou de transmission de leurs données personnelles à des tiers. Ainsi, en phase de test d'un SOC, il se pourrait que l'anonymisation de certaines données soit utilisée (avec des comptes de test par exemple) mais en phase de 'Run' l'anonymisation n'a plus de caractère obligatoire.

Dans le cas de la surveillance des systèmes d'information par le SOC d'Itrust, les données qui pourraient avoir un caractère personnel sont : les adresses IP surveillées si celles-ci sont reliées de manière permanente à des utilisateurs ; Les noms des utilisateurs sous Active Directory ; Les données de connexions des superviseurs ou des administrateurs.

Ces données sont intégralement protégées au sein du SOC Itrust par les mécanismes suivants de sécurisations appliquées aux micro-services :

- Fonctions Firewall /filtrage : le filtrage est total. Les seules connexions possibles se font en ssl sur le port 443 ou en SSH, port 22. Ce filtrage peut être configuré via la console d'administration uniquement.

- Sauvegarde : Une sauvegarde automatique de la base de données est effectuée avant chaque mise à jour du produit. La sauvegarde du système client est sous sa responsabilité.

- Durcissement d'OS : séparation des process avec un utilisateur système par process. La machine est durcie par retrait des fonctions non-essentielles. Le durcissement appliqué est notamment basé sur les pratiques du TopSans et du NIST américain.

- Hachage des mots de passe d'utilisateurs : les mots de passe sont hachés via la fonction SHA256 (cf. cible de sécurité). Mécanisme de déconnexion après inactivité (1h)

- Journalisation et traçabilité : Les connexions, actions effectuées et mises à jour sont historisées au format Syslog

- Des règles d'auto-contrôle du bon fonctionnement sont également présentes dans le SIEM.

ITRUST procède également à des audits trimestriels de la sécurisation de son SOC par son équipe Red Team.

Au-delà de la phase de run (supervision), reste la partie post-traitement avec la sauvegarde des Logs. Les entreprises doivent prévenir dans leur charte informatique que certaines données des utilisateurs soient conservées au travers des logs.

Le SOC d'ITRUST permet de paramétrer la durée de rétention des logs en ligne au format brut ou indexé selon les instructions de son client. Il est d'usage de conserver les Logs sur une durée d'une année, ce qui reste acceptable par la CNIL dans le cadre du SOC même si la durée recommandée est de six mois. L'archivage ultérieur de ces logs devra être fait par l'entreprise selon sa propre politique de sécurisation de la donnée personnelle.

X X X