Proofpoint Threat Response et le RGPD

Assurer la conformité grâce à l'automatisation de la sécurité et aux bonnes pratiques en matière de confidentialité des données

PRINCIPAUX AVANTAGES

Adoption de bonnes pratiques de sécurité

- Neutralisez les menaces ciblées de manière plus rapide et efficace.
- Allégez la charge de travail de vos ressources informatiques grâce à l'automatisation de la réponse aux incidents.
- Limitez la baisse de vigilance engendrée par la multiplication des alertes.
- Collectez et hiérarchisez des données issues d'équipements de sécurité disparates.
- Bénéficiez d'une vue contextuelle de l'ensemble des menaces.

Conformité au RGPD

- Empêchez le partage de données personnelles avec des tiers.
- Assurez l'intégration avec les systèmes de contrôle internes.
- Ajoutez Proofpoint Threat Response à des registres internes de traitement des données.
- Apportez la preuve de votre conformité avec l'aide de Proofpoint.

À l'heure actuelle, la plupart des entreprises performantes font appel à des technologies d'automatisation pour gérer les incidents de sécurité. Que nous révèle cette tendance ? Quels sont les éléments à prendre en considération si vous envisagez d'automatiser les systèmes de sécurité pour des raisons de conformité et de mise en œuvre des bonnes pratiques, ou encore pour bénéficier d'avantages à long terme ?

L'AUTOMATISATION DE LA RÉPONSE AUX INCIDENTS : UNE NÉCESSITÉ

La nature du paysage actuel de la cybersécurité exige de pouvoir réagir rapidement. Malheureusement, les équipes de sécurité sont confrontées à de nombreux problèmes, qui les empêchent de contrer les menaces ciblées de manière rapide et efficace. En voici quelques exemples :

- **Pénurie de personnel :** la réponse aux incidents est un processus généralement lent et fastidieux, dont certaines tâches, extrêmement chronophages, créent des goulets d'étranglement. Par ailleurs, la répétition des mêmes tâches pour chaque incident peut accroître la charge de travail des équipes de sécurité, déjà fort sollicitées.
- **Baisse de vigilance face aux alertes :** plus vous multipliez les équipements de sécurité, plus le nombre d'alertes augmente. Il incombe alors à votre équipe de sécurité de trier ces alertes manuellement. En quoi cela pose-t-il problème ? Cette façon de fonctionner est sujette à l'erreur humaine et les véritables incidents risquent dès lors d'être négligés.
- **Données et équipements de sécurité disparates :** l'investigation d'incidents repose sur des informations issues d'un grand nombre de sources disparates, où chaque donnée constitue une pièce du puzzle. Comme la majorité des entreprises, vous êtes confronté à un nombre croissant de menaces ciblées auxquelles il faut pouvoir réagir en quelques minutes. Malheureusement, cette abondance d'informations disparates a tendance à ralentir la réponse aux incidents.

Les solutions d'orchestration, d'automatisation et de réponse aux incidents de sécurité (SOAR, Security Orchestration, Automation and Response) peuvent contribuer à résoudre ces problèmes. Elles sont en effet capables d'absorber les données d'alertes issues de différentes sources et d'intégrer des tâches d'automatisation de la réponse aux incidents. En optant pour une solution SOAR, non seulement vous gagnez du temps, mais vous limitez aussi le nombre de temps pleins nécessaires pour gérer les incidents de sécurité, et ce grâce à l'automatisation du processus de réponse. En outre, une telle solution contribue à réduire le délai moyen de réponse, de confinement et de neutralisation des menaces.

Proofpoint Threat Response est une solution SOAR qui permet d'éliminer les tâches manuelles et les conjectures associées à la gestion des incidents. Votre équipe de sécurité peut ainsi neutraliser les menaces plus rapidement et avec une efficacité accrue. Proofpoint Threat Response collecte des alertes issues de diverses sources, puis les enrichit et les recoupe automatiquement avec des données contextuelles fournies par le système de veille de Proofpoint, le tout en quelques secondes seulement. Qui plus est, la solution identifie les personnes, les données et les systèmes ciblés, assure le mappage entre les adresses IP et les utilisateurs et fournit des informations de cyberveille externes, telles que des flux STIX et TAXII standard. Les analystes sont ainsi en mesure de classer rapidement les incidents de sécurité. Sur la base des données contextuelles et d'investigation numérique collectées et analysées, Proofpoint Threat Response propose une vue contextuelle très complète de la menace. Celle-ci permet à vos analystes d'appliquer des mesures automatisées, par exemple :

- Retirer des emails remis dans les boîtes de réception des utilisateurs
- Ajouter des utilisateurs à des groupes jouissant de permissions restreintes
- Mettre à jour les listes de blocage des pare-feux et des filtres Web
- Confiner les menaces par leur blocage/mise en quarantaine sur Microsoft Exchange, les pare-feux, les logiciels de détection et de réponse aux incidents touchant les terminaux (EDR, Endpoint Detection and Response), les passerelles Web, Microsoft Active Directory, les solutions de contrôle de l'accès réseau (NAC, Network Access Control), etc.

CONFIDENTIALITÉ DES DONNÉES ET OPÉRATIONS DE SÉCURITÉ

RGPD et licéité du traitement des données

Comme stipulé dans le règlement général sur la protection des données (RGPD) de l'Union européenne, le traitement des données à caractère personnel est une tâche légitime des responsables du traitement des données. C'est particulièrement vrai dans les domaines où des données personnelles sont nécessaires pour assurer la sécurité du réseau et des informations. Le traitement des données personnelles est également légitime dans le cadre de la prévention d'actes illicites ou malveillants susceptibles de compromettre la disponibilité, l'authenticité, l'intégrité et la confidentialité des données personnelles, que celles-ci soient destinées à être stockées ou transférées. Ces « intérêts légitimes » sont définis à l'article 6 du RGPD, « Licéité du traitement ». Les intérêts légitimes sont donc admis par la loi. Mais seulement si vous êtes en mesure de justifier la nécessité du traitement. Par ailleurs, le traitement doit respecter les principes de proportionnalité et de subsidiarité. Ces exceptions à l'usage de données personnelles à des fins de sécurité informatique sont définies à l'article 6, paragraphe 1, point f, et dans le considérant 49 du RGPD.

Pour ce qui est de la conformité au RGPD, en choisissant une solution telle que Proofpoint Threat Response pour étendre et sécuriser votre infrastructure, vous mettez toutes les chances de votre côté. Composante essentielle de toute architecture informatique moderne, cette solution permet de traiter les données au moyen de structures de sécurité externes, telles qu'un fournisseur d'informations de cyberveille ou des services de sécurité. Proofpoint Threat Response ne transmet aucune donnée à des intervenants extérieurs. Elle ne les utilise qu'aux fins convenues, décrites dans le contrat de service écrit conclu entre vous et Proofpoint. De plus, Proofpoint Threat Response est uniquement disponible en déploiement sur site et, par défaut, n'envoie aucune donnée vers l'extérieur.

Ajout de Proofpoint Threat Response aux registres des activités de traitement

Pour être en conformité avec le RGPD, la solution doit également respecter les principes de paramétrage et d'intégration dans d'autres systèmes. Il est possible d'ajouter Proofpoint Threat Response à des registres internes de traitement des données, conformément aux dispositions de l'article 30 du RGPD, « Registre des activités de traitement ».

Échange interne d'informations d'identification

L'article 47 du RGPD, « Règles d'entreprise contraignantes », autorise le partage au niveau international d'informations internes à un groupe d'entités implantées dans différents pays. Ces règles d'entreprise doivent inclure tous les droits opposables et principes fondamentaux de confidentialité des données afin de garantir une protection adéquate des transferts ou catégories de transferts de données personnelles.

Pour assurer votre conformité au RGPD, un système de contrôle interne (ICS) est indispensable. Il vous faut donc mettre en place un tel système. Pour être conforme, cet ICS doit se composer d'un système de contrôle interne et d'un système de surveillance. Comme son nom l'indique, le système de contrôle a pour finalité de contrôler les activités de votre entreprise. Il veille à l'enregistrement correct de vos transactions commerciales et au respect des principes du RGPD.

ÉCHANGE DE DONNÉES AVEC DES TIERS[1]

Afin de garantir un niveau de protection adéquat, le RGPD autorise les entreprises à avoir recours à des experts, outils ou services externes pour appuyer les mesures de sécurité internes. Les dispositions du RGPD visant à s'assurer que ces fournisseurs tiers (sous-traitants) respectent votre niveau de protection des données sont très strictes. Elles sont définies à l'article 28, « Sous-traitant ». Le responsable du traitement ne peut recruter que des sous-traitants capables de garantir que toute mesure technique et organisationnelle appliquée le sera en totale conformité avec le RGPD. Les sous-traitants doivent garantir la protection des droits des personnes concernées.

Pour vous aider à répondre à ces exigences et ainsi assurer votre conformité, Proofpoint met à votre disposition, pour tous les produits connexes, différents types de documents. Ceux-ci incluent notamment les accords de traitement des données que vous devez conserver dans votre registre des activités de traitement.

Conçu en tenant compte des bonnes pratiques du secteur et des exigences en matière de conformité, Proofpoint Threat Response automatise et accélère la réponse aux incidents. Cette solution vous permet également de savoir si l'utilisation que vous faites des données personnelles dans un contexte de sécurité est conforme au RGPD. Autre avantage, Proofpoint met à votre disposition les documents nécessaires pour apporter la preuve de votre conformité.

1 Lors de la configuration d'échanges de données ou de services externes (exemple : Proofpoint Targeted Attack Protection).

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**