elastic

Mise en conformité de la sécurité de vos données avec Elastic

Présentation

Le paysage des menaces liées à la cybersécurité ne cesse de se complexifier. Les cyberattaques sont désormais plus fréquentes, ciblées, furtives et avancées d'un point de vue technique : il est donc devenu indispensable de mettre en place une sécurité des données à la fois robuste et exhaustive. Les contraintes réglementaires et les responsabilités liées à la cybersécurité gagnent également en complexité. Pour y faire face, la mise en œuvre d'une approche de la sécurité axée sur le risque est désormais impérative.

Afin de suivre l'évolution des contraintes légales, d'éviter des ruptures d'activité critiques et de se protéger contre le coût des actions en justice en cas d'intrusion, les organisations sont invitées à privilégier une vision holistique et stratégique de leur cybersécurité. Ne pas s'y conformer expose non seulement les entreprises à d'importantes conséquences juridiques et financières, mais également à des préjudices opérationnels et réputationnels irréparables.

Ce livre blanc explore comment les organisations peuvent utiliser Elastic pour remplir leurs obligations de sécurité et bâtir une défense véritablement résiliente face aux cybermenaces. Grâce à sa solution performante, souple et évolutive, Elastic permet aux organisations de satisfaire à des exigences de conformité et de sécurité opérationnelle multiples, notamment :

- Visibilité accrue et capacité de recherche des données sur les surfaces d'attaque
- Extractions simplifiées de données pour les demandes de conformité
- Détection et automatisation rationalisées pour remédier aux menaces
- Surveillance et démonstration de votre posture de sécurité
- Threat Intelligence enrichie

Dans les sections suivantes, nous détaillons les piliers de la sécurité communs aux textes de loi ; nous passons en revue les préjudices possibles en cas de mauvaise gestion des risques ; et nous expliquons comment tirer parti de la plateforme Elastic pour garantir votre conformité et renforcer votre posture de sécurité.

Attention : *Ce livre blanc est communiqué à titre d'information seulement et ne remplace en aucun cas un conseil juridique formel. Veuillez consulter votre service juridique pour obtenir un avis spécialisé.*

Principes fondamentaux de sécurité et obligations de conformité connexes

Le cadre réglementaire moderne de la sécurité est un véritable patchwork de contraintes propres à chaque juridiction, secteur ou catégorie de données. Vos responsabilités dépendront donc de votre situation géographique, de vos lieux d"exploitation, des types de données traitées et de vos processus, incluant le niveau de criticité des informations et la spécificité de votre métier.

Par exemple, une institution financière mondiale pourrait être soumise simultanément à la Loi fédérale américaine Gramm-Leach-Bliley (« GLBA »), règlement sur la cybersécurité du ministère des Services financiers de New York (« NYDFS »), résilience des opérations numériques de l'UE la Loi (« DORA ») et la Directive 2 de l'UE sur la sécurité des réseaux et de l'information (« Directive NIS2 »), entre autres lois.

Une entreprise de vente au détail basée aux États-Unis et cotée en bourse pourrait, en revanche, être soumise à un ensemble différent d"exigences, telles que les normes PCI Data Security Standards (« PCI-DSS ») pour la sécurité des cartes de paiement, les obligations de la loi Sarbanes-Oxley (« SOX ») pour la sécurité des systèmes de reporting financier, et les lois des États américains sur la notification des violations de données. Sans omettre, naturellement, les législations relatives à la confidentialité et leurs impératifs de sécurité visant à protéger les informations à caractère personnel.

Outre ces obligations légales, beaucoup de sociétés choisissent de suivre des référentiels de sécurité tiers à travers des certifications telles que l’ISO 27001, SOC 2, le NIST CSF ou le programme britannique Cyber Essentials.***

Malgré ces différences, les cadres législatifs, réglementaires, d'autorégulation et sectoriels — ainsi que les bonnes pratiques générales en matière de sécurité — convergent largement autour d'un ensemble de principes fondamentaux de sécurité. Nous présentons ci-dessous les éléments clés de ces principes et illustrons leur adéquation avec différents cadres.

Inventaire, mapping et classification des données

Les organisations ne peuvent pas déployer de contrôles de sécurité basés sur le risque sans comprendre au préalable quelles données elles détiennent (un processus appelé inventaire des données), où elles résident (mapping des données) et leur caractère sensible (classification des données).

Ces processus sont également cruciaux en cas d'incident de violation de données, afin que les entreprises puissent déterminer si les données touchées déclenchent des obligations de notification légales, réglementaires ou contractuelles. Pour ces raisons, l'inventaire, le mapping et la classification des données sont soit explicitement requis par de multiples cadres, soit une condition préalable nécessaire pour se conformer à de nombreux cadres. Par exemple :

- La *règle de sauvegarde de la FTC* (16 CFR § 314), qui met en œuvre les exigences pour certaines institutions financières soumises à la GLBA, oblige les institutions financières concernées à identifier et à évaluer la sensibilité des informations clients dans le cadre de leur processus d'évaluation des risques.
- La *règle Security HIPAA* (45 CFR § 164.308) oblige également les entités couvertes à inventorier et à protéger les informations de santé électroniques protégées (« ePHI »).
- En vertu de l'article 30 du Règlement général sur la protection des données de l'UE (« RGPD »), les organisations doivent assurer la maintenance d'un registre des activités de traitement, ce qui nécessite effectivement un inventaire des données et un mapping pour démontrer la conformité.
- En règle générale, les obligations de signalement propres à chaque État des États-Unis ne s'appliquent que si des catégories spécifiques de données à caractère personnel concernant ses résidents ont été compromises. Par conséquent, en cas de violation de données, les entreprises doivent être en mesure de déterminer quelles catégories de données figurent dans l'ensemble de données compromis.
- Des frameworks comme NIST SP 800-53 et les contrôles CIS mettent l'accent sur la classification des données afin de garantir que les protections soient adaptées à la sensibilité des données. La mise en place d'un inventaire et d'une taxonomie de classification permet aux organisations de sécuriser les accès, de suivre les mouvements de données sensibles et de garantir leur conformité tout en prévenant la diffusion accidentelle de données.

Contrôles d'accès basés sur les rôles

Les contrôles d'accès basés sur les rôles (« RBAC ») sont des mesures conçues pour garantir que les individus n'aient accès qu'aux systèmes et aux données dont ils ont besoin pour exercer leurs responsabilités (un concept également connu sous le nom de « privilège minimal »). L'application cohérente des RBAC réduit le risque d'accès non autorisé par des initiés malveillants et peut contribuer à limiter la portée d'une intrusion. De nombreux frameworks juridiques et industriels exigent explicitement ou recommandent fortement le RBAC :

- Conformément au RGPD de l'UE, seules les personnes dûment autorisées ayant une nécessité de savoir peuvent accéder aux données à caractère personnel. Le règlement va même plus loin en définissant l'accès non autorisé comme un cas de violation de données.
- La norme du Massachusetts sur la protection des informations personnelles, 201 CMR 17.04, exige des entreprises exerçant dans cet État qu'elles mettent en œuvre des mesures de contrôle d'accès sécurisées, limitant l'accès aux dossiers et fichiers contenant des informations personnelles sensibles aux seules personnes dont les fonctions nécessitent de telles informations.
- La Règle de sécurité HIPAA exige que l'accès aux ePHI soit limité aux personnes ayant un besoin légitime de les connaître.
- L'article 9(4) de la DORA de l'UE exige que les institutions financières couvertes mettent en œuvre des politiques qui limitent l'accès physique ou logique aux actifs à ce qui est nécessaire uniquement pour des fonctions et activités légitimes et approuvées.
- Les normes industrielles telles que NIST SP 800-53, ISO/IEC 27001 et les contrôles CIS (par exemple, le contrôle CIS 6) mettent également l'accent sur la RBAC en tant que pratique fondamentale de gestion des accès.

Journalisation et surveillance

Les logs d'événements de sécurité font partie des ressources les plus importantes dont disposent les entreprises pour détecter les incidents de sécurité. Les logs reflétant des informations telles que les dates et heures d'accès, les actions effectuées, ainsi que l'utilisateur qui les a réalisées, sont essentiels pour vérifier si l'accès au système a été autorisé et enquêter sur d'éventuelles activités non autorisées. La surveillance des logs en temps réel ou en temps quasi réel est également essentielle pour détecter et traiter les menaces de manière opportune.

La gestion des logs peut toutefois s'avérer complexe pour les organisations dotées de systèmes complexes et diversifiés susceptibles de générer quotidiennement de grands volumes de logs. Ces organisations doivent s'appuyer sur des solutions techniques pour regrouper efficacement les logs et les monitorer afin de détecter toute activité anormale. Les frameworks juridiques et industriels soulignent l'importance du logging et du suivi :

- La norme de sécurité des données de l'industrie des cartes de paiement (PCI-DSS) exige que toutes les entreprises qui stockent, transmettent ou traitent des données de cartes de paiement loggent et monitorent tous les accès aux composants du système et aux données des titulaires de cartes.
- La règle de sécurité HIPAA impose des contrôles d'audit pour enregistrer et examiner l'activité dans les systèmes contenant des ePHI.
- La section 404 de la loi SOX exige que la direction et les auditeurs évaluent et rendent compte de l'efficacité des contrôles internes des sociétés cotées en bourse en matière de reporting financier. Ces auditeurs évaluent ces contrôles par rapport à des frameworks tels que COBIT, qui exigent le logging d'audit de l'activité des utilisateurs, de l'accès aux systèmes financiers et des modifications apportées aux données financières.
- Le volet « Détection » du NIST CSF précise que les entreprises doivent loguer les événements de sécurité et assurer la maintenance d'une surveillance continue de la sécurité, ce qui est également indispensable pour le reporting en temps opportun des incidents à notifier en vertu, par exemple, de l'article 32 du RGPD de l'UE, de l'article 23 de la directive NIS2 de l'UE ou de l'article 19 de la loi DORA de l'UE.

Détection et réponse aux intrusions

Malheureusement, compte tenu de l'état actuel de la menace, toute organisation est aujourd'hui une cible potentielle pour les cyberattaques. Les organisations doivent se doter de dispositifs de détection d'intrusion et de mécanismes de réponse aux incidents afin de faire face aux tentatives d'intrusion, désormais inévitables. Ces systèmes sont essentiels pour permettre aux entreprises d'identifier rapidement une attaque et d'y répondre avant qu'elle ne dégénère en incident grave. Cependant, les systèmes de détection d'intrusion et les processus de réponse aux incidents sont rarement efficaces tels quels; au contraire, les entreprises doivent établir une base d'activité et adapter les critères d'alerting aux attributs uniques de l'entreprise. Cette adaptation accroît la précision des alertes et contribue à garantir que les incidents sont correctement triés et traités en fonction de leur criticité. La détection et la réponse aux intrusions sont au cœur de nombreux frameworks juridiques et industriels :

- Les lois fédérales, nationales et internationales sur la notification des violations de données exigent que les violations de données soient signalées dans des délais spécifiques. Alors que le délai de 72 heures du RGPD est souvent perçu comme la norme la plus stricte, le règlement européen DORA impose désormais de déclarer les incidents « TIC » majeurs dans un délai de quatre heures après leur découverte.
- Le règlement du Département des services financiers de New York (NYDFS), en sa section 500.16, impose aux entités visées la mise en place de plans de réponse aux incidents destinés à garantir une gestion et une remédiation diligentes des crises cyber.
- La loi DORA exige également que les institutions financières réglementées élaborent des plans détaillés de réponse aux incidents.
- Le NIST CSF précise que les entreprises assurent la maintenance d'une « Détection » détaillée et des contrôles « Réponse » pour détecter les incidents de sécurité et y répondre.

Le coût de la non-conformité

Ne pas mettre en œuvre des contrôles de sécurité conformes et efficaces peut exposer les entreprises, leur direction et leur conseil d'administration à des risques juridiques, financiers et de réputation importants. Concrètement, l'absence de mécanismes de monitoring performants accroît le risque de maintien des accès illicites. Cela offre aux cybercriminels l'opportunité d'effectuer des repérages, de se fondre dans le trafic normal du réseau, de siphonner des données ou de préparer une offensive par ransomware. L'absence de logs exhaustifs peut empêcher de savoir si une action suspecte était en réalité légitime, provoquant ainsi des erreurs de signalement, qu'il s'agisse d'alertes excessives ou, au contraire, d'un manque de notification.

Lors d'une fuite de données ou d'un cyberincident, l'absence d'un recensement et d'un mapping précis complique grandement la tâche lorsqu'il s'agit de déterminer quelles informations ont été touchées. Cette situation risque de retarder le signalement de l'incident aux personnes concernées ainsi qu'aux régulateurs. En conséquence, ces lenteurs amplifient l'impact négatif sur les victimes et placent l'entreprise en infraction vis-à-vis des régulateurs. Au fardeau de la réponse technique s'ajoutent alors des sanctions financières, des actions de groupe et des coûts de défense juridique significatifs. Pour les fournisseurs de solutions B2B, cette opacité empêche de cibler rapidement les comptes clients dont les données ont été compromises durant l'attaque.

Ne pas se conformer aux prescriptions de sécurité des lois sur la confidentialité peut engendrer des amendes record, des sanctions réglementaires et engager durablement la responsabilité juridique de l'organisation. Au-delà des amendes, les organisations risquent des litiges pour manquement à leurs obligations de sécurité ou de contrat, souvent portés par des collectifs de plaignants dont les données personnelles ont été piratées. Notamment, la loi californienne sur la protection de la vie privée des consommateurs (CCPA) établit un droit d'action privé pour les plaignants dont les données sensibles ont été compromises à la suite du manquement d'une entreprise à maintenir des mesures de sécurité « raisonnables ». Les sanctions et les dommages-intérêts prévus par des réglementations telles que HIPAA, le CCPA ou le RGPD de l'UE peuvent rapidement atteindre des montants à sept chiffres.

En plus des amendes de conformité, le préjudice d'image résultant de failles de sécurité peut s'avérer dévastateur pour l'entreprise. Les sociétés victimes d'une intrusion ou en infraction vis-à-vis des normes de cybersécurité s'exposent à un désengagement de leur clientèle, à un « bad buzz », à une paralysie de leurs activités et à un impact délétère sur leur capital de marque. Les sociétés cotées en bourse courent également le risque de voir le cours de leurs actions chuter à la suite de défaillances de sécurité largement médiatisées. Les entreprises s'exposent à une fuite des clients et à des demandes de dommages-intérêts pour manquement à la protection des données, avec pour conséquences directes une perte de parts de marché et de rentabilité. À la lumière de ces risques majeurs, les sociétés se doivent de traiter la sécurité comme un pilier central, en investissant dans la mise en conformité et dans des dispositifs de gestion des risques robustes.

Exploiter Elastic pour la conformité

La plateforme Elasticsearch constitue le socle des deux solutions prêtes à l'emploi d'Elastic : Elastic Observability et Elastic Security. Les sociétés peuvent utiliser la nature ouverte de la plateforme Elastic pour assurer leur mise en conformité et atténuer les risques cyber majeurs sur l'ensemble de leurs infrastructures. Point essentiel, l'agilité et la scalabilité sont au cœur des solutions d'Elastic. Elles s'intègrent à des systèmes diversifiés pour centraliser l'information, offrant des fonctions de recherche performantes pour des applications quasi illimitées. Voici quelques exemples de la manière dont Elastic peut être utilisé pour soutenir les principes fondamentaux d'un programme de sécurité :

Mapping et classification des données

Elastic appuie les démarches de mapping de données en indexant l'ensemble des données, qu'elles soient structurées ou non. Cela garantit aux organisations une vue unifiée et centralisée pour identifier précisément où se trouvent leurs différentes catégories de données. L'usage de métadonnées, de métadonnées et du Machine Learning permet à Elastic de repérer des structures récurrentes dans les données. Ce processus optimise la classification des actifs, comme les logs système ou les données sensibles, pour répondre aux exigences légales de protection. Sans être un outil de classification de données spécialisé, Elastic offre des fonctions de recherche et d'analytique robustes qui s'insèrent parfaitement dans une stratégie globale de gouvernance. Cela facilite le suivi et le recensement des actifs informationnels, qu'ils soient hébergés dans le cloud ou sur site.

Contrôle d'accès basé sur les rôles (RBAC)

Bien qu'Elastic ne soit pas un outil RBAC, la plateforme peut ingérer les logs des systèmes d'une organisation pour aider à identifier les lacunes dans la gestion des autorisations. Les organisations peuvent analyser les modèles d'accès pour identifier les systèmes auxquels les groupes d'utilisateurs peuvent ou non avoir besoin d'accéder, et utiliser ces informations pour orienter l'attribution des privilèges d'accès. Elastic aide également nos clients à ingérer les politiques d'accès par groupe provenant de divers systèmes, ce qui permet aux entreprises de générer des rapports à partir de ces données pour démontrer l'application des droits d'accès lors d'audits ou d'enquêtes de conformité. Et Elastic intègre des fonctionnalités RBAC dans ses Interfaces Elastic Security et Kibana. Les administrateurs peuvent définir des rôles qui limitent l'accès utilisateur à des index, à des tableaux de bord ou à des actions spécifiques (comme les afficher ou les modifier), en soutenant principes d'accès au moindre privilège.

Journalisation et surveillance

L'une des principales forces d'Elastic, et l'un des cas d'utilisation les plus courants, est l'agrégation, le stockage et l'analyse des logs à grande échelle. Grâce à Elastic Agent, les entreprises peuvent ingérer des logs provenant d'Endpoints, de serveurs, de services cloud et d'applications. Ces logs sont indexés dans Elasticsearch, ce qui permet une analyse et une visualisation en temps réel dans Kibana. Elastic prend en charge la rétention des logs à long terme, l'alerte et la détection des anomalies, ce qui en fait une solution idéale d'agrégation des logs et de surveillance de la sécurité, ainsi qu'un outil efficace de reporting de la conformité. Sa suite d'observabilité fournit également un suivi des performances applicatives (APM), des métriques et un monitoring de la disponibilité pour une visibilité holistique de l'infrastructure.

De nombreuses réglementations, telles que la directive M-21-31 pour les agences fédérales américaines, imposent aux organisations de stocker les logs pendant une période déterminée. La structure de hiérarchisation des données d'Elastic permet un stockage rentable, adapté à la fréquence et à la rapidité d'accès et d'utilisation des données. Le mode d'indexation logsdb d'Elasticsearch **réduit l'espace de stockage des données de logs jusqu'à 65 %**, améliorant ainsi la visibilité et la conformité tout en garantissant un accès immédiat à toutes les données pour l'analyse.

Pourne citer qu'un exemple, l'Université d'York a migré son système de gestion des informations et des événements de sécurité (SIEM) vers Elastic Security afin de renforcer ses capacités de cybersécurité, d'améliorer son efficacité opérationnelle et de réduire ses coûts. En déployant environ 9 000 agents Elastic sur ses serveurs et postes de travail, et en collectant les journaux de l'ensemble de son infrastructure cloud hybride (Google Cloud, AWS, Azure et serveurs sur site), l'Université ingère 500 gigaoctets de données par jour, avec 35 téraoctets de logs stockés. Elle s'intègre également à des outils de sécurité tels que les pare-feu Palo Alto Networks, Cloudflare et Duo, garantissant une surveillance complète sur diverses plateformes. Cette configuration permet des recherches ultra-rapides sur de vastes volumes de données, réduisant le temps de requête de plusieurs heures à quelques secondes seulement.

Détection et réponse aux intrusions

Elastic Security inclut des capacités de détection et de réponse aux points de terminaison (EDR) et intègre des flux d'informations sur les menaces pour soutenir la détection des intrusions. Cela permet aux équipes de sécurité de monitorer les menaces connues et inconnues grâce à des analyses comportementales, au mapping des attaques et à des règles de détection personnalisées. Grâce au logging centralisé, les analystes peuvent rapidement corréler les événements entre les systèmes, examiner les alertes dans leur contexte et orchestrer les workflows de réponse. Elastic prend également en charge les réponses automatisées grâce à des intégrations avec des plateformes tierces d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR), ce qui en fait un outil puissant pour améliorer la préparation à la réponse aux incidents et la recherche de menaces. Ces capacités avancées réduisent la probabilité d'une violation et accélèrent le temps de réponse en cas d'intrusion réussie, ce qui, en retour, atténue les responsabilités juridiques potentielles associées à un incident.

AHEAD, un fournisseur de premier plan de plateformes numériques et de transformation, a considérablement renforcé ses capacités de détection et de réponse aux intrusions en intégrant Elastic Security à ses services de sécurité gérés. AHEAD ingère désormais les données de sécurité de ses clients dans Elastic sur Elastic Cloud, où elles sont enrichies, agrégées et connectées à des flux de renseignements sur les menaces (threat intelligence). Elastic sert également de source de données pour le système SOAR de l'organisation. Les analystes de sécurité d'AHEAD peuvent aussi exploiter des alertes basées sur l'IA qui mettent en évidence les informations pertinentes au sein des événements de sécurité, réduisant ainsi le temps nécessaire au tri manuel de vastes volumes de données et aidant à alléger la charge liée aux faux positifs.

Conclusion

L'évolution constante et la sophistication des menaces informatiques rendent la mise en conformité réglementaire et la gestion des risques de plus en plus ardues pour les organisations, confrontées à un arsenal législatif en pleine

expansion. Ne pas agir expose les sociétés à des risques juridiques et financiers majeurs, tout en provoquant des dysfonctionnements opérationnels et une dégradation durable de leur réputation. Elastic peut aider les DSI et les DSI à renforcer la conformité de leurs organisations à ces diverses exigences légales, notamment dans les domaines du mapping et de la classification des données, du RBAC, du logging et de la surveillance, ainsi que de la détection et de la réponse aux intrusions.

