Livre blanc

Établissements de santé

Quelle stratégie de cybersécurité adopter ?

Romain Ravon

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

Table des matières

Introduction

Le secteur de la santé assure non seulement des soins médicaux d'urgence mais aussi la gestion de la santé publique à long terme.

Cela inclut une vaste gamme d'entités, des hôpitaux aux centres de recherche spécialisés. Ces institutions sont cruciales pour l'amélioration continue de la qualité de vie, grâce à l'expertise professionnelle et l'usage de technologies de pointe. Cependant, la digitalisation croissante des données de santé a augmenté la vulnérabilité du secteur aux cyberattaques. Ces attaques ne menacent pas seulement la confidentialité et l'intégrité des données médicales sensibles, elles peuvent également paralyser les systèmes opérationnels, retarder les diagnostics et les traitements, et, dans les cas les plus graves, compromettre directement la sécurité des patients. Par exemple, une attaque par ransomware pourrait verrouiller l'accès aux dossiers médicaux électroniques, entravant gravement les opérations hospitalières.

En outre, le cadre réglementaire, tel que le RGPD ou NIS2 en Europe, impose des exigences strictes en matière de protection des données, incluant les informations de santé. Le non-respect de ces normes peut entraîner des sanctions financières considérables et nuire à la réputation des institutions de santé, affectant ainsi la confiance des patients et des partenaires.

Par conséquent, il est impératif pour le secteur de la santé d'investir dans des systèmes de sécurité robustes et de s'assurer de leur conformité avec les réglementations pertinentes. Cela passe non seulement par des technologies de sécurité avancées mais aussi par une culture de cybersécurité intégrée à tous les niveaux de l'organisation. Former le personnel sur les risques de cybersécurité et les bonnes pratiques est tout aussi crucial que la mise en place de protections technologiques.

Ce guide vise à doter les spécialistes de la sécurité, les analystes, les responsables informatiques et les membres de la direction des outils nécessaires pour naviguer dans le monde complexe de la cybersécurité.

Chapitre 1

Cyberattaques : un défi pour le secteur de la santé

Dans le secteur de la santé, la menace des cyberattaques est devenue une préoccupation majeure, non seulement en raison de la vulnérabilité accrue des systèmes numériques mais aussi du caractère crucial des services qu'ils soutiennent.

IMPACTS SUR LA CONTINUITÉ DES SOINS

Les hôpitaux traitent et stockent des volumes considérables de données personnelles et médicales sensibles sur la santé des patients, leurs antécédents médicaux, ainsi que leurs informations financières. Une cyberattaque réussie, entraînant une violation de ces données, peut compromettre non seulement la confidentialité et l'intégrité des informations mais également leur disponibilité, mettant en danger direct la gestion des traitements et le suivi médical des patients.

CONFORMITÉ RÉGLEMENTAIRE ET RÉPERCUSSIONS FINANCIÈRES

Dans le cas d'une attaque, en plus des frais immédiats tels que la remédiation technique et le renforcement des systèmes de sécurité, les conséquences peuvent être encore plus préjudiciables; amendes, poursuites, demandes de dédommagement ou encore perte de revenus liée à la baisse de confiance des patients. De plus, la réglementation, comme le RGPD ou NIS2, exige pour cela un haut niveau de protection des données, sous peine de sanctions sévères.

LA CYBERSÉCURITÉ DES ÉQUIPEMENTS MÉDICAUX ET LA MENACE ÉVOLUTIVE

Avec l'avancement technologique, de nombreux équipements médicaux essentiels sont désormais connectés à Internet. Ces dispositifs, allant des moniteurs cardiaques aux pompes à insuline, augmentent les risques de cyberattaques ciblées qui peuvent altérer leur fonctionnement. La compromission de ces équipements peut avoir des répercussions directes sur le traitement des patients, soulignant l'urgence de sécuriser ces technologies contre des menaces en constante évolution.

UNE APPROCHE MULTIDIMENSIONNELLE

Face à ces défis, les hôpitaux doivent adopter une stratégie de cybersécurité qui inclut non seulement la mise en place de défenses technologiques avancées mais aussi la formation continue du personnel sur les meilleures pratiques en matière de cybersécurité. Les protocoles de réponse en cas d'incident doivent être agiles et robustes, permettant une réaction rapide et efficace en cas de violation. De plus, la collaboration avec les organismes réglementaires et les partenaires du secteur est essentielle pour partager les renseignements sur les menaces et améliorer collectivement les normes de sécurité du secteur de la santé.

En moyenne, seulement 1,7% des budgets hospitaliers sont alloués au numérique, bien en deçà des standards d'autres secteurs comme la banque (9%).

source : https://www.clubic.com/actualite-548858-cyberattaques-sur-les-hopitaux-dans-un-rapport-choc-la-cour-des-comptes-devoile-des-failles-critiques-et-ses-solutions.html

Chapitre 2

Conformité réglementaire : des enjeux majeurs

La digitalisation est omniprésente, la directive NIS2 et le Règlement Général sur la Protection des Données (RGPD) représentent des piliers fondamentaux pour la sécurisation du secteur de la santé publique en Europe. La mise à jour de la directive NIS, désormais appelée NIS2, marque un tournant décisif en élargissant considérablement la portée et les exigences en matière de cybersécurité, mettant un accent particulier sur la résilience des infrastructures essentielles face aux cyberattaques.

ESET vous accompagne dans la mise en conformité

	CIPA	FERPA	GELBA	HIPAA	PCI	SOX	HITEC	ISO27001	ISO27002	ISO9001	RGPD	FedRAMP
Protection antivirus et antimalware	●	●	●	●	●	●	●	●	●	○	●	●
Cryptage	●	●	●	●	●	●	●	●	●	●	●	●
Authentification à double facteurs	○	○	●	●	●	●	●	●	●	○	●	●
Management centralisé	●	●	●	●	●	●	●	●	●	●	●	●
E-mail sécurisé (inclu E.G anti-phishing)	●	●	●	●	●	●	●	●	●	○	●	●
Évaluation des vulnérabilités	●	●	●	●	●	●	●	●	●	○	●	●
Gestion des mises à jour	●	●	●	●	●	●	●	●	●	●	●	●

● Obligatoire ● Recommandé ○ Facultatif

Des exigences minimales de sécurité toujours plus strictes avec l'arrivée de NIS2 en France en 2025

L'IMPACT DE NIS2 SUR LA SANTÉ PUBLIQUE

NIS2 vise à consolider la sécurité des réseaux et des systèmes d'information au sein des infrastructures critiques, incluant les hôpitaux, les cliniques et les laboratoires de recherche. Ces établissements sont devenus extrêmement dépendants des technologies numériques, ce qui les rend particulièrement vulnérables aux perturbations causées par des cyberattaques. En renforçant la cybersécurité, NIS2 cherche à minimiser ce risque, assurant ainsi la continuité des opérations médicales même en situation de crise.

LE RÔLE DU RGPD DANS LE SECTEUR DE LA SANTÉ

Parallèlement, le RGPD joue un rôle crucial en régulant la gestion des données personnelles et sensibles. Il met l'accent sur le consentement des patients, la transparence des processus de collecte et de traitement des données, et la mise en œuvre de mesures de sécurité adéquates pour prévenir les fuites de données. Il oblige également les établissements à notifier rapidement les autorités de toute violation de données, ce qui permet une réponse et une résolution plus rapides des incidents.

SYNERGIE ENTRE NIS2 ET LE RGPD

L'interaction entre NIS2 et le RGPD crée un cadre robuste pour la cybersécurité et la protection des données dans le secteur de la santé. Alors que NIS2 se concentre sur la sécurisation des infrastructures et la prévention des cyberattaques, le RGPD complète ces efforts en assurant la protection des données individuelles. Ensemble, ils forment un bouclier contre les risques émergents dans un paysage numérique en constante évolution, où les nouvelles technologies médicales et les méthodes de traitement s'appuient de plus en plus sur des données numériques.

Les amendes pour les entités essentielles s'élèvent à

10M €

ou 2% du CA annuel mondial.

Les amendes pour les entités importantes s'élèvent à

7M €

ou 1,4% au moins du CA annuel mondial.

Chapitre 3

Problèmes courants lors de la mise en place d'un plan de cybersécurité

Les établissements de santé font face à de nombreux défis lorsqu'ils tentent de mettre en œuvre un plan de cybersécurité efficace. Les spécificités de ce secteur rendent cette tâche particulièrement complexe, nécessitant une expertise approfondie et une connaissance fine des applications métiers et des infrastructures techniques. Nos équipes de sécurité ESET, avec plus de 20 ans d'expérience dans ce domaine, offrent des conseils et un accompagnement personnalisé pour garantir une transition en douceur vers un environnement sécurisé. Voici quelques-uns des problèmes couramment rencontrés et les solutions que nous proposons.

Pour diverses raisons bien que parfois légitimes, **plus de 20% des postes de travail utilisent des systèmes d'exploitation non mis à jour.**

CONSERVER LES APPLICATIONS MÉTIERS FONCTIONNELLES

Un des principaux défis est de maintenir les applications métiers fonctionnelles tout en renforçant la sécurité. Dans les hôpitaux, certaines applications sont essentielles au bon fonctionnement des services et ne peuvent être interrompues. Chaque application a ses propres exigences et contraintes, et il est crucial de les identifier lors de la phase de découverte. Il est primordial d'être en relation avec des équipes de sécurité qui possèdent l'expertise nécessaire pour analyser ces applications et fournir des ajustements de politiques adaptés, garantissant leur bon fonctionnement tout en renforçant la sécurité.

PROBLÈMES DE MISES À JOUR DES SYSTÈMES D'EXPLOITATION

Les hôpitaux utilisent souvent des machines critiques pour la chaîne de production médicale qui fonctionnent sur des systèmes d'exploitation obsolètes. Ces machines sont difficiles à mettre à jour sans risquer de perturber les services comme les systèmes de gestion des stocks de médicaments ou encore les équipements d'imagerie médicale comme les scanners et IRM. Pour ces équipements, il est également très important d'être en relation avec des équipes de sécurité qui fournissent des recommandations spécifiques visant à maximiser la sécurité sans compromettre leur fonctionnement. Nous proposons des stratégies de contournement pour sécuriser les machines non mises à jour, telles que l'isolement réseau, l'utilisation de pare-feu locaux, et la segmentation réseau.

ÉQUIPEMENTS MÉDICAUX CRITIQUES

Les hôpitaux sont confrontés à des défis uniques en matière de cybersécurité, en particulier avec certains équipements médicaux critiques comme les scanners ou les IRM, où l'installation de logiciels supplémentaires, y compris des solutions de sécurité, est souvent complexe. Ces dispositifs, bien qu'essentiels pour les soins aux patients, fonctionnent sur des systèmes propriétaires ou des versions obsolètes de logiciels qui ne peuvent être modifiés sans risque de compromettre leur fonctionnement. Cela crée des vulnérabilités exploitables par des cyberattaques, et complique la tâche des équipes informatiques qui doivent protéger l'ensemble du réseau sans pouvoir directement sécuriser certains équipements médicaux.

Chapitre 4

Quelle stratégie de défense adopter ?

Les hôpitaux deviennent des cibles de plus en plus fréquentes pour les cyberattaques, c'est pourquoi adopter une stratégie de cybersécurité multicouche est indispensable. Cette stratégie doit intégrer des technologies de pointe, des politiques de gestion des risques rigoureuses, et un engagement profond envers la formation et la sensibilisation du personnel.

ÉVALUATION DES RISQUES ET PLANIFICATION STRATÉGIQUE

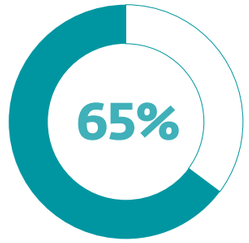
La première étape cruciale consiste en une évaluation des risques exhaustive et récurrente. Cela permet d'identifier les vulnérabilités au sein des systèmes informatiques et des processus opérationnels de l'hôpital. En analysant les menaces potentielles, les hôpitaux peuvent prioriser les risques et développer des plans de réponse aux incidents sur mesure. Cette planification stratégique doit également inclure la préparation à des scénarios de crise divers, en anticipant les types d'attaques qui pourraient survenir et en déterminant les réponses les plus efficaces pour chaque situation possible.

FORMATION ET SENSIBILISATION DU PERSONNEL ÉLARGIE

Une composante souvent sous-estimée mais vitale de la cybersécurité dans les hôpitaux est la formation et la sensibilisation du personnel. Les employés de tous niveaux doivent comprendre les risques de cybersécurité spécifiques à leur environnement de travail, y compris les méthodes courantes utilisées par les cybercriminels comme le phishing et le social engineering. La formation doit être régulière et adaptée aux évolutions des menaces. Elle devrait également inclure des simulations d'attaques pour mieux préparer le personnel à identifier et réagir correctement aux tentatives de sécurité.

RENFORCEMENT DES RÉSEAUX ET DES SYSTÈMES MÉDICAUX

La sécurisation des réseaux et des dispositifs médicaux nécessite l'installation de pare-feu avancés et de systèmes de détection et de prévention des intrusions. Le chiffrement des données en transit et au repos est également crucial pour protéger les informations sensibles. De plus, avec l'augmentation des dispositifs médicaux connectés, il est impératif d'implémenter des mesures de sécurité robustes pour ces appareils, souvent négligés, bien qu'ils constituent un point d'entrée potentiel pour les cyberattaques.



des entreprises victimes d'une cyberattaque ont subi un impact négatif sur leur activité.

GESTION DES ACCÈS ET SURVEILLANCE CONTINUE

Mettre en œuvre une politique de moindre privilège est essentiel pour minimiser les risques d'accès non autorisé aux systèmes critiques. Cela signifie que l'accès est limité strictement aux ressources nécessaires pour que les utilisateurs accomplissent leurs tâches. Une surveillance continue des réseaux est également cruciale pour détecter et répondre rapidement aux activités suspectes ou aux tentatives d'intrusion.

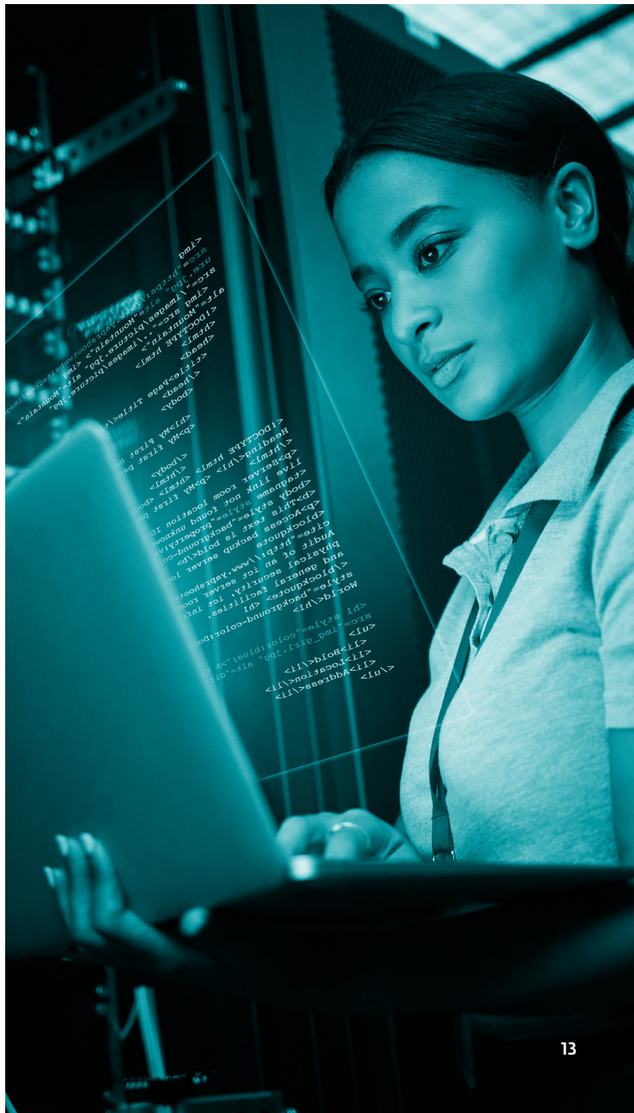
COLLABORATION SECTORIELLE ET RÉPONSE AUX INCIDENTS

Participer à des initiatives de partage d'informations sur les menaces avec d'autres organisations dans le secteur de la santé est vital pour rester informé des dernières tactiques des adversaires. De même, un plan de réponse aux incidents bien défini doit être prêt à être déployé, incluant des procédures claires pour la notification des incidents, l'analyse des brèches, la mitigation des dommages et les étapes de récupération.

En somme, une stratégie de cybersécurité efficace pour les hôpitaux est une combinaison de préparation technologique, de formation continue, de politiques de gestion des risques strictes, et d'une collaboration étroite au sein du secteur. Ce n'est qu'en intégrant tous ces éléments que les hôpitaux peuvent espérer se protéger efficacement contre les cyberattaques de plus en plus sophistiquées.

MAINTENANCE, MISES À JOUR ET SAUVEGARDES

La maintenance régulière des systèmes, y compris les mises à jour des logiciels et des dispositifs médicaux, est essentielle pour corriger les vulnérabilités connues et améliorer les défenses. Parallèlement, une stratégie de sauvegarde robuste et sécurisée doit être en place pour assurer la récupération des données en cas d'attaque, minimisant ainsi les interruptions des services médicaux vitaux.



Chapitre 5

Pertinence des solutions ESET pour le secteur de la santé

Dans le secteur de la santé, où la sécurité des données patient et la continuité des soins sont primordiales, ESET propose des solutions de cybersécurité conçues pour répondre efficacement à ces exigences critiques. Ces solutions sont fondées sur une approche multicouche de la protection, qui englobe la prévention contre les malwares, les ransomwares, le phishing et les attaques par script. Cette méthode complète est essentielle pour les établissements de santé qui gèrent une multitude de données sensibles et d'appareils connectés, nécessitant une protection robuste et fiable.

CERTIFICATION HDS

ESET n'est pas directement soumis à la certification HDS (Hébergeur de Données de Santé), car ses solutions de cybersécurité ne traitent pas ou n'hébergent pas de données de santé. Toutefois, nos solutions opèrent dans des environnements certifiés HDS, comme ceux hébergés sur des plateformes Cloud telles qu'Azure, qui répondent aux exigences strictes de cette certification. Cela garantit que les organisations de santé utilisant ESET bénéficient d'une protection optimale des données tout en étant conformes aux réglementations en vigueur. En résumé, bien qu'ESET n'ait pas besoin d'être certifié HDS, nos partenaires d'hébergement le sont, assurant ainsi une sécurité totale pour les données sensibles.

PERFORMANCE ET LÉGÈRETÉ DES SOLUTIONS

Les solutions d'ESET sont particulièrement appréciées dans les environnements médicaux pour leur performance et légèreté. Elles minimisent l'impact sur les performances des systèmes informatiques et des appareils médicaux critiques, garantissant ainsi la continuité des opérations de santé sans compromettre la sécurité ni la rapidité des services. Cette légèreté est cruciale dans des situations où chaque seconde compte, comme dans le traitement des urgences ou la gestion des soins aux patients chroniques.

GESTION CENTRALISÉE DE LA SÉCURITÉ

La plateforme de gestion de la sécurité d'ESET assure une supervision centralisée, simplifiant la protection d'un réseau étendu d'appareils et de postes de travail dans les hôpitaux et les cliniques. Cette gestion centralisée est vitale pour les administrateurs de systèmes de santé qui doivent assurer une vigilance constante et réagir rapidement à toute menace potentielle, garantissant une protection homogène sur l'ensemble de l'organisation.

SOLUTIONS SPÉCIALISÉES ET SUPPORT CONTINU

ESET offre également des solutions spécialisées pour les environnements de santé, y compris des protections spécifiques pour les serveurs de fichiers et les terminaux, ainsi que des mesures contre les attaques ciblées. De plus, ESET comprend l'importance du support technique et de la formation en cybersécurité, offrant ainsi un accompagnement expert et des ressources éducatives pour aider le personnel de santé à comprendre et à combattre efficacement les cybermenaces.

Conformité réglementaire et protection des données

En plus de répondre aux normes réglementaires strictes telles que le RGPD en Europe et la HIPAA aux États-Unis, les solutions d'ESET aident les établissements de santé à se conformer à la directive NIS2 de l'Union européenne. Cette directive vise à améliorer la résilience des infrastructures nationales critiques, y compris dans le secteur de la santé. ESET facilite cette conformité en offrant des outils de chiffrement et des mécanismes de protection des données qui répondent non seulement aux exigences de sécurité mais aussi aux obligations légales, minimisant ainsi les risques de sanctions et de violations de données.

Découvrez les offres ESET >

Quels produits sont réellement adaptés au secteur de la santé ?

ESET propose des solutions hautement spécialisées pour les environnements de santé, adaptées aux besoins spécifiques de ce secteur. Les protections proposées englobent les serveurs de fichiers et les endpoints, assurant une défense efficace contre les attaques ciblées menaçant les infrastructures critiques de santé. En plus de ces mesures de sécurité robustes, ESET a développé des produits spécialement conçus pour offrir une sécurité maximale dans les environnements de santé, tels que ESET PROTECT Elite et ESET PROTECT MDR.

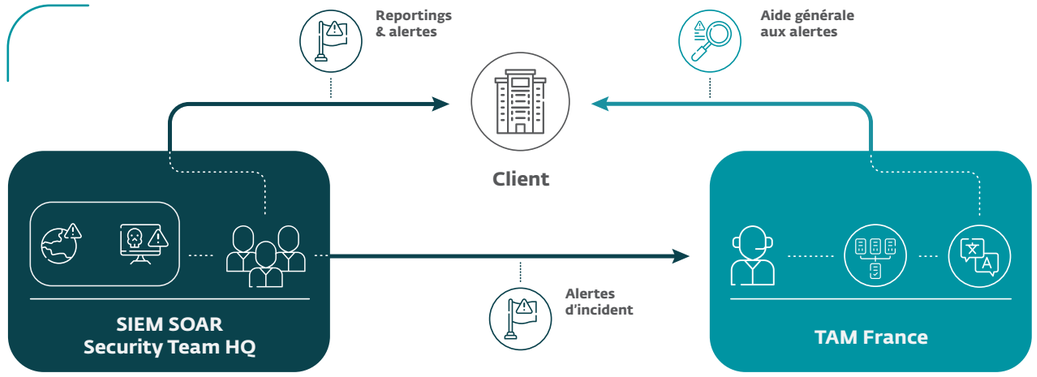
ESET 100% Made in EU IT-Security

	ESET PROTECT ELITE	ESET PROTECT MDR
Console de gestion	●	●
Protection des endpoints, serveurs et mobiles	●	●
Chiffrement des données	●	●
Extended Detection & Response (XDR)	●	●
Scanner des vulnérabilités et gestion des correctifs	●	●
Protection des serveurs de messagerie, Microsoft 365 et Google Workspace	●	●
Authentification multifacteur	●	●
Managed Detection & Response (MDR)		●
Support Premium		●

EXPERTISE ET ACCOMPAGNEMENT PERSONNALISÉS

Forts de notre expertise de plus de 20 ans dans le secteur de la santé, chez ESET France, nous comprenons les besoins uniques des établissements médicaux. Nous offrons un conseil personnalisé qui inclut l'analyse des infrastructures existantes et des recommandations sur mesure. Notre accompagnement continu garantit un support technique et des ajustements réguliers des politiques de sécurité. De plus, nous assurons la formation des équipes en sensibilisant et en formant le personnel aux bonnes pratiques de cybersécurité.

La mise en place d'un plan de cybersécurité dans les hôpitaux présente donc des défis uniques qui nécessitent une expertise spécialisée. Les équipes de sécurité ESET sont parfaitement équipées pour offrir les solutions et l'accompagnement nécessaires à la sécurisation des infrastructures tout en garantissant le bon fonctionnement des applications métiers critiques. Nous nous engageons à travailler en étroite collaboration avec les établissements de santé pour assurer une transition vers un environnement plus sûr et plus résilient.



Technical Account Manager for ESET MDR

Le service Technical Account Manager for ESET MDR assure un suivi personnalisé avec un ingénieur technique dédié, expert certifié en outils EDR/XDR ESET. Ce dernier analyse les incidents générés par le service MDR, fournit des explications claires et propose des optimisations et des réglages spécifiques lors de l'accompagnement à la résolution des problématiques de sécurité. En plus de vous accompagner sur les incidents, l'ingénieur offre des conseils stratégiques pour renforcer l'efficacité des solutions déployées.

Témoignages

Grâce au plan France Relance et au parcours de cybersécurité de l'ANSSI, le Grand Hôpital Est Francilien (GHEF) a pu financer à 70 % son audit de sécurité ainsi que la mise en place d'un SOC, d'un SIEM managés et de l'EDR d'ESET. L'accompagnement du fournisseur a permis un déploiement rapide et efficace.

Fusion, en une seule entité juridique, des CH de Meaux, de Marne la Vallée et de Coulommiers en 2017, puis du CH de Jouarre en 2019, le Grand Hôpital Est Francilien (GHEF) emploie plus de 6000 professionnels, dont plus de 800 médecins, des personnels paramédicaux, administratifs et techniques, pour une capacité de 2076 lits et places, et son SI compte une trentaine de personnes réparties sur 3 sites.

L'aubaine du plan France Relance

Après la fusion, de nombreuses applications ont été centralisées dans le datacenter, bien que certains outils historiques aient été conservés localement. « *La multiplication des cyberattaques imposait de lever notre niveau de sécurité, mais le budget manquait* », explique Agnès Pignolet, RSSI du GHEF. Le plan France Relance a permis de financer un audit des 4 sites et de définir un schéma directeur sur trois ans. « *Il a aussi sensibilisé la direction générale à l'importance de la sécurité pour tous les métiers de l'hôpital* », précise-t-elle.

Un déploiement accéléré en un mois et demi

Après l'audit, le GHEF a rapidement mis en œuvre un SOC, un SIEM managé, et un EDR avec l'appui d'ESET. « *La migration de 90 % des endpoints a été réalisée en deux semaines grâce aux scripts fournis par ESET* », souligne Mme Pignolet. Les modules d'ESET ont été préférés pour leur compatibilité avec Windows 7, contrairement à d'autres solutions. Benoît Grunemwald, expert ESET, ajoute : « *Bien préparer un POC permet de limiter les imprévus lors du déploiement.*»

Vers une surveillance proactive

La RSSI apprécie la légèreté de la solution et son tableau de bord complet, qui offre une visibilité sur les menaces et l'inventaire matériel. « *Nous explorons maintenant les politiques et règles de remédiation en direct* », conclut-elle, soulagée de ne plus gérer la supervision opérationnelle. M. Grunemwald insiste sur l'importance du suivi, notamment pour protéger les accès via le cloud, les objets connectés et les instruments hospitaliers.

Mag TIH
mars 2023

ESET accompagne d'autres organismes

« ESET protège les 85 000 ordinateurs de la Gendarmerie Nationale, dont 77 000 sous Linux[…] ESET a gagné notre confiance. »

Chef d'escadron Olivier MARI,
Chef de la section de la sécurité en profondeur du ST(SI)2.
100 000 endpoints protégés

« Le déploiement s'est fait sur la totalité du parc en une demi-journée. Nous n'avons eu aucun problème, que ce soit sur la partie serveurs ou endpoints. L'ajout de l'EDR a permis de voir le comportement des machines et des utilisateurs, ce qu'on n'identifiait pas avant. »

Bastien V., RSSI,
Brigade des Sapeurs Pompiers de Paris4.
300 endpoints protégés

Chapitre 6

Aspects financiers des solutions ESET

L'aspect financier joue un rôle primordial, surtout dans un contexte où les budgets peuvent être contraints. Conscient de cette réalité, ESET a développé une grille tarifaire spécialement conçue pour répondre aux besoins des établissements de santé publiques. Cette structure tarifaire offre des prix avantageux, permettant aux hôpitaux, cliniques et autres institutions publiques d'accéder à des solutions de sécurité de pointe sans compromettre leur santé financière.

ÉQUILIBRE ENTRE SÉCURITÉ ET GESTION BUDGÉTAIRE

Les tarifs réduits proposés par ESET sont particulièrement bénéfiques pour les établissements de santé qui doivent jongler entre le besoin impérieux de protéger les données sensibles des patients et la gestion efficace de ressources souvent limitées. En offrant des coûts ajustés, ESET aide ces institutions à investir dans une protection robuste tout en préservant leurs capacités à allouer des fonds à d'autres aspects critiques des soins de santé, comme l'achat de nouveaux équipements médicaux ou le financement de programmes de recherche.

UNE SOLUTION DURABLE POUR LE SECTEUR DE LA SANTÉ

De plus, ESET s'engage à fournir non seulement des tarifs compétitifs mais aussi un retour sur investissement significatif grâce à la réduction des risques de cyberattaques et des coûts associés aux violations de données, telles que les amendes pour non-conformité et les coûts de réparation des systèmes endommagés. Cette approche économique et stratégique permet aux établissements de santé de maintenir un équilibre entre la sécurité et la gestion financière prudente, assurant ainsi une opérabilité continue et une protection optimale des informations de santé critiques.

En conclusion, la grille tarifaire d'ESET, spécifiquement adaptée au secteur de la santé publique, est un élément clé qui permet aux institutions de santé d'adopter des solutions de cybersécurité avancées tout en gérant efficacement leurs budgets. Cela représente un avantage considérable dans un secteur où la valeur de chaque euro doit être maximisée pour améliorer la qualité des soins et la sécurité des patients.

« Les tarifs réduits proposés par ESET sont particulièrement bénéfiques pour les établissements de santé qui doivent jongler entre le besoin impérieux de protéger les données sensibles des patients et la gestion efficace de ressources. »

Conclusion

La protection du secteur de la santé contre les cybermenaces est plus qu'une nécessité technique, c'est une obligation éthique et légale qui garantit la sécurité des patients et la continuité des soins de santé. À travers ce livre blanc, nous avons analysé les nombreux défis de la cybersécurité dans ce secteur essentiel, en mettant en avant l'importance d'une stratégie de protection robuste et multicouche, adaptée aux exigences spécifiques des établissements de santé.

Nous avons examiné comment les cyberattaques représentent une menace imminente pour la sécurité des données sensibles des patients et la fonctionnalité opérationnelle des hôpitaux. Ces institutions ne se contentent pas de traiter des données ; elles sauvent des vies, rendant impératif le maintien de systèmes sécurisés et fiables.

En réponse à ces défis, des règlementations tels que NIS2 et le RGPD en Europe ont été mis en place pour renforcer la posture de sécurité des établissements de santé, exigeant de ces derniers qu'ils prennent des mesures préventives et réactives face aux menaces cybernétiques.

Les solutions de cybersécurité d'ESET, notamment ESET PROTECT Elite et ESET PROTECT MDR, ont été mises en avant comme des réponses efficaces aux exigences complexes de ce secteur. Ces solutions ne se contentent pas de répondre aux besoins de protection contre les malwares, elles facilitent également la gestion centralisée de la sécurité et garantissent la conformité aux normes réglementaires tout en étant économiquement viables grâce à une structure tarifaire adaptée.

À propos d'ESET

Quand la technologie permet le **progrès**, ESET est là pour le **protéger**.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour offrir une protection complète et multicouche contre les menaces de cybersécurité aux entreprises et aux particuliers du monde entier.

ESET est depuis longtemps un pionnier des technologies de machine learning et dans le Cloud qui préviennent, détectent et traitent les malwares. ESET est une société privée qui encourage la recherche et le développement scientifiques dans le monde entier.

Canon

protégé par ESET depuis 2016
plus de 32 000 endpoints

T · ·

partenaire FAI depuis 2008
2 millions d'utilisateurs

Allianz Suisse

protégé par ESET depuis 2016
plus de 4 000 boîtes mail

MITSUBISHI MOTORS
Drive your Ambition

protégé par ESET depuis 2017
plus de 9 000 endpoints

Plus de 30 ans
d'innovation continue

1er éditeur Européen
de solutions de sécurité

Focus continu
sur la technologie

Croissance continue
depuis sa création

www.eset.com/fr