Case Study

THALES
Building a future we can all trust

CYBERSECURITY

imperva

SDIS 62
Aider à protéger les applications et données critiques afin d'assurer la sécurité des citoyens avec Thales Imperva Cloud WAF

THALES
Building a future we can all trust

CYBERSECURITY

à propos de SDIS 62

Le Service Départemental d'Incendie et de Secours du Pas-de-Calais (SDIS 62), le 4e de France, est un établissement public français bien connu qui regroupe plus de 5000 agents (3000 à 3500 sapeurs-pompiers volontaires, 1400 sapeurs-pompiers professionnels et 300 personnels administratifs et techniques). Sa mission inclut l'évaluation et la prévention de tous types de risques de sécurité civile, tels que les accidents, les catastrophes technologiques et naturelles, et la préparation des mesures d'intervention d'urgence. Le SDIS est également responsable de l'organisation des ressources de secours, de la lutte contre les incendies, de l' assistance d'urgence aux individus et de la protection des personnes, des biens, et de l'environnement. Leur travail s'articule autour de trois fonctions clés : la prévention, la prévision et les opérations.

Défis

Un WAF dépassé et une surface d'attaque exposée mettent en danger les données critiques et la sécurité des citoyens

En tant qu'organisation de sécurité publique, le SDIS 62 doit maintenir à la fois la disponibilité et la sécurité des systèmes qui contribuent aux réponses d'urgence rapide. L'équipe travaille dans un environnement informatique centralisé et les interruptions de service pourraient sérieusement compromettre les opérations de secours.

Le SDIS 62 s'appuyait auparavant sur un WAF on-premise mais manquait de visibilité et de contrôle, mais aussi peinait à garantir des mises à jour pour des applications tierces spécifiques, laissant des CVE connus non corrigés. Avec 32 adresses IP publiques hébergeant diverses applications, le SDIS 62 se devait d'améliorer leur protection.

« Si nos systèmes tombaient en panne, nous ne pourrions plus coordonner les services d'urgence, car notre système centralisé gère 50 casernes de pompiers, » déclare Romuald Delattre, Chef du Groupement des Systèmes d'Information, Réseaux et Télécommunications.

Le WAF existant ne pouvait pas efficacement bloquer le trafic illégitime ni filtrer les connexions par géographie. L'équipe du SDIS 62 l'avait configuré pour bloquer les IP non françaises mais il continuait à bloquer des utilisateurs légitimes.

Déploiement

Imperva Cloud WAF : un déploiement simple en interne pour sécuriser l'infrastructure exposée au public

Après avoir évalué des solutions alternatives, le SDIS 62 a choisi Imperva Cloud WAF pour sa capacité à éliminer l'exposition des IP publiques et à filtrer le trafic malveillant avant qu'il n'atteigne les systèmes internes.

« Nous avons redirigé tout le trafic via Imperva Cloud WAF, qui sécurise désormais notre infrastructure de bout en bout ; le trafic ne nous parvient plus directement, » a déclaré Romuald Delattre. « Que ce soit des attaques DDoS, des botnets, des abus d'API, ou des tentatives de SQL injection... depuis que nous avons mis en place cette solution, nous pouvons maintenant dormir sur nos deux oreilles. »

Imperva Cloud WAF bloque les attaques avec des faux positifs quasi nuls, utilisant un SOC global pour renforcer les protections de l'organisation contre les dernières attaques quelques minutes après leur découverte. Imperva Cloud WAF fait partie d'une solution de sécurité des applications multicouche qui combine une protection avancée contre les bots, des API et contre les attaques DDoS, le tout à partir d'une console de management unifiée.

Grâce au soutien de Thales, le déploiement a été réalisé très facilement par l'équipe informatique interne. Les démonstrations techniques et la disponibilité constante de l'équipe Thales ont renforcé la confiance tout au long de la transition. Accompagné par un transfert de compétences assuré par Thales, Sofian Saïd, Adjoint

Service Départemental d'Incendie et de Secours du Pas-de-Calais
SDIS62
Sapeurs-Pompiers

Secteur d'activité :
Service départemental d'incendie et de secours

Localisation :
Saint-Laurent-Blangy, France

Site web :
www.sdis62.fr

au Chef du Groupement des Systèmes d'Information, Réseaux et Télécommunications du Service Départemental d'Incendie et de Secours (SDIS 62), basé à Saint-Laurent-Blangy, a pu reproduire le processus dans chaque service, sécurisant progressivement les 32 adresses IP publiques en seulement 15 jours.

« Nous étions un peu anxieux car il y a des services critiques qui sont en jeu, mais tout est automatisé avec Thales, ce qui nous a permis de prendre le contrôle de notre DNS public et de rediriger le trafic en seulement deux clics, » a déclaré Sofian Saïd. « Honnêtement, c'était très impressionnant. »

Résultats

Une exposition réduite et une visibilité accrue pour sécuriser les données critiques et contribuer à la sécurité des citoyens

Le SDIS 62 bénéficie désormais d'une surface d'attaque réduite, d'une meilleure visibilité et d'une plus grande tranquillité d'esprit. La fonctionnalité de géofiltrage à elle seule a conduit à une diminution des menaces entrantes. Le tableau de bord intuitif permet désormais à l'équipe de visualiser les données de sécurité et de présenter des statistiques en temps réel à la direction.

« Avant, nous n'avions ni données, ni graphiques, ni possibilité de personnaliser les informations. Désormais, je peux présenter comité de direction des chiffres clairs, des statistiques et des visuels. Par exemple, je leur demande : "D'après vous, combien d'attaques nos systèmes de sécurité bloquent chaque jour ou chaque semaine ?" Puis je leur montre les données. Leur réaction est souvent : "Wow, autant ? C'est sur un mois ?" Et je réponds : "Non, c'est en une seule journée !" », raconte Sofian.

D'un point de vue opérationnel, Imperva Cloud WAF a réduit les frictions pour les utilisateurs. « Au-delà de la gestion des incidents de sécurité, cela a vraiment allégé ma charge de travail, » confie Sofian. « La précédente fonctionnalité de géofiltrage n'était très efficace. Maintenant, Thales fait exactement ce que nous lui demandons. Ses bases de données sont mises à jour en temps réel, ce qui est complètement transparent pour nous, et qui rend la gestion beaucoup plus facile. »

Imperva Cloud WAF aide le SDIS 62 à rester conforme tout en se développant de manière sécurisée. « Dire aujourd'hui que vous avez réduit, voire éliminé, votre surface d'attaque externe n'est pas un luxe, » déclare Romuald. « Eviter toutes les attaques externes grâce à Imperva Cloud WAF rassure les équipes. Étant donné les gains en sécurité et en tranquillité d'esprit, j'encourage l'investissement dans la solution Imperva Cloud WAF, car cela en vaut absolument la peine. Le retour sur investissement sera significatif. »

> « Que ce soit des attaques DDoS, des botnets, des abus d'API ou des tentatives de SQL injection... depuis que nous avons mis en place [Imperva Cloud WAF], nous pouvons dormir sur nos deux oreilles. »
>
> – **Romuald Delattre, Chef du Groupement des Systèmes d'Information, Réseaux et Télécommunications - SDIS 62**

À propos de Thalès

Thales est un leader mondial de la cybersécurité, aidant les organisations les plus fiables à protéger leurs applications, données, identités et logiciels critiques, partout et à grande échelle. Grâce aux plateformes intégrées de Thales, nos clients bénéficient d'une meilleure visibilité des risques, se protègent contre les cybermenaces, comblent les failles de conformité et offrent chaque jour des expériences numériques fiables à des milliards de consommateurs.

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us