

Assurer le succès des missions de service public

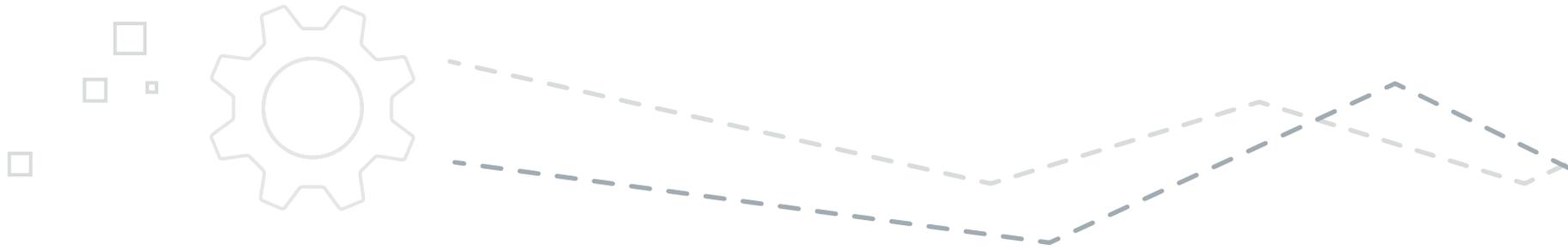
Les organismes gouvernementaux
visionnaires mobilisent les données
dans toutes leurs actions



splunk>
turn data into doing™



Introduction.....	2
La mission : protéger, servir, moderniser	3
Comment nos clients exploitent les données	5
• Le National Ignition Facility au Laboratoire National Lawrence Livermore	5
• La ville de Gold Coast	5
• Le District scolaire du comté de Jefferson.....	5
• Le bureau du recensement des États-Unis.....	6
Organismes axés sur les missions de service public	7
• La Banque d'Angleterre.....	9
• La ville de Gold Coast	10
• La ville de Los Angeles	11
• Les aéroports de Dubaï.....	12
• Le comté de Fairfax.....	13
• Le centre de transport maritime de Hong-Kong	14
• Les écoles publiques du Comté de Jefferson	15
• Leidos.....	16
• L'instance de contrôle des jeux et loteries du Maryland.....	17
• Le National Ignition Facility.....	18
• Les organismes régionaux d'éducation de New York.....	19
• Le cadre « NHS Choices »	20
• Le comté de Prince George	21
• Le Royal flying doctor service	22
• Le bureau du Shérif du Comté de Sacramento.....	23
• Saic.....	24
• Les Laboratoires Sandia.....	25
• L'état de Louisiane.....	26
• Le Ministère de la santé et des services sociaux de l'état du Michigan.....	27
• Le U.S. Census Bureau.....	28
Réussir ensemble les missions de service public.....	29



Les technologies numériques

promettent de transformer la façon dont les agences gouvernementales peuvent accomplir leur mission consistant à servir plus efficacement l'intérêt public. Cependant, l'exploration de nouvelles voies numériques pose également de nouveaux défis. Le secteur public doit trouver de nouveaux moyens de travailler avec de grands volumes de données et de les sécuriser dans un monde où la cybercriminalité et les menaces des États-nations sont en hausse.

Les environnements informatiques des organismes du secteur public sont de plus en plus complexes. La combinaison de plusieurs années d'adoption de nouvelles technologies et de maintien des infrastructures existantes a créé un certain désordre, parsemé de systèmes et d'applications disparates. Cela rend d'autant plus difficile la réussite des missions de service public. En outre, leur échec peut conduire à bon nombre de conséquences, telles que l'insatisfaction des citoyens, la surveillance accrue, les enquêtes réglementaires, les résultats sous-optimaux et l'atteinte à la réputation de l'organisme en question.

Qu'il s'agisse de protéger une nation ou de fournir des services aux citoyens, la réussite d'une mission d'intérêt public nécessite une prise de décision efficace et éclairée. Les dirigeants des organismes publics doivent prendre un nombre croissant de décisions, plus rapidement que jamais. Chaque décision dans notre monde moderne et hyperconnecté est de plus en plus déterminante, avec une marge d'erreur de plus en plus réduite.

Splunk est la plateforme Data-to-Everything qui fournit des informations en temps réel, oriente des décisions informées et permet des actions décisives à la vitesse exigée par la mission. Elle permet aux organismes du secteur public de tirer parti et d'extraire de la valeur réelle de leurs données, indépendamment de la source, de la durée ou de la structure. Cela améliore considérablement le potentiel de réussite de la mission de service public tout en réduisant le coût total de propriété et en augmentant le retour sur investissement.

Les technologies numériques deviennent de plus en plus sophistiquées, les attentes des citoyens augmentent et les données elles-mêmes deviennent plus complexes. Par conséquent, des centaines d'organismes publics, des services municipaux jusqu'au gouvernement national, utilisent la plateforme Splunk pour relever tous les défis liés aux données tout en travaillant afin de mieux protéger notre infrastructure critique, de servir les citoyens, de moderniser les opérations informatiques et d'atteindre les objectifs de leurs missions d'intérêt public.

La mission :

Protéger, servir, moderniser



Pour les organismes du secteur public, la réussite ne se mesure pas en termes de résultats financiers. La mission est noble : assurer le bien-être et la protection des citoyens, promouvoir et maintenir la paix et les bonnes relations dans le monde, et assurer une gestion efficace des ressources publiques. Pour promouvoir leurs différentes missions, les organismes d'intérêt public doivent veiller à offrir les meilleures expériences possibles grâce à des infrastructures modernes et efficaces, tout en protégeant ces systèmes et ces données de tout dommage.

Protéger

La cybersécurité est l'un des plus grands défis auxquels nous sommes confrontés aujourd'hui, compte tenu des menaces croissantes des États-nations et des cybercriminels déterminés à infliger un maximum de dommages. Parallèlement, les menaces internes malveillantes et involontaires augmentent. Un solide dispositif de sécurité et un environnement opérationnel résistant sont essentiels à la réussite des missions des organismes du secteur public.

Servir

Le travail de chaque organisme gouvernemental étant directement lié à l'intérêt du citoyen, une grande partie de la réussite de la mission de service public consiste à garantir que l'expérience du citoyen est satisfaisante et que le processus de livraison est efficace. Pourtant, le concept d'« expérience utilisateur positive » est une cible mouvante. En effet, les applications et les appareils destinés aux consommateurs sont constamment améliorés, ce qui augmente régulièrement les attentes. Les informations en temps réel fournies par la plateforme Splunk garantissent des services en temps opportun et qui répondent aux besoins des citoyens.

Moderniser

Les organismes publics doivent transformer fondamentalement leur fonctionnement. Cette évolution comprend la recherche d'une efficacité accrue, d'une sécurité renforcée, de processus améliorés et d'un niveau de satisfaction élevé des citoyens. Dans le même temps, les organismes sont chargés de maintenir la responsabilité, la transparence et la conformité. Les grands défis d'une telle modernisation transformatrice s'étendent aux centres de données existants, à la migration vers le cloud, au déploiement de services partagés, et bien plus encore. Les données se trouvent au cœur de chaque modernisation.

Splunk aide les clients du secteur public à améliorer les résultats de leur mission, à utiliser efficacement un budget toujours plus limité, à protéger les atouts essentiels et à favoriser la modernisation. Notre approche, qui consiste en une plateforme unique incluant toutes les données, permet aux organismes publics de tirer le meilleur parti de leur investissement tout en réduisant les tâches banales et répétitives. Le personnel à tous les niveaux est habilité à améliorer chaque décision et chaque action grâce aux données.

Voici comment certains de nos clients exploitent les données avec Splunk afin d'accomplir leurs missions.

Réussite stratégique :

Le National Ignition Facility au Laboratoire national Lawrence Livermore

Le National Ignition Facility (NIF) est une unité au sein du Laboratoire national Lawrence Livermore en Californie du Nord. Cette installation de premier ordre est engagée dans trois missions principales : la gestion de l'arsenal nucléaire américain grâce à des essais souterrains sûrs et fiables, l'expérimentation en astrophysique pour renforcer l'avantage concurrentiel du pays dans les efforts scientifiques, et l'exploration du seuil d'ignition, qui pourrait potentiellement libérer une source d'énergie propre et sans carbone. Pour soutenir et promouvoir ces missions, les scientifiques et les ingénieurs ont besoin d'une infrastructure informatique sécurisée et fiable.

« Les données sont essentielles à notre niveau d'apprentissage et à nos progrès sur les questions complexes que nous essayons de comprendre au NIF » a déclaré Bruno Van Wonterghem, le directeur des opérations de l'installation.

Splunk a aidé le NIF à exploiter au maximum la disponibilité du système et à améliorer la fiabilité de l'infrastructure informatique, notamment en améliorant la performance de plus de 66 000 appareils IoT ou en garantissant le fonctionnement précis du plus grand laser du monde.

« Les scientifiques s'attendent à ce que les données soient exactes et livrées rapidement. En effet, elles sont utilisées dans d'autres expériences ainsi que pour faire avancer leur carrière scientifique » explique Philip Adams, le directeur technique du NIF. Il ajoute : « Par conséquent, nous devons veiller à prendre des décisions avec les données correctes pour résoudre efficacement tous les problèmes qui pourraient affecter la prochaine expérience scientifique. »

Grâce à Splunk, le NIF a amélioré la fiabilité des systèmes de contrôle et exploité au maximum les opérations en laboratoire. Splunk a permis aux scientifiques de doubler le nombre d'expériences laser de 200 à 400 par an en optimisant le retour sur investissement non seulement sur la plateforme Splunk, mais aussi dans l'ensemble du travail scientifique de l'installation.

Médaille d'or de la sécurité :

La ville de Gold Coast

Lorsque la **ville de Gold Coast** a accueilli les Jeux du Commonwealth en 2018, la sécurité a été placée à un rang élevé de priorité, parmi de nombreux autres défis inhérents à l'accueil de plus de 4 400 athlètes de 71 pays, ainsi que de milliers d'autres touristes et spectateurs. (Plus d'un million de billets ont été vendus pour les différents événements.) Dans ce contexte, la ville australienne a dû améliorer son niveau de jeu, en particulier en matière de sécurité. La ville de Gold Coast devait agir de façon coordonnée avec les partenaires locaux, étatiques et fédéraux pour atténuer les cyber-risques, ainsi que pour protéger les infrastructures et la sécurité publique dans toute la ville et les sites sportifs.

Splunk a aidé la ville à surmonter les défis en matière de visibilité de l'exécution de plusieurs systèmes de sécurité. « Nous manquions de visibilité sur plusieurs environnements » explique Matthew Walker, un conseiller en sécurité informatique de la ville. « Nous avons besoin d'une solution capable de consolider et d'intégrer plusieurs types d'environnement, tels que des systèmes de contrôle industriel et des systèmes informatiques traditionnels. »

Splunk a permis à Matthew Walker et à ses collègues de superviser plusieurs priorités et profils de menaces dans différents environnements sur une plateforme globale.

Modernisation intelligente :

District scolaire du comté de Jefferson

Le **District scolaire du comté de Jefferson** (Jeffco) de l'État du Colorado a utilisé Splunk pour mettre en œuvre des initiatives ambitieuses de transformation qui prennent en charge l'apprentissage assisté par la technologie du XXI^e siècle. La distribution d'un accès sans fil fiable sur des sites géographiques dispersés a introduit une complexité opérationnelle et des problèmes accrus de sécurité des données, nécessitant une sécurité dans un environnement complexe d'appareils BYOD (Bring Your Own Device) et de dispositifs du district.

Jeffco a fourni une disponibilité sans fil de 99,99 % à 100 000 appareils sur 1 800 km², desservant 86 000 élèves et 15 000 employés sur 156 sites. Grâce à Splunk, Jeffco a amélioré la fiabilité en réduisant le temps moyen de réparation (MTTR) à une demi-heure ou moins.

La plateforme Data-to-Everything de Splunk aide Jeffco à lutter contre la cyber-intimidation ainsi qu'à se protéger contre les tentatives d'hameçonnage et autres menaces externes. Les capacités avancées en matière de données renforcent également la sécurité des écoles en améliorant la sécurité physique.

« Notre plus grand défi était d'offrir la flexibilité à nos enseignants et élèves pour créer du contenu et collaborer de façon innovante, tout en protégeant la sécurité des informations dans notre environnement distribué et complexe » explique Chris Paschke, le directeur de la confidentialité et de la sécurité des données.

La vision d'évolution du district est ambitieuse. Les prochaines étapes incluent l'augmentation de la sécurité, la journalisation des notes des élèves et d'autres données, l'automatisation de plus de processus, et l'amélioration de l'assistance et du dépannage sur le terrain.

Transformation de la décennie : Le Bureau du recensement des États-Unis

Le Bureau du recensement des États-Unis a une mission d'une étonnante complexité : il est le principal fournisseur de données de qualité sur la population et l'économie du pays.

Une fois tous les 10 ans, le Bureau du recensement présente un décompte complet et précis de la population et des logements dans l'ensemble des États-Unis. Cela signifie qu'il faut compter chaque personne, dans chaque coin du pays. Alors que le recensement de 2020 marque le premier recensement numérique du pays, l'organisation utilise la plateforme Splunk pour accomplir plus efficacement sa mission. Celle-ci consiste à façonner les politiques publiques, à distribuer plus de 675 milliards de dollars de financement et à redessiner complètement la carte politique de la prochaine décennie.

Le recensement de 2020 comprend 35 opérations et 52 systèmes, dont les ressources humaines, la paie, et la coordination d'un effort national qui doit

couvrir tous les ménages du pays, notamment les immeubles d'appartements en ville, les chalets ruraux, les prisons et les foyers dans chaque État et territoire américain. Pourtant, grâce à la transformation numérique et à une meilleure gestion des données, l'opération de cette année compte moins de systèmes qu'en 2010. Cela améliorera les performances, la précision et l'efficacité, tout en optimisant l'argent du contribuable.

Splunk rend possible ce projet de données massives de nombreuses façons, avec une dimension numérique plus complexe que jamais. Au départ, Splunk aide le Bureau du recensement à coordonner les listes d'adresses de plusieurs sources, à utiliser les données satellite pour réduire les efforts manuels de porte-à-porte, et à consolider plus efficacement et plus précisément les données de terrain au fur et à mesure de leur arrivée.

Finalement, le recrutement, l'embauche et la rémunération des travailleurs deviennent plus efficaces grâce à l'automatisation et aux workflows numériques de Splunk. Cela résout un problème de taille pour une organisation qui doit embaucher et coordonner 6 000 recenseurs faisant du porte-à-porte pendant plusieurs mois.

Splunk est un partenaire clé du Bureau du recensement, offrant de nombreux services tels que la sécurité, l'infrastructure et les applications. La plateforme Data-to-Everything améliore l'efficacité et garantit l'accès aux données en temps réel.

La capacité à gagner et à maintenir la confiance du public est un élément essentiel de la mission du Bureau du recensement. L'équipe de sécurité du Bureau du recensement dispose de données très sensibles et d'un calendrier serré pour réaliser une opération massive. Elle s'appuie sur Splunk pour identifier de manière proactive les vulnérabilités, isoler et répondre efficacement aux incidents, et se conformer aux politiques de sécurité des données appropriées. En utilisant Splunk pour accomplir des tâches clés telles que l'unification des données sur une seule plateforme, le Bureau du recensement résout plus rapidement les problèmes, gagne en visibilité dans les systèmes et protège les données de leur collection jusqu'à leur transit et leur livraison vers d'autres systèmes.

Missions de service public



```
[cpu] done / done / password found / operation 129 227  
[cpu] negative / negative / [not found] / operation 2289 4  
[cpu] done / negative / error 003  
[cpu] error / error / restart  
[cpu] done / done / access / complete / operation 122 334  
[cpu] error  
[cpu] negative / analyzing / operation 552 390  
[cpu] preparation complete / code xxx000x0xx0x0
```



Splunk, la plateforme Data-to-Everything, aide les organismes du secteur public à mobiliser les données dans chaque aspect de leur travail. Des services municipaux à l'éducation publique, en passant par les soins de santé, la défense, les transports ou encore la recherche scientifique de pointe, Splunk aide les dirigeants des organismes du secteur public à assurer le succès de chacune de leurs missions en prenant rapidement des décisions éclairées et des actions décisives grâce à des informations en temps réel basées sur les données.

Contrairement aux plateformes de données héritées et aux outils cloisonnés de supervision, Splunk offre une plateforme d'analyse rentable, extensible et massivement évolutive qui fournit une visibilité à l'échelle de l'entreprise sur les déploiements de système cloud, sur site et hybrides. Cela permet aux organismes du secteur public de réutiliser les données pour surmonter les défis de programmes distincts et les objectifs des missions.

Dans les pages suivantes, vous découvrirez quelques organismes du secteur public dont nous sommes fiers de soutenir les missions.



La Banque d'Angleterre protège chaque jour 1 trillion de dollars

Fondée en 1694, la Banque d'Angleterre est la banque centrale du Royaume-Uni. Elle facilite des transactions pour un montant d'environ 1 trillion de dollars chaque jour. Le SOC de la Banque d'Angleterre est composé d'une équipe de 10 analystes de sécurité. Il est responsable de la protection de l'infrastructure qui facilite ces transactions, traite un tiers du PIB du pays et est utilisé par 4 200 employés, le tout sur un réseau de 10 000 points de terminaison couvrant les serveurs et les appareils des utilisateurs. Cherchant à évoluer d'un SOC réactif à un SOC proactif, la Banque d'Angleterre a reconnu la nécessité d'un nouveau modèle d'exploitation dans lequel la technologie correspond au modèle, et non l'inverse.

IMPACT SUR L'ACTIVITÉ

- Développement d'analyses pour identifier rapidement les opérations d'attaques sur mesure ;
- Stratégie de défense recadrée, évoluant d'un SOC réactif à un SOC proactif ;
- Habilitation du SOC à recruter des spécialistes de l'analyse de sécurité, plutôt que des ingénieurs système, grâce à la facilité d'utilisation de Splunk.

La nouvelle stratégie de la banque repose sur Splunk pour l'exploration de données à grande échelle, l'analyse des logs, la mise en correspondance des renseignements sur les menaces et les contrôles de prévention. Grâce au développement de recherche rapide et itératif de Splunk, les analystes peuvent développer un grand nombre d'analyses qui offrent plus de flexibilité et d'efficacité dans la détection des attaques. La mise en œuvre de Splunk a également permis au SOC de recadrer sa stratégie de défense, en ciblant les opérations de l'adversaire dans leur cadre MITRE ATT&CK, plutôt que l'attaque elle-même, avec davantage de succès.



La ville de Gold Coast gagne en visibilité en temps réel pour les Jeux du Commonwealth

La ville de Gold Coast, le deuxième plus grand gouvernement local d'Australie, compte 3 900 employés et offre une gamme de services, d'activités et d'installations aux résidents et aux visiteurs. La tenue des Jeux du Commonwealth en 2018 a donné un nouvel élan à la ville en améliorant ses opérations de sécurité et sa visibilité dans l'ensemble de l'organisation. La sécurité de milliers de personnes est un défi majeur pour l'hôte de tout événement sportif. Par conséquent, la ville de Gold Coast a déployé Splunk pour renforcer son dispositif de sécurité.

IMPACT SUR L'ACTIVITÉ

- **Supervision et investigation consolidées pour une meilleure efficacité et sécurité ;**
- **Risque réduit dans un environnement de menace accrue ;**
- **Visibilité en temps réel des événements de sécurité dans différents environnements et systèmes.**

En déployant la plateforme Splunk, la ville de Gold Coast a atténué les cyber-risques. Elle a veillé à la sécurité des participants à l'événement et de la communauté locale. Avec l'aide de Splunk, la ville a établi une capacité opérationnelle de cybersécurité de base qui respecte ses besoins actuels et futurs, même au-delà des jeux. Le succès du service, consolidé par la capacité de supervision de Splunk pendant la période de menace accrue, a créé un climat de confiance dans l'organisation. Le comité de sécurité de la ville a été plus préparé que jamais à gérer les menaces.



« Splunk nous a permis de faire des progrès en matière de maturité des services de sécurité. Le service est désormais stabilisé et la cadence opérationnelle est établie. Nous sommes donc prêts pour de nouveaux cas d'utilisation et de nouvelles sources de données dans d'autres domaines de l'organisation. »

— Matthew Walker, conseiller en sécurité des technologies de l'information, ville de Gold Coast



La ville de Los Angeles

active les renseignements de sécurité en temps réel dans plus de 40 organes

Pour protéger son infrastructure numérique, la ville de Los Angeles a besoin de renseignements sur les menaces et d'une connaissance de la situation de son dispositif de sécurité. Auparavant, les quelques 40 organes de la ville avaient des mesures de sécurité disparates qui compliquaient l'analyse des données. Los Angeles s'est tournée vers Splunk pour évaluer les risques à l'échelle de la ville, gagner en visibilité sur les activités suspectes et atténuer de manière proactive les menaces.

IMPACT SUR L'ACTIVITÉ

- **Création d'un Centre des opérations de sécurité (SOC) intégré à l'échelle de la ville ;**
- **Protection accrue des actifs numériques, de l'infrastructure et des services publics ;**
- **Renseignements sur les menaces et supervision du réseau en temps réel et 24h/24, 7j/7 dans toute la ville.**

La ville utilise désormais Splunk pour ingérer des logs bruts et d'autres données de plus de 40 services. Splunk intègre ensuite ces informations dans un SOC intégré où l'équipe peut analyser et visualiser les données dans des tableaux faciles à utiliser. Grâce à cette vue unifiée, les dirigeants et les analystes peuvent superviser les logiciels malveillants, identifier les principales personnes malveillantes et leurs cibles, et avoir une connaissance de la situation toujours disponible des événements de sécurité pour faire de la ville un endroit plus sûr pour ses habitants.



« Grâce à la connaissance de la situation, nous savons où nous en sommes. Mais avec l'intelligence des menaces, nous savons aussi qui est notre ennemi. Nous administrons désormais un programme intégré d'intelligence des menaces et notre SIEM Splunk fait partie des éléments clés de la plateforme centralisée de gestion de l'information que nous déployons dans notre Centre intégré des opérations de sécurité (ISOC). »

— Timothy Lee, Directeur de la sécurité de l'information, ville de Los Angeles

Cas d'utilisation

Opérations informatiques
Sécurité
Internet des Objets

Les aéroports de Dubaï s'envolent vers l'avenir avec Splunk

Desservant 100 millions de voyageurs par an et offrant des services exceptionnels à chacun d'entre eux, les aéroports de Dubaï se sont tournés vers Splunk Enterprise. L'aéroport atteint son objectif de faire passer le contrôle de sécurité à 95 % des passagers en moins de cinq minutes en supervisant les détecteurs de métaux afin d'identifier les tendances qui permettent aux files d'attente d'avancer de façon efficace. L'équipe informatique supervise tous ses points d'accès Wi-Fi en temps réel : elle détecte et traite les zones de congestion et les points d'accès problématiques lorsqu'ils surviennent.

IMPACT SUR L'ACTIVITÉ

- Contrôles de sécurité passés par 95 % des passagers en cinq minutes ou moins ;
- Wi-Fi d'aéroport le plus rapide au monde, sans aucun angle mort ;
- Expérience client constante et de haute qualité.

Chaque valise dans le système de bagages des aéroports de Dubaï crée plus de 200 points de données, qui sont tous supervisés dans Splunk Enterprise pour que chaque bagage atteigne sa destination. L'aéroport est en mesure d'allouer efficacement les ressources en combinant les données des bagages avec les données d'exploitation pour prédire la charge de bagages. Les aéroports de Dubaï ont dû augmenter la capacité de l'aéroport sans agrandir les terminaux, l'infrastructure ou les pistes. Grâce à Splunk et aux informations sur les données exploitables, les aéroports de Dubaï ont pu accomplir cela.

REGARDER LA VIDÉO :

splunk.com/dubai-airport-video



« Grâce à Splunk, nous améliorons considérablement l'expérience de voyage de millions de personnes. »

— Michael Ibbitson, vice-président exécutif, technologie et infrastructure, aéroports de Dubaï



Cas d'utilisation

Conformité
Sécurité

Le Comté de Fairfax protège les données de ses citoyens

Le comté de Fairfax, situé au cœur de la capitale du pays en Virginie, emploie 12 000 personnes dans plus de 50 organes et sert plus de 1,1 million de citoyens. Son gouvernement est considéré comme un leader en matière de cybersécurité et d'informatique, ce qui permet au comté de servir et de protéger efficacement les citoyens. Depuis le déploiement de Splunk Enterprise Security (ES) avec Splunk Cloud comme plateforme de gestion des événements et des informations de sécurité (SIEM), le comté de Fairfax a réduit la durée d'élaboration de rapports de sécurité, en passant de deux semaines au temps réel.

IMPACT SUR L'ACTIVITÉ

- Soutien proactif de plus de 50 organes régionaux et protection des données de citoyens ;
- Réduction de l'élaboration de rapports de deux semaines au temps réel ;
- Économies significatives grâce à la réduction de l'empreinte matérielle du datacenter.

Le comté de Fairfax utilise la plateforme Splunk pour superviser les e-mails des employés afin de détecter les tentatives de hameçonnage et les millions de menaces quotidiennes ciblant ses systèmes de points d'extrémité. Outre les menaces connues, le comté supervise les logiciels malveillants pour s'en protéger, tout en défendant son infrastructure stratégique, notamment ses systèmes de supervision et acquisition des données (SCADA). Le comté de Fairfax tire profit de son service cloud pour l'intelligence opérationnelle de plusieurs manières, notamment l'élasticité, la sécurité et l'évolutivité, sans l'effort opérationnel.

REGARDER LA VIDÉO :

splunk.com/fairfax-county



« Auparavant, les rapports destinés aux dirigeants étaient difficiles car tout était manuel. Mon personnel consacrait d'innombrables heures, probablement deux semaines de travail, à élaborer un rapport de synthèse de notre position en matière de cybersécurité. Maintenant, grâce à la plateforme Splunk, je dispose d'un accès en temps réel aux données et je peux donner un dispositif de sécurité global à mes dirigeants pour les aviser quand nous rencontrons des problèmes. »

— Mike Dent, Directeur de la sécurité de l'information, Comté de Fairfax en Virginie

Cas d'utilisation

Analyses commerciales
Internet des Objets

Le centre de transport maritime de Hong Kong gagne de la visibilité en Temps Réel sur les opérations portuaires

Le Marine Department (MD) joue un rôle essentiel dans la sécurité des opérations portuaires dans les eaux de Hong Kong. Auparavant, tout en se concentrant sur le trafic maritime des écrans radar et autres systèmes électroniques, les opérateurs devaient saisir manuellement les enregistrements d'activité des bateaux et rechercher dans des piles de papier pour récupérer des données. Ils devaient ensuite transmettre les documents pertinents à l'opérateur suivant lorsque les bateaux traversaient les quatre secteurs du département. Pour augmenter la précision et l'efficacité opérationnelles, le MD a choisi Splunk pour réorganiser l'ensemble de son système.

IMPACT SUR L'ACTIVITÉ

- Réduction du temps de suivi des bateaux de quelques dizaines de minutes à quelques secondes en exploitant les procédures manuelles ;
- Exploitation facilitée grâce à une visibilité complète en temps réel sur le trafic maritime ;
- Image publique améliorée grâce à une sécurité de navigation et à une efficacité du trafic renforcées.

Grâce à Splunk, le MD a créé l'un des premiers systèmes de suivi de bateaux entièrement automatique. Splunk permet au MD de collecter, d'indexer et d'intégrer les big data en temps réel pour l'analyse du trafic. L'opérateur distribue ensuite des informations de navigation et conseille les bateaux via un réseau radio à haute fréquence pour faciliter les arrivées et les départs en toute sécurité. Cette visibilité de bout en bout permet de nombreuses applications, telles que l'identification automatique du bateau et l'analyse statistique. Les opérateurs peuvent désormais se concentrer sur le trafic maritime et conseiller les marins juste à temps, pour parvenir à une exploitation portuaire plus efficace.



« Splunk nous a impressionné par sa flexibilité exceptionnelle et ses capacités de traitement des données. La plateforme nous a aidés à faire le pont entre le système électronique et les systèmes d'information maritime. Elle nous a permis de disposer d'une connaissance approfondie des données, ce qui nous conforte dans l'idée que nous disposons d'une base solide entre les systèmes. Il en résulte une réelle efficacité dans nos opérations quotidiennes. »

— Gordon Yuen, manager en technologies de l'information,
Marine Department du Gouvernement de Hong Kong



Cas d'utilisation

Opérations informatiques
Sécurité

Les écoles publiques du Comté de Jefferson rendent possible L'apprentissage sécurisé au XXie Siècle

Les écoles publiques du comté de Jefferson dans le Colorado sont un district d'écoles primaires et secondaires qui a besoin de la technologie pour assurer un environnement d'apprentissage et d'enseignement performant, flexible et sécurisé. L'équipe de sécurité, composée de cinq membres, prend en charge 86 000 élèves et 15 000 employés dans 156 écoles avec des pare-feu, des passerelles de messagerie, des investigations et d'autres systèmes de protection.

IMPACT SUR L'ACTIVITÉ

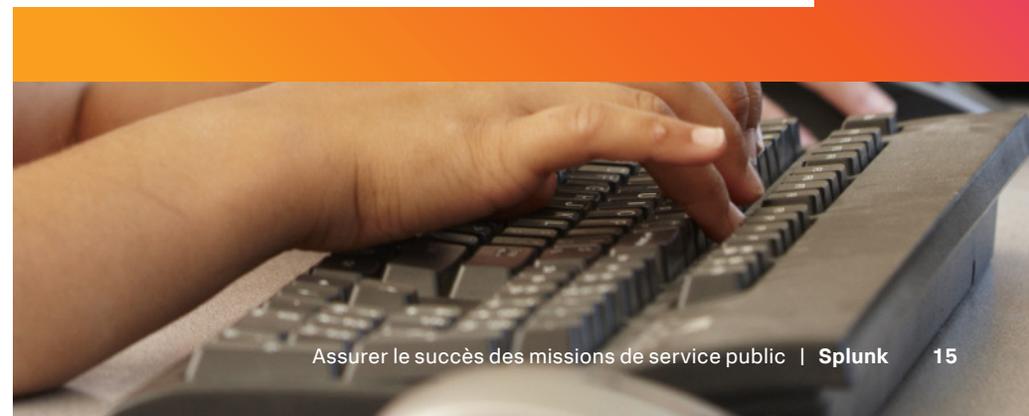
- Disponibilité sans fil de 99,99 % à 100 000 appareils sur 1 800 km² ;
- Réduction du temps moyen de réparation (MTTR) à une demi-heure ou moins ;
- Prise en charge de ressources informatiques distribuées complexes avec une petite équipe informatique.

Pour éviter que les dispositifs de supervision de la sécurité physique ne tombent en panne, l'équipe s'appuie désormais sur Splunk Enterprise pour superviser les codes d'erreur et alerter de façon proactive le personnel, qui peut réparer les systèmes avant qu'ils ne tombent en panne. La plateforme Splunk aide également le district dans sa lutte contre les problèmes de cyber-intimidation en permettant à l'équipe de suivre l'utilisation du système, ainsi que l'accès des utilisateurs et l'accès aux dispositifs.



« Les écoles primaires et secondaires ont toujours un budget limité. Grâce à Splunk, nous pouvons facilement gérer notre large réseau à deux. »

— Michael Kent, ingénieur réseau sans fil,
District scolaire du comté de Jefferson dans le Colorado



Cas d'utilisation

Gestion des opérations informatiques
Gestion des logs
Sécurité

Leidos utilise Splunk pour une meilleure gestion de ses événements

Leader des solutions scientifiques et technologiques et membre de la liste Fortune 500, les 48 ans d'histoire de Leidos sont riches de missions prestigieuses : l'entreprise a notamment appuyé le programme de la navette spatiale américaine et contribué à la conception d'un yacht qui a remporté la Coupe de l'America. Aujourd'hui, Leidos œuvre à relever des défis globaux dans les domaines de la défense, du renseignement, de la santé et d'autres marchés. Leidos doit également résoudre ses propres problèmes pour veiller à ce que ses services soient toujours disponibles pour ses clients. Depuis le remplacement de sa solution de gestion des événements par Splunk IT Service Intelligence (ITSI), le service IT interne de Leidos a constaté de nombreux avantages.

IMPACT SUR L'ACTIVITÉ

- Supervision de l'infrastructure à l'échelle de l'entreprise et corrélation des événements ;
- Meilleure visibilité sur les processus informatiques et commerciaux ;
- Tableaux de bord faciles à partager pour différents publics, des techniciens chargés de résoudre les problèmes aux décideurs de haut niveau.

Leidos avait besoin d'une solution capable de réunir des silos fonctionnels et de trier un grand nombre d'événements s'étendant sur plus de 120 services informatiques. La plateforme Splunk a rompu les silos en permettant aux équipes de voir les données à travers la pile de services. En réglant un nombre croissant de problèmes de gestion des alertes, la plateforme Splunk a également aidé l'entreprise à réduire environ 3 500 - 5 000 alertes quotidiennes à une cinquantaine de tickets destinés aux équipes d'exploitation du réseau et du datacenter.

REGARDER LA VIDÉO :
splunk.com/leidos



« En fin de compte, ma plus grande contribution est que nous changeons les choses en fournissant un service précis et pertinent. Comme Splunk dispose de toutes les informations, les gens peuvent obtenir leurs réponses plus rapidement, plus précisément et plus efficacement. »

- Don Mahler, directeur de la gestion des performances, Leidos



Cas d'utilisation

Sécurité
Conformité
Opérations informatiques
Analyses commerciales

L'instance de contrôle des jeux et loteries du Maryland parie sur Splunk

Administrant la loterie de l'État et chargé de la réglementation des six casinos de l'État, l'instance de contrôle des jeux et loteries du Maryland (MLGCA) supervise des activités de loteries et de jeux. Celles-ci génèrent plus d'un milliard de dollars de contributions annuelles à l'État du Maryland. Avant Splunk, l'instance passait plusieurs heures par semaine sur des processus manuels, comme le respect des critères spécifiques concernant la sécurité des bases de données ou la documentation hebdomadaire des processus informatiques pour répondre aux exigences d'audit. L'instance s'est tournée vers Splunk, la plateforme Data-to-Everything, pour moderniser ses opérations informatiques et de sécurité.

IMPACT SUR L'ACTIVITÉ

- Économie allant jusqu'à six heures par semaine sur la conformité en automatisant les processus essentiels ;
- Amélioration de la détection des anomalies pour l'identification rapide et la prévention des failles de sécurité ;
- Rapports de conformité en temps réel pour les auditeurs, ainsi que supervision de la sécurité pour le directeur et l'équipe informatique.

Grâce à Splunk, la MLGCA a automatisé et modernisé les opérations de sécurité, offrant au personnel une visibilité particulièrement importante en raison de la sensibilité des données collectées par l'instance. Splunk a également aidé l'agence à réduire le temps et les efforts consacrés aux tâches manuelles, ce qui a permis d'économiser en moyenne quatre à six heures par semaine. En automatisant les processus essentiels, le personnel informatique de l'instance peut répondre plus rapidement aux événements qui pourraient indiquer une faille de sécurité. Il peut également maintenir et améliorer plus efficacement le dispositif de sécurité globale de la MLGCA.



« Comment quantifiez-vous les renseignements obtenus sur les événements que nous capturons à des fins préventives ? Splunk nous aide à détecter les failles potentielles avant qu'elles ne se concrétisent, ce qui coûterait des millions de dollars à l'agence et nous plongerait dans un véritable cauchemar sur le plan des relations publiques. »

— Jeff Patchen, directeur des systèmes d'information, instance de contrôle des jeux et des loteries du Maryland

Cas d'utilisation

Opérations informatique
Supervision des applications
Supervision des infrastructures
Analyse prédictive

Données industrielles
Internet des Objets
Supervision de la sécurité

Le National Ignition Facility libère le potentiel de l'énergie propre et protège l'arsenal nucléaire américain

Le National Ignition Facility (NIF), situé au Laboratoire national Lawrence Livermore en Californie du Nord, est le plus grand laser du monde. Pour soutenir les missions principales du NIF, notamment la gestion de l'arsenal nucléaire et les découvertes scientifiques, les scientifiques et les ingénieurs ont besoin d'une infrastructure informatique fiable et sécurisée. Splunk Enterprise et Splunk IT Service Intelligence (ITSI) sont désormais au cœur du système de contrôle du NIF, qui gère plus de 66 000 points de contrôle pour alimenter l'énorme installation laser du NIF.

IMPACT SUR L'ACTIVITÉ

- Disponibilité et performance optimisées du système ;
- Amélioration de la fiabilité des systèmes de contrôle, ce qui permet à l'équipe de maintenir les systèmes nécessaires pour doubler le nombre d'expériences de tir laser de 200 à 400 par an ;
- Garantie de la santé de plus de 66 000 appareils connectés (IoT), en plus de l'infrastructure informatique.

Après avoir intégré les données réseau, d'authentification et d'hôte dans Splunk pour résoudre les défis en matière de sécurité, l'équipe a agrégé ces données avec des sources différentes pour obtenir une visibilité en temps réel à travers l'installation. Les ingénieurs du laboratoire peuvent désormais prendre des mesures sur des événements en fonction des données d'application ou des données de capteurs telles que la tension, la température et la pression du laser.

REGARDER LA VIDÉO :
splunk.com/nif-video



« Splunk ITSI permet à l'équipe de décomposer une machine très complexe en composants distincts. Auparavant, une approche AIOps aurait nécessité beaucoup de ressources pour être mise en œuvre. C'est la première fois que nous pouvons simplifier cette technologie pour une base d'utilisateurs informatiques et l'appliquer à un cas d'utilisation d'infrastructure. »

— Philip Adams, directeur technique et architecte en chef, National Ignition Facility, Laboratoire national Lawrence Livermore

Cas d'utilisation

Gestion des applications
Solutions Cloud
Opérations informatiques
Gestion des logs

Les organismes régionaux d'éducation de New York unifient les données pour améliorer leurs opérations et favoriser l'apprentissage des élèves

La technologie est un élément clé de l'enseignement éducatif des écoles primaires et secondaires et du fonctionnement du district scolaire, mais la sécurité des données des élèves est un défi. Dans l'État de New York, un projet appelé «RIC One» propose une intégration automatisée des données et une authentification unique pour les applications que les élèves, les enseignants et les administrateurs utilisent en vue d'améliorer le fonctionnement des écoles et l'enseignement en classe. RIC One s'est tourné vers Splunk pour améliorer la gestion centralisée des logs et la supervision des applications.

IMPACT SUR L'ACTIVITÉ

- Amélioration de l'expérience pédagogique globale avec un accès aux applications utiles à tout moment ;
- Garantie de la sécurité des données des élèves et des enseignements à l'échelle des districts ;
- Réduction des coûts avec une solution cloud facile à utiliser et à provisionner.

RIC One utilise la plateforme Splunk pour effectuer la supervision proactive des logs et pour veiller au bon fonctionnement quotidien des processus. Splunk Cloud avertit l'équipe en cas d'échec d'un processus, ce qui permet une résolution rapide des problèmes. Splunk Cloud a également réduit le nombre de serveurs que l'équipe doit maintenir et administrer, ce qui lui permet de travailler sur des initiatives plus stratégiques.



« Je ne pense pas que nous pourrions fonctionner sans Splunk. S'il fallait accéder manuellement à ces différentes sources pour obtenir les informations et corréler les données sans notification, nous n'aurions pas atteint ce niveau d'avancement. Splunk est si puissant que, si vous y avez stocké toutes les informations, les possibilités sont infinies. »

— Membre du personnel, RIC One

Cas d'utilisation

Opérations informatiques
Sécurité
Fraude

Le cadre « NHS Choices » renforce sa visibilité pour fournir des Services en ligne essentiels

Le cadre « NHS Choices », le plus grand site Web de soins de santé du Royaume-Uni, vise à être un « service multicanal de pointe pour tous ceux qui s'engagent dans le NHS et les soins sociaux ». Afin de fournir le meilleur service possible à ses 48 millions de visiteurs chaque mois, le cadre « NHS Choices » avait besoin d'une solution pour présenter un aperçu du vaste volume de données de logs produites par l'infrastructure du site Web.

IMPACT SUR L'ACTIVITÉ

- Amélioration de la capacité de résolution des problèmes de sites Web ;
- Meilleure gestion du trafic sur le site Web ;
- Capacités de rapport plus sophistiquées.

En tant que « porte d'entrée » en ligne pour le National Health Service (NHS), le cadre « NHS Choices » devait s'assurer que le site soit optimisé pour fournir le meilleur accès possible à l'information afin d'améliorer la santé publique. Splunk aide le cadre « NHS Choices » à superviser les grands volumes de données machine générées par les visites quotidiennes du site Web, tout en permettant aux équipes technologiques d'identifier et de résoudre rapidement les problèmes, de gérer efficacement le trafic du site Web et d'améliorer les rapports au sein de l'organisation. La plateforme Splunk est désormais également un élément essentiel du cycle de publication mensuel du site Web, donnant à l'équipe un aperçu en temps réel de l'impact des mises à jour au fur et à mesure de leur implémentation.



« Splunk nous permet d'améliorer continuellement les services que nous offrons au public tout en réduisant nos coûts globaux d'infrastructure. »

— Andy Callow, chef de la diffusion des technologies, cadre « NHS Choices »



Cas d'utilisation

Gestion des applications
Opérations informatiques
Sécurité

Dans le Maryland, le comté de Prince George est prêt à remplir sa mission avec la plateforme Splunk

Territoire du Goddard Space Flight Center de la NASA, de l'Université du Maryland et de près d'un million de citoyens, le comté de Prince George du Maryland, situé à l'extérieur de Washington, D.C., s'étend sur près de 1 300 km². L'Office of Information Technology (OIT) centralisé du comté, qui prend en charge l'ensemble des succursales, des organes et des employés du gouvernement, doit relever de nombreux défis pour accomplir sa mission avec des ressources et un financement limités. Le comté s'appuie sur Splunk pour superviser son vaste réseau, qui regroupe environ 100 sites et 500 périphériques réseau.

IMPACT SUR L'ACTIVITÉ

- Amélioration de l'efficacité et de la transparence du gouvernement pour mieux servir les citoyens ;
- Réduction du temps nécessaire à la petite équipe IT pour l'identification et la résolution des problèmes informatiques, qui se compte en heures et non plus en jours ou en semaines ;
- Transformation des opérations du comté : les silos de données ont été remplacés par une plateforme pour les opérations informatiques, la supervision des applications et la sécurité.

Le comté utilise Splunk Enterprise pour superviser les applications. Par exemple, l'une de ces applications permet aux citoyens et aux entreprises du bâtiment de demander et de remplir des permis en ligne. En plus d'offrir à certains directeurs et ingénieurs du comté une visibilité sur les opérations informatiques, les membres du personnel de l'OIT s'appuient également sur Splunk pour les aider en matière de cybersécurité. À l'avenir, le comté prévoit d'accroître son utilisation de la plateforme Splunk pour améliorer son dispositif de sécurité.

REGARDER LA VIDÉO :

splunk.com/prince-georges-county



« Grâce à Splunk, nous sommes en mesure d'avoir une plus grande visibilité auprès des équipes fonctionnelles, d'identifier à l'avance les tendances et les problèmes potentiels, et de résoudre les problèmes plus rapidement en adoptant une vision plus globale du problème. »

— Jayson Loveless, architecte d'entreprise, OIT, comté de Prince George



Sauver Des Vies Grâce À Splunk Et Au **Royal Flying Doctor Service**

Le Royal Flying Doctor Service (RFDS) en Australie est l'une des organisations sanitaires aériennes les plus importantes et les plus complètes au monde. Cet organisme sans but lucratif fournit des services d'urgence et de soins de santé primaires à ceux qui vivent dans des zones rurales et reculées de l'Australie, notamment à des personnes qui ne peuvent pas accéder à un hôpital ou à un cabinet de médecine générale en raison des grandes distances de l'Outback.

IMPACT SUR L'ACTIVITÉ

- Analyse et supervision centralisées des données pour fournir des soins intensifs à 290 000 patients par an ;
- Alertes en temps réel sur la température des vaccins et des médicaments réfrigérés, ce qui a optimisé la distribution des médicaments et réduit les déchets ;
- Communication d'informations détaillées aux donateurs et des missions de sauvetage effectuées dans leur région parrainée.

La flotte de 63 appareils de RFDS, la troisième plus grande compagnie aérienne d'Australie, produit de grands volumes d'avionique et de données de localisation car elle doit pouvoir couvrir sa « salle d'attente », qui s'étend sur plus de 10 000 km². Les tableaux de bord Splunk offrent une visibilité en temps réel sur l'état et les mouvements de la flotte, fournissant au RFDS les informations nécessaires pour fournir efficacement des services de santé essentiels dans des circonstances où chaque seconde compte.



« Splunk est un élément essentiel de notre infrastructure que nous utilisons pour fournir nos services de santé essentiels. Si on me retirait Splunk, j'aurais l'impression de perdre ma main droite. »

— Adam Ind, responsable informatique, Royal Flying Doctor Service



Cas d'utilisation

Analyses commerciales
Internet des Objets

Le bureau du shérif du comté de Sacramento

met en place la police guidée par les renseignements

Le bureau du shérif du comté de Sacramento est responsable des forces de l'ordre pour les secteurs non constitués en municipalités du comté de Sacramento, en Californie, et de plusieurs municipalités incorporées du comté. Le bureau du shérif a mis en œuvre la police guidée par le renseignement (Intelligence-Led Policing, ou ILP), une stratégie qui dépend d'une analyse de données de haute qualité. Il avait besoin d'un moyen d'exploiter les données qui existaient dans des systèmes cloisonnés et disparates.

IMPACT SUR L'ACTIVITÉ

- Visualisations globales et accès en temps réel aux statistiques sur la criminalité et aux informations opérationnelles ;
- Réduction de 50 % du retard en matière de rapports ;
- Économie de centaines d'heures par an dans la génération de rapports ad hoc.

Depuis le déploiement initial de Splunk, l'équipe des applications du bureau du shérif a créé plus de deux douzaines de tableaux de bord, dont plusieurs avec de nombreux panneaux, notamment des vues cartographiques des armes utilisées par emplacement, des aperçus de la criminalité montrant les crimes depuis le début de l'année, les incidents par jour de la semaine, la race des victimes, et bien plus encore.

Les bénéficiaires initiaux des tableaux de bord et des rapports basés sur Splunk étaient le haut commandement du bureau du shérif, y compris le shérif, le sous-shérif, les chefs, les capitaines, les lieutenants et les sergents. La demande de tableaux de bord et de rapports supplémentaires a considérablement augmenté après le premier déploiement. Par exemple, des demandes d'informations spécifiques sur les budgets et les pratiques de dépenses sont venues du County Board of Supervisors, qui supervise le bureau du shérif.



« La plateforme Splunk est essentielle à notre stratégie de police guidée par le renseignement. Notre groupe de commandement est désormais en mesure de voir plus clairement les tendances dans nos statistiques sur la criminalité et de prendre des mesures proactives pour résoudre les sujets de préoccupation et fournir le meilleur service possible au public. »

— John Britto, analyste informatique principal et chef d'équipe d'application, services techniques, bureau du shérif du comté de Sacramento

Cas d'utilisation

Gestion des applications
Opérations informatiques
Sécurité

SAIC construit un nouveau centre des opérations de sécurité de classe mondiale

Science Applications International Corp. (SAIC) est un leader des services d'intégration technologique spécialisé dans les marchés des techniques, de l'ingénierie et de l'informatique d'entreprise. Forte d'une expertise dans des domaines tels que la recherche scientifique, la gestion de programme et les services informatiques, la société devait mettre sur pied un centre des opérations de sécurité (SOC) robuste ainsi qu'une équipe de réponse aux incidents informatiques (CIRT) pour se protéger des cyberattaques.

IMPACT SUR L'ACTIVITÉ

- Amélioration du dispositif de sécurité et de la maturité opérationnelle ;
- Réduction du temps de détection et de résolution des incidents de plus de 80 % ;
- Visibilité complète obtenue sur tout l'environnement de l'entreprise.

Bien qu'elle disposait de la plupart des outils de sécurité dont elle avait besoin pour construire son SOC, SAIC ne possédait pas de solution SIEM pour ancrer ses défenses. La société a décidé de s'appuyer sur Splunk comme plateforme unique de renseignement de sécurité pour tous ses besoins de type «SIEM». Grâce au logiciel Splunk, SAIC a été en mesure de réaliser d'importants projets opérationnels efficaces et de réduire les coûts de main-d'œuvre parmi plus de 50 membres du personnel de sécurité dans le SOC et le CIRT. En outre, le partage de données dans Splunk par différentes équipes a permis d'augmenter le retour sur investissement et d'améliorer l'efficacité informatique globale.

REGARDER LA VIDÉO :
splunk.com/saic



« Le modèle d'une sécurité efficace est la visibilité, l'analyse et l'action. Notre système Splunk nous offre une optique complète et une analyse approfondie basée sur les données, ce qui nous permet de prendre des mesures éclairées pour protéger nos actifs. »

— Jonathan Jowers, directeur des systèmes d'information, SAIC



Les laboratoires Sandia obtiennent des renseignements sur les menaces avancées avec HADES

Organisme réputé pour son innovation scientifique et technique, les laboratoires Sandia sont un laboratoire de recherche et de développement de la National Nuclear Security Administration (NNSA) des États-Unis. Sans surprise, ils ont développé une approche innovante pour relever les défis complexes de la sécurité nationale. Le High Fidelity Adaptive Deception and Emulation System (HADES) des Laboratoires Sandia est une application de cyber-défense à multiples facettes qui résout directement le défi du leurre fondamental qu'est la fusion du leurre humain et du leurre assisté par ordinateur.

IMPACT SUR L'ACTIVITÉ

- Cadre de collaboration axé sur l'automatisation pour une identification et une prise en charge rapides et cohérentes des menaces ;
- Production et partage des informations sur les menaces par les analystes, tout en interagissant avec les attaques en temps réel ;
- Capacité de tromper l'adversaire, de le profiler à son insu pour exposer ses tactiques, ce qui donne aux analystes un avantage compétitif considérable.

L'application HADES utilise la plateforme Splunk pour équiper les analystes d'une visibilité de bout en bout. Ils peuvent déterminer des indicateurs de compromission (IOC) pour développer des profils d'adversaires en temps réel. Ces profils et IOC peuvent détecter les attaques dans les réseaux opérationnels, ce qui minimise et, dans certains cas, empêche les dommages. Grâce à Splunk, l'équipe conserve ainsi une longueur d'avance sur les attaques avec une plateforme qui fait peser les charges sur l'adversaire.



« Nos sources de données dans HADES sont extrêmement complexes et hétérogènes. Nous utilisons déjà la plateforme Splunk dans d'autres domaines, et il était logique de l'appliquer à HADES pour atteindre nos objectifs. »

— Vincent Urias, stratège de recherches en cybersécurité, laboratoires Sandia

Cas d'utilisation

Opérations informatiques

L'État de Louisiane économise des millions en modernisant l'informatique

L'État de Louisiane a récemment consolidé tous ses services informatiques à travers 20 organes de l'exécutif, ce qui a amené 850 employés dans un modèle moderne de services partagés. Le service nouvellement unifié a été chargé de réduire les coûts et d'améliorer la prestation de services à ses principaux clients, c'est-à-dire les organes publics et les citoyens. Depuis le déploiement de Splunk, l'État rapporte que les organes peuvent se concentrer sur leur entreprise plutôt que de passer du temps sur la maintenance informatique et les contrats.

IMPACT SUR L'ACTIVITÉ

- Économie de 70 millions de dollars grâce à l'accélération des efforts de modernisation et d'harmonisation des systèmes hérités ;
- Amélioration de l'efficacité et de l'expérience des clients grâce à l'harmonisation de l'informatique et la centralisation de la gestion des données ;
- Stimulation de l'efficacité commerciale et réduction des coûts grâce à un modèle de services partagés.

Grâce à Splunk, les organes obtiennent désormais une lecture précise de leur utilisation, comme le nombre de documents stockés, la quantité de stockage consommée et le nombre de règles métier exécutées pour l'analyse. L'État planifie déjà la prochaine étape : des tableaux de bord clients pour montrer que les serveurs et les applications des organes sont opérationnels et pour indiquer leur coût, améliorant ainsi la transparence du bureau du gouverneur.

REGARDER LA VIDÉO :

splunk.com/state-of-louisiana



« Splunk est extrêmement efficace et nous aide à faire le meilleur usage possible de l'argent de nos contribuables. Non seulement nous faisons des économies en évitant de devoir effectuer de nombreuses tâches manuelles sur plusieurs systèmes, mais, en outre, la transparence est renforcée. Cela nous offre la possibilité de montrer à nos administrés exactement comment et pourquoi nous utilisons les budgets. »

— Derek Williams, directeur des opérations de datacenter, État de Louisiane

Cas d'utilisation

Gestion des applications
Sécurité

Le Ministère de la santé et des services sociaux de L'État du Michigan offre une expérience citoyenne de qualité supérieure

Le Ministère de la santé et des services sociaux de l'État du Michigan (MDHHS) est chargé de fournir des services dans les domaines des soins de santé, de l'aide alimentaire, du développement et des soins aux enfants, de l'aide financière, et des secours d'urgence de l'État. Pour fournir ces services à plus de 1,7 million de citoyens, le MDHHS utilise le système d'éligibilité intégré appelé BRIDGES, reliant 52 organes différents et plus de 10 000 utilisateurs tout en traitant plus de 12 000 transactions par minute.

IMPACT SUR L'ACTIVITÉ

- Amélioration de 20 % de la résolution des problèmes avant leur impact sur les utilisateurs ;
- Meilleure capacité à respecter les SLA en réduisant le MTTR de 35 % ;
- Garantie de réussite des tableaux de bord d'évaluation de conformité tout en réduisant les efforts manuels de conformité de 50 %.

Après avoir adopté Splunk, la plateforme Data-to-Everything, MDHHS a augmenté l'efficacité de l'entreprise en obtenant une visibilité détaillée de son infrastructure d'application BRIDGES. Grâce à sa capacité à identifier l'utilisation et à analyser les performances, ainsi qu'à ses capacités de prédiction et d'intelligence artificielle, l'organe gouvernemental obtient désormais des informations sur les problèmes bien avant que les utilisateurs ne soient impactés, ce qui permet d'améliorer l'expérience globale des citoyens.

Le respect des mandats de conformité est au cœur des objectifs de tout organe gouvernemental. Grâce à Splunk, MDHHS a acquis une visibilité sans précédent sur sa position de conformité en temps réel, permettant un tableau de bord d'évaluation, augmentant l'efficacité de l'audit et réduisant les efforts manuels du personnel de 50 %.



« L'effort manuel de notre personnel pour fournir et suivre la conformité PCI et d'audit a été réduit de 50 % par Splunk. Cela nous permet d'assurer un tableau de bord d'évaluation pour les audits. »

— Sanjay Srivastava, directeur de division, zone d'admissibilité DTMB, État du Michigan



Cas d'utilisation

Opérations informatiques
Supervision des infrastructures
Supervision des applications
Sécurité

Fraude
Analyses commerciales

Le bureau du recensement des États-Unis passe au numérique pour le recensement le plus efficace du pays

Tous les 10 ans depuis 1790, le Bureau du recensement des États-Unis s'emploie à accomplir le plus grand projet civil du pays : obtenir un décompte précis de chaque personne vivant aux États-Unis et sur ses territoires. Le recensement de 2020, premier recensement numérique national de la décennie, offrira aux Américains la possibilité de répondre en ligne, en plus de pouvoir répondre par téléphone ou par e-mail. Pour explorer ce nouveau domaine, le Bureau du recensement utilise Splunk afin d'adopter une approche novatrice des données pour mettre en place les modalités d'évaluation du nombre de personnes vivant en Amérique.

IMPACT SUR L'ACTIVITÉ

- Contribution à la réussite du recensement 2020, qui représente le recensement de la première décennie numérique et le recensement le plus efficace jamais planifié ;
- Tableaux de bord standardisés et informations en temps réel qui permettent aux dirigeants de prendre des décisions éclairées ;
- Intégrité, disponibilité et sécurité de conformité pour l'infrastructure complexe du Bureau du recensement comptant 52 systèmes et 35 opérations.

Les tableaux de bord et les visualisations de données de Splunk sont devenus un élément essentiel des workflows quotidiens au Bureau du recensement. Ils fournissent des informations en temps réel pour aider les dirigeants et les équipes de sécurité, d'informatique et d'application, à aborder des questions, à prendre des décisions et à transformer les données en action. Avec Splunk au centre de son SOC et de son NOC, le Bureau du recensement a amélioré la disponibilité. Il identifie de manière proactive les vulnérabilités et les problèmes de dépannage plus rapidement pour une expérience plus sûre et plus fiable.



Réussir des missions de service public **ensemble**

Ce ne sont là que quelques exemples de la manière dont Splunk a aidé les organismes du secteur public du monde entier à protéger leur infrastructure, à moderniser leurs opérations et à mieux servir les citoyens.

Pour plus d'informations sur la façon dont Splunk contribue à la réussite des missions de service public, regardez les présentations .conf19 afin d'écouter les récits de nos clients :

État du Michigan : splunk.com/stateofmichigan-conf19

Ville d'Amsterdam : splunk.com/cityofamsterdam-conf19

FBI : splunk.com/fbi-conf19

Banque d'Angleterre : splunk.com/bankofengland-conf19