Sécurité informatique dans le secteur public

Défis, obligations et solutions innovantes

WITH secure

Sommaire

Introduction

Dans un contexte où les cybermenaces sont en constante évolution et deviennent de plus en plus sophistiquées, le secteur public n'est pas épargné. La gestion sécurisée des systèmes d'information et la protection des données sensibles sont devenues des enjeux cruciaux pour les administrations publiques.

Dans un monde connecté où l'information circule à la vitesse de la lumière, les administrations publiques françaises sont confrontées à des défis de sécurité informatique de taille. Cela va au-delà de la simple protection des données; il s'agit aussi de maintenir la confiance du public, de respecter des réglementations toujours plus strictes et de parer à toute une gamme de cybermenaces toujours plus ingénieuses.

Le contexte est d'autant plus sensible que les données manipulées par les administrations publiques sont souvent de nature délicate : informations personnelles, données fiscales, dossiers de santé, et plus encore. Une faille de sécurité peut donc avoir des répercussions graves, non seulement sur l'intégrité des systèmes mais aussi sur la vie des citoyens.

Ce livre blanc a pour vocation d'éclairer ces problématiques à travers un prisme éducatif. Nous explorerons les différents types de risques et menaces auxquels le secteur est exposé, tout en présentant les obligations réglementaires en vigueur. De plus, nous vous présenterons les solutions innovantes offertes par WithSecure™ qui peuvent aider à adresser ces défis.

La connaissance est la première étape vers la protection. Et c'est précisément l'objectif de cette publication : armer les administrations publiques des connaissances et des outils nécessaires pour mieux sécuriser leur environnement numérique.

“Les 37 000 attaques contre nos institutions en 2022 ne sont pas juste des chiffres, elles sont un cri d'alarme.

Dans cette guerre silencieuse du cyberespace, il est impératif d'allier expertise, innovation et éducation pour anticiper les incidents et sauvegarder la confiance du public.”

Guillaume Gamelin,
Vice-Président France, WithSecure™

Les risques et menaces dans le secteur public

WITH secure

Face à une augmentation alarmante des cyberattaques, les responsables en sécurité informatique des organisations publiques ne peuvent plus se contenter d'approches défensives minimes. D'autant plus quand les chiffres de 2022 indiquent que ces attaques ont déjà coûté 2 milliards d'euros aux secteurs public et privé en France, avec le secteur public représentant un quart de cette somme. Des institutions clés aux petites communes, la menace est réelle et les conséquences durables.

Les chiffres parlent d'eux-mêmes. Selon une enquête récente du cabinet Asterès*, 37 000 attaques ont été perpétrées contre des organisations publiques en France en 2022. Ce n'est pas une mince affaire. Ces cyberattaques ont des conséquences à long terme, notamment une hausse des dépenses publiques et une baisse de satisfaction citoyenne.

Pour comprendre l'ampleur du problème, prenons quelques exemples. L'assurance Maladie française a vu un million d'identifiants volés, et l'hôpital de Corbeil-Essonnes a été paralysé pendant deux mois. Et ce n'est que la pointe de l'iceberg. Des villes entières, comme Caen, ont vu leurs services en ligne interrompus pendant des semaines. Ce ne sont pas des incidents isolés; ils montrent la nécessité d'adopter des mesures de sécurité robustes.

Certains secteurs, comme la santé, sont plus vulnérables que d'autres. Dans le même temps, une fausse idée de sécurité règne dans les petites communes. Selon une étude du GIP Cybermalveillance, 65% des communes de moins de 3.500 habitants se croient à l’abri des cyberattaques. Ce sentiment de complaisance peut se révéler fatal.

Comment alors trouver l'équilibre entre conformité réglementaire et sécurité effective? Il ne suffit pas de cocher des cases pour respecter les directives de l'ANSSI ou la directive NIS. La transformation digitale en cours ne fait qu'élargir la surface d'attaque. Le phishing et le spearfishing, ainsi que l'exploitation de failles existantes, sont des vecteurs d'attaque courants. Pour s'en prémunir, il faut une stratégie solide.

Pour les spécialistes en sécurité informatique des organisations publiques, la cybersécurité n'est pas seulement une contrainte, mais aussi une opportunité majeure. En investissant dans des solutions professionnelles comme celles de WithSecure™, vous ne faites pas que protéger vos systèmes et vos données, vous contribuez aussi à la création d'une culture de sécurité et à la valorisation de votre organisation.

*Le cabinet Asterès, spécialisé dans la recherche et les études économiques, a été mandaté par le CRiP (Club des Responsables Infrastructures, Technologies et Production IT) pour proposer une estimation du coût des cyberattaques réussies en France en 2022.

Passer d'une défense réactive à une approche proactive

WITH secure

Face à l'explosion des cyberattaques ciblant les organisations publiques, les experts en sécurité des systèmes d'information des organisations publiques ne peuvent plus se contenter de mesures de sécurité traditionnelles. Voici une liste d’actions précises à entreprendre, éclairées par les dernières directives de l'ANSSI, tout en mettant l'accent sur les risques encourus et les impacts associés.

6 recommandations issues de l'ANSSI pour la Cybersécurité

1 Authentification et contrôle des accès

Intégrez une authentification multifactorielle associant tokens, mots de passe et authentification biométrique pour tous les utilisateurs, internes et externes.
Risque en cas d'inaction : intrusions malveillantes, pertes de données et usurpations d'identité.

2 Renforcer la sécurité des postes et serveurs

Activez tous les modules de prévention, tels que l'anti-malware, le filtrage d'URL et l'analyse comportementale.
Risque en cas d'inaction : vulnérabilités exploitables, diffusion de malware et compromissions des ressources critiques.

3 Maintenir le système d'information à jour

Automatisez les mises à jour de sécurité à travers un déploiement de patchs centralisé.
Risque en cas d'inaction : failles de sécurité non corrigées, exploitation par des cyberattaquants.

4 Implémentation EDR contre les attaques avancées.

Adoptez une plateforme EDR pour une visibilité accrue des activités suspectes et une réponse rapide aux menaces.
Risque en cas d'inaction : détection tardive des intrusions, augmentation des temps de compromission et escalade des coûts d'intervention.

5 Mise en place et contrôle de sauvegardes déconnectées

Priorisez des sauvegardes régulières, isolées du réseau, pour garantir la récupération des données.
Risque en cas d'inaction : pertes de données irréversibles, arrêts d'activité prolongés et pertes financières significatives.

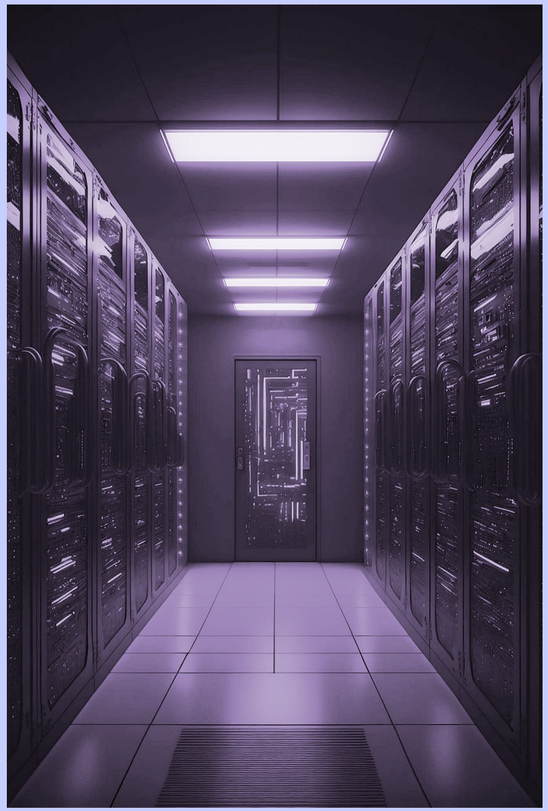
6 Sécuriser ses applications SaaS

Assurez-vous d'une gestion rigoureuse des accès et des configurations, tout en surveillant les activités anormales.
Risque en cas d'inaction : fuites de données, compromissions de comptes et non-conformité réglementaire.

Sécurité des données dans le Cloud

WITH secure

La **migration vers le cloud** est devenue une priorité pour les administrations publiques françaises, encouragée par des directives gouvernementales. Mais avec la transformation numérique viennent des défis en matière de cybersécurité. Les plateformes de cybersécurité basées sur le cloud émergent comme une solution clé, permettant de naviguer dans ce paysage complexe tout en optimisant la gestion de la sécurité.



La France s'oriente résolument vers une architecture cloud pour ses administrations publiques, y compris les collectivités territoriales, les ministères et les autres institutions publiques. Ces entités bénéficient d'offres de cloud diversifiées allant des solutions souveraines contrôlées par l'État aux offres commerciales accessibles via des marchés publiques. Bien que la transition vers le cloud offre des avantages indéniables en termes d'efficacité opérationnelle et d'évolutivité, elle pose des défis en matière de cybersécurité. Heureusement, l'émergence de plateformes de cybersécurité basées sur le cloud offre une réponse nuancée à ces défis.

Dans ce contexte, ces plateformes se distinguent par l'adoption de modèles de gouvernance en matière de sécurité, appuyés par des contrôles de conformité rigoureux, issus des meilleures pratiques et alignés sur des référentiels. Pour les entités publiques avec des contraintes budgétaires différentes, ces plateformes permettent une granularité dans la mise en œuvre des politiques de sécurité, tout en offrant des mécanismes d'audit et de reporting efficaces.

L'utilisation de plateformes de cybersécurité dans le cloud offre une solution performante pour minimiser le temps consacré aux tâches de maintenance opérationnelle. Leur architecture centrée permet aux organisations de consolider leurs opérations de sécurité via un tableau de bord unifié, offrant ainsi une visibilité complète sur l'environnement de sécurité.

En résumé, pour les administrations publiques françaises, les plateformes de cybersécurité basées sur le cloud se présentent comme des vecteurs d'optimisation stratégique. Elles permettent également aux équipes de cybersécurité de réaffecter leurs ressources vers des initiatives plus stratégiques. C'est une démarche qui allie performance et conformité, tout en offrant les moyens de maintenir une posture de sécurité proactive dans un environnement de plus en plus menaçant.

Dans le secteur public, la transformation numérique accélérée par les **applications Microsoft 365** est un véritable levier de performance. Cependant, elle soulève des enjeux critiques de cybersécurité. Décryptons les risques associés et comment les plateformes de cybersécurité cloud, en offrant une gestion unifiée et une réponse rapide aux incidents, se positionnent comme un rempart efficace pour les organisations publiques.

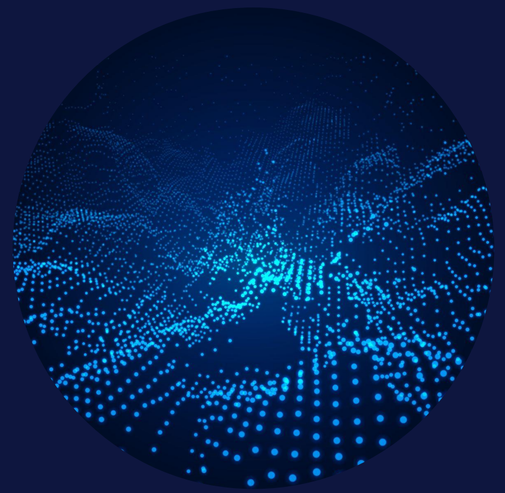
Malgré les polémiques, la montée en puissance des applications Microsoft 365 dans les administrations publiques françaises est un indicateur du changement radical des méthodes de travail. Teams, Exchange, SharePoint et OneDrive sont devenus des piliers de la collaboration et de la communication. Cependant, cette dépendance a aussi ouvert de nouveaux modèles d'attaque, qui doivent être pris en compte dans la sécurisation du système d'information des organisations. Des solutions Cloud existent pour sécuriser ces applications devenues critiques.

La gamme Microsoft 365 regroupe des outils axés sur la productivité qui sont devenus quasi-indispensables dans le monde professionnel. Leurs fonctionnalités de collaboration en temps réel et d'automatisation des workflows simplifient et accélèrent les processus métier. Mais il serait négligent de passer sous silence les risques associés à cette large adoption. Phishing, fuite de données, attaques par diffusion de fichiers malveillants sont autant de menaces qui pèsent sur ces plateformes cloud.

Les plateformes de cybersécurité cloud, qui étendent la protection des endpoints aux services cloud, apportent une réponse efficace à ces défis. Elles permettent de gérer efficacement les principales capacités de sécurité via un portail unique, avec des données unifiées pour tous les composants. En combinant la gestion des vulnérabilités, la protection des endpoints, la détection et la réponse aux endpoints (EDR), ainsi que la protection de la collaboration, ces plateformes offrent un contrôle granulaire et une réponse rapide aux incidents de sécurité.

L'adoption des applications Microsoft 365 dans le secteur public est à la fois une opportunité et un défi. Les solutions de protection des environnements collaboratifs Microsoft sont des alliés de taille pour sécuriser cet écosystème complexe tout en permettant aux organisations de se concentrer sur leur mission première : le service public.

Formation et sensibilisation du personnel



WITH secure

Naviguer dans le paysage complexe de la cybersécurité requiert plus que des compétences techniques; il s'agit d'un effort collectif. Pour les experts en cybersécurité au sein des organisations publiques, la formation et la sensibilisation du personnel sont essentielles pour garantir une défense robuste et une réponse agile aux menaces en constante évolution.

Dans le secteur public, où la cybermenace est omniprésente et les ressources souvent limitées, la formation et la sensibilisation du personnel deviennent des piliers incontournables de la stratégie de cybersécurité. L'expertise technique ne suffit plus ; elle doit être complétée par une culture de la sécurité intégrée à tous les niveaux de l'organisation.

Une maitrise pointue des solutions de cybersécurité est indispensable pour comprendre et sécuriser efficacement l'environnement numérique dans lequel évoluent les services publics.

Le rôle des experts en cybersécurité va bien au-delà de la simple mise en œuvre de technologies ; ils doivent être des vecteurs de changement, formant et sensibilisant le personnel aux meilleures pratiques de sécurité. Cela implique une connaissance intime des solutions de sécurité, des configurations optimales aux paramètres avancés, afin de garantir une protection robuste et une réponse rapide en cas d'incident.

Il est donc crucial d’investir dans des programmes de formation continus, conçus par des experts pour des experts.

L’objectif est double : maintenir à jour les compétences techniques et comprendre les dynamiques comportementales qui peuvent influencer la sécurité. La collaboration interfonctionnelle est également clé ; les experts en sécurité doivent travailler de concert avec les équipes opérationnelles pour s'assurer que les processus et les politiques sont non seulement efficaces mais aussi pragmatiques.

La maîtrise des solutions de cybersécurité, de la protection des endpoints aux systèmes avancés de gestion des menaces, doit être au cœur de ces initiatives de formation. Ces solutions, lorsqu'elles sont pleinement comprises et correctement appliquées, deviennent des multiplicateurs de force, permettant aux experts en sécurité de focaliser sur des tâches stratégiques plutôt que de se perdre dans la gestion quotidienne des risques.

Pour assurer une cybersécurité optimale, il est essentiel de renforcer non seulement les infrastructures mais aussi la formation des équipes. Les bonnes pratiques en matière de formation visent à doter chaque collaborateur des compétences et réflexes nécessaires pour faire face aux menaces actuelles, en alliant prévention et préparation proactive aux incidents.

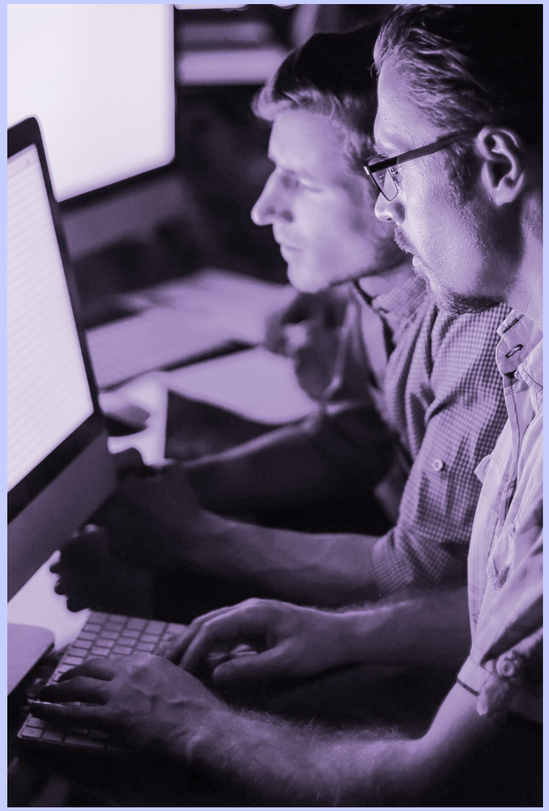
Bonnes pratiques en matière de formation

1. **Phishing simulé:** Simulez des attaques de phishing pour évaluer la vulnérabilité de votre personnel et les éduquer sur la manière de repérer des e-mails suspects.

2. **Mots de passe forts:** Instruisez les employés sur l'importance de mots de passe robustes et de l'utilisation d'un gestionnaire de mots de passe.

3. **Double authentification:** Éduquez votre équipe sur la nécessité de l'authentification à deux facteurs comme mesure de renforcement de la sécurité.

4. **Sensibilisation aux crises cyber:** Des simulations d'incidents aux ateliers de gestion de crise, la préparation cyber est aussi cruciale que la réponse technique.

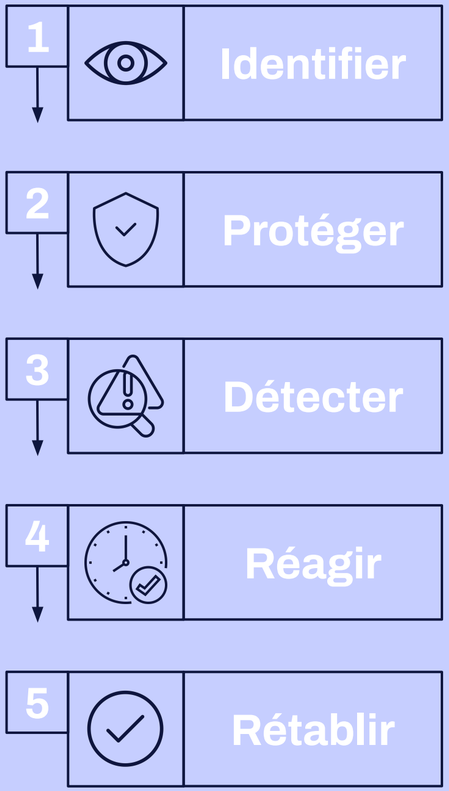


Réponse aux incidents et gestion des crises

WITH secure

Référentiel NIST de cybersécurité

L'incident de sécurité n'est pas une question de "si", mais de "quand". La préparation aux incidents est donc une étape cruciale pour minimiser les dommages et accélérer la reprise. L'adoption du référentiel NIST peut jouer un rôle central pour sécuriser efficacement les actifs numériques.



Dans les organisations publiques, le référentiel NIST (National Institute of Standards and Technology) sert de guide pour l'établissement d'une cybersécurité robuste. L'adoption de ce cadre permet non seulement de s'aligner avec les meilleures pratiques internationales, mais aussi de répondre aux exigences réglementaires spécifiques aux entités gouvernementales.

Le référentiel NIST repose sur cinq fonctions principales : Identifier, Protéger, Détecter, Réagir et Rétablir. Chacune de ces fonctions est cruciale pour la construction d'un écosystème de cybersécurité efficace et adaptatif.

La fonction **'Identifier'** prend une importance accrue dans les organisations publiques où le volume de données sensibles est élevé. Des audits réguliers et des évaluations des risques sont nécessaires pour garantir que les ressources sont allouées efficacement.

La fonction **'Protéger'** se matérialise souvent par l'adoption de solutions de sécurité avancées, telles que les plateformes de gestion de la sécurité qui offrent une visibilité globale et des capacités de réponse automatisées.

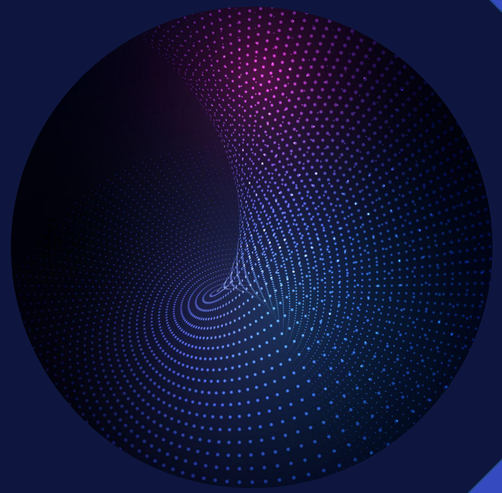
La fonction **'Détecter'** nécessite l'intégration de systèmes de détection et de surveillance en temps réel. Des plateformes avancées, offrant une analyse comportementale et des algorithmes d'apprentissage machine, peuvent détecter des anomalies que les systèmes traditionnels pourraient manquer, y compris les solutions EDR (Endpoint Detection and Response).

La fonction **'Réagir'** consiste à répondre à une attaque, utilisant des outils spécifiques, y compris les solutions EDR. Elle nécessite une coordination des parties prenantes et une préparation à des scénarios spécifiques de cyberattaques.

La fonction **'Rétablir'** vise à maintenir les fonctions vitales opérationnelles pendant une attaque (résilience) et à restaurer intégralement le système d'information dans les meilleurs délais.

Pour réussir cette adoption, il est impératif de disposer d'une stratégie d'implémentation bien conçue, d'outils adaptés et d'une formation continue pour le personnel. Le référentiel NIST n'est pas seulement un guide mais un atout stratégique pour renforcer la posture de cybersécurité dans le secteur public.

RETEX
Comment WithSecure™ a transformé la protection cyber d'une mairie



WITH secure

Découvrez comment une collectivité territoriale a transformé sa gestion de la cybersécurité avec WithSecure™. Face à des défis multiples, cette mairie a choisi notre solution pour sa simplicité, son efficacité et son excellent retour sur investissement. Le résultat ? Une sécurité renforcée, des opérations optimisées et une vision claire pour une stratégie de cybersécurité durable.

Contexte et défis

Les collectivités territoriales font face à une menace croissante de cyberattaques, mettant en péril les services publics, la sécurité des données et la confiance citoyenne. Les défis pour les équipes informatiques sont multiples :

- Sensibiliser élus, agents et usagers au risque cyber ;
- Améliorer compétences et outils pour contrer des attaques toujours plus sophistiquées ;
- Évaluer et sélectionner les solutions adaptées aux besoins ;
- Pallier le déficit de main-d'œuvre qualifiée dans un marché tendu.

Comment ces défis affectaient-ils les opérations de la mairie ?

Dans un tel environnement, les équipes techniques peuvent se retrouver en surcharge de travail, focalisant leurs efforts sur des mesures correctives au détriment d’une approche préventive.

Cette orientation vers le curatif peut entraîner :

- Des retards dans la prestation de services publics ;
- Une vulnérabilité accrue aux attaques sophistiquées ;
- Une dilution des ressources, entravant les initiatives de sécurité à long terme ;
- Une érosion de la confiance du public due à des incidents de sécurité récurrents.

Quels étaient les critères qui ont guidé le choix du client pour WithSecure™ ?

Plusieurs facteurs ont influencé le choix en faveur de WithSecure™ :

1. L'efficacité opérationnelle offerte par la simplicité de la solution, prouvée dès la phase d'évaluation.
2. Le support proactif de l'équipe WithSecure™ locale pendant la phase d'évaluation.
3. Des avantages financiers, rendus possibles grâce à notre ancrage européen et la compatibilité avec le plan France relance.

Description du processus de mise en œuvre de la solution WithSecure™ ?

Le processus de déploiement s'est déroulé en trois étapes clés :

1. Un pilote au sein de la DSI pour une prise en main de la solution et l'élaboration du plan de déploiement.
2. Extension du déploiement aux services de l'hôtel de ville.
3. Déploiement final sur les sites distants.

Quels ont été les résultats immédiats après l'implémentation de la solution WithSecure™?

L'impact le plus significatif a été la visibilité accrue sur le système d'information. Ce gain en clarté a mis en lumière les zones vulnérables du réseau et a permis à la solution WithSecure™ de cibler des problèmes spécifiques, tels que les patchs manquants, les défauts de configuration du système d'exploitation, les équipements sans protection, la nécessité de redémarrage, les comportements à risques, etc.

Ce diagnostic détaillé a facilité les actions correctives nécessaires.

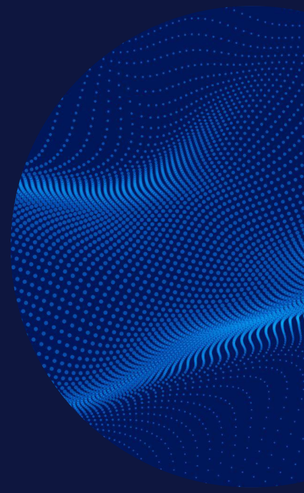
Comment la solution a-t-elle affecté les opérations à long terme ?

Avec WithSecure™, le client a optimisé la gestion de sa sécurité. Grâce à une interface unique, il a une vue d'ensemble de son environnement et peut prioriser des actions en fonction de leur urgence et importance. Le gain de temps et l'efficacité résultants ont permis d'adopter une approche plus proactive que réactive en matière de cybersécurité.

Quels sont les points forts de la solution WithSecure™ ?

Ce qui distingue WithSecure™, c'est sa capacité à fournir une posture de sécurité robuste. En rectifiant les faiblesses de base du système d'information, WithSecure™ permet de bâtir un programme de sécurité plus solide et évolutif.

Meilleures pratiques et recommandations



WITH secure

La cybersécurité ne repose pas uniquement sur des solutions technologiques avancées. Elle implique également une gouvernance, une préparation et une formation du personnel. Dans ce qui suit, nous explorons les meilleures pratiques adaptées aux organisations publiques pour optimiser la sécurité en cette ère numérique complexe. De la mise en place de solutions EPP+EDR à la préparation face aux incidents de sécurité, ces lignes directrices façonnent une posture de sécurité robuste.

1 Stratégie de sauvegarde avancée

Adoptez une stratégie de sauvegarde hiérarchisée, couplée à des réplications géographiquement dispersées et chiffrées. Utilisez des solutions qui supportent la déduplication des données, et assurez-vous de tester régulièrement la restauration pour des scénarios de menace spécifiques comme le ransomware.

2 Déploiement de solutions EPP+EDR multi-couches

L'association de solutions de protection des points de terminaison (EPP) et de détection et de réponse aux points de terminaison (EDR) doit être soutenue par une orchestration SOAR pour une réponse automatisée. Le déploiement de ces solutions doit être soutenu par une analyse comportementale et une corrélation d'événements en temps réel.

3 Limitation et standardisation des piles de sécurité

La diversité des outils peut être un obstacle à la sécurité. Standardisez les solutions en fonction des cas d'usage et des besoins métier tout en rationalisant leur gestion. Une approche unifiée facilite la surveillance, optimise les ressources, et assure une intervention rapide en cas d'incidents.

4 Préparation aux crises cyber

Élaborez des scénarios de table-top et de red-teaming pour confronter votre organisation à des attaques APT (Advanced Persistent Threats). Cette démarche met à l'épreuve les protocoles de réponse et renforce la préparation aux menaces cybernétiques avancées.

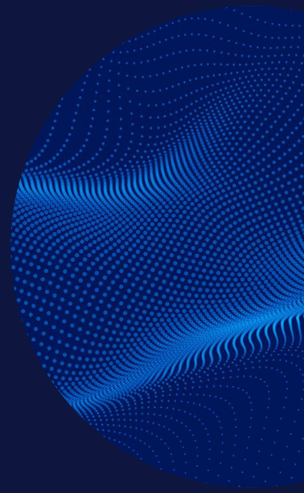
5 Gestion proactive des vulnérabilités

Ne vous contentez pas de patcher; adoptez une approche proactive en intégrant les flux de travaux de gestion des vulnérabilités à un tableau de bord centralisé. Utilisez les évaluations des menaces et les scores CVSS pour prioriser les patchs et minimisez la fenêtre d'exposition.

6 S’entourer d’experts en cybersécurité

Établissez des liens avec des experts certifiés, qu'ils soient internes, prestataires locaux, ou de l'éditeur, disponibles à la demande, en co-gestion ou externalisés. Leur maîtrise en réponse aux incidents, analyse de menaces et gestion de la sécurité assure une intervention experte et rapide en cas de violation.

Les solutions WithSecure™



Postes de travail

Windows, Mac, Linux

Serveurs

Windows, Linux

Email

Microsoft Outlook

Applications cloud collaboratives

Microsoft Teams, Sharepoint, One drive

Réseaux

Analyse de la vulnérabilité

Elements™

Single agent

Les données unifiées sont analysées à l'aide de renseignements sur les menaces à l'échelle mondiale

One Security Center

Elements™

WithSecure™ Elements Vulnerabilty Management

Pour minimiser votre surface d’attaque et les risques associés, cette solution indexe les actifs de votre entreprise et identifie leurs vulnérabilités critiques.

WithSecure™ Elements Endpoint Protection

Le cœur de votre protection : cet outil puissant allie renseignements sur les menaces mondiales, analyses comportementales et analyse réputationnelles. Il neutralise les ransomwares, les malwares et les menaces 0-day les plus sophistiquées.

WithSecure™ Elements Collaboration Protection

Un niveau supérieur de protection pour renforcer la sécurité intégrée des plateformes de collaboration cloud. Cette protection puissante neutralise les contenus malveillants, bloque les attaques de phising, identifie les piratages de comptes et détecte les violations de règles de la messagerie.

WithSecure™ Elements Endpoint Detection and Response

Ce composant Elements vous offre la précision et la rapidité dont vous avez besoin pour détecter les menaces avancées et y répondre, sans être confronté à une inondation d’alertes. Traquez efficacement les menaces grâce à un système de détection et de réponse intuitif et flexible. Repérez même les anomalies comportementales les plus sophistiquées.

WithSecure™ Elements Cloud Security Posture Management

Gestion de la sécurité de votre infrastructure cloud grâce à une analyse régulière et proactive des erreurs de configuration.
Cette solution effectue des analyses et des vérifications complètes des configurations non sécurisées du cloud. Elle fournit ensuite des conseils sur les actions correctives à mener.

Threat intelligence en temps réel

WithSecure™ Security Cloud est la pierre angulaire de votre sécurité. Notre service d’analyse et de détection des menaces cloud rassemble des renseignements sur les menaces en temps réel provenant de dizaines de millions de sondes de sécurité à travers le monde. Les renseignements sur les menaces du Security cloud évoluent constamment, et nos meilleurs analystes affinent sans relâches notre logique de détection.

À propos de WithSecure™

WithSecure™ est le partenaire de référence en matière de cybersécurité. Les fournisseurs de services informatiques, les MSSP, les entreprises, les grandes institutions financières, les industriels, les milliers de fournisseurs en communications et technologies de pointe, ainsi que des comptes publics de premier plan, nous font confiance.

Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir leur continuité opérationnelle. Notre protection basée sur l'IA sécurise les endpoints et protège les collaborations cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Nos consultants, quant à eux, proposent leurs conseils aux entreprises et challengers technologiques qui souhaitent renforcer la résilience. Depuis plus de 30 ans, nous élaborons une offre de pointe, pour nous développer au côté de nos partenaires, grâce à des modèles commerciaux flexibles.

WithSecure™ fait partie de F-Secure Corporation, fondée en 1988 et cotée au NASDAQ OMX Helsinki Ltd.

WITH secure™