Livre blanc

Collectivités locales et administrations publiques

Sécuriser le service public à l'ère des menaces 2025

Romain Ravon

Digital Security
Progress. Protected.

Digital Security
Progress. Protected.

Table des matières

Editorial

Les collectivités locales et administrations publiques sont les piliers de la production et de la gestion de services essentiels pour nos citoyens. De l'eau à l'énergie, des transports à l'éducation, en passant par la santé et la sécurité civile, la continuité et la fiabilité de ces services sont primordiales. Dans un paysage numérique en constante évolution, des efforts significatifs ont été engagés pour faire face à un paysage de menaces de plus en plus complexe.

Les cyberattaques continuent de se sophistiquer et de poursuivre différents objectifs. L'ingénierie sociale et en particulier les campagnes d'hameçonnage, alimentées par l'Intelligence Artificielle Générative, sont de plus en plus crédibles, rendant leur détection par les victimes difficile sans outils de protection. Si ces attaques ciblent souvent des entités au hasard, elles peuvent se tourner vers les organismes publics en raison de leur sensibilité. Parmi les plus dévastatrices, les attaques se terminant par des rançongiciels sont une menace majeure. Bien que les collectivités territoriales aient vu une diminution des incidents en 2024[1], les établissements d'enseignement supérieur ont été particulièrement ciblés. D'autre part, les prises de position de la France au niveau international entraînent régulièrement des manœuvres de déstabilisation ou des tentatives de sabotage.

Ces attaques peuvent perturber les services essentiels, compromettre la sécurité des données sensibles, générer des coûts financiers considérables et altérer la confiance du public. Des incidents, comme l'arnaque au président subie par le département de Saône-et-Loire[2] ou les fuites de données massives affectant des prestataires du secteur social[3], illustrent l'impact de ces menaces.

Face à cette réalité, les collectivités locales et administrations publiques se heurtent à des défis multiples pour protéger efficacement leurs systèmes d'information : des contraintes budgétaires, la complexité et le vieillissement de leurs infrastructures, une nécessaire sensibilisation des agents publics, l'interconnexion des services et un manque de compétences internes spécialisées en cybersécurité.

Il est essentiel de continuer à développer une stratégie de cybersécurité proactive, axée sur la prévention, la protection, la détection, la supervision et la mutualisation d'expertise. Non seulement pour bloquer les attaques et assurer la résilience des services publics, mais aussi pour satisfaire aux exigences des réglementations comme le RGPD et la directive NIS2. Ces cadres réglementaires fournissent des lignes directrices essentielles pour guider les investissements mais exigent des comptes rendus d'attaques détaillés, impossibles à produire sans outillage ni anticipation.

Ce livre blanc s'appuie sur des ressources documentaires telles que le Panorama de la cybermenace 2024 de l'ANSSI, les recherches d'ESET[4] ou les travaux de cybermalveillance.gouv.fr[5] et les retours terrains de nos équipes. Son ambition est de vous accompagner dans l'identification des risques principaux auxquels vous pourrez être confrontés et de proposer des pistes et des solutions adaptées pour renforcer votre posture de sécurité.

Benoit Grunemwald
Directeur des affaires publiques
ESET France

Qui est concerné ?


Services Publics Administratifs


Services de Sécurité Civile et de Secours


Services Publics de Communication


Services Publics de Logement et Urbanisme


Services Publics de l'Environnement et des Ressources Naturelles


Services Publics de Transport et Mobilité


Services Publics Éducatifs et Culturels


Services Publics Sociaux

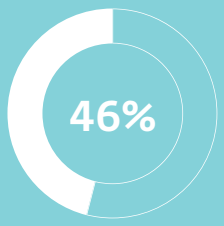
Chapitre 1

Panorama des menaces spécifiques aux collectivités locales

Les collectivités locales et les administrations publiques font face à un paysage de menaces de plus en plus complexe. La diversification des attaques et la sophistication des cybercriminels augmentent les risques pour des organisations souvent sous-préparées.

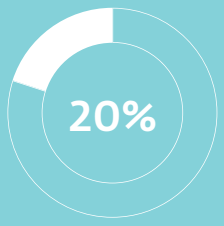
1 collectivité sur 10
déclare avoir déjà été victime d'une ou plusieurs cyberattaques au cours des 12 derniers mois.

ITpublic



46% des cyberattaques ont été réalisées par hameçonnage.

ITpublic



20% des collectivités ont subi une destruction de données, et **20%** ont enregistré une perte financière.

cybermalveillance.gouv

Un exemple concret

En 2023, le département de Saône-et-Loire a été victime d'une arnaque au président, où les attaquants ont usurpé l'identité du président du conseil départemental pour détourner une subvention destinée au SDIS, entraînant une perte de près de 350 000€.

Les différents types de menaces

Les cyberattaques entraînent la perturbation des services essentiels tels que l'eau, l'électricité, les transports, la santé, les secours et l'éducation. Elles compromettent la sécurité des données sensibles des citoyens, génèrent des coûts financiers considérables liés à la gestion des incidents et à la restauration des systèmes, et peuvent gravement altérer la confiance du public envers les institutions.

RANSOMWARES
Les logiciels malveillants chiffrent les données essentielles (données citoyennes, financières) et exigent une rançon pour les débloquer.

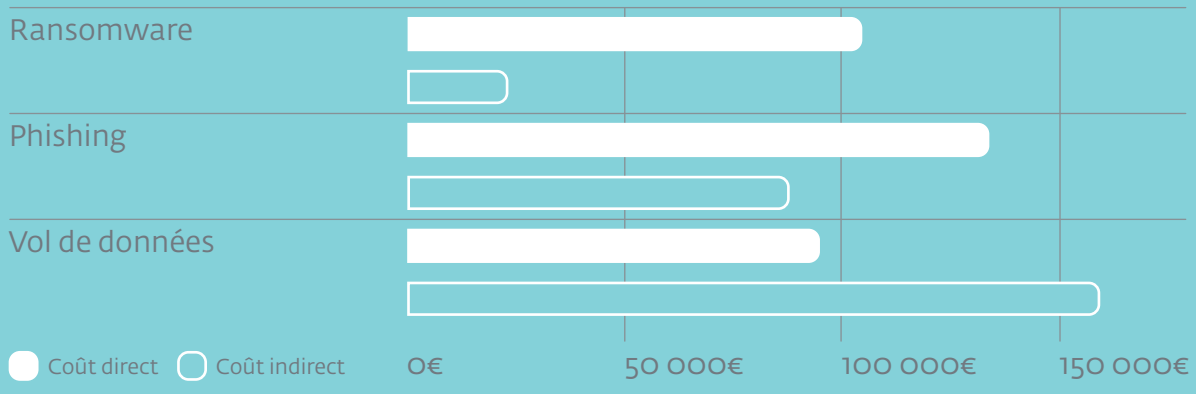
ATTAQUES DDOS
Ces attaques visent à rendre les services publics indisponibles en surchargeant les infrastructures réseau. Elles peuvent paralyser des portails administratifs critiques.

PHISHING ET INGÉNIERIE SOCIALE
L'exploitation de la vulnérabilité humaine est courante. Les e-mails frauduleux incitent les agents à divulguer des informations sensibles ou à cliquer sur des liens malveillants.

INTRUSIONS SUR LES SYSTÈMES DE TRAITEMENT AUTOMATISÉ DES DONNÉES (STAD)
Accès non autorisés pour voler des données, perturber des services ou installer des logiciels espions.

MENACES INTERNES
Erreurs humaines, négligences, ou actions malveillantes de la part d'employés ou de prestataires.

Le coût des attaques



Chapitre 2

Les défis des collectivités locales face aux cybermenaces

Les collectivités locales font face à des défis multiples pour protéger efficacement leurs systèmes de traitement automatisé des données (STAD) contre les cybermenaces. Ces défis sont liés à des contraintes organisationnelles, financières et techniques.

SENSIBILISATION INSUFFISANTE DES AGENTS

Le facteur humain reste l'un des maillons faibles de la cybersécurité. Le manque de formation et de sensibilisation des agents publics aux bonnes pratiques de sécurité accroît les risques d'incidents liés à des erreurs humaines.

MANQUE DE COMPÉTENCES INTERNES

La pénurie de professionnels de la cybersécurité est un défi récurrent. De nombreuses collectivités n'ont pas les moyens de recruter des experts spécialisés, ce qui limite leur capacité à détecter et réagir rapidement aux incidents de sécurité.

INTERCONNEXION DES SERVICES

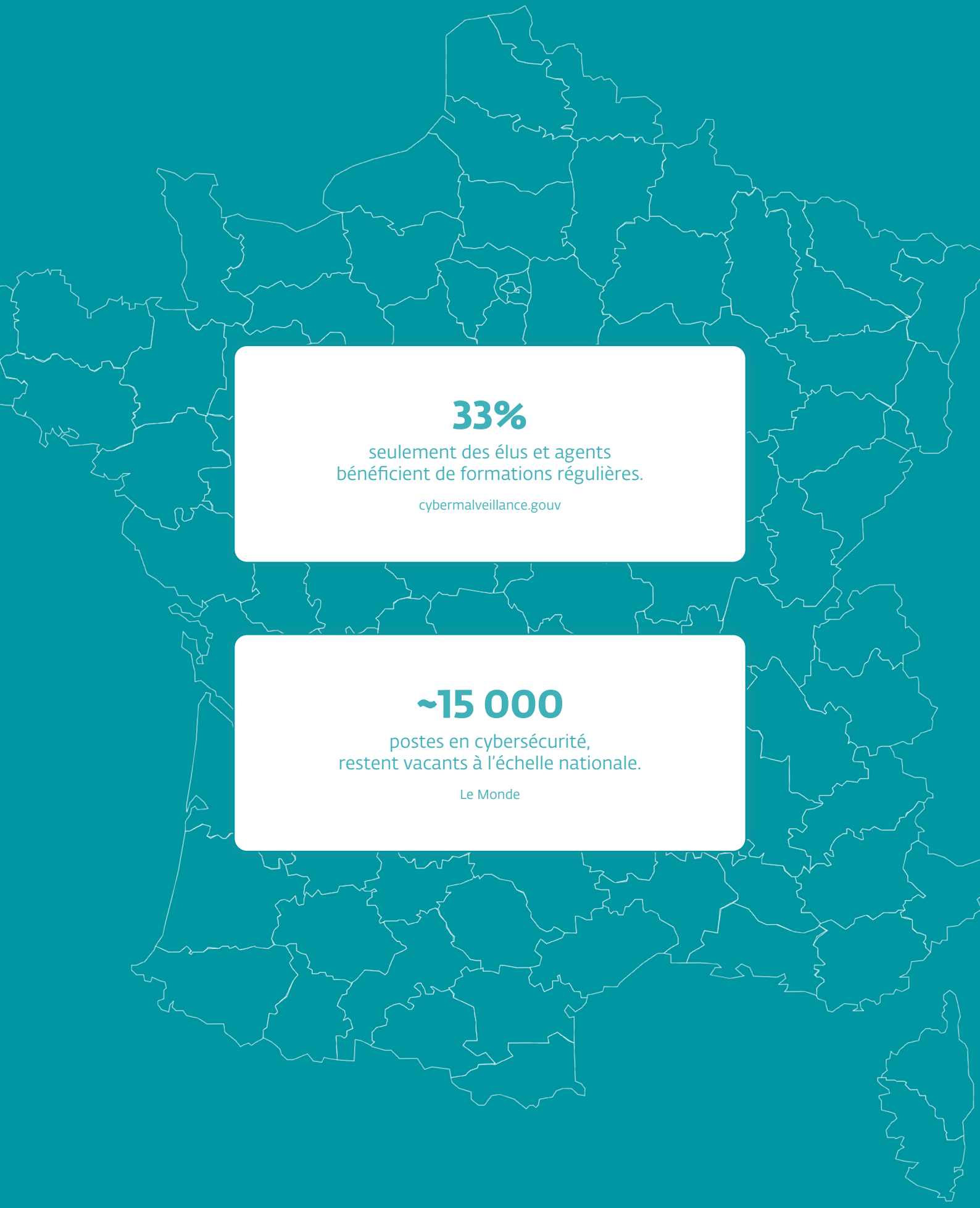
La numérisation croissante des services publics entraîne une interconnexion des STAD, augmentant la surface d'attaque potentielle. Une faille dans un système peut rapidement se propager à d'autres services critiques.

COMPLEXITÉ DES STAD

Les collectivités gèrent des infrastructures informatiques hétérogènes et souvent vieillissantes. La cohabitation de systèmes anciens avec des technologies plus récentes crée des vulnérabilités difficiles à corriger.

CONTRAINTES BUDGÉTAIRES

Les ressources financières limitées sont l'un des principaux obstacles à la mise en place de politiques de cybersécurité robustes. Les collectivités doivent souvent arbitrer entre des investissements dans des infrastructures essentielles et des dépenses en cybersécurité, ce qui conduit à des systèmes sous-financés et vulnérables.



33%

seulement des élus et agents
bénéficient de formations régulières.

cybermalveillance.gouv

~15 000

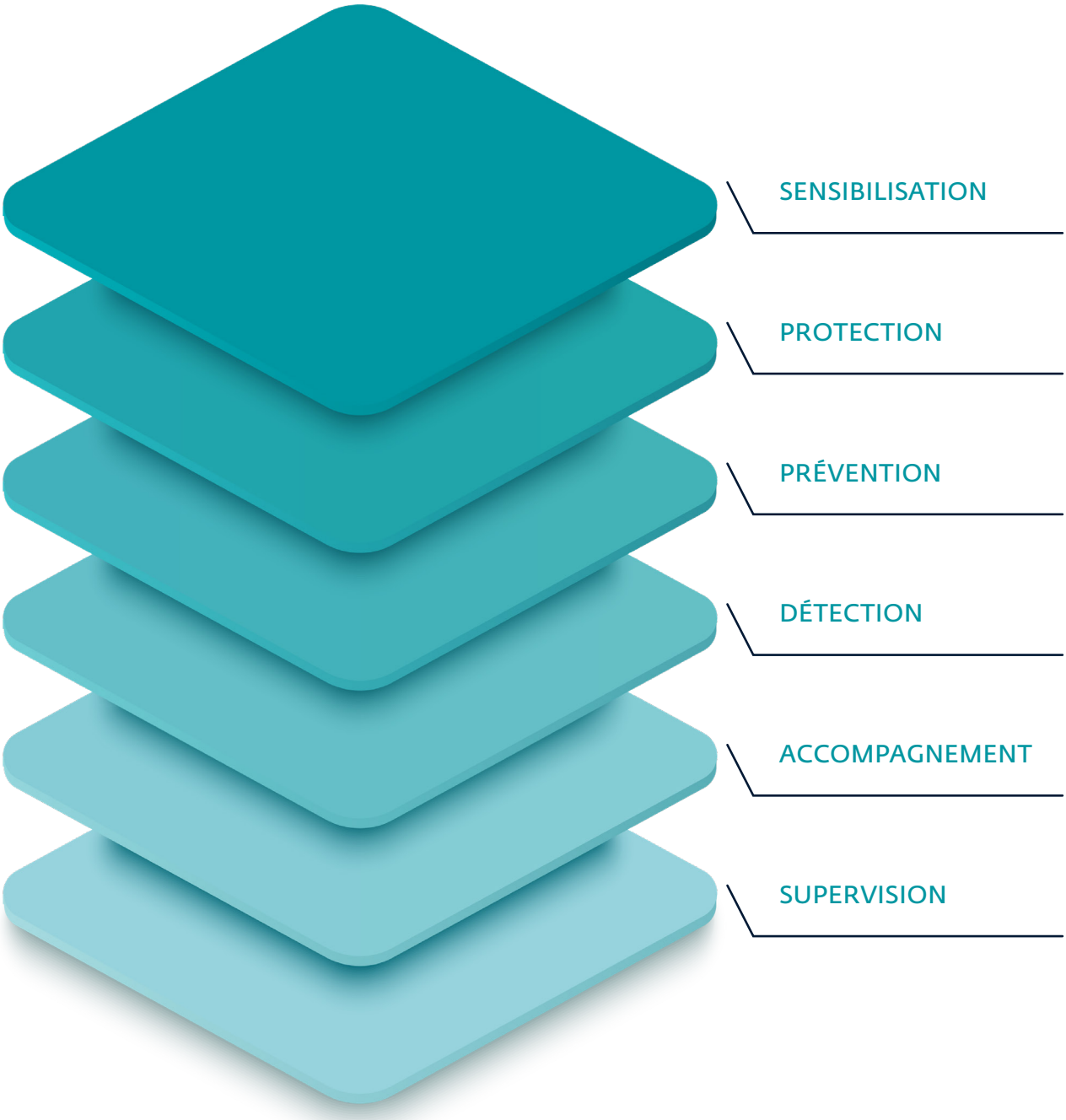
postes en cybersécurité,
restent vacants à l'échelle nationale.

Le Monde

Chapitre 3

Renforcer la cybersécurité des collectivités locales

Face aux cybermenaces croissantes, les collectivités locales doivent adopter des mesures stratégiques et technologiques pour renforcer leur résilience.



Développer une stratégie de cybersécurité adaptée n'est plus une option, mais une nécessité.

SENSIBILISATION

Former les équipes aux bonnes pratiques, comme l'usage de mots de passe robustes et la vigilance face aux e-mails frauduleux. Des ateliers réguliers renforcent la culture de la cybersécurité et impliquent chacun dans la protection de son environnement.

PROTECTION

Il existe des solutions de sécurité pour entreprises accessibles et efficaces qui permettent de sécuriser les STAD en bloquant les tentatives d'intrusion, avec des fonctionnalités centralisées qui simplifient la gestion et optimisent le budget.

PRÉVENTION

C'est en anticipant que l'on réduit la surface d'attaque. Il est nécessaire de sécuriser les accès, de limiter les privilèges des utilisateurs selon leurs besoins réels, et de définir des règles claires pour le partage de fichiers, la navigation et la gestion des mots de passe.

DÉTECTION

Les solutions d'Endpoint Detection & Response (EDR/XDR) permettent d'identifier des comportements anormaux sur les postes de travail et serveurs. Elles offrent une visibilité en temps réel sur les incidents potentiels et facilitent une réponse rapide avant qu'une menace ne se propage.

ACCOMPAGNEMENT

Les collectivités peuvent bénéficier de l'expertise d'entités spécialisées en cybersécurité comme le CERT FR, ou de partenaires tels que les éditeurs de solutions de sécurité. Ces collaborations facilitent l'accès à des technologies de pointe et à des compétences spécifiques pour renforcer la résilience des infrastructures publiques.

SUPERVISION

En s'appuyant sur des équipes d'experts qui sont disponibles 24/7, les services de Managed Detection & Response (MDR) permettent une détection plus précise des menaces (85 % contre 60 % en moyenne pour les solutions classiques) et garantissent une réponse rapide en cas d'incident.

Chapitre 4

Réglementations & conformité

Un cadre renforcé pour la cybersécurité des services publics

Conformité réglementaire et protection des données

Les collectivités doivent respecter des réglementations strictes en matière de protection des données, notamment le RGPD, la directive européenne NIS2 et les recommandations de l'ANSSI. Les solutions ESET intègrent des fonctionnalités qui facilitent la conformité à ces exigences et assurent la protection des données sensibles des citoyens et des administrations.

Le **Règlement Général sur la Protection des Données (RGPD)** impose aux collectivités de garantir la confidentialité et la protection des informations personnelles des citoyens. Cela implique un contrôle strict des accès aux données, des mesures de protection contre les fuites de données et la conservation sécurisée et le chiffrement des données sensibles.

La récente directive **Network and Information Security (NIS2)** impose, elle, des exigences accrues aux entités essentielles, incluant certaines administrations publiques et collectivités locales.

PRINCIPALES OBLIGATIONS

1. ÉVALUATION ET GESTION DES RISQUES
   Mise en place d'une politique de cybersécurité proactive.

2. NOTIFICATION DES INCIDENTS
   Obligation de signaler toute cyberattaque majeure dans un délai restreint.

3. SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT
   Vérification des prestataires et partenaires.

Les offres ESET

La valeur ajoutée d'ESET

ESET est un leader mondial de la cybersécurité reconnu pour son expertise et son engagement à protéger les infrastructures critiques. Pour les collectivités locales, choisir ESET signifie bénéficier d'une protection avancée, adaptée aux besoins et budgets spécifiques des administrations publiques.

EXPERTISE ET SUPPORT LOCAL

ESET met à disposition des collectivités des équipes locales d'experts en cybersécurité pour les accompagner tout au long du processus. L'implémentation et la configuration des solutions bénéficient d'un suivi personnalisé. Le support technique est réactif et disponible en français, avec des niveaux d'assistance adaptés aux besoins des administrations. ESET propose également des formations et des campagnes de sensibilisation afin d'améliorer la posture de sécurité des agents publics.

UNE SOLUTION ADAPTÉE AUX COLLECTIVITÉS

Conscientes des contraintes budgétaires et des besoins en cybersécurité des collectivités, les solutions ESET sont faciles à déployer et à administrer grâce à une console de gestion centralisée. Elles sont compatibles avec les infrastructures existantes et peu gourmandes en ressources, garantissant ainsi un haut niveau de sécurité sans affecter la performance des systèmes.

Une Protection Multicouche

ESET propose une approche de cybersécurité multicouche spécifiquement adaptée aux défis du secteur public afin de les aider à se mettre en conformité :

- **Protection des endpoints** pour sécuriser les appareils
- **Chiffrement** des données sensibles
- **Authentification Multifacteur** pour renforcer les accès
- **Extended Detection & Response (XDR)** pour la détection avancée des menaces
- **Managed Detection & Response (MDR)** pour la gestion proactive des incidents

ESET propose des tarifs adaptés au secteur public, permettant d'accéder à des solutions avancées à coût maîtrisé, optimisant ainsi la sécurité et le budget.

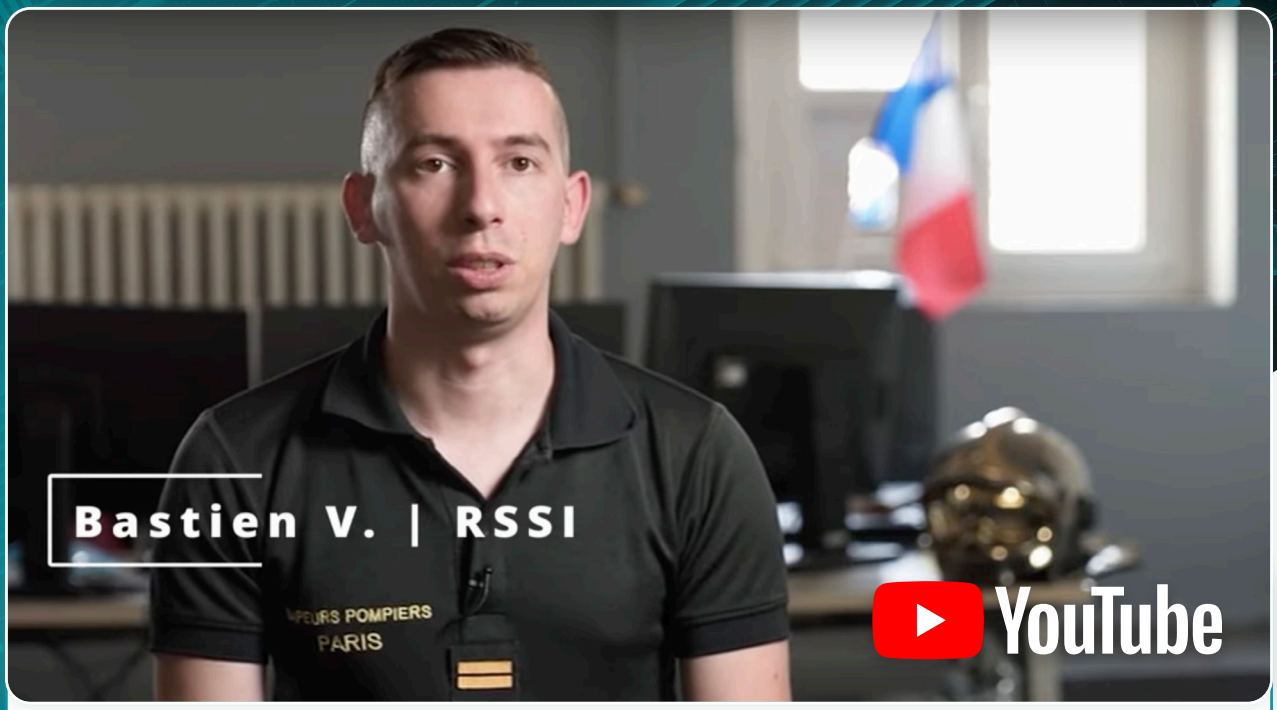
Témoignages

Découvrez les témoignages de la Gendarmerie nationale et de la Brigade des sapeurs-pompiers de Paris sur ESET et comment leurs équipes bénéficient de ses solutions de cybersécurité.

https://www.youtube.com/watch?v=A-Rhgbv2U1Q

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

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



https://www.youtube.com/watch?v=cV-p1cY4k-M

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

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

Conclusion

Face à l'augmentation des cyberattaques et à des exigences réglementaires de plus en plus strictes, les collectivités locales doivent impérativement renforcer leur posture de sécurité afin de protéger les infrastructures publiques et garantir la continuité des services essentiels. Le respect des cadres comme NIS2, le RGPD ou encore les recommandations de l'ANSSI nécessite une approche rigoureuse, proactive et adaptée aux réalités du secteur public.

Acteur européen de référence en matière de cybersécurité, ESET accompagne les collectivités avec des solutions éprouvées, alliant efficacité, conformité et simplicité de gestion. En plus de proposer des tarifs préférentiels spécialement conçus pour le secteur public, ESET bénéficie déjà de la confiance de structures majeures comme la Gendarmerie nationale ou les Pompiers de Paris.

Choisir ESET, c'est opter pour une cybersécurité robuste, durable et en parfaite adéquation avec les besoins et contraintes des administrations publiques.

À propos d'ESET

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

ESET, entreprise européenne de cybersécurité reconnue mondialement, se positionne comme un acteur majeur dans la protection numérique grâce à une approche technologique innovante et complète. Fondée en Europe et disposant de bureaux internationaux, ESET combine la puissance de l'intelligence artificielle et l'expertise humaine pour développer des solutions de sécurité avancées, capables de prévenir et contrer efficacement les cybermenaces émergentes, connues et inconnues.

Ses technologies, entièrement conçues dans l'UE, couvrent la protection des terminaux, du cloud et des systèmes mobiles, et se distinguent par leur robustesse, leur efficacité et leur facilité d'utilisation, offrant ainsi une défense en temps réel 24/7 aux entreprises, infrastructures critiques et utilisateurs individuels. Grâce à ses centres de recherche et développement et son réseau mondial de partenaires, ESET propose des solutions de cybersécurité intégrant un chiffrement ultra-sécurisé, une authentification multifactorielle et des renseignements approfondis sur les menaces, s'adaptant constamment à l'évolution rapide du paysage numérique.

MADE IN EUROPE

CYBER TASK FORCE

CLUSIF

Plus de 30 ans
d'innovation continue

1er éditeur Européen
de solutions de sécurité

Focus continu
sur la technologie

Détenu par
ses fondateurs

www.eset.com/fr