



Circet France sécurise 6 000 terminaux avec Action1 pour garantir une connectivité fiable à l'échelle nationale

Leader des télécommunications en France, Circet adopte une approche proactive et conforme à la norme ISO 27001 pour la gestion des vulnérabilités, garantissant une disponibilité constante et un haut niveau de sécurité.



Historique de l'entreprise:

Circet France est un leader de l'installation d'infrastructures télécoms, spécialisé dans le déploiement, la modernisation et la maintenance des réseaux fixes et mobiles. Partenaire des grands opérateurs, Circet accompagne le développement de la fibre, de la 5G et des technologies de demain, au service de la connectivité sur tout le territoire.

Localisation : Solliès-Pont (83), France

Secteur : Déploiement fibre / Télécoms

Site web : www.circet.fr

Endpoints : 6,000

Faire face à l'absence de cadre structuré et au déficit de visibilité dans un contexte de cybersécurité en mutation constante

En tant qu'acteur majeur des télécommunications en France, Circet joue un rôle essentiel dans le déploiement et la maintenance des infrastructures qui assurent la connectivité du pays, de la fibre optique à la 5G. Une telle responsabilité exige une continuité de service sans faille et une cybersécurité renforcée, indispensables pour maintenir les standards de qualité de Circet et protéger les infrastructures nationales critiques.

L'un des objectifs stratégiques du service informatique de Circet était de mettre en place une stratégie unifiée et complète de gestion des correctifs afin de réduire de manière proactive les risques de sécurité dans un environnement IT complexe. Bien que plusieurs couches de protection aient été déployées, l'équipe ne disposait pas d'une solution fiable pour automatiser le déploiement des mises à jour de sécurité, un aspect clé d'un processus de remédiation des

vulnérabilités robuste et réactif. « **Notre gestion des correctifs manquait de structure et d'automatisation,** » explique Franck Andreux, Directeur de la Sécurité des Systèmes d'Information et Responsable Cybersécurité chez Circet France. En raison de cette configuration morcelée, le département IT manquait de visibilité sur l'état réel des vulnérabilités et des correctifs en place. Cela augmentait le risque de retards dans les mises à jour, de non-conformité et d'exposition potentielle aux cyberattaques.

Faute de visibilité suffisante sur les terminaux, d'absence d'automatisation et de capacités de reporting, l'équipe IT devait s'appuyer sur des efforts manuels pour gérer les correctifs et répondre aux exigences de conformité – un processus inefficace qui mobilisait du temps et des ressources précieuses. « **Nous souhaitons proactivement renforcer notre cybersécurité en nous dotant d'outils plus adaptés et centralisés,** » ajoute Franck Andreux. « **Pour nous, en tant qu'organisation certifiée ISO 27001 depuis 2022, disposer d'un cadre de sécurité cohérent est un pilier fondamental de notre stratégie IT.** »

Franck et son équipe ont alors entrepris la recherche d'une solution robuste et tout-en-un, capable de rationaliser la gestion des vulnérabilités et des correctifs, tant pour les systèmes d'exploitation que pour les applications tierces.

Trouver la plateforme qui couvre tout

Après une évaluation approfondie des solutions, les équipes techniques de Circet France ont choisi Action1 pour ses puissantes fonctionnalités d'autogestion des terminaux, clients et serveurs, incluant la gestion unifiée et automatisée des correctifs pour les systèmes d'exploitation et les applications tierces ainsi que des fonctions de scan et d'évaluation des vulnérabilités en temps réel. De plus, les équipes ont apprécié les capacités de scripting d'Action1 ainsi que la possibilité de déployer et gérer des paquets personnalisés, apportant une valeur ajoutée supplémentaire à leurs opérations IT.

Renforcer la sécurité, l'efficacité et la conformité grâce à la gestion automatisée des vulnérabilités

L'un des bénéfices immédiats du déploiement d'Action1 a été une visibilité et un contrôle accrus sur l'environnement IT depuis une console unique. Cette visibilité en temps réel, offerte par Action1, a posé les bases d'un processus structuré et efficace de remédiation des vulnérabilités. « **Nous avons pu reprendre pleinement le contrôle de nos machines,** » a déclaré Franck Andreux. « **Le scan de vulnérabilités et l'évaluation des postes sur Action1 nous donnent une vision claire de notre environnement et des risques associés.** »

Grâce à ces nouvelles données, l'IT a pu mettre en place une stratégie de gestion des correctifs complète et structurée. En exploitant les capacités d'automatisation d'Action1, ainsi que sa souplesse dans la définition de politiques personnalisées, elle a affiné l'ensemble du processus. Des phases de pré-production ont notamment été instaurées pour tester les correctifs en amont, avant leur déploiement massif sur des milliers de postes. Cette approche rigoureuse a permis d'éliminer les perturbations potentielles et d'optimiser la fiabilité des mises à jour. Résultat : plus de 10 000 vulnérabilités corrigées, une surface d'attaque drastiquement réduite et un environnement nettement plus sécurisé pour Circet.

Un autre gain important pour Circet a été l'amélioration de l'efficacité de ses équipes, obtenue grâce à l'automatisation des tâches routinières, telles que le déploiement des mises à jour, l'exécution de scripts et la suppression des logiciels non autorisés. Par exemple, l'IT a facilement géré la mise à niveau des postes de Windows 10 vers Windows 11 via une politique d'automatisation, évitant l'installation manuelle de la nouvelle version sur chaque appareil et économisant ainsi un temps considérable.

Aujourd'hui, toute l'infrastructure IT de Circet est gérée par un seul technicien à plein temps utilisant Action1, ce qui permet au reste de l'équipe de se concentrer sur d'autres tâches.



Avec Action1, nous avons pu reprendre pleinement le contrôle sur nos machines. Nous bénéficions désormais d'un environnement plus sécurisé, d'une réponse plus rapide aux vulnérabilités critiques et d'une efficacité opérationnelle accrue.

Franck Andreux, Directeur de la Sécurité des Systèmes d'Information et Responsable Cybersécurité chez Circet France

Franck Andreux a souligné qu'Action1 est devenu clé pour maintenir la conformité à la norme ISO 27001 au sein de leur organisation. Ses puissantes automatisations, ses capacités avancées de déploiement et sa piste d'audit intégrée aident l'équipe à rester alignée avec les standards de sécurité ISO 27001. « **Aujourd'hui, nous bénéficions d'une meilleure traçabilité, d'une réduction significative des interventions manuelles, et d'un environnement plus sécurisé, avec des temps de réaction plus courts en cas de vulnérabilité critique,** » a expliqué Franck.

Grâce à Action1, le service IT de Circet est devenue une force structurée et proactive dans la gestion des vulnérabilités. L'entreprise a non seulement renforcé sa posture de sécurité, mais a également franchi un cap en matière d'efficacité opérationnelle, permettant à son équipe d'anticiper les menaces émergentes avec sérénité.



SIGN UP
action1.com/signup



WATCH DEMO
action1.com/watch



SWITCH TO ACTION1
action1.com/switch