Elever le niveau de sécurité de la gestion des accès tout en optimisant l'expérience utilisateur

Enjeux :

> Répondre aux enjeux liés au virage ambulatoire pour l'accès à distance au DPI

> Réduire la surface d'exposition du SI en s'appuyant sur une stratégie Zero Trust

> Optimiser l'expérience utilisateur tout en simplifiant les tâches de l'équipe IT

Solutions :

> cyberelements Access
> cyberelements Cleanroom
> cyberelements Gate
> cyberelements Identity
> Virtual Desktop Workplace

Bénéfices :

> Améliorer l'expérience utilisateur

> Elever le niveau de sécurité des accès à distance

> Supprimer le risque cyber lié aux « comptes orphelins »

« Nous avons établi une relation de proximité et de confiance avec Systancia qui est un partenaire sur lequel nous pouvons compter. Les équipes nous accompagnent depuis plusieurs années dans la mise en œuvre de notre stratégie Zero Trust pour réduire notre surface d'exposition et répondre aux enjeux liés au virage ambulatoire de notre offre de soin qui nécessite un accès flexible et hautement sécurisé aux données de santé. »

Stéphane Wicker *-*
Responsable des Services Numériques

Les enjeux

L'EPSM Metz Jury est un établissement public de santé mentale, membre du Groupement Hospitalier de Territoire Lorraine Nord, qui prend en charge les patients des secteurs de psychiatrie au centre et au nord de la Moselle. L'EPSM regroupe les pôles psychiatrie adultes, psychiatrie infanto juvénile et addictologie ce qui représente plus de 750 agents (dont 55 personnels médical et près de 680 personnels non médical). Il est composé d'un hôpital qui dispose de 156 lits, mais également de centres médicaux psychologiques, d'hôpitaux de jour et de cliniques, ce qui représente une vingtaine de sites distants.

L'EPSM Metz Jury a passé avec succès le virage ambulatoire, ce qui réduit drastiquement les hospitalisations longues et favorise les déplacements en soin ambulatoire, en centres médicaux psychologiques ou en soin psychiatrique intensif à domicile. L'établissement a donc eu besoin de mettre en place des solutions favorisant une mobilité sereine et sécurisée du personnel soignant et de l'ensemble des agents.

Le besoin originel en 2016, qui était de simplifier les tâches d'administration de l'équipe IT tout en améliorant l'expérience utilisateur, a amené l'EPSM à déployer Virtual Desktop Workplace, en remplacement de la solution Citrix vieillissante, pour virtualiser les applications métiers. Puis, toujours avec la volonté d'offrir aux agents une expérience utilisateur optimale, tout en élevant le niveau de sécurité des accès, l'EPSM a décidé de déployer cyberelements Access, solution de SSO permettant une authentification unique, cyberelements Gate, solution de ZTNA, pour sécuriser les accès distants des soignants dans le cadre des soins ambulatoires, et cyberelements Cleanroom pour sécuriser les accès à privilèges des prestataires.

Précurseur en matière de mobilité sécurisée, l'EPSM était ainsi prêt, lors du confinement en mars 2020, à proposer du jour au lendemain le télétravail à l'ensemble de son personnel.

Puis, afin de supprimer le risque cyber lié aux comptes toujours actifs du personnel ayant quitté l'établissement, l'EPSM a mis en place cyberelements Identity, solution d'Identity Governance and Administration permettant une gestion rigoureuse des identités et des habilitations des agents.

Améliorer l'expérience utilisateur

Dès 2016, afin de permettre un accès flexible aux applications à l'ensemble du personnel, l'EPSM a souhaité remplacer ses fermes Citrix vieillissantes. *« Après différents tests, notre choix s'est porté sur la solution Virtual Desktop Workplace qui nous a permis de gagner en efficacité »*, explique Stéphane Wicker, Responsable des Services Numériques de l'EPSM. Aujourd'hui, l'ensemble des applications métiers, dont le Dossier Patient Informatisé (DPI) sont publiées via le portail Virtual Desktop Workplace (HTML 5), alors que les applications bureautiques et les accès Internet sont en local sur les postes de travail. *« Nous avons ainsi mis en place un cloisonnement sécuritaire, en adéquation avec notre stratégie Zero Trust. »*

L'EPSM a ensuite mis en place une authentification simplifiée pour ses utilisateurs en déployant cyberelements Access, solution d'authentification SSO qui permet d'authentifier de manière transparente les utilisateurs sur leurs applications dès qu'ils se connectent au portail d'accès.

Elever le niveau de sécurité des accès à distance

Il y a eu ces dernières années une vraie mutation en matière de soins. Auparavant il suffisait d'installer des postes de travail dans les services de soins de l'hôpital. Aujourd'hui de plus en plus de personnels soignants sont amenés à aller voir les patients chez eux ou dans des structures distantes de l'hôpital. Pour répondre à cet enjeu d'accès flexible et sécurisé aux applications métiers, l'EPSM a déployé cyberelements Gate pour favoriser l'accès des collaborateurs en mobilité ou en situation de télétravail.

Ainsi les soignants du service psychiatrique intensif à domicile, accèdent de manière sécurisée aux dossiers patients à distance depuis des postes managés par l'établissement. Dans le cadre du télétravail les agents peuvent utiliser les postes de l'établissement ou leur poste personnel. *« Nous avons renforcé l'authentification primaire en mettant en place du MFA, OTP via SMS, et réduit notre surface d'exposition en mettant en place des règles de sécurité liées au contexte d'accès. »*

Parallèlement, l'EPSM Metz Jury souhaitait pouvoir contrôler les actions des prestataires externes. La DSI a donc fait l'acquisition de la solution cyberelements Cleanroom, dans le but de surveiller les actions de ces utilisateurs à pouvoirs sur le SI. La solution enregistre les sessions des prestataires et la fonctionnalité Live Streaming permet de visionner en temps réel les actions menées et de réagir immédiatement en cas de problèmes détectés, en décidant de suspendre ou d'interrompre la session. *« cyberelements Cleanroom est indispensable, je ne peux plus m'en passer. La solution nous donne des yeux, c'est-à-dire que l'on peut voir en temps réel ce qui se passe sur le SI ce qui élève nettement le niveau de sécurité de nos accès. »*

Supprimer le risque cyber lié aux « comptes orphelins »

« Le risque cyber identifié comme n°1 au sein de l'établissement était le maintien des accès aux agents qui n'étaient plus dans l'établissement. Nous n'avions pas l'information en temps et en heure concernant les arrivées et les départs des agents ce qui nous a amené à rechercher une solution permettant une gestion rigoureuse des accès.» explique Stéphane Wicker. En 2023, l'EPSM a donc décidé de déployer cyberelements Identity pour automatiser cette gestion.

Auparavant, l'équipe IT créait les comptes d'accès manuellement, ce qui était extrêmement chronophage et comportait de nombreux risques d'erreurs. Aujourd'hui, Systancia Identity s'appuie sur le référentiel RH pour créer les comptes AD, provisionner de manière automatisée 70% des droits d'accès et déprovisionner les comptes lors des départs.

« Nous sommes bluffés par la puissance de l'outil qui génère des alertes précises au bon moment, pour un changement de nom par exemple, et nous permet de gagner un temps considérable que nous pouvons consacrer à des projets plutôt qu'à des tâches fastidieuses sans valeur ajoutée. » conclut Stéphane Wicker.

À propos de Systancia

Systancia est un éditeur de logiciels de cybersécurité indépendant et souverain, animé par le concept de Zero Trust.
Notre mission est de fournir aux organisations les éléments cyber nécessaires pour booster leur performance grâce à la confiance numérique. Pour ce faire, nous réunissons nos propres technologies dans une plateforme unique, combinant rapidité et facilité d'utilisation pour favoriser la productivité des utilisateurs et la performance des organisations.

La plateforme Zero Trust de Systancia permet de donner aux collaborateurs ou aux prestataires, quel que soit leur contexte (au bureau, en télétravail, chez un prestataire, opérateur industriel …) un accès transparent, immédiat, sécurisé et tracé (métier ou privilégié, local ou distant, …) à toutes les ressources dont ils ont besoin pour travailler (applications cloud, applications dans le datacenter de l'organisation, postes de travail, données, infrastructures informatique ou industrielles, services).