Indominus
Services-conseils

Notre implication dans le projet a permis de dresser une feuille de route efficace et intelligente afin de limiter les vulnérabilités au niveau de la cybersécurité.

ESI TECHNOLOGIES

FICHE DE PROJET
AUDIT DE CYBERSÉCURITÉ (PHASE 1)

CLIENT

CENTRE INTÉGRÉ UNIVERSITAIRE EN SANTÉ ET SERVICES SOCIAUX DE L'ESTRIE | CENTRE HOSPITALIER UNIVERSITAIRE DE SHERBROOKE (CIUSS DE L'ESTRIE ET CHUS)

DÉFI

Évaluer les capacités en cybersécurité en tenant compte du nouveau cadre établi par le Ministère de la Santé et des Services sociaux.

Exécution

Notre équipe, en collaboration avec ESI technologies, s'est appuyé sur une méthodologie en deux étapes menées en parallèle ; l'audit par ateliers et les tests d'intrusion. Tout d'abord, dès que le protocole d'intervention fut approuvé par le client, nous avons procédé à une série d'entretiens avec les équipes responsables des divers départements. Ces ateliers nous ont permis de collecter les données nécessaires en matière de cybersécurité en tenant un registre complet des preuves fournies et en les classifiant. Pour compléter cette phase d'information, nous avons procédé à des tests de défaillance pour détecter les vulnérabilités susceptibles de faire l'objet d'une attaque. L'une des défis majeur de ce mandat résidait dans l'importance d'une confidentialité totale des données.

Résultats

L'audit par ateliers ainsi que les tests d'intrusion, nous ont permis de tracer un portrait de l'état de santé de la cybersécurité du CIUSSS de l'Estrie en lien avec le nouveau cadre référentiel de sécurité fondé sur ISO 27002. C'est grâce à ce portrait que nous avons pu présenter nos recommandations au Conseil d'administration afin d'optimiser la structure en place.

Personne-ressource : Joël Paradis