ÉTUDE DE CAS

HITACHI
Inspire the Next

SERVICES GÉRÉS DE SÉCURITÉ POUR UNE MUNICIPALITÉ

EN BREF

Industrie : Secteur public

Type d'entreprise : Municipalité

Localisation : Canada

Employés : plus de 10 000

Besoins et exigences :

- Sécuriser les actifs informationnels corporatifs contre toutes vulnérabilités et intrusions
- Répondre aux exigences annuelles de conformité PCI DSS
- Informer l'équipe exécutive de toutes nouvelles observations
- Surveiller l'infrastructure 24 heures sur 24, 7 jours sur 7
- Réduire la charge de travail de l'équipe TI interne

ENJEUX

La ville a connu une croissance exponentielle en raison d'importantes vagues d'immigration au cours des dernières années. Celle-ci a pu maintenir le pas, répondant aux besoins de son nombre grandissant de citoyens, tout en gagnant en efficacité par la mise en œuvre de-services variés. La ville fournit près de 250 services distincts développés par 15 unités opérationnelles pour environ 1 million de citoyens. Nombreux services sont soutenus par l'infrastructure TI de la ville, consistant en un réseau géographiquement généralisé contenant de multiples catégories de données publiques comme sensibles. Quelques parties segmentées de l'environnement informatique font l'objet d'exigences rigoureuses en matière de conformité, telle que la Norme de Sécurité des Données de l'Industrie des Cartes de Paiement (PCI DSS), ou bien même, elles ont de très hautes exigences de disponibilité, tel que l'environnement des communications des Services de Police et des Incendies avec une exigence de disponibilité à hauteur de 99,999%.

Tout comme de nombreuses autres équipes de sécurité de l'information au sein des gouvernements municipaux, l'équipe de la ville était constituée d'un petit nombre d'analystes fournissant des services réactifs pendant les jours ouvrés de la semaine. Les services du soir, de la nuit et des fins de semaine sont couverts par la rotation du récepteur pour les incidents critiques. Considérant les cas de brèches de sécurité ne prenant que quelques minutes alors que la capacité d'une organisation à réagir à une telle situation se compte en jours, semaines, voire en mois, le temps joue en la faveur de l'attaquant en considérant le meilleur modèle traditionnel d'investissement en matière de sécurité.

De plus, la solution de Gestion des Informations et Évènements de Sécurité (SIEM) de la ville a pris fin et n'apportait aucune valeur car l'équipe TI manquait simplement de temps pour maintenir la solution tout en gardant les règles opérationnelles à jour.

SOLUTION

Faisant face à des difficultés pour recruter et conserver les ressources spécialisées requises pour une surveillance proactive de la sécurité 24 heures sur 24, 7 jours sur 7, la ville a décidé d'engager un fournisseur canadien de services gérés de sécurité (Managed Security Service Provider/MSSP) pour compléter son équipe interne et gérer des alertes générées par des outils déjà déployés dans son environnement.

Hitachi Systems Security a déployé son service de surveillance des menaces, consistant en un contrôle continu en temps réel et une gestion des menaces internes et externes pouvant affecter l'environnement du réseau de la ville. Soutenue par des Analystes de Sécurité de l'Information certifiés d'Hitachi Systems Security, un déroulement des opérations sur mesure pour la maîtrise des incidents et la corrélation des évènements a été personnalisé pour répondre aux processus et exigences de gestion de la menace de la ville. Maintenant, toute activité malveillante, perte de données ou évènement de menace est identifié et validé par l'équipe d'Hitachi Systems Security qui informe alors l'équipe TI de la ville de la menace potentielle afin qu'une action corrective puisse être prise.

Les services de gestion des journaux ont également été déployés pour étendre les capacités de gestion des menaces, fournissant des données référentielles vitales acquises par la collecte et le traitement des informations du registre historique. Ce service est essentiel pour assurer la bonne enquête des intrusions. Il peut aider à l'audit et constitue un élément obligatoire pour nombreux programmes de conformité tel que le PCI DSS. Tous ces services sont offerts par l'ensemble du réseau mondial des centres des opérations de sécurité d'Hitachi Systems Security.

AVANTAGES PRINCIPAUX

Grâce aux services gérés de sécurité d'Hitachi Systems Security Inc., la ville bénéficie d'une équipe de réponse aux incidents qui est opérationnelle 24 heures sur 24, 7 jours sur 7, celle-ci étant désormais nécessaire pour faire face aux menaces ciblées avancées et initiées. La ville a ainsi été capable de :

- Obtenir une visibilité en temps réel des menaces impactant l'environnement TI de la ville d'une manière hiérarchisée
- Faciliter les audits annuels PCI DSS grâce à la piste de vérification laissée par la console de surveillance de la menace
- Parvenir à un temps de réaction aux incidents de sécurité bien supérieure
- Augmenter le rapport signal/bruit afin que les employés de la ville puissent être impliqués seulement si nécessaire et optimiser leur temps précieux
- Améliorer le rapport de gestion avec des comptes-rendus exécutifs mensuels produits par les Analystes de Sécurité de l'Information certifiés d'Hitachi Systems Security
- Renforcer la posture de sécurité globale de la ville
- Parvenir à une uniformité et une efficacité qui s'étendent à travers toute l'organisation, laissant davantage de temps aux employés de sécurité TI de la ville pour s'impliquer dans des activités à valeur ajoutée
- Utiliser les frais de gestion et de permis annuels à hauteur de 100 000 $ liés à la solution complexe SIEM d'une façon plus efficace en

SERVICES FOURNIS

Une équipe d'experts chevronnés en cybersécurité d'Hitachi Systems Security Inc. a collaboré avec les ressources de sécurité TI de la ville sur ce projet pour :

- Effectuer une surveillance de la cybersécurité de son infrastructure TI de manière continue, 24 heures sur 24, 7 jours sur 7, 365 jours dans l'année
- Déployer un large capteur conçu comme remplacement une fois la solution SIEM en fin de vie
- Configurer le service et personnaliser le moteur de corrélation, conduisant à une augmentation itérative perpétuelle de l'efficacité
- Rapporter toute activité de la menace dans les 15 minutes suite à sa détection
- Offrir un balayage de vulnérabilités en libre-service
- Fournir l'archivage de données sur site pour les enquêtes du registre historique et répondre aux exigences de conformité

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, bureau 244, Blainville (Québec) J7C 5J6 Canada
Tél: +1 450-430-8166 Fax: +1 450-430-1858
www.hitachi-systems-security.com