ITRUST.

ÉTUDE DE CAS

Opter pour le SOC Managé d'ITrust

SECTEUR : Bancaire

POURQUOI ITRUST ?

La plateforme SOC innovante d'ITrust est dotée d'une technologie unique d'analyse comportementale reposant sur des techniques d'intelligence artificielle. Il permet de détecter efficacement les APT, virus et attaques sophistiquées. Équipée d'une technologie mêlant IA et threat intelligence, elle permet de capitaliser sur les évènements qui ont pu menacer le système d'information. Le SOC ITrust est préconfiguré par des moteurs de corrélations développés depuis une décennie par nos équipes de R&D en collaboration avec des laboratoires de recherche.

CONTEXTE

Une banque d'affaires de référence en France, spécialisée dans le financement du commerce extérieur, regroupant une centaine de collaborateurs.
L'établissement a souhaité mettre en place une politique d'amélioration et de sécurisation de son système d'information, afin de faire face à des risques croissants et à un environnement normatif et réglementaire plus contraignant.
L'objectif de cette politique visait à réduire le risque cyber et à se conformer aux recommandations du régulateur, l'ACPR (autorité de contrôle prudentiel et de résolution).

ENJEUX

UN RISQUE CYBER CROISSANT POUR LES BANQUES

Par exemple, la banque Centrale du Bangladesh a été victime en mai 2016 d'une cyberattaque ayant permis aux cybercriminels de dérober un total de 80 millions de dollars. Les cybercriminels avaient exploité des failles de sécurité et gagné l'accès au réseau interbancaire SWIFT, utilisé pour opérer des virements entre différents établissements bancaires. Grâce à cet accès, ils étaient parvenus à envoyer près de 80 millions de dollars vers des comptes situés aux Philippines et au Sri Lanka. Face à cette montée des risques, il était évident pour la banque d'augmenter la sécurisation de son SI.

UN ENVIRONNEMENT RÈGLEMENTAIRE ET NORMATIF PLUS EXIGEANT

En effet, le programme CSP (Customer Security Program) de SWIFT regroupe les règles imposables à l'ensemble des établissements bancaires, afin qu'elles puissent utiliser leur infrastructure/plateforme. L'une des règles est de disposer d'un SOC.

MISE EN PLACE DE LA RGPD

La règlementation sur la protection des données personnelles (RGPD), impose de sécuriser son infrastructure pour éviter la fuite des données.

POURQUOI OPTER POUR LE SOC ITRUST ?

Une relation ancienne de confiance a été établie entre la banque qui avait commencé à travailler avec ITrust sur la gestion des vulnérabilités en utilisant IKARE, puis avait ajouté la partie intelligence artificielle et analyse comportementale avec Reveelium pour ensuite compléter l'offre avec le SOC.
C'est donc tout naturellement que la Banque a décider de continuer avec ITrust sur l'offre SOC Managé. Un autre élément ayant aidé le client à valider son choix : un rapport qualité/prix comparé à la concurrence beaucoup plus intéressant pour client.

LES RÉSULTATS

- Mise en conformité règlementaire
- Meilleure visibilité du SI
- Capacité de détection plus rapide
- Réduction des risques

UTILISATION DU SOC REVEELIUM

La banque travaille en 3 jalons :

1) Analyse et traitement quotidien des alertes remontées en fonction des scénarios pré- établis en amont par ITrust, en fonction du besoin du client.

2) Réunion technique mensuelle sur le SOC (afin d'assurer un suivi technique de la prestation et d'identifier les axes d'amélioration à-même de garantir un niveau de sécurité toujours plus performant).

3) Rapport trimestriel qui permet d'avoir une vision plus haute de la solution, des alertes et des KPI sous forme de synthèse d'activité.
les résultats.

Nous étions à la recherche d'un prestataire capable de comprendre les enjeux de notre marché et de nous garantir une amélioration de la sécurité de notre système d'information. Les solutions proposées par ITrust, la proximité de ses équipes, son expertise des technologies de détection des vulnérabilités et son savoir-faire dans la gestion d'un SOC ont su nous convaincre.

- Client SOC

Le déploiement d'une solution complète d'analyse comportementale basée sur le Machine Learning et l'intelligence artificielle était un véritable atout pour mener à bien l'ensemble du projet de consolidation de notre sécurité.

- Responsable Sécurité

LES GAINS POUR LE CLIENT

« Les outils que nous utilisons désormais nous permettent de travailler de manière beaucoup plus productive et efficace, notamment grâce aux remontées d'alertes du SOC qui nous permettent un gain de temps considérable et un contrôle en continu de notre infrastructure »

ITRUST.