Cilasoft & IBM Security QRadar SIEM®

SmartYou est une marque qui réunit des entreprises spécialisées autour de différentes compétences dans les domaines de l'informatique avec un but commun « réussir la transformation digitale de votre entreprise ». Ses initiateurs sont à votre service depuis près de 30 ans et disposent sur le marché suisse, d'un important réseau relationnel. Ses règles de gouvernance répondent à des valeurs éthiques et déontologiques irréprochables avec des principes fondamentaux "satisfaction clients et collaborateurs". Cette vision, tournée vers l'avenir, permet de bâtir une stratégie globale face à tous ces défis actuels et futurs des entreprises.

SmartYou Managed Services est une ligne d'affaire gérée par **SR opérations SA (SRO)** qui est basée à Gland en Suisse. SmartYou Managed Services propose du conseil d'experts pour dessiner, adapter, optimiser et gérer les applications informatiques de ses clients avec facilité et agilité.
SmartYou Managed Services permet de garder vos services informatiques prêts et fonctionnels avec la précision suisse.

Situation initiale

Jusqu'en 2013, un des clients de SRO dans le monde de la finance utilisait une solution dite globale qui assurait la partie sécurité et audit des partitions IBM i et offrait de plus une console SIEM. L'intégration de l'activité IBM i dans cette SIEM était déterminante pour SRO ; le choix de cette solution avait donc initialement du sens.
Cependant, même si la mécanique fonctionnait correctement, les besoins essentiels étaient faiblement couverts. En effet, la configuration des règles restait très basique, ainsi que les informations remontées. Au final, l'ingénieur SRO se retrouvait noyé par des alertes trop nombreuses, peu corrélées et pauvres en contexte.

Le choix de QRadar

Fin 2013, le projet de remplacer la partie SIEM fut déclenché. Après étude des solutions leaders du marché, le choix s'est porté sur IBM Security QRadar SIEM®. Les limitations liées à la précédente SIEM ont été vite balayées. L'ingénieur SRO s'attendait à une complexité importante, mais ce ne fut pas le cas. Beaucoup de règles étaient déjà pré-configurées et la majorité des devices disposaient d'agents standards. L'effort de remplacement fut finalement faible au regard du service rendu. Au bout de 3 mois, l'ensemble des devices hors IBM i étaient déjà couverts.

Le DSM AJLIB

Il était naturel pour SRO de choisir le DSM AJLIB pour la partie IBM i, fourni gratuitement par IBM. Cette seconde phase s'est avérée beaucoup plus laborieuse. La mise en place s'est faite avec l'aide du support IBM qui a aussi peiné pour y arriver, peu de documentation étant disponible.
En final, les transactions IBM i remontaient bien dans QRadar, mais des lacunes et faiblesses similaires au précédent SIEM furent constatées.

Les directives du groupe bancaire s'étant renforcées en matière de sécurité et d'audit, SRO a du se mettre en recherche d'une solution de remplacement pour la partie IBM i, une forte intégration avec QRadar étant un critère de choix majeur.

Le choix de Cilasoft

Fin 2015, le choix s'est porté sur Cilasoft, l'ensemble des besoins exprimés étant rempli et SRO étant conscient des possibilités additionnelles de la solution en anticipation des demandes futures du groupe bancaire.

«... le process Cilasoft est très stable, sans dégradation de performances, et jusqu'à ce jour sans aucun incident d'exploitation»

« La solution combinée QRadar-Cilasoft permet d'aller bien au-delà des besoins initiaux »

Après quelques ajustements de configuration, les transactions nettoyées de leur « bruit » ont pu être remontées dans QRadar, avec un niveau de détail suffisant pour pouvoir interpréter directement les évènements mais aussi pour créer des règles beaucoup plus facilement. Le délai de transmission (entre la survenance de l'évènement et son arrivée dans QRadar) fut en plus considérablement réduit.

Les gains

En ce début d'année 2017, approximativement 150 devices sont contrôlées, incluant des équipements réseau (routeur, firewall, appliances, proxy, vpn, etc…) et des serveurs (Windows, AIX, IBM i, Exchange). SRO a poussé l'intégration jusqu'à développer ses propres parseurs pour certaines applications bancaires critiques. La solution combinée QRadar-Cilasoft permet désormais au client final d'aller bien au-delà des besoins initiaux du groupe bancaire, en monitorant par exemple des tâches spécifiques réalisées par SRO en liaison avec leur helpdesk.
SRO a ainsi pu acquérir une parfaite maîtrise des 2 solutions QRadar et Cilasoft ce qui lui donne un avantage concurrentiel certain.
Côté IBM i, l'ingénieur SRO en charge de l'administration des partitions précise que : « *... le process Cilasoft est très stable, sans dégradation de performances, et jusqu'à ce jour sans aucun incident d'exploitation* ».

Les projets

Les projets d'amélioration se poursuivent en 2017, avec une montée de version Cilasoft qui permettra une meilleure catégorisation des évènements, un passage en LEEF2, des possibilités d'enrichir encore plus le payload. De quoi servir de nouveaux besoins…

QJRN/400 fournit les services suivants sur IBM i :

- *Filtrage efficace des logs en amont*
- *Formatage des traces collectées aux formats LEEF, CEF, RFC3164, RFC5424*
- *Envoi des traces par protocole direct Syslog ou par LFP*
- *Sécurisation possible via SSL, TLS*

cilasoft

www.cilasoft.com

Advanced Business Partner IBM
Ready for Security Intelligence

Cilasoft & IBM Security QRadar SIEM®