La FINRA protège les investisseurs américains avec Splunk Cloud et AWS

Défis clefs

La Financial Industry Regulatory Authority (FINRA) avait besoin d'une solution centralisée pour traiter et analyser ses données, tout en les protégeant des menaces inattendues.

Résultats clefs

La FINRA utilise maintenant Splunk pour importer les données de 170 applications, améliorer son efficacité organisationnelle et sa rentabilité, et protéger les investisseurs de la fraude.

Secteur : Services financiers

Solutions : Sécurité, Opérations IT

L'intégrité du marché est un facteur clé pour favoriser le dynamisme des marchés financiers.

La FINRA réglemente une dimension essentielle du secteur des valeurs mobilières : les sociétés de courtage qui s'adressent aux particuliers aux États-Unis. La FINRA traite et analyse des quantités massives de données, et l'un des défis qu'elle rencontre consiste à protéger ces données contre les menaces nouvelles et inattendues. La solution de gestion des informations et des événements de sécurité (SIEM) de la FINRA, malgré des coûts élevés, offrait des fonctionnalités limitées.

Transformer les données en actions

- Ingère les données de 170 applications différentes
- Analyse les données issues de la plupart des transactions des places boursières américaines
- A amélioré sa rentabilité et son efficacité organisationnelle avec Splunk sur AWS

Assurer l'intégrité du marché

Chaque jour aux États-Unis, jusqu'à 100 milliards de transactions financières ont lieu sur le marché des valeurs mobilières, impliquant des milliards de dollars d'investisseurs. Organisation à but non lucratif agréée par le Congrès, la FINRA supervise l'intégrité du marché.

Gary Mikula, Directeur principal de la cybersécurité et de la sécurité de l'information à la FINRA, explique : « Nous apportons des quantités massives de données, chaque commande, cotation et transaction sur presque tous les marchés d'actions et d'options aux États-Unis, et nous recherchons les anomalies. Mais nous voulions exploiter bien d'autres logs, comme des informations sur les badges et différents journaux d'accès, et notre SIEM ne pouvait pas les importer. Deuxièmement, il n'offrait pas une interface utilisateur flexible permettant d'interroger les données comme nous le voulions. »

À la recherche d'une meilleure solution, la FINRA a envisagé plusieurs SIEM. Les produits pouvaient générer des alertes, mais ils n'amélioraient pas de manière significative l'ingestion ou l'analyse des données. Puis M. Mikula a assisté à SplunkLive! à Washington et a trouvé ce qu'il cherchait : un moyen de capturer, d'indexer et de corréler les données massives de toutes les sources intéressant la FINRA en temps réel, et de personnaliser les requêtes via des tableaux de bord flexibles.

M. Mikula explique : « Les concurrents s'efforçaient de reproduire des capacités déjà présentes dans Splunk®. Nous ne voulions pas jouer à ce jeu. »

Tout miser sur le cloud

Déjà impressionnée par les capacités de Splunk Enterprise et de Splunk Enterprise Security (ES), la FINRA a appris l'arrivée de Splunk Cloud sur le marché et décidé de devenir son premier gros client. Le modèle cloud de paiement à l'utilisation permet à la FINRA d'adapter ses coûts informatiques aux fluctuations de la demande. Et plutôt que de passer des mois à créer un environnement, la FINRA a tiré parti des agents de collecte de données matures de Splunk pour commencer à consommer

des données dès les premiers jours suivant la signature du contrat. Aujourd'hui, Splunk importe les logs de 170 applications et services AWS différents, notamment Amazon Simple Storage Service (S3), Amazon CloudWatch, AWS Config et AWS CloudTrail. « Aucun SIEM ne pourrait rivaliser avec cela », affirme M. Mikula.

Une véritable centrale

L'intégration avec Amazon Web Services amplifie la puissance de la solution Splunk Cloud de la FINRA. AWS Lambda permet à la FINRA d'exécuter du code sans provisionner ni gérer de serveurs, en ne payant que pour le temps de calcul consommé. Amazon Kinesis Data Firehose, un service entièrement géré, fournit des données de flux en temps réel à Splunk. Mikula considère Amazon Kinesis Data Firehose comme une solution idéale pour créer des filtres d'abonnement afin de déplacer de manière fiable, sécurisée, rapide et économique les logs AWS vers la solution Splunk à des fins d'analyse. Cette capacité profite autant aux développeurs qu'au personnel du réseau ainsi qu'aux spécialistes de la sécurité, unifiant ainsi les silos.

> Lorsque nous avons examiné ce que d'autres sociétés fournissaient, elles s'efforçaient de reproduire des fonctionnalités déjà présentes dans Splunk. »
>
> **Gary Mikula,** Directeur principal de la cybersécurité et de la sécurité de l'information, FINRA

> Nous prenons nos biens les plus précieux, à savoir notre capacité à relever chaque jour toutes les transactions qui ont lieu dans quasiment toutes les places boursières américaines, puis à analyser ces données dans le cloud, et nous les confions à Splunk pour les mettre à l'abri. La combinaison de Splunk et AWS nous donne les meilleures armes possibles pour protéger nos investisseurs. »
>
> **Gary Mikula,** Directeur principal de la cybersécurité et de la sécurité de l'information, FINRA

M. Mikula déclare : « Cela a permis d'établir un partenariat entre nos équipes de sécurité et d'exploitation. Nous avons un objectif commun : nous voulons les mêmes logs. Maintenant, nous pouvons les récupérer et les exploiter à un même endroit. »

Ces gains d'efficacité permettent à la FINRA d'avoir une longueur d'avance sur les menaces en constante évolution en donnant aux équipes les moyens d'analyser les données de manière flexible. La FINRA est l'un des plus grands utilisateurs du framework EMR Hadoop d'Amazon ; le déploiement de l'agent Splunk sur cette plateforme en tant que service fournit des informations qui permettent à la FINRA d'optimiser l'allocation des ressources. De plus, la FINRA a supprimé un outil de facturation tiers dédié et l'a remplacé par son propre processus d'importation des données dans Splunk. Avec Splunk Cloud, la FINRA dispose d'analyses et de rapports de meilleure qualité, ce qui a permis un meilleur suivi des projets des services AWS et une réduction des coûts.

M. Mikula affirme : « Nous gérons plus efficacement nos coûts liés au cloud grâce à notre solution Splunk et à moins de cinq pour cent du prix des outils dédiés. En plus de son investissement dans le cloud, la FINRA soutient le développement de logiciels open source et parraine plusieurs projets open source dans les domaines du big data, du DevOps et de l'assurance qualité. L'équipe de Mikula a même créé un outil pour collecter les journaux AWS CloudTrail et les importer dans Splunk.

En poursuivant des innovations telles que l'informatique serverless dans le cloud, la FINRA constate qu'elle doit plus que jamais suivre les journaux. M. Mikula explique : « Vous ne pouvez jamais savoir quelle sera la prochaine menace et quelles questions nous voudrons poser à nos données. Splunk nous permet de collecter facilement toutes les données que nous voulons et de les interroger à la volée. « Et ce n'est pas tout : les informations de Splunk nous permettent d'utiliser davantage de services AWS. Nous prenons nos biens les plus précieux, à savoir notre capacité à relever chaque jour toutes les transactions qui ont lieu dans quasiment toutes les places boursières américaines, puis à analyser ces données dans le cloud, et nous les confions à Splunk pour les mettre à l'abri. La combinaison de Splunk et AWS nous donne les meilleures armes possibles pour protéger nos investisseurs. »

20-15394-Tier2-FINRA-A4-101-CS_fr-FR