40 manières d'utiliser Splunk dans les **services financiers**

splunk>
turn data into doing™

Sommaire

La seule constante pour les institutions de services financiers : **le changement.**

Les réglementations évoluent en permanence, tout comme les attentes des clients, les menaces de sécurité, les tendances géopolitiques ou, tout simplement, les technologies. Les institutions de services financiers sont confrontées à des perturbations constantes.

La banque ouverte (« open banking ») exige des API ouvertes et « ouvre » la voie à toute une série de défis opérationnels et de sécurité, mais elle met également au jour des opportunités d'améliorer le parcours du client.

Avec la multiplication des offres et des plateformes et points de contact associés, les institutions doivent prêter la plus grande attention à leur exposition aux risques de sécurité et aux failles de performances qui peuvent avoir un impact en termes de conformité réglementaire, de réputation et de résultats financiers.

Les sociétés de service financiers doivent réinventer les stratégies actuelles d'analyse de données pour tirer profit de l'innovation produit et l'optimisation des risques, améliorer l'expérience client et renforcer leur position de sécurité, ce que seule une plateforme d'analyse des données en temps réel permet.

Splunk entre en jeu

Splunk est bien connu dans la communauté des services financiers. Cela fait de nombreuses années que les institutions déploient des solutions Splunk dans leurs services informatiques et leurs datacenters pour faciliter leurs opérations IT, la supervision des infrastructures, les DevOps et la gestion des événements.

La plateforme Splunk est employée pour la sécurité dans de nombreux domaines ; elle est notamment déployée dans le centre des opérations de sécurité (SOC) de certaines des plus grandes banques et compagnies d'assurance au monde. Les logiciels Splunk couvrent un large éventail de scénarios de sécurité allant de la détection des menaces avancées à l'orchestration, à l'automatisation et à la réponse.

Splunk est également employé pour la détection et la prévention des fraudes, la lutte contre le blanchiment d'argent, le respect des sanctions et la détection des menaces internes.

Les capacités d'analyse en temps réel de Splunk se prêtent bien à l'analyse des transactions, et c'est pourquoi plusieurs réseaux et passerelles de paiement comptant parmi les plus répandus dans le monde utilisent Splunk pour de nombreux scénarios d'usage, qui vont de l'agrégation des paiements à la prévention de la fraude liée aux cartes de crédit en passant par l'analyse des marchands et le respect de la norme de sécurité des données de l'industrie des cartes de crédit (PCI DSS).

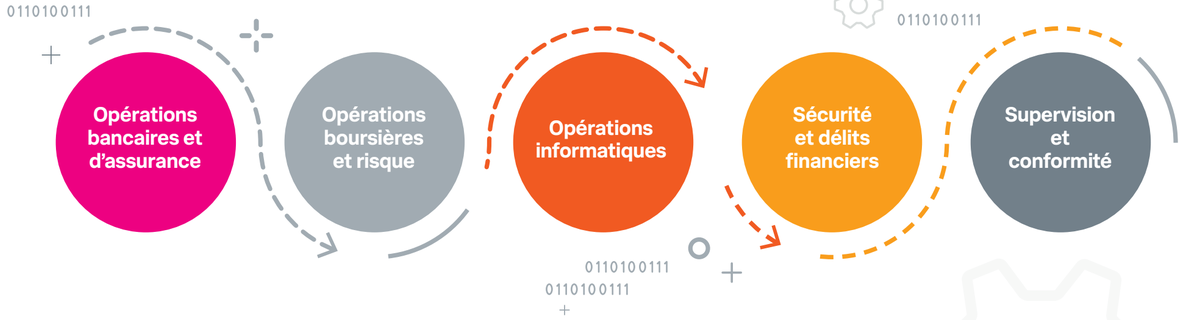
Plusieurs institutions et leurs équipes de gestion des risques utilisent Splunk pour des scénarios d'utilisation couvrant par exemple la conception et le développement de stratégies de transactions à faible latence, ou la constitution de centres des opérations boursières et de gestion des risques à l'attention des responsables des risques et de leurs équipes.

Pourquoi Splunk est-il appliqué à une telle diversité de scénarios d'utilisation ?

Dans le monde de la finance, les utilisateurs ignorent généralement quelle sera leur prochaine question jusqu'à ce qu'il soit le moment de la poser. Splunk est toujours prêt à relever les défis que vous lui présentez. Les utilisateurs peuvent élaborer de nouvelles questions et voir les réponses s'actualiser en temps réel au fil de l'arrivée de nouvelles données.

Splunk est une plateforme d'analyse en temps réel. Ses logiciels présentent une architecture robuste et évolutive capable de gérer les besoins des institutions financières en termes de volume et de faible latence. Ils n'obligent pas les utilisateurs à élaborer des modèles de données avant de charger les données, et ils sont suffisamment souples pour permettre aux utilisateurs comme aux développeurs de poser n'importe quelle question et d'obtenir une réponse immédiate. Le logiciel Splunk ne se soucie pas de la provenance des données ni de leur format. Il suffit de charger les données.

Ce document présente plusieurs exemples des utilisations impressionnantes de Splunk par nos clients. Ce n'est que la partie émergée de l'iceberg : ces utilisations sont innombrables et varient considérablement. La créativité des personnes qui utilisent Splunk repousse chaque jour les limites des logiciels.



Opérations bancaires sur internet et sécurité

Défi

Les banques cherchent à différencier leurs services et à remporter des parts de marché en offrant à leurs clients une expérience en ligne et mobile supérieure. De plus en plus de services bancaires deviennent disponibles sur Internet, et l'on se rend de moins en moins souvent en agence parce qu'il est plus facile d'accomplir les tâches de routine en ligne. La banque en ligne s'est démocratisée et les applications mobiles se développent quatre fois plus rapidement. Nous estimons qu'elle supplantera la banque physique dans de nombreuses institutions cette année.

La banque en ligne couvre traditionnellement les possibilités d'effectuer des activités quotidiennes telles que la consultation des soldes, des transactions et des relevés. Plus récemment, ces plateformes sont devenues beaucoup plus complexes et ont intégré de nombreux services numériques tels que les paiements, la mise en avant de produits, des moteurs de conversation et des applications mobiles, et les banques cherchent aujourd'hui à faire converger les différents canaux sur leurs plateformes Internet.

Ces applications complexes dépendent de nombreuses technologies et présentent par conséquent de nombreux défis de sécurité. Sans surprise, les cybercriminels ciblent les sites de banque en ligne dans l'espoir de recueillir assez d'informations pour obtenir l'accès à des comptes personnels : ces pratiques nuisent gravement à la confiance des clients et à leur fidélité et dégradent l'image de marque de la banque.

L'approche de Splunk

Les cybercriminels utilisent des vecteurs d'attaque de plus en plus sophistiqués pour découvrir et exploiter des vulnérabilités potentielles dans les applications bancaires. Ils sont de plus en plus difficiles à détecter et dépassent le champ d'un produit de sécurité particulier.

Splunk propose un portefeuille de produits de sécurité indépendants des technologies. Ces produits analysent, suivent, supervisent et génèrent des alertes sur des aspects stratégiques des applications de banque en ligne en temps réel. Ils étendent ainsi l'écosystème de sécurité de la banque quelles que soient les technologies. Splunk sait mettre en évidence des comportements anormaux même lorsqu'ils peuvent être légitimes pris isolément. Par exemple, au cours d'une attaque par bourrage d'identifiants, on enregistre un grand nombre d'accès simultanés à des comptes et ce pic peut passer inaperçu devant les règles de sécurité traditionnelles.

En exploitant toutes les données associées à une application de banque en ligne, générées depuis le développement jusqu'à la production, Splunk offre une couverture totale du parc (matériel, réseau, stockage, virtualisation, cloud et applications), facilitant ainsi la détection des comportements anormaux internes et externes et des indicateurs de compromission touchant les plateformes de banque en ligne qui sont sensibles à de nombreuses formes d'attaque internes et externes, comme indiqué ci-dessous :

Menaces externes

- Scripts entre sites
- Injection SQL
- DOS, DDoS
- Hameçonnage
- Vol d'identifiants ou d'identité
- Connexions par force brute
- Échecs d'authentification à 2 facteurs (2FA)
- Échecs de réinitialisation de mots de passe
- Fraude

Menaces internes

- BotNets
- Logiciels malveillants
- Virus
- Vers
- Chevaux de Troie
- Logiciels espions
- Logiciels publicitaires

Splunk est capable de détecter toutes les formes de menaces grâce à ses règles de corrélation et ses workflows sophistiqués.

En tant que cible de choix pour les hackers, les équipes de sécurité doivent mettre en place un dispositif complet de supervision des logs en temps réel, et ce sur toute la plateforme. Splunk Enterprise Security (ES) va plus loin que les solutions traditionnelles de gestion des incidents de sécurité (SIEM) en proposant une approche axée sur l'analyse de la sécurité. En capturant les données brutes de la plateforme bancaire et de son architecture sous-jacente, les recherches de corrélation de Splunk recherchent les comportements anormaux par le biais d'approches mathématiques, qui emploient des statistiques et le machine learning pour déclencher des événements qui seront ensuite examinés par les analystes du centre des opérations de sécurité (SOC).

Les analystes trient alors les événements de sécurité et mènent des enquêtes dans Splunk ES en exploitant les données brutes. Les étapes de l'enquête sont consignées dans un log et les enquêtes incomplètes peuvent être transmises à d'autres analystes.

Valeur

La banque en ligne et par application est aujourd'hui la norme, et les plateformes des grandes banques doivent être au service de dizaines de milliers d'utilisateurs simultanément sans que la sécurité, la résilience et les performances n'en soient affectées.

Avec Splunk, les institutions de services financiers peuvent avoir confiance dans le maintien de leur position de sécurité en détectant les attaques malveillantes en temps réel et en prenant des mesures de blocage avec Splunk Phantom, notre outil d'orchestration, d'automatisation et de réponse de sécurité, capable d'automatiser les actions nécessaires pour arrêter une attaque en cours et y remédier.

Analyse des performances commerciales et de la rentabilité des clients

Défi

Les institutions financières aspirent à de la simplicité dans leurs produits et leurs services. Elles vont très loin pour concevoir, mesurer et peaufiner l'expérience de leurs clients pour que ceux-ci puissent utiliser leurs produits avec un minimum d'efforts, en espérant que ces démarches seront récompensées par la fidélité de leur clientèle et un haut score de promoteur net (NPS).

Tout cela paraît idéal en théorie, mais les institutions financières injectent tant de complexité dans leurs propres opérations qu'il peut parfois être difficile de satisfaire un ensemble d'exigences pourtant simples en apparence.

La complexité commence par la forme de l'organisation. Beaucoup d'institutions sont implantées dans plusieurs pays.

Elles opèrent sur plusieurs fuseaux horaires et avec de nombreuses devises, leur personnel et leurs clients parlent de nombreuses langues, et elles doivent se conformer à une multiplicité d'autorités de régulation qui scrutent chaque mot de leurs communications.

Et ça ne fait qu'empirer. Les institutions ont des centaines voire des milliers de produits. Certains sont récents, d'autres plus anciens, mais tous doivent être pris en charge pendant des années. Les réglementations encadrant la vente de chaque produit diffèrent d'un marché à l'autre, et un produit rentable ici peut générer des pertes ailleurs.

Outre cette complexité inhérente, les institutions doivent maintenir des dispositions financières pour compenser les erreurs du passé et, dans certains pays, les banques font l'objet d'un examen complet des gouvernements qui leur reprochent de ne pas avoir traité équitablement leurs clients. Dans ce contexte, nous comprenons que le concept de simplicité des produits et des services soit plus difficile à concrétiser.

L'approche de Splunk

Tout espoir n'est pas perdu. Splunk est employé dans de nombreux domaines pour réduire la complexité de ces opérations et doter les décideurs d'informations plus simples et plus exploitables. Ces informations sont données en temps réel, et c'est là que Splunk se distingue.

Les vues en temps réel du parcours des clients peuvent améliorer considérablement la capacité d'une institution à faire face à une interruption de service dans un processus et à éviter qu'un petit problème ne vienne détruire ses relations avec un client.

Les firmes disposant d'équipes commerciales utilisent Splunk pour produire des tableaux de bord opérationnels qui démontrent les performances commerciales et permettent aux responsables d'étudier l'écart-type au sein d'une équipe, mettant ainsi en évidence les éléments performants et ceux qui ont besoin d'être développés dans un domaine spécifique. Les performances de chaque collaborateur d'une équipe varient d'un KPI à l'autre.

La rentabilité peut se mesurer à l'échelle du client, mais aussi à celle du produit, de l'équipe ou du pays, ou de toute autre échelle intéressante. L'un des atouts clés de Splunk est qu'il vous offre la possibilité de poser précisément la question que vous voulez et donne ensuite des réponses en temps réel à envisager. Vous n'aurez plus jamais besoin d'attendre qu'une requête soit traitée durant la nuit. Les utilisateurs de Splunk obtiennent leurs réponses au moment où ils en ont besoin et peuvent agir sans attendre.

Ces informations peuvent avoir une valeur inestimable pour ceux qui travaillent au siège d'une entreprise, mais les avantages de Splunk ne s'arrêtent pas là. Splunk est à disposition des utilisateurs où qu'ils se trouvent. Il est en effet possible de créer des tableaux de bord pour présenter l'ensemble d'informations qui intéresse quelqu'un, peu importe son rôle et sa localisation. C'est particulièrement utile pour les gestionnaires de relations mobiles et les équipes des succursales.

Les banques ont, pour beaucoup, essayé d'élaborer des systèmes analytiques pour doter les employés de leurs agences des informations dont ils ont besoin, mais elles ont été freinées par la complexité des modèles de données, ainsi que par leur volume et leur ancienneté. Splunk met un terme à ce cycle en délivrant les informations en temps réel, quelles que soient la source, la diversité et la vélocité des données, pour apporter des réponses toujours à jour.

Valeur

Le fait de fournir des informations opérationnelles exploitables au personnel de terrain ou d'assistance clientèle est extrêmement précieux. En plus de cela, la capacité à détecter un problème avant qu'il ne s'aggrave joue un rôle essentiel dans la réussite client. La clientèle se fidélise, l'érosion recule, la rentabilité augmente et les employés restent plus longtemps car le personnel d'assistance interagit avec des clients plus satisfaits.

En sachant quels produits et services sont les plus rentables, dans quelles régions et pour quelles raisons, les décideurs sont en mesure d'élaborer des stratégies et de réagir en temps réel à l'évolution de la demande. Tous ces progrès se traduisent par des résultats tangibles.

Les autorités de régulation exigent que les clients soient traités de façon équitable. Splunk permet aux institutions financières de mesurer leurs performances dans ce domaine et d'enregistrer précisément leurs actions. De plus, cette richesse d'informations leur permet d'introduire des changements en cas d'erreur.

ING Bank utilise Splunk Enterprise pour son analyse commerciale et pour obtenir des informations sur ses clients. En indexant les données de ses services web et de ses applications mobiles, la banque sait désormais (en temps réel) quelles pages du service ING BankOnLine ses clients sont en train de consulter. La fonction commerciale utilise ces informations pour prendre des décisions stratégiques telles que des décisions relatives aux offres de produits sur mesure ou d'autres initiatives marketing.

En savoir plus sur Splunk chez ING Bank.

OPÉRATIONS BANCAIRES ET D'ASSURANCE

Opérations bancaires en agence

Défi

Au cours de ces dernières années, les banques pour particuliers ont totalement métamorphosé leur approche de la prestation de services aux clients en agences. En effet, les agences coûtent très cher et représentent souvent la moitié des coûts d'exploitation d'une banque. Les banques ont donc déployé de grands efforts pour réduire à la fois le nombre d'employés et d'agences tout en gagnant en efficacité grâce à une utilisation judicieuse des technologies et de l'automatisation.

Les progrès technologiques ont permis aux banques de numériser une grande partie de leurs offres de services, donnant ainsi une plus grande autonomie à leurs clients.

Les banques évaluent et équilibrent constamment le tarif des services clients souhaités mais coûteux, ainsi que la possibilité de numériser et d'automatiser autant de processus que possible.

Les banques sont encore nombreuses à ne pas savoir comment exploiter la valeur des données d'agence pour optimiser les niveaux de service. Une supervision en temps réel de bout en bout est indispensable à la fluidité de fonctionnement de cette nouvelle catégorie d'agences. La moindre interruption de service touchant les DAB en agence, les machines de dépôt, les bornes de libre-service, les terminaux d'accueil, les réseaux Wi-Fi ou les tablettes, vient nécessairement perturber et dégrader l'expérience client en agence. Les interruptions doivent donc être réduites au minimum pour préserver la satisfaction des clients.

Grâce aux tablettes, désormais très utilisées dans les agences pour réaliser des opérations, les banques peuvent communiquer un sentiment de familiarité et de simplicité d'utilisation rendant les clients plus satisfaits. Pourtant, ces mêmes tablettes introduisent une nouvelle gamme de défis de gestion, de suivi et d'administration.

Disposer ne serait-ce que d'une visibilité de base sur l'inventaire des tablettes peut être difficile pour les équipes d'assistance, ce qui dégrade l'expérience client. Face à la rotation des employés, aux vols et aux déconnexions d'appareils, il n'existe pas de moyen simple de tracer toutes ces tablettes. Nous comprenons que les pertes d'appareils puissent être la cause d'une expérience utilisateur irrégulière d'une agence à l'autre.

Dernier facteur à prendre en compte : la sécurité. Étant donné que les réseaux Wi-Fi sont indispensables à de nombreuses interactions utilisateur, la sécurité devient essentielle pour les services proposés par l'agence.

L'approche de Splunk

Bien qu'il soit possible de comprendre l'activité de chaque agence en supervisant les systèmes back-end, comme la demande d'un prêt personnel, l'utilisation de Splunk pour recueillir directement des informations auprès des appareils de l'agence peut offrir des renseignements plus détaillés sur le parcours du client et le comportement des employés. À terme, cela mène à une visibilité accrue, une meilleure prise de décision et une amélioration du fonctionnement de l'agence, en somme, un avantage concurrentiel.

Les tablettes qui exécutent les applications bancaires sont conçues pour traiter rapidement les demandes des clients en agence. La collecte des habitudes d'utilisation des applications mobiles exécutées sur les tablettes offre des informations stratégiques sur le parcours du client et l'expérience utilisateur.

Le framework Splunk Mobile Intelligence permet aux développeurs d'applications mobiles de générer des logs d'application directement injectés dans Splunk afin d'analyser les habitudes d'utilisation et les tendances, et ainsi de soutenir les décisions prises en agence.

En corrélant les données collectées auprès des applications mobiles et les données d'infrastructure réseau, vous pouvez obtenir un décompte plus précis des appareils à partir des logs Wi-Fi et ainsi tenir rigoureusement à jour l'inventaire de chaque agence.

En cas d'interruption de service, les banques peuvent s'appuyer sur un modèle d'impact des perturbations élaboré en utilisant les puissantes capacités d'analyse, de machine learning et de visualisation des données de Splunk. Elles peuvent ainsi quantifier le nombre de clients et/ou de transactions affectés pour aider la banque à évaluer l'impact et le coût de la défaillance.

Valeur

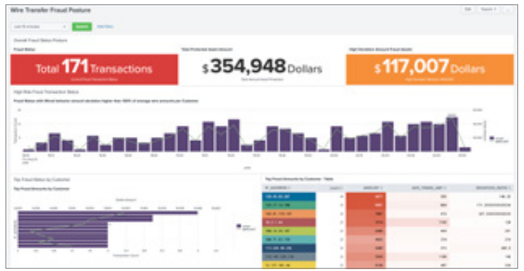
L'évolution vers des agences aux effectifs réduits et très dépendantes des technologies impose que chaque composant fonctionne de façon optimale. Cette évolution exige en outre une visibilité en temps réel sur l'efficacité opérationnelle et sur la fiabilité.

Splunk recueille les données de l'infrastructure de l'agence et fournit des analyses qui permettent à la banque de renforcer sa sécurité, de suivre ses inventaires et d'optimiser ses processus, lui offrant ainsi la possibilité d'être au service de plus de clients dans un espace identique, voire réduit.

Et avec l'introduction de nouvelles technologies telles que les DAB équipés de caméras, la stratégie de supervision doit être assez flexible pour prendre en charge de nouvelles sources de données et établir des corrélations entre différentes applications à l'échelle de l'infrastructure.

Grâce à la plateforme de données Splunk, la supervision des agences tient le rythme de l'afflux des nouvelles technologies adoptées pour mieux servir les clients.

Il est impératif de corréler les activités des clients et d'analyser la façon dont ils interagissent avec la banque pour savoir s'il faut augmenter ou réduire le nombre d'agences. Bien que certains clients préfèrent réaliser leurs opérations en ligne, d'autres apprécient de pouvoir se rendre en agence. Les banques doivent également être en mesure d'être au service de leurs clients fortunés dans leurs agences.
À l'avenir, elles exploiteront les analyses pour disposer de ces informations avant de prendre des décisions commerciales critiques.



Modèle de l'activité de transfert depuis une agence bancaire

Opérations bancaires mobiles et sécurité

Défi

Les applications bancaires mobiles disponibles sur les plateformes Apple ou Google permettent aux banques de proposer de nombreux services bancaires à leurs clients. Ces applications offrent aux utilisateurs une expérience native, engageante et réactive, ainsi que des fonctionnalités telles que les notifications push qui alertent les clients en cas d'actualité importante.

En raison de la nature portable des appareils mobiles, les téléphones et tablettes sur lesquels sont installées les applications peuvent aisément tomber entre de mauvaises mains en cas de perte ou de vol. C'est pourquoi il est impératif de mettre en place des contrôles de sécurité robustes pour assurer la confiance et l'adoption des utilisateurs.

L'approche de Splunk

Splunk Mobile Intelligence (MINT) est une application qui élargit l'intelligence opérationnelle de Splunk aux applications mobiles pour aider les institutions financières à proposer des outils plus performants, plus fiables et plus sécurisés. Splunk MINT fournit des informations sur les versions de production d'une application mobile, en couvrant tous les types d'appareils et systèmes d'exploitation.

Les kits de développement logiciels (SDK) Splunk MINT recueillent les données des applications mobiles par le biais d'un programme et les envoient à Splunk Enterprise.

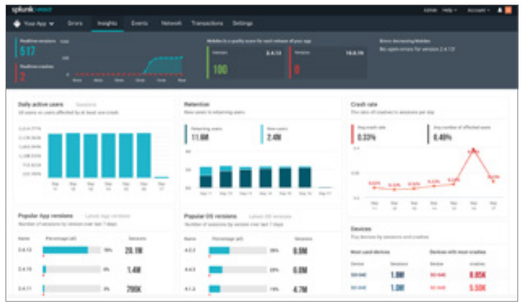
L'intégration de MINT dans Splunk offre des informations approfondies sur les applications, le comportement des utilisateurs et les données d'expérience utiles pour identifier les activités inhabituelles ou anormales, comme suit :

- Pour identifier la cause des interruptions de service et des mauvaises performances des applications.
- Pour découvrir les erreurs se produisant le plus souvent selon le système d'exploitation, l'appareil et la version de l'application.
- Pour apprendre ce que faisaient les utilisateurs lorsque l'interruption de service est intervenue.
- Pour visualiser la trace de la pile et les occurrences d'instance pour des erreurs spécifiques.
- Pour capturer les sorties LogCat et NSLog des appareils.
- Pour visualiser les informations réseau et analyser les capacités du système.
- Pour mesurer la latence, le volume et les codes d'état de tous les appels HTTP.
- Pour superviser des événements et transactions spécifiques.
- Pour filtrer les informations par type de connexion et par opérateur.
- Pour suivre les processus exécutés à l'aide de l'application mobile de bout en bout et comprendre l'expérience utilisateur.
- Pour produire des rapports sur des événements personnalisés de l'application.
- Pour utiliser les transactions et suivre des tâches spécifiques du début à la fin.
- Pour ajouter des fils d'Ariane aux rapports d'interruption de service pour indiquer à quel moment sont intervenues des actions spécifiques.
- Pour obtenir des informations sur l'utilisation des applications mobiles.
- Pour savoir quelles plateformes et quels appareils sont utilisés le plus souvent.
- Pour découvrir les performances des applications selon le système d'exploitation et l'appareil.
- Pour savoir combien d'utilisateurs sont affectés par les erreurs.
- Pour obtenir des informations sur l'utilisation et les performances de l'application en fonction de la localisation des utilisateurs.
- Pour corréler les performances et l'utilisation de l'application sur différents appareils mobiles, sur le web et sur les autres canaux.

Valeur

Les applications mobiles jouent un rôle clé dans la façon dont les utilisateurs interagissent avec leurs banques, et une excellente expérience mobile peut améliorer l'image de marque et la fidélité des clients, et donc les scores de promoteur net (NPS).

Splunk MINT permet aux institutions financières de collecter des données directement sur les appareils mobiles et de les corréler avec les données internes pour identifier les problèmes de sécurité et réaliser des analyses des causes profondes, afin de réduire le temps moyen de résolution (MTTR).



Proposez l'expérience multicanale et mobile que vos clients attendent grâce à une visibilité totale sur votre application, corrélée à votre plateforme de données globale, grâce à Splunk.

OPÉRATIONS BANCAIRES ET D'ASSURANCE

Opérations sur DAB et sécurité

Défi

La plupart des banques possèdent un vaste réseau de DAB, souvent implantés dans plusieurs pays et généralement membres de réseaux interbancaires comme NYCE ou LINK.

Le trafic de l'utilisation des DAB varie considérablement et dépend de la période de l'année et d'événements ponctuels. Il est donc nécessaire de mettre en place des systèmes pour superviser et anticiper cette utilisation afin de réapprovisionner les machines à temps.

Les DAB sont à la merci de l'environnement extérieur ; ils dépendent souvent de sources externes d'alimentation électrique et d'une connectivité au réseau. Ils sont vulnérables face aux bourrages papier causés par les billets de banque usagés et aux pannes de réseau et d'électricité. Ce sont des cibles faciles pour les activités criminelles.

Tous ces facteurs combinés expliquent que les banques doivent superviser attentivement leurs réseaux et accorder la plus grande importance à la localisation de leurs DAB.

L'approche de Splunk

De nombreuses banques utilisent Splunk pour obtenir une vision globale de leur réseau de DAB. Les DAB génèrent une télémétrie détaillée et il est facilement possible d'obtenir des informations sur l'état d'un distributeur spécifique.

Splunk propose donc un ensemble de tableaux de bord en temps réel qui présentent l'état de l'intégralité du réseau. Ces tableaux de bord incluent des informations complètes telles que :

- l'état du réseau ;
- la vue d'ensemble des incidents ;
- les incidents prédits ;
- toute activité suspecte ;
- les performances du réseau ;
- les performances financières ;
- l'état de la sécurité.

Les tableaux de bord Splunk examinent l'historique des incidents au fil du temps et utilisent des algorithmes de machine learning pour prédire les futurs problèmes. Ces algorithmes sont capables d'anticiper les incidents ayant le plus de probabilité de survenir selon l'emplacement et le type de machine. Armée de cette capacité de prédiction, la banque peut adopter une approche proactive et planifier des routines de maintenance sur cette base, ce qui lui permet d'économiser du temps et des ressources tout en améliorant la disponibilité du réseau.

La sécurité est un aspect clé pour les réseaux de DAB, et Splunk est capable d'identifier les menaces en temps réel et d'automatiser la réponse le cas échéant. Les réseaux de DAB doivent être conformes à la norme PCI DSS 3.2, et Splunk peut vous y aider.

Valeur

Les interruptions de service de DAB nuisent à l'image de marque de la banque, et c'est pourquoi le maintien de la disponibilité revêt une importance stratégique. Le maintien de la sécurité des DAB réduit les pertes dues à la fraude et les interruptions de service. La maintenance prédictive améliore la disponibilité et fait baisser les coûts en intégrant le réapprovisionnement aux plannings de maintenance et en accordant une attention particulière aux DAB les plus utilisés.

La sécurité est un aspect clé pour les réseaux de DAB, et Splunk est capable d'identifier les menaces en temps réel et d'automatiser la réponse le cas échéant. La maintenance prédictive améliore la disponibilité et fait baisser les coûts en intégrant le réapprovisionnement aux plannings de maintenance et en accordant une attention particulière aux DAB les plus utilisés.

Les banques utilisent Splunk pour avoir une vision holistique de leur réseau de DAB. Les DAB génèrent une télémétrie détaillée et il est facilement possible d'obtenir des informations sur l'état d'un distributeur spécifique.

La compréhension des processus impliqués dans les transactions sur DAB permet à la banque de diagnostiquer rapidement ceux qui sont trop lents ou qui peuvent présenter des signes d'activité frauduleuse.

Banque ouverte, opérations PSD2 et sécurité

Défi

La nouvelle version de la directive 2 sur les services de paiement (PSD2), souvent appelée « Open banking »(ou banque ouverte), est entrée en vigueur en janvier 2018 et a pour objectif de moderniser le marché du paiement pour les particuliers au moyen d'une législation encourageant l'innovation, la concurrence et la sécurité sous la forme de nouveaux services numériques pour les consommateurs.

Les banques sont donc tenues de faire en sorte que les données qu'elles détiennent sur leurs clients (les soldes de compte, par exemple) soient accessibles aux prestataires de services de paiement tiers (TPP) via des interfaces de communication (API) sécurisées, une fois le consentement du client obtenu, tout en assurant les mêmes niveaux de disponibilité et de performances que si le client accédait directement aux services de sa banque.

La banque ouverte permet à des TPP comme FinTech ou autres d'innover et de proposer de nouveaux produits, élargissant ainsi les choix accessibles au consommateur. Ces services peuvent être répartis dans les catégories suivantes :

1. Agrégateurs et prestataires de services d'informations de compte (AISP) : ces prestataires dotent leurs clients d'une vue d'ensemble de leurs comptes et de leurs soldes.
2. Prestataires de services d'initiation de paiement (PISP) : ces prestataires effectuent des paiements pour le compte de leurs clients. Ils donnent aux commerçants l'assurance que l'argent leur parviendra.

La sécurité est la pierre angulaire de PSD2, et les normes techniques réglementaires (RTS) spécifient une authentification robuste des clients (SCA) : les transactions en ligne sont vérifiées au moyen d'une authentification à deux facteurs et de mots de passe à usage unique afin de réduire la fraude. Les banques doivent mettre leurs systèmes de sécurité de paiement au niveau des exigences RTS.

L'approche de Splunk

Pour se conformer à la législation PSD2, les banques doivent mettre en place un canal de communication avec les TPP, que ce soit en adaptant leur interface de banque en ligne côté client ou en créant une nouvelle interface dédiée. Dans un cas comme dans l'autre, l'interface sera inévitablement une cible pour les cybercriminels qui tenteront de s'approprier des informations, d'obtenir un accès non autorisé ou d'effectuer des attaques par déni de service (DoS) pour nuire à la disponibilité des services.

La supervision de la sécurité et des performances des API revêtira une importance stratégique non seulement pour la banque, qui devra superviser la disponibilité, la vitesse, la latence et la fréquence d'utilisation des terminaux, mais aussi pour les organismes de régulation qui devront veiller à ce que les TPP ne soient pas désavantagés, dans la mesure où les API imposeront une charge supplémentaire à l'infrastructure existante.

Les menaces qui pèsent sur l'infrastructure de l'API de banque ouverte peuvent provenir de vecteurs d'attaque directs, mais elles peuvent aussi être indirectes, par exemple, lorsqu'un auteur d'attaques exploite une vulnérabilité ailleurs sur le réseau puis évolue latéralement pour infliger des dommages ou exfiltrer des données. Dans tous les cas, la supervision de l'API ne suffit pas car elle donnerait une vue en silo de l'activité de l'API. Pour être efficace, la supervision de la sécurité de l'infrastructure d'API de banque ouverte exige une approche globale.

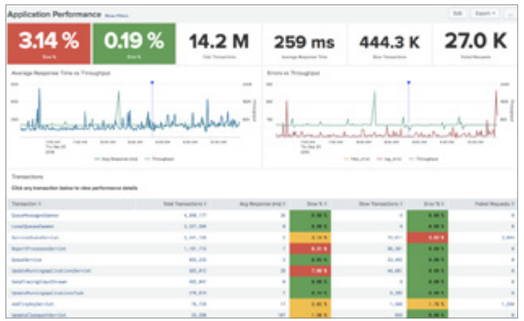
Si des indications de comportements anormaux en termes de latence, d'utilisation ou de disponibilité sont utiles pour un technicien de maintenance, elles pourraient être autant de symptômes de cyberattaque et donc intéresser les analystes du SOC, qui examineront les mêmes données sous une perspective différente.

La corrélation de ces informations à d'autres sources peut permettre d'isoler rapidement les anomalies pour, par exemple, conclure à un problème de stabilité de la plateforme, ou donner de la visibilité sur un risque plus étendu touchant les opérations IT ou la sécurité.

Valeur

Avec Splunk, les banques pourront aisément élargir la couverture de leur supervision de sécurité aux nouvelles API de banque ouverte sans avoir à investir dans de nouveaux outils de sécurité ou solutions ponctuelles.

Les grandes banques découvriront de nouvelles opportunités d'amélioration de leurs produits et services en mettant au jour des informations inédites grâce à Splunk. Elles pourront explorer les données de leurs API PSD2 pour comprendre comment leurs clients interagissent avec leurs services, par comparaison avec ceux des TPP, afin d'élaborer une meilleure expérience et de réduire l'érosion de la clientèle.



Supervisez la disponibilité et la sécurité des API à l'échelle du partenaire pour mieux gérer l'expérience client et votre position de sécurité.

Opérations blockchain et sécurité

Défi

Le gain de popularité de la blockchain au sein des services financiers s'explique par la conviction qu'elle permet de nombreuses applications pouvant potentiellement éliminer des intermédiaires et donc réduire les coûts. Les banques, les courtiers, les assureurs, les autorités de régulation et autres expérimentent activement pour trouver de nouvelles manières de récolter les fruits de la blockchain et des technologies qui en découlent, comme les Smart Contracts.

Les scénarios d'utilisation sont nombreux : accélération et simplification des paiements transfrontaliers, meilleure gestion de l'identité des clients et optimisation des transactions boursières grâce à l'amélioration du processus de règlement.

Dans le domaine de l'assurance, la mise en place d'un grand livre commun à tous les assureurs offrirait une visibilité immédiate sur les fraudeurs qui déclarent un même sinistre auprès de plusieurs compagnies.

Jusqu'à présent, les autorités de régulation n'ont pas encore défini de normes pour le contrôle et la protection des systèmes reposant sur la blockchain. À l'heure où les institutions financières investissent activement dans des projets de blockchain, il faudra s'attendre à ce que les problématiques de la sécurité et de la supervision deviennent des priorités.

En théorie, la blockchain va appuyer les objectifs de sécurité des entreprises, parce que l'intégrité de la blockchain est garantie par un dispositif de sécurité inhérent, et parce qu'une comptabilité commune élimine les points de faiblesse uniques ciblés par les adversaires. Toutefois, l'infrastructure qui supporte le réseau peer-to-peer devra toujours faire l'objet d'une supervision de sécurité traditionnelle pour empêcher que les pirates n'y voient un terrain de jeu privilégié.

Mais comme toute technologie à ses balbutiements, la blockchain et la façon dont les entreprises choisissent de l'implémenter peuvent créer des vulnérabilités dont nous n'avons pas encore connaissance. Cette dépendance vis-à-vis d'un nouveau code de programmation et la complexité qui en découle pourrait également introduire des failles exploitables, ce qui souligne encore davantage l'importance de disposer d'un processus DevOps faisant de la sécurité sa priorité.

Il est essentiel que les institutions financières qui lancent des projets de blockchain fassent intervenir des collaborateurs de l'IT et de la sécurité aussi tôt que possible, pour leur donner tout le temps de s'adapter à la nouvelle technologie et d'analyser la provenance des menaces potentielles.

L'approche de Splunk

Sécurité

La technique de stockage des données sans schéma de Splunk permet aux sociétés d'incorporer rapidement les flux de données de log de leurs projets de blockchain et d'exploiter les capacités d'analyse et d'intelligence artificielle (IA) basée sur le machine learning pour établir des comportements de référence et rechercher les anomalies. Le SOC pourra ainsi détecter les signatures inhabituelles, qui se détacheront sur la toile de fond des comportements normaux.

Les données de sécurité ingérées par la plateforme seront ensuite exploitables dans Splunk Enterprise Security, ce qui permettra de générer, trier, explorer et corriger les événements de sécurité.

Informatique

Les données exploitées par l'équipe de sécurité sont tout aussi utiles aux équipes d'assistance IT qui doivent garantir le bon fonctionnement et la performance de l'infrastructure de blockchain. En combinant logs et métriques, Splunk offre une visibilité de bout en bout sur les problèmes du système, les taux d'utilisation et la planification des capacités.

DevOps

L'expertise dans le domaine de la blockchain est encore rare, et c'est pourquoi il y a tout intérêt à mettre l'accent sur la sécurité dans le cycle de vie du développement logiciel (SDLC), et à faire sien le mantra de la sécurité dès la conception. La supervision de bout en bout du processus DevOps et les outils associés pourraient bien faire la distinction entre un hacker dans les rangs de l'équipe de développement, la présence de code malveillant et l'installation d'extensions tierces non autorisées pouvant contenir des vulnérabilités.

Valeur

Il reste encore beaucoup de zones d'ombre concernant la blockchain, son potentiel réel et les risques sécurité associés à sa mise en œuvre. Splunk est en très bonne position pour aider les sociétés à relever les défis de développement, de sécurité et de stabilité qui peuvent être pris en charge par une meilleure visibilité sur les données.

Supervisez la sécurité et la santé opérationnelle de votre infrastructure de blockchain et de comptabilité distribuée avec Splunk.

OPÉRATIONS BANCAIRES ET D'ASSURANCE

Opérations de paiement en temps réel et sécurité

Défi

Les passerelles et les réseaux de paiement doivent assurer 100 % de disponibilité à leurs clients tout en préservant tous les aspects du réseau face aux failles de sécurité et à la fraude.

Les réseaux de paiement doivent maintenir un ensemble complexe de communications avec les banques et gérer la multitude de variantes internationales de systèmes et de processus.

Les commerçants ont besoin d'une fiabilité opérationnelle parfaitement fluide et de systèmes capables de prévenir les transactions frauduleuses et de respecter les normes PCI.

Les banques qui reçoivent et traitent des paiements doivent également gérer une multitude de systèmes et de niveaux de performances variables. Les banques doivent agréger les paiements reçus sur tous les réseaux pris en charge afin d'obtenir une image unique des clients, des commerçants et des réseaux ; cette vision globale facilite la sécurisation des processus et accélère l'identification des comportements suspects.

Les paiements génèrent des messages volumineux et complexes qui incluent des informations sur le paiement, le commerçant et le destinataire, ainsi que des données de routage qui permettent au paiement d'atteindre sa destination. Tous ces facteurs, combinés à un trafic aussi volumineux qu'irrégulier, imposent à tous les participants d'assurer de hauts niveaux de performances techniques.

L'approche de Splunk

La plupart des passerelles et réseaux majeurs de paiement ont déjà choisi d'utiliser Splunk pour gérer de multiples aspects de leurs opérations. Les solutions Splunk affectent le processus de paiement à plusieurs niveaux :

DevOps et DevSecOps
Les sociétés de service qui développent des applications de paiement utilisent les capacités DevOps de Splunk pour améliorer la livraison des applications et faciliter les mises à jour continues. Les mises à jour en temps réel dotent les développeurs d'informations en temps réel sur toutes les étapes du cycle de développement. Ils peuvent ainsi adopter une méthodologie de publication continue.

Opérations IT et réseau
Pour assurer 100 % de disponibilité, il faut une approche spécialisée de la gestion des applications, de l'infrastructure, de la sécurité et de la supervision. Splunk peut superviser l'intégralité du processus de bout en bout, mettre en évidence les goulets d'étranglement et anticiper la demande. Splunk utilise l'IA basée sur le machine learning pour prévoir l'apparition des problèmes, ce qui permet aux ingénieurs de les résoudre avant qu'ils ne provoquent une interruption de service. Splunk automatise la gestion des incidents et permet aux équipes de collaborer à distance.

Opérations de sécurité
La sécurité est, depuis toujours, une problématique fondamentale de l'industrie du paiement. La diversité des produits et des services, ainsi que les complexités qui les accompagnent, font de la protection des systèmes de paiement une tâche ardue.

La directive PSD2 rehausse les exigences en matière de sécurité et contraint les banques à améliorer l'authentification et la sécurité des processus entourant les API.

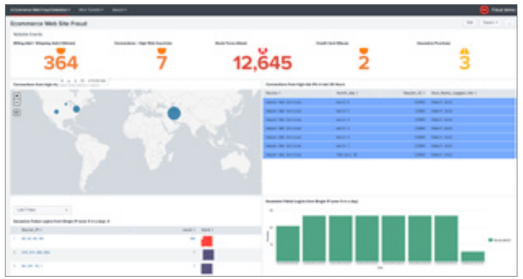
La norme de sécurité des données (DSS) PCI exige que l'ensemble des commerçants, prestataires de services et institutions financières appliquent des critères minimaux de sécurité et de supervision des systèmes dans l'environnement de données des possesseurs de cartes (CDE).

Toute entreprise qui conserve, traite ou transmet des données de possesseur de carte de paiement est tenue de superviser régulièrement son CDE conformément à la norme DSS PCI.

La DSS comprend 12 exigences contraignantes pour les entreprises, et qui englobent des politiques de sécurité, des procédures et des directives pour le stockage, le traitement et la transmission des données des possesseurs de cartes.

Valeur

Les passerelles, les réseaux et les banques affichent tous une disponibilité supérieure, une latence de paiement réduite, un recul du taux de fraude et un coût d'exploitation à la baisse.



Les tableaux de bord Splunk facilitent le suivi des problèmes de sécurité courants et des ICP stratégiques pour votre activité, afin que vous puissiez prendre des décisions informées et agir pour protéger et développer votre entreprise.

Tous les acteurs parviennent à respecter les obligations DSS PCI et mettent sur pied une plateforme de données permettant de gérer d'autres réglementations et rapports. De nombreuses sociétés indiquent que Splunk les aide à mettre au point de nouveaux produits et services. La durée et le coût de la livraison sont réduits.

Worldpay compte parmi les leaders internationaux du paiement. Cette société utilise Splunk pour superviser, analyser et protéger son infrastructure de paiement. Cet organisme traite chaque année 40 milliards de transactions de paiement issues de l'e-commerce, soit 1 500 milliards de dollars répartis dans 146 pays et 126 devises. Il ingère 6 To de données par jour, provenant de 25 000 sources différentes. Worldpay utilise Splunk comme plateforme de données pour sa sécurité et son infrastructure et exploite les données machine pour superviser son cloud, obtenir des informations en temps réel sur les transactions et contrôler l'état de santé des applications.

En savoir plus sur Splunk chez Worldpay.

worldpay

Suivi des transactions

Défi

Les sociétés de services financiers doivent impérativement être en mesure de suivre les transactions tout au long de leur cycle de vie. Cela leur permet d'offrir un meilleur niveau de service à leurs clients, d'améliorer la sécurité et de résoudre rapidement les problèmes techniques.

Les outils de gestion des performances des applications (APM) utilisent l'instrumentation bytecode pour modifier le code des applications compilées à la volée, permettant ainsi de retracer les transactions commerciales au fil des différentes étapes du processus. Les sociétés peuvent obtenir des informations plus précises sur leurs applications clés en exposant les nouvelles métriques du code des applications afin de corriger les défauts d'efficacité.

L'un des inconvénients de l'instrumentation bytecode est qu'elle est considérée comme une forme intrusive de supervision, dans la mesure où elle introduit une consommation supplémentaire de ressources pour l'hôte sous-jacent.

Par exemple, une consommation de ressources accrue sur des systèmes de transactions haute fréquence peut augmenter la latence au point d'impacter la vitesse à laquelle une société peut exécuter ses transactions. À cause de cette latence supplémentaire, la société n'aura pas la vision la plus à jour de l'état du marché, ce qui peut influencer ses décisions d'opérations et lui faire perdre des opportunités au profit de nombreuses autres sociétés bénéficiant d'une image plus actuelle du marché, et donc en meilleure position de réagir à son évolution.

Dans un autre scénario, l'utilisation de l'instrumentation bytecode sur un site bancaire international, au service de dizaines de milliers d'utilisateurs simultanés, peut avoir un impact inacceptable sur les performances et dégrader l'expérience des utilisateurs finaux.

Les banques cherchent à assurer une supervision de bas niveau impliquant des alternatives à l'instrumentation bytecode sur les systèmes qui sont sensibles à la consommation de ressources supplémentaires. Toutes les applications ne se prêtent pas à une supervision à l'aide de l'instrumentation bytecode, en particulier les logiciels commerciaux qui ne fournissent pas les points d'accroche requis pour exposer leurs composants internes ; les clients utilisent alors au mieux les logs et les métriques disponibles.

L'approche de Splunk

Il faut donc inventer une autre approche pour les applications qui exigent une supervision détaillée et bas niveau des performances, mais ne peuvent supporter la consommation de ressources demandée par l'instrumentation bytecode. Avec Splunk, il est possible d'élaborer des ID de transaction synthétiques dans la sémantique de journalisation pour les applications critiques, de façon à ce que les transactions puissent être reliées les unes aux autres et tracées tout au long du processus à l'aide des fichiers de log de l'application, sans recourir à l'instrumentation bytecode. Cette approche est considérée comme non intrusive et réduit considérablement la consommation de ressources supplémentaires sur les hôtes concernés par rapport à l'instrumentation bytecode.

Avec Splunk, il est possible de conserver, extraire et afficher les événements consignés en temps réel pour visualiser le parcours des transactions, tout en évitant que le processus de supervision ne dégrade les performances de l'application. Le forwarder Splunk permet de recueillir et transmettre les données de l'hôte aux indexeurs Splunk. Le forwarder est conçu pour consommer le strict minimum de ressources, car il se contente de joindre les fichiers de log et d'envoyer les données directement aux indexeurs Splunk, qui en assurent la lecture. Quelques secondes après qu'un client s'est connecté à une plateforme et navigue dans différents services, les utilisateurs de Splunk peuvent suivre son parcours et identifier les points problématiques.

Lorsqu'une demande supplémentaire de performance est acceptable, les outils APM permettent de mesurer les applications par injection de bytecode, afin de recueillir les métriques des serveurs, de détecter les défauts de performance du code et de calculer les temps de réponse pour l'utilisateur. En revanche, les APM présentent des limitations rédhibitoires et ne permettent pas de superviser toute la pile, comme l'exige le dépannage des incidents IT complexes. C'est là que Splunk excelle, car il couvre toute la pile logicielle et matérielle tout en consommant les métriques bas niveau capturées par les solutions APM si nécessaire.

Valeur

Avec Splunk, une entreprise peut mener une supervision bas niveau de ses applications sans exercer de pression indue sur les ressources du système. Grâce à l'introduction dans les logs un ID traçable permanent pour chaque transaction, les équipes d'assistance peuvent superviser les flux de bout en bout, bénéficier d'informations plus détaillés sur le code de l'application, et identifier les goulets d'étranglement potentiels sans outil APM, contribuant ainsi à la consolidation des outils et à la réduction des coûts.

Visualisez une transaction du début à la fin, quels que soient les systèmes, les utilisateurs et les régions. Splunk fournit une source de vérité unique pour la traçabilité des transactions.

OPÉRATIONS BANCAIRES ET D'ASSURANCE

Traçabilité ouverte

Défi

La complexité des architectures modernes peut transformer la résolution des problèmes en un véritable casse-tête pour les équipes IT et DevOps. La pile technologique comprend de nombreuses couches et dépendances et les problèmes les plus granulaires peuvent intervenir au niveau du code, ce qui rend la recherche de la cause profonde et sa résolution encore plus difficiles.

La traçabilité distribuée ajoute un identifiant persistant à l'échelle de tout un environnement technologique distribué et offre de nombreux avantages dans les architectures logicielles d'aujourd'hui telles que les environnements serverless et les contextes de microservices ayant chacun leur autonomie et leurs fichiers de log. L'identifiant traçable permet de comprendre le flux d'exécution intervenant entre les différents microservices. Zipkin et Jaeger sont capables de lier les transactions entre elles pour créer une trace représentant l'ensemble d'une opération.

Ils ne permettent toutefois pas de corréler les logs et les métriques de l'ensemble de la pile pour les équipes informatiques et les développeurs qui cherchent à identifier la cause profonde des problèmes pour les résoudre, en particulier lorsqu'ils ne sont pas liés au code.

Dans un environnement serverless ou de microservices, les clients préfèrent aujourd'hui la traçabilité distribuée à l'intégration d'un agent d'injection de bytecode, et cette nouvelle pratique est en train de devenir la norme. La traçabilité distribuée permet aux équipes informatiques et aux développeurs de suivre une requête tout au long de son cheminement entre les différents composants logiciels répartis dans de multiples applications, services et bases de données, mais aussi lors de son passage auprès d'intermédiaires tels que les proxys. Des étiquettes peuvent être ajoutées aux données pour que les utilisateurs puissent les filtrer selon le contexte, mais aussi analyser et représenter les traces afin de visualiser le parcours de chaque requête et la durée de chaque étape.

La supervision traditionnelle s'applique aux machines, aux réseaux et aux applications ; le suivi des transactions dépasse cette approche pour atteindre l'observabilité des interactions, ce qui facilite :

- le débogage ;
- la traçabilité distribuée ;
- l'analyse des performances ;
- l'analyse comportementale.

L'OpenTracing est un standard permettant de mettre en œuvre la traçabilité distribuée. Elle spécifie des informations clés comme la provenance d'un appel, sa destination, l'identifiant de transaction et son type. Ces informations peuvent être consignées sans qu'un agent intrusif n'injecte de byteCode, ce qui consomme des ressources et ajoute de la latence.

Avec l'adoption progressive des microservices, de la conteneurisation et des technologies serverless, les développeurs souhaitent pouvoir ajouter du code OpenTracing à leurs applications pour faciliter l'identification des problèmes et l'amélioration des niveaux de service. Un identifiant unique est inséré dans l'en-tête de chaque requête afin d'identifier la transaction directement dans le code de l'application. Cette transaction est normalement appelée « trace » et représente l'intégralité du parcours de la transaction, de bout en bout. Chaque trace est composée de plusieurs périodes telles qu'une demande d'assistance ou une requête de base de données. Chaque période est associée à un identifiant unique et peut générer des périodes « enfants », ayant elles-mêmes potentiellement plusieurs parents.

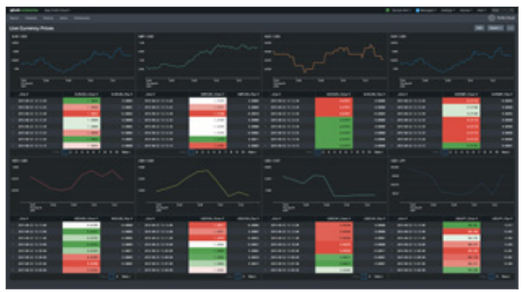
L'approche de Splunk

L'OpenTracing inclut une spécification d'API, des frameworks, des bibliothèques et de la documentation pour spécifier le projet. L'OpenTracing permet aux développeurs d'ajouter une instrumentation au code de leurs applications en utilisant des API ouvertes et indépendantes pour transmettre des entrées de log à un traceur comme Splunk, via le collecteur d'événements HTTP (HEC). Les données de performances des applications et les traces des transactions sont ainsi rassemblées et corrélées avec d'autres sources (système d'exploitation, applications, réseau, stockage, virtualisation, etc.) à des fins de résolution des problèmes et de supervision des performances.

Les développeurs peuvent utiliser la traçabilité distribuée pour établir le profil de leurs applications et les superviser, ce qui facilite le débogage et l'optimisation de leur code. Une fois que le code de l'application contient ces instruments de mesure, les équipes informatiques et de développement peuvent détecter et diagnostiquer les problèmes de performances et assurer plus facilement le niveau de service attendu. Les utilisateurs qui examinent les données peuvent ensuite isoler les points de latence et de blocage grâce aux outils du Splunk Machine Learning Toolkit, et ainsi détecter plus rapidement les comportements anormaux qui peuvent émerger entre deux publications de code.

Valeur

En quelques lignes de code, Splunk peut remplacer les traceurs existants. Les traces de transaction obtenues viennent enrichir les données d'infrastructure et de log déjà recueillies pour offrir une meilleure visibilité sur les architectures logicielles distribuées d'aujourd'hui. Le nombre d'incidents est réduit, la visibilité des points sensibles et des goulots d'étranglement des applications est renforcée, et les niveaux de service s'améliorent, améliorant ainsi la satisfaction des utilisateurs et le score de promoteur net.



La supervision des traces et des transactions en temps réel présente de nombreux avantages. Ici, les prix en devises sont actualisés dans un modèle.

Centre des opérations de gestion des risques

Défi

Les Responsables des risques (CRO) et leurs équipes sont submergés d'informations. Ils doivent tout traiter, de la vue à grande échelle du capital et des liquidités d'une société, jusqu'aux informations granulaires des transactions individuelles. Il faut ensuite qu'ils les remettent en contexte pour que les décideurs puissent les comprendre et agir en conséquence.

Les données exploitées par les équipes de gestion des risques sont nombreuses et vont des déclarations réglementaires hebdomadaires et mensuelles agrégées de haut niveau, aux limites quotidiennes et expositions en temps réel sur les instruments échangés. Cet environnement de données est si complexe qu'il arrive souvent que le CRO dispose de son propre service informatique (CRO/IT), armé des compétences et systèmes spécialisés pour faire face aux exigences inhérentes à la complexité, au volume et à la latence.

Au défi posé par les données s'ajoutent la complexité et le coût des circuits à faible latence (réseaux entre les banques et les places boursières), la complexité des exigences réglementaires des transactions et les cadres réglementaires toujours plus étroits à respecter pour rester en conformité avec la loi et les limites de risque acceptables de la banque.

L'approche de Splunk

De nombreux directeurs du risque ont mis en place un centre des opérations de risque où les équipes de risque et les cadres de l'entreprise peuvent consulter toutes les informations de risque en contexte, et surtout, en temps réel.

Les domaines et indicateurs de risque les plus courants sont les suivants :

- Capital économique
- Capital réglementaire
- Métriques des risques liquidité : ratios de financement net/stable
- Métriques des risques du marché : actifs pondérés selon le risque, sensibilités et valeur à risque, collatéraux
- Métriques de risque de crédit : limites, exposition, expositions potentielles attendues, radiation
- Risque de crédit de contrepartie et ajustement de valeur de crédit (CVA)
- Échanges Forex
- Facteurs de risques opérationnels
- Menaces de cybersécurité
- État des réseaux de paiement
- État des réseaux de DAB

Les défis techniques associés à l'apport d'une telle variété d'informations sont tous sauf triviaux et conviennent parfaitement à Splunk. De nombreuses grandes banques utilisent Splunk pour superviser et capturer des milliers de sources de données. Splunk est capable d'établir des corrélations entre des milliers de sources et de mettre ces corrélations en évidence en temps réel. Ces mêmes données peuvent être conservées pendant une période définie (les périodes de conservation étant automatisées) pour servir à de futures investigations ou à des rapports réglementaires (MiFID II par exemple).

Splunk est alors utilisé pour créer des applications de type tableau de bord mais, contrairement aux tableaux de bord traditionnels, les différents éléments qui les composent peuvent être actualisés indépendamment, ce qui permet de combiner facilement mesures lentes et rapides. Il est possible de définir des agrégations de façon ponctuelle pour permettre aux utilisateurs professionnels de poser leurs questions en fonction de l'état du marché un jour donné. Les opérations d'exploration de routine sont simplifiées, et si quelqu'un souhaite poser une question inédite et très complexe sur les données, les capacités de recherche de Splunk permettent d'obtenir tous types de réponse ou presque, et de les actualiser en temps réel. Il peut s'agir, par exemple, d'un calcul d'exposition ad hoc ou même d'un calcul plus complexe comme l'évaluation du prix d'un nouvel instrument.

C'est la possibilité de définir une agrégation, de concevoir une recherche et de diffuser des données en temps réel qui rend Splunk supérieur aux autres outils.

De nombreuses banques utilisent Splunk pour développer des applications de risque riches en informations et des visualisations graphiques parlantes de leurs activités, pour révéler les motifs remarquables et les exceptions, et identifier dans les données des tendances émergentes qui pourraient autrement passer inaperçues. Splunk est capable d'alimenter les modèles de ML avec des données en temps réel pour offrir à l'entreprise un modèle opérationnel plus compétitif.

Valeur

Les sociétés de services financiers qui font reposer leur centre des opérations de gestion des risques sur Splunk bénéficient d'une vision du risque à l'échelle de toute l'entreprise. Elles peuvent observer plusieurs classes d'actif en contexte et obtenir des niveaux supérieurs de flexibilité. Les informations peuvent être agrégées à tous les niveaux requis.

Surtout, elles bénéficient de la souplesse d'une plateforme capable d'alimenter le centre des opérations mais aussi d'être au service de différentes équipes opérationnelles, qu'elles soient impliquées dans la planification ou dans la préparation des déclarations réglementaires.

Splunk permet aux sociétés de services financiers de bénéficier d'une vision globale de leurs niveaux de risque en temps réel, mais aussi de la possibilité de s'adapter aux marchés et à l'évolution des exigences des autorités de régulation.

« Nous réunissons nos fleurons, 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 d'AWS nous donne les meilleures armes possibles pour protéger nos investisseurs. »

— Gary Mikula
Directeur senior, Sécurité informatique et en ligne, FINRA

En savoir plus sur Splunk chez FINRA.

Tests de résistance financiers

Défi

Cela fait longtemps que les banques et les compagnies d'assurance doivent effectuer des tests de résistance. La fréquence et la complexité de ces tests de résistance change chaque année. Les banques doivent tester leurs portefeuilles en interne par rapport aux risques de crédit et de marché. Splunk est généralement employé pour deux types de tests de résistance : (a) évaluation d'un portefeuille par un trader (b) test de résistance réglementaire portant généralement sur toute l'entreprise (banque ou compagnie d'assurance). Les tests de résistance à l'échelle de la société sont obligatoires en vertu de réglementations telles que Basel III, Solvency 2 et CCARS. La fréquence des rapports peut être hebdomadaire, mensuelle ou trimestrielle. Certaines sociétés effectuent ces tests tous les jours, selon leur modèle commercial.

Les tests de résistance sont simples dans leur concept : dans leur forme la plus élémentaire, il s'agit d'évaluer comment une position unique est sensible à une modification d'un seul facteur de risque sur le marché, par exemple, une variation d'un point de base du cours du pétrole brut.

Il est également possible d'effectuer un test pour déterminer comment cette même position réagit à un certain nombre de facteurs de risques : le cours du pétrole brut, le taux de change entre livres/dollars américains, et le niveau du S&P 500. Mais il est aussi possible d'évaluer un grand nombre de combinaisons différentes des facteurs ci-dessus, en allant éventuellement même jusqu'à 1 000 combinaisons, ce qui ajoute de la complexité.

Dans un test de résistance portant sur toute l'entreprise, chaque position est évaluée dans un large éventail de scénarios de résistance, qui sont conçus pour tester un événement de marché majeur ou une grave détérioration des conditions économiques. Ces tests peuvent exploiter les moteurs d'estimation existants de la société, mais d'autres tâches sont nécessaires pour les mener à bien de façon exhaustive. Bien souvent, ils exigent une grande puissance de calcul et peuvent prendre des heures, voire des jours, même avec un matériel informatique conséquent. Certaines sociétés testent jusqu'à 50 000 scénarios différents. Les sociétés qui calculent spécifiquement la valeur conditionnelle à risque (CVaR) doivent parfois traiter de très grands volumes. Il n'est pas inhabituel que le nombre de simulations atteigne les 500 000.

Les tests de résistance produisent des fichiers de données massifs incluant les résultats de chaque test. En outre, les moteurs de gestion des risques produisent souvent des fichiers au format complexe et difficile à lire pour les logiciels conventionnels. Ils doivent être agrégés et chargés dans un moteur d'analyse adapté pour pouvoir être visualisés et interprétés. Les résultats des tests doivent être régulièrement communiqués sous un format de rapport spécifique aux autorités de régulation.

Les gestionnaires de risques doivent analyser attentivement les données pour déterminer s'il faut modifier leur portefeuille pour augmenter ou réduire le risque, en fonction des résultats obtenus et comment le faire. Avant de commencer ce processus, l'entreprise doit avoir agrégé toutes les données de risque pertinentes et les avoir mises à disposition du processus de test.

L'approche de Splunk

Les tests de résistance puis l'analyse et la distribution des résultats représentent un exercice parfaitement adapté aux capacités de Splunk. Splunk peut agréger les données de risque de plusieurs emplacements, et ce quasiment en temps réel, tout en prenant en charge les grands volumes de données impliqués. Splunk charge ensuite les résultats des moteurs d'estimation, du scénario de résistance, des moteurs Monte-Carlo et de CVaR, ainsi que toutes les autres données externes utiles, et les rendre exploitables au sein d'un seul et même environnement.

Les gestionnaires de risques qui doivent exécuter des recherches complexes peuvent tirer parti de l'évolutivité horizontale de Splunk et le déployer sur le matériel adapté à leurs données. Les sociétés qui effectuent les tests une fois par mois peuvent opter pour la version cloud (privé ou public) de Splunk et profiter ainsi de l'évolutivité proposée, en ne payant le fournisseur de cloud que pour la capacité réellement nécessaire.

Les gestionnaires de risques tireront parti des capacités de machine learning intégrées à Splunk pour exécuter des modèles analytiques à partir des données contenues dans Splunk et réaliser des tests de résistance. L'entreprise peut ainsi extraire une valeur supplémentaire de sa plateforme de test et utiliser les données de risques et les résultats des tests pour prendre d'autres décisions.

Valeur

Les sociétés qui réalisent leurs tests de résistance avec Splunk peuvent économiser des milliers d'heures d'efforts dans la gestion de leurs données de risque. La possibilité de charger d'abord les données sans avoir à élaborer un modèle de données est en cela un atout considérable.

Splunk peut charger les événements de sources multiples puis les agréger à la demande, ce qui rend le système bien plus agile tout en réduisant les efforts de développement requis au départ. Le fait de pouvoir apporter aux autorités de régulation la preuve que les données de risque et le processus de test sont robustes réduit la probabilité que les autorités n'imposent de quelconques limites aux opérations de la société.

Transactions à haute fréquence et faible latence

Défi

Les personnes qui réalisent des transactions à faible latence exercent leurs activités à des niveaux de performances techniques extrêmes. Leurs exigences poussent les machines, les logiciels, les réseaux et les personnes jusqu'à leurs limites. Ne pas atteindre les performances les plus rapides et la fiabilité la plus élevée, c'est automatiquement manquer des opportunités, perdre des affaires et potentiellement subir des pertes. Quelques nanosecondes peuvent faire la différence entre une bonne journée et un désastre.

Les acteurs de ce marché doivent donc développer, superviser et optimiser les algorithmes des stratégies à faible latence. Une société possède souvent des centaines de modèles différents qui peuvent être déployés en quelques secondes selon le type d'instrument échangé, la place boursière et l'état du marché ce jour-là. Il est indispensable de disposer en permanence du meilleur algorithme possible en production.

Les participants doivent également comprendre et gérer les différents « circuits », ces réseaux privés qui relient leurs datacenters aux différentes places boursières. De nombreuses places d'échange proposent une stratégie de colocation (installation d'un serveur sur place). Cette option doit encore être gérée et optimisée de manière à offrir la latence la plus faible possible (par rapport aux autres serveurs en colocation) et une disponibilité de 100 %. Il faut également superviser les performances de chaque site, du point de vue technique, bien sûr, mais aussi de l'exécution des ordres, en déterminant par exemple la proportion de tentatives de transactions qui se concrétisent effectivement. Des « taux de remplissage » élevés sont essentiels pour conserver l'activité d'un client : il arrive souvent qu'un client déplace ses opérations si les performances ne sont pas à la hauteur des niveaux attendus. Les participants doivent superviser et optimiser les informations provenant des algorithmes, des systèmes PC, des réseaux, des systèmes d'exécution FPGA et des API, qui doivent tous fonctionner parfaitement ensemble pour délivrer les performances voulues.

L'approche de Splunk

De nombreux participants aux opérations boursières à faible latence utilisent Splunk. Pour la plupart d'entre eux, la plateforme leur permet de superviser leur infrastructure boursière, de mesurer les performances des différents réseaux, places et algorithmes, et de signaler les anomalies. Les développeurs utilisent largement les capacités DevOps de Splunk en insérant des balises meta dans les algorithmes de transaction pour en mesurer l'efficacité et corréler leurs performances à l'état du marché, à la place d'échange et à l'instrument.

Splunk peut établir une corrélation entre une série chronologique d'événements et des milliers d'événements simultanés pour mettre au jour des informations jusqu'ici ignorées des traders et des développeurs d'algorithmes. Ces informations permettent d'affiner les algorithmes et de mettre au point de nouvelles stratégies.

Les développeurs d'algorithmes doivent souvent tester de nouvelles stratégies sur les données historiques et celles-ci peuvent être très volumineuses en raison de la fréquence des échanges. On analyse couramment des jeux de données de 50 To ou plus, ce qui impose d'utiliser une plateforme évolutive. Heureusement, l'évolutivité horizontale de Splunk facilite ce type d'analyse. D'ailleurs, les plus grands clients de Splunk indexent plus de 5 pétaoctets de données par jour.

Les équipes techniques qui gèrent l'infrastructure disposent ainsi d'une visibilité sur les opérations de l'ensemble du réseau et peuvent détecter les pics de processeur ou de latence, ce qui leur permet de résoudre les problèmes de performances et d'améliorer la fiabilité. Splunk ne réagit pas à l'échelle de la nanoseconde des algorithmes, mais la plateforme peut prendre en charge et enregistrer les données à l'échelle de la nanoseconde pour produire des analyses et des informations dans les secondes qui suivent les événements. Cette capacité est indispensable pour la conformité MiFID II, la 2e édition de la directive sur les marchés d'instruments financiers, qui exige qu'une banque tienne des registres précis de ses opérations et de ses prix afin d'apporter la preuve de « meilleure exécution possible ». MiFID II spécifie que les horloges doivent être synchronisées avec une précision de 100 microsecondes, ce que permet Splunk. Il se peut que cette limite de 100 microsecondes doive être améliorée à l'avenir, en fonction de l'évolution de l'industrie. Splunk peut également déclencher des processus capables d'automatiser la résolution d'écarts de qualité.

Valeur

Il permet aussi aux entreprises d'obtenir une image globale de leurs opérations boursières à faible latence. La plateforme permet aux développeurs d'algorithmes d'affiner leurs modèles et de mettre au point de meilleures stratégies. Elle identifie les corrélations entre des événements connexes, permettant ainsi aux équipes de délivrer une qualité de service supérieure. Les sociétés qui utilisent Splunk dans leurs opérations boursières à faible latence sont plus fiables et potentiellement plus rentables.

Superviser l'ensemble de l'environnement de transactions à faible latence permet d'atteindre les meilleures performances, mais aussi de reconnaître les caractéristiques des places d'échange susceptibles de les accroître.

Agrégation des données de risque en temps réel

Défi

La plupart des banques et des compagnies d'assurance ont déjà intégré une forme de dépôt de données de risque centralisé pour respecter les exigences d'agrégation des données de risque du Comité de Bâle sur la supervision bancaire (BCBS 239), du cadre Comprehensive Capital Analysis and Review (CCAR) (pour les banques) ou de Solvency II (pour les assureurs).

Beaucoup d'institutions ont développé des solutions à la hâte en s'appuyant sur des bases de données relationnelles existantes ou des lacs de données. D'autres ont encore des difficultés à remplir leur obligation quotidienne d'agréger les données de risque et de les rendre disponibles à des fins de tests de résistance et de déclarations réglementaires.

Face au volume impressionnant de données, à la diversité des sources et des systèmes, à la complexité des données et aux aspects logistiques d'opérations internationales actives 24h/24, 7j/7, beaucoup d'institutions cherchent une solution plus simple et plus rentable, qui soit capable de faire face aux modifications fréquentes des réglementations tout comme à l'évolution des produits et des marchés.

Bien des exigences émanant de l'industrie et des autorités de régulation incitent les institutions à mettre en place un environnement en temps réel pour la gestion des données de risque. Il est donc logique pour elles de gérer leurs données de risque avec un modèle d'exploitation en temps réel similaire à celui de leurs environnements de transaction.

Vous trouverez ci-dessous deux extraits de la réglementation BCBS 239 sur l'agrégation des données de risques qui illustrent cette exigence :

BCBS 239 : Principe 5
Ponctualité : une banque doit pouvoir générer des données de risque agrégées et à jour sans délai, tout en respectant les principes d'exactitude, d'intégrité, d'exhaustivité et d'adaptabilité. La ponctualité dépend de la nature et de la volatilité potentielle du risque mesuré ainsi que de son degré de criticité pour le profil de risque global de la banque. La ponctualité dépendra également des exigences de fréquence de rapports de gestion des risques qui s'appliquent à la banque, en situation normale comme en situation de résistance ou de crise, selon les caractéristiques et le profil de risque global de la banque.

BCBS 239 : Principe 6
Adaptabilité : une banque doit pouvoir générer des données de risque agrégées pour respecter un large éventail d'exigences de déclarations ponctuelles de gestion des risques, notamment en situations de résistance ou de crise, en cas d'évolution des besoins internes, et pour répondre à des demandes réglementaires.

L'approche de Splunk

Splunk peut servir d'agrégateur et de dépôt central pour toutes les données de risque. Splunk peut charger les données d'une myriade de systèmes de négociation, moteurs de gestion des risques et flux de données de marché différents, qu'ils soient locaux ou distants.

Splunk n'a pas besoin que les modèles de données soient établis à l'avance : vous pouvez donc charger directement tout type de nouvelles données. Les schémas ne sont créés que sur demande, en fonction du type de recherche requis par l'utilisateur ou le processus.

Les données sont chargées en temps réel et les tableaux de bord présentent la position de risque en temps réel de l'institution aux responsables du risque et autres parties intéressées.

En plus des tableaux de bord en temps réel, les sociétés ont besoin d'exploiter les données historiques pour effectuer des tests de résistance, des modélisations, des simulations et des déclarations réglementaires. Splunk peut prendre en charge toutes ces tâches car la plateforme peut s'étendre pour accueillir de grands volumes de données et analyser des séries chronologiques de données de risque.

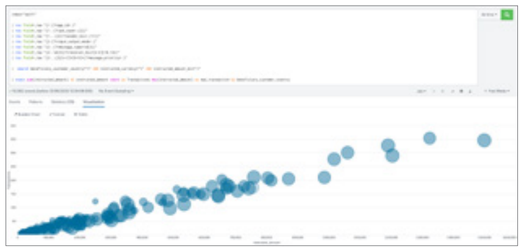
Les capacités de machine learning intégrées de Splunk permettent aux utilisateurs d'élaborer et de déployer une large gamme de techniques de modélisation différentes et d'effectuer des analyses statistiques en s'appuyant sur des données historiques et très récentes.

Valeur

Les institutions peuvent extraire une valeur considérable de l'utilisation de Splunk comme source centralisée de données de risque.

Cela leur permet non seulement de remplir toutes leurs obligations réglementaires, mais aussi de gérer leurs données de risque dans un environnement hautement évolutif, flexible et sécurisé, en ayant la possibilité d'exploiter ces mêmes données dans de nombreux scénarios d'utilisation allant des rapports quotidiens aux tests de résistance.

Splunk peut devenir le dépôt qui alimentera toutes les déclarations réglementaires, ainsi que le moteur qui générera les tableaux de bord utilisés par le responsable des risques ou le centre des opérations de gestion des risques.



Les institutions peuvent respecter les exigences des éléments de BCBS 239, tout en bénéficiant d'une plateforme robuste qui permet l'agrégation, le stockage et l'analyse des données de risque.

OPÉRATIONS BOURSIÈRES ET RISQUE

Opérations annulées et modifiées

Défi

Les opérations ne se concrétisent pas toutes. Elles ne sont pas toujours saisies correctement. Il arrive souvent qu'une opération doive être annulée ou modifiée pour des raisons légitimes : on veut apporter une information qui n'était pas encore disponible au moment de l'échange, ou ajouter un code de contrepartie ou un identifiant d'entité juridique. Certains produits sont difficiles à négocier et le volume de modification peut être élevé. Tout cela est parfaitement normal… sauf quand ça ne l'est plus.

L'approche de Splunk

Tous ceux qui travaillent dans un environnement de trading ont déjà vu un rapport d'annulations et d'amendements. Toutes les banques en produisent quotidiennement, généralement à la fin de la journée après la clôture du marché, ou parfois le matin suivant. Ces rapports sont essentiels pour déterminer si une opération a été interrompue ou modifiée pour de bonnes raisons, pour produire des rapports quotidiens de profits et de pertes et pour corriger les erreurs.

On peut souvent y reconnaître des motifs, et voir par exemple qu'un produit ou un instrument particulier est difficile à négocier, ou qu'un collaborateur multiplie les fautes de frappe et ajoute des zéros supplémentaires ou déplace les virgules. Ce sont des choses qui arrivent. Certains daltonismes qui empêchent de voir la différence entre rouge et vert sont également sources de problèmes.

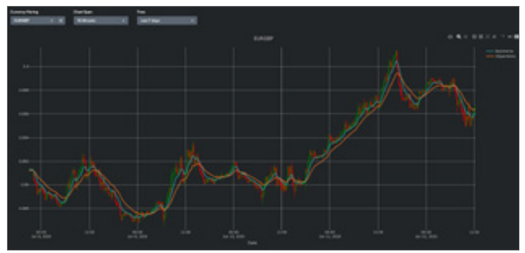
En plus de ces aspects, les rapports d'annulation et de modification sont très utiles pour mettre en évidence les comportements de trading abusif. Des séquences d'opérations régulièrement annulées puis reprogrammées peuvent mener un enquêteur jusqu'à un opérateur malhonnête ; c'est d'ailleurs l'un des signes clés utilisés dans les contrôles de risque opérationnel. Les banques connaissent bien ces types de séquences suspectes et savent comment les détecter.

Elles doivent également réconcilier les opérations de multiples comptes utilisés par un trader spécifique. Malheureusement, les données ne sont pas en temps réel et les enquêteurs ont souvent affaire à des événements passés dont ils s'efforcent de reconstituer le puzzle.

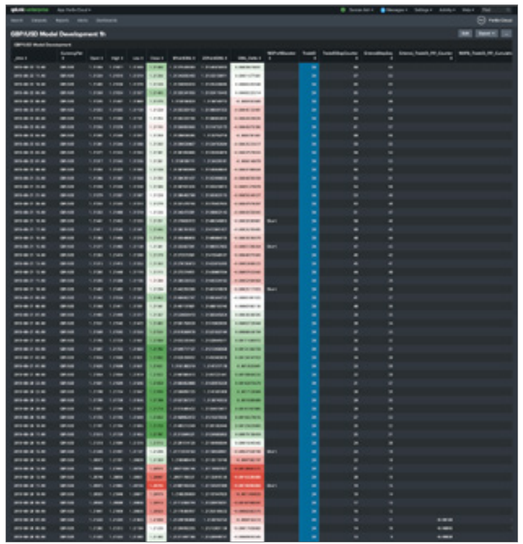
Ce n'est pas le cas avec Splunk. Les événements peuvent être supervisés en temps réel, ce qui permet de procéder rapidement à la réconciliation pour avertir au plus tôt un responsable du risque lorsqu'une séquence particulière se produit. Splunk utilise les algorithmes de machine learning pour superviser les comportements et rechercher des motifs suspects et des séquences d'événements qui sortent de ce qu'on considère la « normalité ». Le produit Phantom de Splunk peut être utilisé pour automatiser l'orchestration et la réponse à un incident.

Valeur

La réconciliation rapide des opérations P&P après une annulation ou une modification fait économiser du temps et de l'argent, met en évidence les problèmes opérationnels touchant des produits spécifiques et permet de les résoudre rapidement. Identifier un opérateur qui agit hors des limites autorisées peut éviter des coûts, protéger la réputation de l'institution et même, dans certains cas, éviter des pertes considérables.



Les sociétés de services financiers qui gèrent leurs données d'échange et de risque dans Splunk produisent et gèrent leurs rapports d'annulation et de modification avec une grande efficacité, et actualisent les données en quasi-temps réel. Vous pouvez donc facilement détecter les anomalies et mener une enquête plus approfondie.



En supervisant chaque transaction en temps réel, il devient possible de comprendre la cause profonde des annulations, des modifications et des rejets de transactions, et d'identifier les personnes et les processus concernés.

OPÉRATIONS BOURSIÈRES ET RISQUE

MiFID II : éviter les écarts horaires et les échecs de transactions

Défi

La transparence, le signalement et la traçabilité sous-tendent de nombreuses normes techniques réglementaires (RTS) de MiFID II, comme la nécessité de conserver une trace précise des événements à des fins d'audit et de conformité. L'horodatage précis des transactions financières et des messages inclus dans le cycle de vie d'une opération est indispensable, car c'est lui qui permet d'effectuer une supervision globale des ordres de plusieurs places et de détecter les cas d'abus de marché. Il permet également d'établir une comparaison claire entre la transaction et les conditions du marché au moment de l'exécution. RTS 25 stipule ce qui suit :

- Les opérateurs des places boursières et leurs membres (ou participants) doivent mettre en place un système de traçabilité de leurs horloges par rapport à l'heure UTC.
- Les opérateurs des places boursières et leurs membres (ou participants) doivent être en mesure d'apporter la preuve que leurs systèmes respectent les exigences.

MiFID II exige que les serveurs d'application soient synchronisés à l'heure UTC avec un écart maximal acceptable basé sur le type de plateforme de négociation. Les problèmes réseau tels que le jitter (ou gigue), la charge du réseau et l'instabilité peuvent créer des décalages, des imprécisions et des écarts par rapport à l'heure UTC, exposant ainsi les entreprises au risque d'enfreindre les normes RTS. Les institutions doivent respecter les limites ci-dessous imposées par MiFID II :

Opérations de transactions haute fréquence
- Écart maximal de 100 microsecondes par rapport à l'heure UTC
- Granularité de 1 microseconde

Opérations de transactions automatisées générales
- Écart maximum de 1 milliseconde par rapport à l'heure UTC
- Granularité de 1 milliseconde

Opérations de transactions manuelles
- Écart maximum de 1 seconde par rapport à l'heure UTC

Les événements à signaler, comme les serveurs présentant un écart d'horloge supérieur à la marge de tolérance et les opérations affectées, doivent être communiqués aux autorités de régulation en continu ou à la demande (avec un historique de cinq ans).

En utilisant des protocoles établis comme NTP et PTP, il est possible d'exploiter des solutions de supervision ponctuelles pour signaler les décalages temporels touchant l'infrastructure. Toutefois, l'identification des opérations potentiellement affectées et porteuses d'un horodatage inexact peut s'avérer plus difficile.

L'approche de Splunk

Les banques conscientes des défis que représente la conformité à MiFID II savent mettre rapidement sur pied des solutions pour satisfaire les exigences de signalement et de supervision : avec Splunk, cela ne prend que quelques jours, et non des semaines. Splunk est idéalement placé pour signaler les écarts horaires au sein de l'infrastructure de négociation, car la plateforme est capable d'ingérer et de visualiser tous les types de données machine. Comme elle offre la possibilité de corréler les sources temporelles PTP et NTP avec les messages des transactions (FIX, par exemple), elle donne aux places d'échange et aux autorités de régulation une image consolidée de la position de conformité. Il est alors possible de visualiser la gigue temporelle et de déclencher automatiquement des alertes en temps réel lorsque l'écart dépasse un certain seuil.

Avec Splunk, on peut rapidement isoler les opérations qui peuvent avoir été mal horodatées à cause d'un écart horaire excessif, les étudier de près et les signaler aux autorités de régulation. Splunk peut aussi mettre en lumière les opérations dont le prix diffère du meilleur cours acheteur et vendeur national (NBBO, ou EBBO sur le marché européen) à cause d'un problème d'horloge. Avec Splunk, les banques peuvent superviser et déclarer leur état de synchronisation temporelle pour satisfaire la RTS 25 de la MiFID II. En corrélant les données temporelles aux données de transaction, Splunk vous permet d'identifier les opérations qui peuvent avoir été affectées par un décalage temporel.

Valeur

L'assimilation des messages de transaction et des données de décalage temporel dans Splunk aide les banques à se conformer à RTS 25 et de réaliser des économies dans le même temps, en évitant des acquisitions inutiles et des coûts de développement élevés.

Les banques ont souvent des difficultés à analyser les échecs de transaction, en raison de la complexité des workflows et de la diversité des systèmes. Comprendre où et pourquoi une transaction a échoué peut nécessiter beaucoup de temps et d'efforts. Splunk réduit le délai d'investigation sur les échecs à quelques minutes, ce qui permet également d'en réduire le nombre.

En corrélant les données temporelles et les données de transaction, Splunk vous permet d'identifier les opérations qui peuvent avoir été affectées par un décalage temporel.

Opérations IT des institutions financières

Défi

Les institutions financières sont soumises à des exigences informatiques comptant parmi les plus strictes. Les services informatiques doivent prendre en charge des opérations métier qui génèrent une complexité considérable. Les facteurs sont multiples :

- Des bureaux, des collaborateurs et des opérations répartis dans le monde entier
- Une base de clients vaste, distribuée sur plusieurs régions, et qui nécessite un fonctionnement 24h/24, 7j/7
- Des partenaires commerciaux, des contreparties, des réseaux de paiement et des lieux de négociation d'une grande diversité
- Une multiplicité de réseaux publics et privés, avec des opérations à faible latence
- Des milliers d'applications, de produits et de services
- Une grande diversité d'autorités de régulation, de devises, de langues et de fuseaux horaires
- Des équipes de développement qui manipulent des environnements multiples
- Une technologie utilisée comme actif compétitif
- Un environnement de sécurité difficile perpétuellement confronté à des cybermenaces et à des problématiques de confidentialité des données

Ces complexités se traduisent généralement par un vaste service informatique, des accords de niveau de service extrêmement ambitieux et un impératif de disponibilité à 100 % ou presque dans un environnement de haute sécurité.

L'approche de Splunk

Splunk est né dans les opérations IT et elles sont à l'origine de tous les produits Splunk. Les premières versions de Splunk étaient conçues pour relever les défis rencontrés par un service informatique lorsqu'une application rencontrait une défaillance et que les équipes devaient parcourir manuellement les fichiers de log pour diagnostiquer le problème.

Les choses ont considérablement évolué depuis, tout comme Splunk qui peut désormais superviser des milliers de systèmes en temps réel, établir des corrélations entre des milliers de flux de données, et utiliser les informations extraites en temps réel pour orienter la prise de décision. Les professionnels de l'informatique peuvent exploiter toute la puissance des algorithmes de machine learning qui reçoivent les signaux des données en temps réel pour prédire les défaillances potentielles des systèmes et avertir le personnel avant qu'un incident ne se produise, évitant ainsi souvent une interruption de service généralisée.

Pour les équipes qui gèrent l'informatique d'une institution financière, cette idée est proche de l'utopie. Splunk permet aux équipes informatiques de gérer proactivement l'ensemble de leur environnement ; la plateforme permet au centre des opérations réseau (NOC) de superviser le réseau en temps réel et d'affecter des ressources supplémentaires en fonction de la demande. Elle offre aux équipes responsables des applications de la possibilité de prédire la demande et de mettre à disposition les ressources nécessaires à l'avance.

Les développeurs logiciels utilisent les capacités DevOps de Splunk pour gérer tous les aspects du cycle de vie du développement : ils y gagnent un meilleur contrôle du nouveau code, de meilleures procédures de test et d'audit, et la possibilité d'adopter un modèle opérationnel permettant de publier plusieurs fois par jour.

Ces approches améliorent la satisfaction des clients mais aussi la qualité du code qui présente moins de bugs.

Les équipes opérationnelles informatiques doivent collaborer étroitement avec leurs homologues de la sécurité, et ces deux équipes peuvent alors exploiter pleinement la même plateforme de données Splunk pour répondre à une multiplicité de scénarios d'utilisation informatiques et de sécurité, indispensables pour délivrer des services de qualité optimale avec les plus hauts niveaux de sécurité.

Valeur

La valeur provient des niveaux de service exceptionnels qu'il devient possible d'atteindre, avec un taux de disponibilité extrêmement élevé et une résolution très rapide des problèmes. Grâce au modèle opérationnel rendu possible par le machine learning de Splunk et la maintenance prédictive, les problèmes n'entraînent plus d'interruptions de service : ils ne sont même plus remarqués par les utilisateurs.

Les équipes de négociation qui dépendent d'opérations à faible latence ont besoin que l'informatique assure 100 % de disponibilité et des niveaux de latence extrêmement bas sur l'ensemble des réseaux et des systèmes boursiers. Tout défaut entraîne nécessairement des pertes de transactions. À l'inverse, le leadership technologique qui résulte d'une latence plus basse peut être source d'avantage compétitif et de profits plus élevés.

Des milliers d'institutions financières dépendent de Splunk pour assurer le bon fonctionnement de leurs opérations et respecter les exigences techniques extrêmes d'une organisation financière.

« Il est essentiel de comprendre les tendances des volumes de clients pour bien gérer ses activités. Lorsque le trafic sort d'une plage définie, une alerte est immédiatement générée. Le machine learning Splunk nous permet d'enquêter très tôt sur ces phénomènes pour assurer une expérience client parfaitement fluide. »

— Steve Koelpin
Responsable en chef du développement Splunk, TransUnion

En savoir plus sur Splunk chez TransUnion.

OPÉRATIONS IT

Plateforme de grille informatique globale

Défi

Les banques internationales et les hedge funds exploitent des clusters réseau informatiques répartis avec une grande complexité qui englobent souvent des milliers d'hôtes. Ceux-ci exécutent des centaines d'applications qui alimentent les systèmes de gestion des risques et d'estimation, sur lesquels reposent les transactions, la gestion des risques et les obligations réglementaires. Les sociétés de services financiers dépendent fortement des cycles de traitement nocturnes, dont les charges sont prévisibles. Toutefois, la demande exercée sur la plateforme de grille peut varier considérablement car celle-ci est généralement mise au service des analystes quantitatifs, ou « quants », dont les tâches sont plus ponctuelles.

Les réseaux informatiques sont utilisés pour exécuter des applicatifs volumineux dans des délais spécifiques. Par exemple, un traitement de nuit peut nécessiter des centaines d'heures de CPU, ne peut commencer qu'à la fin de la journée d'échange et doit être terminé avant le début de la journée suivante. Le travail est réparti en plusieurs tâches qui sont exécutées en parallèle sur le réseau.

Au cours de ces dernières années, ces plateformes ont commencé à tirer parti de la puissance de calcul supplémentaire offerte par les clouds privés et publics. Les applicatifs sont encore traités en priorité sur des machines locales, mais ils peuvent mobiliser des ressources supplémentaires sur demande dans l'ordre suivant : serveurs physiques locaux > cloud privé > cloud public. Une architecture informatique hybride complique le suivi et la supervision de l'état de santé, des performances et de la sécurité du réseau car les hôtes rejoignent et quittent la plateforme selon la demande. Les quants jouent le même rôle que les équipes DevOps et transmettent continuellement de nouvelles versions de code sur la plateforme réseau. Bien souvent, les plateformes réseau reposent entièrement ou partiellement sur une infrastructure partagée, ce qui rend difficile l'analyse des causes d'origine des ralentissements, en raison du manque de visibilité sur l'environnement partagé. Les équipes responsables des réseaux doivent déterminer si les problèmes sont liés au code ou à l'infrastructure matérielle (goulots d'étranglement notamment), ce qui peut être très long et frustrant.

L'élargissement des plateformes et la nature distribuée de l'infrastructure exige des outils capables de produire une vision complète de tous les composants en quasi-temps réel, sur un large éventail de silos technologiques.

L'approche de Splunk

La gestion efficace d'une plateforme réseau informatique présente de nombreux défis. Les équipes responsables des réseaux ont besoin d'une visibilité complète pour superviser les performances du système de bout en bout, afin d'assurer le bon fonctionnement et la santé de la plateforme.

Plusieurs banques internationales utilisent Splunk pour superviser leur plateforme réseau distribuée, et recueillent des données de log et des métriques auprès des groupes de ressources. Quelques exemples de ces données :

Logs des :
- daemons réseau ;
- applications réseau.

Compteurs de performances des systèmes d'exploitation :
- processeur, mémoire, activité réseau, etc. ;
- métriques de niveaux de virtualisation ;
- métriques de niveaux de stockage (IO, etc.).

Entrées scriptées par :
- appels d'API réseau, provenant par exemple du planificateur de tâches réseau ;
- requêtes de la base de données.

Ces sources de données peuvent être analysées et corrélées pour aider les équipes responsables des réseaux à comprendre le comportement de leur plateforme et à exécuter les tâches suivantes plus efficacement :

- le suivi et la supervision de la santé du système en temps réel ;
- la réduction des temps de résolution des incidents et d'investigation sur les problèmes ;
- l'amélioration de l'efficacité et de la gestion des capacités ;
- l'accélération de l'évolution et l'optimisation du système ;
- l'orchestration d'une plus grande puissance de calcul via Splunk lorsque la capacité de la plateforme ne peut pas satisfaire la demande.

Valeur

Grâce aux alertes proactives en temps réel, Splunk peut informer les équipes responsables des réseaux en cas d'anomalie sur la plateforme, ce qui réduit le temps de recherche et libère les ingénieurs pour leur permettre de travailler sur l'amélioration de l'efficacité. Les indicateurs d'utilisation de la plateforme peuvent être monétisés via des lookups de coût unitaire pour aider les responsables commerciaux à identifier les faibles rentabilités dans leur utilisation du réseau.

La supervision en temps réel de l'environnement réseau permet de maintenir le fonctionnement des opérations à 100 % et de prédire les futurs problèmes

Connectivité et analyse des ordinateurs centraux

Défi

Les ordinateurs centraux se trouvent dans un environnement extrêmement polarisé. Une étude Forrester de 2018 a permis de découvrir que le nombre d'entreprises exécutant des applications critiques sur leur ordinateur central était en réalité à la hausse, contrairement aux rumeurs sur son déclin, et que cela s'accompagnait d'une demande accrue de capacité. Les derniers chiffres suggèrent que la valeur des transactions par carte de crédit traitées sur les ordinateurs centraux représente 6 000 milliards de dollars chaque année. En revanche, le manque de compétences devient un problème de croissance sur le terrain, car les ordinateurs centraux et les personnes qui les administrent sont souvent, au propre comme au figuré, séparés du reste de l'environnement informatique.

La croissance n'est pas négligeable, ce qui s'explique par la fiabilité, la disponibilité et la sécurité des ordinateurs centraux, sans comparaison avec celles des autres plateformes, mais cette approche n'est pas exempte de difficultés. Le manque de visibilité sur les millions d'unités de service (MSU) et les moyennes sur quatre heures peuvent avoir un lourd impact sur les frais de licence mensuels. Cet impact est particulièrement douloureux lorsque l'ordinateur central est en-dehors du champ de vision d'une organisation qui est par ailleurs axée sur les données ; le système est enfermé dans un silo derrière d'obscurs outils en ligne de commande qui limitent l'accès à la couche transactionnelle de la fonction d'une application.

La gestion des défis de ce silo est plus difficile encore lorsque la sécurité et la conformité entrent en jeu : cette problématique est d'ailleurs considérée comme l'objectif numéro 1 ou 2 par plus de 60 % des clients possédant un ordinateur central.

L'approche de Splunk

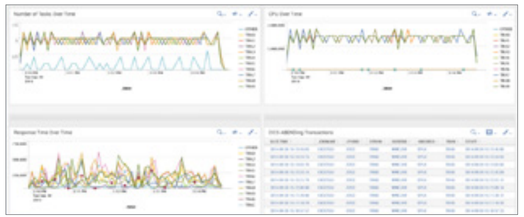
Les solutions ponctuelles imposent des limitations lorsque l'on tente de superviser un ordinateur central au sein du paysage plus large des plateformes informatiques et de sécurité d'une entreprise. Avec l'appui de Splunk et de nos fournisseurs partenaires, il est aussi possible d'intégrer les logs volumineux et complexes figurant dans les outils de gestion des systèmes (SMF) et le SYSLOG de l'ordinateur central à une même plateforme offrant une vision à 360° en temps réel de toute l'infrastructure informatique.

L'intégration avec Splunk IT Service Intelligence (ITSI) permet aux entreprises d'associer des KPI aux composants mainframe de leurs applications stratégiques, ce qui permet d'avoir une connaissance complète des services sous-jacents et de visualiser les relations au sein du flux d'applications.

Lorsque l'on s'intéresse à la sécurité, Splunk peut non seulement offrir la possibilité de superviser et de détecter le parcours des données dans l'ordinateur central et en-dehors, mais aussi d'apporter une visibilité à l'échelle de la plateforme pour réduire le risque de menaces internes, tout en conservant un suivi d'audit pour respecter les exigences des responsables de la sécurité et des contrôleurs.

Valeur

Les processus manuels d'analyse des données ne suffisent plus. Face à la vitesse, au volume et à la nature critique des transactions, les entreprises ne peuvent plus se contenter d'une approche purement réactive. En utilisant Splunk pour examiner cette vaste source de données dans un contexte plus large et en identifiant les problèmes de façon proactive, il est possible de réduire considérablement le MTTR. Étant donné que des données peuvent facilement être recherchées dans Splunk pour produire des tableaux de bord, les données d'ordinateur central, qui étaient jusque-là quasiment inaccessibles sans expertise dans le domaine, sont désormais à la portée de nouvelles équipes commerciales et informatiques, en dépit de l'épuisement du vivier de talents spécialisés.



Suivez les transactions du système de contrôle des informations client (CICS), bénéficiez d'une visibilité sur les performances globales et l'utilisation des ressources, et comparez facilement les données historiques pour analyser les tendances.

Supervision et gestion de la configuration des systèmes et des serveurs

Défi

La gestion et la conformité des configurations de serveurs vont de pair avec le respect des cadres de contrôle des autorités telles que le CIS (centre pour la sécurité sur Internet), le NIST (institut national des normes et des technologies), la PCI (industrie des cartes de paiement) ou la BSI (institution normative britannique). Ces cadres de contrôle décrivent les configurations recommandées et les bonnes pratiques conçues pour renforcer les environnements informatiques contre les attaques, et pour combler les failles facilement exploitées par les acteurs malveillants.

Au vu de ces cadres, de plus en plus d'entreprises doivent examiner leur infrastructure pour déterminer si elle est conforme aux références normalisées de sécurité et de renforcement. Ces exigences s'accompagnent toutefois de nombreux défis. Dans un premier temps, l'entretien de la configuration des serveurs répartis sur de multiples sites et dans plusieurs datacenters représente une lourde charge d'administration et de maintenance pour les équipes informatiques.

Les erreurs de configuration des serveurs peuvent également créer des ouvertures pour les hackers. Les configurations non documentées, qui compliquent le processus de résolution des problèmes, sont souvent la cause d'interruptions de service entraînant des indisponibilités prolongées.

Le Centre pour la sécurité sur Internet (CIS) maintient que l'un des aspects les plus critiques de la sécurité d'une entreprise réside dans « la configuration sécurisée du matériel et des logiciels des appareils mobiles, ordinateurs portables, postes de travail et serveurs. »

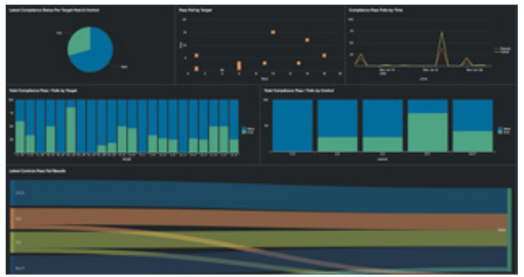
Entre autres choses, cette injonction renforce la nécessité d'appliquer des configurations de système d'exploitation sécurisées par défaut, afin de réduire la surface d'attaque du réseau autant que localement, à l'échelle du système. De nombreux systèmes d'exploitation sont fournis avec des configurations qui facilitent l'installation et l'utilisation, mais elles tendent à élargir la surface d'attaque en autorisant l'exécution d'un code arbitraire et l'escalade des privilèges. En contrôlant et en supervisant les modifications apportées à la configuration des systèmes, les utilisateurs peuvent maintenir leur intégrité et leur sécurité et recevoir des alertes en cas de modification non autorisée.

Impact

Les systèmes qui n'ont pas de configuration sécurisée augmentent la surface d'attaque en augmentant la probabilité que des acteurs malveillants n'installent des malwares ou n'exploitent des privilèges.

Les logiciels malveillants fournissent aux malfaiteurs de nouveaux vecteurs de contrôle. Autoriser les modifications du système sans contrôle ni supervision donne à des agresseurs une plus grande liberté d'utiliser le système comme base pour inspecter le réseau, répandre des virus ou exfiltrer des données.

Enfin, une mise en œuvre déficiente des politiques et procédures de gestion des modifications peut être à la source de divergences croissantes entre les configurations, qui résultent de la multiplication des modifications et mises à jour manuelles. C'est un véritable défi d'obtenir une vue globale de la conformité des serveurs, de comprendre quels serveurs échouent régulièrement aux contrôles de conformité et d'identifier ceux qui ne sont plus conformes. Plus généralement, pour savoir si l'environnement s'approche ou s'éloigne des objectifs de conformité des multiples cadres de contrôle, il faut une approche flexible de l'analyse et des rapports, soit des tâches parfaitement exécutables par Splunk.



L'inspection des serveurs en temps réel permet de veiller à ce qu'ils soient configurés conformément aux spécifications appropriées.

Supervision et gestion de la configuration des systèmes et des serveurs (suite)

L'approche de Splunk

Il existe plusieurs manières d'exploiter à la fois Splunk et éventuellement des technologies complémentaires telles que « Bolt » de Puppet Software pour effectuer des tests de conformité. Il est notamment possible d'inspecter les serveurs d'un environnement afin de vérifier si les configurations attendues sont présentes, puis de créer un événement de log contenant les métadonnées pertinentes afin de faciliter la génération de rapports dans Splunk.

L'outil Bolt de Puppet applique une approche sans agent et se connecte à un serveur distant via le protocole SSH ou WinRM. Il est possible de développer des scripts basés sur différents frameworks (Python, PowerShell, Bash, etc.) et de les faire exécuter par n'importe quelle plateforme. Avec une telle approche, des scripts vérifient les configurations stipulées dans les cadres de contrôle, comme celui du CIS, et renvoient les résultats en temps réel.

Il est également envisageable de développer les entrées de scripts sous la forme d'applications déployées sur les forwarders universels (UF) Splunk exécutés sur chaque hôte, afin qu'ils effectuent les contrôles de conformité et les envoient directement à Splunk. Dans une situation classique, les UF auront déjà été déployés dans le parc de serveurs des clients Splunk, ce qui réduit la distance à parcourir pour recueillir tous les avantages de ce scénario d'utilisation.

Outre les configurations, Splunk vous permet de récupérer d'autres informations utiles auprès de chaque hôte, comme un aperçu des programmes installés. Des entrées scriptées peuvent être configurées de manière à s'exécuter à intervalles réguliers pour superviser constamment les applications installées. Les données envoyées dans Splunk peuvent ensuite être comparées à une liste blanche d'applications approuvées pour détecter les erreurs et les logiciels non autorisés.

En utilisant aussi bien des approches avec et sans agent, les tests de conformité peuvent être exécutés plusieurs fois par jour, offrant ainsi aux institutions une vision actualisée de leur position vis-à-vis des cadres de contrôle, sur des tableaux de bord interactifs Splunk.

Splunk peut ingérer les données des logiciels de supervision système et réseau tels que les solutions de gestion de l'intégrité des fichiers (FIM) qui lisent le contenu et les permissions de fichiers et créent des sommes de contrôle des fichiers statiques. Splunk peut également assimiler les données des inspecteurs de ports qui contrôlent chaque port d'une IP et indiquent lesquels répondent. En plus d'intégrer les rapports et les alertes générés par les solutions FIM et les inspections de port, Splunk compare les résultats aux données stockées précédemment et informe les administrateurs en cas de changement.

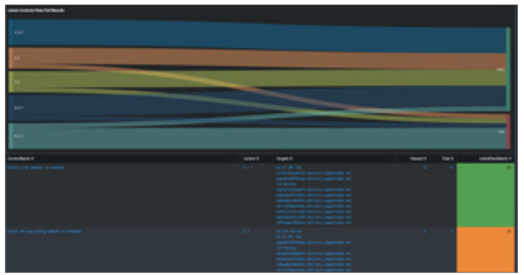
Splunk peut ensuite exploiter les résultats de plusieurs manières. Il peut envoyer des alertes par e-mail ou avertir des systèmes externes au moyen d'appels d'API. Il peut interagir avec des systèmes de tickets externes et ouvrir des tickets, ou initier des procédures d'orchestration ou d'automatisation via un produit SOAR comme Splunk Phantom pour une réponse de sécurité immédiate.

Valeur

Face aux erreurs humaines et aux problèmes de gestion des appareils, deux causes majeures des pannes informatiques, la supervision efficace des configurations revêt une importance stratégique, non seulement pour se protéger contre les attaques mais aussi pour éviter les interruptions et réduire les pertes de revenus.

Offrant la possibilité de recueillir et de visualiser les données des hôtes et des points de terminaison, mais aussi d'exécuter des scripts personnalisés sur les UF et d'autres technologies, Splunk se démarque comme étant la meilleure option pour la supervision de la conformité d'un parc informatique.

Proposant des solutions prêtes à l'emploi pour de nombreux cadres de contrôle comme celui de la PCI, ainsi que des actifs et des scripts développés par la communauté, Splunk est la plateforme idéale pour mettre en œuvre une stratégie de conformité.



Cet écran montre comment Splunk peut être utilisé pour superviser les divergences de configuration et informer un administrateur des modifications requises.

Supervision des infrastructures de bureaux virtuels

Défi

Dans un monde où le partage de postes et le télétravail sont monnaie courante, cette capacité vient simplifier les processus en permettant aux utilisateurs de se connecter depuis n'importe quel appareil, partout et à tout moment : trois aspects essentiels de tout environnement d'infrastructure de bureau virtuel (VDI). L'emploi des VDI est aujourd'hui très répandu, en particulier dans les grandes entreprises où des dizaines (voire des centaines) de milliers d'utilisateurs doivent pouvoir accéder à un ordinateur.

Mettre sur chaque bureau de chaque site un terminal lourd muni de capacités importantes de calcul, de stockage et d'applications crée de nombreuses difficultés qui rendent l'approche inefficace et en font un véritable cauchemar d'administration et d'assistance.

Les grandes entreprises tendent à privilégier les clients légers, grâce auxquels les utilisateurs peuvent se connecter à n'importe quel terminal basique pour reprendre leur travail et accéder à toutes les applications d'entreprise requises pour remplir leurs fonctions.

Les technologies de bureaux virtuels à la gestion centralisée, comme CITRIX, offrent à l'IT un degré supérieur de contrôle, de sécurité et de gestion sur un large parc d'utilisateurs, mais créent un point unique de défaillance qui accroît le risque.

Il faut donc mettre l'accent sur la santé et la sécurité de la plateforme VDI en dépit de l'incorporation de la redondance, et élaborer des plans de continuité des activités et des procédures de récupération en cas de sinistre. Le moindre problème peut entraîner une interruption du travail pour des milliers d'utilisateurs, ce qui représente une perte de productivité considérable pour les entreprises.

Les problèmes ne provoquent pas nécessairement des interruptions de service complètes, mais des dégradations de performance, des ralentissements et une mauvaise expérience utilisateur peuvent susciter du ressentiment chez les employés et une perte de productivité, et nuire à la réputation des propriétaires de la plateforme. L'IT est là pour soutenir l'entreprise et doit avant tout fournir un environnement VDI rapide et fiable aux utilisateurs.

La gestion d'un tel environnement est complexe et il faut de nombreuses couches technologiques pour faire fonctionner le service. De plus, les ressources en calcul ne sont pas infinies, ce qui fait de la supervision et de la planification des capacités un aspect crucial du bon fonctionnement du service.

La gestion des ressources d'un environnement VDI est un numéro de jonglage élaboré. L'IT doit attribuer à chaque utilisateur les ressources nécessaires à la bonne exécution du système d'exploitation invité, afin de prendre en charge les applications requises par son rôle. Parallèlement à cela, il faut éviter tout surprovisionnement, qui réduirait le nombre d'utilisateurs que la plateforme peut prendre en charge sans avoir à acquérir du matériel supplémentaire.

Une allocation excessive des ressources peut entraîner une saturation et une dégradation de l'expérience de tous les utilisateurs, mais aussi éroder toute la marge d'expansion, ce qui imposerait l'achat de nouvelles machines.

Le bon fonctionnement d'une plateforme VDI efficace repose sur plusieurs exigences clés :

- l'automatisation des contrôles de début de journée ;
- la supervision de l'utilisation ;
- la planification des capacités ;
- la supervision de l'expérience utilisateur ;
- le routage des pods ;
- le calcul ;
- le stockage ;
- la résolution des problèmes de réseau.

L'IT a besoin de voir les problèmes avant qu'ils ne se produisent, sans attendre que les utilisateurs ne prennent leur téléphone pour se plaindre de ralentissements, qui peuvent avoir des causes tout autres comme une mauvaise connexion Internet au domicile. La seule façon de répondre à ces situations consiste à produire des preuves solides, à l'aide de l'analyse des données.

L'approche de Splunk

La capacité de Splunk à recueillir et à centraliser les données de toutes les couches technologiques connectées à l'environnement VDI en temps réel assure à l'IT une visibilité complète sur la plateforme VDI et sur toutes les technologies de support.

En cas de problème, les données stockées dans Splunk peuvent être interrogées, corrélées et visualisées pour identifier rapidement la cause profonde et détecter les dégradations de performance de façon précoce. En plus, avec Splunk IT Service Intelligence, le produit Splunk pour l'AIOps, l'état de santé global des services peut être supervisé en temps réel : le machine learning (ML), la détection des anomalies et les seuils adaptatifs se conjuguent pour établir un état de référence et produire des alertes lorsque le service s'écarte du comportement attendu. Dans certains cas, le ML peut alerter à l'avance en cas de dégradation de service s'il voit des signes précurseurs dans les données, permettant aux équipes d'assistance d'agir rapidement et d'éviter des incidents qui entraîneraient une augmentation du temps moyen de résolution.

Les contrôles de début de journée peuvent être automatisés pour laisser aux équipes d'assistance la possibilité de se concentrer sur des tâches plus rentables. Les métriques d'utilisation et de capacité en temps réel permettent aux techniciens de garder une longueur d'avance sur les problèmes, notamment en assurant une distribution homogène des utilisateurs sur les pods disponibles.

Non seulement Splunk peut vous permettre de superviser l'environnement DVI réel, mais aussi les performances de l'OS invité de chaque utilisateur. En intégrant les forwarders universels à l'image de l'OS invité, on peut recueillir de nombreuses métriques qui offriront aux équipes de support une image plus détaillée encore de l'expérience utilisateur. La prochaine fois qu'un utilisateur se plaindra qu'Outlook met trop de temps à s'ouvrir, vous pourrez mener l'enquête et tirer des conclusions sur la base des preuves fournies par les données.

Valeur

Splunk apporte une visibilité et des capacités de supervision sur tout l'environnement VDI, y compris les VM invitées. Les équipes de support de VDI bénéficient ainsi d'un point unique de résolution et d'une image complète de tous les aspects de la plateforme, ce qui garantit une utilisation optimisée de la plateforme et permet de reporter, voire d'éviter, l'achat de machines supplémentaires.

MiFID II : Tests de résistance des systèmes de transaction à haute fréquence

Défi

La transparence, le signalement et la traçabilité sous-tendent de nombreuses normes techniques réglementaires (RTS) de MiFID II, comme la nécessité de conserver une trace précise des événements à des fins d'audit et de conformité. MiFID II et la réglementation des marchés d'instruments financiers (MiFIR) définissent un certain nombre d'obligations de déclarations en lien avec la divulgation des données de négociation au public et aux autorités compétentes. Le champ d'action de MiFID II comprend les classes d'actifs suivantes :

- actions ;
- obligations ;
- indices/paniers ;
- Forex ;
- taux d'intérêt ;
- matières premières.

Cette législation poursuit plusieurs objectifs fondamentaux :

- renforcer la protection des investisseurs ;
- réduire le risque d'instabilité des marchés ;
- réduire les risques systémiques ;
- augmenter l'efficacité des marchés financiers et réduire les coûts inutiles pour les participants.

Les réglementations sont conçues pour moderniser et réguler les nouvelles pratiques de négociation, notamment les transactions algorithmiques et les transactions haute fréquence, qui ont transformé le paysage boursier au cours des dernières années et rendu obsolète le précédent ensemble réglementaire. À l'heure où de plus en plus de sociétés dépendent des négociations algorithmiques, il devient impératif de démontrer sa conformité, et le meilleur moyen d'y parvenir est d'obtenir une visibilité en temps réel sur l'infrastructure sous-jacente.

Normes techniques réglementaires (RTS 6) – Tests de résistance
Dans le cadre de leur autoévaluation annuelle, les cabinets d'investissement doivent tester leurs systèmes de transactions algorithmiques ainsi que les procédures et contrôles associés pour vérifier qu'ils sont capables de supporter une augmentation du débit d'ordres ou des contraintes du marché. Ces tests doivent au minimum comprendre les éléments suivants :

- la réalisation de tests de hauts volumes de messages utilisant au moins le double de la quantité maximale de messages reçus et envoyés par l'institution au cours des six derniers mois ;
- la réalisation de tests de hauts volumes de transactions utilisant au moins le double de la quantité maximale de transactions atteinte par l'institution au cours des six derniers mois.

L'approche de Splunk

Voici quelques extraits des normes techniques réglementaires de la MiFID II qui intéressent Splunk :

- tests de résistance et gestion des capacités (les applications de négociation doivent supporter plus du double des pics de volume) ;
- supervision en temps réel des systèmes de transactions haute fréquence et de transactions algorithmiques avec génération d'alertes ;
- supervision des performances et du degré d'utilisation des éléments des systèmes de négociation en temps réel ;
- conservation des données sur cinq ans ;
- identification des transactions et ordres suspects (machine learning) ;
- protection contre les accès non autorisés à tout ou partie du système de négociation ;
- supervision de l'accès aux systèmes informatiques des cabinets d'investissement pour en assurer la traçabilité à tout moment (examen des accès privilégiés).

Splunk permet aux institutions d'exploiter leur plateforme Splunk existante pour se mettre plus rapidement en conformité avec MiFID II et d'éviter ainsi de recourir à des solutions ponctuelles ou à des logiciels développés sur mesure pour respecter des exigences réglementaires spécifiques.

Les places boursières peuvent remplir leurs obligations de déclaration aux autorités, ce qui permet d'établir une transparence avant et après les transactions.

Les capacités de conservation des données de Splunk permettent de respecter les exigences de conservation énoncées par MiFID II tout en stockant les données. Les données qui atteignent leur date de péremption sont automatiquement supprimées, évitant ainsi qu'elles soient conservées plus longtemps que ne l'exige la conformité.

Le moteur en temps réel de Splunk permet aux clients de dépasser les exigences de déclaration et d'alerte en temps réel stipulées par MiFID II et d'offrir une visibilité complète des accès autorisés et non autorisés, via les logs informatiques et d'applications. La capacité des systèmes d'échange peut être déterminée au cours de tests de résistance pour confirmer sa conformité aux réglementations édictées.

Valeur

Splunk aide ses clients à se mettre en conformité à MiFID sans acquérir ou déployer de solutions informatiques supplémentaires. L'évolutivité de Splunk et ses nombreuses capacités avec supervision en temps réel s'étendent à l'analyse des données, la production de rapports, au machine learning, à la génération d'alertes et à la supervision de données utiles pour pertinents pour MiFID II.

Opérations transfrontalières internationales

Défi

Des institutions de services financiers qui opèrent dans le monde entier le font sous une chape d'exigences réglementaires qui les soumettent à des lois différentes dans chaque juridiction. Des pays comme la Suisse, Singapour et le Brésil appliquent des lois strictes pour protéger les données qui quittent leurs frontières. Les banques désignent souvent ces régions comme « zones restreintes », ce qui signifie que seuls les employés situés dans la zone en question peuvent accéder aux données stockées dans celle-ci.

Les institutions qui cherchent à normaliser leur gestion des données sur l'ensemble de leurs opérations peuvent avoir des difficultés à élaborer des solutions pour garantir la confidentialité dans ces zones restreintes et l'ouverture dans les autres régions.

L'approche de Splunk

Grâce à sa capacité à prendre en charge une architecture de données très évolutive et distribuée, Splunk permet aux institutions de respecter les obligations d'accès transfrontalier, en veillant à ce que les données générées dans ces zones puissent être conservées au point d'origine pour respecter les exigences réglementaires de chaque juridiction.

Un utilisateur domicilié dans une zone restreinte aura accès aux données de cette zone mais aussi à celles des autres régions, dans la mesure des prérogatives de son rôle. Un utilisateur qui se trouve dans une zone interdite ne pourra pas accéder aux données qui se trouvent dans une autre zone interdite.

Dans les zones ouvertes, les données peuvent être consolidées au sein d'un même cluster Splunk d'entreprise, permettant aux institutions d'interroger leur jeu de données global depuis un même point, en excluant les données situées dans des régions protégées.

Grâce aux fonctionnalités de niveau entreprise de Splunk, les institutions peuvent personnaliser et déployer Splunk pour satisfaire leurs propres exigences de confidentialité des données sans développement personnalisé, et ce grâce à la quantité quasi-illimitée de topologies de déploiement disponibles.

Outre la mise en place de partitions physiques dans l'architecture de Splunk et la séparation des zones restreintes et ouvertes, Splunk peut aussi détecter et signaler les tentatives d'accès transfrontalier à la direction.

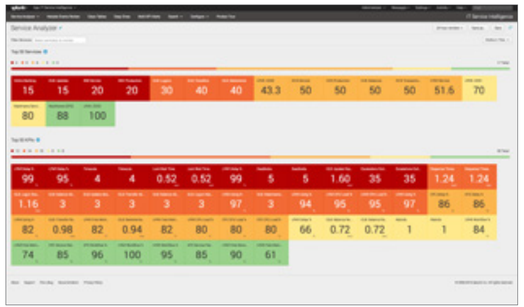
Splunk peut ingérer les données de connexion d'Active Directory, les données réseau et les données RH pour mettre en évidence les utilisateurs qui se connectent aux systèmes depuis un autre pays que celui où ils sont domiciliés. Les visualisations cartographiques de Splunk facilitent l'identification des accès transfrontaliers et le signalement des personnes qui tentent d'accéder à un système ou à des données situés dans une zone protégée depuis l'extérieur, ce qui peut être le signe d'une violation de conformité.

Les données de connexion peuvent être visualisées sur une carte et corrélées avec l'emplacement des bureaux pour révéler les connexions provenant de pays où l'entreprise n'est pas implantée, potentiellement symptomatiques d'activité illicite ou de tentative de piratage.

Valeur

Splunk fait en sorte que les entreprises puissent déployer la bonne architecture globale dès le départ, en intégrant la séparation des données dès la conception et en apportant aux autorités de régulation la preuve que l'architecture est conforme aux règles et réglementations relatives à la confidentialité des données et à leur circulation transfrontalière.

La capacité de Splunk à détecter les accès transfrontaliers et les tentatives de piratage dote les équipes de sécurité d'une visibilité complète sur ces connexions suspectes, renforçant ainsi la position globale de sécurité et de conformité de l'institution.



Splunk fait en sorte que les entreprises puissent déployer la bonne architecture globale dès le départ, en intégrant la ségrégation des données dès la conception et en apportant aux autorités de régulation la preuve que l'architecture est conforme aux règles et réglementations sur la confidentialité des données et leur circulation transfrontalière.

Criminalité financière

Défi

La criminalité financière est en hausse, et elle gagne en complexité et en sophistication. En période de difficultés économiques, le volume d'attaques augmente et les techniques utilisées évoluent. Les équipes de lutte contre la criminalité financière doivent avoir des compétences diversifiées, couvrant aussi bien l'investigation des fraudes traditionnelle que les sciences des données et l'analyse commerciale. Les équipes de données doivent adopter une approche agile ; elles doivent pouvoir combiner des techniques d'analyse sophistiquées et un portefeuille de sources de données variées aux compétences et à l'expertise nécessaires pour les exploiter.

Les institutions bancaires sont confrontées à un large spectre de défis : fraude distribuée, personnel de sécurité, applications et données en silos, outils et systèmes de lutte anti-fraude obsolètes, et un large éventail de types de données structurées et non structurées difficiles à comparer et à analyser.

Lorsqu'elles mettent en place de nouveaux produits, ceux-ci sont souvent vulnérables à des formes inédites de criminalité financière : les institutions doivent donc se tenir prêtes et s'adapter à l'évolution de ces menaces en temps réel. Les criminels professionnels ont également recours aux données et au machine learning pour affiner leurs attaques et amplifier leur rayon d'action. Si l'on observe toujours des attaques par force brute à l'ancienne, les malfaiteurs se montrent de plus en plus sophistiqués et les institutions doivent être prêtes à faire face.

L'approche de Splunk

La spécialité de Splunk réside dans les aspects de données et d'analyse de la criminalité financière, et de nombreuses grandes institutions s'appuient sur Splunk pour relever divers défis, de la fraude transactionnelle au blanchiment d'argent, en passant par les déclarations de conformité. Les institutions les plus sophistiquées utilisent Splunk pour abattre les silos qui isolent les différentes disciplines et partager les données. Splunk est utilisé comme une plateforme de données unique couvrant tous les types de criminalité financière, ainsi que les rapports de conformité et les enquêtes également indispensables.

Historiquement, les institutions ont organisé leurs opérations de lutte contre la criminalité financière en silos qui traitent chacun de ses aspects. Dans bien des cas, les personnes, les processus, les données et le financement ont des origines différentes. Ce n'est pas seulement inefficace sur le plan financier, cela signifie également que chaque équipe est privée de la possibilité d'analyser les informations dans le contexte des autres processus. En conséquence, ces équipes prennent souvent des décisions basées sur des données parcellaires, et qui pourraient être bien plus complètes si la collaboration avec d'autres équipes était possible.

Les institutions peuvent extraire une valeur importante en incluant les données de comportements humains, comme les registres d'activité des sites web, des applications mobiles, des applications d'entreprise internes et des accès aux systèmes. Ces systèmes contiennent d'infimes indices qui peuvent délivrer des informations utiles sur un système ou une équipe au cours d'une investigation. Des chiffres tels que le nombre de fois qu'une personne n'a pas réussi à se connecter au système ne sont pas inclus dans la transaction mais sont enfouis dans les fichiers de log des sites web, et ils peuvent apporter le contexte requis pour confirmer la probabilité d'une transaction suspecte.

La criminalité financière peut prendre de nombreuses formes :

- fraude sur les transactions ;
- blanchiment d'argent ;
- respect des sanctions ;
- financement du terrorisme ;
- trafic d'êtres humains ;
- fraude sur les applications ;
- menaces internes ;
- appropriation de compte ;
- détection de mot de passe ;
- compromission du courrier électronique d'entreprise ;
- comptes mules ;
- vol d'identité, identités synthétiques ;
- fraude/erreurs de saisie des dépôts distants ;
- détection des dispositifs d'espionnage des DAB ;
- logiciels malveillants ;
- fraude sur les sites web et applications mobiles ;
- exfiltration de données en centre de contact ;
- détection de robots ;
- télémétrie des dispositifs ;
- parcours numérique.

Les sites et applications mobiles de banque en ligne présentent souvent les plus grands défis. Les sites web sont généralement supervisés en analysant les logs http produits par le serveur web. Ces logs sont détaillés et contiennent une quantité importante de texte superflu (la ventilation numérique), souvent considéré comme ayant une valeur faible voire nulle. Dans cette ventilation numérique se trouvent pourtant des pépites d'informations très précieuses qui (lorsqu'elles sont extraites) peuvent fournir des informations cruciales.

Le problème est que ces logs ne sont pas bien structurés et varient à chaque fois qu'un utilisateur emprunte un autre chemin dans le site web. Tenter de modéliser cette trajectoire à l'aide d'une technologie de base de données est (quasiment) impossible.

Splunk a été conçu pour gérer cette complexité : la plateforme est capable d'importer les logs de milliers de systèmes en temps réel et de corréler les points de données pertinents nichés dans les différents logs. Elle peut extraire ces points de données au moment voulu et fournir la structure dont les entreprises ont besoin pour analyser leurs données.

Valeur

Les institutions financières doivent prendre en compte de nombreux facteurs pour traiter la criminalité financière et la structure de l'organisation est l'un des plus importants. Les institutions ont de nombreux avantages à rassembler les équipes, à partager les ressources, les données et les outils, et surtout à œuvrer ensemble à l'élaboration des processus et des systèmes de supervision des transactions. Cela permettrait également de disposer de normes communes de travail, de définir des références pour le calcul des scores de risque des transactions associées à certains types courants de fraude, et de créer des réglementations pour lutter contre le blanchiment d'argent, le non-respect des sanctions et les menaces internes.

Les institutions ont beaucoup à gagner en rassemblant les données structurées des transactions, des clients et des employés, et les données non structurées des systèmes utiles comme les sites web et les plateformes de banque en ligne et d'authentification/sécurité. Les données non structurées peuvent apporter aux transactions un contexte important qui serait autrement perdu. Splunk est le moteur qui réunit ces mondes séparés et donne aux institutions financières l'avantage sur les acteurs malveillants.

Splunk aide les sociétés à appliquer des fonctions de modélisation pondérée selon le risque à leur lutte contre la criminalité financière.

Sécurité des services financiers

Défi

La sécurité est une problématique qui concerne les plus hauts niveaux de direction dans l'industrie des services financiers. Les institutions qui subissent une faille de sécurité peuvent rapidement faire la une des journaux et les enjeux sont graves.

La sécurisation d'une institution financière est l'une des tâches les plus complexes qui puisse incomber aux professionnels de sécurité, et ce à cause de multiples facteurs :

- les structures complexes des organisations et des opérations internationales ;
- la large gamme de produits très divers et la nécessité de prendre en charge des produits obsolètes pendant des années ;
- le grand nombre de clients et d'employés ;
- les points d'accès nombreux et diversifiés pour les clients et les employés ;
- les multiples réseaux, notamment des réseaux privés à haute vitesse ;
- de nombreuses contreparties et des relations avec des organismes tiers (réseaux de paiement, places boursières, fournisseurs de données) ;
- la réglementation stricte et multiples autorités de régulation ;
- les attaques quasiment constantes ;
- les réseaux sociaux.

Ce sont surtout les banques qui ont le plus à perdre. Les braquages d'agences bancaires sont aujourd'hui moins fréquents, mais les cyberattaques augmentent, tout comme leur sophistication.

L'approche de Splunk

Les institutions financières utilisent souvent Splunk comme centre névralgique de leur SOC. Splunk propose une plateforme de produits de sécurité qui permet à une institution de mener une large gamme d'activités : capture de données en temps réel, détection avancée, informations sur les menaces, mais aussi orchestration, automatisation et réponse. Les produits Splunk comme Enterprise Security et Phantom sont armés de centaines de scénarios prédéfinis pour permettre à une société de déployer rapidement son SOC et de le rendre opérationnel en un minimum de temps.

Les grandes forces de Splunk proviennent de sa flexibilité : la plateforme peut établir des corrélations entre des milliers de sources de données en temps réel tout en conservant la possibilité de réagir à un nouveau type d'attaque sans préavis. Le langage de recherche (SPL) de Splunk permet de créer de nouvelles recherches en quelques instants pour conserver une flexibilité exceptionnelle au cours d'une enquête et produire des résultats rapidement, même face aux scénarios les plus complexes.

Splunk est utilisé par les organisations les plus variées, de l'Aflac à la FINRA en passant par la Banque d'Angleterre. Leurs modèles commerciaux sont tous différents et leurs organisations varient considérablement, mais elles parviennent toutes à respecter leurs exigences de sécurité grâce à la flexibilité de la plateforme Splunk.

Valeur

Il est difficile de quantifier en termes monétaires la valeur dès l'arrêt d'une attaque avant son évolution en incident, mais il s'agit là clairement d'un précieux atout pour toute entreprise.

Dans un environnement de sécurité, il est nécessaire de se munir de plusieurs outils et services, car la solution unique et ultime n'existe pas. Splunk joue le rôle de centre névralgique des opérations de sécurité : il est capable de réunir les données de tous les systèmes et de superviser l'ensemble de l'infrastructure et des opérations en temps réel. Splunk Phantom gère l'orchestration et l'automatisation des événements de sécurité ; c'est lui qui veille à ce que les problèmes critiques soient rapidement pris en charge.

Les tableaux de bord de position de sécurité agrègent et hiérarchisent les événements notables de tout l'écosystème de vos outils de sécurité pour aider les analystes à réagir en disposant de tout le contexte nécessaire, ou pour automatiser les réponses dans les situations qui le permettent.

Les opérations de sécurité efficaces présentent de véritables avantages : elles permettent de réagir rapidement et de minimiser le temps passé à pourchasser les faux positifs. Splunk permet de gérer ces opérations tout en maintenant d'excellents niveaux de service.

« Splunk Phantom apporte de la précision et de la cohérence au processus de réponse aux incidents. Auparavant, face aux volumes d'alertes croissants, les analystes étaient rapidement submergés d'informations, ce qui les poussait souvent à ignorer des indices essentiels. De même, des analystes expérimentés pouvaient être tentés de "suivre leur intuition" basée sur de précédents incidents et des informations incomplètes. Avec une procédure Phantom, les mêmes données sont collectées pour chaque alerte, et chaque alerte est systématiquement étudiée et mémorisée de la même façon. L'automatisation de la réponse aux incidents avec Phantom a eu de nombreuses conséquences positives chez Blackstone et a permis à l'équipe de consacrer moins de temps à des tâches fastidieuses et répétitives, d'enquêter plus rapidement sur les problèmes et d'améliorer la cohérence pour des résultats plus rapides et précis. »

En savoir plus sur Splunk chez Blackstone.

SÉCURITÉ ET DÉLITS FINANCIERS

Fraude liée aux cartes de crédit et de débit : détection et résolution

Défi

La fraude internationale liée aux cartes de crédit est passée d'une moyenne de 4,78 centimes pour 100 $ en 2006 à 7,2 centimes pour 100 $ aujourd'hui, une augmentation significative sur 12 ans, alimentée par l'accroissement des paiements par carte et les transactions sans présence de carte (CNP). Les États-Unis enregistraient 40 % de la fraude mondiale en 2016, alors qu'ils sont seulement à l'origine de 24 % des transactions par carte.

Les fraudeurs qui utilisent ce support emploient un large éventail de techniques pour obtenir des informations personnelles : appels téléphoniques malveillants, e-mails et sites web d'hameçonnage et faux points d'accès Wi-Fi.

Le « skimming », une méthode courante, consiste à placer un lecteur de carte discret sur un DAB ou une caisse de point de vente pour copier les informations de la carte à l'insu des clients qui viennent retirer de l'argent. Les informations sont ensuite récupérées et utilisées pour faire des achats, ou alors revendues sur le marché noir.

La technologie de paiement sans contact facilite le quotidien des consommateurs mais a entraîné une augmentation des délits car les fraudeurs cherchent à exploiter les nouvelles fonctionnalités des cartes.

Les fraudeurs peuvent se procurer des lecteurs RFID (identification par radio-fréquence) qu'il suffit d'approcher d'une carte pour en obtenir les informations. De même, la technologie NFC (communication en champ proche) permet de partager des informations de carte de paiement avec un système de point de vente. Apple Pay, Google Wallet, Visa et d'autres applications similaires utilisent cette technologie de paiement. Les lecteurs NFC compromis risquent de transmettre des informations de carte de crédit à un criminel.

Une fois les informations de la carte et d'autres détails personnels obtenus, le fraudeur peut alors manipuler des produits financiers en utilisant une application.

L'approche de Splunk

Les données et l'analyse en temps réel à l'aide du machine learning comptent parmi les outils les plus puissants dans la lutte contre la fraude. Elles permettent en effet d'observer les comportements suspects et d'agir en conséquence. Voici quelques exemples de scénarios de fraude fréquemment pris en charge dans Splunk.

Fraude externe :

- Retraits quasi-simultanés sur le même compte à deux DAB ou plus situés dans des régions distantes
- Compte présentant des retraits quotidiens dépassant les limites normales
- Transfert d'une somme anormalement élevée ou grand nombre de transactions par rapport aux normales de référence
- Transferts bancaires vers des pays/régions à haut risque ou des institutions financières liées à la fraude
- Multiplication de petits paiements depuis un compte pendant plusieurs jours consécutifs

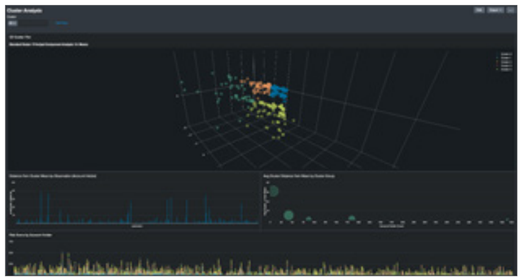
Fraude interne :

- Agents bancaires effectuant des transactions en dehors des heures normales ou traitant leurs propres transactions
- Personnel informatique et développeurs se connectant à une application pour effectuer des transactions
- Trader utilisant des identifiants différents de ceux du propriétaire de la machine physique

Valeur

Certains cas de fraude nécessitent des données récentes pour être détectés. Il est ainsi possible de repérer les cartes clonées en détectant des retraits successifs rapides sur des DAB distants géographiquement. Cette attaque est souvent surnommée « attaque Superman » car il serait impossible pour un être humain de voyager d'un DAB à l'autre dans le délai requis pour faire ces multiples retraits.

D'autres scénarios d'utilisation requièrent de grandes quantités de données historiques pour créer des profils de référence du comportement des possesseurs de carte. Par exemple, les montants moyens minimum et maximum de transactions par jour permettent de détecter les écarts et les anomalies.



L'utilisation du machine learning contribue à l'identification des activités potentiellement frauduleuses en délivrant une vue en quasi-temps réel de la position de fraude pour hiérarchiser les investigations et automatiser d'autres actions de remédiation.

Splunk peut évoluer pour analyser des pétaoctets de données chaque jour, ce qui permet aux prestataires de paiement de mettre en place une détection avancée de la fraude et de générer des alertes en temps réel. Splunk Phantom permet ainsi d'automatiser des procédures qui agissent sans intervention de l'utilisateur en cas de détection de fraude : il peut par exemple annuler une carte de crédit et en initier une nouvelle.

La plupart des banques offrent une protection contre la fraude dans le cadre de leurs services. Si un possesseur de carte est victime d'une fraude et qu'il n'a pas fait preuve de négligence, la banque rembourse ses pertes : l'identification rapide de la fraude a donc un impact direct sur la rentabilité.

« PostFinance utilise Splunk comme plateforme de gestion de la fraude et exploite les renseignements pour protéger les comptes bancaires et les paiements numériques de ses clients. Son portail bancaire en ligne compte à lui seul 1,6 millions de clients à protéger. L'équipe PostFinance ne se contente pas de détecter et d'identifier les nouveaux patterns de fraude avec Splunk, elle opérationnalise également son workflow, ce qui lui permet de transmettre les signalements aux autorités en fournissant toutes les informations nécessaires. »

En savoir plus sur Splunk chez PostFinance.

SÉCURITÉ ET DÉLITS FINANCIERS

Détection des menaces internes

Défi

Un trader malhonnête peut agir de façon indépendante, souvent avec témérité, en poursuivant des stratégies à haut risque/bénéfice et en contournant les contrôles internes. Au fil des ans, les banques ont mis au point des modèles de risque sophistiqués pour contrôler la négociation des instruments ; ces contrôles internes ne sont toutefois pas infaillibles. Un trader déterminé peut trouver un moyen de contourner le système pour accroître ses gains.

Les banques cherchent à consolider leurs fonctions de conformité et de contrôle des risques opérationnels en élaborant et en développant des systèmes complexes d'informations sur les salariés afin de superviser leurs comportements et d'identifier proactivement les menaces internes potentielles pour l'institution. Ces systèmes offrent une vision holistique et permettent de superviser les salariés pour détecter et prévenir les activités illicites, les fuites de données et la fraude à l'aide d'analyses avancées et de capacités de machine learning.

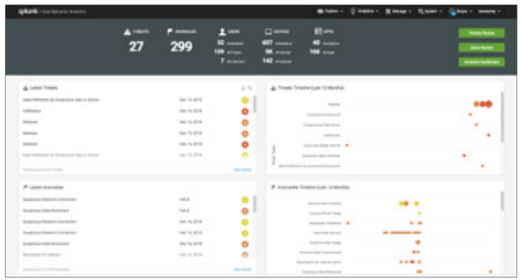
L'identification des domaines ou des salariés à risque grâce à l'analyse permet aux banques de prendre des mesures préventives (initiatives de formation et de sensibilisation, modification des contrôles internes, introduction de nouvelles règles et procédures, voire application de mesures disciplinaires dans les cas extrêmes) pour préserver l'intégrité, favoriser la responsabilisation et prévenir la fraude, toujours pour réduire le risque.

L'approche de Splunk

Chaque entreprise développe ses propres critères pour identifier les menaces internes ou les salariés à risque et détecter les conduites illégales. Il faut au départ procéder avec des règles rudimentaires puis progresser vers des scénarios d'utilisation plus complexes au fil du temps en intégrant des techniques comme l'analyse des groupes de pairs. Les clients qui ont mis en place Splunk et y ont intégré les flux de données associés aux opérations IT et à la sécurité vont pouvoir exploiter ces données pour mettre sur pied, dans des délais très courts, des dispositifs de supervision des employés. Ils vont ainsi exploiter leurs investissements existants et réduire le temps nécessaire à l'acquisition des données, ce qui renforce leur position de conformité.

Splunk permet aux clients d'élaborer des tableaux de bord personnalisés pour superviser les salariés. Splunk Enterprise Security contient des tableaux de bord prédéfinis qui offrent de la visibilité sur les activités courantes indicatrices de comportement à risque. Splunk User Behavior Analytics (UBA), avec ses capacités de détection des menaces avancées, découvre les anomalies et les menaces inconnues ignorées par les outils de sécurité traditionnels, en utilisant des capacités d'investigation approfondie et de puissantes références comportementales pour évaluer n'importe quelle entité, anomalie ou menace.

Les banques sont tenues d'imposer une période de congé continu à chaque salarié chaque année pour permettre la découverte d'éventuelles fraudes ou arrangements illicites. En établissant des corrélations entre les données de connexion aux systèmes IT, les données d'accès aux bâtiments et les données RH, les banques peuvent déterminer si des employés ont accédé aux systèmes et aux locaux pendant cette période, enfreignant ainsi leur congé.



Automatisez la détection des menaces avec le machine learning pour consacrer plus de temps à l'étude des alertes comportementales de haute fiabilité et apporter une réponse rapide.

Valeur

En exploitant la plateforme Splunk, les banques peuvent analyser de nombreux scénarios de comportement d'employés pour détecter les comportements anormaux à l'aide de multiples techniques statistiques et de machine learning :

- la détection des logiciels malveillants : signale les employés qui accèdent à des sites dangereux ;
- les comptes fréquemment verrouillés ;
- les utilisateurs affichant un trafic web important et des transferts et téléchargements volumineux ;
- les utilisateurs ayant une activité e-mail hors entreprise ;
- les utilisateurs se connectant successivement depuis des lieux très distants dans le même laps de temps ;
- analyse du comportement de fraudeurs connus en vue de faciliter la reconnaissance préventive de futurs fraudeurs ;
- l'utilisation des cartes de crédit d'entreprise jusqu'au plafond ;
- les factures téléphoniques inhabituelles par rapport aux collègues ;
- les accès pendant le congé imposé.

« Splunk a eu de nombreuses répercussions positives sur notre activité. Nous avons considérablement gagné en efficacité : nos analystes ont accéléré les investigations de plus de 50 %. Splunk UBA nous donne à tout moment des informations approfondies sur les menaces internes au NASDAQ et sur l'activité de nos utilisateurs de confiance. »

— AVP, NASDAQ

En savoir plus sur Splunk chez NASDAQ.

SÉCURITÉ ET DÉLITS FINANCIERS

Exfiltration des données

Défi

L'exfiltration des données désigne le transfert non autorisé de données d'une entreprise. C'est souvent l'une des dernières étapes d'une cyberattaque. L'un des aspects les plus ardus de l'exfiltration des données tient au fait qu'elle peut se faire de multiples façons : scripts automatisés, chiffrement des données, protocoles réseau, données tronquées et exfiltration physique. Il devient donc très difficile de savoir comment réduire cette menace.

Pour les institutions de services financiers, l'exfiltration des données représente un défi important en raison d'architectures IT de plus en plus ouvertes, l'adoption croissante de technologies centrées sur le client et la complexité des systèmes IT hérités. Bien que ces nouveaux défis renforcent l'opportunité de masquer les tunnels de données, ils permettent aussi aux exfiltrations d'avoir lieu au vu et au su de tous.

Pour les institutions financières, l'exfiltration des données peut avoir un grave impact sur leur position financière et leur réputation. La faille d'Equifax en septembre 2017 a entraîné l'exfiltration d'informations personnellement identifiables (IPI) concernant 148 millions de personnes. Au cours de cette cyberattaque de 76 jours, les auteurs de l'attaque ont exploité plus de 9 000 requêtes non détectées pour accéder à une base de données non chiffrées contenant des IPI. Selon les rapports, le coût total pour Equifax a dépassé les 275 millions de dollars, auxquels s'ajoutent 200 millions de dollars de dépenses en infrastructure de sécurité.

L'approche de Splunk

Notre approche de la détection et de la prise en charge des exfiltrations de données se base sur une analyse efficace de la sécurité. Splunk permet aux entreprises de déployer tout un éventail d'approches axées sur les données pour détecter et prendre en charge les tentatives d'exfiltration des données. Une première étape judicieuse consiste à déterminer la localisation et la nature plus ou moins critique des données que vous détenez, ainsi que les moyens d'y accéder.

Une fois cela connu, la plateforme d'analyse Splunk Enterprise et ses applications de sécurité peuvent détecter et prendre en charge les indicateurs d'exfiltration. Cela peut aller de la détection des patterns anormaux du trafic réseau à l'utilisation d'algorithmes de machine learning avancés pour identifier les comportements inconnus ou suspects. Vous pouvez également automatiser les workflows d'investigation et de réponse pour réduire les délais de détection et de réaction, ainsi que le temps de maintien global de l'attaque.

Grâce à l'analyse prescriptive, Splunk prend également en charge de nombreuses normes industrielles comme le framework MITRE ATT&CK et la Cyber Kill Chain, qui permettent toutes deux aux institutions financières d'adopter une approche encadrée dans l'élaboration de leur stratégie de réduction des risques. Les institutions financières doivent développer ces techniques en les alliant à de bonnes pratiques de sécurité comme la maintenance opérationnelle et la gestion des correctifs des systèmes informatiques, ainsi qu'à des mesures efficaces telles que le chiffrement des données et le contrôle des accès.

Valeur

Prévenir les exfiltrations de données a de nombreux avantages :

- la protection de la propriété intellectuelle et des secrets industriels ;
- la protection des données personnelles, notamment des informations couvertes par le RGPD et la loi de Californie sur la Protection du consommateur ;
- la protection de la marque et de la réputation ;
- la réduction des risques d'amendes et de pénalités ;
- une compétitivité accrue.

SÉCURITÉ ET DÉLITS FINANCIERS

Attaques ciblées avancées

Défi

Les attaques ciblées avancées (ATA) et les menaces avancées telles que les menaces persistantes avancées (APT) font partie des plus grands risques encourus par les systèmes d'entreprise. Ces menaces, généralement exécutées par des États mal intentionnés, sont caractérisées par un long cycle de vie et un impact potentiellement dévastateur.

Les hackers peuvent infiltrer le réseau sans être détectés pendant des semaines, des mois voire des années, collecter silencieusement des informations sur leur cible avant de finir par exploiter les vulnérabilités identifiées.

Lors de l'attaque tristement célèbre de la Banque du Bangladesh, les pirates ont transféré 81 millions de dollars vers des comptes aux Philippines et au Sri Lanka, devenant l'un des plus grands braquages numériques de notre époque.

Au cours de cet assaut, les agresseurs ont utilisé le réseau SWIFT pour effectuer les transferts de fonds. Une fois qu'ils ont eu accès au réseau, ils ont installé des logiciels malveillants conçus pour dissimuler toute trace des paiements frauduleux des bases de données locales de la banque.

Impact

Risque financier :
Ces cyberattaques ont un impact financier net et évident, car les malfaiteurs exploitent les vulnérabilités dans le but d'en tirer un gain financier considérable. Lors de l'attaque de la Banque du Bangladesh, les pirates ne sont parvenus à voler que 81 millions de dollars à cause d'une faute de frappe dans l'instruction de transfert contrefaite, qui a empêché l'extraction des 900 millions de dollars restants. Une fois qu'une somme a été transférée par SWIFT, tout trajet retour est normalement impossible.

Risque pour la réputation :
Le risque pour la réputation a un impact plus grave encore sur l'entreprise que la perte financière. Si une entreprise se fait une réputation de négligence en matière de contrôles de sécurité à la suite d'une faille, elle perdra vraisemblablement la confiance indispensable de ses actionnaires comme de ses clients.

L'approche de Splunk

Splunk propose une suite complète pour les opérations de sécurité qui prend en charge tout le cycle de vie de la sécurité, de l'exploration des menaces à la supervision, l'analyse et l'orchestration. En ingérant à la fois les données machine et tout type de données structurées, les comportements anormaux peuvent être détectés en identifiant les corrélations entre des données connexes.

Par exemple, les flux de données réseau peuvent être corrélés aux transactions en temps réel et aux données structurées de clients et de comptes pour obtenir une visibilité complète sur tout le profil de l'entreprise. Les données de points de terminaison peuvent également être supervisées, pour vérifier si un processus anormal est exécuté sur le système SWIFT après qu'un utilisateur a accédé à un compte à une heure inhabituelle.

Ces capacités sont associées aux « Mises à jour de contenu » du produit Enterprise Security (ES) de Splunk, un ensemble de recherches de corrélation mis au point par des chercheurs et envoyé chaque mois à tous les utilisateurs d'ES. Dès la détection d'un problème, Splunk Phantom agit automatiquement pour orchestrer l'environnement et se connecte à plus de 260 technologies tierces pour agir en temps réel.

Enfin, l'outil User Behaviour Analytics (analyse du comportement des utilisateurs) exploite des modèles de machine learning (ML) pour détecter les menaces internes, une capacité cruciale dans un scénario ATA.

La supervision des URL malveillantes compte parmi les nombreux outils de défense et de contrôle dans un environnement de sécurité.

SÉCURITÉ ET DÉLITS FINANCIERS

Hameçonnage

Défi

L'hameçonnage reste le principal vecteur de menace des cyberattaques, en partie parce que l'exploitation des vulnérabilités humaines est l'un des moyens les plus efficaces d'atteindre une entreprise ou un individu. En 2018, les attaques par hameçonnage traditionnel ont ainsi augmenté de 12 % pour représenter 47 % de l'ensemble des types d'attaques détectées.

Dans une attaque par hameçonnage, l'agresseur emploie diverses techniques d'ingénierie sociale pour effectuer un vol d'identité. L'hameçonnage s'effectue généralement en envoyant un message factice (e-mail, message privé ou message de réseau social) imitant ceux des sites de banque et de paiement en ligne. Le message redirige l'utilisateur vers une page web trompeuse, soigneusement conçue pour ressembler à la page de connexion d'un site légitime. Les pirates tentent ensuite de recueillir des informations sensibles et personnelles (noms d'utilisateur, mots de passe, numéros de carte de crédit, etc.) et même de l'argent en usurpant l'identité d'une entité légitime dans le cyberespace.

Une attaque par hameçonnage présente trois grandes caractéristiques : 1) l'identité d'une entreprise légitime est usurpée ; 2) le processus d'usurpation doit impliquer un site web, ce qui le distingue d'autres formes d'escroquerie (le transfert de fonds illégaux, par exemple) ; 3) le but est l'obtention d'informations sensibles sur l'entreprise.

Une variante, l'hameçonnage ciblé, vise des profils spécifiques d'une entreprise en leur envoyant des messages extrêmement personnalisés. Ce type d'attaque est de plus en plus répandu et il est associé aux plus grandes cyberattaques de l'histoire récente, visant notamment JPMorgan Chase & Co., eBay, Target, Anthem, Sony et plusieurs administrations américaines.

Impact

Les attaques par hameçonnage ont de graves conséquences pour les victimes. Plus que toutes autres, elles coûtent extrêmement cher aux entreprises. Selon le Rapport 2019 d'Accenture et Ponemon sur le coût de la cybercriminalité, ce type de délit coûte en moyenne aux banques 16,55 millions de dollars par an de pertes, et le coût annuel moyen d'une attaque d'hameçonnage est passé de 1,3 million de dollars en 2017 à 1,4 millions de dollars en 2018.

Il n'est donc pas surprenant que plus de 80 % des entreprises victimes d'une attaque par hameçonnage ciblé déclarent avoir subi des dommages et pertes considérables. Les dommages les plus importants concernent la productivité des employés (41 %), les pertes financières (32 %), la réputation de la société (29 %), la réputation de la marque (27 %), les clients (25 %) et la propriété intellectuelle (25 %). De plus, à la suite de ces attaques, certaines entreprises ont observé une baisse du cours de leur action allant jusqu'à 15 %.

Ces attaques se produisent régulièrement et ne font qu'augmenter. Dans une enquête de Cloudmark sur l'hameçonnage ciblé, environ 70 % des participants ont indiqué que leur entreprise mettait en œuvre une solution spécifique pour éviter ce type d'attaque, soit un investissement moyen de 319 327 $ au cours des 12 derniers mois ; toutefois, ils sont 84 % à estimer que les auteurs d'hameçonnage ciblé avaient réussi à pénétrer dans la solution de sécurité de leur entreprise.

Les attaques par hameçonnage vont maintenant de plus en plus cibler les appareils mobiles. Depuis 2015, les attaques par hameçonnage sur mobile ont augmenté de 680 %, et une sur cinq est effectuée par le biais d'applications mobiles. On ne sera donc pas surpris d'apprendre que 82 applications malveillantes sont publiées chaque jour sur les boutiques d'applications mobiles selon RSA.

Ces attaques mobiles prennent la forme du « smishing », qui utilise les SMS plutôt que l'e-mail, de l'hameçonnage par 2FA mobile, une variante du smishing qui consiste à contourner l'authentification à deux facteurs, et les logiciels mobiles malveillants qui exploitent les vulnérabilités des OS mobiles pour prendre le contrôle de l'appareil d'un utilisateur. Que ce soit par e-mail, réseau social ou appareil mobile, l'hameçonnage fonctionne et il n'y a pas de raison qu'il disparaisse sous peu.

L'approche de Splunk

De nombreuses institutions ont déjà mis en œuvre des solutions pour lutter contre les incidents liés à l'hameçonnage. Les solutions habituelles de détection et de correction permettent aux clients de contrôler, d'assainir et d'éliminer les logiciels malveillants d'un e-mail, un processus qui prend normalement entre 30 minutes et six heures. C'est là que l'automatisation intervient : elle peut réduire ces durées à moins d'une minute.

Splunk Phantom, la plateforme leader de sécurité, d'orchestration, d'automatisation et de réponse (SOAR), fournit une plateforme d'orchestration et d'automatisation visant à réduire la durée d'une enquête d'hameçonnage à quelques secondes. Plus précisément, Phantom permet de créer des workflows automatisés qui génèrent des actions, des décisions et des interactions avec les analystes, en impliquant différentes technologies. Cette automatisation invoque ensuite des commandes d'API et les orchestre pour éviter à l'analyste de manipuler lui-même les outils. Phantom propose de loin la plus grande bibliothèque d'applications (plus de 250 intégrations), et de nouvelles applications sont créées pratiquement toutes les semaines.

La plateforme Splunk et Phantom coopèrent de façon parfaitement fluide : l'application Phantom pour Splunk permet une intégration bidirectionnelle des deux solutions pour que les utilisateurs puissent, entre autres, initier des recherches et des requêtes ou ingérer des événements. Il devient alors possible d'enrichir l'initiation des workflows des investigations existantes, et inversement. Pour aider les équipes de sécurité à visualiser leur travail, Splunk puise dans la base de données Phantom pour produire des rapports et des tableaux de bord complexes à partir des données d'une entreprise.

En réduisant la durée de ces enquêtes à moins d'une minute pour un e-mail, nous aidons les entreprises à réduire leur effort et nous leur donnons les moyens d'agir sur le moindre élément malveillant. Nous les aidons ainsi à réduire le temps, les efforts et les coûts associés à ces opérations tout en garantissant la satisfaction et les performances de leur équipe de sécurité.

SÉCURITÉ ET DÉLITS FINANCIERS

Mesures contre le blanchiment d'argent

Défi

Le Fonds monétaire international (FMI) estime que le blanchiment d'argent représente entre 2 et 5 % du PIB mondial, soit entre 800 et 2 000 milliards de dollars, dont 1 % seulement est saisi par les autorités en raison de l'obsolescence des systèmes de lutte contre le blanchiment.

De nombreuses institutions de services financiers fonctionnent de façon décentralisée et n'ont pas évalué les risques face au blanchiment d'argent sur leur portefeuille global, laissant ainsi subsister des failles où peuvent se glisser des activités illégales.

Nous avons récemment observé des banques poursuivies et sanctionnées par de lourdes amendes chiffrées en centaines de millions de dollars pour défaut d'investigation et de signalement de transactions suspectes, et pour l'insuffisance de leurs procédures de contrôle et de vérification de leurs clients.

Ce qui accroît la difficulté, ce sont les technologies datées et les systèmes de lutte obsolètes qui ne parviennent pas à couvrir une entreprise internationale et produisent un fort taux de faux positifs qui handicapent leur usage. Le Groupe d'action financière (FATF) affirme que les institutions financières devraient être tenues de conserver pendant au moins cinq ans tous les registres nécessaires de transactions nationales et internationales pour leur permettre de répondre sans délai aux demandes d'informations émanant des autorités compétentes. Les données financières couvrant cinq années peuvent atteindre des volumes considérables, et c'est pourquoi elles sont difficiles à gérer et à exploiter pour produire des rapports qui nécessitent un haut niveau d'expertise technique.

L'approche de Splunk

Splunk appuie les services financiers dans la lutte contre le blanchiment d'argent grâce à sa plateforme d'analyse des données qui centralise et extrait des informations, fournissant aux institutions de services financiers une vision holistique des sources de données pertinentes dans ce domaine. Lorsqu'il n'est pas possible de faire sortir les données d'un pays, l'architecture de Splunk permet de les interroger à distance et donne accès aux sources de données, aux alertes et aux références de contexte nécessaires pour détecter efficacement les tentatives de blanchiment d'argent, même si elles sont dispersées géographiquement.

L'architecture d'entreprise évolutive de Splunk permet d'assimiler et de stocker de grandes quantités de données brutes, structurées ou non, afin de remplir les obligations de conformité et de superviser les angles morts.

Les utilisateurs peuvent aisément interroger, corréler et visualiser les données stockées sans compétences de programmation, ce qui démocratise la lutte anti-blanchiment (AML) et permet aux équipes responsables de la conformité de superviser les transactions, de mener des enquêtes et d'automatiser des tâches. Les utilisateurs les plus avancés peuvent utiliser le Machine Learning Toolkit (MLTK) de Splunk pour élaborer des modèles AML capables d'identifier les anomalies.

Des applications Splunk AML sont disponibles sur Splunkbase pour faciliter le démarrage et aider les analystes et les opérateurs du secteur bancaire dans de nombreux domaines :

- la détection des patterns de transaction suspects en fonction des données historiques individuelles ;
- la découverte des tentatives d'échelonnement de transactions impliquant de grosses sommes ;
- des alertes en cas d'activité inattendue sur des comptes bancaires dormants ;
- l'identification de transactions entre des parties détentrices de bureaux virtuels ;
- le filtrage des sanctions et des listes noires.

Les capacités analytiques de Splunk aident les clients à identifier la fraude en tant qu'entité et non pas comme simple analyse d'une transaction inhabituelle.

Valeur

Le blanchiment d'argent est illégal car il permet à des criminels de profiter de leurs activités illicites, et il comprend généralement plusieurs étapes illégales. Les efforts d'AML imposent aux institutions d'investir dans de nouvelles technologies capables de résoudre les vulnérabilités de leurs approches actuelles, afin d'avoir une chance de réduire significativement la large part de blanchiment d'argent qui passe aujourd'hui inaperçue. Elles démontreront ainsi aux autorités de régulation qu'elles prennent l'AML au sérieux, ce qui peut leur éviter de lourdes amendes.

Les tableaux de bord et les vues synthétiques de transactions sur DAB peuvent permettre de repérer les activités anormales qui méritent une investigation.

Détection et prévention de la fraude à l'assurance

Défi

La lutte contre la fraude à l'assurance est une priorité stratégique pour le secteur. Actuellement, les fausses déclarations atteignant en tout des milliards de dollars sont faites chaque année, l'intention étant de frauder auprès des compagnies d'assurance. Bien que les assureurs mettent en place des stratégies de détection toujours plus sophistiquées, le problème est très envahissant, et nous estimons que des milliards de dollars de déclarations frauduleuses restent invisibles.

La fraude dégrade le ratio de sinistre des assureurs, qui sert à calculer les prix ; les assurés honnêtes se retrouvent donc à payer la facture de la fraude en voyant leur prime augmenter chaque année.

Les compagnies d'assurance investissent lourdement pour lutter contre la fraude et exploitent des approches innovantes basées sur les données pour leur faciliter la détection des fraudes. Les méthodes de fraude habituelles, comme l'augmentation du niveau de couverture peu de temps avant un sinistre ou un vol, peuvent être mises en évidence au moyen de simples requêtes sur les données des assurés et des sinistres, contenues dans la base de données de l'assureur.

Grâce à la télématique, certains assureurs proposent à leurs assurés de baisser leur prime à la condition qu'ils installent certains dispositifs de suivi qui enregistrent des milliers de données dans leur véhicule. Ces appareils capturent des informations telles que les coordonnées GPS, la vitesse de conduite, la distance, l'heure, le style d'accélération, les habitudes de freinage et de virage : toutes ces données peuvent être utilisées pour produire un rapport de reconstitution d'accident, ce qui réduit les temps d'investigation et arme l'assureur de données précieuses pour dénoncer les fausses déclarations, comme un coup du lapin lors d'une collision mineure.

L'approche de Splunk

Les données comptent parmi les outils les plus puissants dans la lutte contre la fraude. Les assureurs comprennent que plus ils possèdent de données, plus ils sont en mesure d'utiliser une analyse pour détecter la fraude avec un degré supérieur de précision et de couverture. L'identification et la prédiction de la fraude ne reposent plus uniquement sur les données de la base d'assurés et de sinistres, mais aussi sur un éventail plus large de sources externes comme les réseaux sociaux, les dispositifs IoT, les données de centre d'appel, les données de site web, les agences de score de crédit et même des données météorologiques.

Splunk agit comme plateforme de données intégrée qui permet aux assureurs d'exploiter pleinement des sources de données disparates pour produire une image plus précise de la fraude en temps réel. Cela leur permet de délivrer un large éventail de recherches allant de la simple requête à la prédiction des candidats à la fraude, qui utilise des techniques plus complexes exploitant des modèles de machine learning guidés fournis dans le Machine Learning Toolkit.

Valeur

Une solution de données intégrée permettra aux assureurs d'automatiser leurs décisions et d'extraire de précieuses informations, ce qui est essentiel pour accroître la rentabilité et acquérir un avantage compétitif dans le secteur.

Le moteur temps réel de Splunk permet aux évaluateurs de sinistre d'être avertis lorsqu'ils travaillent sur un cas de fraude potentielle avant même qu'ils n'aient commencé, ce qui fait gagner du temps et de l'argent à la compagnie en réduisant les dédommagements indus.

Disposer d'une visibilité sur l'ensemble du processus de demande de prime permet à l'opérateur de comprendre à quels niveaux il est moins performant, et à quel moment les clients modifient leurs informations pour obtenir un meilleur tarif.

« Pour la réussite de votre centre des opérations de sécurité, tout repose sur la connaissance des événements de votre réseau. Les hackers emploient des pratiques de plus en plus sophistiquées, et disposer du niveau de visibilité nécessaire est souvent un défi, tout particulièrement lorsque vous exploitez comme nous plus de 20 sources de données différentes. Depuis que nous avons déployé Splunk Enterprise Security comme centre névralgique de notre centre de sécurité, nous avons découvert que Splunk était la solution idéale pour créer et mettre en œuvre des analyses de sécurité rapides et efficaces portant sur un large éventail de sources de données et de scénarios de sécurité. »

— Tim Callahan,
Vice-président exécutif, Directeur sécurité globale d'Aflac

En savoir plus sur Splunk chez Aflac.

SÉCURITÉ ET DÉLITS FINANCIERS

Respect des sanctions

Défi

La mondialisation accrue et le paysage des menaces en constante évolution créent de nouveaux obstacles pour les institutions de services financiers qui doivent se conformer aux sanctions administrées dans différentes juridictions et par de multiples autorités. Ces institutions s'exposent ainsi à un risque accru d'infraction dans le contexte de la supervision opérationnelle.

Les institutions financières sont tenues de détecter les transactions suspectes et de mettre en place des contrôles et des vérifications adaptés pour identifier les infractions aux sanctions ou les tentatives de blanchiment d'argent. Elles sont encouragées à signaler spontanément les infractions pouvant concerner des transactions passées ou en cours. La divulgation spontanée est vue d'un œil favorable par les autorités de régulation et considérée comme un outil de lutte.

Les contrôles réglementaires examinent généralement l'infraction signalée et la qualité du programme de conformité aux sanctions de l'entreprise afin de détecter d'éventuels signes de négligence. La mise en place d'outils et de processus robustes pour détecter les infractions aux sanctions est indispensable pour qu'une institution ait confiance dans sa capacité à respecter ses obligations réglementaires. Les autorités de régulation examineront ses affaires sous un meilleur jour, ce qui peut lui éviter de lourdes amendes et une dégradation de sa réputation.

L'approche de Splunk

Les institutions financières doivent exploiter les sources d'informations sur les menaces comprenant des informations sur des cibles identifiées et les corréler avec leurs processus et systèmes internes pour identifier les situations pouvant être source d'infractions aux sanctions. Les données fournies sont généralement non structurées, ce qui rend leur stockage et leur analyse difficiles, sauf si l'on choisit une plateforme comme Splunk qui est capable d'établir des corrélations entre des données structurées et non structurées, et qui fournit un mécanisme pour saisir des recherches en texte libre permettant d'obtenir rapidement des noms de menaces connues ou suspectées.

Le moteur temps réel de Splunk peut avertir le personnel chargé de la conformité à chaque fois qu'une menace connue est identifiée par la corrélation de données provenant d'un flux de menaces et d'autres sources opérationnelles. Des tickets d'incident peuvent être créés automatiquement pour veiller à ce que les événements soient traités avec le sérieux et l'urgence nécessaires.

Les parties sanctionnées cherchent constamment de nouvelles méthodes pour contourner les contrôles et se soustraire aux sanctions, ce qui rend le filtrage des noms insuffisant à lui seul. Les institutions financières doivent impérativement s'armer d'une plateforme analytique de sécurité offrant la capacité de détecter les infractions avec des approches plus sophistiquées, par exemple en effectuant des recherches géographiques sur tout le trafic entrant pour repérer les clients qui se connectent depuis des régions interdites.

Valeur

Les amendes imposées en cas de violation peuvent être lourdes. Bien souvent, les sanctions et les peines peuvent atteindre plusieurs millions de dollars. Ces lourdes pénalités ont un impact direct sur la rentabilité et la réputation de l'institution. Pouvoir donner aux autorités de régulation la preuve que tout le soin et toute la diligence ont été apportés à la conformité aux sanctions, à l'aide d'une plateforme de supervision et de rapport appliquant des contrôles efficaces pour détecter les activités illégales, contribuera grandement à la réduction des risques d'amende.

« Grâce à la plateforme d'analyse Splunk, The Japan Net Bank, Ltd. (JNB) a pu mettre en place une nouvelle mesure de cybersécurité offrant gratuitement à tous les utilisateurs un mot de passe à usage unique. De plus, Splunk Enterprise envoie automatiquement des emails d'alerte en temps réel à l'équipe de réponse aux incidents de sécurité informatique de JNB lorsqu'il détecte le moindre signe d'attaque par hameçonnage. Les capacités de l'équipe ont ainsi été renforcées, ce qui lui a permis d'identifier plus de 20 sites frauduleux en une année et ainsi d'atteindre un niveau supérieur de sécurité. JNB a également mis son centre des opérations de sécurité en position d'aller plus loin dans la lutte contre les cyberattaques. »

En savoir plus sur Splunk chez Japan Net Bank.

SUPERVISION ET CONFORMITÉ

Supervision de l'automatisation

Défi

Les banques traditionnelles sont menacées par les entreprises plus petites et plus agiles de la FinTech qui peuvent innover et passer rapidement de l'idée au lancement du produit, ce qui leur donne un avantage en termes de délai de commercialisation.

Les banques cherchent à optimiser leurs opérations par la technologie, notamment en automatisant les tâches routinières et répétitives. Dans cette optique, elles investissent dans des outils qui leur permettent de réduire l'intervention manuelle dans les processus pour devenir plus performantes, rapides et rentables, et ainsi en faire plus avec moins.

Le problème reste que chaque nouvelle opportunité bancaire présente des risques. Certains de ces risques sont associés au comportement indésirable d'une tâche répétitive, que ce comportement soit accidentel ou malveillant. L'automatisation peut aussi comporter des risques, car une tâche automatisée peut retourner un résultat indésirable des centaines, voire des milliers de fois avant que quelqu'un ne le remarque (si quelqu'un le remarque !), ou encore exposer des données confidentielles ou sensibles.

Les risques sont clairs, et les banques doivent étudier des moyens de conserver une trace immuable des opérations et de superviser proactivement leurs outils d'automatisation et leurs tâches. Si une banque doit expliquer aux autorités de régulation l'existence d'une tâche automatisée, avec quoi elle a interagi, à quel moment elle a eu lieu, ce qu'elle a demandé et ce qui a été modifié, elle aura immédiatement des justificatifs à sa disposition.

Les règles visant à superviser les personnes cherchent à protéger leur vie privée. Mais contrairement aux êtres humains, les automatisations doivent être supervisées sans réserve pour comprendre pleinement et en permanence chaque action. Des contrôles tels que les congés obligatoires sont là pour aider les entreprises à identifier les comportements irréguliers. Toutefois, ces contrôles n'existent pas pour l'automatisation, ce qui veut dire qu'un employé peut potentiellement créer une automatisation pour effectuer des tâches malveillantes sans être détecté.

Le degré de visibilité d'un flux d'automatisation d'un processus, de ses déviations par rapport à la normale et de l'auteur des anomalies est un sujet que les entreprises doivent pouvoir traiter en totale confiance.

L'approche de Splunk

Splunk a la possibilité de consigner chaque étape au sein d'une procédure automatisée, stockée dans un dépôt inviolable, en conservant aussi bien les logs des outils d'automatisation que les systèmes avec lesquels ils interagissent (programmes, applications, bases de données et services contrôlés par la sécurité).

Étant donné que l'automatisation tend à générer des événements dynamiques, les données de ces systèmes sont naturellement non structurées. Il s'agit généralement des informations suivantes :

- les entrées (requêtes de base de données, commandes de système d'exploitation, clics RPA) ;
- les sorties résultantes reçues (exceptions, résultats textuels, codes de retours).

Ces données sont difficiles à traiter avec des analyses traditionnelles et des ensembles de règles fixes. Splunk est capable d'exploiter ces données pour observer les patterns qui dévient de leur comportement normal.

Avec Splunk, les banques sont en mesure de produire des rapports sur les statistiques de l'automatisation : automatisations accomplies avec succès, temps d'exécution et autres KPI. Elles peuvent aussi superviser proactivement les procédures afin de détecter les activités inhabituelles en temps réel.

La procédure interroge-t-elle le dépôt de mots de passe comme prévu, ou le nom d'utilisateur et le mot de passe ont-ils été saisis via une intervention matérielle pour contourner cette étape ? L'automatisation exploite-t-elle la CMDB ou utilise-t-elle une liste statique d'actifs sous forme d'un fichier CSV ? Une automatisation migrée en production invoque-t-elle toujours des actifs se trouvant dans des environnements Dev ou UAT ?

En capturant les logs des outils d'automatisation au fil de leur génération, les banques peuvent empêcher la modification des logs par un ingénieur en automatisation, et ainsi les valider pour l'ensemble de leurs outils d'automatisation.

Grâce aux capacités analytiques de Splunk, il est possible de définir une base de référence pour chaque procédure afin de générer des rapports, mais aussi de détecter les automatisations anormales lorsqu'elles dévient de leur comportement typique.

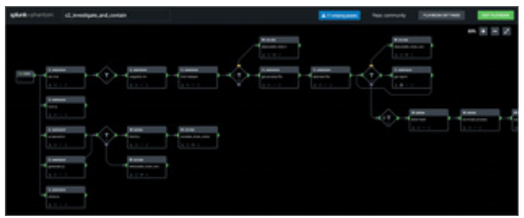
Splunk peut présenter le parcours de chaque procédure visuellement pour faciliter l'identification des comportements anormaux et des changements de comportement. Splunk représente graphiquement chaque parcours et le nombre de fois qu'il s'est produit, mettant en évidence la latence entre chaque étape pour reconnaître aussi bien les comportements typiques que les cas marginaux. Splunk facilite ensuite la mise en œuvre de la diligence raisonnable et vérifie que les appels aux autres systèmes sont conformes au comportement attendu.

Valeur

L'automatisation est maintenant un sujet faisant l'objet de débats des équipes de direction en raison des gains d'efficacité, des économies et du retour sur investissement qu'elle promet aux entreprises. Et comme ce retour sur investissement est quantifiable, les banques cherchent activement des moyens d'automatiser autant que possible en supervisant les déploiements au niveau de la direction.

Comme toute technologie, les outils d'automatisation peuvent faire l'objet d'abus. Utilisés de la mauvaise façon, ils peuvent déclencher des catastrophes et causer des dommages à long terme et à grande échelle.

Les banques doivent veiller au bon usage des technologies d'automatisation, en mettant en œuvre certaines précautions pour se protéger contre les malveillances. Grâce à l'observabilité qu'elle apporte, la mise en œuvre de Splunk va réduire les risques d'abus et d'erreurs accidentelles tout en apportant une agilité accrue face aux demandes des autorités de régulation.



L'automatisation des processus rend les institutions plus compétitives mais nécessite une supervision en temps réel pour garantir la conformité des opérations aux normes imposées.

Conformité aux normes de l'industrie des cartes de paiement (PCI)

Défi

Depuis début 2005, on estime qu'au moins 1,1 milliard d'enregistrements de données sensibles ont été compromis lors de failles rendues publiques.

La sécurité des paiements électroniques dans le domaine de l'e-commerce et des cartes génère de nouveaux défis car les criminels utilisent des techniques toujours plus sophistiquées pour s'introduire sur les réseaux, écouter les données et saboter les dispositifs.

Les données PCI peuvent être violées de différentes manières :

- Des hackers peuvent exploiter les réseaux et les connexions Internet qui ne sont pas protégés par les dernières mises à jour de sécurité.
- Des cambrioleurs, et parfois des acteurs internes malveillants, peuvent dérober des disques physiques, des CD ou des DVD.

PCI DSS est une norme industrielle qui s'applique à toutes les entreprises qui manipulent des données de possesseurs de cartes. PCI DSS protège ainsi les données des cartes de crédit, de débit et de retrait ainsi que les informations de leurs possesseurs pour réduire le risque de vol et/ou de perte de ces données.

PCI DSS exige que l'ensemble des commerçants, prestataires de services et institutions financières appliquent des critères minimaux de sécurité et de supervision des systèmes dans l'environnement de données des possesseurs de cartes (CDE).

Toute entreprise qui conserve, traite ou transmet des données de possesseur de carte de paiement est tenue de superviser régulièrement son CDE conformément à la norme PCI DSS.

La norme de sécurité des données comprend 12 exigences pour les entreprises, et qui englobent des politiques de sécurité, des procédures et des directives pour le stockage, le traitement et la transmission des données des possesseurs de cartes.

Établir et maintenir un réseau et des systèmes sécurisés :

1. Installer et maintenir un pare-feu configuré pour protéger les données des possesseurs de carte.
2. Ne pas utiliser les mots de passe et autres paramètres de sécurité par défaut créés par les fournisseurs des systèmes.

Protéger les données des possesseurs de carte :

3. Protéger les données stockées des possesseurs de carte.
4. Chiffrer la transmission des données des possesseurs de carte sur les réseaux ouverts et publics.

Maintenir un programme de gestion des vulnérabilités :

5. Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels et programmes antivirus.
6. Développer et maintenir des systèmes et des applications sécurisés.

Mettre en œuvre des mesures robustes de contrôle des accès :

7. Limiter l'accès aux données des possesseurs de carte aux seules personnes ayant professionnellement besoin d'en avoir connaissance.
8. Identifier et authentifier l'accès aux composants du système.
9. Limiter l'accès physique aux données des possesseurs de carte.

Superviser et tester régulièrement les réseaux :

10. Suivi et supervision de tous les accès aux ressources réseau et aux données des possesseurs de carte.
11. Tester régulièrement les systèmes et processus de sécurité.

Maintenir une politique de sécurité des informations :

12. Maintenir une politique traitant de la sécurité des informations et s'appliquant à tout le personnel.

Les tableaux de bord de l'application Splunk pour la conformité PCI présentent l'état de vos contrôles techniques de conformité pour vous permettre d'identifier et d'explorer les domaines qui nécessitent une attention particulière, et de répondre rapidement aux demandes de données formulées par les contrôleurs.

Conformité aux normes de l'industrie des cartes de paiement (PCI) (suite)

L'approche de Splunk

Les rapports sont les mécanismes officiels permettant aux commerçants et autres entités de déclarer leur état de conformité à PCI DSS à leurs institutions financières ou marques de carte de paiement réceptrices.

Selon les exigences du fournisseur de carte, les commerçants et les prestataires de services peuvent être tenus de remettre chaque trimestre un rapport d'évaluation et de conformité.

L'application pour la conformité PCI est développée et maintenue par Splunk pour aider les entreprises à satisfaire les exigences de PCI DSS 3.2. Elle examine et mesure l'efficacité et l'état des contrôles techniques de conformité PCI en temps réel, tout en conservant les données pour délivrer un historique de la position de conformité PCI et établir une tendance au fil du temps. Elle peut identifier et hiérarchiser les domaines de contrôles qui doivent faire l'objet d'une attention particulière et permet aux utilisateurs de répondre rapidement à toute demande de rapport d'audit ou de données.

Valeur

L'application Splunk dédiée à la conformité PCI capture les informations provenant d'applications, de systèmes et d'appareils du PCI CDE pour offrir une vision unique de la position de conformité PCI de l'ensemble de l'entreprise. L'application offre les capacités suivantes :

- Capture, supervision et déclaration des données provenant des dispositifs, systèmes et applications de l'entreprise dans l'environnement de données des possesseurs de carte.
- Supervision des tentatives d'accès aux actifs PCI.
- Supervision du trafic entre des domaines PCI.
- Identification des vulnérabilités trouvées sur des actifs PCI.
- Avertissement des administrateurs en cas de logiciel malveillant détecté sur des actifs PCI.
- Exploration et résolution des problèmes de conformité.
- Possibilité pour les responsables de la conformité PCI de superviser la conformité PCI DSS et de produire des rapports sur les activités significatives.
- Vues basées sur des rapports pour chaque contrôle de conformité pertinent.
- Fiches de notation de conformité offrant une vue d'ensemble de la conformité à chaque catégorie d'exigences PCI.
- Génération et affectation d'alertes, évaluation des risques et réponse aux incidents de sécurité potentiels.
- La corrélation des actifs et des identités facilite la production de rapports de conformité concernant des actifs et des utilisateurs spécifiques du PCI CDE.

Pour que les contrôles de sécurité restent pleinement opérationnels, l'application Splunk dédiée à la conformité PCI facilite l'intégration de la supervision PCI aux activités quotidiennes et à la stratégie globale de sécurité de l'entreprise. Elle garantit ainsi une supervision efficace et continue des contrôles de sécurité et le maintien d'un environnement conforme à PCI DSS entre deux évaluations.

PagSeguro est le leader des solutions de paiement en ligne sur le marché brésilien. PagSeguro voulait se doter d'une solution flexible de supervision en temps réel et souhaitait disposer d'une visibilité complète sur son environnement de production, en particulier dans le cadre de ses obligations face aux exigences de contrôles de conformité PCI. Depuis le déploiement de Splunk Enterprise, PagSeguro a observé plusieurs avantages :

- **une meilleure conformité aux normes de sécurité PCI ;**
- **l'amélioration de la satisfaction des clients ;**
- **une visibilité complète sur l'infrastructure.**

En savoir plus sur Splunk chez PagSeguro.

Conformité banque centrale et superviseurs

Défi

Les banques centrales endossent de nombreuses responsabilités qui varient d'un pays à l'autre, mais elles doivent par-dessus tout agir comme « prêteur de dernier recours » et prêter de l'argent aux banques quand elles sont en difficulté. Leurs responsabilités habituelles incluent la mise en œuvre des politiques monétaires et la supervision des institutions bancaires par une approche macroprudentielle.

La supervision consiste généralement à superviser les institutions pour vérifier qu'elles élaborent des politiques de contrôle (réglementations, orientations politiques, directives, etc.). Les institutions doivent également rester en conformité avec la loi et les réglementations. Les banques centrales vérifient si les institutions financières sont impliquées dans des pratiques dangereuses et prennent des mesures pour qu'elles corrigent leurs pratiques le cas échéant.

Lorsque des mesures de correction sont nécessaires, les banques centrales émettent des instructions assorties d'une date d'échéance et d'un niveau de gravité variable, en les adressant directement au comité de direction de l'institution pour l'enjoindre à corriger ses pratiques. Ces instructions écrites, souvent appelées affaires nécessitant une attention (MRA) et affaires nécessitant une attention immédiate (MRIA), ont la priorité sur tous les autres projets en cours et imposent un lourd fardeau imprévu aux services internes. Le personnel clé doit abandonner momentanément des projets potentiellement générateurs de recettes pour travailler à la résolution des problèmes, qui touchent généralement les contrôles et systèmes de gestion des risques de l'institution.

Le non-respect des échéances des MRA et MRIA peut entraîner de lourdes amendes, voire la révocation des autorisations de négociation dans les cas extrêmes. Pour les banques, la priorité n'est alors plus l'innovation mais la conformité.

Les banques centrales émettent régulièrement des MRA et MRIA. La capacité à réagir rapidement et efficacement aux instructions de cette autorité centrale peut devenir un véritable avantage compétitif permettant aux institutions d'économiser des millions en répondant sans délai et de libérer le personnel pour qu'il se consacre au cœur d'activité.

L'approche de Splunk

La transparence et la visibilité sont des aspects fondamentaux de la sécurité bancaire et comptent parmi les thèmes clés des nouvelles législations adoptées depuis la crise de 2008.

MiFID II et MiFIR en sont la parfaite illustration : elles favorisent des marchés plus équitables, plus sûrs et plus efficaces, ainsi que la transparence des échanges pour tous les participants.

À l'heure où la majorité des services des banques sont numérisés, cette transparence accrue se traduit par un meilleur accès aux données générées par toute l'entreprise ; les contrôleurs internes et externes ont ainsi la possibilité de comprendre le fonctionnement de l'institution et de reconstituer le déroulement des événements en cas d'incident.

Splunk réunit rapidement l'ensemble des données structurées et non structurées d'une institution financière internationale au sein d'un dépôt unique où les contrôleurs pourront trouver une copie parfaite des données brutes pour les analyser.

La technologie d'intégrité intégrée donne aux contrôleurs et aux autorités de régulation l'assurance que les données stockées dans Splunk sont parfaitement conformes aux données d'origine et n'ont pas été modifiées. Pour parvenir à ce résultat, Splunk calcule des hashes (avec SHA 256) pour chaque tranche de données ; il les stocke ensuite de manière à permettre l'exécution de vérifications assurant l'intégrité des données.

L'importation des données peut devenir une tâche onéreuse lorsqu'il existe potentiellement des centaines de sources de données d'intérêt pour les autorités de régulation. Ce n'est pas le cas avec Splunk. D'autres solutions imposent une étude détaillée pour comprendre chaque source de données en détails avant qu'il ne soit possible de produire le schéma qui permettra de répondre à des questions connues. À l'opposé, l'importation des données dans Splunk ne nécessite de définir à l'avance que l'horodatage et la délimitation des enregistrements, ce qui réduit le temps, l'argent et les efforts requis lors de cette phase et permet aux institutions de réagir rapidement aux demandes de données. Splunk établit un schéma dynamique à la volée lorsque l'utilisateur interroge les données, ce qui évite d'avoir à redéfinir un schéma à chaque fois que l'on pose une nouvelle question qui n'entre pas dans le cadre du précédent.

Les banques centrales peuvent également tirer un bénéfice direct de l'utilisation de Splunk. Les demandes de rapport adressées par les banques centrales aux institutions bancaires, en particulier de ceux de nature financière, doivent souvent être transmis au format XBRL (eXtensible Business Reporting Language). Les banques centrales peuvent donc utiliser Splunk pour interpréter et importer les rapports XBRL nativement, ce qui les rend immédiatement interrogeables et analysables. Les banques centrales peuvent réunir des rapports récurrents pour créer une image chronologique, détecter des tendances et des anomalies qui passeraient autrement inaperçues lors de l'analyse manuelle de multiples rapports.

Valeur

Les MRA/MRIA peuvent gravement perturber les opérations d'une banque. L'anticipation des requêtes de l'autorité centrale en disposant de données journalisées et interrogeables permet de gagner en agilité et de réagir efficacement, tout en réduisant la quantité de travail imprévue pour le personnel stratégique. Et comme les MRA/MRIA imposent de strictes échéances, Splunk peut aider les grandes institutions financières à assimiler les flux de données nécessaires plus rapidement que d'autres solutions du marché, et ainsi à respecter voire anticiper les échéances des autorités pour une conformité irréprochable.

« Lorsque nous recevons une alerte, nous nous posons des questions : ai-je déjà rencontré une situation similaire, ou même identique ? En utilisant Splunk comme plateforme de données, nous pouvons circonscrire la menace et découvrir les autres incidents qui font potentiellement partie du même puzzle. Nous disposons ainsi d'une plateforme de tri instantané pour transmettre tous ces éléments à l'analyste. »

— Jonathan Pagett,
Responsable du centre des opérations de sécurité de la Banque d'Angleterre

En savoir plus sur Splunk à la Banque d'Angleterre.

SUPERVISION ET CONFORMITÉ

Conformité SWIFT et ISO 20022

Défi

SWIFT (Société pour les télécommunications financières interbancaires internationales) est un vaste réseau de messagerie employé par environ 10 000 banques et autres institutions financières pour envoyer chaque jour des dizaines de millions de messages en toute sécurité. Il existe différents types de message, parmi lesquels :

Type de message	Description
MT0xx	Messages système
MT1xx	Paiements et chèques de clients
MT2xx	Transferts entre institutions financières
MT3xx	Marchés de trésorerie
MT4xx	Lettres de recouvrement et de créance
MT5xx	Marchés des titres
MT6xx	Marchés de trésorerie – Métaux et syndications
MT7xx	Crédits documentaires et garanties
MT8xx	Travellers Cheques
MT9xx	Gestion des liquidités et statut de client

Le réseau SWIFT ne traite aucune transaction : il relaie plutôt des messages formatés entre les banques membres. Ces messages contiennent des instructions sur les transactions financières ou d'autres communications commerciales.

En février 2016, la Banque du Bangladesh a été victime d'une cyberattaque ciblant son infrastructure SWIFT. Depuis, l'industrie a fait de la cybersécurité une priorité et s'est attachée à renforcer la protection de l'ensemble du réseau SWIFT.

Au cours d'une autre attaque, en mai 2018, la Banque du Chili a été ciblée par un virus qui a atteint des milliers de postes de travail. Par la suite, il est apparu que le logiciel malveillant n'était qu'un leurre conçu pour détourner l'attention de la véritable attaque, qui a soustrait 10 millions de dollars à la banque en utilisant le système de paiement SWIFT.

Outre les dommages pour l'image de la marque et les exfiltrations de données, les attaques SWIFT peuvent aboutir à des fraudes, du blanchiment d'argent, du contournement de sanctions, du financement d'activités criminelles et des problèmes de sécurité nationale.

De plus, les acteurs malveillants emploient des stratégies de plus en plus complexes pour échapper à toute détection, ainsi que des techniques de dissimulation comme l'émission de paiements frauduleux en dehors des heures ouvrées. Plus récemment, ils ont commencé à émettre des paiements de sommes plus faibles pendant les heures ouvrées pour les dissimuler dans le trafic commercial normal, tout en utilisant de nouveaux couloirs de paiement jusqu'ici inexplorés (combinaisons de banques cibles et bénéficiaires) afin de contourner la détection.

Les auteurs d'attaques consacrent un temps considérable à la phase de reconnaissance : ils s'introduisent dans les postes de travail des utilisateurs et observent les comportements sur une période prolongée avant de tenter d'accéder aux systèmes de paiement de la banque. Au cours de cette phase, les banques doivent être proactives et faire preuve de vigilance afin de détecter les menaces apparemment insignifiantes et courantes comme les logiciels malveillants, l'objectif étant d'éradiquer les attaques plus vastes à la racine.

Selon de récentes études SWIFT, les hackers utilisent ensuite le « transfert de crédit client unique » ou un message de type MT103 pour accomplir des opérations frauduleuses transfrontalières. Dans la plupart des cas, les transactions frauduleuses émises au cours des cyber-incidents touchant SWIFT impliquent des messages MT103.

Bien que les messages SWIFT contiennent une mine d'informations sur les transactions, il leur manque des données de référence contextuelles, comme le nom du responsable du compte client. Le format des messages MT et MX est moins réactif face aux évolutions de l'économie, des technologies émergentes et de l'innovation. Ces messages seront bientôt remplacés par une nouvelle norme, ISO 20022, qui offrira de nombreux avantages.

Entre autres choses, ISO 20022 embarquera bien plus de données dans le message, dotant ainsi les banques d'informations de référence plus détaillées qui seront extrêmement utiles pour détecter la fraude et lutter contre la criminalité financière.

L'approche de Splunk

Il est possible d'ingérer les messages SWIFT dans Splunk et d'appliquer des extractions de champ pour effectuer facilement des analyses sur les données.

Traditionnellement, les cyberattaques et les transactions inhabituelles sont analysées de façon indépendante, sans corrélation. Les équipes de sécurité recherchent les signes d'infection dans les systèmes informatiques en utilisant des outils traditionnels de gestion des incidents de sécurité (SIEM), tandis que les équipes spécialisées dans la fraude créent des modèles cherchant à détecter les transactions suspectes. Jusqu'à présent, il manquait des outils pour corréler les données informatiques et métier à l'échelle requise par une institution financière internationale.

Splunk change la donne en permettant aux institutions de corréler l'apparition d'un logiciel malveillant avec une transaction au comportement inhabituel. Il est ainsi possible d'évaluer rapidement si un logiciel malveillant n'est qu'un aspect d'une attaque plus grave. Des vérifications ponctuelles portant sur les volumes et la distribution des messages peuvent ensuite être utilisées comme indicateurs de suivi initiaux.

Dans les premières phases d'une attaque, Splunk Enterprise Security peut détecter la présence de logiciels malveillants et ainsi limiter la durée de la phase de reconnaissance employée par les hackers avant une attaque plus sophistiquée.

Conformité SWIFT et ISO 20022 (suite)

Les capacités d'analyse de Splunk offrent de nombreux moyens de détecter les signes de transactions suspectes. L'analyse des couloirs de paiement inhabituels, employés dans le blanchiment d'argent, ou de simples vérifications des données manquantes dans les enregistrements SWIFT, peuvent révéler que des auteurs d'attaques masquent intentionnellement des données pour éviter d'être détectés par les filtres d'application des sanctions et de l'AML.

Dans cette optique, ISO 20022 est conçue pour embarquer bien plus de données dans un message, ce qui démultipliera les possibilités de détection.

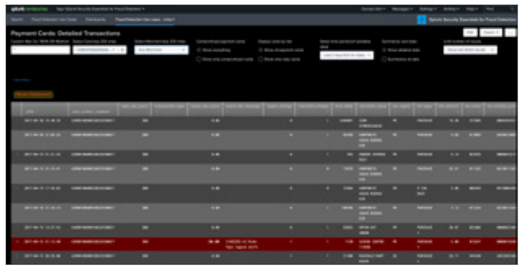
Et lorsque les institutions adopteront la nouvelle norme de messagerie SWIFT, l'analyse des données jouera un rôle croissant dans la lutte contre la criminalité financière. Les grandes institutions stockeront les messages SWIFT à différents emplacements pour respecter les exigences de protection des données et les réglementations transfrontalières. L'architecture de Splunk est idéale pour faire en sorte que les données soient stockées dans les régions appropriées, en maintenant le niveau souhaité de contrôle d'accès. La plateforme permet en outre aux personnes autorisées d'interroger et de consulter rapidement les données.

Toujours avec Splunk, les banques pourront encore enrichir leurs messages SWIFT de données supplémentaires. Entre autres choses, la plateforme permettra d'analyser les messages SWIFT afin d'apporter un contexte supplémentaire aux données, à la volée.

Enfin, les institutions qui utilisent le langage de recherche Splunk pourront relier les messages entre eux pour obtenir une vision de bout en bout des transactions.

Valeur

Au cours des dernières années, de nombreuses attaques de premier plan ont ciblé l'infrastructure SWIFT. Pour relever ce défi émergent, Splunk propose une plateforme d'analyse cohérente qui intègre sécurité, détection des fraudes, lutte contre le blanchiment d'argent et détection des contournements de sanctions, pour accroître la possibilité de détecter les comportements malveillants qui ciblent les systèmes de paiement. La sophistication accrue des défenses des banques, combinée à la réduction des délais de détection, est accueillie avec enthousiasme par les autorités de régulation.



Pour respecter les mandats de conformité liés aux paiements, vous devez disposer d'une visibilité sur toutes vos transactions, en temps réel.

SUPERVISION ET CONFORMITÉ

Enregistrement des appels

Défi

Les places d'échange sont soumises à de strictes réglementations exigeant l'enregistrement et l'archivage de toutes les communications concernant des transactions et impliquant des employés réglementés, et imposant que ces informations soient facilement accessibles afin de répondre rapidement à toute requête concernant la conformité. Aux États-Unis, la loi Dodd-Frank de réforme de Wall Street réglemente les marchés financiers et protège les consommateurs d'une récidive de la crise financière de 2008. La loi Dodd-Frank impose notamment de pouvoir enregistrer, lire et analyser n'importe quel appel téléphonique, passé depuis n'importe quel appareil, concernant une transaction ou donnant un consentement verbal à une transaction ou à une opération. Dodd-Frank stipule ce qui suit :

- Les enregistrements d'appels doivent être conservés, libellés et rendus consultables par transaction pendant 12 mois.
- L'enregistrement vocal ne peut se faire à la discrétion de l'appelant ou de son interlocuteur. Il doit toujours être actif.

D'autres organismes de réglementation financière dans le monde prévoient des dispositions similaires à Dodd-Frank concernant l'enregistrement des appels, comme COBS 11.8, mandaté par l'Autorité britannique de conduite financière.

Les appels mobiles et en VoIP en lien avec des transactions doivent être enregistrés de façon centralisée pour assurer la conformité. Les institutions sont tenues de mettre en place un système résilient et des contrôles de sécurité robustes pour garantir la protection des systèmes d'enregistrement des appels contre les temps d'arrêt résultant d'une cyberattaque ou d'une panne informatique. Inversement, pour respecter les lois relatives à la protection de la vie privée, ces mêmes institutions doivent veiller à interrompre l'enregistrement des appels d'un employé quittant un service où l'enregistrement des appels est obligatoire, pour rejoindre un service où il ne l'est pas.

L'approche de Splunk

Pour respecter les exigences de conformité, les institutions doivent assurer la disponibilité et la sécurité de leurs systèmes d'enregistrement d'appels. La plateforme Splunk est capable d'assimiler toutes les données associées à l'administration d'un système d'enregistrement des appels. Elle va veiller à la détection des cyberattaques et superviser en temps réel la santé et le bon fonctionnement général des applications, pour assurer une disponibilité maximale et empêcher toute perte d'appels. Avec Splunk, les clients analysent généralement les données suivantes de leurs systèmes d'enregistrement :

- les logs et métriques du système d'exploitation ;
- les logs et métriques de l'infrastructure (stockage, réseau, hyperviseur) ;
- les logs et métriques des applications d'enregistrement des appels (Nice NTR par exemple) ;
- les sources de données d'enrichissement (syslogs, métadonnées, CDR, VOX, etc.) pour enrichir les informations et apporter une visibilité améliorée sur l'état de santé du système, à des fins d'assurance qualité ;
- les informations d'en-tête des fichiers *.wav pour enrichir encore davantage les données et faciliter les processus d'assurance (qualité des voix, coupures, etc.) ;
- la messagerie instantanée ;
- la transcription textuelle des appels.

Les institutions peuvent utiliser Splunk pour enrichir les données d'enregistrement des appels à l'aide de données RH, afin que les enregistrements ne concernent que les personnes occupant un rôle sensible ou travaillant dans un service qui exige l'enregistrement des appels. Selon la même approche, les rapports d'exception générés par Splunk peuvent mettre en évidence les employés qui sont enregistrés alors qu'ils ne le devraient pas (par exemple, suite au transfert d'un employé vers un service moins sensible de l'entreprise), ce qui améliore encore la conformité et évite toute infraction aux lois sur la confidentialité.

Valeur

Superviser un système d'enregistrement des appels avec Splunk permet de le rendre plus fiable et plus sûr, et aide donc les institutions à démontrer leur conformité aux autorités de régulation, tout en réduisant les risques et en assurant la protection de l'entreprise et de ses employés en cas de conflit, de plainte ou de poursuite. Splunk réduit les temps d'indisponibilité des applications et propose des règles de détection contre les cyberattaques, en protégeant à la fois le système et les enregistrements à proprement parler. Une grande banque a ainsi rapporté une réduction de 97 % du temps nécessaire aux contrôles de fonctionnement et aux investigations. Les institutions auront également la possibilité d'améliorer l'expérience des clients en supervisant et en analysant les données dans Splunk, ce qui leur permet de visualiser des métriques telles que la qualité des appels, les temps d'attente et les interactions avec les clients.

Splunk aide les institutions à assurer leur conformité en optimisant la disponibilité des systèmes d'enregistrement d'appels, requis légalement pour superviser toute activité liée aux transactions. Les institutions auront également la possibilité d'améliorer l'expérience des clients en supervisant et en analysant les données dans Splunk, ce qui leur permet de visualiser des métriques telles que la qualité des appels, les temps d'attente et les interactions avec les clients.

SUPERVISION ET CONFORMITÉ

Examen des accès privilégiés

Défi

L'examen des accès privilégiés (PAR), parfois appelé « examen des activités privilégiées », impose aux banques de suivre et de superviser les employés qui ont la possibilité d'apporter des modifications critiques aux systèmes informatiques. Si les autorités de régulation stipulent qu'un programme de supervision des accès privilégiés est obligatoire, elles ne précisent pas comment les banques doivent le mettre en œuvre et laissent cet aspect à la discrétion de chaque institution. Pour se protéger contre les menaces internes, les banques doivent appliquer le principe de moindre privilège, ce qui signifie qu'elles doivent limiter les permissions d'accès des utilisateurs au strict minimum requis pour accomplir leurs tâches.

La supervision des accès privilégiés joue un rôle essentiel en veillant à ce que les utilisateurs possédant des permissions et des accès de haut niveau sur des systèmes critiques disposent d'une demande d'accès autorisé avant d'exécuter des commandes privilégiées sur un serveur ou une application. Chaque commande intrusive (inversion, mise à jour, suppression) soumise à des applications et technologies entrant dans le champ de la disposition doit d'abord être identifiée. Elle doit ensuite être corrélée et réconciliée avec un processus d'approbation, et l'accès accordé doit être rapproché de l'enregistrement de la demande comprenant les détails de la modification, la fenêtre temporelle pendant laquelle la modification est possible et les utilisateurs pouvant l'effectuer. Les sources généralement concernées sont les suivantes :

- les bases de données ;
- les applications d'entreprise ;
- Unix ;
- Windows ;
- les réseaux et périphériques réseau.

Chaque institution devra mener un processus interne afin de circonscrire la signification de « privilégié » pour chaque technologie concernée et définir les règles de reconnaissance qui permettront d'identifier une commande intrusive dans les données de log. Ce processus est généralement mené avec l'aide d'experts dans chaque domaine.

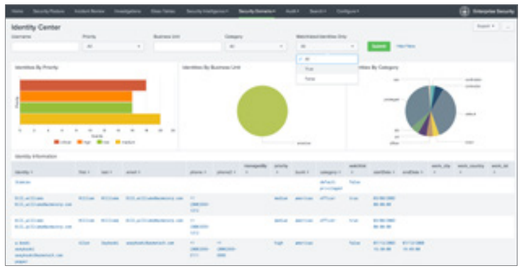
L'approche de Splunk

Une fois le champ d'application défini, les données doivent être collectées dans Splunk. Outre les données de log, les tickets de demande de modification, généralement conservés dans un système de gestion des services informatiques, doivent aussi être ingérés pour établir des corrélations. Des millions, voire des milliards d'enregistrements de logs selon la taille de l'entreprise, sont produits et ingérés. Toutefois, la plateforme Splunk, capable de s'étendre horizontalement, permet d'isoler les commandes intrusives grâce à la reconnaissance des mots, ce qui facilite considérablement l'identification des modifications privilégiées.

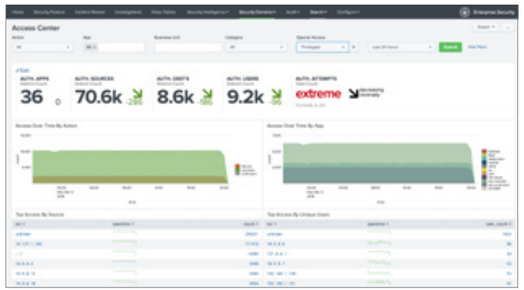
Splunk peut filtrer les événements en fonction de leur degré d'importance, de manière à conserver les commandes privilégiées considérées comme intrusives ou placées sur liste noire. Ces événements sont alors corrélés avec les données des tickets de modification pour vérifier si ces commandes intrusives ont bien été émises dans la fenêtre autorisée et par une personne approuvée. Il est ainsi possible de trier des millions d'entrées de log en fonction de milliers d'activités privilégiées pour en extraire les centaines d'infractions potentielles à contrôler. Toute exception devra être transmise à la hiérarchie pour investigation. Un programme de PAR s'exécute en continu car les systèmes et les applications sont constamment mis à niveau vers des versions plus récentes, ce qui entraîne nécessairement des modifications dans la sémantique de journalisation. Des faux positifs peuvent apparaître, imposant de modifier la logique de reconnaissance de Splunk pour réduire les occurrences et optimiser les procédures de contrôle.

Valeur

La mise en œuvre du PAR dans Splunk apporte aux contrôleurs la preuve qu'une institution sait ce qu'il se passe au sein de son service informatique grâce à une journalisation détaillée des activités clés. Le PAR peut également contribuer à la résolution des incidents car il capture une quantité considérable de données sur les événements qui ont eu lieu sur une machine ou dans une application donnée. Les institutions qui ingèrent déjà de grands volumes de données dans Splunk disposent de toutes les données de base nécessaires pour élaborer des applications PAR dans Splunk sans acheter ou développer de nouvelles solutions.



Les mises à jour et les nouvelles fonctionnalités des applications peuvent modifier la journalisation et rendre les règles de reconnaissance en place inopérantes. Ces dernières peuvent alors manquer des accès privilégiés. Splunk est suffisamment agile pour permettre aux entreprises de tenir ce rythme et d'adapter la reconnaissance des patterns pour détecter les accès privilégiés sans restructurer ou réingérer les données.



Des millions, voire des milliards de lignes de log doivent être analysées et enrichies par les données de la gestion des services informatiques et des ressources humaines pour fournir aux contrôleurs tout le contexte nécessaire pour détecter les abus d'accès privilégié, et pour cela, il faut une solution très évolutive. Les clients peuvent démultiplier la valeur des données ingérées par le PAR en les exploitant dans la correction et l'investigation sur les incidents informatiques et de sécurité.

Conformité au RGPD

Défi

Le Parlement européen a récemment adopté le nouveau règlement général sur la protection des données (RGPD), une loi harmonisée unique qui lie tous les états membres de l'UE. Le RGPD assure une prévisibilité et une efficacité renforcées pour les entreprises et offre aux citoyens de l'UE des droits accrus de protection des données dans le cadre de la nouvelle ère numérique, et s'applique depuis mai 2018.

Exigences essentielles du RGPD :

- Droits accrus pour les personnes concernées, dont le droit à l'oubli et la portabilité des données.
- Logiciels développés en tenant compte de la sécurité (confidentialité au niveau de la conception et par défaut).
- Pseudonymisation ou chiffrement des données personnelles (confidentialité dès la conception et par défaut).
- Traitement sécurisé des données.
- Notification sous 72 heures des violations des données personnelles.
- Amende pouvant atteindre 20 millions d'euros ou quatre pourcents des revenus annuels, selon le montant le plus élevé.
- En outre, le RGPD s'applique également aux entreprises du monde entier qui destinent leurs biens et services aux citoyens européens.

Splunk a identifié trois solutions pouvant soutenir un programme de conformité au RGPD.

1. **Gestion de la sécurité et notification des violations**

   Article 32 : Sécurité du traitement
   Le RGPD exige une sécurité de traitement (article 32), ce qui signifie que les organisations qui traitent des informations personnelles doivent mettre en œuvre « des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté face au risque ». Cela inclut des mesures techniques de pointe visant à éviter tout accès non autorisé aux données personnelles.

   Articles 33 et 34 : Notification
   Le RGPD exige la notification et la communication des violations. Cela signifie que les entreprises doivent avertir les autorités de tutelle dans les 72 heures suivant l'identification de la violation de données à caractère personnel susceptible de nuire aux droits et aux libertés de citoyens de l'UE (article 33), et qu'elles doivent avertir sans délai les personnes concernées (article 34). La notification doit comporter, entre autres, des informations sur la nature de la violation, notamment le nombre d'objets de données concernés, et les mesures prises pour y remédier.

2. **Audits de protection des données**

   Article 58 : Pouvoirs d'investigation et de supervision
   Le RGPD accorde à chaque autorité de tutelle le pouvoir de procéder à des investigations sous la forme d'audits de protection des données, d'émettre des avertissements, des réprimandes ou des interdictions de traitement des données (article 58). L'article 82 offre à toute personne ayant subi des dommages matériels ou non matériels le droit de bénéficier d'une compensation. Les amendes peuvent être évitées si une partie est en mesure de prouver qu'elle n'était en aucun cas responsable de l'événement à la source des dommages. Pour ce faire, les entreprises doivent documenter leurs actions et démontrer leur conformité à l'autorité de tutelle.

3. **Recherches et rapports sur le traitement des données personnelles**

   Articles 15, 17, 18 et 28 : Droits des personnes concernées
   Le RGPD garantit aux citoyens de l'UE le droit de savoir quelles données personnelles les concernant sont détenues, avec qui elles sont partagées et où elles sont traitées (article 15). Les personnes concernées peuvent également demander à ce que leurs données personnelles soient corrigées (article 16) ou supprimées (article 17). Les personnes responsables du traitement doivent s'assurer que seules des personnes autorisées traitent les données personnelles, et quand le traitement est terminé et le contrat résilié, le contrôleur peut demander à ce que toutes les données personnelles soient supprimées ou renvoyées, y compris dans certains cas, toutes les copies de sauvegarde existantes.

L'approche de Splunk

Les données machine offrent les informations historiques dont les entreprises ont besoin pour fournir la preuve aux autorités de tutelle qu'elles ont mis en place des contrôles de sécurité appropriés. En enregistrant l'activité des clients et des utilisateurs, les transactions traitées, l'activité des applications, des serveurs, des réseaux et des appareils mobiles, les organisations peuvent démontrer aux autorités qu'elles ont mis en place des contrôles de sécurité appropriés et mis en œuvre des efforts proactifs de réduction des risques (articles 32 et 58).

Splunk apporte une visibilité sur les activités de traitement et expose les comportements anormaux et les accès non autorisés, ce qui est essentiel pour la conformité au RGPD. Splunk informe les entreprises sur tous les accès aux données personnelles (heure, utilisateur, motif d'utilisation) (articles 15, 17, 18 et 28), ce qui aide les sociétés à remplir leurs obligations de notification (articles 33 et 34). Splunk Enterprise Security (ES), la solution SIEM leader de Splunk, est l'exemple parfait d'un contrôle mis en place pour réduire les risques : il délivre des rapports prêts à l'emploi qui permettent aux entreprises de démontrer leur conformité au RGPD.

Valeur

Les institutions qui utilisent Splunk ES pour leurs analyses de sécurité prouvent clairement aux autorités qu'elles prennent leurs obligations RGPD au sérieux et qu'elles sont en mesure de respecter les articles susmentionnés, ce qui réduit considérablement le risque de lourdes amendes.

À propos de Splunk.

Les données machine ont le pouvoir de résoudre les problèmes complexes propres au secteur des services financiers. À partir de ces mêmes données, il est également possible de produire des renseignements métier inédits et puissants. En analysant des quantités massives de données machine en temps réel, vous pouvez donner un nouvel élan à votre carrière et à votre entreprise.

La plateforme Splunk d'analyse en temps réel des données peut avoir de nombreux avantages pour votre société de services financiers.

En savoir plus

splunk> turn data into doing®

20-14076-SPLK-40-Ways-To-Use-Splunk-in-Financial-125