Grâce à l'analyse en temps réel des données, OhioHealth investigue plus rapidement les incidents

OhioHealth

Résumé

Fondée en 1891, OhioHealth est un organisme de santé à but non lucratif qui réunit 28 000 employés, médecins et bénévoles, et englobe un réseau de 11 hôpitaux, plus de 50 centres ambulatoires, un hospice, des services de soins à domicile, de l'équipement médical et d'autres services de santé couvrant une région de 40 comtés. OhioHealth s'appuie sur un environnement en réseau pour assurer l'accès transparent et sécurisé aux données médicaux des patients, à la télémédecine et autres services de santé. Depuis le déploiement de Splunk Enterprise, la société a observé plusieurs avantages :

- Les enquêtes sur les incidents sont plus rapides ;
- 5 000 $ d'économies environ sur chaque cas de phishing ;
- Jusqu'à 30 000 $ par an de frais de maintenance économisés pour le logiciel d'audit d'Active Directory.

Pourquoi Splunk

Le réseau de santé est équipé de nombreux outils logiciels et matériels pour protéger son environnement IT : pare-feux, logiciels de prévention de la perte de données (DLP), détecteurs de vulnérabilités, contrôleurs de domaines Active Directory, antivirus et protection contre les malware, et solution de gestion des événements et des informations de sécurité (SIEM). Si chacun de ces outils est efficace à son échelle, ils ne sont pas suffisamment intégrés, ce qui rend les analyses ponctuelles difficiles et empêche d'agréger et corréler des données de sécurité disparates. OhioHealth avait besoin d'une solution englobant ses différents silos de données pour harmoniser ses outils de sécurité, mettre au point un programme de sécurité à la pointe de l'industrie et offrir un moyen simple d'informer l'entreprise des risques potentiels.

L'équipe des opérations de sécurité d'OhioHealth a déployé Splunk Enterprise et installé des forwarders Splunk sur l'ensemble de ses pare-feux, contrôleurs de domaines, switches et autres dispositifs. Les forwarders Splunk assurent, de façon fiable et sécurisée, la collecte et la transmission des données à la plateforme Splunk à des fins d'indexation, de stockage et d'analyse. Dès que Splunk Enterprise a commencé à ingérer les logs et autres données, l'équipe s'est servie de la plateforme pour mieux protéger son infrastructure et garantir sa conformité à la loi HIPAA (une loi américaine) et à d'autres réglementations. Le logiciel Splunk a permis d'accélérer les investigations sur les incidents, d'améliorer la corrélation des événements et de fournir des analyses en temps réel et automatisées des données.

Secteur d'activité

- Santé

Scénarios d'utilisation Splunk

- Opérations informatiques
- Sécurité

Les défis

- Manque d'intégration entre les différents outils de sécurité en place
- Analyses ad hoc difficiles à réaliser
- Agrégation et corrélation impossibles des données de sécurité disparates
- Projet de bâtir un programme de sécurité à la pointe de l'industrie

Impact sur l'entreprise

- Corrélation et analyse des données de sécurité à l'échelle de la plateforme
- Accélération des enquêtes sur les incidents
- Automatisation de l'analyse des métriques et des données en temps réel
- 5 000 $ d'économies environ sur chaque cas de phishing
- Jusqu'à 30 000 $ par an de frais de maintenance économisés pour le logiciel d'audit d'Active Directory
- Économies à prévoir suite à la suppression des frais de licence du SIEM précédent

Sources de données

- Logs du pare-feux et du contrôleur de domaine
- Switches, routeur et autres dispositifs réseau
- Systèmes antivirus des points de terminaison
- Détecteurs de vulnérabilités
- Logs d'accès des serveurs web Apache
- Logs DLP (prévention de la perte de données)

Produits Splunk

- Splunk Enterprise
- Splunk Enterprise Security

Sensibilisation au hameçonnage et à la réduction des risques

OhioHealth évaluait des services afin de conduire des audits sur le hameçonnage au sein de son réseau de santé. Le groupe de sécurité envisageait de faire appel à un service qui aurait coûté 5 000 $ par session de test de hameçonnage. Au lieu de cela, il a associé un serveur web de hameçonnage interne à Splunk Enterprise et écrit un script de base pour envoyer des emails de hameçonnage à 700 destinataires sélectionnés au hasard sur le réseau OhioHealth. Après des mois de test, l'équipe a réalisé une démonstration en direct devant l'équipe de direction en utilisant des tableaux de bord Splunk pour afficher les résultats en temps réel. L'équipe a ainsi pu voir exactement qui cliquait sur l'email, sachant que s'il s'était agi d'une véritable tentative de hameçonnage, cela aurait pu entraîner une infection ou un vol d'identifiants.

« La démonstration en direct de Splunk a sensibilisé nos décideurs commerciaux à l'importance de l'analyse et de la réduction des risques, » affirme le directeur des Technologies d'infrastructure d'OhioHealth. Il poursuit : « Non seulement Splunk nous a permis de créer notre propre système de test de phishing, mais nous économisons le budget que nous avions prévu pour faire appel à un service externe. »

Des économies considérables en audits Active Directory

Au cours de la mise en œuvre d'un nouveau système d'accès biométrique pour les médecins d'OhioHealth et d'autres personnels cliniques, des groupes critiques d'utilisateurs avaient été accidentellement supprimés d'Active Directory. Si l'équipe d'implémentation est parvenue à restaurer les utilisateurs, la cause de la suppression restait inconnue. « Nous avions pensé à une solution de sécurité et de conformité réputée mais traditionnelle, mais nous avons compris que ce n'était pas exactement ce qu'il nous fallait, et cela nous aurait coûté environ 30 000 $ par an, » explique le directeur. « Il nous fallait un outil pour auditer nos services Active Directory et déterminer ce qui se passait – et à quel moment. Nous avons découvert que nous pouvions créer ce système en utilisant Splunk Enterprise, quasiment gratuitement. »

« Notre SIEM n'était qu'un SIEM, alors que Splunk est une plateforme d'analyse de données avec une fonction SIEM. Dans les cas où nous avons besoin d'explorer des logs ou des rapports d'utilisation Internet, tout va bien plus vite avec Splunk Enterprise. Quelle que soit notre question, avec les bonnes données nous obtenons toujours une réponse grâce à Splunk. En matière de détection des anomalies, on peut compter sur Splunk Enterprise Security. »

Directeur des Technologies d'infrastructure
OhioHealth

En déployant des forwarders Splunk sur chaque contrôleur de domaine pour recueillir des informations au sujet de ces dispositifs, puis les transmettre de façon fiable et sécurisée à l'instance centrale de Splunk pour analyse, le groupe des opérations de sécurité a acquis la possibilité de superviser l'ensemble de la Forêt Active Directory en temps réel, et notamment toute modification apportée aux répertoires et comptes utilisateurs. Lorsque le même problème d'accès s'est reproduit, grâce à Splunk, l'équipe a localisé la source du problème en quelques minutes.

Des renseignements plus approfondis sur les opérations réseau

Le groupe Réseau d'OhioHealth envoie les données de log provenant de tous les routeurs et switches, pour qu'elles soient indexées dans Splunk Enterprise. Le groupe a observé des bénéfices immédiats : il obtient des renseignements bien plus détaillés sur les opérations réseau. Tous les détails opérationnels jusque-là indétectables, comme les ventilateurs à l'arrêt, sont aujourd'hui faciles à voir et à corriger. Le groupe réseau prévoit d'intégrer Splunk à son NOC (centre des opérations réseau) nouvelle génération. OhioHealth prévoit également de remplacer son SIEM par Splunk Enterprise Security, qui fournit des fonctionnalités prêtes à l'emploi d'examen et classification des incidents, de rapports, de métriques de sécurité, d'analyse des risques, d'intelligence des menaces et d'analyse statistique, et s'accompagne d'un éditeur de recherche unifié et de tableaux de bord flexibles.

FINAL_CS-Splunk-OhioHealth-A4-FR