Le SOC Splunk atteint un MTTD de 7 minutes pour les attaques de phishing avec Splunk Attack Analyzer et Splunk SOAR

Défis clés

Les analystes du SOC étaient submergés par des centaines d'alertes de phishing chaque mois. Le MTTR était long et limitait le nombre d'investigations approfondies qu'ils pouvaient effectuer chaque mois.

Résultats clés

Splunk Attack Analyzer donne davantage de contexte à l'équipe de réponse aux incidents pendant les investigations, ce qui lui permet de contenir les menaces sans délai et de résoudre les alertes de phishing 90 % plus rapidement.

splunk>

Secteur d'activité : Technologie

Solutions : Sécurité

Produits : Splunk SOAR, Splunk Attack Analyzer

Pour que personne ne morde à l'hameçon

Le phishing est l'un des vecteurs d'attaque les plus fréquents et les plus coûteux : 88 % des entreprises interrogées dans notre rapport État de la cybersécurité en 2024 s'attendent à ce que les attaques de phishing augmentent en nombre et en efficacité avec l'utilisation de l'IA générative. Lorsque les employés de Splunk reçoivent un e-mail suspect, ils peuvent le signaler à l'équipe de détection et de réponse pour protéger l'entreprise de tout risque de faille. Des centaines d'alertes inondent l'équipe chaque mois. La plupart d'entre elles sont de fausses alertes, mais certaines signalent un risque réel. Dans tous les cas, les analystes doivent mener une investigation approfondie pour faire la part des choses.

Pour faire face à ce volume considérable d'alertes, l'équipe Splunk a décidé d'adopter Splunk SOAR. Quand une alerte e-mail arrivait, Splunk SOAR créait automatiquement un ticket et extrayait les informations utiles. C'était un bon point de départ, mais l'équipe de détection et de réponse de Splunk voulait faire passer le MTTD sous le seuil des 7 minutes. Autrement dit, il fallait aussi automatiser l'étape d'investigation. Et c'est là que Splunk Attack Analyzer entre en jeu.

Résultats

- Résolution des alertes de phishing 90 % plus rapide
- Amélioration de la précision de la détection du phishing
- Accélération de la prise en charge et du confinement des menaces de cybersécurité

Jusque-là, le volume de signalements de phishing était tel que l'équipe avait un gros arriéré de tickets à trier. Après avoir adopté Attack Analyzer, les tickets étaient étudiés et résolus 90 % plus rapidement. Quand un utilisateur signale une suspicion d'attaque de phishing, SOAR ouvre un ticket et l'e-mail suspect est automatiquement envoyé à Attack Analyzer pour analyse. Attack Analyzer examine l'intégralité de la chaîne d'attaque puis produit pour chaque cas un score et un verdict indiquant le degré de gravité de la menace. Attack Analyzer ajoute ensuite les résultats de l'analyse et toutes les preuves pertinentes au ticket. Tout cela se déroule en quelques minutes seulement, ce qui simplifie considérablement la tâche de l'analyste chargé de contenir la menace. Aujourd'hui, le SOC de Splunk répond bien plus vite à ces menaces et réduit le risque de violation et de perturbation associé au phishing.

Faire face aux incidents les plus graves

Si vous travaillez dans le domaine de la réponse aux incidents, vous savez que les erreurs de jugement peuvent coûter cher. C'est le cas dans toutes les fonctions de cybersécurité, dans toutes les entreprises. Et c'est d'autant plus vrai pour l'équipe Advanced Threat Response de Splunk, qui s'attaque aux incidents les plus graves et les plus retors ciblant l'entreprise. Cette unité de dix professionnels travaille avec le SOC et d'autres acteurs internes pour préserver la sécurité de Splunk. Quand un problème survient, la mission de l'équipe consiste à minimiser son impact sur les opérations, les finances et la réputation de l'entreprise, et à faire en sorte que tous les employés de Splunk puissent continuer de travailler dans les meilleures conditions.

L'équipe a récemment adopté Splunk Attack Analyzer pour approfondir ses investigations et augmenter sa capacité d'analyse. Depuis, c'est son outil numéro un dès qu'il faut analyser des fichiers ou des domaines suspects. Splunk Attack Analyzer permet aux membres de l'équipe de détecter plus rapidement les incidents et de réduire le risque pour l'entreprise. « Cela nous a aidés à faire face aux incidents les plus inextricables, » affirme Tony Iacobelli, Responsable senior de l'équipe Advanced Threat Response de Splunk.

> Attack Analyzer est un outil que nos spécialistes adorent utiliser, ce qui n'est pas monnaie courante. Ils savent qu'ils peuvent pousser l'outil dans ses retranchements et qu'il continuera de fonctionner. Et lorsque nous avons affaire à un incident étrange et inconnu, Attack Analyzer est l'un des premiers outils que nous utilisons pour y voir plus clair. »
>
> **Tony Iacobelli,** Responsable senior, Splunk Advanced Response

Avec un puissant outil d'analyse comme Splunk Attack Analyzer dans son arsenal, l'équipe peut élargir le champ de ses détections. Auparavant, lorsqu'une malveillance se manifestait, l'équipe Advanced Threat Response s'appuyait essentiellement sur sa solution EDR pour l'arrêter automatiquement. Avec Attack Analyzer, les analystes peuvent repérer des tendances et obtenir des informations supplémentaires sur la source de l'attaque – notamment les indicateurs de compromission et les artefacts d'hôte. Ces éléments permettent de détecter d'autres cas d'activité suspecte qui peuvent avoir échappé à l'EDR. Grâce aux modes de détonation interactive intégrés, l'équipe peut examiner les malwares sans courir le risque d'infecter ses machines.

Ce nouvel outil est arrivé à point nommé. M. Iacobelli explique : « Nous étions en train d'élargir le nombre de scénarios d'utilisation et de domaines sur lesquels nous avons de la visibilité. Malheureusement, il ne suffit pas d'agrandir l'équipe au fur et à mesure. Il fallait également accroître la productivité de l'équipe en améliorant notre efficacité globale. Et c'est exactement ce que fait Attack Analyzer. » Attack Analyzer a augmenté l'efficacité de toutes les équipes de réponse aux incidents de Splunk, à tel point qu'elles ont atteint leur objectif : faire passer le temps moyen de détection des cas critiques sous le seuil des sept minutes.

24-643263-Splunk-SOC-CS-103_FR