MAGNET FORENSICS®

Étude de cas Breadcrumb Cybersecurity et Magnet Axiom Cyber

Comment une société de sécurité a fait face à la compromission d'e-mails professionnels et triplé sa capacité de traitement des dossiers.

Breadcrumb™ CYBERSECURITY

Breadcrumb Cybersecurity aide les organisations à protéger leur infrastructure, leurs données et leur réputation contre les cybermenaces avancées.

Défis

- Accompagner les clients dans l'explosion des coûteuses attaques de compromission d'e-mails professionnels
- Traiter le volume élevé de données d'enquête
- Équiper le personnel de la DFIR pour qu'il puisse travailler efficacement

Solutions

Axiom Cyber permet à Breadcrumb Cybersecurity de :

- Réduire le champ d'investigation aux preuves pertinentes pour le dossier en l'espace d'une journée
- Recenser les liens entre les nombreux artefacts
- Maîtriser une suite d'outils unique

Résultats

- La clôture des dossiers de compromission d'e-mails professionnels prend deux fois moins de temps
- La capacité de traitement des dossiers a augmenté de 300 %.
- Capacité reconnue de résolution des problèmes

Le défi

> « Face à des attaques complexes de compromission d'e-mails professionnels, il est pratiquement impossible de déjouer efficacement les parties, les domaines et autres acteurs malveillants sans un outil comme AXIOM Cyber. »
>
> —
>
> **Brian Horton**
> PDG, Breadcrumb Cybersecurity

La compromission des e-mails professionnels explose

C'est arrivé en un éclair. En l'espace de quelques mois, le nombre d'attaques de compromission d'e-mails professionnels (Business Email Compromise, BEC) a dépassé celui des ransomwares, au point de devenir la première source de préoccupation pour Breadcrumb Cybersecurity et de ses clients.

« Le nombre d'attaques a explosé », déclare Brian Horton, PDG de l'entreprise. « Pour nous, la BEC constitue désormais le plus grand nombre de dossiers et de pertes par victime, et de loin ». En fait, dit-il, les attaques ont touché les entreprises du centre de la Californie dix fois plus durement que les ransomwares, avec des pertes dépassant parfois le demi-million de dollars.

Un seul dossier peut impliquer des millions d'artefacts répartis entre de multiples sources de données. « Nous disposons d'un ensemble de compétences et de connaissances, mais pouvoir les appliquer à un ensemble de données aussi vaste est tout simplement stupéfiant », note M. Horton.

Et puis l'affaire est pour le moins délicate. Les attaques de compromission d'e-mails professionnels sont devenues exponentiellement plus complexes, impliquant de multiples usurpations d'identité et faux fils se déroulant en même temps.

2X PLUS RAPIDE
CLÔTURE DES DOSSIERS

3X LE VOLUME DE DOSSIERS TRAITÉS

Les outils traditionnels ne suffisent pas

Avant l'explosion du nombre de compromissions d'e-mails professionnels, Breadcrumb avait armé ses experts en sécurité d'outils robustes pour lutter contre les ransomwares et autres menaces de cybersécurité. Cependant, par expérience, M. Horton considérait que les produits traditionnels de criminalistique numérique et de réponse aux incidents (Digital Forensics and Incident Response, DFIR) manquaient de capacités et nécessitaient beaucoup de formation.

Alors qu'il cherchait l'outil adéquat pour son laboratoire, M. Horton a appris qu'une agence fédérale et le bureau d'un procureur local utilisaient Magnet Axiom Cyber avec acquisition à distance intégrée.

Breadcrumb a commencé un essai.

« Lorsque nous avons importé notre premier disque dur et notre premier téléphone portable et que nous avons vu les nombreuses catégories d'artefacts extraites, je me suis dit que cet outil était incroyablement utile », se souvient M. Horton.

Comment Magnet Axiom Cyber nous aide

> Axiom Cyber nous permet de réduire rapidement le contenu. À chaque fois, nous pouvons circonscrire les artefacts pertinents à notre dossier en l'espace d'une journée.
>
> —
>
> **Brian Horton**
> PDG, Breadcrumb Cybersecurity

La réduction avant le sauvetage

Breadcrumb accélère la collecte et l'analyse des preuves provenant des ordinateurs, du Cloud et des appareils mobiles avec Axiom Cyber, ce qui permet d'agir rapidement pour lutter contre de nombreux types de menaces de sécurité, y compris l'augmentation récente des attaques de compromission d'e-mails professionnels.

Les examinateurs de Breadcrumb utilisent l'Explorateur Timeline pour réduire le champ d'investigation des preuves pour chaque dossier. Ensuite, des examinateurs qualifiés conservent une vue d'ensemble en recherchant des mots-clés, en pivotant sur les chronologies et en créant des étiquettes pour établir leur propre ordre des événements, une capacité indispensable pour contrer les modifications liées à la BEC effectuées par des acteurs malveillants toujours présents dans l'environnement, selon M. Horton.

Une fois l'analyse terminée, les examinateurs étiquettent également les éléments pour créer des rapports spécifiques à l'artefact qui aident à présenter les résultats aux clients : « Ils peuvent ainsi voir ce qui s'est passé et atteindre les mêmes conclusions que nous. »

Maîtrise des examinateurs

Contrairement à d'autres systèmes, les examinateurs de Breadcrumb trouvent qu'Axiom Cyber est facile à utiliser avec des flux de travail intuitifs. Par exemple, un analyste de laboratoire expérimenté dans le domaine de la police, mais novice en matière d'outils de criminalistique numériques, n'a pas perdu de temps à se familiariser avec le système.

« Notre analyste est passé de l'inexpérience totale du produit à sa maîtrise en l'espace de trois mois, ce qui a été un énorme avantage pour nous », a déclaré M. Horton.

> « Notre analyste est passé de l'inexpérience totale du produit à sa maîtrise en l'espace de trois mois, ce qui a été un énorme avantage pour nous. »
>
> —
>
> **Brian Horton**
> PDG, Breadcrumb Cybersecurity

Une protection renforcée

Pour servir ses clients, Breadcrumb doit gérer des dizaines de dossiers à la fois, en faisant remonter les détails pertinents et les informations exploitables pour que les choses avancent.
« Avec Axiom Cyber, nous gérons notre charge de travail à grande échelle », explique M. Horton.

Les examinateurs de Breadcrumb ont accru la vitesse à laquelle ils importent et trient les données. « L'analyse des artefacts permet d'abord de les réduire au maximum », a expliqué M. Horton. Ensuite, les examinateurs appliquent leurs compétences spécialisées uniquement aux éléments de preuve pertinents pour le dossier.

« Lorsque nous travaillons sur un dossier, nous sommes en mesure de réduire le contenu, puis de suivre notre processus... notre délai de clôture est deux fois plus rapide », note M. Horton. « Dans les cas d'attaques de compromission d'e-mails professionnels, il est pratiquement impossible de déjouer les parties malveillantes, les faux domaines et autres sans un outil comme Magnet AXIOM Cyber. »

Pour les clients de Breadcrumb, le raccourcissement des délais augmente leurs chances d'arrêter les pertes financières ou de les inverser et de renforcer leur position contre de futures attaques.

Augmentation du nombre de dossiers

Pour Breadcrumb elle-même, la facilité et l'efficacité permettent à l'entreprise de servir plus d'organisations aux prises avec la compromission d'e-mails professionnels, les ransomwares ou d'autres cyber-attaques.

« Nous pouvons traiter trois fois plus de dossiers qu'auparavant », explique M. Horton.

Cela représente trois fois plus d'opportunités de faire tomber les délinquants en tant que solutionneur fiable de problèmes pour les compagnies d'assurance et les fournisseurs de services gérés (Managed Service Providers, MSP), ainsi que pour les organisations avec lesquelles Breadcrumb entretient des relations directes.

En outre, comme l'entreprise propose des services de centre d'opérations de sécurité (Security Operations Center, SOC), l'augmentation de la capacité se traduit directement par une nouvelle source de revenus. « Pratiquement tous les clients ayant été victimes finissent par devenir clients du SOC », explique M. Horton.

En bouclant la boucle, les efforts du SOC servent ensuite à affiner l'offre de Breadcrumb en matière de réponse aux incidents et de criminalistique.

« Nous avons une connaissance concrète de la manière dont d'autres organisations sont ciblées et attaquées », explique M. Horton. « Nous prenons donc ces connaissances et nous les réutilisons dans notre travail avec les victimes ».

MAGNET FORENSICS®

Pour en savoir plus, rendez-vous sur magnetforensics.com.

Prenez dès aujourd'hui rendez-vous pour une démonstration en appelant le 1 844 638-7884 ou en envoyant un e-mail à sales@magnetforensics.com.