Cyberpion

ETUDE DE CAS

Une entreprise Internationale du secteur de l'Energie renforce ses défenses contre les attaques de la chaîne d'approvisionnement numérique

LE DÉFI

E.ON, une entreprise européenne de services publics d'électricité basée à Essen, en Allemagne, exploite l'un des plus grands services publics d'électricité au monde appartenant à des investisseurs. L'entreprise emploie plus de 80 000 personnes et sert 53 millions de clients dans 30 pays.

L'équipe de cybersécurité d'E.ON a reconnu la nécessité d'étendre de manière proactive ses processus et procédures pour protéger l'organisation et ses clients d'une éventuelle perte de données via leur écosystème en ligne tiers. Pour soutenir l'initiative, l'équipe d'E.ON a identifié une tâche stratégique clé : comprendre les risques auxquels elle est exposée dans le cadre de sa surface d'attaque externe.

La surface d'attaque externe d'E.ON comprend à la fois ses actifs détenus et gérés directement, ainsi que les actifs informatiques tiers qui sont détenus et gérés par des fournisseurs et des partenaires. La surface d'attaque d'E.ON n'a cessé de croître au fur et à mesure qu'elle intégrait les produits et les capacités de ces fournisseurs pour offrir un service et une assistance de premier ordre à ses clients. Alors que l'équipe d'E.ON commençait à considérer toute l'étendue de cet écosystème en ligne et les menaces possibles auxquelles E.ON était exposé.

L'équipe d'E.ON a compris le besoin critique d'obtenir une image claire de ce vaste écosystème et était une exigence clé de la solution.

LA SOLUTION

Tout en recherchant des solutions pour soutenir cette initiative, E.ON a identifié la plate-forme de sécurité de l'écosystème de Cyberpion comme un candidat solide. L'exploration des capacités de Cyberpion comprenait une démonstration complète du produit Proof-of-Concept (PoC). La solution de Cyberpion est fournie sous la forme d'un portail Web SaaS et ne nécessite aucune installation, configuration ou modification de l'informatique existante d'E.ON. En raison de la vitesse à laquelle le PoC a été déployé, E.ON a pu obtenir immédiatement des informations précieuses et exploitables sur son écosystème en ligne.

EN UN COUP D'ŒIL

LE DÉFI

- Réduire le cyber-risque lié aux relations avec les fournisseurs et les partenaires N-partie

LA SOLUTION

- Obtenir une visibilité complète de la surface d'attaque externe, y compris son vaste réseau de partenaires et de fournisseurs

LE RESULTAT

- Réduction des frais généraux et des heures supplémentaires grâce à la découverte et au mappage automatisés des ressources informatiques et tierces
- Prévention des perturbations opérationnelles, des pertes de données et des attaques de rançongiciels grâce à l'identification, l'atténuation et la correction proactives des vulnérabilités

"Après avoir travaillé avec Cyberpion pendant plus d'un an, nous sommes convaincus que sa plate-forme Ecosystem Security nous donne la visibilité essentielle dont nous avons besoin pour résoudre le défi difficile de la gestion des risques et des vulnérabilités dans l'ensemble de notre offre numérique."

René Rindermann, CISO
E.ON

Deux des principales capacités de Cyberpion ont été identifiées comme des exigences de solution clés pour le projet d'E.ON.

Premièrement, la capacité de Cyberpion à découvrir et à inventorier en continu non seulement les actifs Internet d'E.ON et les actifs des fournisseurs directs sur lesquels il s'appuie, mais également les longues chaînes de quatrième, cinquième, etc. relations avec les fournisseurs et partenaires. Cela était essentiel pour comprendre son exposition totale au risque.

Une fois que la taille et la portée réelles de l'écosystème ont été comprises, E.ON a découvert une deuxième exigence de solution clé E.ON nécessaire : une méthode d'identification et de hiérarchisation des risques éventuels pour maximiser les ressources humaines dédiées à la protection et à la gestion de cette surface d'attaque.
La capacité de Cyberpion à combiner une évaluation multicouche des risques et des vulnérabilités des infrastructures Web, Cloud, DNS et PKI minimise les faux positifs et le bruit tout en priorisant les vulnérabilités les plus critiques. Les membres de l'équipe E.ON ont trouvé que les informations de Cyberpion ont amélioré leur efficacité, ainsi que leur efficacité.

Lorsqu'elles sont combinées, la capacité d'inventorier l'ensemble de la surface d'attaque et de présenter les données d'évaluation des risques dans un format exploitable a fait de Cyberpion la solution de choix pour E.ON.

LE RESULTAT

La plateforme Ecosystem Security de Cyberpion a permis à E.ON d'agir de manière préventive sur les vulnérabilités. En agissant avant que les pirates ne puissent exploiter ces vulnérabilités, E.ON a pu éviter des dommages importants en termes de dollars, de réputation de marque ou de confiance et fidélité des clients.

"L'approche de Cyberpion en matière de gestion de la surface d'attaque externe permet à mon équipe de passer à l'attaque. Nous sommes désormais en mesure de rechercher, de trouver et de corriger activement les menaces critiques de cet environnement numérique dynamique et vaste avant qu'elles n'affectent notre organisation et nos clients. ».”

René Rindermann, CISO
E.ON

Get started today.

US: +1 (917) 702-3850 | Intl: +972 33752005
sales@cyberpion.com | Learn more at cyberpion.com

Cyberpion™