Pourquoi votre entreprise a besoin de services SOC managés

Barracuda

Votre entreprise a-t-elle besoin de services SOC ?

L'amélioration de la cybersécurité tout en maîtrisant les coûts est un défi pour presque toutes les organisations. C'est pourquoi nombre d'entre elles se tournent vers un centre d'opérations de sécurité (SOC) managé.

Un SOC est une unité centralisée comprenant des experts en cybersécurité et des outils chargés de la surveillance 24/7, de la détection des menaces et de la réponse aux incidents pour améliorer la cyberdéfense d'une organisation. Les SOC utilisent des technologies de pointe et des processus normalisés pour protéger les actifs numériques, tout en garantissant la conformité avec les réglementations de sécurité en vigueur. La mise en œuvre d'un SOC offre une protection continue, une réponse rapide aux incidents et l'accès à une expertise spécialisée en cybersécurité, réduisant ainsi les coûts et améliorant la sécurité globale.

Le développement et la gestion d'un SOC efficace requièrent une expertise et des ressources qui dépassent les capacités de nombreuses entreprises. C'est pourquoi, faute de moyens, nombre de PME se passent de services SOC. La conséquence est un environnement moins sécurisé et une pression accrue sur les personnes chargées de la cybersécurité au sein de l'entreprise. Pour surmonter les défis liés à l'exploitation d'un SOC en interne, une alternative est apparue : les SOC managés. Un SOC managé externalise les tâches à un prestataire professionnel qui fournit des services de cybersécurité SOC moyennant des frais.

Ce que fournit un SOC

Le principal avantage d'un SOC est de procurer à votre entreprise une protection continue contre les cybermenaces, dont le nombre et la sophistication augmentent chaque jour. Sans SOC, votre entreprise est exposée à de nombreux risques :

- Détection tardive des menaces
- Temps de réponse aux menaces (TTR) plus long
- Manque de visibilité sur la sécurité
- Non-conformité aux réglementations
- Présence prolongée des cybercriminels après une violation
- Augmentation des coûts de récupération

Un SOC fournit une gamme complète de protections et d'informations sur les opérations informatiques et la posture de sécurité de votre organisation. Il offre une protection et une surveillance continues avec une couverture 24/7. En cas d'incident, un SOC lance une réponse aux incidents efficace, avec des équipes dédiées qui traitent toutes les menaces détectées. Les SOC ne se contentent pas de répondre aux incidents. Ils assurent une protection proactive, analysant les activités pour identifier les menaces éventuelles. Ils améliorent ainsi la protection contre les menaces et contribuent à empêcher les violations.

Pourquoi un SOC géré est le bon choix pour votre entreprise

Malgré ses nombreux avantages, le développement et la gestion d'un SOC en interne représentent un coût trop important pour la plupart des entreprises et nécessitent un niveau d'expertise qu'elles ne possèdent généralement pas. Pour autant, cela ne signifie pas que les avantages du SOC sont inaccessibles à votre entreprise.

Un SOC managé, qui implique d'externaliser les services SOC auprès d'un fournisseur spécialisé, peut offrir les avantages de l'exploitation d'un SOC interne, mais à une fraction du coût. L'utilisation d'un SOC permet également à l'entreprise d'augmenter son expertise en matière de sécurité. Les SOC peuvent assurer une défense en profondeur grâce aux diverses compétences en cybersécurité mises à disposition, notamment des intervenants en cas d'incident, des analystes, des chasseurs de menaces et des enquêteurs judiciaires.

Un SOC géré ne résout pas seulement le problème du coût. Pour de nombreuses entreprises, il est très difficile de combler le déficit de compétences en sécurité informatique. Le Forum économique mondial (WEF) estime qu'il manque environ quatre millions de professionnels de la cybersécurité. Il est difficile de recruter et de conserver du personnel qualifié, et les meilleurs éléments exigent des salaires élevés. Dans un contexte de pénurie mondiale de professionnels de la cybersécurité, un SOC managé permet aux entreprises d'accéder à des talents qui seraient autrement inaccessibles.

En plus d'éliminer les problèmes de personnel, un SOC managé permet d'accéder à des technologies avancées. Les SOC managés utilisent généralement les dernières technologies et solutions de sécurité qui sont maintenues à jour, ce que les équipes de sécurité internes peuvent avoir du mal à réaliser.

En plus de ses atouts dans le domaine de la sécurité, un SOC géré offre également des avantages commerciaux. Ainsi, un SOC managé évite les dépenses d'investissement dans la mise en place et la gestion d'un SOC en interne, remplacées par des frais de service. Le fournisseur de SOC managé est responsable du maintien des niveaux de personnel et prend à sa charge les coûts de licences logicielles. Tout est inclus en tant que dépenses d'exploitation, simplifiant ainsi la comptabilité. Le recours à un fournisseur de services managés qui propose des services SOC contribue à protéger l'entreprise contre les cybermenaces et à assurer le respect de ses obligations réglementaires.

Les capacités de surveillance d'un SOC managé peuvent aider à répondre aux exigences de conformité réglementaire, telles que le Règlement général sur la protection des données (RGPD), la loi californienne sur la protection de la vie privée des consommateurs (CCPA), la directive 2 sur les systèmes de réseaux et d'information (NIS2) et le règlement sur la résilience opérationnelle numérique (DORA), pour n'en citer que quelques-unes. Les fonctionnalités de journalisation d'un SOC simplifient les rapports de conformité. Ces capacités peuvent également améliorer la réputation d'une entreprise, car l'accès aux services fournis par un SOC managé démontre aux employés, aux clients et aux parties prenantes que cette organisation prend la sécurité et la confidentialité des données au sérieux. Bien qu'il ne s'agisse pas d'obligations de conformité, la confiance instaurée par un SOC peut renforcer les relations.

Découvrez comment Barracuda peut vous aider

Toutes les organisations peuvent bénéficier d'un SOC managé qui leur offre une protection permanente contre les cybermenaces. À ce titre, les clients de Barracuda bénéficient d'un accès simplifié à un service SOC managé et mature.

Tous les SOC ne se valent pas. Un SOC mature intègre une combinaison sans précédent de compétences complètes, de structures d'équipes diverses, de processus avancés et de technologies de pointe. Un SOC véritablement mature n'est pas seulement opérationnel ; il est également innovant. Il doit se composer de plusieurs équipes spécialisées opérationnelles en permanence, possédant une expertise approfondie en matière de sécurité offensive et défensive, d'automatisation et d'IA/ML. Ses membres doivent détenir des certifications d'élite et maîtriser la programmation afin d'automatiser la réponse aux menaces et la cartographie des runbooks. Il doit également être intégré à des systèmes et plateformes de pointe (SIEM, SOAR, Threat Intelligence) et à des capacités de détection avancées basées sur le ML. Un SOC innovant offre une cyberdéfense intelligente, agile et résiliente contre toutes les menaces, y compris les attaques zero-day. C'est là que Barracuda établit la référence en matière de fourniture de services de cybersécurité.

Barracuda propose un service de détection et de réponse étendues (XDR) complet et entièrement géré, dénommé Barracuda Managed XDR. Les entreprises clientes de Barracuda Managed XDR bénéficient automatiquement d'un accès 24 h/24, 7 j/7 et 365 j/an au SOC mondial de niveau expert de Barracuda. Ce SOC assure une surveillance des menaces en temps réel et des conseils proactifs fournis par cinq équipes dédiées d'experts en cybersécurité. Chaque équipe SOC travaille en arrière-plan pour fournir des services proactifs de détection et de réponse.

L'équipe rouge du SOC de Barracuda a développé des centaines de règles de détection, toutes conformes au framework standard MITRE ATT & CK, une base de connaissances complète sur les tactiques, techniques et procédures (TTP) des cybercriminels. L'équipe rouge et les autres équipes du SOC de Barracuda recherchent et développent en permanence de nouvelles détections de sécurité, permettant à Barracuda Managed XDR de garder une longueur d'avance sur le paysage en constante évolution des cybermenaces.

Pour en savoir plus sur Barracuda Managed XDR et accéder à un SOC mature doté de 5 équipes d'experts en cybersécurité, n'hésitez pas à nous contacter. Nous serons ravis de vous aider.

Barracuda en quelques mots

Barracuda est une entreprise de cybersécurité leader sur son marché, offrant aux entreprises de toutes tailles une protection complète face aux menaces complexes. Notre plateforme BarracudaONE, propulsée par l'IA, sécurise les emails, les données, les applications et les réseaux grâce à des solutions innovantes, un XDR managé et un tableau de bord centralisé afin de maximiser la protection et renforcer la résilience cyber. Des centaines de milliers d'organisations et de fournisseurs de services managés (MSP) du monde entier nous font confiance pour les protéger et les accompagner, avec des solutions faciles à acquérir, déployer et utiliser. Pour plus d'informations, visitez fr.barracuda.com.

Barracuda