Autres Services de Sécurité y Guider

Insight

Introduction

Tout le monde, des PDG aux membres du conseil d'administration en passant par les individus dans leur vie privée, reconnaît l'importance de la cybersécurité. Il est rare de passer une journée sans rencontrer l'actualité d'une grande marque ayant subi une faille de sécurité ou sans traiter un incident de phishing par e-mail. Internet est vital pour une grande partie de notre vie professionnelle et personnelle, et la nature mondiale d'Internet nous expose également à un ensemble mondial de risques.

Si le « coût de la cybercriminalité » était un pays, il aurait la troisième plus grande économie mondiale, derrière les États-Unis et la Chine seulement, à 9 tonnes $ en 2024[1].

Nous vivons à une époque marquée par la géopolitique et les guerres hybrides. Les conflits ne sont plus limités au champ de bataille : les États nationaux et les acteurs alignés sur l'État utilisent régulièrement la perturbation de notre monde numérique pour poursuivre leurs objectifs dans le monde réel. Les groupes criminels organisés sont devenus de haute technologie et se sont rendu compte qu'il y avait de grandes fortunes à gagner grâce aux attaques par rançongiciel, avec malheureusement peu de chances d'être poursuivis en justice.

Dans environ 45 % des cas cette année, les attaquants ont exfiltré des données en l'espace d'un jour de compromission[2].

L'environnement réglementaire n'a jamais été aussi strict : l'Union européenne a introduit des lois telles que NIS 2 et DORA qui obligent les organisations à améliorer leur cybersécurité.

Les organisations opérant dans cet environnement complexe, entre un paysage de menaces qui s'aggrave et des exigences réglementaires strictes, nous espérons que ce guide vous aidera à décomposer un peu le jargon et vous fournira un guide pragmatique sur la manière de naviguer dans cette période turbulente.

Pour les incidents non liés à l'extorsion en 2022 et 2023, le délai médian d'exfiltration des données est resté constamment inférieur à un jour, ce qui signifie que les défenseurs doivent réagir à une attaque de rançon en moins de 24 heures[3].

Le prix de l'inaction :

Ne pas investir dans une cybersécurité robuste peut avoir de graves conséquences :

- **Perte financière :** Les violations de données et les attaques par rançongiciel peuvent entraîner des amendes, des frais juridiques et une perte de revenus.
- **Atteinte à la réputation :** Un incident de sécurité peut éroder la confiance des clients et des parties prenantes.
- **Cookies opérationnels :** Les cyberattaques perturbent souvent les processus commerciaux, entraînant des retards et Améliorez la productivité.
- **Pénalités réglementaires :** La non-conformité à des cadres tels que la NIS2 ou le RGPD peut entraîner des amendes importantes.

Bien qu'il soit clair que sous-investir dans la sécurité comporte des risques évidents, surinvestir dans la sécurité ou investir dans les mauvais domaines est également mauvais pour l'entreprise. Une sécurité excessive peut frustrer les collaborateurs et les clients, sans parler du coût éventuel d'utiliser ce budget pour développer votre entreprise.

La sécurité est toujours un acte d'équilibre– dans le but d'obtenir une sécurité «juste assez» sans causer d'autres impacts sur votre entreprise.

Comprendre l'entreprise

Il existe une gamme étonnante d'acronymes utilisés par le secteur – le marketing des fournisseurs contribue fortement à la confusion. Il vaut la peine de connaître et de comprendre quelques-unes des plus courantes pour être sûr de parler la même langue avec les fournisseurs et les partenaires.

Technologie :

- **Détection et réponse des terminaux managés (MEDR) :** Se concentre sur l'identification et la réponse aux menaces sur les terminaux individuels (ordinateurs portables, serveurs, appareils mobiles) en fournissant des données forensiques détaillées et des outils de remédiation.
- **Network Detection and Response (NDR) :** est une approche de cybersécurité qui utilise des analyses avancées, l'apprentissage automatique et la détection comportementale pour surveiller le trafic réseau en temps réel, identifier les anomalies ou les menaces et fournir des insights exploitables pour atténuer les risques et améliorer les temps de réponse.
- **Détection et réponse étendues managées (MXDR) :** Va au-delà des terminaux, en intégrant des données provenant de multiples sources (réseau, messagerie, Cloud) pour une détection et un contexte plus larges des menaces.
- **Security Information and Event Management (SIEM) :** Collecte et analyse les journaux de l'ensemble de l'organisation pour identifier les activités suspectes. Parfait pour la conformité et la centralisation des données.
- **Ingestion:** Une voiture est inutile sans le bon type de carburant, et le SIEM est le même. Il a besoin d'être alimenté par les journaux de vos Asset IT existants, et la quantité de journaux que vous ingérez aura un impact sur le coût de la solution. Généralement mesuré en gigaoctets par jour ou en événements par seconde. (EPS).
- **Security Orchestration, Automation and Response (SOAR) :** désigne un ensemble d'outils et de processus qui permettent aux équipes de sécurité de rationaliser et d'automatiser les flux de travail de détection, d'investigation et de réponse aux menaces. En intégrant des systèmes de sécurité disparates

et en automatisant les tâches répétitives, SOAR améliore l'efficacité, réduit les temps de réponse et permet aux analystes de se concentrer sur activités à plus grande valeur ajoutée.

Personnes et processus :

- **Service de détection et de réponse managés :** Services de sécurité externalisés qui combinent la technologie (souvent SIEM ou XDR) avec une équipe d'experts chargée de la détection, de l'investigation et de la réponse.
- **Centre des opérations de sécurité :** Une équipe ou une installation centralisée responsable de la surveillance et de la réponse aux incidents de sécurité, soit en interne, soit managés par un fournisseur.

Comment cela fonctionne-t-il ?

Un service de sécurité managés se compose de personnes, de processus et de technologies. La technologie est cruciale pour pouvoir collecter toutes les données nécessaires pour fournir des insights aux personnes qui gèrent le service. Absolument L'exigence minimale est un outil EDR qui fournit des données sur ce qui se passe au niveau des terminaux. De nombreux éditeurs passent de l'EDR à l'XDR, qui inclut plus que les données des terminaux, pour fournir une vue plus large de l'ensemble de l'entreprise.

Les outils XDR sont parfaits pour détecter les incidents « à l'instant même », mais ils ont généralement une vision plus à court terme du monde. De nombreuses organisations choisissent d'augmenter la XDR avec une solution SIEM, qui conserve les données de journalisation brutes pendant une période prolongée, généralement un minimum de 90 jours, mais qui peut durer de nombreuses années. Un SIEM peut s'avérer nécessaire si votre organisation a besoin de s'aligner sur les exigences de conformité.

Les personnes et les éléments de processus proviennent généralement du fournisseur de services managés. Si vous avez déjà investi dans la technologie, vous aurez besoin d'un partenaire qui est compétent dans cette technologie et qui a développé de l'expérience, des règles et des détections basées sur ce fournisseur afin qu'il puisse fournir de la valeur immédiatement. Si vous n'avez pas encore investi dans la technologie, de nombreux partenaires se feront un plaisir de vous en suggérer une.

Si vous avez décidé d'utiliser un partenaire pour la sécurité managée, assurez-vous d'acheter un résultat. Si la technologie est un leader éprouvé du marché, il est plus important de sélectionner un partenaire sur le service qu'il propose et sur la façon dont il peut répondre à vos besoins de sécurité. Concentrez-vous sur la manière dont vous travaillerez ensemble pour améliorer la sécurité et laissez le partenaire s'inquiéter la bonne technologie.

SIEM vs XDR: Quelle est la différence?

Bien que les systèmes SIEM et XDR soient des technologies fondamentales en matière de cybersécurité, ils ont des objectifs différents:

CARACTÉRISTIQUES	SIEM	XDR
Principales fonctions	Agrége et analyse les journaux pour la conformité et la détection des menaces.	Détection unifiée des menaces sur plusieurs vecteurs avec des réponses automatisées.
ID déploiement	Nécessite généralement une configuration et une maintenance internes.	Livrés sous forme de services managés complets ou de plateforme de logiciel.
Scope	Large et flexible, support d'intégrations personnalisées.	Périmètre plus étroit mais intégration plus profonde entre les outils pris en support.
Exemples d'utilisation	Idéal pour les organisations axées sur la conformité disposant d'une expertise existante.	Idéal pour les entreprises à la recherche d'une détection et d'une réponse simplifiées et intégrées.

Les deux ont leurs points forts. De nombreuses organisations associent les capacités de conformité d'un SIEM à la détection avancée des menaces d'XDR pour couvrir toutes les bases.

L'argumentaire commercial pour la sécurité managée

Il y a quelques décennies, de nombreuses organisations n'envisageaient pas du tout la sécurité. Alors que les premières cybermenaces survenaient, les entreprises ont commencé à investir dans des antivirus, des pare-feu et d'autres contrôles de sécurité basiques pour les protéger. La «personne chargée de la sécurité» gérait ces contrôles et les choses étaient simples. Cependant, l'augmentation des menaces a entraîné un investissement accru dans de nouveaux contrôles. Le «gars de la sécurité» devient une équipe de sécurité, chaque membre ayant un ensemble de compétences différent. La sécurisation des données, des applications, de l'infrastructure, du cloud et des systèmes d'IA nécessite tous un ensemble de compétences différent, et tous ces ensembles de compétences différents doivent être managés de manière cohérente pour garantir une couverture de sécurité de bout en bout.

Le coût et la complexité de la gestion de la sécurité en interne constituent un obstacle à l'entrée pour beaucoup. Vous pouvez également vous associer à un fournisseur de services de sécurité managés.

ASPECT	SOC interne	Partenaire MSSP
Imputation	Coûts initiaux élevés pour l'infrastructure, les outils et la location.	Réduction des coûts initiaux et des coûts de service continus grâce au paiement d'un ETP fractionné.
Compétences	Nécessite l'embauche et la rétention de professionnels hautement qualifiés.	Accès à un large éventail d'expertises sans recrutement.
L'Évolutivité	L'évolutivité nécessite des investissements supplémentaires en ressources, collaborateurs et infrastructure.	Facilement évolutif avec l'infrastructure existante du MSSP.
Couverture 24/7	Coûteux et complexe à réaliser avec les collaborateurs internes. A besoin d'au moins 12 personnes pour couvrir en permanence.	Généralement inclus dans le service.

ASPECT	SOC interne	Partenaire MSSP
Contrôle	Contrôle total des opérations SOC, des personnalisations et de la priorisation.	Contrôle limité, avec une certaine dépendance vis-à-vis des processus et de la priorisation du MSSP.
Feuille de route de la mise en œuvre	Plus long en raison de la configuration, de la location et de la configuration.	Configuration plus rapide, car les MSSP ont souvent des solutions et des processus préconçus.
Mises à jour de la technologie	L'organisation est responsable de se tenir au courant des outils et des technologies.	Les MSSP fournissent un accès aux outils et technologies les plus récents dans le cadre du service.
Conformité et gouvernance	Responsabilité totale de la réunion des exigences réglementaires et de conformité.	Les MSSP fournissent généralement des services alignés sur les exigences de conformité, mais peuvent ne pas couvrir les nuances spécifiques à l'organisation.
Intelligence des données	Nécessite la création ou l'abonnement à des flux de renseignements sur les menaces de manière indépendante.	Accès à des informations agrégées sur les menaces provenant de plusieurs clients/clientes.
Personnalisation	Hautement personnalisable en fonction des besoins et des flux de travail spécifiques de l'organisation.	Les offres standardisées peuvent ne pas s'aligner entièrement sur des exigences uniques.
Connaissance du contexte commercial	Solide compréhension de la structure organisationnelle, des priorités et du contexte.	Compréhension limitée de l'environnement spécifique de l'organisation.
Collaboration accrue	Il est plus facile d'aligner les opérations du SOC avec les équipes informatiques et de sécurité internes.	Nécessite plus de coordination entre l'organisation et le MSSP.

Quels sont les coûts liés à la mise en place d'une équipe interne?

La mise en place d'un centre d'opérations de sécurité (SOC) interne nécessite une planification financière minutieuse, car plusieurs facteurs de coûts doivent être pris en compte:

1. Coûts collaborateurs
- Analystes SOC: Supposons un minimum absolu de deux analystes par équipe pour maintenir une couverture 24/7, en tenant compte des maladies, des congés et de la prévention du burn-out.
- Ingénieurs sécurité: Au moins deux ingénieurs dédiés pour construire, gérer et mettre à jour les outils SOC Construire une infrastructure;
- Rôles spécialisés: Envisagez d'ajouter des intervenants en cas d'incident, des chasseurs de menaces et un responsable SOC pour vous assurer que l'équipe fonctionne efficacement.
- Formation et certification: Formation continue pour tenir l'équipe informée de l'évolution des menaces, des outils et des exigences de conformité.

2. Coûts SIEM (Security Information and Event Management)
- Frais de licensing et d'abonnement: Les coûts sont souvent basés sur le volume de données de journalisation ingérées.
- Infrastructure: L'hébergement du SIEM sur site ou dans le cloud peut entraîner des coûts supplémentaires pour les serveurs, le stockage et la bande passante.
- Alternatives open source: Bien qu'il existe des plateformes gratuites, elles peuvent nécessiter des investissements substantiels dans du personnel qualifié ou des conseils externes pour la configuration, la maintenance et le réglage.

3. Coûts des renseignements sur les menaces
- Abonnements Accès payant aux flux de renseignements sur les menaces pour l'enrichissement des données et la contextualisation des alertes.
- Intégration Coûts supplémentaires pour intégrer des plateformes de renseignements sur les menaces dans votre écosystème existant.

4. Coûts de détection et de réponse des terminaux (EDR/XDR)
- Licences outils: Licences de détection et de réponse aux menaces sur les terminaux, les réseaux et autres actifs.
- Coûts d'échelle: Échelle des coûts basée sur le nombre d'appareils ou d'actifs surveillés.

5. Renforcer son infrastructure
- Matériel informatique et logiciel: Serveurs, appareils de stockage et logiciels pour la collecte, l'analyse et le stockage des journaux.
- Redondance et reprise après sinistre: Systèmes de sauvegarde et plans de reprise après sinistre pour les opérations SOC.
- Encombrement: Sécuriser l'espace de bureau ou une salle d'opération dédiée avec des contrôles environnementaux appropriés.

6. Outils de surveillance et de détection
- Outils de surveillance du trafic réseau, d'analyse comportementale et de systèmes de détection d'intrusion (IDS/IPS).
- Mises à jour et ajustements réguliers pour garantir l'efficacité contre les menaces en constante évolution.

7. Réponse aux incidents (IR)
- Développement du guide opérationnel : Temps et ressources pour développer des processus et des flux de travail détaillés de réponse aux incidents.
- Outils forensiques: Outils spécialisés pour des enquêtes approfondies sur les violations ou les activités suspectes.

8. Coûts de conformité et de réglementation
- Garantir le respect des standards industriels (par exemple, ISO27001, NIS2, PCI DSS) peuvent nécessiter des investissements supplémentaires dans les outils, l'audit et l'expertise.
- Assessments et audits périodiques pour vérifier la conformité.

9. Évaluation de la vulnérabilité
- Outils d'analyse et de management des vulnérabilités dans votre environnement informatique.
- Temps de collaborateurs ou conseils pour le patch management et les efforts de remédiation.

10. Licensing pour les plateformes de sécurité
- Frais de licensing supplémentaires pour DLP (Data Loss Prevention), outils de sécurité cloud ou pare-feu intégrés à } **OPÉRATIONS SAM**

11. Coûts de test et d'optimisation
- Tests de pénétration Tests réguliers des processus et des défenses SOC pour identifier les lacunes.
- Exercices Red Team/Blue Team: Exercices de formation pour améliorer la préparation du SOC et affiner l'incident capacités de réponse.

12. Intégration aux systèmes informatiques existants
- Coûts d'intégration des outils SOC avec les systèmes de management informatique tels qu'Active Directory, systèmes de ticketing et plateformes ITSM.

13. Maintenance et mises à jour continues
- Mises à jour régulières du logiciel, correctifs et ajustements de la configuration.
- Remplacement au fil du temps du matériel informatique ou des logiciels obsolètes.

14. Conseils et partenariats avec des tiers
- Coûts à court terme pour des consultants spécialisés pour aider à la configuration initiale ou à des tâches complexes.
- Partenariats potentiels avec les fournisseurs pour le support et la cogestion au cours des premières étapes opérationnelles.

15. Coûts cachés et indirects
- Optimiser les investissements Temps considérable requis pour configurer, ajuster et optimiser l'état de charge avant qu'il ne soit entièrement opérationnel.
- Coûts d'opportunité: Temps et ressources détournés d'autres projets informatiques et de sécurité.

Quels sont les coûts liés au partenariat avec un MSSP?

Comme le fournisseur a déjà investi dans tous les éléments ci-dessus, vous payerez une partie de ces coûts, généralement en fonction de votre consommation. L'avantage pour vous est que vous ne paierez pas pour toute une équipe qui sera sous-utilisée, mais que vous aurez accès à toute une équipe lorsqu'elle sera nécessaire.

Les fournisseurs de services de sécurité managés typiques factureront un service sur la base d'une combinaison des éléments suivants:

- **Nombre d'utilisateurs :** bien sûr, plus il y a d'utilisateurs– l'hypothèse est qu'il y aura plus d'incidents à gérer.
- **Nombre de terminaux :** de nos jours, les utilisateurs ont souvent plusieurs terminaux et les serveurs sont également essentiels à surveiller.
- **Volume de données de journalisation :** Certaines petites organisations génèrent beaucoup de données, tandis que d'autres grandes organisations peuvent avoir une infrastructure assez simple. En examinant la quantité de données de journal que vous génèrez, les MSSP peuvent supposer le niveau de réponse aux incidents qui sera requis.

Bien que vous connaissiez probablement le nombre d'utilisateurs et de terminaux, à moins que vous n'ayez déjà un SIEM ou un SOC, le volume de données de journalisation peut ne pas être connu. Un bon partenaire vous aidera à estimer cela en fonction de la quantité et des types d'appareils que vous avez dans votre parc ; ce travail est généralement effectué gratuitement dans le cadre de l'engagement de prévente.

Le prestataire peut proposer un paiement initial pour couvrir les travaux de conseil nécessaires à la mise en place du service, suivi d'une redevance mensuelle– ou il peut combiner les deux en un seul Frais mensuels. Dans l'idéal, ils pourront travailler avec l'un ou l'autre, selon vos préférences.

Des coûts peuvent être associés à la licence de la plateforme SIEM elle-même. Cela peut être inclus dans les frais mensuels ou payé séparément à un fournisseur SaaS comme Microsoft ou Cisco. Le partenaire doit indiquer clairement si des frais supplémentaires sont payables à des tiers et doit les estimer pour que vous fournissiez un prix total.

SLA et reporting: La base du service

Un accord de niveau de service (SLA) définit les attentes, les responsabilités et les indicateurs de performance entre vous et votre fournisseur de sécurité managés. Un SLA solide assure la clarté, la responsabilité et l'alignement sur vos besoins commerciaux, mais tous les SLA ne sont pas créés de la même manière.

- **Temps moyen de détection:** combien de temps s'écoule entre la survenance d'un incident et sa détection par le SOC? Avec les plateformes SIEM modernes, la détection doit être quasiment en temps réel. Cependant, la détection d'un incident dépend de la configuration de la plateforme, des sources de journaux ingérées et de la qualité des règles. Il est difficile de comparer directement les SLA à ce niveau.

- **Temps de réponse moyen:** Une fois qu'un incident est détecté, à quelle vitesse le SOC réagit-il? Bien que cette mesure soit souvent la plus importante, elle n'est pas aussi simple que de chercher le partenaire le plus rapide... (voir l'intitulé «À quoi ressemble un bon SLA»)

- **Temps moyen de remédiation:** Combien de temps faut-il entre la réponse et la résolution du problème? Il existe un large éventail de types d'incidents et de complexités– donc, une fois de plus, ce nombre est difficile à comparer. De plus, certaines activités de correction peuvent nécessiter que votre équipe informatique interne ou un tiers les résolve– les MSSP excluent ces moments de ce SLA.

À quoi ressemble un bon SLA

Un SLA bien conçu équilibre performance et praticité. Rechercher:

- **Priorisation basée sur les risques:** Priorité plus élevée pour les incidents critiques et priorité plus faible pour les problèmes mineurs.

- **Indicateurs transparents:** Définitions claires des temps de réponse et de résolution avec des résultats mesurables.

- **Calendrier réaliste:** À la surface, un temps de réponse de 5 minutes peut sembler meilleur qu'un temps de réponse de 30 minutes. Mais qu'est-ce qu'une «réponse»? Souhaitez-vous vraiment être appelé à 3 heures du matin chaque soir parce qu'un partenaire donne la priorité à son SLA plutôt qu'à la suppression des faux positifs? Vous payez le partenaire pour trier et confirmer les vrais positifs– pas seulement pour vous transmettre chaque alerte du SIEM directement.

Les SLA sont la base de la confiance entre vous et votre fournisseur. Un bon SLA ne promet pas seulement de la rapidité, il garantit la qualité, la responsabilisation et l'alignement sur vos objectifs commerciaux.s.

Reporting

Vous rencontrerez généralement deux types de rapports. Rapports «ad hoc» qui sont générés lorsqu'un incident est détecté et vous est notifié. Ils sont destinés à la communication rapide d'un problème– généralement quelque chose qui nécessite votre intervention ou une notification en temps opportun.
Toutefois, le MSSP ne doit pas uniquement contacter en cas de problème. Il doit y avoir une cadence régulière de réunions, à la fois avec les parties prenantes techniques et commerciales, couvrant des sujets tels que:

- **Couverture de la source du journal:** Ta qualité du service dépend des journaux auxquels il a accès. Le fournisseur utilise-t-il un cadre tel que MITRE ATT&CK pour vous conseiller sur les sources de journaux supplémentaires qui pourraient ajouter de la valeur?
- **Performance par rapport au SLA:** L'occasion d'examiner les performances du service par rapport au SLA et de mettre en place des plans correctifs si nécessaire.
- **Revue des incidents précédents:** Rétrospective sur certains des incidents les plus graves– qu'est-ce qui s'est bien passé et qu'est-ce qui pourrait être amélioré?
- **Une vision plus large:** le monde ne s'arrête pas– votre organisation évoluera au fil du temps, tout comme le paysage des menaces. Vous devriez avoir l'occasion d'informer régulièrement le fournisseur de tout changement commercial (par ex. fusions et acquisitions) qui pourrait avoir un impact sur le service, et pour que le fournisseur fournisse des perspectives sur les nouvelles menaces et solutions.

Capacités à rechercher dans un partenaire de sécurité managés

L'Automatisation et l'IA

Les menaces modernes nécessitent une détection et une réponse rapides. Les fournisseurs doivent tirer parti de l'automatisation et de l'IA pour:

- Identifiez les anomalies en temps réel, ce qui réduit la dépendance à l'égard de l'analyse manuelle.
- Rationalisez les flux de travail de réponse aux incidents, en garantissant un confinement rapide.
- Peut automatiser des actions courantes telles que l'isolement d'un appareil ou le verrouillage d'un compte compromis. C'est particulièrement important si vous souhaitez que le partenaire puisse agir en votre nom en dehors des heures d'ouverture.

Intelligence des données

Les informations exploitables sur les menaces vous aident à garder une longueur d'avance sur l'évolution des risques. Recherchez des fournisseurs qui:

- Maintenir à jour les flux de menaces et les intégrer à leurs services.
- Partagez des analyses sur les nouvelles tendances d'attaque pertinentes pour votre secteur.
- Utilisez l'intelligence pour améliorer la détection et hiérarchiser les menaces critiques.ts.

Recherche de menaces:

La recherche proactive des menaces garantit que les menaces ne passent pas inaperçues. Évaluer si le prestataire:

- Offre des activités de chasse aux menaces manuelles régulières.
- Utilise des outils avancés pour identifier les risques cachés.
- Fournit des rapports détaillés sur les résultats et les étapes d'atténuation.

Les alertes ne font qu'une partie de l'équation:

La correction efficace est essentielle. Assurez-vous que le fournisseur:

- Fournit des conseils clairs sur les stratégies de confinement.
- Possède des capacités de conseil pour vous aider à mettre en œuvre des projets plus importants afin d'améliorer la maturité de la sécurité.

Aspects pratiques

Nos certifications

Tout partenaire sera en mesure de vous montrer des supports marketing épurés, mais quelle validation externe peut-il fournir pour soutenir l'efficacité de leur service?

- Recherchez une validation externe impartiale auprès de sources telles que MSSP Alert : www.msspalert.com/top-250

- Vérifiez s'ils sont accrédités auprès du fournisseur de leur choix. Vous voulez vous assurer qu'ils sont experts dans leur ensemble d'outils et que leur service a été vérifié par le fournisseur. Cela indique également ils travailleront en étroite collaboration avec le fournisseur sur les améliorations et auront une bonne relation avec leur équipe d'ingénieurs.

- Vérifiez les cadres de conformité pertinents dans votre région ou votre secteur. Des certificats tels que Cyber Essentials+ et ISO27001 indiquent que l'organisation prend sa propre sécurité au sérieux et qu'il doit s'agir d'une exigence minimale pour un fournisseur de sécurité.

Processus d'intégration faciles

Vous devez vous attendre à ce qu'un bon partenaire vous guide tout au long du processus d'intégration. Les étapes de haut niveau impliquées sont reprises dans le tableau ci-dessous. Alors que le partenaire doit effectuer le levage lourd, il est important d'être conscient de toute dépendance vis-à-vis de vos collaborateurs afin que vous puissiez le planifier.

Quoi?	Votre implication
Scoping et découverte: Pour pouvoir fournir une solution appropriée, le partenaire devra poser de nombreuses questions sur vos aspirations en matière de service et votre pile technologique actuelle.	Vous devez vous attendre à impliquer plusieurs parties prenantes pour pouvoir donner un aperçu de la composition et de la taille de votre patrimoine. Connaître le nombre d'appareils terminaux et la marque, le modèle et la quantité de pare-feu, de services cloud et d'autres actifs vous aidera à vous assurer que la conception répond à vos besoins.
Construction de la plateforme: Si un outil SIEM doit être déployé ou si XDR a besoin d'être déployé sur l'ensemble de votre parc, vous devrez vous impliquer pour minimiser les perturbations pour les utilisateurs.	Votre équipe informatique peut avoir besoin de fournir un accès à votre environnement cloud pour que le partenaire déploie le SIEM. Vous devez vous attendre à travailler avec le partenaire pour créer un plan commun sur la manière et le moment de déploiement des agents des terminaux.
Personnalisation: Tout bon partenaire disposera d'un ensemble de règles par défaut qui fonctionnent pour détecter les incidents pour la plupart des organisations. Mais si vous avez des personnalisations spécifiques dont vous avez besoin, vous devrez travailler avec le partenaire pour vous assurer que ces exigences sont prises en compte.	Si vous avez des règles existantes dans un ancien système qui doivent être réécrites, leur mise à disposition peut entraîner une intégration plus rapide que de recommencer de zéro. S'il s'agit de nouvelles exigences, documenter celles-ci en langage naturel peut aider à communiquer vos besoins au partenaire.
Support précoce: Une fois que le service sera opérationnel, il y aura une période de réglage supplémentaire pour réduire les faux positifs et ajuster le système à votre environnement spécifique.	Vous devrez fournir une carte de contact pour savoir qui doit être notifié en cas d'incident de sécurité. Il pourrait s'agir d'une liste de distribution unique pour les petites organisations, mais cela aurait pu ajouter de la complexité, comme des chemins d'escalade différents pendant ou en dehors des heures de bureau, ou des groupes de résolution spécifiques pour les problèmes avec une certaine technologie. Cela peut même inclure des tiers pour lesquels vous avez externalisé certaines opérations.
Opérations IT: Une fois le support précoce terminé, la solution passera à l'état stable. Le travail de personnalisation du partenaire ne s'arrête pas à ce stade, mais devrait ralentir considérablement au fur et à mesure que l'accent est mis sur la détection des incidents.	You will need to provide a contact map for who should be notified when a security incident occurs. This could be a single distribution list for smaller organisations but could have added complexity like different escalation paths in or out of business hours, or specific resolver groups for issues with certain technology. This could even include third parties where you have outsourced some operations.

Services à valeur ajoutée

Bien que votre principale préoccupation lors de la recherche d'un fournisseur de sécurité managée soit de vous aider à détecter et à corriger les incidents de sécurité, il existe souvent d'autres services qui conviennent naturellement à un fournisseur de sécurité managée, et il vaut la peine d'examiner si l'un d'entre eux pourrait vous être utile– et pourrait être intégré en même temps. Il est souvent avantageux d'avoir plusieurs services fournis par le même partenaire, car ils auront une visibilité plus large de votre sécurité et pourront souvent prendre des décisions plus éclairées.

La gestion des vulnérabilités est un compagnon naturel d'un SOC, qui identifie, évalue et hiérarchise de manière proactive les failles de sécurité dans l'environnement numérique d'une organisation. En intégrant ce service, les organisations bénéficient d'une surveillance continue des vulnérabilités et de plans de correction actionnables qui s'alignent sur les capacités de détection des menaces du SOC. Cela réduit le risque d'exploitation en comblant les failles de sécurité avant que les attaquants ne puissent les exploiter.

Les services de protection contre les risques numériques (DRPS) offrent un autre ajout stratégique, étendant la portée du SOC au-delà du réseau de l'entreprise dans le paysage numérique plus large. Le DRPS surveille les menaces dans les environnements externes tels que le dark web, les réseaux sociaux et les systèmes externes. En identifiant l'usurpation d'identité de marque, les fuites d'identifiants ou les données sensibles exposées, les entreprises peuvent obtenir des avertissements précoces sur les menaces potentielles, ce qui permet au SOC de réagir rapidement et d'atténuer les risques.

Pour les organisations confrontées à des menaces actives ou à des violations, la fusion de la forensique numérique et de la réponse aux incidents (DFIR) avec la sécurité managée garantit un confinement rapide et une analyse détaillée post-incident. Les équipes DFIR peuvent tirer parti la télémétrie et les journaux du SOC pour enquêter sur les causes profondes, évaluer l'étendue de la violation et recommander des étapes de récupération. Cette approche holistique permet aux entreprises de réagir de manière décisive tout en acquérant des rapports pour prévenir la récurrence. Le regroupement de ces services crée une solution de sécurité harmonieuse et de.

Étapes suivantes

Les menaces à la cybersécurité augmentent et le coût de ne rien faire est élevé. N'attendez pas que cette violation se produise, contactez Insight, un MSSP de premier plan, et découvrez comment nos services de sécurité managés peuvent vous aider à protéger votre entreprise de manière rentable.

- **fr.insight.com**
- **0130672500**

[1] source: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[2] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[3] source: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report