LOGPOINT

Automatisation et Intégration des MSSP

www.logpoint.com

SOMMAIRE

PRÉSENTATION

Il n'est pas surprenant, dans le marché actuel, que les Fournisseurs de Services de Sécurité Gérés (MSSP) soient soumis à de nombreuses pressions. Ces sujets ont été au premier plan depuis un certain temps alors que la course aux armements cybernétiques se poursuit.

1. **Augmentation des menaces cybernétiques:** Alors que le nombre et la sophistication des menaces cybernétiques continuent d'augmenter, les fournisseurs de services de sécurité gérée (MSSP) sont sous pression pour fournir des solutions de sécurité efficaces et complètes à leurs clients. Les MSSP doivent suivre les dernières menaces et technologies afin d'offrir la meilleure protection possible à leurs clients.
2. **Rentabilité:** Les organisations recherchent des solutions de sécurité rentables qui peuvent offrir une protection maximale pour leurs données sensibles et leurs systèmes. Les MSSP sont sous pression pour fournir des services de sécurité abordables sans compromettre la qualité de la protection.
3. **Exigences de conformité:** De nombreuses organisations doivent se conformer à diverses réglementations et normes, telles que NIS2, RGPD, HIPAA et PCI-DSS. Les MSSP se doivent de fournir des solutions qui respectent ces réglementations et normes pour aider leurs clients à rester conformes.
4. **Pénurie de talents:** Il y a une pénurie de professionnels qualifiés en cybersécurité sur le marché, ce qui rend difficile pour les MSSP de trouver et de conserver les meilleurs talents . Les MSSP se doivent de construire une équipe solide et développer des solutions innovantes pour relever ce défi.
5. **Attentes des clients:** À mesure que les menaces en cybersécurité deviennent plus complexes, les clients s'attendent à ce que les MSSP fournissent des solutions plus avancées et sophistiquées. Les MSSP sont contraint d'innover constamment et d'améliorer leurs services afin de répondre à ces attentes.

Bien que ce ne soit pas un nouveau défi, la gestion de la complexité croissante des menaces en cybersécurité est devenue plus difficile avec des approches traditionnelles de superposition d'outils et de services cloisonnés. Au lieu de cela, une approche basée sur l'écosystème pour la sécurisation devient de plus en plus favorable. Le défi sous-jacent consiste à faire plus avec moins, et en réponse, Logpoint a réalisé une enquête pour comprendre comment les MSSP s'adaptent à ce besoin et transforment numériquement leurs services via l'intégration, l'automatisation et l'orchestration, qui jouent tous un rôle clé dans cette énigme.

Ainsi, les défis actuels auxquels les clients sont confrontés pour répondre efficacement à ces demandes évolutives exigent que le marché des MSSP se réinvente. De nombreuses organisations dépendent encore des technologies de gestion cloisonnées traditionnelles, mais l'adoption d'une approche plus avancée capable de protéger efficacement contre les attaques sophistiquées qui exploitent les éventuelles failles dans les mesures de sécurité devient inévitable

- **Compétences & Connaissances**
- **Temps & Ressources**
- **Stratégie d'Implémentation**
- **Technologie Implémentée**

L'efficacité de toute grande entreprise dépend fortement de la rapidité à laquelle les tâches nécessaires sont traitées. Celles-ci concernent inévitablement plusieurs départements, reposent à la fois sur des processus manuels et automatisés, et dépendent à la fois de l'exactitude et de la rapidité avec lesquelles les données peuvent être échangées. L'efficacité opérationnelle dépend donc des flux de processus pour toutes ces différentes activités. L'idée clé est qu'il existe de nombreuses voies de communication, chacune présentant des caractéristiques variées, contextuelles selon la situation et sensibles au temps.

- **65 % déclarent que les opérations du SOC** (Centre des Opérations de Sécurité) peuvent être chronophages en raison de procédures inefficaces.
- **57% déclarent que l'écart entre** le temps moyen de détection et le temps moyen de réponse est inférieur aux objectifs fixés
- **35 % déclarent ne pas disposer** des meilleurs processus ou outils pour élaborer des schémas de détection des menaces émergentes

UN SCÉNARIO

1. **Nous avons un directeur des opérations, travailleur, concentré et efficace**
2. **Nous avons aussi un directeur des opérations en back-office tout aussi travailleur et méticuleux.**

Sur la base des commandes passées, (2.) travaille sur une base cyclique en sachant la quantité et la fréquence à laquelle les ingrédients doivent arriver pour (1.) Ces ingrédients seront stockés, manipulés de manière appropriée et finalement transformés pour créer leur produit final.

Pour simplifier, ce sont les seules deux unités d'affaires que nous considérons du point de vue de l'interaction. Supposons qu'un acheteur effectue un paiement et récupère son produit dès qu'il est prêt, dans la quantité souhaitée et disponible.

Jusqu'à présent, tout est parfaitement logique, mais les systèmes sont rarement aussi simples.

Imaginons maintenant un scénario sur une année d'exploitation avec comme éléments :

- La production s'arrête lorsque le stock d'ingrédients est épuisé
- Au sein de l'entreprise de production, (1.) ne parle pas à (2.).
- (1.) cesse de recevoir régulièrement un ensemble d'ingrédients dans des quantités parfaites.
- (2.) fait quelques substitutions d'ingrédients

Maintenant, imaginez tous les scénarios compliqués qui pourraient leur être lancés, qu'il s'agisse d'activités externes, de défaillances internes, de problèmes cumulés et de situations improbables mais plausibles.

Ont-ils été suffisamment mis au défi et ont-ils eu assez de raisons pour exiger du changement ?

IMPACTS

Le point ici est qu'un processus cyclique, susceptible de changer avec le temps, et ayant également des activités environnantes dépendantes de certaines de ses activités ou informations, n'est pas une solution durable ;

Si un processus n'est pas conçu pour être adaptable et flexible face aux changements qui surviennent, il peut devenir obsolète ou inefficace, entraînant des perturbations dans les activités qui en dépendent, telles que :

- **Des décisions prises sur des hypothèses plutôt que sur des faits ;**
- **Des décisions non prises en temps opportun en raison d'un manque d'exposition à des défis ;**
- **Une absence de vision sur les tendances négatives pour éviter les problèmes avant qu'ils ne deviennent critiques ;**
- **Une chaîne de processus fragmentée entraînant des pertes opérationnelles ;**
- **Une méconnaissance des changements environnants dans le processus qui ont un impact sur les procédures ;**
- **Une pression excessive et des attentes non satisfaites sur chacun des processus isolés.**

Malheureusement, de nombreuses organisations fonctionnent avec une logique cloisonnée dans leur gestion de l'infrastructure, où les outils ne communiquent pas directement les uns avec les autres. Des opérations de chaise pivotante et des interactions humaines sont utilisées pour relever ce défi, ce qui repose fortement sur des processus documentés et de l'expérience, rendant difficile l'imposition ou la régulation de la cohérence dans l'échange de données.

Comme dans de nombreuses expériences de la vie, il y a une tendance à négliger le temps consacré à la réflexion aux scénarios d'échec, et en mettant l'accent sur les activités réussies. Cela amène à réfléchir à une célèbre question philosophique :

"Si un arbre tombe dans une forêt et qu'il n'y a personne pour l'entendre, fait-il un bruit ?" est souvent utilisée pour discuter de la nature de la réalité et de la perception, mais elle soulève également la question pertinente de savoir si notre approche de la planification et de la prise de décision inclut la capacité de détecter les échecs. Nous avons tendance à négliger la possibilité d'échec et ses conséquences potentielles. En omettant de considérer les scénarios d'échec, nous risquons de nous exposer à des déceptions, voire à des désastres, car nous ne sommes pas suffisamment préparés à faire face à des résultats inattendus.

Il est important de se rappeler que l'échec fait naturellement partie du processus d'apprentissage, et c'est grâce à l'échec que nous pouvons acquérir des enseignements précieux et améliorer nos compétences en prise de décision. En prenant le temps de considérer les scénarios d'échec et de les planifier, nous pouvons atténuer les risques et accroître les chances de succès. De cette manière, nous pouvons aborder nos activités et projets avec une perspective plus équilibrée et réaliste, en reconnaissant la possibilité d'échec tout en aspirant toujours à la réussite.

Reconnaître cette logique conduit à une nouvelle éthique où des mécanismes de rétroaction proactive existe pour introduire un processus évolutif plutôt qu'un schéma statique.

RÉSULTAT

La logique simple pour faire face à cette situation est de :

• Créer une culture conversationnelle pour résoudre les problèmes de manière individuelle, en combinant connaissances et expériences au bon moment pour résoudre un ou plusieurs petits problèmes afin d'éviter les impacts importants.

• Mettre en place une structure de collecte, de validation, d'analyse et de correction pour une visibilité complète de l'information.

Ce défi de logique simple n'est pas très différent de la façon dont les organisations gèrent leurs outils de gestion pour leur architecture informatique et leur sécurité grâce à l'automatisation et à l'orchestration.

- L'automatisation fait référence à l'utilisation de la technologie pour automatiser des tâches répétitives et routinières. Cela implique l'utilisation de logiciels et de matériels pour effectuer des tâches qui nécessiteraient sinon l'intervention humaine. L'automatisation est généralement utilisée pour accroître l'efficacité, réduire les erreurs et améliorer la fiabilité d'un système.
- L'orchestration, quant à elle, désigne la coordination et la gestion de plusieurs systèmes et processus automatisés pour atteindre un résultat souhaité. L'orchestration implique l'utilisation d'un système ou d'une plate-forme centralisée pour gérer et automatiser des flux de travail complexes impliquant plusieurs systèmes, applications et sources de données. Elle nécessite généralement l'utilisation d'API (interfaces de programmation d'applications) et d'autres outils d'intégration pour connecter différents systèmes et permettre la communication et l'échange de données entre eux.

En résumé, l'automatisation se concentre sur l'automatisation de tâches ou de processus individuels, tandis que l'orchestration se concentre sur la gestion et l'automatisation de flux de travail complexes impliquant plusieurs systèmes et processus. Alors que l'automatisation est utile pour améliorer l'efficacité et réduire les erreurs dans les tâches individuelles, l'orchestration est essentielle pour gérer et optimiser de grands systèmes complexes impliquant plusieurs composants automatisés.

QUELLE AUTOMATISATION DEVRAIT-ON VISER ?

Les outils de gestion et leurs fournisseurs offrent de plus en plus de capacités sous la pression du marché, ce qui a abouti à la mise en place d'API documentées. Dans le monde de l'informatique, de nombreuses choses sont cycliques à mesure que les technologies progressent et approfondissent leurs capacités, nous avons vu des basculements entre :

- **La centralisation et la décentralisation.**
- **Les terminaux et les utilisateurs finaux.**

Ce que nous observons maintenant est le plus grand arc de ces tendances. Au cours des premières années des réseaux, les spécialistes de l'informatique bricolaient des solutions en combinant :

- **Leur connaissance d'un défi ou d'un moyen d'optimiser une activité**
- **Leur intérêt pour regrouper des données provenant de plateformes très différentes pour obtenir de meilleures perspectives.**
- **Leur compréhension des composants à un niveau très profond de fonctionnement interne.**

Cependant, il est important de noter que cette tendance vers des solutions pilotées par des API n'est pas nécessairement une approche innovante. Les spécialistes de l'informatique ont passé des années à assembler des solutions en rassemblant des données provenant de plateformes disparates, en optimisant des activités et en comprenant le fonctionnement interne de différents composants.

Ici la nouveauté est l'échelle et la complexité de l'infrastructure et le volume d'informations traitées.

Dans l'ensemble, l'utilisation croissante des API et la tendance vers des solutions pilotées par des API reflètent l'évolution continue de l'industrie informatique vers une plus grande interopérabilité, efficacité et automatisation. À mesure que le volume de données et la complexité de l'infrastructure informatique continuent de croître, il est probable que cette tendance continue de gagner en importance dans les années à venir.

Playbooks d'automatisation via la recherche sur les menaces émergentes

Agent Tesla – Téléchargement

Russie/Ukraine - Téléchargement

PLAY – Téléchargement

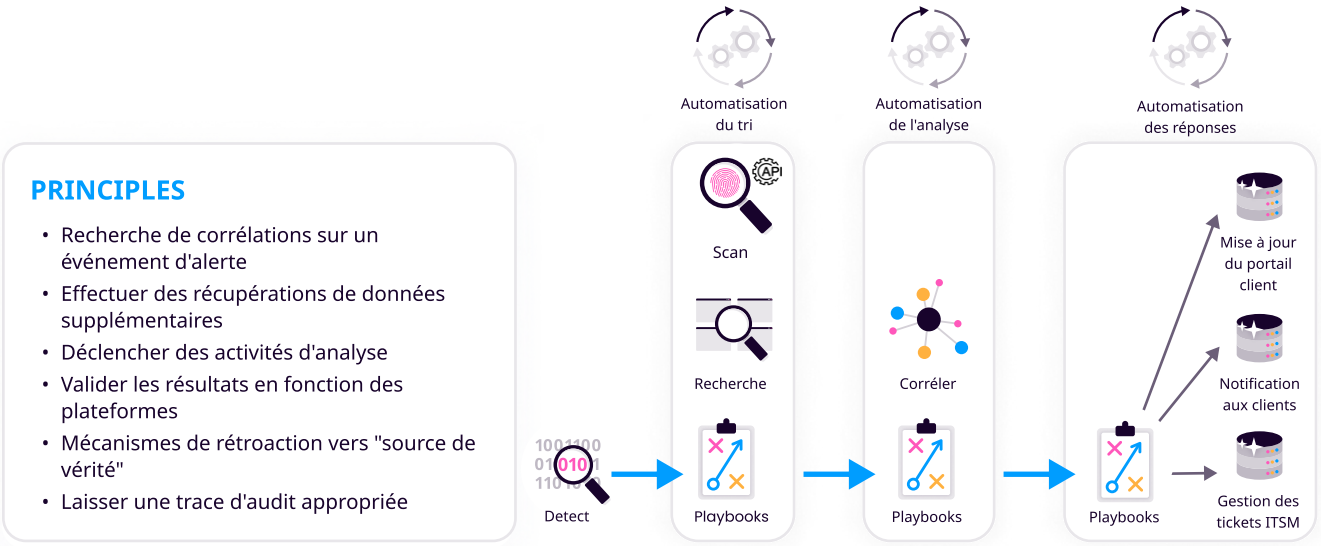
HIVE - Téléchargement

Il n'est pas réalisable pour un individu ou une équipe au sein d'une entreprise de gérer tous les aspects de la sécurité, car la complexité des technologies modernes est vaste. Bien qu'il soit possible d'apprendre sur des aspects spécifiques de la sécurité et d'acquérir une compréhension approfondie grâce à des post-mortems individuels, cette approche n'est pas pratique à l'échelle de toute une industrie. De plus, la plupart des individus ont une spécialisation dans une ou plusieurs technologies de sécurité et manquent de connaissances dans certains domaines technologiques. En tant que prestataire de services de sécurité géré (MSSP), la frontière entre la simple maintenance et la véritable gestion d'une plateforme en matière de sécurité est mince. Ce qui fait la différence entre fournir un service précieux ou un service remplaçable est :

- **Se fier uniquement à la technologie limite la curiosité face à l'inhabituel.**
- **Le recours aux bons outils de suivi des tendances du marché.**
- **Le service manque de processus pour évoluer, et le style de gestion limite la capacité d'adaptation.**

En intégrant un ensemble de compétences de type DevSecOps dans les intégrations des systèmes de sécurité, une approche complète et proactive de la cybersécurité peut être atteinte. Cette approche favorise la collaboration entre les équipes de sécurité et les équipes opérationnelles en utilisant les approches d'outils DevOps dans les activités quotidiennes, ce qui devient de plus en plus essentiel pour identifier et atténuer les risques de sécurité de manière rapide et efficace.

SIMPLIFIEZ LES INVESTIGATIONS GRÂCE À L'ORCHESTRATION



Lorsqu'on examine la logique du processus pour une « vraie gestion de la sécurité », un service ne peut pas être statique, il doit évoluer et s'adapter aux menaces changeantes. Cela se traduit par trois traits souhaitables dans la prochaine génération de services SOC de détection et de réponse gérés :

1. **Capacité à créer de nouvelles tâches d'orchestration en tant qu'activité opérationnelle quotidienne.**
2. **Changement de priorité en faveur de la chasse aux menaces plutôt que de dépendre uniquement des alertes pour déclencher des activités.**
3. **Promotion dynamique d'une chasse aux menaces qualifiée en tant qu'extension de service**

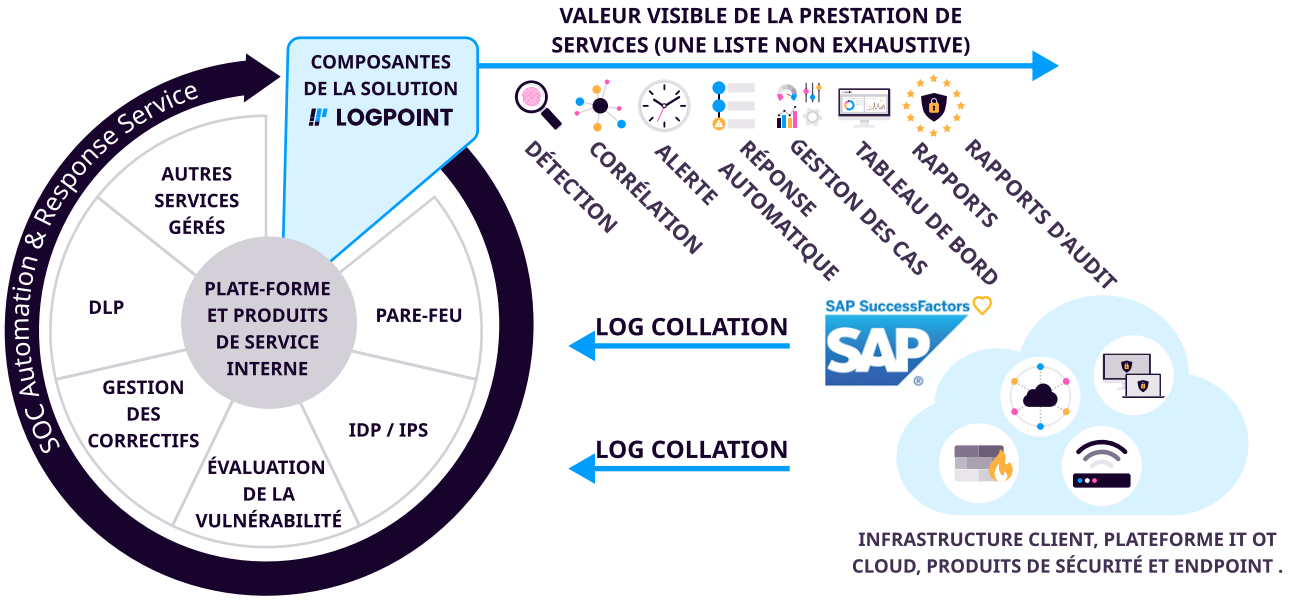
Dans le contexte d'un fournisseur de services de sécurité, ces points sont particulièrement pertinents. En tant que fournisseur de services de sécurité, il est important d'avoir la capacité de créer de nouvelles tâches d'orchestration en tant qu'activité opérationnelle quotidienne, car cela permet à l'organisation de rester en avance sur les menaces émergentes et de réagir rapidement aux nouvelles vecteurs d'attaque.

De même, orienter l'accent vers une chasse proactive aux menaces plutôt que de simplement compter sur les alertes peut aider les fournisseurs de services à fournir des solutions de sécurité plus efficaces et globales à leurs clients. En développant la capacité de promouvoir dynamiquement les chasses aux menaces qualifiées en tant qu'extension de service, les fournisseurs de services peuvent mettre en valeur leur expertise et se différencier de leurs concurrents sur le marché.

Dans l'ensemble, ces points soulignent la nécessité pour les fournisseurs de services d'adopter une approche proactive et agile des opérations de cybersécurité, ce qui leur permet de rester en avance sur les menaces évolutives et de fournir des services à valeur ajoutée à leurs clients. Ce faisant, les fournisseurs de services peuvent aider leurs clients à atténuer les risques, protéger leurs actifs critiques, et gagner la confiance et la crédibilité dans leurs offres de sécurité.

RÉVISION

De la même manière que des conversations très simples et régulières entre (1) et (2) auraient pu aider à éviter toutes les situations mentionnées précédemment, la création d'une communication interplateforme et de points centraux d'analyse peut également être simple lorsque l'évaluation de la dépendance des données et de la logique des processus est effectuée.



Les fournisseurs de services de sécurité gérée (MSSP) ont l'opportunité de fournir des services compétents et très précieux, car l'externalisation à un tiers peut apporter de nombreux avantages à un client, tels que l'accès à une expertise spécialisée, des économies de coûts opérationnels, une efficacité accrue et, surtout, une réduction du risque de dommages à la marque dus à des violations de sécurité.

- **Accès à des ressources expertes :** Un MSSP emploie généralement une équipe de professionnels de la sécurité compétents avec une expertise dans la gestion et la surveillance des solutions SIEM (gestion des informations et des événements de sécurité) et SOAR (automatisation et orchestration de la réponse à la sécurité). En externalisant auprès d'un MSSP, les entreprises peuvent bénéficier de l'expertise, des connaissances et de l'expérience du MSSP.
- **Service Orchestre Empilé :** En empilant les services de sécurité avec les intégrations qu'un MSSP offre, on obtient une approche globale et multicouche de la cybersécurité, réduisant le risque de cyberattaques et améliorant la posture de sécurité globale. En combinant plusieurs services, les entreprises peuvent bénéficier d'une visibilité accrue, de capacités de détection de menaces et de réponse aux incidents améliorées.
- **Solution rentable :** Mettre en place un centre opérationnel de sécurité (SOC) en interne avec la technologie, les outils et le personnel nécessaires peut être coûteux. L'externalisation à un MSSP peut offrir une solution rentable qui permet aux entreprises de bénéficier de la technologie de pointe et de l'expertise sans les dépenses en capital et opérationnelles associées à la construction d'un SOC en interne.

- **Scalabilité :** Un MSSP peut offrir une solution évolutive qui peut s'adapter à l'évolution des besoins de l'entreprise. Cela permet aux entreprises de s'adapter rapidement aux exigences de sécurité changeantes sans avoir à investir dans une infrastructure ou un personnel supplémentaire.
- **Détection des menaces et réponse améliorées :** Les solutions SIEM (gestion des informations et des événements de sécurité) et SOAR (automatisation et orchestration de la réponse à la sécurité) permettent une surveillance en temps réel et une détection des menaces, ce qui permet une réponse rapide aux incidents de sécurité. En externalisant à un MSSP, les entreprises peuvent bénéficier des capacités avancées de détection et de réponse aux menaces du MSSP, réduisant ainsi le risque de violations de sécurité et minimisant l'impact de tout incident.
- **Conformité aux normes de sécurité :** De nombreuses industries sont soumises à des normes de sécurité telles que HIPAA, PCI-DSS ou GDPR. Externaliser à un MSSP qui maîtrise ces normes peut aider les entreprises à se conformer aux réglementations et à éviter de lourdes amendes.
- **Concentration sur le cœur de métier de l'entreprise :** Externaliser les fonctions SIEM et SOAR du SOC à un MSSP permet aux entreprises de se concentrer sur leurs compétences de base et leurs activités stratégiques, plutôt que de s'inquiéter des opérations de sécurité.

EXTERNALISATION

Dans l'ensemble, externaliser les fonctions SIEM (Security Information and Event Management) et SOAR (Security Orchestration, Automation, and Response) d'un SOC (Security Operations Center) à un prestataire de services de sécurité géré (MSSP) peut offrir aux entreprises des capacités de surveillance et de réponse en matière de sécurité efficaces, évolutives et expertes, leur permettant de se concentrer sur leurs activités principales et d'éviter les coûts et la complexité liés à la mise en place d'un SOC interne.

Cependant, l'externalisation présente également des risques en matière de sécurité qui doivent être gérés avec soin. L'une des principales préoccupations liées à l'externalisation est qu'elle peut créer des silos de sécurité supplémentaires, ce qui peut entraîner un manque d'intégration et une fragmentation des données. Cela peut être particulièrement problématique si les services externalisés nécessitent l'accès à des données ou des systèmes sensibles. Pour atténuer ce risque, il est important d'établir des politiques et des procédures claires pour intégrer de manière sécurisée les systèmes et les données du prestataire tiers avec ceux de l'entreprise.

Un autre élément essentiel d'une solide posture de sécurité est la réalisation d'une évaluation complète des risques avant d'externaliser des services quelconques. Cette évaluation devrait identifier les risques potentiels et les vulnérabilités associées aux services externalisés, ainsi que toutes les exigences réglementaires à respecter. Cette évaluation devrait être effectuée régulièrement, et toute modification des services externalisés ou du paysage de la sécurité devrait être évaluée promptement.

RÉSULTATS DE L'ENQUÊTE

- Le temps moyen pour détecter par rapport au temps moyen pour répondre est mitigé, avec un score moyen de 3 sur 5. Cela peut indiquer un risque de délais de réponse lents aux menaces, ce qui pourrait avoir un impact sur la capacité de l'organisation à fournir des protections efficaces.
- Les organisations MSSP offrent une large gamme de services, notamment la surveillance de sécurité gérée, la gestion des vulnérabilités, le renseignement sur les menaces, les tests d'intrusion, la gestion des correctifs, et plus encore. Bien que cela soit un signe positif, cela indique également que l'organisation peut être étendue trop finement, ce qui rend difficile la fourniture de services de haute qualité dans tous les domaines.
- La réponse manuelle aux alertes indique que certaines opérations de SOC ont un faible pourcentage (25 %) de procédures automatiques pour la réponse aux alertes. Cela signifie que les alertes pourraient ne pas être traitées en temps voulu, entraînant un risque accru pour les clients.
- Certains services de SOC peuvent ne pas avoir d'intégration API avec d'autres technologies, ce qui limite potentiellement leur efficacité et leur capacité à répondre aux menaces.
- Lorsqu'on examine la capacité à créer des schémas de détection, certains répondants ont évalué leur capacité à créer des schémas de détection pour les menaces émergentes comme étant faible (1) ou moyenne (3). Cela pourrait entraîner des retards dans la détection et la réponse aux menaces émergentes.
- L'examen de l'automatisation technologique montre que certaines opérations de SOC pourraient ne pas automatiser les réponses dans des technologies clés telles que EDR, pare-feu et gestion des utilisateurs, ce qui pourrait accroître l'écart sur le MTTR (Mean Time to Respond) et les risques.
- Des procédures inefficaces révèlent que certaines opérations de SOC pourraient perdre du temps en raison de procédures inefficaces, ce qui pourrait entraîner des temps de réponse plus lents et des risques accrus.
- L'enquête révèle que la plupart des MSSP prévoient de créer de nouveaux services au cours des 12 à 24 prochains mois, notamment NDR (Network Detection and Response), EDR (Endpoint Detection and Response) et CSIRT géré, SOAR (Security Orchestration, Automation, and Response), NDR et MDR (Managed Detection and Response), ainsi que SOC pour les petites et moyennes entreprises.

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**