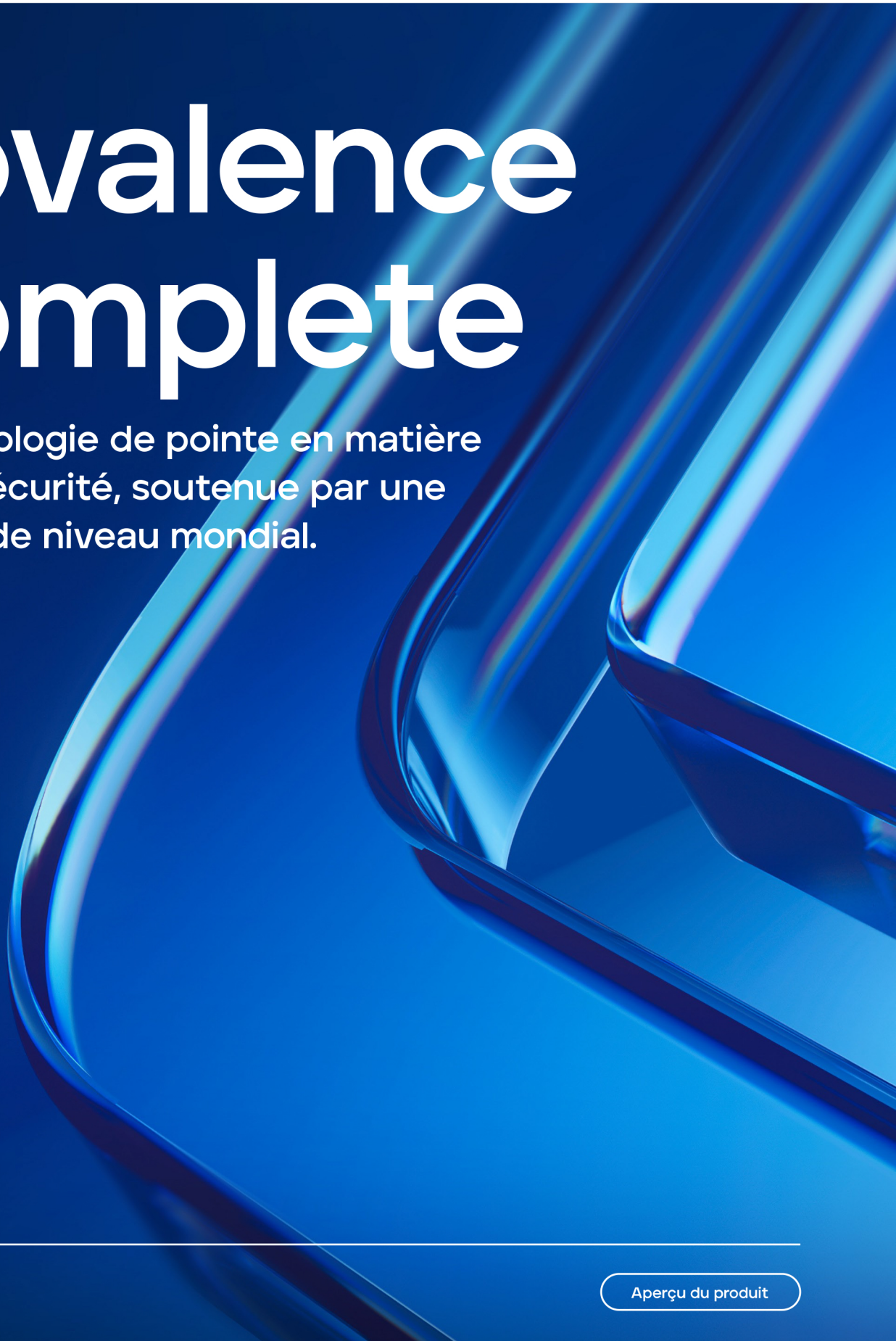
FIELD EFFECT Hamster

Covalence Complete

Une technologie de pointe en matière de cybersécurité, soutenue par une expertise de niveau mondial.



Covalence

Aperçu du produit

La sécurité est plus complexe que jamais.

Protéger votre entreprise contre les cybermenaces demande du temps, des efforts et de l'expertise.

Cependant, repérer et arrêter une activité suspecte avant qu'elle ne vous affecte requiert des connaissances et une expérience auxquelles tout le monde n'a pas accès.

En réponse, les entreprises superposent de nouveaux outils et technologies de sécurité pour protéger leurs données et leurs actifs sur leur réseau, leurs services en nuage et leurs points d'extrémité.

Les outils de sécurité sont plus complexes que jamais, ce qui entraîne une surcharge d'informations et une lassitude face aux alertes.

Et s'il y avait un meilleur moyen?

Vous avez besoin d'une solution permanente qui vous protège des cybermenaces. Vous avez besoin d'informations concrètes qui vous aident à améliorer et à renforcer votre sécurité, sans vous faire perdre de temps dans votre journée chargée.

Pour prévenir les cybermenaces et éliminer facilement les failles de sécurité, vous avez besoin d'une vision continue des cyberrisques potentiels et des activités malveillantes, étayée par une expertise.

Votre solution de cybersécurité mains libres.

MDR, XDR, SIEM, SOC… tout est compris. De la détection des menaces à l'analyse et à la réponse, Covalence vous protège.

Conçue dès le départ pour détecter et répondre aux comportements anormaux sur les terminaux, les services en nuage et les réseaux, Covalence est une solution de cybersécurité holistique qui offre une visibilité sur les menaces et les risques auxquels votre entreprise est confrontée, vous offrant ainsi les avantages d'une cybersécurité automatisée, soutenue par l'intelligence humaine.

Quelle que soit la taille de votre équipe ou l'endroit où elle travaille, Covalence s'étend à l'ensemble de votre infrastructure informatique. Elle identifie les cybermenaces et les vulnérabilités qui visent votre entreprise et vous fournit les informations dont vous avez besoin pour y répondre, le tout à partir d'une plateforme conviviale.

Réponse active en temps réel

Covalence est toujours prête à répondre à toute activité suspecte dans votre environnement informatique, comme par exemple :

- L'exécution de processus anormaux
- L'accès inapproprié entre les processus
- Les tentatives de chargement de modules en mode utilisateur ou noyau
- L'accès anormal au système de fichiers
- Un trafic réseau suspect
- L'accès anormal au registre
- Et bien plus encore

Lorsqu'elle repère quelque chose d'anormal, Covalence se met immédiatement au travail, identifie la menace et prend les mesures appropriées pour assurer votre sécurité. Covalence bloque automatiquement les principales menaces comme les rançongiciels et les menaces persistantes avancées (MPA), tout en vous tenant informé de ce qui se passe.

De plus, comme elle a été conçue pour fonctionner de manière transparente sur vos terminaux, votre réseau et vos services en nuage, Covalence comprend ce que l'activité d'une partie de votre environnement signifie pour le système.

L'utilisation de profils de réponse active vous permet d'adapter davantage Covalence à vos besoins, ce qui vous donne un aperçu et un contrôle inégalés de votre protection.

FIELD EFFECT / Hamster

Apprenez à connaître les ARO.

Alerte intelligente. Remédiation guidée. Conseils d'experts.

Les résultats de la détection et de l'analyse des menaces avancées de Covalence sont transformés en informations exploitables qui vous aident à comprendre rapidement et de manière proactive la réponse nécessaire pour sécuriser votre entreprise.

Nous fournissons des données sur les menaces vérifiées par des analystes sous forme de rapports simples, hiérarchisés et exploitables qui vous aident à comprendre vos menaces sous forme d'actions, de recommandations et d'observations (ARO). Notre approche exclusive élimine le bruit pour vous montrer les alertes qui comptent avec le contexte nécessaire pour les résoudre.

Dites adieu à un volume d'alertes qui prennent des heures à examiner. Pas de journaux d'événements de sécurité à trier. Vous ne perdrez plus de temps à collecter des données sur votre réseau à partir de plusieurs outils.

Actions

Lorsqu'une action immédiate est nécessaire pour une menace active ou imminente qui pourrait compromettre votre réseau ou vos appareils, nous la signalons comme une Action requise.

Recommendations

Si une modification de la configuration de votre réseau, de vos logiciels ou de votre technologie est nécessaire pour remédier à des vulnérabilités spécifiques ou à des menaces éventuelles, nous l'indiquerons sous forme de Recommandation.

Observations

Des conditions ou des événements spécifiques dans votre réseau peuvent être des indicateurs précoces d'une activité malveillante qui pourrait avoir un impact sur votre cybersécurité. Nous les signalons comme des Observations.

Besoin d'aide? Nous assurons vos arrières.

À l'instar d'un service de conciergerie de sécurité professionnelle, vous bénéficiez de la tranquillité d'esprit que procure une équipe dédiée de cyber pros et d'analystes expérimentés qui vous apportent un soutien, des conseils et des recommandations d'experts. Du soutien technique aux conseils en matière de stratégie de sécurité, nous sommes à vos côtés pour vous aider à protéger en permanence votre entreprise.

La cybersécurité simplifiée grâce à la détection, l'analyse et la réponse aux menaces tout-en-un.

Nous avons conçu la solution Covalence Complete pour qu'elle réponde aux besoins évolutifs de votre entreprise moderne.

01.	Analyse du trafic réseau 24 h/24 et 7 j/7	Sécurisez votre réseau en analysant tout le trafic réseau, y compris les appareils connus et inconnus, les appareils de l'Internet des objets (IdO) et les appareils mobiles. Identifiez et répondez aux menaces et aux vulnérabilités potentielles de votre réseau.
02.	Détection et réponse complètes aux menaces sur les points d'extrémité	Protégez tous vos points d'extrémité, y compris les serveurs, les ordinateurs de bureau et les ordinateurs portables, et identifiez les comportements anormaux pour bloquer activement les logiciels malveillants et les techniques d'attaque connus et émergents.
03.	Protection active contre les logiciels malveillants et les MPA	Identifiez et bloquez automatiquement les logiciels malveillants, les rançongiciels et les menaces persistantes avancées (MPA) à l'aide de politiques et de technologies fondées sur une expertise cybernétique de premier plan.

04.	**Détection et réponse aux menaces dans le nuage**	Utilisez notre capteur de surveillance natif du nuage pour protéger le domaine de votre entreprise et les programmes et applications basés sur le nuage, notamment Microsoft 365, Google Workspace, Amazon Web Services, Azure, Dropbox, Box, Okta, Salesforce, etc.
05.	**Renforcement du périmètre de votre réseaur**	Faites confiance à notre pare-feu DNS pour garantir une navigation et un accès internet sûrs en bloquant les connexions aux sites web malveillants.
06.	**Atténuation des vulnérabilités et des risques**	Identifiez les changements importants et l'activité dans votre environnement informatique qui indiquent des risques - y compris les services en nuage mal configurés et les logiciels non corrigés - et recevez des étapes détaillées pour résoudre les problèmes et améliorer votre sécurité.
07.	**Accès à un moteur analytique avancé**	Bénéficiez de capacités d'apprentissage automatique et d'analyse qui fournissent une analyse continue des données des utilisateurs et des services pour identifier et traiter les menaces. Il en résulte une visibilité en temps réel pour détecter, surveiller, mesurer, gérer et réduire les points attaquables de bout en bout.
08.	**Chasse aux menaces menée par des experts**	Obtenez un meilleur aperçu et des recommandations de sécurité grâce à nos chasseurs de menaces experts qui plongent dans les données du réseau et de Covalence pour identifier les vulnérabilités et les menaces nouvelles, émergentes ou non détectées
09.	**Réponse active**	Bloquez automatiquement les logiciels malveillants, isolez les appareils ou prenez d'autres mesures pour protéger votre entreprise. Covalence prend les mesures appropriées en votre nom et en fonction de votre tolérance au risque, en s'appuyant toujours sur une analyse humaine.
10.	**Découvrez ce qu'il se passe en coulisses avec le Tableau de bord Covalence**	Regardez de plus près comment nous analysons les données de votre réseau, de vos points d'extrémité et des différentes couches du nuage pour assurer votre sécurité. Le Tableau de bord Covalence vous permet d'accéder à toutes les informations relatives à votre posture de sécurité dans un format facile à utiliser et à visualiser.

11.	**Minimisez votre impact grâce à la préparation aux incident**	Mettez en place dès maintenant les préparatifs adéquats pour minimiser l'impact d'un futur incident de sécurité. Grâce à notre solution de préparation à la réponse aux incidents (RI), nous identifions les améliorations et les meilleures pratiques et processus nécessaires pour se préparer à d'éventuels incidents. Nous vous aidons à préparer le terrain dès le début pour réagir rapidement en réduisant les coûts de récupération et les temps d'arrêt.
12.	**Priorisez les efforts de sécurité**	Mettez en œuvre des contrôles de sécurité, des politiques d'utilisation et des efforts de formation grâce à des informations et des conseils ciblés provenant de nos alertes et rapports intelligents sur les actions, recommandations et observations (ARO).
13.	**Marquez l'activité suspecte des courriels pour un examen par des experts**	Protégez les communications par courrier électronique grâce à notre service d'analyse des courriers électroniques suspects, qui permet aux utilisateurs de transmettre rapidement tout courriel suspect à nos cyber experts pour une analyse rapide.
14.	**Accédez à la fonctionnalité d'intégration**	Utilisez les API et SDK de Covalence pour intégrer facilement Covalence à d'autres systèmes et fournir une surveillance et des alertes ARO à partir d'une seule plateforme, y compris l'intégration d'une API RESTful simple avec la plateforme principale de Covalence, un SDK et une API Python avancés pour travailler avec les capteurs Covalence, ainsi que des intégrations et des modules complémentaires pour les produits tiers.
15.	**Alignez-vous sur les cadres de cybersécurité**	Découvrez des vulnérabilités avancées et créez des rapports en vous appuyant sur les cadres des meilleures pratiques de l'industrie, notamment le cadre de cybersécurité du NIST, la norme ISO 27001, les contrôles de base du Centre canadien de cybersécurité (CCSC BC), la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) et les huit mesures d'atténuation essentielles de l'ACSC en Australie.
16.	**Faites confiance à de dispositifs de pointe faciles à installer**	Choisissez parmi une gamme de dispositifs Covalence pour compléter votre déploiement Covalence et assurer une surveillance, une détection et une analyse sophistiquées de la cybersécurité pour votre environnement informatique spécifique.
17.	**Accédez à une expertise en matière de sécurité 24 h /24**	Obtenez de l'aide à chaque étape du processus. Nos cyber-analystes experts sont à votre disposition pour répondre à vos questions sur la sécurité et vous fournir les conseils dont vous avez besoin

Hamster

Services informatiques
Logitem inc.

Contactez notre
équipe aujourd'hui.

Courriel

logitem@logitem.qc.ca

Téléphone

819-629-2816 Ext 102