Détecter les menaces de manière proactive

Protection complète contre les menaces connues et avancées reposant sur un service managé 24 heures sur 24

Kaspersky MDR: les points forts

- Fonctions de sécurité informatique rapides et évolutives
- Aucun investissement ou personnel supplémentaire n'est nécessaire
- Une protection de premier ordre contre les menaces très complexes et innovantes
- Eviter les interruptions d'activité
- Traitement entièrement géré ou guidé des incidents de sécurité
- Visibilité de la situation actuelle de tous les actifs et de leur statut de protection
- Fonctionne avec Kaspersky Endpoint Security, EDR et Anti Targeted Attack.

Kaspersky a été fondé à Moscou en 1997. Aujourd'hui, le spécialiste de la sécurité est présent dans 200 pays, emploie plus de 4000 spécialistes hautement qualifiés et est considéré comme l'un des principaux fournisseurs de solutions de sécurité. Les technologies Kaspersky protègent environ 400 millions d'utilisateurs dans le monde et sont utilisées par plus de 270 000 entreprises et organisations. Les solutions et services de cybersécurité de Kaspersky englobent des services managés dans le cloud et des solutions sur site notamment Endpoint Security, Hybrid Cloud Security et Enterprise Security de nouvelle génération, y compris les solutions de sécurisation de l'IoT et des applications industrielles. La plateforme Kaspersky Automated Security Awareness Platform (ASAP) propose une formation en ligne automatisée mais personnalisée sur la sécurité, en fonction des rôles et des compétences de chaque collaborateur. Des exemples pratiques et des simulations enseignent des compétences qui peuvent être directement mises en œuvre dans la vie quotidienne. Les divers sujets abordés comprennent la gestion des comptes, les mots de passe, les appareils mobiles et les données confidentielles, la sécurité des e-mails, y compris la sensibilisation au phishing et le comportement sur les réseaux sociaux. ASAP offre également une gestion automatisée de la formation, de l'e-mail d'invitation jusqu'à l'évaluation de la réussite de l'apprentissage, et convient en tant que solution cloud évolutive pour toutes les tailles d'entreprise.

kaspersky

Dépliant du fabricant
Kaspersky / Managed Detection and Response

Sécurité confortable avec Managed Detection and Response

Face aux incidents de cybersécurité, la plupart des équipes de sécurité adoptent une approche fondée sur les alertes et n'interviennent qu'une fois que l'incident s'est produit. Pendant ce temps, les nouvelles menaces échappent aux radars, donnant littéralement un faux sentiment de sécurité. Kaspersky Managed Detection and Response recherche de manière proactive les menaces non détectées mais pourtant actives au sein de l'infrastructure informatique.

Comment fonctionne Kaspersky MDR

Managed Detection and Response travaille avec les solutions Endpoint Security de Kaspersky et vérifie les alertes émises par les produits. Il analyse également les métadonnées d'activité des systèmes, à la recherche du moindre signe d'une attaque active ou imminente.

Ces métadonnées sont collectées via Kaspersky Security Network et sont automatiquement mises en corrélation en temps réel avec la Threat Intelligence inégalée de Kaspersky, afin d'identifier les stratégies, les techniques et les procédures utilisées par les attaquants. Les indicateurs d'attaque développés en interne par Kaspersky garantissent la détection des menaces furtives non malveillantes qui imitent des activités autorisées.

Le produit s'adapte à votre infrastructure durant les deux à quatre premières semaines afin de garantir un taux de faux positifs nul, en vous demandant la confirmation de ce qui est légitime ou non.

Deux variantes: Optimum et Expert

Kaspersky MDR est disponible en deux versions, pour répondre aux besoins des entreprises de toutes les tailles et des secteurs ayant des niveaux de maturité différents en matière de sécurité informatique.

Kaspersky MDR Optimum accroît instantanément les capacités de sécurité informatique sans avoir à investir dans du personnel ou des compétences externes supplémentaires.

Kaspersky MDR Expert offre également des fonctionnalités et une flexibilité supplémentaires aux équipes de sécurité informatique expérimentées, qui peuvent confier à Kaspersky la sélection et l'investigation des incidents, ce qui leur permet de concentrer leurs propres ressources limitées en matière de sécurité informatique sur la défense contre les cas critiques qui leur sont présentés.

La recherche de menaces automatisée incluse dans la solution MDR Optimum utilise des détections automatiques s'appuyant sur des indicateurs d'attaque propriétaires à des fins de validation, d'investigation et d'identification plus poussées des nouvelles menaces.

La recherche de menaces gérée offerte par la solution MDR Expert repose sur l'intervention manuelle fastidieuse des experts expérimentés de Kaspersky, qui traquent de manière proactive les menaces qui échappent à la détection automatique.

En outre, il existe un ensemble d'éléments complémentaires en option. Il s'agit notamment d'une option de stockage des données conforme à la législation, d'un «incident response retainer», d'une évaluation globale des menaces et de la formation des analystes SOC.

BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

BOLL
IT Security Distribution