McAfee MVISION Insights

Le premier module de protection des terminaux capable de renforcer de manière dynamique votre niveau de sécurité afin de garder une longueur d'avance sur les cybercriminels

Le rythme et l'évolution des cybermenaces sont un danger et une source de tension constants. Confrontées par ailleurs à une pénurie de compétences en cybersécurité, les entreprises ont réagi en augmentant leur budget de sécurité. Malgré cela, elles restent incapables de soutenir le rythme imposé par des adversaires qui ne cessent de mettre à jour leur arsenal d'outils, de tactiques et de techniques. Les options de cyberveille actuelles sont très souvent isolées et nécessitent une intervention manuelle. Elles peuvent détecter les menaces immédiates, mais la multiplication et la variété des cyberattaques mettent constamment les équipes de sécurité sur la défensive. Une plate-forme de cyberveille peut offrir un grand lac de données (data lake) sur les menaces, mais elle nécessite une intégration et des cycles d'analyse manuels, ce qui limite ses possibilités d'exploitation immédiate et de correction. Une solution de gestion des vulnérabilités peut identifier les vulnérabilités existantes et leur gravité, mais elle offre des informations limitées lorsqu'il s'agit de déterminer si votre dispositif de sécurité actuel peut ou non vous protéger contre les menaces réelles en circulation.

La solution : McAfee® MVISION Insights, une cyberveille en temps réel qui vous permet de prendre des mesures proactives. Condensée et analysée par l'intelligence artificielle et des spécialistes, cette cyberveille très complète peut prioriser les menaces et les campagnes d'attaques afin d'identifier les plus susceptibles de cibler votre entreprise. MVISION Insights prédit avec précision l'impact d'une menace sur votre protection globale et vous indique la procédure à suivre pour optimiser votre niveau de sécurité.

Principaux avantages

- **Informations sur les risques collectées auprès d'un milliard de capteurs —** Identifiez proactivement les menaces en dehors de votre périmètre grâce à une source approuvée. Priorisez les menaces par secteur, région et niveau de protection des terminaux de votre entreprise.
- **Identification des campagnes avant l'attaque et priorisation du niveau de risque à partir d'une seule console —** Bénéficiez d'informations directement exploitables sur une menace et sur l'efficacité de votre protection de vos terminaux à cet égard, y compris des recommandations sur les mesures correctives à appliquer.
- **Réduction du délai moyen entre la détection et la résolution —** Optimisez les flux de travail pour accélérer la mise en place de mesures de protection supplémentaires. Évaluez le niveau de protection actuel de vos terminaux grâce à des contre-mesures recommandées et accélérez les temps de réponse (de plusieurs mois à quelques heures).

Gardez le contact

La nécessité d'une approche plus proactive

MVISION Insights propose de nouvelles fonctionnalités intégrées à la plate-forme de gestion McAfee® qui s'alignent parfaitement avec la gestion des risques et des menaces et la soutiennent dans le but d'améliorer les contre-mesures défensives à appliquer et d'accélérer les temps de réponse tout en utilisant moins de ressources. Les informations sur les risques compilées à partir de données collectées auprès d'un milliard de sondes offrent à votre entreprise les connaissances dont elle a besoin pour prioriser ses défenses. Une multitude de tâches, dont la détection, la correction, des interventions préventives accélérées et une réduction sensible des risques, peuvent être effectuées à partir d'une seule et même console.

Certes, les stratégies de cyberdéfense réactives ont un rôle important à jouer, mais elles sont souvent à la traîne par rapport aux techniques déployées par les cybercriminels et se limitent généralement à des interventions d'urgence. Les cybercriminels mobilisent des outils de nouvelle génération pour élaborer des campagnes conçues pour mettre à mal les défenses traditionnelles ; ils testent les produits de sécurité réactifs afin d'identifier les techniques capables de percer ces défenses. Les entreprises doivent disposer d'une solution capable de couvrir l'ensemble du cycle de vie des attaques, avant et après avoir été touchées.

Cycle de vie d'une attaque

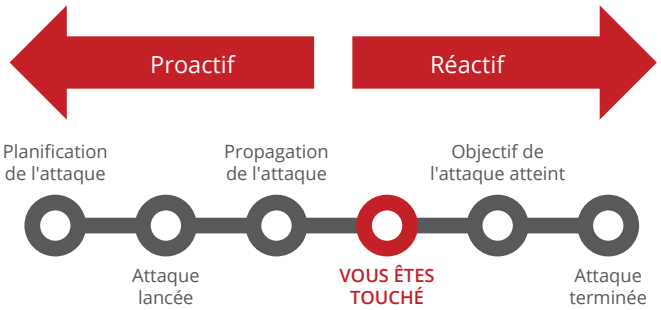

Figure 1. Cycle de vie classique d'une attaque.

Au final, la cyberveille et des informations directement exploitables vous permettent de renforcer votre cybersécurité par l'application de mesures proactives contre les menaces les plus probables, et d'être plus serein quant à l'état de vos défenses. L'action de McAfee MVISION Insights comporte trois volets :

- **Réduction des zones d'ombre et amélioration de la connaissance situationnelle :** Vous connaissez parfaitement la couverture offerte par votre solution de sécurité avant que les menaces ne frappent votre entreprise. MVISION Insights suit et priorise de façon proactive les menaces locales et mondiales susceptibles de toucher votre entreprise.

MVISION Insights répond aux questions critiques en matière de risques pour les terminaux

- Êtes-vous vulnérable ? Quel est votre niveau d'exposition ?
- Comment prioriser les attaques susceptibles de frapper votre entreprise ? Comment vous renseignez-vous sur celles-ci ? Quelle procédure de recherche est en place ?
- Comment vous renseignez-vous sur les menaces qui n'ont pas encore touché votre entreprise, mais sont susceptibles de le faire ?
- Même si vous disposiez d'une plate-forme de cyberveille (TIP), comment pourriez-vous prioriser toutes les attaques dans la base de données TIP ?
- Comment vous renseignez-vous sur les menaces qui ont touché les entreprises de votre secteur ?
- Quelle est la prévalence de ces menaces dans votre secteur et votre région ?
- Dans quelle mesure votre dispositif de protection actuel est-il capable de contrer ces menaces ?
- Quelle confiance avez-vous en votre protection face au paysage des menaces et pourquoi ?

- **Analyse basée sur l'apprentissage automatique :** Cette fonctionnalité permet de déterminer l'efficacité de votre niveau de sécurité spécifique et vous communique les mesures préventives à appliquer pour bloquer rapidement et facilement ces attaques.
- **Identification automatique de la plupart des menaces mondiales que votre dispositif de sécurité n'a pas détectées :** La solution s'appuie sur un immense lac de données (data lake) de cyberveille issue d'une source approuvée qui communique des données télémétriques significatives d'un point de vue statistique.

Tableau de bord MVISION Insights

Figure 2. Exemple d'un tableau de bord MVISION Insights.

Évaluation des risques

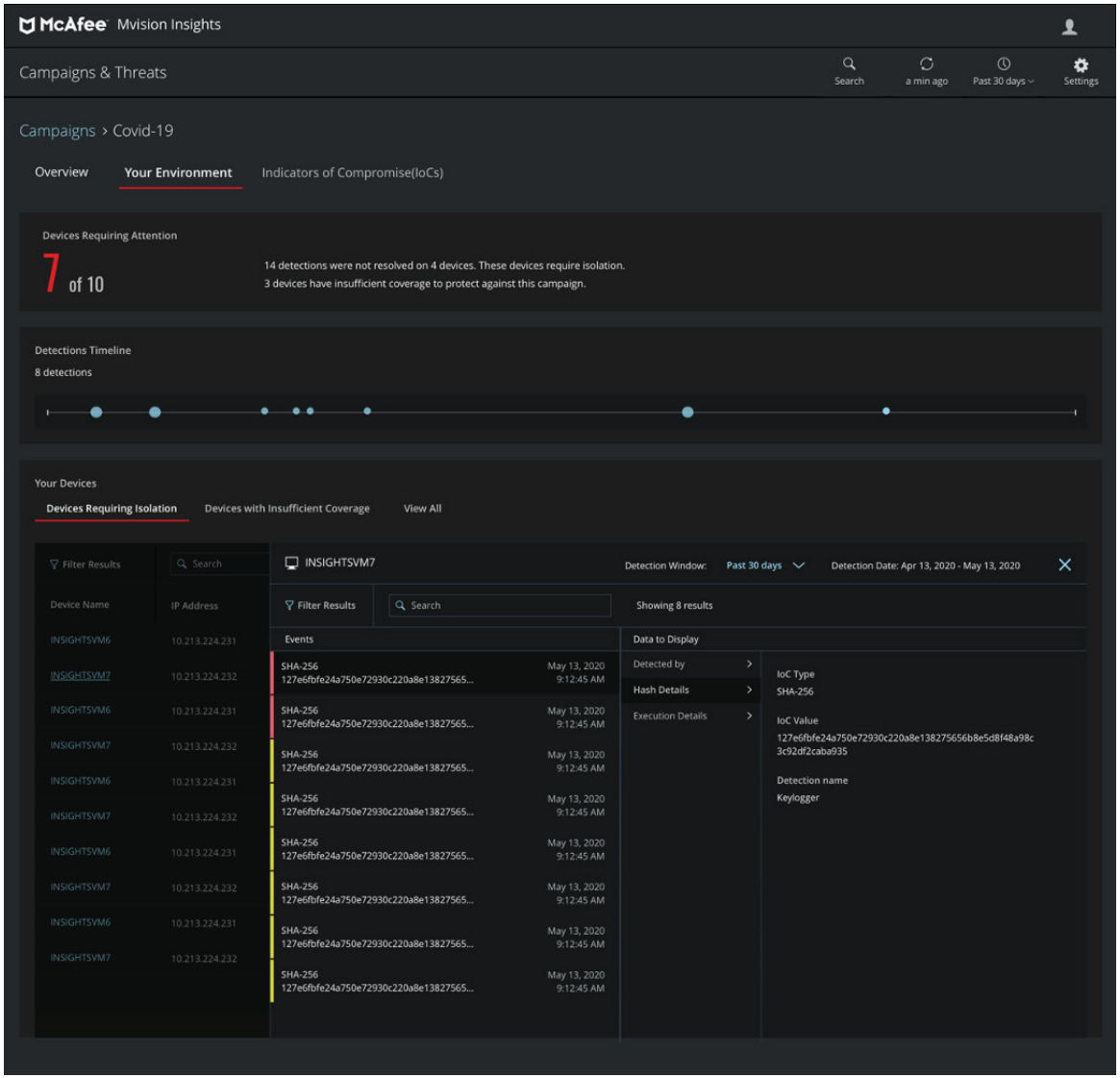

Figure 3. Identifiez avec précision les points vulnérables de votre environnement pour contrer la menace de façon proactive.

Détection et temps de réponse fortement accélérés

MVISION Insights aide votre entreprise à corriger et renforcer la sécurité de votre environnement spécifique, en vous indiquant la procédure à suivre et en proposant des actions automatisées. L'automatisation vous permet de contrer plus efficacement les attaques externes. La solution analyse et compare automatiquement les menaces externes et propose des mesures de protection proactives avant même toute attaque.

- **Réduction des délais moyens de détection et de résolution de plusieurs mois à quelques minutes —** L'association de l'homme et de la machine (apprentissage profond et apprentissage automatique) et des capacités d'analyse avancées permettent d'examiner d'énormes volumes de données afin de présenter des informations de cyberveille directement exploitables. Une capacité de détection étendue et préventive accélère les temps de réponse et réduit sensiblement les risques.
- **Amélioration du rapport signal-bruit pour les indicateurs de menaces —** L'analyse avancée améliore la détection des menaces et l'interprétation des alertes. La fonction d'analyse des menaces de MVISION Insights peut facilement basculer vers McAfee® MVISION EDR pour rechercher un contexte supplémentaire, par exemple les indicateurs de compromission, et réduire les cycles d'investigation.
- **Les menaces vous sont présentées de manière compréhensible et priorisée, avec en plus des conseils concernant les mesures à appliquer —** Une intervention guidée, basée sur des informations de cyberveille analysées et priorisées, améliore l'efficacité des analystes même les plus inexpérimentés. Depuis la console intégrée, vous pouvez intervenir rapidement et facilement en modifiant vos configurations, en isolant les équipements infectés, en mettant à jour les stratégies ou en basculant vers la solution EDR (Endpoint Detection and Response).

Autonomie renforcée des ressources SOC

Les équipes de sécurité sont submergées par les volumes de renseignements qu'elles doivent examiner pour assurer la protection de leur environnement. Le manque de temps et de ressources constitue un frein à l'analyse des menaces et des défenses. Quelles que soient les compétences des analystes, l'association de l'homme et de la machine permet d'étendre les capacités d'analyse et de faire le tri dans d'énormes quantités de données afin de présenter des informations de cyberveille directement exploitables. MVISION Insights permet à votre entreprise de pallier sa pénurie de compétences et offre au personnel du centre SOC les informations dont il a besoin pour agir. Comme les équipes de sécurité sont mieux informées, elles peuvent prendre des décisions plus avisées.

- La compréhension humaine forgée à partir des informations de cyberveille permet aux équipes de sécurité de personnaliser et de renforcer les défenses d'une entreprise pour assurer une protection optimale sans devoir augmenter les effectifs ni acquérir de nouvelles compétences. MVISION Insights alimente MVISION EDR en données plus pertinentes pour réduire le cycle d'investigation, et offre l'expertise et les ressources nécessaires pour mener des investigations. Les analystes peuvent vérifier le risque posé par l'incident et sa cause de façon plus rapide et efficace.
- La solution permet aux directeurs de la sécurité de tirer le meilleur parti de leur personnel et de leurs produits, en libérant les analystes en sécurité des tâches routinières et en aidant les membres de l'équipe peu expérimentés à devenir plus performants. Les entreprises peuvent réduire les heures passées à gérer la sécurité. Les flux de travail peuvent être rationalisés pour accélérer la mise en place de protections supplémentaires.
- La solution automatise de façon préventive la détection, la réponse et la protection contre des menaces priorisées à partir d'une seule console, ce qui évite aux analystes de devoir passer d'une tâche à l'autre. MVISION Insights collecte et analyse les données pertinentes et communique les procédures à suivre pour contrer les menaces dans un seul et même emplacement, aisément accessible aux analystes.

Informations plus pointues et pertinentes

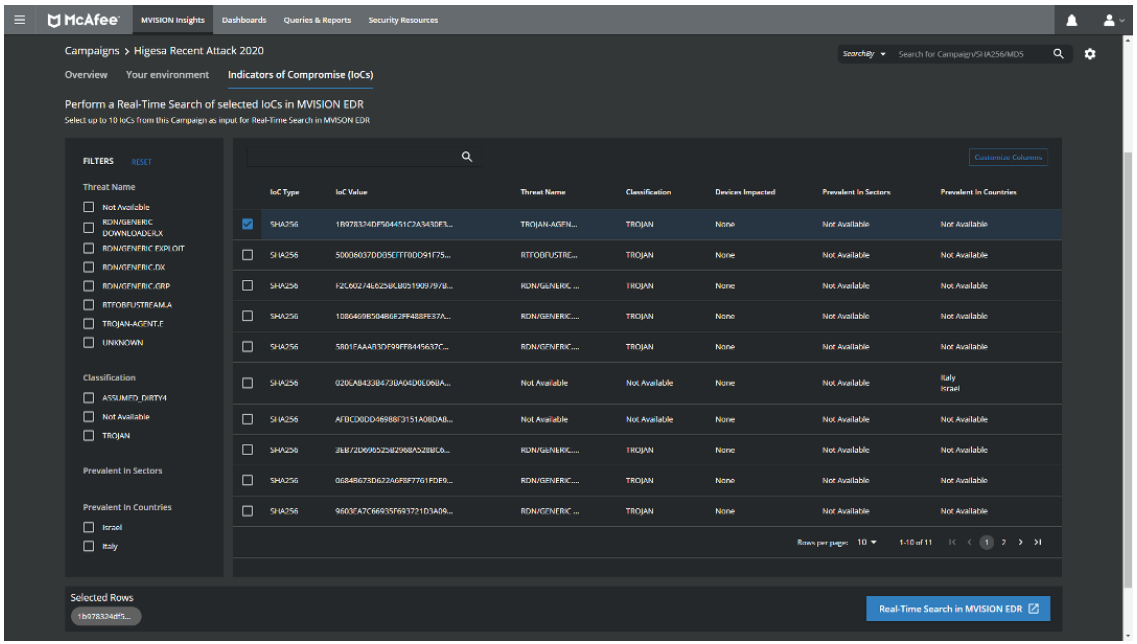

Figure 4. Bénéficiez d'une analyse plus approfondie pour mieux appréhender les menaces et déterminer votre capacité à protéger votre entreprise.

Configuration requise pour MVISION Insights

MVISION Insights est géré par McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.10 (sur site et IaaS) et McAfee® MVISION ePO™ (SaaS). La solution est optimisée pour être utilisée avec notre toute dernière technologie de protection des terminaux : McAfee® Endpoint Security et McAfee® Agent. Pour que MVISION Insights soit efficace, l'option d'envoi de données de télémétrie de McAfee Endpoint Security doit être activée.

Exemples de scénarios d'utilisation

Problème	Solution	Résultat
Suis-je la cible d'une attaque ? **S'agit-il d'une nouvelle variante de campagne ?**	▪ Évaluation des menaces liées aux campagnes connues ▪ Analyse rétrospective d'une attaque donnée ▪ Rapport comparatif du degré d'efficacité des mesures de protection ▪ Analyse rétrospective de l'attaque avec les indicateurs de compromission de l'utilisateur	Réponse à la question : Suis-je concerné par ce risque ?
La configuration de mon dispositif de sécurité actuel peut-elle me protéger ?	▪ Contrôle du niveau de protection local	Évaluation de mon niveau de protection actuel
Quelles modifications spécifiques dois-je apporter pour être protégé ?	▪ Contrôle du niveau de protection local	Conseils prescriptifs sur les mesures à prendre
Mes autres fonctions de sécurité peuvent-elles isoler la menace ?	▪ Publication en vue d'isoler ou de confiner dans d'autres fonctions de sécurité	Envoi des actions de confinement à d'autres fonctions de sécurité pour limiter encore plus le risque (via DXL)

En savoir plus

Pour plus d'informations, visitez le site www.mcafee.com/fr.

McAfee

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr