McAfee Investigator

Transformez vos analystes en enquêteurs chevronnés

McAfee® Investigator aide les analystes à résoudre les incidents plus rapidement et à en déterminer la cause sous-jacente avec un plus grand degré de certitude. Les alertes catégorisées déclenchent un examen par des experts : ceux-ci étudient à la fois les données SIEM pertinentes et les données collectées en temps réel sur les terminaux. Les centres SOC peuvent ainsi investiguer correctement les logiciels malveillants, les menaces ciblant les réseaux et les indicateurs de compromission en s'appuyant sur l'automatisation, l'intelligence artificielle et les compétences de leur personnel.

Défis pour les SOC

Le volume des événements et la durée de validité des données sont deux facteurs qui compliquent l'évaluation précise des alertes, notamment en termes de gravité ou d'ampleur. Il arrive souvent que les analystes ignorent certaines alertes car ils ne disposent pas des informations ou des éléments contextuels nécessaires pour déterminer s'il s'agit réellement d'incidents.

Les investigations des incidents sélectionnés peuvent alors prendre du temps et nécessiter une connaissance étendue des différents vecteurs de menaces afin de déceler l'origine du problème. La demande en analystes SOC compétents augmente, mais pas le vivier de talents.

Nouvelles fonctions d'analyse

D'après les recherches menées par McAfee[1], les SOC matures s'attaquent à ce problème en utilisant des outils d'automatisation et d'analyse sophistiqués. Ils poursuivent ce faisant un double objectif : accélérer les délais de neutralisation d'une attaque, tout en identifiant la cause sous-jacente.

McAfee Investigator place l'automatisation et l'analyse avancées à la portée de chaque SOC. En tant que solutions SaaS, les systèmes experts et les outils de capture des données des terminaux s'intègrent aux sources de données et aux systèmes de gestion de la sécurité existants, pour une rentabilité immédiate et un minimum d'efforts.

Ces analyses interactives offrent des fonctions d'automatisation, des informations et des recommandations actualisées en permanence. Elles permettent ainsi à l'équipe de réponse aux incidents d'effectuer une analyse rapide, détaillée et précise des logiciels malveillants, des menaces ciblant les réseaux et des compromissions.

Principaux avantages

- **Réduction de la durée d'implantation des menaces :** L'examen approfondi des données d'incidents permet de déterminer la cause sous-jacente du problème, plutôt que de corriger un symptôme.
- **Focalisation sur les cas plutôt que sur les alertes :** L'équipe consacre moins de temps aux investigations manuelles et aux cas à faible priorité.
- **Traitement prioritaire des événements inconnus :** Priorité est donnée aux artefacts et informations nécessitant une intervention humaine et une prise de décision.
- **Amélioration du tri :** L'équipe peut traiter davantage d'incidents, plus rapidement et plus efficacement.
- **Réduction de la charge de travail des analystes :** Les analystes exploitent au mieux leur temps, leur énergie et leurs capacités cognitives.

Tri précis et rapide

McAfee Investigator améliore le tri en permettant aux opérations de sécurité d'octroyer automatiquement un niveau de priorité élevé aux situations exigeant une attention immédiate. Pour ces cas particuliers, et pour tout autre qu'un analyste souhaite explorer, McAfee Investigator collecte, organise, synthétise et visualise les alertes, les activités, les éléments de preuve et les informations recueillies sur une attaque présumée.

Les données pertinentes sont réunies en arrière-plan et comprennent uniquement les informations nécessaires pour une investigation des menaces déclenchant une décision. Les données émanant de solutions SIEM peuvent être enrichies par des données provenant des terminaux, sans qu'un agent EDR (Endpoint Detection and Response) soit requis sur chaque poste. Ce modèle élimine le cloisonnement en offrant une visibilité contextuelle sur les indicateurs de compromission, sur les tactiques, techniques et procédures des attaques et sur les relations entre tous ces éléments.

Un moteur d'analyse des données et d'apprentissage automatique compare les données de preuve aux bases de référence et aux sources de cyberveille connues. Il traite les artefacts et élève le degré de priorité des principaux éléments suspects.

En collectant et en priorisant les données pertinentes de façon automatique, McAfee Investigator permet de déterminer plus aisément et plus rapidement les risques et le degré d'urgence de l'incident. Les analystes peuvent alors prendre les bonnes décisions de tri sans attendre et se concentrer sur les menaces les plus importantes.

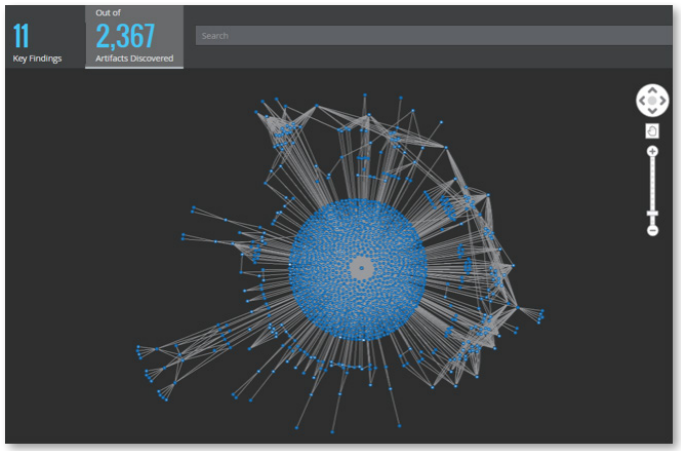

Figure 1. McAfee Investigator recueille des milliers d'éléments de preuve.

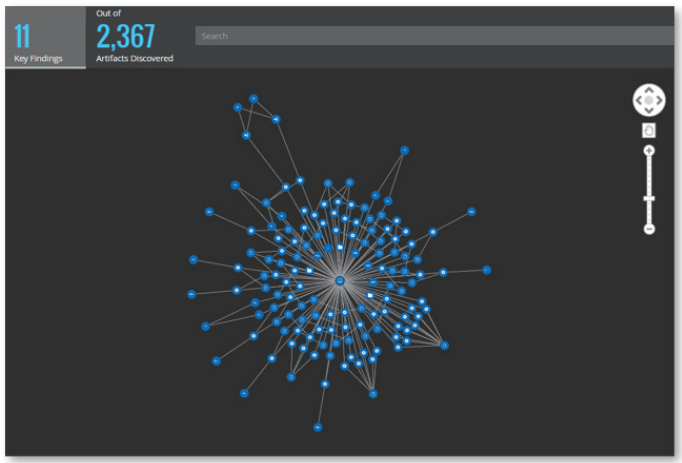

Figure 2. McAfee Investigator applique ensuite des analyses et des recommandations d'experts pour présenter les conclusions importantes.

Principaux avantages (suite)

- **Renforcement des compétences :** Des guides stratégiques et des renseignements pertinents aident les analystes à se poser les bonnes questions et à formuler les meilleures hypothèses.
- **Renforcement de la valeur des systèmes actuels :** Les sources de données et les fonctions d'analyse existantes sont améliorées afin d'assurer une plus grande précision.

Principales caractéristiques

- Collecte de données précises à la demande
- Agent de collecte de données de terminaux temporaire
- Interprétation des données recueillies, sur la base de recommandations d'experts et de l'intelligence artificielle
- Visualisations interactives
- Hypothèses multivectorielles pour explorer les données probables
- Bases de référence pour l'intelligence institutionnelle
- Gestion des cas axée sur les investigations

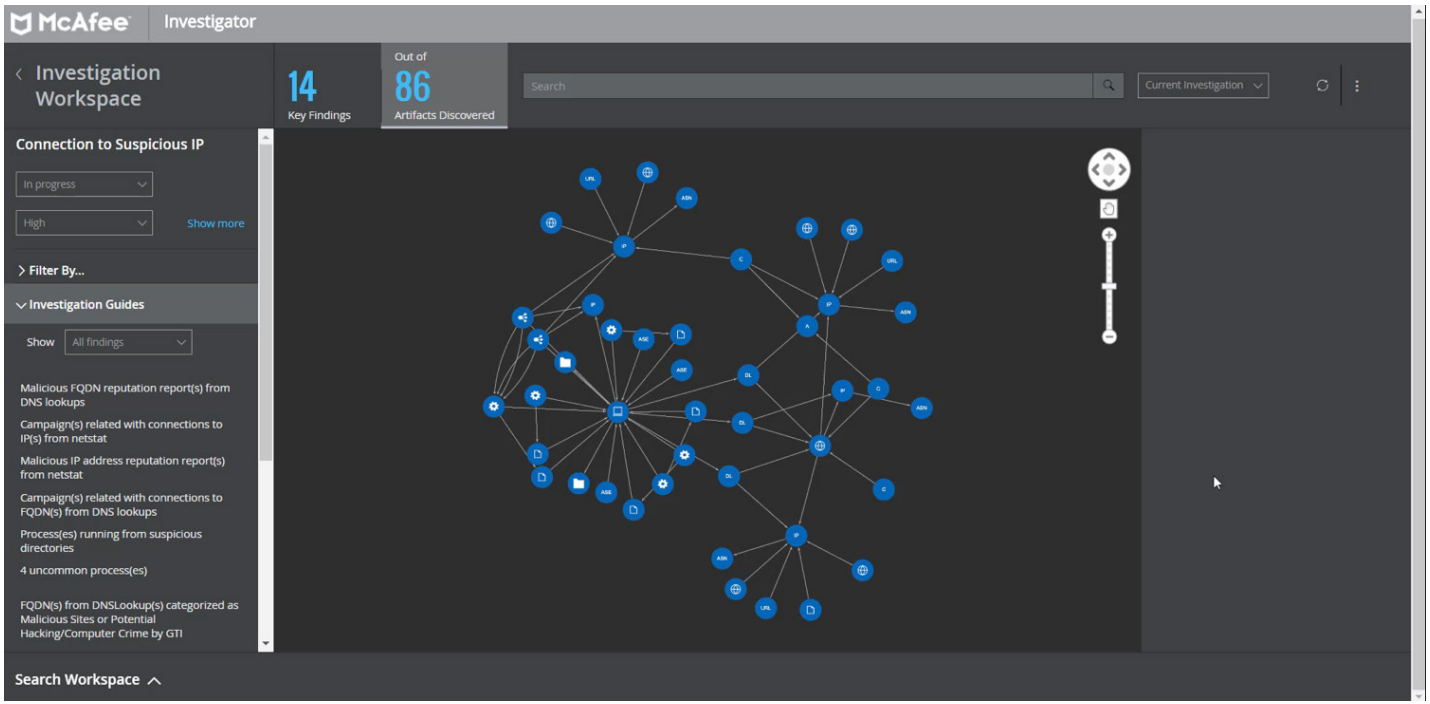

Figure 3. L'espace de travail permet de visualiser et d'explorer aisément les principales conclusions.

À un niveau organisationnel, les avantages sont multiples. Le tri avancé permet de passer de l'analyse d'alertes à l'examen de cas contextualisés. Ainsi, un plus grand nombre de cas sont résolus par les analystes de niveau 1 et, de manière générale, les analystes sont plus efficaces et peuvent se consacrer davantage aux activités à valeur ajoutée.

Lorsqu'un incident doit faire l'objet d'une investigation détaillée, les analystes se reportent à des guides stratégiques interactifs, qui leur permettant de se concentrer sur les éléments importants lorsqu'ils évaluent la portée et la gravité de l'incident. Ces guides ne sont pas statiques ni basés sur des scripts. Le système imite le mode de fonctionnement du cerveau humain et explore de nombreuses hypothèses en parallèle pour garantir une vitesse et une précision maximales.

Ces guides en langage humain intelligible combinent le savoir-faire des chercheurs de Foundstone® et les techniques d'intelligence artificielle. McAfee Investigator matérialise en cela la collaboration entre l'homme et la machine.

L'espace de travail propose des informations et des conclusions relatives aux incidents dans le but d'aider les analystes à poser les bonnes questions. Cette exploration multivectorielle et rigoureuse permet de résoudre les incidents de façon efficace et précise, et d'en identifier les causes sous-jacentes avec un grand degré de certitude.

Développement des compétences et de la collaboration

L'espace de travail interactif intégré de McAfee Investigator s'inscrit dans la tradition d'innovation de McAfee. Il permet aux analystes de mettre en place des workflows et de parcourir les données dans un environnement cognitif unique. Ce modèle limite la surabondance d'informations générée par la multitude d'alertes et offre une vue centralisée sur un seul écran.

L'espace de travail aide les analystes novices et moyennement expérimentés à appliquer les raisonnements des analystes confirmés, leur permettant ainsi de développer leurs compétences sans formation supplémentaire. Il active également des workflows liés aux incidents pour simplifier l'accès, l'enregistrement, le partage et la mise à jour des incidents pour les différentes équipes. Un partage cohérent des données revêt une importance cruciale en raison de la distribution géographique et des différents niveaux de compétences des équipes SOC.

Une conception fondée sur les données et outils existants

McAfee Investigator fonctionne avec une solution SIEM et le logiciel McAfee® ePolicy Orchestrator® afin d'ajouter une analyse avancée aux sources de données, bases de référence, corrélations et alertes existantes. Un agent temporaire recueille des données auprès des terminaux, pour assurer l'interprétation précise de preuves complexes. Des services professionnels accélèrent l'intégration et l'activation.

En savoir plus

Grâce à McAfee Investigator, il n'est plus nécessaire de passer des heures à collecter et à interpréter des données chaque fois qu'un élément éveille vos soupçons. Son moteur d'analyse avancé inspecte et trie les alertes sur les menaces dans une interface contextuelle, pour permettre une application appropriée des opérations de sécurité. McAfee Investigator automatise l'emploi des connaissances des experts en sécurité dans le cadre des investigations, permettant ainsi aux analystes de travailler de façon plus intelligente, plus rapide et plus précise.

En bref, une collaboration efficace entre l'homme et la machine.

Pour en savoir plus, visitez notre site à l'adresse **www.mcafee.com/fr/products/investigator.aspx**.

1. https://www.mcafee.com/fr/resources/reports/rp-disrupting-disruptors.pdf

McAfee Together is power.

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