RAPID7 | insightVM

PRODUCT BRIEF

Évaluation des vulnérabilités et analyse des Endpoints en direct

À mesure que les réseaux modernes évoluent, votre exposition au risque change de minute en minute. Chaque année, vous voyez la quantité de données croître de manière exponentielle, la menace d'attaques devenir plus sophistiquée, et les défis : minimiser le risque et optimiser les opérations deviennent plus difficiles. On a parfois l'impression d'une bataille sans fin, mais il est possible de surmonter le risque en le comprenant. Comment ? Grâce à une visibilité partagée, à l'analyse et à l'automatisation, principes fondamentaux de la pratique des SecOps.

Utilisant la puissance de la plateforme Insight de Rapid7 et l'héritage de notre produit primé Nexpose, Insight-VM offre un moyen entièrement disponible, évolutif et efficace de collecter vos données de vulnérabilité, de les transformer en réponses et de minimiser les risques. Insight-VM exploite les dernières technologies d'analyse et de terminaux pour découvrir les vulnérabilités en temps réel, les localiser, les classer par ordre de priorité pour votre activité, faciliter la collaboration avec d'autres équipes et confirmer que votre exposition a été réduite.

"Rapid7 a déjà mis en œuvre ce à quoi ressemblera le VRM à l'avenir."

—The Forrester Wave™: Vulnerability Risk Management, Q1 2018

Sécurisez votre réseau moderne

Adaptez-vous à votre réseau moderne en bénéficiant d'une visibilité totale de votre écosystème, d'une hiérarchisation des risques à l'aide d'analyses basées sur les attaques et d'une remédiation pilotée par SecOps. Ajoutez à cela une recherche continue et sans précédent sur l'état d'esprit des attaquants, et vous serez prêt à agir avant l'impact.

Obtenez une visibilité totale de votre écosystème :

- **Surveillance continue des Endpoints grâce à l'Insight Agent**
  L'agent Rapid7 Insight collecte automatiquement les données de tous vos Endpoints, même celles des travailleurs distants et des actifs sensibles qui ne peuvent pas être analysés activement, ou qui rejoignent rarement le réseau de l'entreprise. Associez InsightVM à Rapid7 InsightIDR pour obtenir une image complète des risques posés par vos terminaux et leurs utilisateurs.
- **Des tableaux de bord vivants et non pas statiques**
  S'appuyant sur des données de vulnérabilités récentes, les tableaux de bord d'InsightVM sont vivants et interactifs par nature. Vous pouvez facilement créer des cartes personnalisées et adaptées ainsi que des tableaux de bord complets pour n'importe qui (des administrateurs système aux RSSI) et interroger chaque carte avec un langage simple pour suivre les progrès de votre programme de sécurité. Visualisez, hiérarchisez, attribuez et réparez vos risques plus facilement que jamais.
- **Évaluation du Cloud, de l'infrastructure virtuelle et des conteneurs**
  InsightVM s'intègre aux services de cloud, à l'infrastructure virtuelle et aux référentiels de conteneurs tels qu'Amazon Web Services, Microsoft Azure et VMware pour s'assurer que vous ne manquez aucune nouvelle instance et aucun conteneur Docker mis en ligne. Vous pouvez également établir une corrélation entre les conteneurs déployés et les actifs, afin de sécuriser à la fois les conteneurs et les hébergeurs, le tout sans coût supplémentaire.

MIEL

Établir des priorités en utilisant l'analyse des attaquants

- **Analyse de risque basée sur l'attaquant**
  Hiérarchisez les risques comme le feraient les attaquants. InsightVM traduit des décennies de connaissance des attaquants en analyses fiables. Le score granulaire de risque réel 1-1000 tient compte des scores CVSS, de l'exposition aux logiciels malveillants, de l'exposition aux exploits et de leur facilité d'utilisation, ainsi que de l'âge de la vulnérabilité. Il est ainsi plus simple - et plus précis que le seul CVSS - de hiérarchiser les vulnérabilités à corriger. Les données Rapid7 Project Sonar et les flux de menaces se traduisent par des tableaux de bord dans InsightVM, afin que vous puissiez comprendre quelles sont les portes du réseau externe que vous manquez et quelles sont les vulnérabilités que les attaquants exploitent activement.
- **Planification de la remédiation en direct**
  Une fois que les vulnérabilités les plus critiques sont remontées à la surface, attribuez et suivez les tâches de remédiation en temps réel grâce aux workflows de remédiation. InsightVM s'intègre à des solutions de gestion de tickets informatiques comme **Atlassian Jira** et **ServiceNow**,ce qui permet aux service informatique d'agir facilement. InsightVM s'intègre également à Rapid7 **InsightConnect**, notre plateforme d'orchestration et d'automatisation de la sécurité, afin d'automatiser et de hiérarchiser le processus d'application des correctifs.

Remédier avec SecOps Agility

Pour évoluer plus rapidement et de manière plus sécurisée, vous devez aller au-delà de l'analyse en silos. InsightVM est conçu pour permettre la collaboration avec les opérations informatiques et les développeurs grâce à une visibilité, des analyses et une automatisation partagées.

À quoi cela ressemble-t-il dans la pratique ? InsightVM s'intègre aux workflows et aux systèmes de billeterie existants de l'informatique pour fournir des instructions de remédiation en fonction du contexte, ce qui accélère la remédiation, et fournit des rapports exploitables sur ll'avancement du programme pour tous les publics - de l'informatique et de la conformité à la C-Suite. Du côté du développement, InsightVM vous permet d'évaluer les conteneurs pour garantir la sécurité des services avant leur mise en production, et Rapid7 Insight Agent aide les équipes chargées de l'infrastructure à évaluer automatiquement les nouvelles infrastructures de cloud dès leur mise en service.

Conformité et configurations sécurisées, sans casse-tête

Montrez aux auditeurs comment votre environnement a évolué au fil du temps, en démontrant que vous êtes conforme aux normes OCI DSS, NERC CIP, FISMA (USGCB/FDCC), HIPAA/HITECH, Top 20 CSC, DISA STIGS et CIS pour la gestion des risques, des vulnérabilités et des configurations. Allez plus loin et renforcez vos systèmes en vous appuyant sur les meilleures pratiques du secteur, telles que CIS et DISA STIG, pour mettre votre réseau en ordre.

©RAPID7

"Ces dashboards sont la meilleure vue que nous ayons de notre posture de sécurités, et les workflows de remédiation permettent aux services informatiques d'intégrer facilement la remédiation dans le reste de leur travail."

- Centre médical de Sierra View

Prêt à commencer ?

Commencez dès aujourd'hui votre essai gratuit de 30 jours d'InsightVM.

Support

Appelez le +1.866.380.8113

Portail Client

MIEL