RAPID7

PRODUKTBESCHREIBUNG

InsightVM

Live-Schwachstellen-Management und Endpoint-Analytik

Ihr Netzwerk wächst. Nicht nur im klassischen Sinne, sondern auch durch die wachsende Bedeutung von Endpoints, Geräten und dem Internet der Dinge (IoT). Die Datenmenge wächst Jahr für Jahr beträchtlich, die Gefahr von Angriffen wird immer ausgefeilter und die Herausforderungen bei der Risikominimierung und Optimierung des Betriebs werden immer größer. Es mag sich wie ein Kampf anfühlen, den man nicht gewinnen kann, aber wir geben nicht auf und versuchen, die Transparenz zu erhalten, um alles zu sehen. Wozu? Für Antworten und Verständnis.

Die Identifikation, Priorisierung und Verwaltung von Schwachstellen bis zu deren Behebung ist nicht nur möglich, sondern kann auch einfach sein. Schon jetzt nutzen tausende Unternehmen Lösungen von Rapid7, um ihre Asset- und Schwachstellendaten in Antworten zu verwandeln und ihre Sicherheitsinitiativen zu stärken.

Rapid7 InsightVM ist die nächste Entwicklungsstufe beim Schwachstellen-Management. Getrieben durch unser preisgekröntes Nexpose-Produkt, nutzt InsightVM neuste Analytiken und Endpoint-Technologien, um Schwachstellen aufzudecken, deren Ort genau zu bestimmen, sie in Ihrem Unternehmen zu priorisieren und nachzuweisen, dass sich Ihr Risiko verringert hat.

„Dank des Endpoint Agent stellen diese Dashboards den besten Einblick in die Sicherheitslage unserer ganzen Organisation dar, und die Remediation Workflows erleichtern der IT die Remediation-Integration im Arbeitsalltag."

- Sierra Vista Medical Center

Im richtigen Moment handeln

InsightVM Live Monitoring und Adaptive Security geben Ihrem Schwachstellen-Management aktuelle Daten, genaue Risikobewertungen und das Wissen darüber, wonach Angreifer suchen, so dass Sie handeln können, während Veränderung stattfindet.

Live-Monitoring von Bedrohungen: Sammeln Sie aktuelle Daten und prüfen Sie diese automatisch auf Veränderungen und Bedrohungen und machen Sie damit Gegenmaßnahmen zu einer Sache von Minuten. Gleichzeitig erhalten Sie Live-Einblick in Schwachstellen, während diese auftreten.

Wechselnde Endpoints greifbar machen: Nutzen Sie Live Monitoring für Endpoints, unabhängig davon, ob Sie Adaptive Security oder Rapid7-Agents einsetzen, um mobile Arbeitskräfte und neue Geräte im Blick zu behalten. Kombinieren Sie Rapid7 InsightIDR, um ein umfassendes Bild der Risiken für Ihre Endpoints und Anwender zu erhalten.

Implementierung sicherer Konfigurationen: Härten Sie Ihre Systeme gemäß Best Practices der Branche, wie CIS und DISA STIG, um Ihr Netzwerk in Form zu bringen.

Anpassung an veränderte Umgebung: Mit InsightVM Adaptive Security können Sie neue Geräte automatisch erkennen und scannen, sobald diese in Ihr Netzwerk kommen, und identifizieren, welcher Geräte kritische Schwachstellen haben, sobald diese bekannt werden.

Skalierbarkeit als Schüsselfaktor: Ob Sie ein kleines Startup betreuen oder 1 Mio. IPs pro Tag scannen müssen, die Cloud-Analytik und die fortschrittlichen Erkennungsfähigkeiten (einschließlich der Integration von VMware und DHCP) von InsightVM erleichtern Ihnen die Verwaltung Ihres Schwachstellen-Managements. Unser Service-Team kann zudem alles für Sie aufsetzen, während Sie sich auf das konzentrieren, was wirklich zählt – Sicherheit.

Wie ein Angreifer denken

Keine zwei Schwachstellen sind gleich und Sie ändern sich zusammen mit den Aspekten Ihres Netzwerks. Das Wissen um die gefährlichste Schwachstelle erfordert aktuelle Daten und mehr als eine Liste alter Scan-Ergebnisse mit CVSS-Scores. Sie benötigen einen stets aktuellen Handlungsplan, der genau auf Ihr Unternehmen abgestimmt ist.

Fortschrittliche Bedrohungsanalytik: InsightVM übersetzt jahrzehntelange Erfahrung mit Angreifern in eine bewährte Analytik-Bibliothek. Angereichert durch aktuelle Daten von Agents oder Adaptive Security erkennt InsightVM Exposure Analytics Veränderungen, während diese geschehen, und priorisiert automatisch die Suche, so dass Sie schnell und sicher handeln können.

Risikobewertung ohne Wartzeiten: CVSS ist statisch, Angreifer aber sind dynamisch, und Sie dürfen nicht auf CVSS warten, um zu handeln. InsightVM ist der einzige Scanner, der für einen Exploit die Bedrohung, die Verfügbarkeit von Malware und das Alter betrachtet, um Schwachstellen genauso zu priorisieren, wie es ein Angreifer täte.

Geschlossener Regelkreis stellt Behebung sicher: Integrieren Sie InsightVM mit Metasploit, dem weltweit meistgenutzten Framework für Penetration Tests zur Echtzeit-Validierung, welche Systeme bedroht sind und welche Maßnahmen wirken.

Innovative Forschung für innovatives Sicherheit: Zapfen Sie Project Sonar von Rapid7 an, um zu verstehen, welche externen Netzwerkzugänge in Ihrer Betrachtung fehlen, und abonnieren Sie unsere Threat Feeds, um neue Schwachstellen schnell zu scannen und zu adressieren.

Betrachten Sie Ihren Score – von Compliance zum Fortschritt – mit Liveboards

InsightVM verwandelt Ihre Daten zum Bedrohungs-Management in detaillierte Visualisierungen mit denen Sie Ihre Ressourcen gezielt einsetzen können und jede Aktion mit allen beteiligten Abteilungen abstimmen können.

Liveboards statt Dashboards: Im Gegensatz zu den meisten Dashboards, die statisch und datengetrieben sind, zeigen die InsightVM Liveboards in Echtzeit, wie es steht. Sie nutzen dazu Live-Daten und zugängliche Analytiken, so dass Sie Ihre Bedrohungen visualisieren, priorisieren, zuweisen und beheben können.

Einfache Compliance und Reports: Zeigen Sie Auditoren, wie sich Ihre Umgebung über die Zeit verändert hat, wie Sie PCI DSS, NERC CIP, FISMA (USGCB/FDCC), HIPAA/HITECH, Top 20 CSC, DISA STIGS und CIS-Standards für Risiko-, Schwachstellen- und Konfigurationsmanagement erfüllen.

Erzählen Sie Ihre Geschichte und zeigen Ihren Fortschritt: Erstellen Sie einfach Reports um das übergreifende Programm zum Schwachstellen-Management verschiedenen Zielgruppen, von der IT- und Compliance-Abteilung bis zum Management vorzustellen.

Eine Plattform, die nicht nur Ihre Daten speichert: Die Insight-Plattform von Rapid7, die 2015 vorgestellt wurde, verbindet das Wissen aus der Schwachstellenforschung von Nexpose, die Exploit-Daten von Metasploit, Angreiferverhalten weltweit, Internet-weite Scan-Daten und Bedrohungsanalysen, um aus Ihren Daten Antworten zu liefern. Als einziger Anbieter, der zur CVE-Nummernvergabe berechtigt ist, versteht Rapid7 wie niemand sonst wie sich Ihr Netzwerk verändert und wie Angreifer denken.

Machen Sie sich die IT zum Freund und verbessern die Produktivität

Behebungsmaßnahmen von Hand sind zum Scheitern verurteilt. Die Alarmierung der IT in der Hoffnung, dass Dinge erledigt werden, führt in der Regel zu Reibung zwischen den Teams und keiner Verbesserung der IT-Sicherheit. Der InsightVM Remediation Workflow verwandelt Schwachstellendaten in Aktionen und hilft Ihnen, die Integration der Personen, Teams und Technologien voran zu treiben.

Planen, Ausführen und Überwachen der Behebung: Zeigen Sie Ihrem Team genau, was behoben werden muss und warum. Priorisieren Sie je nach Wahrscheinlichkeit der Nutzung bei einem Angriff; wenn sie heute nur 10 Probleme beheben können, wissen Sie, dass es die richtigen sind. Indem Sie Ihre bestehende Ticketing-Lösung integrieren, können IT-Teams die Behebung nahtlos in ihre bestehenden Tätigkeiten einordnen.

Nutzen Sie Ihre Sicherheits-Tools bestmöglich: InsightVM ist eine Ressource mit großer Datenfülle, die andere Lösungen in Ihrem Portfolio unterstützen kann, von SIEM über Firewalls bis hin zu Ticketing-Systemen. Nur InsightVM integriert mit über 50 anderen führenden Technologien, wie McAfee ePO, ServiceNow und führenden SIEM-Anbietern; mit der offenen InsightVM-API können Ihre bestehenden Daten Ihre anderen Werkzeuge noch wertvoller machen.

Asset-Organisation: Ordnen Sie Assets nach Ort und Besitzer, um schnell zu erkennen, wer was besitzt. Markieren Sie diejenigen Assets, die für Ihr Unternehmen von größter Bedeutung sind, um deren Risikobewertung automatisch zu erhöhen und an die Spitze Ihrer Remedation Reports zu setzen.

GET STARTED TODAY

Call: +49 89 97 007 007

Email: sales@rapid7.com

Try: www.rapid7.com/InsightVM