

InsightIDR

Von der Bedrohung zur Abwehr. Schnell.

Verabschieden Sie sich von schlaflosen Nächten und dem flauen Gefühl, dass die Bösen auch weiterhin in Ihrer IT-Umgebung sind. InsightIDR ist die einzige vollständig integrierte Lösung, mit der Sie Eindringlinge noch während des Angriffs erkennen und untersuchen können, bevor alles außer Kontrolle gerät.

BRINGEN SIE LICHT INS DUNKEL, UM DIE ANGRIFFE ZU ERKENNEN

Erhalten Sie zu viele wertlose Warnungen?

Rapid7 InsightIDR nutzt Angriffsanalytiken, um Einbrüche zu erkennen und die Anzahl falscher Warnmeldungen und damit tagelange Arbeit für Ihr Security-Team zu reduzieren. Es sucht nach Aktionen, die auf kompromittierte Zugangsdaten hinweisen, erkennt Querbewegungen innerhalb der Assets, spürt Malware auf und stellt Fallen für Eindringlinge.

An neue Bedrohungen anpassen

InsightIDR unterstützt maschinelles Lernen, sodass sich die Lösung mit den Verhaltensweisen der Angreifer ständig weiterentwickelt.

Verstecke der Angreifer identifizieren

InsightIDR überwacht und verfolgt schadhafte Prozesse und Protokollmanipulationen, um den Missbrauch lokaler Konten zu identifizieren.

Eindringlinge in die Irre führen

InsightIDR vereinfacht das Aufspüren von Eindringlingen mithilfe von Fallen, wenn diese eine erste Erkundung des Netzwerkes durchführen, noch bevor Schäden angerichtet werden können.

Die Flut an Warnmeldungen reduzieren

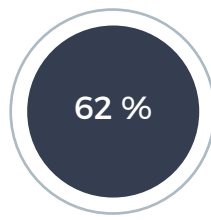
Die Intruder-Analyse von InsightIDR, die auf jahrelanger Erfahrung unserer Incident Response-, Penetration-Test- und Metasploit-Teams basiert, spürt schnell potentiell gefährliches Angriffsverhalten auf.

SCHNELLERE UNTERSUCHUNG VON VORFÄLLEN

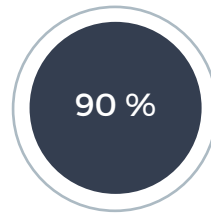
Nimmt die Untersuchung von Vorfällen viele Stunden mühsamer Arbeit in Anspruch? Bevor eine Untersuchung überhaupt beginnt, verarbeitet InsightIDR in Sekundenschnelle Daten aus allen Netzwerken und weist Ereignisse bestimmten beteiligten Benutzern und Assets zu. Damit können Ihre Security-Experten schneller die gesamte Umgebung nach Hinweisen eines aufgespürten Angriffs durchsuchen.



Bei 33 % aller gemeldeten Vorfälle dauert es länger als einen Monat und bis zu einem Jahr, um sie zu entdecken.
- Verizon- Data Breach Investigations Report 2014/15



62 % der Unternehmen erhalten mehr Meldungen als sie bearbeiten können.*



90 % der Unternehmen befürchten Angriffe mit gestohlenen Zugangsdaten.*

* Daten aus der Rapid7 2015 Incident Detection and Response Survey

Fehlende Puzzleteile mit sonderbarem Verhalten auffinden

InsightIDR erstellt eine Zeitachse aller wesentlichen Ereignisse, sodass die Sicherheitsteams Vorfälle bis zur Wurzel zurückverfolgen können.

Bringen Sie Endpoint-Daten in einen Kontext ohne Benutzerunterbrechung

InsightIDR ermöglicht Ihnen, kontextbezogene Endpoint-Daten On-Demand zu ziehen, ohne die Arbeit der Benutzer zu unterbrechen – selbst dann, wenn der Benutzer unterwegs und nicht im Unternehmensnetzwerk eingeloggt ist.

Das Ausmaß eines Angriffs bestimmen

Angrifer nutzen nur selten einen Zugriffspunkt. Mit der fortschrittlichen Suche von InsightIDR können die Sicherheitsanalysten schnell von der Auswertung eines Vorfalls auf die Bestimmung des Ausmaßes schließen, um den Vorfall möglichst zeitnah unter Kontrolle zu bekommen.

BEENDEN SIE DIE PLAGEREI BEIM MANAGEMENT VON SECURITY-DATEN

Verbringen Sie zu viel Zeit damit, Daten und Berge von Regeln zu verwalten? InsightIDR ist eine einzelne Lösung mit einer umfangreichen Datenabdeckung und Transparenz. Im Vergleich zu vielen anderen SIEMs und Technologien, die überwiegend auf Compliance ausgerichtet sind, erweitert InsightIDR die Datenerfassung und Erkennung von Endpoints, sowie die beliebten Cloud-Anwendungen.

Erhalten Sie den Mehrwert in Tagen, nicht in Wochen oder Monaten

Sie müssen nicht mehr wochenlang warten, um Ihre Sicherheitsdaten und Analyseplattform einzurichten. Die Cloud-basierte Lösung von InsightIDR lässt sich mit Ihren internen Datenquellen verbinden und senkt den Aufwand und die Zeit zum Einrichten und Pflegen der Datenerfassung, -aktualisierung und -verwaltung.

Darstellung Ihrer Sicherheitsdaten in einem einzigen, korrelierenden Kontext. InsightIDR bringt Daten über Assets, Benutzer und Verhaltensweisen in einer Ansicht zusammen, sodass Analysten nicht länger zwischen Tools hin und her springen müssen. Das spart Zeit und ermöglicht eine schnelle Untersuchung von Vorfällen.

Kreuzen Sie das Compliance-Kästchen an. PCI DSS erfordert die Protokollierung aller Ereignisse, die Prüfung von Sicherheitsmeldungen und die Dokumentation der Ergebnisse von Untersuchungen. InsightIDR erfüllt all diese Anforderungen ohne die Notwendigkeit eines SIEM.

Umfangreiche Transparenz des gesamten Netzwerks. InsightIDR bietet Security-Teams eine umgehende Einsicht auf alle Netzwerke sowie sämtliche potentielle Gefahren, ohne darauf warten zu müssen, dass komplexe Regeln geschrieben und genehmigt werden müssen.

„[Mit InsightIDR] stehen mir alle Informationen zur Verfügung, die ich zum Verstehen und Lösen eines Problems benötige.“

-Jordan Schroeder, Security Architect, Visier

STARTEN SIE NOCH HEUTE

Starten Sie Ihre 30-tägige kostenlose Testversion unter:
www.rapid7.com/products/insightidr