

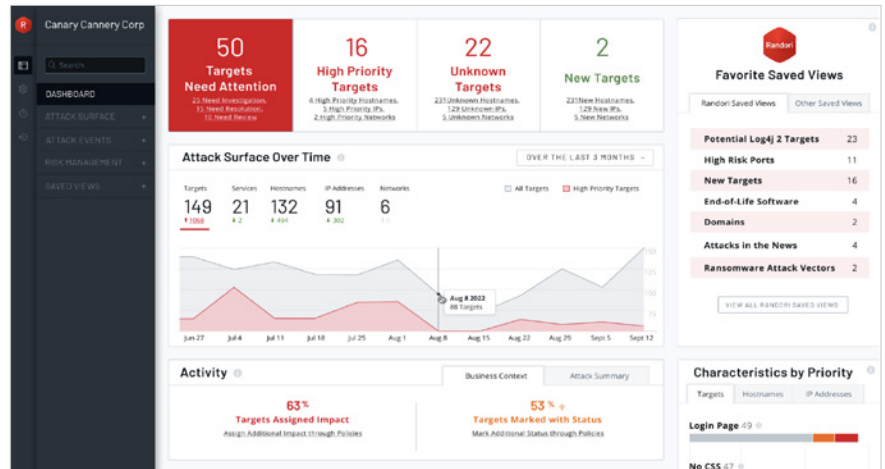
IBM Security Randori Recon: Angriffsflächenmanagement

Ihre Angriffsfläche aus Sicht des Angreifers

Um zu wissen, wo Angreifer zuschlagen werden, wie diese Ihre Angriffsfläche beurteilen. IBM® Security Randori Recon bietet fortlaufende Assesterkennung und Problempriorisierung aus Sicht des Angreifers.

Durch Cloud-Migrationen, Schatten-IT sowie Fusionen und Übernahmen (M&A) ändert sich Ihr Perimeter fortlaufend. Diese Veränderungen erzeugen Ansatzpunkte für Angreifer. Mit Randori Recon können Sie sie selbst entdecken – keine Installation oder Konfiguration erforderlich.

Genau wie echte Bedrohungsakteure überwacht Randori Recon fortlaufend Ihre externe Angriffsfläche und deckt so blinde Flecken, fehlerhafte Konfigurationen und Prozessfehler auf, die ansonsten unbemerkt bleiben würden. Mithilfe eines Black-Box-Ansatzes findet Randori IPv6- (Internet Protocol Version 6) und Cloud-Assets, die von anderen übersehen werden.



„Dank Randori kann ich mit dem Führungsteam vollkommen anders kommunizieren. Der Zugriff auf eine umfangreiche und fortlaufende externe Beurteilung unserer Angriffsfläche erlaubt es mir, das Angriffsflächenrisiko zu einer Metrik auf Firmenebene zu machen.“

Douglas Graham
Chief Trust Officer
Lionbridge

Wichtige Anwendungsfälle

- Angriffsflächenerkennung
- Schatten-IT
- Schwachstellenpriorisierung
- M&A-Risiko
- Angriffe in der Presse

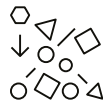
Hauptvorteile

- **Erkennung von Unbekannten**
Betrachten Sie Ihren Perimeter wie ein Angreifer und decken Sie auf diese Weise fehlerhafte Konfigurationen und Prozessfehler auf. Keine Installation erforderlich.
- **Priorisierung von Erkenntnissen**
Ermitteln Sie die Hauptziele Ihres Angreifers mit unserem auf Hacker-Logik basierenden Modell, das zum Patent angemeldet wurde.
- **Reduzierung der Angriffsfläche**
Seien Sie Schatten-IT, M&A und unerwarteten Veränderungen immer einen Schritt voraus.
Alerts informieren Sie über neue Risiken, sobald sie erkannt werden.

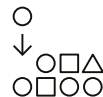
Funktionsweise von Randori Recon



E-Mail eingeben: Für die reibungslose Einrichtung ist lediglich eine E-Mail-Adresse notwendig



Angriffsfläche erkennen: Randori durchsucht das Internet, um Assets mit Internetverbindung zu erkennen, zuzuordnen und zu identifizieren



Erkenntnisse priorisieren: Angreifer werden zur automatischen Bewertung und Priorisierung der verlockendsten Angriffsziele nachgeahmt

Was macht Randori Recon so einzigartig?

1. Authentische Erkennung

Angreifer beginnen nicht damit, das gesamte Internet zu scannen – und wir auch nicht. Wir nutzen dieselben Techniken wie Angreifer. Das ermöglicht es uns, die IPv6- und Cloud-Assets zu finden, die andere übersehen.

2. Fortlaufender Einblick

Randori bleibt stets wachsam und auf der Suche nach neuen Assets und Veränderungen Ihrer Angriffsfläche. Identifizieren Sie schnell Probleme mithilfe unseres zum Patent angemeldeten Target-Temptation-Modells, das auf Basis der Angreifertrends und der Daten von IBM Security Randori Attack aktualisiert wird.

3. Proaktive Korrektur

Erhalten Sie Informationen über gefährdete Assets, wie sie erkannt werden können, welches Risiko besteht und was Sie tun sollten – bevor Angreifer zuschlagen. Sie brauchen Beweise? Prüfen Sie Ihr Risiko mithilfe von Randori Attack.

Was spricht für IBM?

IBM Security Randori Recon bietet Angriffsflächenmanagement (ASM) auf einer zentralen einheitlichen Plattform und ermöglicht dadurch eine fortlaufende, proaktive und authentische offensive Sicherheitserfahrung. [Erfahren Sie mehr](#) über Randori Recon und darüber, wie Sie und Ihr Unternehmen Angreifern damit stets einen Schritt voraus sein können.

© Copyright IBM Corporation 2022

IBM Deutschland GmbH

IBM-Allee 1
71139 Ehningen
[ibm.com/de](https://www.ibm.com/de)

IBM Österreich

Obere Donaustraße 95
1020 Wien
[ibm.com/at](https://www.ibm.com/at)

IBM Schweiz

Vulkanstrasse 106
8010 Zürich
[ibm.com/ch](https://www.ibm.com/ch)

Produziert in den
Vereinigten Staaten von Amerika
September 2022

IBM und das IBM-Logo sind Marken oder eingetragene Marken der International Business Machines Corporation, eingetragen in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der Marken von IBM finden Sie auf [ibm.com/trademark](https://www.ibm.com/trademark).

Das vorliegende Dokument ist mit Stand vom Datum der ersten Veröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

Es liegt in der Verantwortung der Anwender, die Nutzbarkeit anderer Produkte oder Programme neben den Produkten und Programmen von IBM zu evaluieren und verifizieren. DIE INFORMATIONEN IN DIESEM DOKUMENT WERDEN OHNE JEDLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE ZUR VERFÜGUNG GESTELLT, EINSCHLIESSLICH DER GARANTIE DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER GARANTIE ODER BEDINGUNG DER NICHTVERLETZUNG VON RECHTEN. Die Garantie für Produkte von IBM richtet sich nach den Bestimmungen und Bedingungen der Vereinbarungen, unter denen sie bereitgestellt werden.

