IBM Security Randori Recon:

Attack surface management

See your attack surface like an attacker

To know where attackers will strike, you first need to know how they view your attack surface. IBM® Security Randori Recon provides continuous asset discovery and issue prioritization from an attacker's perspective.

With cloud migrations, shadow IT, and mergers and acquisitions (M&A), your perimeter is constantly changing. These changes represent windows of opportunities for attackers. Discover them with Randori Recon—no installation or configuration required.

Just like real threat actors, Randori Recon continuously monitors your external attack surface, uncovering blind spots, misconfigurations and process failures that would otherwise be missed.

Using a black-box approach, Randori finds the Internet Protocol version 6 (IPv6) and cloud assets that others miss.

All enquiries online@scc.com
Contact our team 0121 766 7000
Visit scc.com

Randori has changed the conversations I am able to have with the executive team. Having a rich and continuous external assessment of our attack surface has enabled me to make attack surface risk a company-level metric."

Douglas Graham

Chief Trust Officer
Lionbridge

What sets Randori Recon apart?

Authentic discovery
Attackers don't start by scanning the entire internet, and neither do we. We use the same techniques attackers do, allowing us to find the IPv6 and cloud assets that others miss.

Continuous insight:
Randori is always watching, looking for new assets and changes in your attack surface. Identify issues fast with our patent-pending Target Temptation model, which updates based on attacker trends and IBM Security Randori Attack data.

Proactive remediation:
Understand what's exposed, how it can be discovered, what the risk is and what you should do—before attackers strike. Need proof? Validate the risk with Randori Attack.

Key use cases

- Attack surface discovery
- Shadow IT
- Vulnerability prioritization
- M&A risk
- Attacks in the news

How Randori Recon works

Enter email: Low-friction setup only requires an email address to get started

Discover attack surface: Searches internet to discover, associate and identify internet-facing assets

Prioritize findings: Emulates adversary to automatically score and prioritize the most tempting targets for attack

Key benefits

- **Discover your unknowns**
  View your perimeter like an attacker to expose misconfigurations and process failures. No installation required.
- **Prioritize your findings**
  Pinpoint an attacker's top targets with our patent-pending model built on hacker logic.
- **Reduce your attack surface**
  Stay a step ahead of shadow IT, M&A, and unexpected change. Alerts inform you of new risks as they arise.

Why SCC and IBM?

With an incredible 40-year partnership, SCC is the UK's first IBM Platinum Business Partner. We collaborate to deliver next-level solutions, helping businesses amplify their operations with world-class technology, whilst prioritising optimum safety and security. For added peace of mind, our dedicated experts are always by your side when you need us most.

This is what incredible technology solutions truly look like.

All enquiries online@scc.com
Contact our team 0121 766 7000
Visit scc.com