



Internet Footprint Review

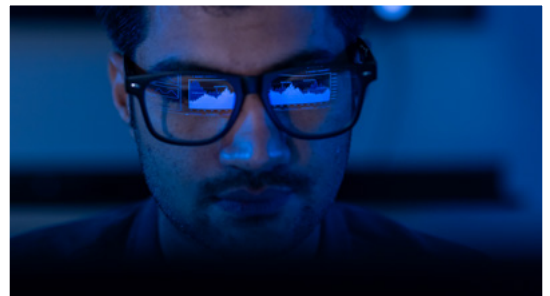
Intelligence-driven defence



Receive a clear understanding of your exposure, what matters most, and where to focus your remediation efforts for maximum risk reduction.

In many cases attackers are cautious when gathering information in preparation for an attack, avoiding “noisy” vulnerability scanners that can be easily detected by defenders, opting more for lower hanging fruits.

Our Internet Footprint Review provides a view of your digital footprint through the eyes of an attacker, using publicly available information and open-source intelligence.



What you'll gain from our Internet Footprint Review

We provide a report highlighting the information and exposures an attacker may identify when researching your organisation online.

By identifying areas of exposure early, organisations can better understand their risk profile and take targeted action before issues are leveraged by malicious actors.



Identify externally exposed assets



Discover vulnerable internet-facing services



Detect credential exposure and data leakage



Understand potential phishing targets



Know where attackers are most likely to succeed and prioritise action to reduce risk.



What attackers commonly look for across your digital footprint

Exposed credentials

Username, passwords and corporate email addresses that have appeared in public breaches can be used to gain unauthorised access or support credential-stuffing attacks.

Potential phishing targets

Employee information, email patterns and publicly available business details can help attackers craft convincing phishing and social engineering campaigns.

Internet-facing services

Unnecessary or poorly secured internet-facing systems can provide attackers with an entry point into your environment.

Open ports and weak configurations

Misconfigured services, exposed management interfaces and outdated protocols may create opportunities for compromise.

Vulnerable technologies

Publicly visible software versions and technologies may reveal known vulnerabilities that attackers actively target.

External attack surface

Domains, cloud services, subsidiaries and forgotten assets can expand your attack surface and create blind spots that introduce risk.

Why work with us?



Gain an unbiased view of your exposure. Our external assessment helps uncover risks that can be easily overlooked from inside the organisation.



Our team combines threat intelligence, cyber consulting and operational cyber expertise to provide practical recommendations, not just observations.



Recommendations are prioritised by risk, helping you focus effort where it will have the greatest impact.

Know your exposure, reduce your risk. Contact us today

