SECURE IMPACT

Your security team.

Digital Footprint

Our digital footprint service allows a business, members of its C-suite, or a HNWI to understand their attack surface from a human and technical perspective. Using passive techniques only, to minimise disruption to the client, digital foot printing shows you everything a potential adversary could access and collect with the intention to then leverage against you and/or your business.

Secure Impact offer a digital footprint service which is conducted remotely and results in zero disruption to your business or day-to-day life as an individual. This is in part down to the tools, technologies and military-led passive techniques used to collect information.

Our digital reconnaissance team have a unique and necessary skillset to conduct in-depth research into an organisation, its C-suite leadership team or a HNWI to portray them and any vulnerabilities from the view of an external entity.

The aim is to determine your attack surface without the need for intrusion. We will determine what information is available which may be used for phishing, impersonation, blackmail resulting in insider threat, and more.

Examples include but not limited to:

- Compromising photos of employees or individuals which can be leveraged to provide access to a network
- Metadata providing BYOD details allowing adversaries to target those devices
- Compromised email addresses
- Open cameras within your organisation or domestic life

This service is scalable dependent on the client requirements and size of the organisation.

A full threat assessment will be provided as part of the service including recommendations to reduce the potential attack surface.

What we Collect

- Organisation/Individual Network
- Geographical Intelligence
- Phone Numbers
- Email & IP Addresses
- DNS, Mail Servers, URLs
- Open Ports & Services including internal camera feeds
- Key Stakeholders & Hierarchy including their information (Social Media accounts etc.)
- Usernames / Accounts
- Website technologies

Key Benefits

- Visibility of employee-borne threats
- Protection of key stakeholders e.g., CEO or HNWI and their personal life
- Protection of physical assets
- Zero disruption