+44 345 094 0945
www.waterstons.com

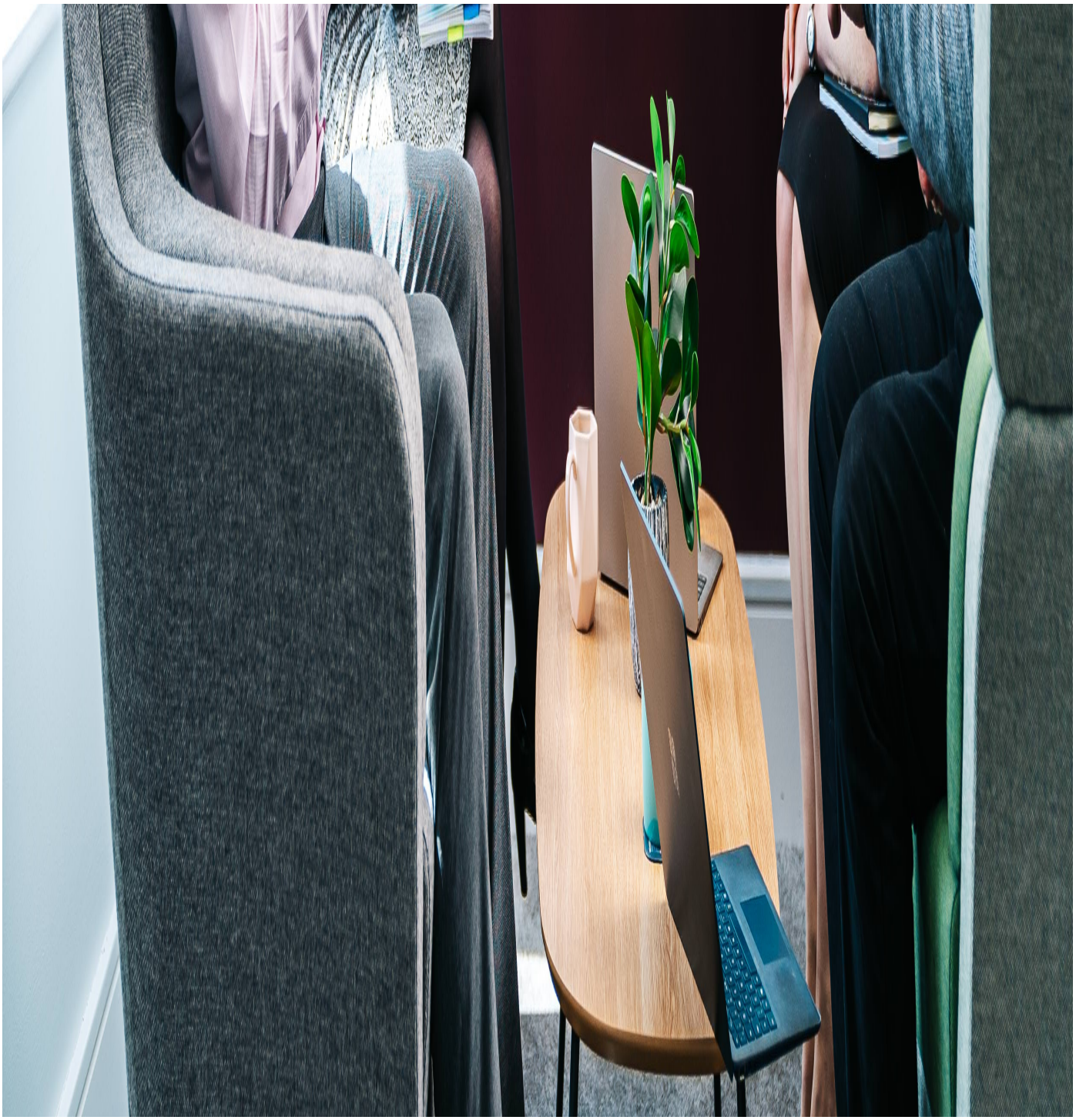
Article

Aug 2023

What is OSINT?

OSINT (Open Source Intelligence) is a valuable technique used to gather information from publicly available sources, such as websites, social media platforms, forums, and other online resources.

Craig Archdeacon
Head of Cyber Assurance
Email craig.archdeacon@waterstons.com



When it comes to identifying vulnerabilities within organisations, OSINT plays a crucial role by providing insights into potential weaknesses that can be exploited by attackers to gain unauthorised access to external and internal systems.

In the digital age, organisations have an extensive online presence, making a significant amount of information available to anyone with internet access. This includes details about their infrastructure, technologies, employees, partners, and even sensitive information inadvertently disclosed through various channels.

By leveraging OSINT techniques, attackers can piece together this publicly available information to identify potential vulnerabilities and launch targeted attacks.

Website Analysis

Attackers can analyse an organisation's website to extract valuable information about its infrastructure, content management systems, plugins, and other technologies in use. Outdated software versions or known vulnerabilities can be identified, providing an opportunity for exploitation.

Social Media Monitoring

Employees often share information about their work on social media platforms. Attackers can gather insights into an organisation's internal structure, departments, key personnel, and even potential weak links in security by monitoring social media accounts.

Employee Information

OSINT can reveal personal details of employees, including their roles, email addresses, and contact information. This information can be exploited for phishing attacks, social engineering, or targeted attacks against specific individuals.

Data Leaks and Breaches

Publicly accessible databases, leaked credentials, and data breaches can provide a wealth of information about an organisation's infrastructure, systems, and vulnerabilities. By aggregating this data, attackers can identify weak points that have not yet been addressed.

Third-Party Information

Organisations often collaborate with external partners, vendors, or contractors so by examining information available about these third parties, attackers can identify potential weak links that can be targeted to gain unauthorized access to the organisation's systems.

To mitigate the risks associated with OSINT-based attacks, organisations should adopt robust security practices, including:

- Regularly monitoring and assessing their online presence.
- Implementing strict social media guidelines for employees.
- Conducting regular security audits and vulnerability assessments.
- Educating employees about the risks associated with disclosing sensitive information online.
- Maintaining up-to-date software and promptly patching vulnerabilities.
- Monitoring and responding to data breaches and leaks promptly.

By recognising the power of OSINT, and taking proactive measures to protect their online presence, organisations can significantly reduce the risk of being targeted and exploited by attackers leveraging publicly available information.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members - 24/7

info@waterstons.com.au | 02 9160 8430