COGNISYS

MANAGED SERVICES

OSINT analysis

Personal data is the perfect starting point for cyber criminals.

Open-Source Intelligence (OSINT) gathers information from published or otherwise publicly available sources. Identifying unintentional leakage of sensitive data through social media networks and other platforms can help you plug the leaks and make it as difficult as possible for potential attackers.

The OSINT Analysis service demonstrates how much information a threat actor can find about an organisation quickly and easily online, without ever touching your system or running any scans.

Information discovered may include the exposure of data, breached work email credentials, personal staff data and other useful identity information. Your public data footprint is probably much bigger than you think. You can access electoral registers and telephone numbers through a regular web browser.

Companies House stores company data, including officers data. Company websites often display hierarchical team structures. Platforms such as Facebook, Instagram, LinkedIn, TikTok and X hold personal data on individuals, including friends, interests, hobbies, activities, pictures and events.

Not hacking, just looking

It is not uncommon for threat actors to use open-source intelligence tools and techniques to discover potential targets and exploit weaknesses in networks. As soon as a vulnerability or a weakness is identified, it can be used to accomplish a breach.

OSINT is often initial reconnaissance for sophisticated social engineering campaigns using smishing, spear-phishing, whaling and vishing against a target. Social engineering campaigns use seemingly innocuous information shared in social networks or blogs to develop compelling campaigns and trick people into compromising their organisation. The importance of OSINT Analysis becomes apparent when it uncovers weaknesses in your organisation's user network and helps you to remove sensitive information before it's used for exploitation.

Method

Using our OSINT Framework, the scope can be tailored to each organisation according to specific requirements. Searches utilise specialist tools to uncover the maximum results. Analysis typically includes:

- Search of the dark web for personal and company data.
- Search of social platforms including imagery.
- Assess common TLS/SSL issues.
- Search of the organisation's digital footprint for information and metadata.
- Web search for names, emails, addresses and phone numbers of staff.
- Search of DNS records and ensure they are configured correctly.
- Attempt to discover technologies used, e.g., on the website or infrastructure, which would provide a threat actor with useful information.
- Check for suspicious behaviour of the domain, website, and IP.

Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BACK TO CONTENTS