
WÜRTHPHOENIX
EXPOSURE ASSESSMENT
SEARCH ALL THINGS ABOUT YOUR ORG

WHAT IS IT FOR?

Identify and continuously monitor attack surfaces, manage exposed data over time and respond proactively to avoid potential exploits.
The Exposure Assessment service identifies **misconfigurations,** unmanaged **vulnerabilities** and **malicious activities** that are difficult for your organisation to control.

misconfiguration	malicious activity	unmanaged vulnerabili-
sensitive paths exposed	spear phishing	public exploitation
industrial devices exposure	similar domains creation	unmanaged vulnerability disclosure
SSL weaknesses	cloned mobile apps	promiscuous e-mail account usage
display of metadata	credential stuffing	presence within blacklists
management interfaces exposure	password guessing	technologies usage details

WHAT'S INVOLVED?

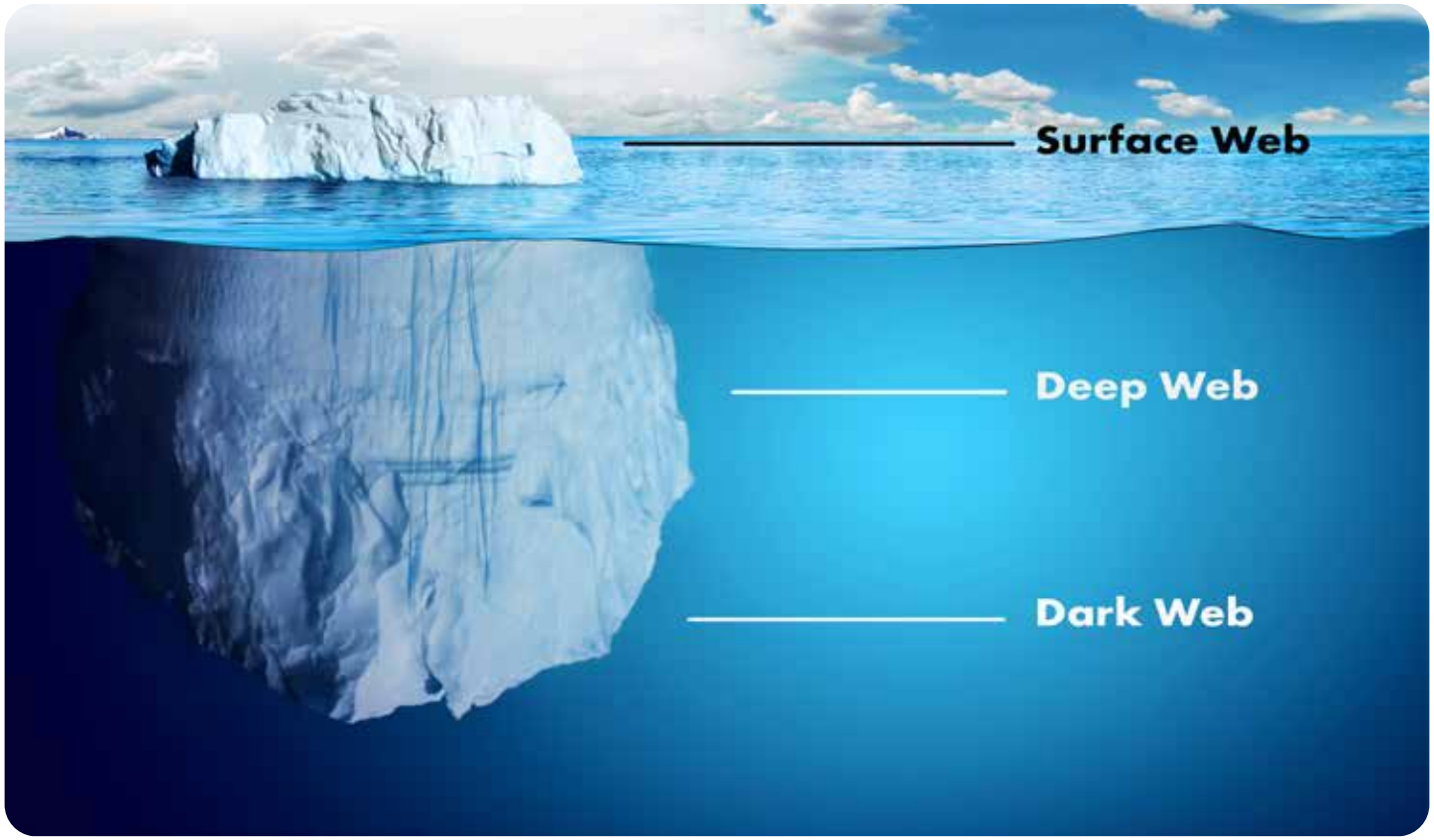
The Exposure Assessment service uses the SATAYO software platform, fully developed and continuously updated by the Würth Phoenix cyber security team. SATAYO is designed to check your organisation's exposure and anticipate attacks from cyber criminals.

HOW DOES IT WORK?

SATAYO is an OSINT and Threat Intelligence system that searches for evidence traceable to your organisation within public domain sources on the Surface Web, Deep Web and Dark Web. SATAYO mimics the actions of cyber attackers during the initial phase of an attack.

satayo

SEARCH ALL THINGS ABOUT YOUR ORG



The features of SATAYO

- Responsive web interface
- Data Analysis Dashboard
- Web based and exportable reports
- Summary Executive Report
- Exposure Assessment Index Value
- Exposure trend over time
- Notifications
- Data export in CSV format and via API
- Option to integrate with SIEM platforms
- Feed reputation
- Online documentation
- Multilingual and multichannel tech support

WHAT DO WE OFFER?

Using basic information, like the organisation's domain names and some keywords (services, products, names of key people), SATAYO compiles data on a daily basis, such as hostnames, IPs, emails, usernames, files, phone numbers, passwords, similar domains and data breaches.

Benefits of SATAYO

Unlike other platforms on the market, SATAYO is able to:

- Carry out targeted and customised research based on your organisation's domain
- Continuously monitor exposure trends over time
- Provide an exposure index based on accurate metrics

Managed service

Exposure Assessment is also available as a managed service, which actively involves the cyber security team in supporting the client to mitigate and resolve any critical issues.

Consultancy and support

During the service start-up phase, the cyber security team works with your organisation to identify which elements to monitor. SATAYO is periodically updated through the release of new features and integration of the latest OSINT and Threat Intelligence sources.

WÜRTHPHOENIX

OUR SERVICES

DEFENSIVE

EXPOSURE ASSESSMENT
OneTime | SaaS | SaaS&Managed

VULNERABILITY ASSESSMENT
OneTime | On-Prem

GAP ANALYSIS

SECURITY TRAINING

OFFENSIVE

PENETRATION TEST

PASSWORD AUDIT

SOCIAL ENGINEERING

RED TEAMING

www.wuerth-phoenix.com
info@wuerth-phoenix.com