
WÜRTHPHOENIX
EXPOSURE ASSESSMENT
SEARCH ALL THINGS ABOUT YOUR ORG

IHRE VORTEILE

Angriffspunkte zu erkennen und kontinuierlich zu überwachen, exponierte Daten langfristig zu verwalten und proaktiv zu reagieren, um potenzielle Schwachstellen zu vermeiden.

Mit dem Service Exposure Assessment können **Fehlkonfigurationen**, nicht gemanagte **Schwachstellen** und **schädliche Aktivitäten** identifiziert werden, die Ihre Organisation andernfalls nur schwer unter Kontrolle halten kann.

Fehlkonfiguration	Schädliche Aktivitäten	Nicht gemanagte Schwachstellen
Sensitive Paths Exposed	Spear Phishing	Public Exploitation
Industrial Devices Exposure	Similar Domains Creation	Unmanaged Vulnerability Disclosure
SSL Weaknesses	Cloned Mobile Apps	Promiscous E-Mail Account Usage
Display Of Metadata	Credential Stuffing	Presence Within Blacklists
Management Interfaces Exposure	Password Guessing	Technologies Usage Details

WORUM GEHT ES?

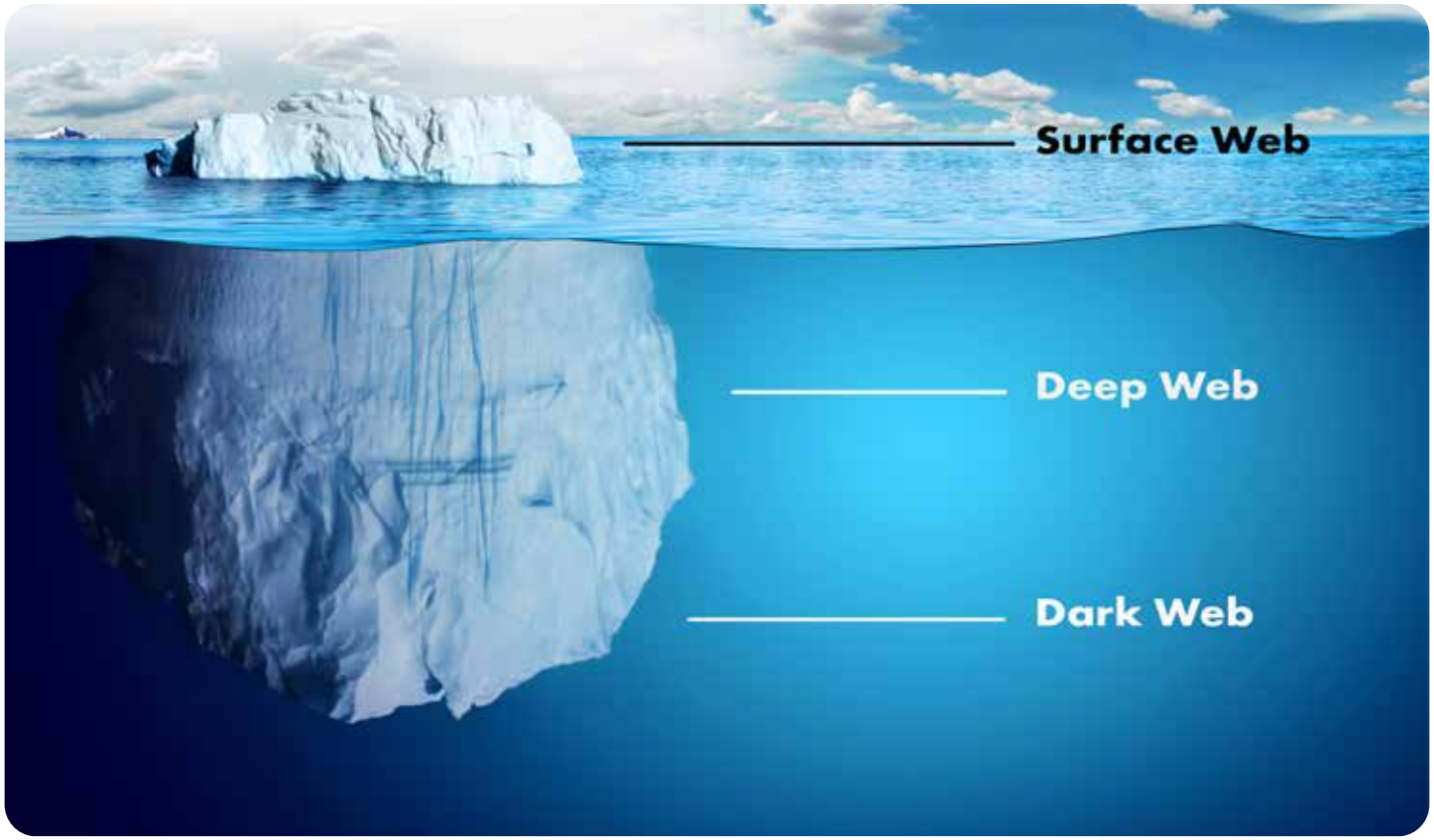
Grundlage für den Dienst „Service Exposure Assessment“ ist die Nutzung der Software-Plattform SATAYO, eine komplette Eigenentwicklung des Würth Phoenix Cyber Security-Teams, die konstant aktualisiert wird. SATAYO ist in der Lage, die Exposure Ihrer Organisation zu prüfen, um den Angriffen von Cyberkriminellen zuvorzukommen.

So funktioniert‘s

SATAYO ist eine OSINT- und Threat Intelligence-Plattform, die in öffentlich zugänglichen Quellen im Internet, im Deep Web und Darknet Elemente sammelt, die auf Ihre Organisation zurückführbar sind. SATAYO simuliert das Vorgehen von Cyber-Angreifern in der ersten Phase des Angriffs.

satayo

SEARCH ALL THINGS ABOUT YOUR ORG



Die Funktionen von SATAYO

- Web Responsive Interface
- Data Analysis-Dashboard
- Report online mit Exportfunktion
- Summary Executive Report
- Exposure Assessment Index Value
- Verlauf der Exposure-Entwicklung
- Meldungen
- Datenexport als CSV-Datei und mit API
- in SIEM-Plattformen integrierbar
- Feed Reputation
- Online-Dokumentation
- Mehrsprachiger technischer Support über verschiedene Kanäle

WAS BIETEN WIR?

Über einfache Informationen, wie die Internet-Domains Ihrer Organisation und ein paar entsprechende Keywords (Dienstleistungen, Produkte, Personen in Spitzenpositionen) sammelt SATAYO tagtäglich verschiedenste Elemente wie Hostname, IP, E-Mail, Username, Datei, Telefonnummer, Passwort, ähnliche Domains und Data Breach.

Die Vorteile von SATAYO

Anders als bei vergleichbaren Plattformen kann SATAYO:

- eine gezielte, passgenaue Recherche auf der Grundlage der Domain Ihrer Organisation durchführen
- kontinuierlich die Entwicklung der Exposure im Auge behalten
- einen Exposure-Index auf der Grundlage präziser Parameter liefern



Managed Service

Das Exposure Assessment wird auch als Managed Service, also mit aktiver Beteiligung des Cyber Security-Teams angeboten, um unseren Kunden bei der Eindämmung und Lösung der festgestellten Schwachstellen zur Seite zu stehen.



Beratung und Support

In der ersten Phase unterstützt das Cyber Security-Team Ihre Organisation bei der Identifizierung aller Elemente, die überwacht werden müssen. SATAYO wird regelmäßig durch die Freigabe neuer Funktionen und die Einbindung der neuesten Quellen für OSINT und Threat Intelligence aktualisiert.



WÜRTHPHOENIX

UNSERE LEISTUNGEN

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