

Findalyze[®]

Attack Surface Explorer



Risiko-Management für KMU

Findalyze bietet mehr als die reine Erkennung von bekannten Schwachstellen. Wir verfolgen jede Änderung in Ihrer externen IT-Infrastruktur, ob verwundbar oder nicht, und priorisieren die Funde für eine effektive Behebung.

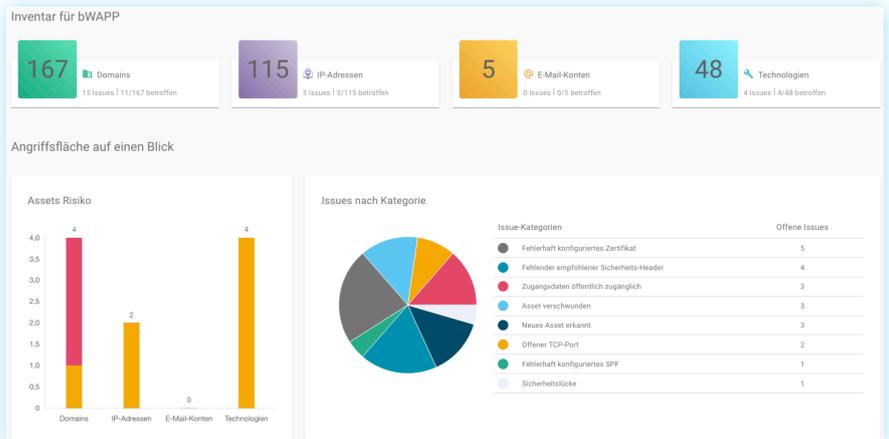
Findalyze ist Enterprise Technologie für KMU.

Findalyze Dashboard

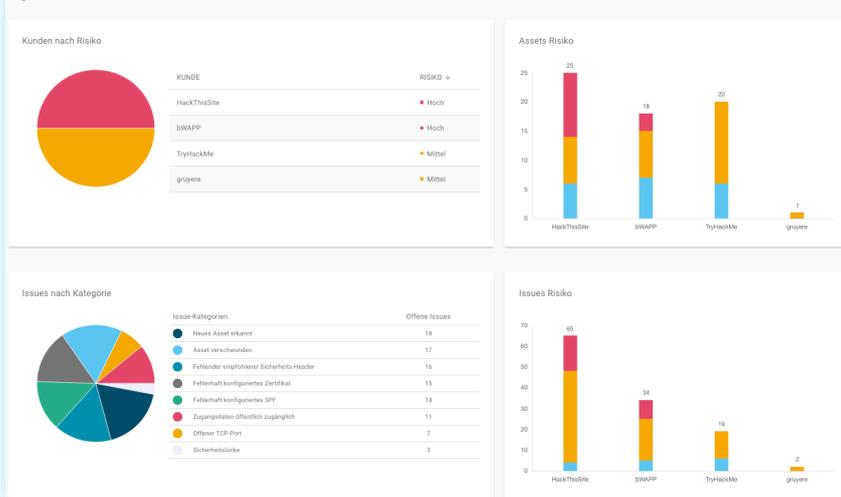
Sehen Sie, was ein Angreifer sieht und erfahren Sie alles über die Beschaffenheit und die Veränderungen Ihrer digitalen Angriffsfläche direkt im Findalyze Dashboard.

Alle Ihre Assets stets im Blick

Sie haben immer einen aktuellen Überblick über Ihre externen IT-Assets. Etwas Neues wird entdeckt? Kein Problem! Findalyze zeigt es Ihnen an. Ein Asset ist nicht mehr online? Auch das erkennt Findalyze.



Angriffsfläche der Kunden auf einen Blick



Multi Tenancy

Mit dem Tenant-Dashboard haben Sie für alle Mandanten ein Inventory mit allen Risiken.

Springen Sie aus dem Dashboard direkt in den Mandanten für noch mehr Informationen.

Kundenübergreifende kürzliche Aktivitäten

Die kürzlich gefundenen Issues helfen dabei, Änderungen der Angriffsfläche über Kunden hinweg zu verfolgen. Ähnlich wie bei den individuellen Kundendashboards führen wir ebenfalls eine Ansicht mit kürzlichen Aktivitäten ein, die beispielsweise über neu geöffnete oder geschlossene Issues und Kommentare informieren. Damit wird die effiziente Nutzung von Findalyze mit mehreren Benutzern vereinfacht, da man schnell überblicken kann, was sich in letzter Zeit verändert hat.

ISSUE	DATUM	BEWERTUNG	KUNDE	STATUS
Ungültiges Zertifikat für Domain itacgames.com	16. Okt. 2023	Kritisch	bWAPP	Offen
2 Sicherheitslücken von nginx auf hackthissite.org	4. Sept. 2023	Kritisch	HackThisSite	Offen
Neues Asset gefunden: git.hackthissite.org	4. Sept. 2023	Warnung	HackThisSite	Offen
Empfohlener DNS-Eintrag für SPF fehlt für Domain git.hackthissite.org	4. Sept. 2023	Warnung	HackThisSite	Offen
Ungültiges Zertifikat für Domain gqb.hackthissite.org	21. Aug. 2023	Kritisch	HackThisSite	Offen
Abgelaufenes Zertifikat auf Domain gqb.hackthissite.org	21. Aug. 2023	Kritisch	HackThisSite	Offen
Ungültiges Zertifikat für Domain irc-www.hackthissite.org	21. Aug. 2023	Kritisch	HackThisSite	Offen
Abgelaufenes Zertifikat auf Domain irc-www.hackthissite.org	21. Aug. 2023	Kritisch	HackThisSite	Offen
Abgelaufenes Zertifikat auf Domain www.hackthissite.org	21. Aug. 2023	Kritisch	HackThisSite	Offen
Neues Asset gefunden: assets.tryhackme.com	24. Juli 2023	Warnung	TryHackMe	Offen

EVENT	KUNDE	ZEIT
Issue automatisch gelöst	bWAPP	vor 8 Stunden
Issue automatisch gelöst	bWAPP	vor 8 Stunden
Issue automatisch wiedereröffnet	TryHackMe	vorgestern
Issue automatisch gelöst	TryHackMe	vor 3 Tagen
Issue automatisch gelöst	bWAPP	vor 6 Tagen
Issue automatisch gelöst	bWAPP	vor 6 Tagen
Issue automatisch gelöst	bWAPP	vor 6 Tagen
Issue automatisch gelöst	bWAPP	vor 7 Tagen
Neues Issue gefunden	bWAPP	vor 7 Tagen
Issue automatisch gelöst	bWAPP	vor 8 Tagen
Issue automatisch gelöst	bWAPP	vor 8 Tagen
Issue automatisch wiedereröffnet	bWAPP	vor 10 Tagen

Findalyze®

Attack Surface Explorer

Issues

Alle Issues stets im Blick. Dank der Filterfunktionen behalten Sie alles Blick.

Historie

Auch in 2 Jahren noch wissen was war. Findalyze behält alle Informationen und Kommentare je Issues.

Erklärung und Rat

Findalyze zeigt Ihnen nicht nur Probleme auf, sondern auch eine Lösung.

The screenshot shows the Findalyze web interface. On the left, there is a table of issues with columns for 'ISSUE', 'DATUM', 'BEWERTUNG', and 'STATUS'. The table lists various issues such as 'Ungültiges Zertifikat für Domain itsecgames.com' and 'Asset nicht mehr gefunden: mail1.mmebba.com'. On the right, there is a detailed view of a specific issue titled '6 Sicherheitslücken von JQuery auf itsecgames.com'. This view includes the issue ID (39314), the time and date (26. Juni 2023 13:34), the category (Sicherheitslücke), and the severity (Schweregrad (CVSS) 4.3 / 10.0). It also lists the domain (itsecgames.com) and the technology (jQuery). The detailed view lists several CVEs (CVE-2020-11029, CVE-2020-11023, CVE-2019-1358, CVE-2012-6708, CVE-2019-8531, CVE-2011-4669) and provides a description of the vulnerabilities and a link to the jQuery library.



Keine lokale Installation notwendig (SaaS)



Nur Domain oder Mailadressen als Startpunkt nötig



Multimandantenfähig



Alle Ergebnisse auf einem Dashboard

Funktionen

Scan

- E-Mail Passwort-Leak
- Besitzer von IP-Adressen
- Offene Ports
- Sicherheits-Header
- Sicherheitslücken
- SPF Einträge
- Zertifikate
- Zugangsdaten
- Verschwundene Assets
- Neue Assets
- Blacklist-Einträge
- Vergessene sensible Daten
- Erkennung unverschlüsselter Webseiten
- Subdomain-Takeover Schwachstellen
- E-Mail Benachrichtigung
-

Zugriffsverwaltung

- Multi-User
- Mandantenfähig
- Rechteverwaltung für Benutzer

Schnittstellen

- Anbindung externer Ticketsysteme
- Anbindung externer Monitoring-Software
- Rest-API

Export

- CSV
- PDF Bericht

IHR FINDALYZE PARTNER



Informationstechnik Klumpp GmbH

Theodor-Kaufmann-Str. 31 | 77933 Lahr

Telefon: +49 (0) 7821 99 666-0

E-Mail: info@klumpp-systeme.de

<https://www.klumpp-systeme.de>



AIS Advanced IT Security Solutions GmbH | Ensheimer Straße 42 | 66386 St. Ingbert | Germany

www.findalyze.com